

| | |
|---|-----|
| SOC Playbooks | 4 |
| old Archived Playbooks | 5 |
| old Copy of Application of Risk Assessment | 7 |
| old CVD Reward Payout | 10 |
| old Datacenter Manual Wireless Audit | 12 |
| old DSR - HIPS General/PCI Actionable Malware | 16 |
| old DSR - ModSec Review | 21 |
| old DSR - ModSec Review - PKI | 24 |
| old DSR - PCI Linux Logon Report | 26 |
| old DSR - PCI Windows Logon Report | 30 |
| old DSR - PKI Linux Logon Report | 34 |
| old DSR - PKI Windows Logon Report | 37 |
| old GenPact Transition Tracking | 41 |
| old HaveIBeenPwned (Draft) | 47 |
| old HIVE Incident Testing | 50 |
| old Incident Prioritization | 51 |
| old Major Incident Workflow | 53 |
| old Monthly ASV Audit Scans (PCI) | 56 |
| old Monthly External Vulnerability ASV Audit Scans-Qualys (PCI and PKI) | 70 |
| old Monthly Internal Audit Scan | 76 |
| old Security@ General Inbox (Old) | 79 |
| old Server Patching Playbook - Vulnerability Management | 84 |
| old ServerScans Playbook - On-demand and On-build | 93 |
| old Suspicious User Behavior - Monitoring and Response | 98 |
| old Vendor Advisory Handling Playbook | 102 |
| old Employee Phishing Incidents | 106 |
| old Retired - IsItBad Process | 113 |
| old Incident Escalation Procedures | 120 |
| old Removing Old Okta Factors - Steps and FAQ | 121 |
| old ServiceNow Create Trend AV (EMEA) Incident From SEC Incident | 123 |
| old InfoSec/CMDB/SNOW Support | 125 |
| old CMDB - Check for Placeholder CI | 127 |
| old CMDB - Duplicate CI check | 128 |
| old HackerOne Process | 129 |
| old MVR Playbook | 131 |
| old IWSaaS/URL Reclassification Requests | 136 |
| old OnCall Escalation Procedure | 139 |
| Data Loss Reporting | 140 |
| Disable Employee Access | 141 |
| Reviewing Call Recording in ORECX | 143 |
| Security@ Archive | 145 |
| Security@ General Inbox | 147 |
| Revoke Compromised Certificate | 150 |
| ServiceNow General Usage | 152 |
| old Email Un-Quarantine Requests | 155 |

| | |
|--|-----|
| Tanium Useful queries | 157 |
| How to enter a Vertigo child VM | 158 |
| Using HUE to Query Hadoop | 159 |
| KnowBe4 PhishER | 161 |
| OnCall Escalation Procedure Old | 166 |
| Alert Tuning Request | 170 |
| DSR Failed Logons Review | 171 |
| DSR - FIM Review Procedure | 175 |
| DSR - PCI Cloud Review Procedure | 179 |
| DSR - SQL Failed Login Reports | 181 |
| Device Environment | 184 |
| Employee Workstation Intrusion Incidents | 185 |
| IDS Alerts Procedure | 188 |
| Windows Log Clear Event Procedure | 190 |
| User Altered the Windows System Clock | 191 |
| System Activity Investigations | 193 |
| Endpoint Intrusion Incidents v2 Draft | 198 |
| Event Comments Standard | 203 |
| Quarterly Control Audit (WIP) | 206 |
| Catalog of Investigation Data / commands | 209 |
| Employee Compromise Containment | 220 |
| Credential Mitigation | 224 |
| Security@ and SecurityBreach Mailbox Process | 229 |
| How-To Guides | 233 |
| Hostname Conventions and Machine Information | 234 |
| How to use Kentik | 237 |
| Convert shopperIDs to CustomerIDs | 240 |
| Custom Assessment and Remediation Scanning and Reporting | 242 |
| AWS Account Investigations | 245 |
| AWS Overview | 246 |
| AWS Logs | 249 |
| Using Athena to Search Historical Logs | 253 |
| Hosting VS Non-Hosting Content | 257 |
| Common Customer Environments | 261 |
| Defender for O365: Email Un-Quarantine Requests | 262 |
| Email DLP Incident | 264 |
| Employee Phishing Incidents | 268 |
| Phishing Reporting Architecture | 277 |
| Proofpoint TRAP Workflows | 278 |
| Email Architecture | 279 |
| Investigating SentinelOne Hologram (Attivo) Activity | 281 |
| SentinelOne Deep Visibility Log Headers | 286 |
| Monitoring Standup Procedure - needs to be redone! | 314 |
| Alert Analysis Playbook | 315 |
| Identity Identification Playbook | 324 |

| | |
|--|-----|
| AWS Defense Evasion Delete Cloudtrail | 331 |
| Delete ShadowCopy With PowerShell Playbook | 334 |
| Mission Control Events WorkFlow | 337 |
| Powershell Creating Thread Mutex Playbook | 347 |
| Powershell Fileless Process Injection via GetProcAddress | 350 |
| Slack Reports Workflow | 354 |
| Splunk Events WorkFlow | 357 |
| SentinelOne IOC Block Playbook | 366 |
| Workstation Quarantine (Draft) | 372 |
| Blocking Velia Brand IPs Procedure | 377 |
| Compromised Workstation Playbook | 379 |
| Lateral movent investigation - in progress | 384 |
| SentinelOne URL blocking | 390 |
| Forcefield-support : IP Unblock request | 395 |
| Phishing email analysis in Proofpoint | 398 |
| Remediate customer hosting account | 406 |
| Communication Procedure (Draft) | 407 |
| Responding to Security Reports in Slack | 410 |
| OnCall Escalation Procedure | 413 |
| Alert Tuning/Changes Request | 418 |
| VDI Login via User Impersonation | 420 |
| Spoofed Emails analysis | 424 |
| Device Intrusion Incidents | 428 |
| Identifying Persistence (Draft) | 435 |
| GCSO Ticket standards | 437 |
| Security MailBox Integration with Splunk | 441 |
| Investigation and Response Workflow in ES8 v1 | 452 |
| Communication templates | 461 |
| File collection from OneDrive using S1 | 469 |
| Incident Response mindset and OODA loop | 473 |
| Blocking Domains using Splunk Playbook | 476 |
| Forensic collection playbook | 485 |
| How to create a PhishLabs ticket | 491 |
| Prisma URL Filtering Playbook | 499 |
| How to view SQLite raw data in more readable format | 509 |
| Playbook for GDDY_AWS_Root_Account_Activity_Detected | 514 |
| IDS Alert Playbook | 517 |
| OnCall Escalation Procedure - MC Playbook | 524 |
| Volatility cheat sheet | 529 |
| RF Domain Abuse Alert Playbook | 540 |
| Abnormal Connection count from hosting to non hosting alert handling playbook- Draft | 543 |
| High Volume Data Exfiltration to Cloud Storage services | 547 |
| How to upload Proofpoint Trap logs to Splunk | 551 |

SOC Playbooks

Table of Contents

- [Table of Contents](#)
- [Current Process](#)
- [Knowledge Base](#)

Current Process

Create procedure playbook from template

| Title | Creator | Modified |
|--|-----------------|--------------|
| Monitoring Standup Procedure - needs to be redone! | David Hernandez | May 19, 2025 |
| Employee Phishing Incidents | David Hernandez | Jan 24, 2025 |
| Identity Identification Playbook | Darko Zecic | Feb 29, 2024 |
| Alert Analysis Playbook | Darko Zecic | Oct 11, 2023 |

Knowledge Base

old Archived Playbooks

- [old Copy of Application of Risk Assessment](#)
- [old CVD Reward Payout](#)
- [old Datacenter Manual Wireless Audit](#)
- [old DSR - HIPS General/PCI Actionable Malware](#)
- [old DSR - ModSec Review](#)
- [old DSR - ModSec Review - PKI](#)
- [old DSR - PCI Linux Logon Report](#)
- [old DSR - PCI Windows Logon Report](#)
- [old DSR - PKI Linux Logon Report](#)
- [old DSR - PKI Windows Logon Report](#)
- [old GenPact Transition Tracking](#)
- [old HaveIBeenPwnd \(Draft\)](#)
- [old HIVE Incident Testing](#)
- [old Incident Prioritization](#)
- [old Major Incident Workflow](#)
- [old Monthly ASV Audit Scans \(PCI\)](#)
- [old Monthly External Vulnerability ASV Audit Scans-Qualys \(PCI and PKI\)](#)
- [old Monthly Internal Audit Scan](#)
- [old Security@ General Inbox \(Old\)](#)
- [old Server Patching Playbook - Vulnerability Management](#)
- [old ServerScans Playbook - On-demand and On-build](#)
- [old Suspicious User Behavior - Monitoring and Response](#)
- [old Vendor Advisory Handling Playbook](#)
- [old Employee Phishing Incidents](#)
- [old Incident Escalation Procedures](#)
- [old Removing Old Okta Factors - Steps and FAQ](#)
- [old ServiceNow Create Trend AV \(EMEA\) Incident From SEC Incident](#)
- [old InfoSec/CMDB/SNOW Support](#)
- [old HackerOne Process](#)
- [old MVR Playbook](#)
- [old IWSaaS/URL Reclassification Requests](#)
- [old OnCall Escalation Procedure](#)
- [Data Loss Reporting](#)
- [Disable Employee Access](#)
- [Reviewing Call Recording in ORECX](#)
- [Security@ Archive](#)
- [Security@ General Inbox](#)
- [Revoke Compromised Certificate](#)
- [ServiceNow General Usage](#)
- [old Email Un-Quarantine Requests](#)
- [Tanium Useful queries](#)
- [How to enter a Vertigo child VM](#)
- [Using HUE to Query Hadoop](#)
- [KnowBe4 PhishER](#)
- [OnCall Escalation Procedure Old](#)
- [Alert Tuning Request](#)
- [DSR Failed Logons Review](#)
- [DSR - FIM Review Procedure](#)
- [DSR - PCI Cloud Review Procedure](#)
- [DSR - SQL Failed Login Reports](#)
- [Device Environment](#)
- [Employee Workstation Intrusion Incidents](#)
- [IDS Alerts Procedure](#)
- [Windows Log Clear Event Procedure](#)
- [User Altered the Windows System Clock](#)
- [System Activity Investigations](#)
- [Endpoint Intrusion Incidents v2 Draft](#)
- [Event Comments Standard](#)
- [Quarterly Control Audit \(WIP\)](#)

old Copy of Application of Risk Assessment

Table of Contents

- [Table of Contents](#)
- [Procedure Information](#)
- [Procedure](#)
 - [Vulnerability Reported](#)
 - [Complexity](#)
 - [System Affected](#)
 - [Compensating Controls](#)
- [Procedure Diagram](#)
- [Procedure Resources](#)
 - [Internal Resources](#)
 - [External Resources](#)
 - [Communication Template](#)
- [Procedure Time Table/Reviews](#)

Procedure Information

ⓘ DELETE THIS AFTER COMPLETING - This Section is to give a high level overview of the steps that get taken to get into this current procedure if any other inputs lead up to this, so that it is clear. An example for a vulnerability assessment has been given the idea here is to be able to reference any other step from any other point in the process, and the creator would then link the procedure documents for the various inputs and outputs as it progresses. Please delete the contents of the table that was provided as an example.

| Goal/Intent | Input | Medium | Output |
|----------------------------------|------------------------------|-------------------------|----------------------------------|
| Gain Security's Approval/Opinion | ESA | x.co/ESASubmit | SRA Epic/Story & RoE |
| Assessment Scope | SRA Epic/Story & RoE | Meeting/Slack | Assessment Plan & Time Frame |
| Assessment Work | Assessment Plan & Time Frame | Meeting/Slack | Report & Deliverables |
| Assessment Delivered | Report & Deliverables | Report Email/Sharepoint | Approvals |
| Assessment Close | Approvals | SNOW | Transition to Problem Management |

Procedure

Vulnerability Reported

Once a vulnerability has been reported to security it will go through a decision gate depending on what the base CVSS scoring of the vulnerability is. At the most basic level, these gates will only apply to CVSS scores that are at least a High in ranking. There will be edge cases where mediums and lows may be upgraded to High but that will be taken on a case to case basis and does not apply for the overall structure described here. Please follow the instructions below to appropriately rate a vulnerability that is discovered.

Complexity

- Can the vulnerability be exploited with common tools such as metasploit, or can it be scripted because of its simplicity
- Is there poc code available (can check exploit-db, metasploit, securityfocus, etc.)
- Is there an active TA that's exploiting it in the wild or any news of it being exploited
- If any above true, then move to the systems affected gate, otherwise this will remain as a high

System Affected

- Look up system in CMDB to find out if it's public
- Look up system in CMDB to find out what service tier it belongs to
- If system is public or in tier 0/1 then the vulnerability is automatically a critical
- Else move through next phase

Compensating Controls

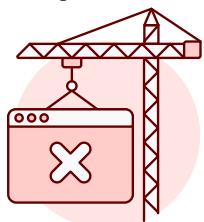
- Work with service owner to determine what compensating controls are in place in regard to the specifics of the vulnerability
- Work with security teams associated to relevant compensating controls based on the vulnerability
- If compensating controls exist the vulnerability will remain a high or be downgraded to a high, else it will turn into a critical

Procedure Diagram



Oops, Diagram Unavailable

This diagram cannot be displayed. It may have been moved, deleted, or you do not have permission to view it.



Oops, Error 500!

Diagram Unavailable

Our system is currently under maintenance. Reach out to your administrator for a fix.



You have an unpublished draft.

- ⓘ DELETE THIS AFTER COMPLETING - Please create a gliffy diagram detailing out this procedure for a visual representation for how this procedure works

Procedure Resources

- ⓘ DELETE THIS AFTER COMPLETING - Please link any internal or external resources that assist with this procedure, this should be links other than the inputs/outputs as those should be linked in the table above, so this may be links like to the nessus scanner or any other documentation that may be referenced as additional reading/study for the procedure

Internal Resources

- <Links>

External Resources

- <Links>

- ⓘ DELETE THIS AFTER COMPLETING - If this procedure is likely to be communicated out to large groups of people e.g., DevOps or any other large org, or it has the capability of traveling up the chain pretty heavily, work with corporate comms to build a template for communication and place that information in the panel below or any other copy paste type communication that may be useful for the procedure.

Communication Template

Communication Name

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean libero risus, tristique viverra tortor eu, **VARIABLE** accumsan pellentesque dolor. Maecenas euismod, tellus ac vestibulum viverra, nulla ligula fermentum turpis, ut blandit dui sapien ac purus. Mauris ut nunc ante. Fusce nec arcu magna. Proin eget mattis quam.

Procedure Time Table/Reviews

- ① **DELETE THIS AFTER COMPLETING** - Please track the dates for this procedure creation and all other relevant dates. The procedure should be reviewed by someone other than the original author to see if there are gaps missing within the document, and afterwards should be reviewed at an annual basis at minimum to ensure relevancy.

| Comment | Date | Commenter |
|--------------------|----------|-------------|
| Procedure Defined | xx/xx/xx | <your name> |
| Procedure Tested | xx/xx/xx | <your name> |
| Procedure Reviewed | xx/xx/xx | <your name> |

old CVD Reward Payout

⚠ Deprecated Process

This process is no longer in use and exists only to provide historical information. Please refer to the [old Security@ General Inbox \(Old\)](#) process for current state.

Table of Contents

- [Expectations](#)
- [Process Workflow](#)
- [Initial Report Validation](#)
- [Calculating Reward Offering](#)
- [Issuing Rewards](#)
- [Resources](#)
 - [Internal](#)
 - [External](#)
 - [Communication Templates](#)

Expectations

At this time GoDaddy does not operate a formal Bug Bounty program, however we have been asked to be receptive to external reporters who are requesting a reward in exchange for providing us with valuable report of a vulnerability in our services. This means that we must be able to quantify the threat level of a reported vulnerability and tie that to an excepted reward value, provide an approved method for issuing rewards, and have an understanding of the limitations and exceptions surrounding these reports.

Some basic guidelines around handling these requests are as follows:

1. Most CVD type reports should be directed initially to the GCSO via the [Security@](#) mailbox, however we may receive reports via various internal or external avenues.
To ensure we consolidate these for the purpose of tracking **all reports outside of Security@ should be redirected**.
2. While we have official communications that suggest that a reward is possible, **we do not guarantee rewards to reporters in communications**.
3. Whether or not we decide to issue a reward, we must ensure that **all communications are aligned with public documentation**.
 - a. [Coordinated Vulnerability Disclosure Policy](#)
 - b. [Coordinated Vulnerability Disclosure - GoDaddy Help Page](#)

Process Workflow



Initial Report Validation

For the majority of reports the GCSO team will not be directly responsible for validating if a reported vulnerability exists. However it is possible for the GCSO to make the initial determination as to whether or not a report *could* be granted a reward based on whether or not it complies with our [Coordinated Vulnerability Disclosure Policy](#). Per this policy, we do not accept the following types of reports for:

- Non GoDaddy Domains
- GoDaddy Hosted Customer Content (Websites, Services, Etc.)
- Third-party Programs and Plug-ins

ⓘ Regarding Non-GoDaddy Domains

Because we potentially will receive reports for domains that not [GoDaddy.com](#) (due to EMEA Brand support) it is important to note that for our consideration we will consider ANY GoDaddy owned corporate domain.

In addition to these requirements our policy discourages the following types of reports/techniques:

- DoS, brute force, user enumeration or DDoS attacks
- Physical attacks
- Phishing attacks
- Any bug that relies on Social engineering
- CRIME/BEAST attacks
- Logout CSRF
- Banner or version disclosures
- Missing SPF records
- Directory listing (unless sensitive data can be found)
- Blackhat SEO techniques

- Any bug that relies upon an outdated browser

⚠ GoDaddy will not accept reports from automated vulnerability scanners.

Calculating Reward Offering

Once a vulnerability report has passed our initial validation we will need to follow current SOP to direct the report to the appropriate parties for review. During this review a CVSS Score should be determined for the reported vulnerability. This will be used to determine the payout amount that a reporter is eligible for in most cases. This can be adjusted with the approval of CISO leadership.

CVSS Reward Matrix

| Internal CVSS Score | TI/VM Recommendation (Where CVSS N/A) | Reward Value |
|---------------------|--|--------------|
| 10 | Critical | \$500.00 |
| 7-9 | High | \$250.00 |
| 4-6 | Medium | \$100.00 |
| 1-3 | Low | \$0.00 |

If we are unable to make a determination based on the CVSS or at the recommendation of our Threat Intel or Vulnerability Management teams this *MUST* be escalated to leadership for determination.

Issuing Rewards

Approved rewards will be issued by leadership upon written acceptance of the reward by the reporter. The current method for issuing CVD payouts to our reporters is via Amazon Gift card. This requires that an authorized individual purchase the gift card via a p-card from the appropriate Amazon account. The process for issuance of rewards is as follows:

1. Management is notified via email of a reward request and the analyst provides a summary of the findings and a suggested reward value.
 - [Example](#)

SEC0049337 - User reported a vulnerability which could allow a TA to acquire sensitive account data including the account PIN for a target that was signed into their account. We had actually closed the matter at one point and the reporter continued to follow up to ensure the matter was closed. I am recommending we reward this as a HIGH (\$250.00)
2. Management determines if the reward request is valid and approves the appropriate reward amount via reply.
3. The reporter is notified and we request that they provide us with the address for delivery of the reward to confirm their acceptance.
4. Upon confirmation, the details are resubmitted to management for issuance.
5. Management signs into the Amazon account and issues a reward with the following information:
6. Once management confirms that the reward has been issued the reporter is notified.

Resources

Internal

- [GCSO Process - Security@ General Inbox](#)
- [VulnMgmt Process - Major Vulnerability Response \(MVR\)](#)
- [Coordinated Vulnerability Disclosure Policy](#)
- [Coordinated Vulnerability Disclosure - GoDaddy Help Page](#)

External

- [CVSS_v3 User Guide](#)
- [NIST CVSS_v3 Calculator](#)

Communication Templates

[Need More Info + Reward Request](#)

➢ [Expand source](#)

old Datacenter Manual Wireless Audit

Table of Contents

- General Information
 - Process Summary
 - Process-Specific Definitions
- Process Workflow
- Process Outline and Details
 - General Outline
 - Process Details
 - Step 2 - Route Maps
 - Step 2A - Sweep Using Mac OSX Airport
 - Mac OSX has a built-in Wireless Diagnostic tool which can be used to perform this sweep. The expected distance at which you should be able to detect an access point is approximately 150ft) [Wikipedia] .
 - Step 6 - Completing the Wireless Review
 - Template Details
 - This template has some functions defined which complete several initial review actions.
- FAQs
 - What are SSID, BSSID and RSSI and why do we review them?
 - What exactly is a Rogue Access Point?
- Resources and Definitions
 - Internal Resources
 - External Resources
 - Communication Templates
 - Associated Audit Controls / Requirements

General Information

| | |
|-----------------------|--|
| Responsible Team | Global Cyber Security Operations (GCSO) |
| Process Owner | Provide an individual contributor or team contact that handles initial process questions or requests. @David Dubois (Deactivated) |
| Last Review Date | @David Dubois (Deactivated) 2019-09-13 |
| Escalation Contact(s) | @David Dubois (Deactivated) |
| Requests for Updates | Via Email or GCSO JIRA |

Process Summary

This process provides direction for the completion of a physical walkthrough wireless audit for the Perimeter (S2) and Buckeye (P3) datacenters. This review must be performed on a quarterly cadence to meet PCI compliance requirements.

Process-Specific Definitions

- **Authorized Networks:** In general, GoDaddy has two enterprise networks (SSID **Earth** and **Moon**) which are expected at most corporate locations. These are to be identified by both SSID and BSSID to be considered authorized.
- **Rogue Access Point (Rogue AP):** An access point which is unexpected on the authorized networks or is attempting to mimic authorized networks.

Process Workflow



Process Outline and Details

General Outline

1. Travel to the datacenter in question. Access requests can be created here: [Employee Restricted Area Access](#)
2. Using the [provided map\(s\)](#) as a guideline, perform a sweep of the location.

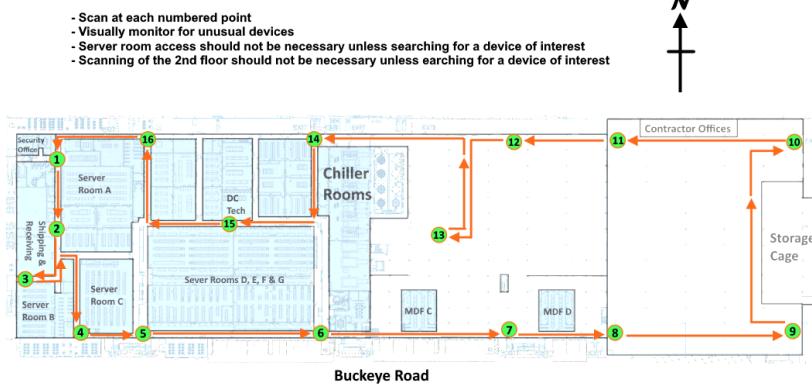
- a. At the indicated checkpoints, perform a scan of the wireless environment and record.
 - i. If only authorized networks are identified, continue to the next checkpoint.
 - ii. If unauthorized networks are identified, record for continued testing and continue to the next checkpoint.
- 1. At each checkpoint, determine if the signal for any unauthorized networks have changed.
- 3. Once all checkpoints are scanned, compile the data into the report CSV file and review for evidence of Rogue APs:
 - a. Did any unauthorized access point reach a RSSI above -85dBm?
 - b. Did any unauthorized access point have a stronger signal near the central points of the walkthrough?
 - c. Did any unauthorized access point attempt to use an SSID which spoofed or was similar to an authorized network device?
- 4. If a Rogue AP was identified:
 - a. Locate the device, take a picture of the device prior to removal, and confiscate if possible.
 - b. Generate a ticket to document findings and action.
- 5. At this point no further action is required at the datacenter directly.
- 6. Compile the Wireless Review for the location.
- 7. Copy the report file to the evidence storage location and update the [/wiki/spaces/VULNMGMT/pages/76588626](#) and associated JIRA (if exists).

Process Details

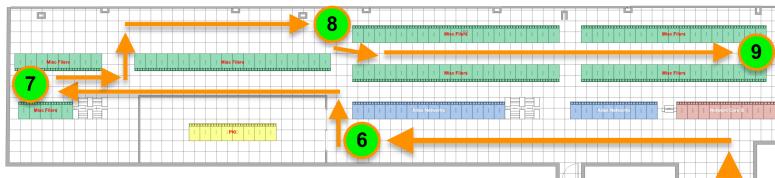
Step 2 - Route Maps

» P3 (Buckeye) Datacenter

P3 Wireless Scan Route

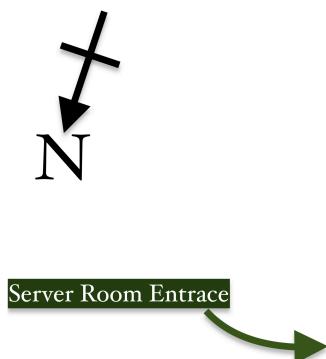


» S2 (Perimeter) Datacenter



S2 Wireless Scan Route

- Scan at each numbered point
- Visually monitor for unusual devices



Step 2A - Sweep Using Mac OSX Airport

Mac OSX has a built-in Wireless Diagnostic tool which can be used to perform this sweep. The expected distance at which you should be able to detect an access point is approximately 150ft) [\[Wikipedia\]](#).

To perform this sweep:

1. Locate the **airport** utility on your Mac (Path: /System/Library/PrivateFrameworks/Apple80211.framework/Resources/).
2. Run the **airport -s** command to scan the environment.
3. To easily capture the data for later use, this can be written to a file on the system.

Mac OSX Scan Example

» Expand source

A python3 script was developed to provide a quick method of running, parsing and capturing this data during walkthroughs: [wireless_scan.py](#)

Using wireless_scan.py

» Expand source

Step 6 - Completing the Wireless Review

After completing the location walkthrough you will need to compile the data into a report for consumption by the audit team(s). A sample of this report can be found here → [Wireless Report Template](#)

To complete this report, you need to do the following:

1. Copy the list outputs to the **ScanLog** table on the ScanLog tab on the document, be sure not to overwrite the pre-configured fields (Authorized?, AuthBSSID_1, AuthBSSID_2)
2. Go to the Network page and Right-click → Refresh the pivot table to generate the Networks list.
3. Go to the Review tab:
 - a. Review the SSID auto-review in the upper-left.
 - b. Complete the Review table by generating a unique list of SSIDs and entering the appropriate information.
 - c. Add your name, the date, and summary to the upper-right fields.
 - d. Save the document as YYYY-MM-DD_S2/P3_Wireless_Review.xlsx (ex. 2019-09-06_S2_Wireless_Review.xlsx)

Template Details

This template has some functions defined which complete several initial review actions.

1. The template contains 3 tables which match the tab names (Review, ScanLog, AuthNets)
2. The AuthNets table is locked to prevent accidental modification ("godaddy") , and contains a list of authorized WAP devices provided by Networking (John Flowers.)
3. The ScanLog table has 3 auto-generated fields based on data entered into the SSID/BSSID fields:
 - a. Authorized? → This field checks the SSID to determine if it should be an authorized network (Moon/Earth) and then compares the associated BSSID to the AuthNets table.
 - i. N/A → The SSID is not Earth or Moon
 - ii. No → The SSID is Earth or Moon AND the BSSID does not have a match in AuthNets
 1. Yes → The SSID is Earth or Moon AND the BSSID does have a match in AuthNets
 - b. AuthBSSID_1 → Populates with a BSSID if there is a match in "1st Radio MAC Address" in AuthNets
 - c. AuthBSSID_2 → Populates with a BSSID if there is a match in "2nd Radio MAC Address" in AuthNets
4. The Network tab contains a pivot table which breaks down the seen networks by SSID then BSSID based on the values in ScanLog
5. The Review tab has 4 auto-generated fields:
 - a. Unique SSIDs Seen → Counts unique values in the ScanLog SSID column
 - b. Unique BSSIDs Seen → Counts unique values in the ScanLog BSSID column
 - c. GoDaddy Authorized Networks (SSID Earth/Moon) → Checks the ScanLog SSID column for "Earth" or "Moon"; Returns "None" if no results; Returns "Present" if matches
 - d. Authorized Networks Confirmed by MAC Address? → Counts "Earth" and "Moon" entries with "Authorized?" = "Yes" over the sum of "Earth" and "Moon" values in the ScanLog SSID column.

The Process Details section is where depth can be provided for the various steps within your process. Not all steps may require this. Be sure to provide concise direction where possible. Examples are permitted if necessary.

FAQs

What are SSID, BSSID and RSSI and why do we review them?

When we are attempting to identify potential Access Points (APs) of interest we have a few things we can use to help us determine if these need further investigation.

- The **SSID** or "Name" of the network is a configurable field which provides the ability to set a friendly identifier for the network. In general, when a user is attempting to connect to a specific network they are going to be looking at the SSID and, as a result, a similar SSID could cause confusion and cause the user to access an incorrect network (ex. "GoDaddy" vs "Godady"). This is a common low-effort method of creating a malicious AP to siphon user traffic.
- The **BSSID** is the MAC address for the wireless connection. These are unique identifiers which can be used to verify if an unexpected device is connected to a network, even if it otherwise has the appropriate configurations. For example, an internal actor may be able to connect a device to the Earth network which would support the expected certificate authentication. At a glance, the SSID and function would appear valid, but by checking against known-good BSSIDs we can verify if that specific AP is supposed to be connected to the network.
- The **RSSI** is the signal level of the AP in question. As the RSSI value nears -10dBm [\[Wikipedia\]](#) the higher quality the signal becomes. In general, a device with an SSID of below -85dBm is unable to maintain a connection.

| Acceptable Signal Strengths | | | |
|-----------------------------|-----------|--|------------------------------|
| Signal Strength | TL;DR | Required for | |
| -30 dBm | Amazing | Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world. | N/A |
| -67 dBm | Very Good | Minimum signal strength for applications that require very reliable, timely delivery of data packets. | VoIP/VoWiFi, streaming video |
| -70 dBm | Okay | Minimum signal strength for reliable packet delivery. | Email, web |
| -80 dBm | Not Good | Minimum signal strength for basic connectivity. Packet delivery may be unreliable. | N/A |
| -90 dBm | Unusable | Approaching or drowning in the noise floor. Any functionality is highly unlikely. | N/A |

(Example provided by [MetaGeek](#))

What exactly is a Rogue Access Point?

In general, a Rogue AP is a device which has been added to a network without authorization [\[Wikipedia\]](#). For example, if an employee were to notice that the wireless signal were weaker in one section of the building and decide to attach an extender that was not specifically authorized by our Network teams, this would be considered a Rogue AP. For the purposes of this exercise, we extend the definition to include malicious intents surrounding APs such as attaching a device to the network with the explicit intention of sniffing traffic and/or the intentional configuration of a device to mimic an existing authorized network.

Resources and Definitions

Internal Resources

- [/wiki/spaces/VULNMGMT/pages/76588626](#)
- [Template - XLSX Report](#)
- [Scan Route - P3](#)
- [Scan Route - S2](#)

External Resources

- https://en.wikipedia.org/wiki/Template:802.11_network_standards
- https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf
- <http://pcidsscompliance.net/pci-dss-requirements/how-to-comply-to-requirement-11-of-pci-dss/>
- <https://wifitodd.com/2017/02/22/pci-dss-11-1-and-11-1-2-rogue-aps/>
- <https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-15-controlled-access/>

Communication Templates

- None

Associated Audit Controls / Requirements

| Audit Type | Process Specifics | Requirement | Requirement Label |
|------------|-------------------|--|-------------------|
| PCI | Full Process | Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis | PCI DSS 11.1 |
| CIS | Full Process | Detect wireless access points connected to the wired network <ul style="list-style-type: none"> Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network. | CIS 15.2 |

old DSR - HIPS General/PCI Actionable Malware

⚠ This process has been deprecated. Please see [System Activity Investigations](#) for the current process.

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [Process-Specific Definitions](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [Process Details](#)
 - [Trend Micro Hips Malware Scan](#)
 - [Run Tanium IR Gatherer to gather forensic data](#)
- [Process FAQs](#)
 - [What happens if "X"?](#)
 - [How can I determine if "Y"?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)

General Information

| | |
|-----------------------|---|
| Responsible Team | Intrusion Prevention Engineering (IPE) Slack: #intrusion_prevention Email: ipe@godaddy.com |
| Process Owner | @Former user (Deleted) |
| Last Review Date | 2018-11-19 @David Dubois (Deactivated) |
| Escalation Contact(s) | @Former user (Deleted) @Logan Zahn (Deactivated) @Former user (Deleted) |
| Requests for Updates | @Former user (Deleted) ipe@godaddy.com |

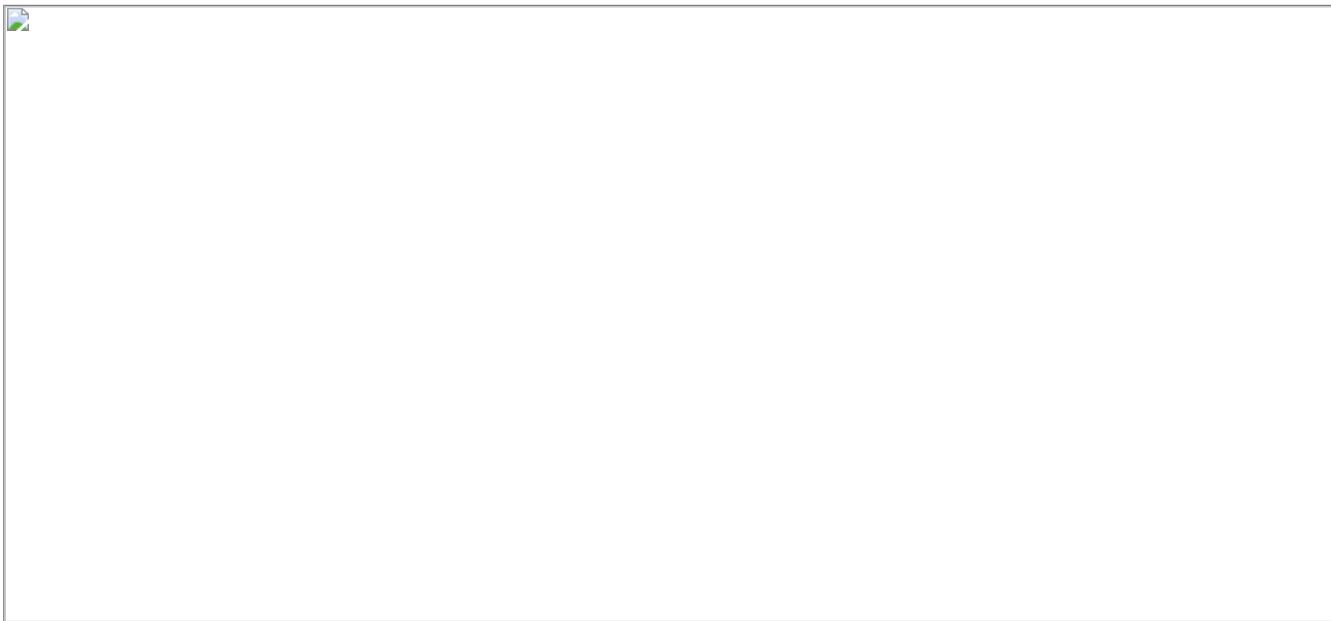
Process Summary

This process provides direction for the review of any alerts generated by the AV software. From this report other Child Tickets may be created to carry out Intrusion review for effected machines.

Process-Specific Definitions

- **Hosting System:** Any system that falls in the gdhosting.gdg domain
- **Malicious Files:** Any file that is malicious in nature as determined by review of the file

Process Workflow



Process Outline and Details

Incident Recording Guide

| Escalation to Tier 2 | |
|----------------------|--------|
| Assignment Group | TO ADD |
| | |

| Escalation to IPE | |
|-------------------|-----------|
| Assignment Group | ENG-GDIRT |
| Impact | 2 |
| Urgency | 2 |

General Outline

TIER 1

1. Gather the Hostname of the affected machine from the Ticket

Security Incident - SEC0026490

| | | | |
|--------------------|---|--------------------|--------------------------------|
| Number | SEC0026490 | Impact | 3 - Low |
| Priority | S - Minor | Urgency | 3 - Low |
| * State | Closed | Reporting Location | |
| * Assignment Group | ENG-Intrusion Prevention Engineering | Parent Ticket | |
| * Assigned To | Albert Rivera | Parent Task | |
| Incident Category | Intrusion | Associated Req | |
| Sub Category | Server | * Affected CIs | P3NW8SHG316.php1.gdhosting.gdg |
| Allowed Groups | | Affected Users | Al Fama |
| Allowed Users | | | |
| * Title | HIPS general/PCI Actionable Malware P3NW8SHG316.php1.gdhosting.gdg | | |
| * Summary | HIPS Jenkins: https://seckick-rproxy.cloud.dev.phx3.gdg/kibana/_/dashboard/HIPS-AV Job Name: Jenkins @timestamp: 2018-09-23T09:19:12.405-07:00 @version: 2018-09-23T09:18:04-07:00 cef-hips_cef_name: Jenkins cef-hips_cef_ext_filePath: D:\temp\temp\rad89B57.tmp\svchost.exe cef-hips_cef_ext_msg: Realtime cef-hips_cef_ext_act: Quarantine cef-hips_cef_ext_csi: None | | |

2. Run a Trend Micro AV Scan against the system using the "[Trend Micro HIPS Malware Scan](#)" Process

- a. Once done go ahead and log out of the Trend Micro HIPS Console

- i. Any new detections that are found will create a new ticket.

3. Determine if the host is a Hosting System

- a. This is done by taking the FQDN of the system and verifying if the domain contains "gdhosting.gdg".

4. If it is a hosting system continue following this process. If not; Immediately Escalate the ticket to Tier 2.

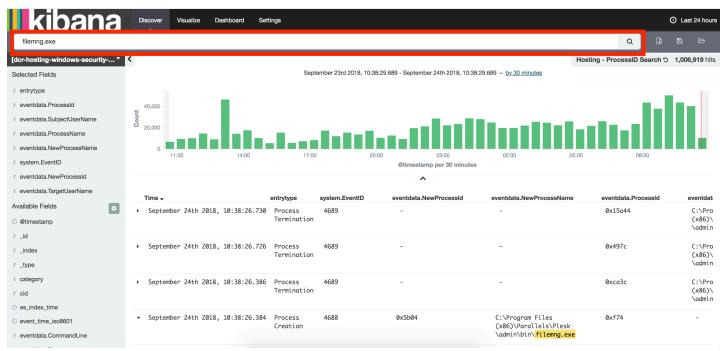
5. Gather both the Hostname and the File name from the original ticket.

- a. File Path will look like this in the ticket: "cef-hips.cefilePath: D:\temp\temp\rad89B57.tmp\svchost.exe"

- b. The File Name in this case is "svchost.exe"

6. Navigate to [Kibana](#). Then while that is still open select this link to take you to the correct location: [Process Search](#)

7. Once you are there you will want to put the File Name and Shortname of the host in the Search Window and run the search over the last 24 hours. Example Search would be "php-cgi.exe AND P3NW8SHG323"



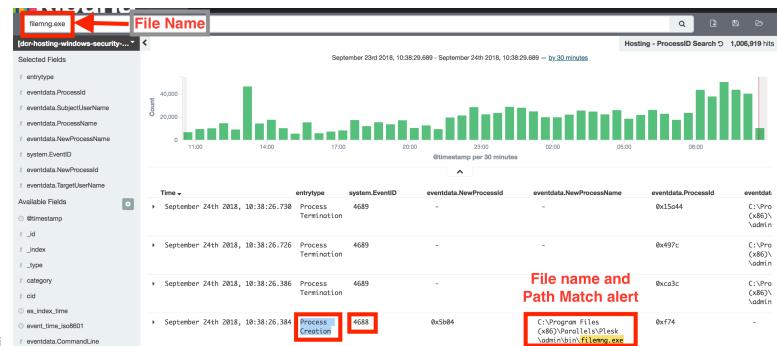
a.

8. If there are no results then the file wasn't executed. Proceed to step 12. Otherwise continue on.

9. If you see any results you will need to verify if the execution was blocked or not

a. Here are things you are looking for:

- i. A "Process Creation" that matched the File Name and Path



b. If you see the above log (or similar) this means the file attempted to run. The only thing that would block that would be App-locker

c. Verify if App-locker blocked it

- i. In the Process Creation event found in step 9.A you will want to make a note of the eventdata.NewProcessId field. This Number will be used to determine if it was blocked or not. It will be in a hex value (no conversion is needed) Similar to "0xb1c".
- ii. Look for logs of event id 4689 around that same time with an eventdata.ProcessId field that contains the "eventdata.NewProcessId" value from 9.C.i
- iii. If you don't see one it means the process is still running. Note in the Ticket and Immediately Escalate to Tier 2
- iv. If you do see one you will need to expand out the log and look to see if the eventdata.Status field contains "0xc0000364"
 - 1. If it does contain that value. Take a screenshot (or copy the log) and add it to the ticket with a note that states that Applocker blocked execution and continue to step 10.
 - 2. If it does not contain that value make a note that the process executed successfully in the ticket and escalate to Tier 2.

10. If you are at this point in the process you should have confirmed that the file in the initial alert didn't execute. Login to [Tanium](#)

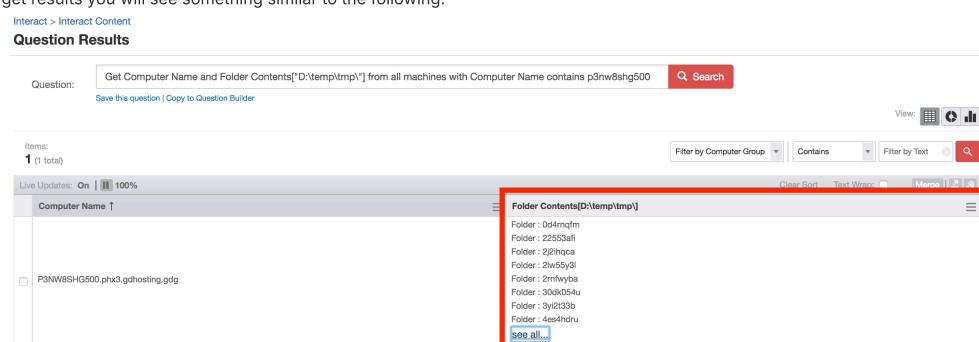
11. Go to "Interact"

12. In the search bar run the following search:

- a. Get Computer Name and Folder Contents["D:\\temp\\tmp\\rad89B57.tmp"] from all machines with Computer Name contains P3NW8SHG516
 - i. You will need to replace "D:\\temp\\tmp\\rad89B57.tmp" with the path that you got from the initial alert and replace "P3NW8SHG516" with the shortname of the host in your alert
- b. When the following pops use "Please select one of the following queries:" you will want to click on the first result.

13. If you see the following in the results "No machines matched the question." It means that the Tanium client isn't working. Note that in the ticket and close.

14. If you get results you will see something similar to the following:



a.

b. Select "See all..." to show all contents.

c. In the popup you are looking mostly for executable files such as .exe, .msi, .vbs, .ps1, and .bat files on windows systems.

d. If you see no indication of suspicious files note the Ticket and Close.

e. If you see indications of additional suspicious files take the new data and go back to Step 5 to look for process execution.

TIER 2

1. Gather Currently running processes and network connections from the affected system

a. Login to [Tanium](#)

b. Run the following command in the "Ask a Question" section:

- i. Get Computer Name and "Running Processes With Parent" and "Established Connections with MD5 Hash" from all machines with Computer Name contains p3nw8shg500

1. Replace p3nw8shg500 with the hostname from the ticket
- ii. Copy all results from Tanium in to the Ticket
2. If this is a hosting system check for Privilege Escalation. If not continue to step 3.
 - a. Navigate to [Kibana](#). Then while that is still open select this link to take you to the correct location: [Process Search](#)
 - b. Run a search on the Hostname looking for eventId of 4668
 - i. Example search: "P3NW8SHG323 AND system.EventID:4668"
 - c. Look for the malicious file in the results
 - d. Determine which user executed the original process
 - i. This is done by looking at the "eventdata.SubjectUserName" field
 - e. If this field contains a value that doesn't start with "Iusr" immediately note and continue to step 3.
 - f. If that field contains a value that starts with "Iusr" take the "eventdata.NewProcessId" value and look for any other processes that have that as their "eventdata.ProcessID"
 - g. If you find any other processes verify that the user that created the original process is the same as the user that created each child process.
 - i. If it is not then continue to step 3.
 - ii. **If it is the same user.** Note in the ticket that no privilege execution was seen and resolve.
3. Run Tanium's IR gatherer package on the affected system by following the [Process](#)
4. Document that IR Gatherer has been completed in the ticket and that the output is located in /home/genpact/
5. Escalate ticket to IPE

Process Details

Trend Micro Hips Malware Scan

Use the Trend Micro Hips Console to request a Malware Scan on a system

- a. Login to the [Trend Micro HIPS Console](#)
- b. Once logged in Select the "Computers" Tab at the top of the page
- c. Take the hostname from Step #1 and search for that host in the Computer list

| NAME | DESCRIPTION | PLATFORM | POLICY | STATUS |
|--------------------------------|-------------|------------------|---------------------|------------------|
| P3NW8SHG516.phx3.gdhosting.gdg | | Microsoft Win... | GD_WINDOWS_HOSTI... | Managed (Online) |
- i.
- d. Double click on the result in the "Computers" List in the bottom selection once the search completes. This will open up a new window.
 - i. If there is no system in the results Shorten your search to just the Shortname. Ex: FQDN: P3NW8SHG516.phx3.gdhosting.gdg. Shortname: P3NW8SHG516
 - ii. If there are still no results immediately escalate the ticket to ENG-GDIRT
- e. On the left hand side of the new window select "Anti-Malware"
- f. Scroll Down in the window to find "Full Scan for Malware".

Run Tanium IR Gatherer to gather forensic data

- a. Login to [Tanium](#)
- b. Ask the following question:
 - i. Get Tanium Client IP Address from all machines with Computer Name contains P3NW8SHG500
 1. Replace P3NW8SHG500 with the correct Hostname
 2. Make a note of the Value returned by "Tanium Client IP Address"
- c. Ask the following Question:
 - i. Get Computer Name from all machines with Computer Name contains [p3plcsirtstr01].
- d. Select the Computer name in the results and select "Deploy Action"
 - i. Fill in "IP Tables Rule Addition" in the "Deployment Package" section
 - ii. Below you will find a text box that is labeled "IP Address". Put the IP address that you noted from b.i.2 above in the text box
 - iii. Scroll to the bottom of the page and look for "Action Group:". It should be set currently to "Default". Select this dropdown and select "GD-Default"
 - iv. Select the "Show preview to Continue" button
 - v. Ensure that system ["p3plcsirtstr01.prod.phx3.gdg"] shows up in the results.
 - vi. Select Deploy Action
 - vii. Complete Re-authentication to perform deployment and verify that it completes
- e. Ask the following question:
 - i. Get Computer Name and Operating System from all machines with Computer Name contains P3NW8SHG500
 1. Replace P3NW8SHG500 with the correct Hostname from the ticket
- f. Select the Computer name in the results and select "Deploy Action"
- g. Select the correct package by which Operating System the endpoint is
 - i. Windows:
 1. "IR Gatherer - Collect Info To Central Server"

- ii. Linux:
 - 1. "IR Gatherer - Linux"
- h. Set the following options:
 - i. Method: SCP
 - ii. Destination: 68.178.213.185
 - iii. Username: genpact
 - iv. Password: <<REMOVED>>
 - v. Enable: Standard & Extended
 - vi. Action Group: GD-Default
- i. Select "Deploy Action"

Process FAQs

What happens if "X"?

"X" is caused by A,B or C. Can be handled by doing "D".

How can I determine if "Y"?

"Y" is determined by E or F. If "G", then sometimes "H".

Resources and Definitions

Internal Resources

[Trend Micro](#)

[Tanium](#)

External Resources

old DSR - ModSec Review

⚠ This process has been deprecated. Please see [ModSec Review](#) for the current process.

Table of Contents

- Table of Contents
- General Information
 - Process Summary
- Process Workflow
- Process Outline and Details
 - Incident Recording Guide
 - General Outline
 - Process Details
 - Dashboard Review
 - Child SECINC Review
 - Captured Metrics
 - Process FAQs
 - Which widgets are associated with IIS Modsec?
 - Which widgets are associated with QSC/Nemo Modsec?
- Resources and Definitions
 - Internal Resources
 - External Resources
 - Communication Templates

General Information

| | |
|-----------------------|---|
| Responsible Team | Intrusion Prevention Engineering (IPE) Slack: #intrusion_prevention Email: ipe@godaddy.com |
| Process Owner | @Former user (Deleted) |
| Last Review Date | 2018-11-14 by @Jonathan Wade (Deactivated) |
| Escalation Contact(s) | @Former user (Deleted) @Logan Zahn (Deactivated) @Former user (Deleted) |
| Requests for Updates | @Former user (Deleted) ipe@godaddy.com |

Process Summary

This process provides direction for the review of ModSecurity alerts across various environments. Environments which contain ModSecurity alerts for review fall within PCI or PKI scope. While the audit requirements themselves don't require that we take additional action on alerts this process will outline the scenarios in which additional action may be warranted and how to proceed.

Process Workflow

Process Outline and Details

Incident Recording Guide

| Incident Type | |
|------------------|-----------|
| Assignment Group | ENG-GDIRT |

| | |
|-------------------|---------------------|
| Incident Category | Intrusion |
| Sub Category | Server |
| Title | WAF Event - #IP |
| Summary | |
| Impact | 3 - Low |
| Urgency | 3 - Low |
| Log Entry Type | Other |
| Detection Method | Log Review - Kibana |

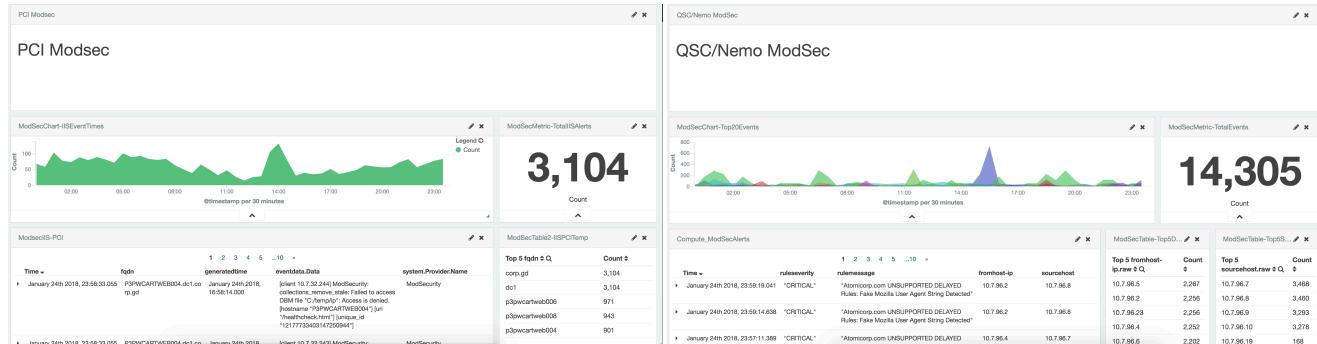
General Outline

1. DSR PKI WAF Event Ticket Generated at 12:00AM MST
2. Navigate to [Kibana](#). Then while that is still open select this link to take you to the correct location: [Kibana dashboard](#)
3. Follow Dashboard Review steps
4. If child ticket created, follow Child SECINC Review steps

Process Details

Dashboard Review

ⓘ It's important to note that due to oddities in Kibana, the widgets on the dashboard may shift around and not be organized correctly on subsequent page loads. Refer to Process FAQs for a listing of which widgets are associated with which log sources (IIS vs QSC/Nemo). You may need to re-organize the widgets on the dashboard into a more logical order.



1. Perform these steps separately for both the IIS Modsec and QSC/Nemo Modsec sections:
 - a. Review data for exceptionally anomalous behavior:
 - i. Review events over time for sharp spikes of events
 - ii. Review top sources for far outliers
 - iii. Review top destination for far outliers
 - iv. Review top rule hits (where applicable)
 - b. For identified anomalous behavior determine the TYPE of rule hit
 - i. SQLi/RCE are highest severity
 - ii. XSS/XSRF are medium severity
 - iii. Odd User-Agents, requests, scanning activity are low severity
 - c. Create a child ticket if
 - i. Over 100 events of high severity within 20 minutes
 - ii. Over 200 events of medium severity within 20 minutes
 - iii. Over 500 events of low severity within 20 minutes
 - d. When creating child ticket include the following:
 - i. Note affected destination IP
 - ii. Note source IP
 - iii. Link sample event, provide time frame of anomalous activity

Child SECINC Review

Check the following tools: (1), (2) & (3)

Document findings determine if "X"

Captured Metrics

- Metric A - Captured using E; (Required/Optional); Reporting example (if needed)
- Metric B - Captured using F; (Required/Optional); Reporting example (if needed)
- Metric C - Captured using G; (Required/Optional); Reporting example (if needed)

Process FAQs

Which widgets are associated with IIS Modsec?

1. ModSecChart-IISEventTimes
2. ModSecMetric-TotalIISAlerts
3. ModSecIIS-PCI
4. ModSecTable-Topo5DestIIS

Which widgets are associated with QSC/Nemo Modsec?

1. ModSecMetric-TotalEvents
2. Compute_ModSecAlerts
3. ModSecTable-Top5Destinations

Resources and Definitions

Internal Resources

External Resources

Communication Templates

| Communication Name |
|---|
| Placeholder content for communication template. |

Placeholder content for communication template.

old DSR - ModSec Review - PKI

⚠ This process is deprecated. Please see [ModSec Review](#) for the current process.

Table of Contents

- Table of Contents
- General Information
 - Process Summary
- Process Workflow
- Process Outline and Details
 - Incident Recording Guide
 - General Outline
 - Process Details
 - Dashboard Review
 - Captured Metrics
 - Process FAQs
- Resources and Definitions
 - Internal Resources
 - External Resources

General Information

| | |
|-----------------------|---|
| Responsible Team | Intrusion Prevention Engineering (IPE) Slack: #intrusion_prevention Email: ipe@godaddy.com |
| Process Owner | @ Logan Zahn (Deactivated) |
| Last Review Date | @ Logan Zahn (Deactivated) - 12/3 |
| Escalation Contact(s) | @ Former user (Deleted) @ Logan Zahn (Deactivated) @ Former user (Deleted) |
| Requests for Updates | @ Former user (Deleted) ipe@godaddy.com |

Process Summary

This process provides direction for the review of ModSecurity alerts across various environments. Environments which contain ModSecurity alerts for review fall within PCI or PKI scope. While the audit requirements themselves don't require that we take additional action on alerts this process will outline the scenarios in which additional action may be warranted and how to proceed.

Process Workflow

Process Outline and Details

Incident Recording Guide

| Incident Type | |
|-------------------|-----------|
| Assignment Group | ENG-GDIRT |
| Incident Category | Intrusion |
| Sub Category | Server |

| | |
|-------------------------|---------------------|
| Title | WAF Event - #IP |
| Summary | |
| Impact | 3 - Low |
| Urgency | 3 - Low |
| Log Entry Type | Other |
| Detection Method | Log Review - Kibana |

General Outline

1. DSR PKI WAF Event Ticket Generated at 12:00AM MST
2. Navigate to [PKI Kibana](#). Then while that is still open select this link to take you to the correct location: [Kibana dashboard - PKI Mod Sec](#)
3. Follow Dashboard Review steps
4. If child ticket created, follow Child SECINC Review steps

Process Details

Dashboard Review



1. Perform these steps separately for the PKI ModSecChart-Top20Events_PKI section:
 - a. Review data for exceptionally anomalous behavior:
 - i. Review events over time for sharp spikes of events
 - ii. Review top sources for far outliers
 - iii. Review top destination for far outliers
 - iv. Review top rule hits (where applicable)
 - b. For identified anomalous behavior determine the TYPE of rule hit
 - i. SQLi/RCE are highest severity
 - ii. XSS/XSRF are medium severity
 - iii. Odd User-Agents, requests, scanning activity are low severity
 - c. Create a child ticket if
 - i. Over 100 events of high severity within 20 minutes
 - ii. Over 200 events of medium severity within 20 minutes
 - iii. Over 500 events of low severity within 20 minutes
 - d. When creating child ticket include the following:
 - i. Notate affected destination IP
 - ii. Notate source IP
 - iii. Link sample event, provide time frame of anomalous activity

Captured Metrics

- **Metric A** - Captured using E; (Required/Optional); Reporting example (if needed)
- **Metric B** - Captured using F; (Required/Optional); Reporting example (if needed)
- **Metric C** - Captured using G; (Required/Optional); Reporting example (if needed)

Process FAQs

Resources and Definitions

Internal Resources

External Resources

old DSR - PCI Linux Logon Report

⚠ This process has been deprecated. Please see [DSR Failed Logons Review](#) for the current process.

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [Process Details](#)
 - [Graph Review](#)
 - [Log Review](#)
 - [Captured Metrics](#)
 - [Process FAQs](#)
 - [What happens if "X"?](#)
 - [How can I determine if "Y"?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)

General Information

| | |
|-----------------------|---|
| Responsible Team | Intrusion Prevention Engineering (IPE) Slack: #intrusion_prevention Email: ipe@godaddy.com |
| Process Owner | @Former user (Deleted) |
| Last Review Date | 2018-11-27 |
| Escalation Contact(s) | @Former user (Deleted) @Logan Zahn (Deactivated) @Former user (Deleted) |
| Requests for Updates | @Former user (Deleted) ipe@godaddy.com |

Process Summary

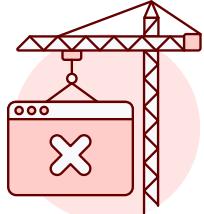
This process provides direction for the review of Linux logon events within PCI scoped environments to meet audit requirements. The process is designed to review logon events in an attempt to identify anomalous or malicious logon activity

Process Workflow



Oops, Diagram Unavailable

This diagram cannot be displayed. It may have been moved, deleted, or you do not have permission to view it.



Oops, Error 500!

Diagram Unavailable

Our system is currently under maintenance. Reach out to your administrator for a fix.



You have an unpublished draft.

Process Outline and Details

Incident Recording Guide

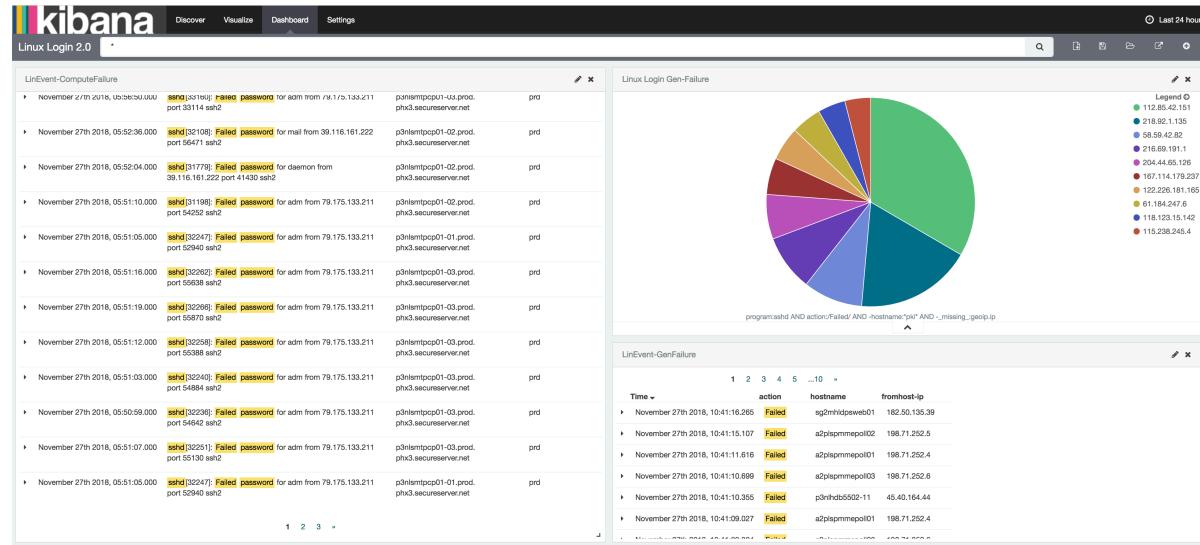
| Incident Type | |
|-------------------|------------------------|
| Assignment Group | ENG-GDIRT |
| Incident Category | Intrusion |
| Sub Category | Server |
| Title | PCI Linux Logons - #IP |
| Summary | |
| Impact | 3 - Low |
| Urgency | 2 - Medium |
| Data Type | Employee-Credential |
| Detection Method | Log Review - Kibana |

General Outline

1. Navigate to [Kibana](#). Then while that is still open select this link to take you to the correct location: [Kibana dashboard](#)
2. Review each IP listed in Upper Right Graph by following the "Graph Review" Process
3. Review All logs in the Left Pane looking for IP's with large numbers of results (50+) and follow "Log Review" Process

Process Details

Graph Review



- Top Five Failing IP Addresses: Select IP from upper right graph
- Perform a whois lookup on the IP Address. If the IP is owned by GoDaddy then create a SNOW ticket and Assign to IPE
- Using one of the below links to check the IP address to see if it is associated with malicious activity:
 - <https://www.abuseipdb.com/>
 - If the IP shows more than 10 results associated with "Brute Force", "SSH", "FTP" or "Hacking" proceed to step 4
 - https://www.talosintelligence.com/reputation_center
 - If the IP has a "Weighted Reputation" of Poor proceed to step 4
- Navigate to [Protect](#) and perform a search for the IP address if one is found proceed to step 7
- If you don't find any result note the result in the original DSR SNOW incident to document any IPs we block
- In the Protect UI select the Green "+" button and fill in the following:
 - Name should be the Name of the SNOW ticket you created the type of activity and the IP address being blackholed (Ex: SEC0030661 SSH_Brute_58.218.92.47)
 - Network should be the IP address as a /32
 - 58.218.92.47/32
 - TTL should be set for 1 day
 - Click Submit
 - Update ticket that the blackhole has been performed
- Back in Kibana do a search using the IP address you just searched
 - Example Query: 58.218.92.47
- Look at the 2 bottom Kibana tables for any successful logins
- If any are found copy logs and upload to the SNOW Ticket and immediately escalate to IPE
- If none are found close the ticket

Log Review

- In the Top left table look for any IP Addresses that are seen failing any authentication 50+ times
- If any are found complete the Graph Review process above

Captured Metrics

- Metric A** - Captured using E; (Required/Optional); Reporting example (if needed)
- Metric B** - Captured using F; (Required/Optional); Reporting example (if needed)
- Metric C** - Captured using G; (Required/Optional); Reporting example (if needed)

Process FAQs

What happens if "X"?

"X" is caused by A,B or C. Can be handled by doing "D".

How can I determine if "Y"?

"Y" is determined by E or F. If "G", then sometimes "H".

Resources and Definitions

Internal Resources

Kibana

Service Now

External Resources

[Talos](#)

[AbuseIPDB](#)

old DSR - PCI Windows Logon Report

⚠ This process has been deprecated. Please see [DSR Failed Logons Review](#) for the current process.

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [Process Details](#)
 - [Dashboard Review](#)
 - [Child SECINC Review](#)
 - [Captured Metrics](#)
 - [Process FAQs](#)
 - [What happens if "X"?](#)
 - [How can I determine if "Y"?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)
 - [Communication Templates](#)

General Information

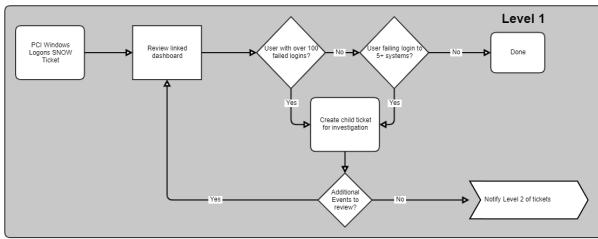
| | |
|-----------------------|---|
| Responsible Team | Intrusion Prevention Engineering (IPE) Slack: #intrusion_prevention Email: ipe@godaddy.com |
| Process Owner | @Former user (Deleted) |
| Last Review Date | 2018-11-14 by @Jonathan Wade (Deactivated) |
| Escalation Contact(s) | @Former user (Deleted) @Logan Zahn (Deactivated) @Former user (Deleted) |
| Requests for Updates | @Former user (Deleted) ipe@godaddy.com |

Process Summary

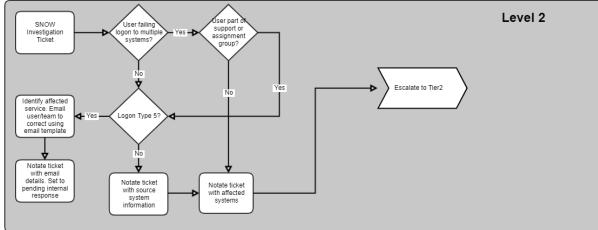
This process provides direction for the review of Windows logon events within PCI scoped environments to meet audit requirements. The process is designed to review logon events in an attempt to identify anomalous or malicious logon activity.

Process Workflow

IPE - PCI Windows Logons Report



IPE - Windows Logon Incident Review



Process Outline and Details

Incident Recording Guide

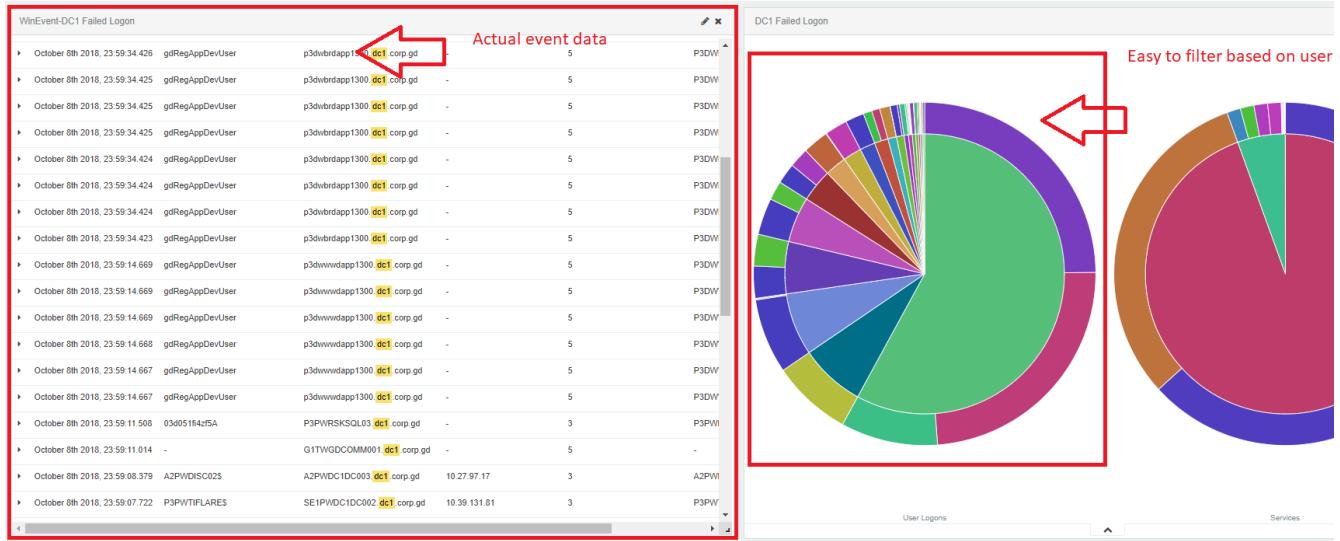
| Incident Type | |
|--------------------------|--------------------------------|
| Assignment Group | ENG-GDIRT |
| Incident Category | Intrusion |
| Sub Category | Server |
| Title | PCI Windows Logons - #Username |
| Summary | |
| Impact | 3 - Low |
| Urgency | 2 - Medium |
| Data Type | Employee-Credential |
| Detection Method | Log Review - Kibana |

General Outline

1. Navigate to [Kibana](#). Then while that is still open select this link to take you to the correct location: [Kibana dashboard](#)
2. Follow [Dashboard Review](#) steps
3. If child ticket created, follow [Child SECINC Review](#) steps

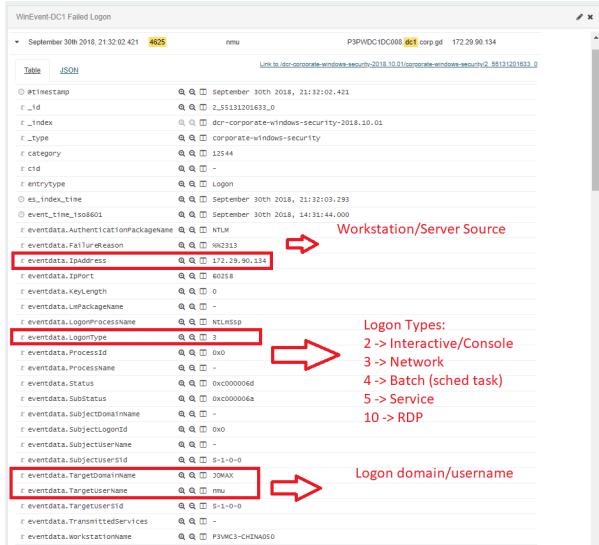
Process Details

Dashboard Review



1. Review pie chart to easily identify **Top 5** failed user logons
2. Inner ring identifies username, outer ring the source of the event (many are shipped directly from Domain Controller)
3. If over **100 failed logon** events per user OR more than **5 unique destinations** create child incident
 - a. Note affected username in ticket
 - b. Note affected destination systems in ticket
 - c. Link a sample event

Child SECINC Review



1. Lookup user account in ADUC (Active Directory Users and Computers)
 - a. Install ADUC from External Resources (if needed)
 - b. Open ADUC
 - c. Select the proper domain:
 - i. dc1.corp.gd
 - ii. jomax.paholdings.com
 - d. Right click on domain and select find
 - e. Search for user account
 - f. Look in the Member Of tab to see which groups they are a member of
 - i. You're looking to compare their member groups against the assignment/support group of the server itself
2. Utilize <https://x.co/cmdbsearch> to look up Owner/Assignment Group of system(s)
3. Review members of Assignment Group to determine if affected username is a member
 - a. If username is NOT part of assignment group, escalate for incident response tier 2
 - b. If user is part of assignment group, check event for logon type value
 - i. If LOGON TYPE 5 – Email user/team asking them to review configuration of service. Utilize email template
 1. [List of Team E-mail Distros](#)
 - ii. If NOT LOGON TYPE 5 – escalate for incident response tier 2
 - c. Set Child Tickets to "Pending Internal Response"; So we can confirm the activity has stopped the next day(Our next review)

Captured Metrics

- Most fields associated to metrics will be required by default in order to close the ticket. The following is a brief summary of metrics specific to this process:
 - **Affected CI** – Identified endpoints which are the SOURCE of the logon attempt
 - **Affected User** – User accounts which are observed performing failed logons

Process FAQs

What happens if "X"?

"X" is caused by A,B or C. Can be handled by doing "D".

How can I determine if "Y"?

"Y" is determined by E or F. If "G", then sometimes "H".

Resources and Definitions

Internal Resources

PCI Windows Logons Dashboard – <https://secstack-rproxy.cloud.dev.phx3.gdg/kibana/?#/dashboard/WinLogon-Jmx%5CDC1>

Team-Email Distro List(IPE Maintained): [List of Team E-mail Distros](#)

CMDB Search – <https://x.co/cmdbsearch>
› Temp_Workflow



External Resources

ADUC: <https://www.microsoft.com/en-us/download/details.aspx?id=28972>

Communication Templates

Service Logon Failures

During our daily review of logon activity we observed the username **USERNAME** failing a significant number of logon attempts against **SYSTEM**. Based on our review of available data this appears to be due to a mis-configuration local to the system. We ask that you review the configuration of services present on the server to correct this issue. Alternatively if the service or system is no longer necessary we ask that you either disable the service or work to retire the system. If you have any questions please respond to this message or reach out to us on Slack via #gcs0_team.

User Logon Failures

During our daily review of logon activity we observed the username **USERNAME** failing a significant number of logon attempts against **SYSTEM**. Based on our review of available data this appears to be due to a recent password change where you did not then log out and back in. In the future please log out and back in after password changes to ensure your system is not generating failed logons due to old cached credentials. If you have any questions please respond to this message.

old DSR - PKI Linux Logon Report

⚠ This process has been deprecated. Please see [DSR Failed Logons Review](#) for the current process.

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [Process Details](#)
 - [Log Review](#)
 - [Captured Metrics](#)
 - [Process FAQs](#)
 - [What happens if "X"?](#)
 - [How can I determine if "Y"?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)

General Information

| | |
|-----------------------|---|
| Responsible Team | Intrusion Prevention Engineering (IPE) Slack: #intrusion_prevention Email: ipe@godaddy.com |
| Process Owner | @Former user (Deleted) |
| Last Review Date | 2018-11-27 |
| Escalation Contact(s) | @Former user (Deleted) @Logan Zahn (Deactivated) @Former user (Deleted) |
| Requests for Updates | @Former user (Deleted) ipe@godaddy.com |

Process Summary

This process provides direction for the review of Linux logon events within PKI scoped environments to meet audit requirements. The process is designed to review logon events in an attempt to identify anomalous or malicious logon activity

Process Workflow

Process Outline and Details

Incident Recording Guide

| Incident Type | |
|-------------------|------------------------------|
| Assignment Group | ENG-GDIRT |
| Incident Category | Intrusion |
| Sub Category | Server |
| Title | PKI Linux Logons - #Username |
| Summary | |
| Impact | 3 - Low |

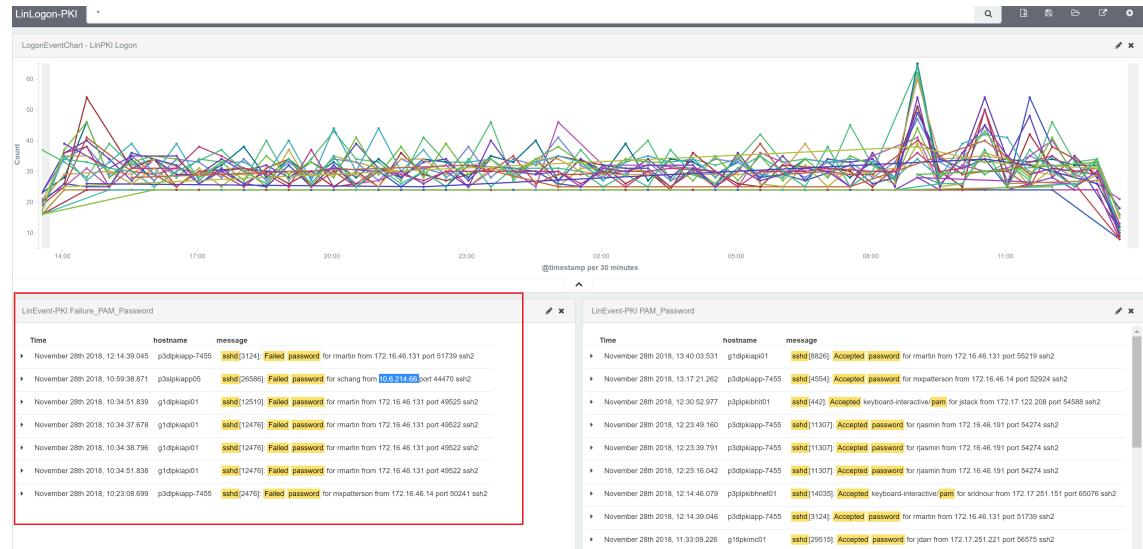
| | |
|------------------|---------------------|
| Urgency | 2 - Medium |
| Data Type | Employee-Credential |
| Detection Method | Log Review - Kibana |

General Outline

1. Navigate to [Kibana](#). Then while that is still open select this link to take you to the correct location: [Kibana dashboard](#)
2. Review each event listed in the 'LinEvent-PKI Failure_PAM_Password' widget
3. For any users which have **10+** failed logins follow "Log Review" Process

Process Details

Log Review



1. Review each event listed in the 'LinEvent-PKI Failure_PAM_Password' widget
 - a. If a user has failed **10+** logons proceed to Step 2
 - b. If no users have failed **10+** logons proceed to Step 3
2. Create child ticket using Incident Recording Guide above and assign to ENG-GDIRT. Include the following in the Summary:
 - a. Username failing logons
 - b. Number of failed logons
 - c. Destination system(s)
 - d. Source IP information
 - e. Link to sample event
3. No further review necessary, close ticket

Captured Metrics

- **Affected CI** - Server(s) failed logons attempted to
- **Affected User** - User attempting logon

Process FAQs

What happens if "X"?

"X" is caused by A,B or C. Can be handled by doing "D".

How can I determine if "Y"?

"Y" is determined by E or F. If "G", then sometimes "H".

Resources and Definitions

Internal Resources

[Kibana](#)

[Service Now](#)

External Resources

old DSR - PKI Windows Logon Report

⚠ This process has been deprecated. Please see [DSR Failed Logons Review](#) for the current process.

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [Process Details](#)
 - [Dashboard Review](#)
 - [Child SECINC Review](#)
 - [Captured Metrics](#)
 - [Process FAQs](#)
 - [What happens if "X"?](#)
 - [How can I determine if "Y"?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)
 - [Communication Templates](#)

General Information

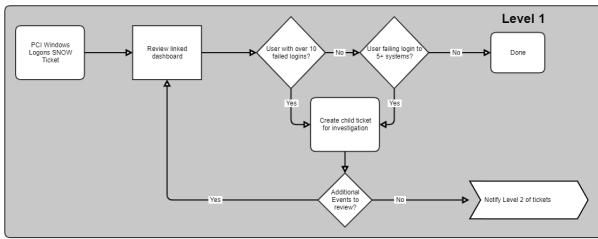
| | |
|-----------------------|---|
| Responsible Team | Intrusion Prevention Engineering (IPE) Slack: #intrusion_prevention Email: ipe@godaddy.com |
| Process Owner | @Former user (Deleted) |
| Last Review Date | 2018-11-14 by @Jonathan Wade (Deactivated) |
| Escalation Contact(s) | @Former user (Deleted) @Logan Zahn (Deactivated) @Former user (Deleted) |
| Requests for Updates | @Former user (Deleted) ipe@godaddy.com |

Process Summary

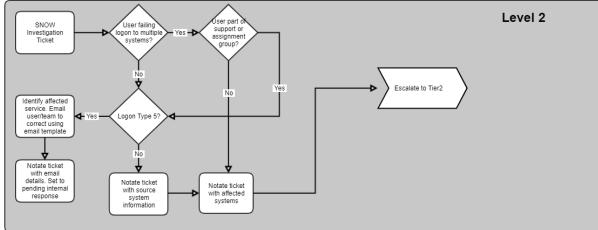
This process provides direction for the review of Windows logon events within PKI scoped environments to meet audit requirements. The process is designed to review logon events in an attempt to identify anomalous or malicious logon activity.

Process Workflow

IPE - PKI Windows Logons Report



IPE - Windows Logon Incident Review



Process Outline and Details

Incident Recording Guide

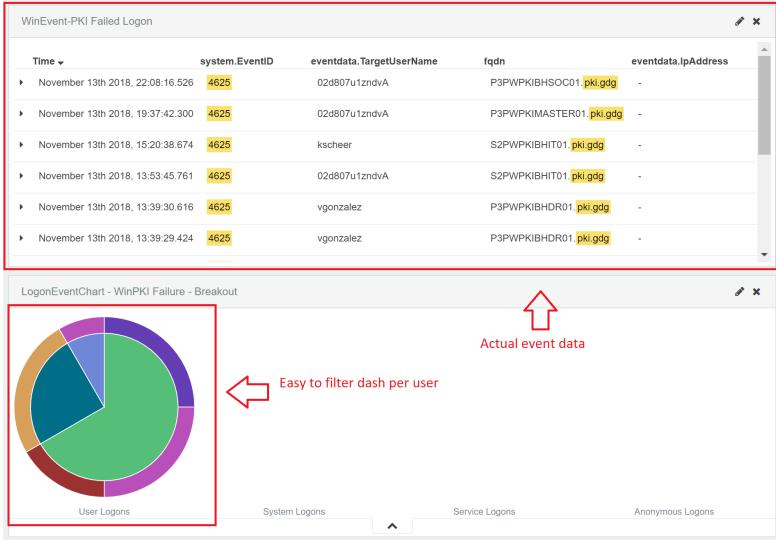
| Incident Type | |
|--------------------------|--------------------------------|
| Assignment Group | ENG-GDIRT |
| Incident Category | Intrusion |
| Sub Category | Server |
| Title | PKI Windows Logons - #Username |
| Summary | |
| Impact | 2 - Medium |
| Urgency | 2 - Medium |
| Data Type | Employee-Credential |
| Detection Method | Log Review - Kibana |

General Outline

1. Navigate to [Kibana](#). Then while that is still open select this link to take you to the correct location: [Kibana dashboard](#)
2. Follow [Dashboard Review](#) steps
3. If child ticket created, follow [Child SECINC Review](#) steps

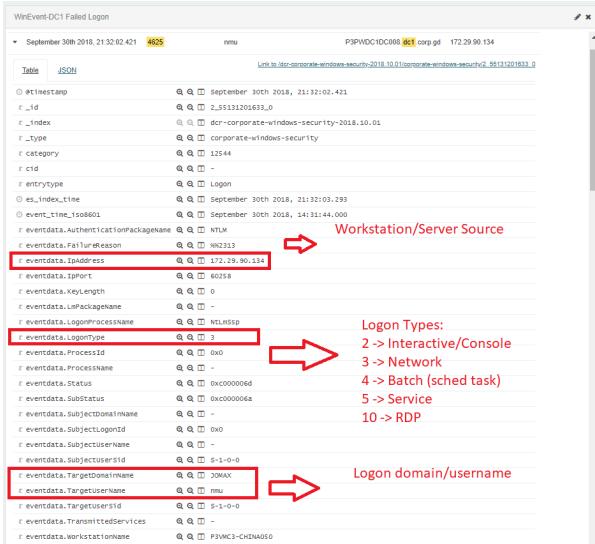
Process Details

Dashboard Review



1. Review pie chart to easily identify **Top 10** failed user logons
2. Inner ring identifies username, outer ring the source of the event
3. If over **10 failed logon** events per user OR more than **5 unique destinations** create child incident
 - a. Note affected username in ticket
 - b. Note affected destination systems in ticket
 - c. Link a sample event

Child SECINC Review



1. Lookup user account in ADUC (Active Directory Users and Computers)
 - a. Install ADUC from External Resources (if needed)
 - b. Open ADUC
 - c. Select the proper domain:
 - i. pki
 - d. Right click on domain and select find
 - e. Search for user account
 - f. Look in the Member Of tab to see which groups they are a member of
 - i. You're looking to compare their member groups against the assignment/support group of the server itself
2. Utilize <https://x.co/cmdbsearch> to look up Owner/Assignment Group of system(s)
3. Review members of Assignment Group to determine if affected username is a member
 - a. If username is NOT part of assignment group, escalate for incident response tier 2
 - b. If user is part of assignment group, check event for logon type value
 - i. If LOGON TYPE 5 - Email user/team asking them to review configuration of service. Utilize email template
 - ii. If NOT LOGON TYPE 5 - escalate for incident response tier 2

Captured Metrics

- Most fields associated to metrics will be required by default in order to close the ticket. The following is a brief summary of metrics specific to this process:
 - **Affected CI** – Identified endpoints which are the SOURCE of the logon attempt
 - **Affected User** – User accounts which are observed performing failed logons

Process FAQs

What happens if "X"?

"X" is caused by A,B or C. Can be handled by doing "D".

How can I determine if "Y"?

"Y" is determined by E or F. If "G", then sometimes "H".

Resources and Definitions

Internal Resources

PKI Windows Logons Dashboard – <https://secstack-rproxy.cloud.dev.phx3.gdg/kibana/?#/dashboard/WinLogon-PKI>

CMDB Search – <https://x.co/cmdbsearch>

External Resources

ADUC: <https://www.microsoft.com/en-us/download/details.aspx?id=28972>

Communication Templates

Service Logon Failures

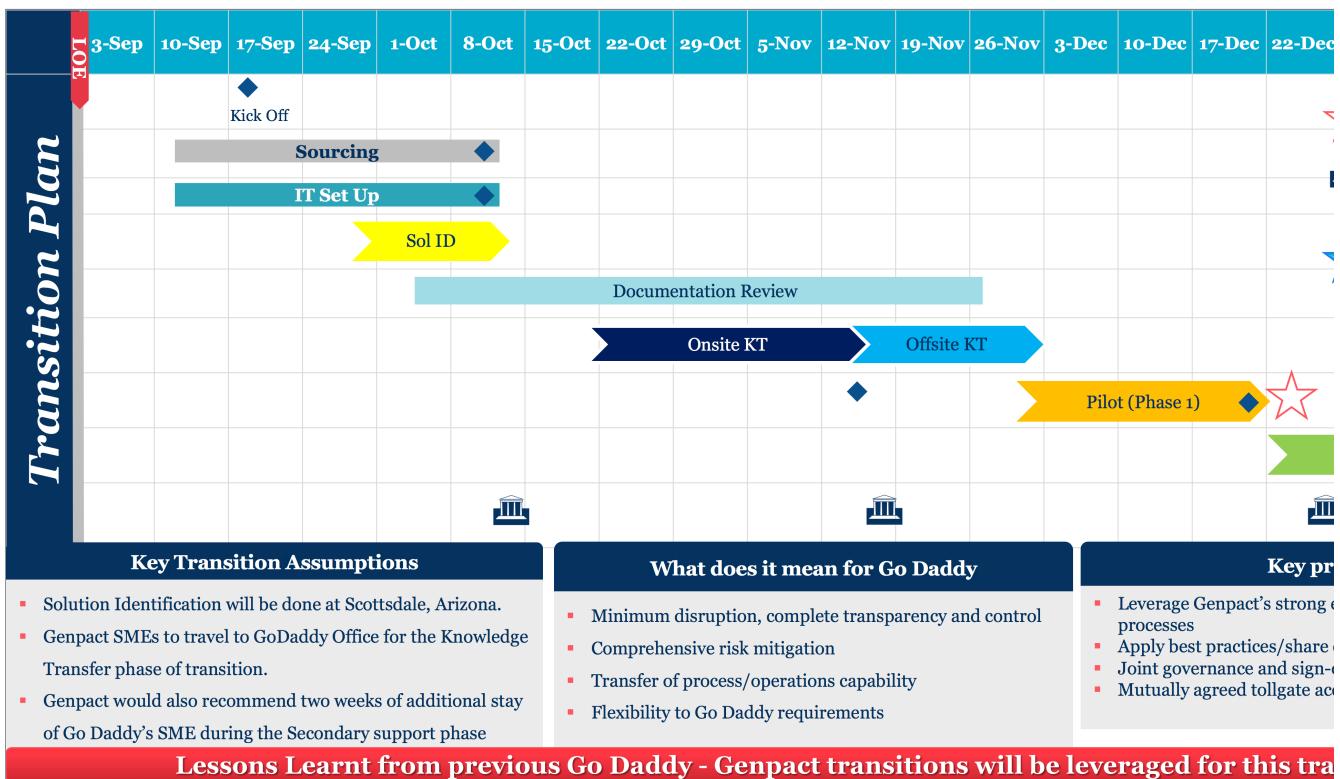
During our daily review of logon activity we observed the username **USERNAME** failing a significant number of logon attempts against **SYSTEM**. Based on our review of available data this appears to be due to a mis-configuration local to the system. We ask that you review the configuration of services present on the server to correct this issue. Alternatively if the service or system is no longer necessary we ask that you either disable the service or work to retire the system. If you have any questions please respond to this message or reach out to us on Slack via #intrusion_prevention.

old GenPact Transition Tracking

Table of Contents

- GenPact Transition Plan
- Transition Phases
- Major Project Goals
- Current Requests
- Access Tracking

GenPact Transition Plan



Transition Phases

| | Phase | Description | Status | Expected Start Date | Expected End Date | Actual Start Date | Actual End Date | Reqs. |
|---|---------------------------------------|---|----------|---------------------|-------------------|-------------------|-----------------|-------------------|
| 1 | Solution ID (SOL ID) Phase | Initial data collection and discussion with GenPact | COMPLETE | 27 Sep 2018 | 10 Oct 2018 | 27 Sep 2018 | 10 Oct 2018 | N/A |
| 2 | On-Site Knowledge Transfer (KT) Phase | On-site training for GenPact SME. | COMPLETE | 24 Oct 2018 | 21 Nov 2018 | 26 Oct 2018 | 21 Nov 2018 | L2 SME On-Site |
| 3 | Off-Site KT Phase | GenPact SME trains off-site SOC. | COMPLETE | 14 Nov 2018 | 30 Nov 2018 | 29 Oct 2018 | 23 Nov 2018 | |
| 4 | Pilot Phase | Gradual hand-off of processes | COMPLETE | 01 Dec 2018 | 21 Dec 2018 | 26 Nov 2018 | 23 Dec 2018 | Training Complete |

| | Phase | Description | Status | Expected Start Date | Expected End Date | Actual Start Date | Actual End Date | Reqs. |
|---|------------------------------|---|--------|---------------------|-------------------|-------------------|-----------------|------------------|
| | | to the GenPact team. | | | | | | |
| 5 | Production - Go Live Phase 1 | Official transition of processes to GenPact | DONE | 22 Dec 2018 | N/A | 24 Jan 2019 | N/A | Successful Pilot |

Major Project Goals

| | Goal | Status | Expected Completion Date | Actual Completion Date | Requirements | Notes |
|---|--|--------|--------------------------|------------------------|--|--|
| 1 | Employee Daily AV Report Transition | DONE | 24 Dec 2018 | 24 Dec 2018 | | |
| 2 | Employee Phishing (IsItBad) Transition - Phase 1 | DONE | 24 Dec 2018 | 04 Feb 2019 | <ul style="list-style-type: none"> ▪ Additional controls must be added and approved for Message Purge process. See /wiki/spaces/IRKB/pages/49251303 | |
| 3 | Cloud App Security (CAS) Un-Quarantine Request Transition | DONE | 24 Dec 2018 | 24 Dec 2018 | | |
| 4 | Daily Security Report Transition - Phase 1 | DONE | 24 Dec 2018 | 24 Dec 2018 | | |
| 5 | Address Major Access Control Needs (MVP: Okta, Tanium, O365) | DONE | 31 Jan 2019 | 04 Mar 2019 | <input checked="" type="checkbox"/> Okta - Reset Password & Clear Sessions <input checked="" type="checkbox"/> Okta - Enroll in MFA <input checked="" type="checkbox"/> Tanium - Outline RBAC Options <input checked="" type="checkbox"/> Allow Standard Censors <input checked="" type="checkbox"/> Allow Trace Access <input checked="" type="checkbox"/> Allow IR Gatherer Use <input checked="" type="checkbox"/> O365 Admin - Clear Sessions <input checked="" type="checkbox"/> O365 S&C - Content Search & Message Trace | <p>Tanium Access is currently blocked by the following:</p> <input checked="" type="checkbox"/> DC1 Credential Creation <input checked="" type="checkbox"/> DC1/Jomax Group Controls <input checked="" type="checkbox"/> RSA Tokens for 2FA ONLY <input checked="" type="checkbox"/> PKI Concerns <input checked="" type="checkbox"/> PKI Trust Role <input checked="" type="checkbox"/> PKI Training Group |

Current Requests

| Summary | Status | Priority | Requestor | Entered On | Completed On | Notes |
|-------------------------------------|--------|----------|-----------------------------|-------------|--------------|---|
| Integrate EMEA into Daily AV Report | DONE | HIGH | @David Dubois (Deactivated) | 19 Oct 2018 | 29 Nov 2018 | Integration for report only. Analysts reviewing the Daily AV detections and generating tickets for EMEA (GetHelp) |

| Summary | Status | Priority | Requestor | Entered On | Completed On | Notes |
|---|---------|----------|------------------------------|-------------|--------------|--|
| Integrate EMEA into Employee Phishing (IsItBad) | DONE | HIGH | @ David Dubois (Deactivated) | 19 Oct 2018 | 10 Dec 2018 | Initial integration into process to provide protection for all users in Office 365. Users in external tenants still require EMEA action. Expected transition of a majority of EMEA users into O365 is by 10 Dec 2018. US will process EMEA-originating reports and handle per SOP on US-side. Need to determine how to extend capabilities to EMEA for in-depth investigation as we proceed. |
| Add Basic Architecture Diagrams to all Process Documents | SKIPPED | MEDIUM | GenPact | 19 Oct 2018 | | Completed: Employee Security (ALL) DSR () |
| Create 3-5 Use Case Examples for Each Process | SKIPPED | MEDIUM | GenPact | 19 Oct 2018 | | <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Daily AV <input checked="" type="checkbox"/> Phishing <input checked="" type="checkbox"/> Unquarantine <input checked="" type="checkbox"/> Workstation Investigation <input checked="" type="checkbox"/> Compromise Containment <input checked="" type="checkbox"/> DSR <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Failed Logon (Win) <input checked="" type="checkbox"/> Failed Logon (Lin) <input checked="" type="checkbox"/> Failed Logon (SQL) <input checked="" type="checkbox"/> HIPS AV <input checked="" type="checkbox"/> FIM <input checked="" type="checkbox"/> ModSec |
| Provide Escalation Contacts for the Primary Team(s) | DONE | MEDIUM | GenPact | 22 Oct 2018 | 14 Nov 2018 | Escalation Example.xlsx |
| Provide List of Support Locations (Physical) | DONE | LOW | GenPact | 22 Oct 2018 | 23 Oct 2018 | locationlist.rtf /wiki/spaces/PHY/pages/12 |
| Review SNOW Dashboards and Refine for GenPact T1 Daily/Weekly Standup | DONE | MEDIUM | @ Jason Veiock (Deactivated) | 24 Oct 2018 | 21 Nov 2018 | Daily standup has been created. Proper stakeholders are currently present. GenPact has had some limited experience running and will continue to take over as we continue the handoff. |
| Internal Testing of Processes to Identify Gaps and Clarify | DONE | MEDIUM | @ David Dubois (Deactivated) | 24 Oct 2018 | 21 Nov 2018 | |
| Provide Detailed Tools Access List | DONE | HIGH | GenPact | 24 Oct 2018 | 26 Oct 2018 | GenPact tools.xlsx |
| General ServiceNow Incident Workflow | DONE | HIGH | GenPact | 30 Oct 2018 | 15 Nov 2018 | ServiceNow General Usage |
| GenPact Team Distribution List | DONE | LOW | GenPact | 07 Nov 2018 | 09 Nov 2018 | DL (gcs0@godaddy.com) has been created for GenPact team.] @ David Dubois (Deactivated) @ Jason Veiock (Deactivated) initial visibility. |

Access Tracking

| Access Management (Tools In Use) | | | | | | |
|----------------------------------|---|---|---|--|------------------------|--------------------------|
| Pri. | General Tools | URL | Function | Associated Process(es) | Account Control | Acc Met |
| HIGH | Confluence | https://confluence.godaddy.com/ | Needed for access to documentation. | N/A | OKTA | Brows Ok |
| HIGH | Slack | https://godaddy.slack.com/ | Needed for communication to users and GESS team. | N/A | OKTA | Brows Ok |
| HIGH | Skype/Lync | (Install Application) | Needed for communication to users. | N/A | AD | VDI In |
| HIGH | ServiceNow | https://godaddy.service-now.com | Needed for access to create, update and close incident tickets. | N/A | OKTA | Brows Ok |
| MED | The Planet (Jive) | https://godaddy.jiveon.com/ | Allows for review of basic user info and access to necessary documents. | N/A | OKTA | Brows Ok |
| MED | Active Directory Users & Computers (ADUC) | (Install Application) | Allows review of user access; Used to disable accounts. | N/A | AD | VDI In |
| Security & Admin | | URL | Function | Associated Process(es) | Account Control | |
| HIGH | ServiceNow Group (OPS-GCSO) | N/A | ServiceNow group utilized by the GenPact SOC group. | All | LOCAL | Service - Browsing via C |
| MED | Security Kibana | https://secstack-rproxy.cloud.dev.phx3.gdg/kibana/ | Review of various logs currently housed in ELK | DSR (multiple); Employee Compromise | AD | |
| MED | PKI Kibana | https://infosec-rproxy.cloud.dev.phx3.gdg/kibana/#/ | Review of various logs currently housed in ELK | DSR (multiple) | AD | |
| MED | Tanium | https://tanium.int.godaddy.com | Query against machines to review machine activity; Trace access for investigations; IR Gatherer | Employee Phishing, Workstation Intrusion; DSR (multiple) | UNKNOWN | |
| HIGH | Office 365 Security & Compliance Center | https://protection.office.com/ | Search against emails sent to the organization; Review of messages sent to/from the organization. | Employee Phishing | LOCAL | |
| HIGH | Powershell (o365ContentTools.ps1) | https://github.secureserver.net/GESS/o365-tools | Required for Purging messages; Reviewing Inbox Rules | Employee Phishing | OKTA:GIT LOCAL:GESS | |

| | | | | | | |
|---------------|--------------------------------------|---|--|---|--------------|--|
| | | | | | | |
| HIGH | Trend OfficeScan as a Service (TMCM) | https://daxu3d.manage.trendmicro.com/webapp/index.html | Allows review of OfficeScan-generated alerts. | Daily AV Report; Workstation Intrusion | OKTA | |
| HIGH | Trend Cloud App Security | https://admin.tmcas.trendmicro.com/#/login | Allows review of CAS events and release of quarantined messages. | Un-Quarantine Requests | LOCAL | |
| HIGH | IsItBad Distro | (Internal Email Distro Group) | Needed for receipt of phishing messages. | Employee Phishing | LOCAL | |
| LOW | Fame | http://malwareautomation.int.godaddy.com:4200/ | Allows for sandboxing of suspicious files and review of previous submissions | Employee Phishing, Workstation Intrusion | LOCAL | |
| V. LOW | Absolute | https://cc.absolute.com | Provides the ability to track device activity and potentially remediate. | [FUTURE] Employee Phishing | LOCAL | |
| V. LOW | IWSaaS Console | https://adminportal-uw2.iws-hybrid.trendmicro.com/login.html | Allows for review of user web activity and blocking of URLs | [FUTURE] Employee Phishing, Workstation Intrusion | LOCAL | |
| HIGH | Trend Deep Security (HIPS) | https://hips.int.godaddy.com/ | Review of server AV events; Initiating system scans | DSR (AV) | AD | |
| MED | ServiceNow Security Reimage Request | https://godaddy.service-now.com/gdsp? id=gd_sc_cat_item&sys_id=db5b84dc4f4cdf804a92e3414210c78d | Submission of re-image requests to GetHelp | Employee Compromise | AD | |

| LOW | Office 365 Admin | https://admin.microsoft.com/AdminPortal/Home#/homepage | Review user account status; Clear Office 365 Sessions | Employee Compromise | OKTA LOCAL | |
|------------|---|---|---|--|-----------------------------|--|
| | External Tools | URL | Function | Associated Process(es) | Account Control | |
| N/A | GoDaddy Abuse Form | https://supportcenter.godaddy.com/AbuseReport | Used to submit customer-targeted complaints to the Customer Security team | Employee Phishing | N/A | |
| N/A | Google Safebrowsing - Report | https://safebrowsing.google.com/safebrowsing/report_phish/?hl=en | Used to submit phishing pages to Google | Employee Phishing | N/A | |
| N/A | Virus Total | https://www.virustotal.com/#/home/search | File and URL reputation; IOC Gathering | Workstation Intrusion; DSR (multiple) | N/A | |
| N/A | Reverse.it | https://www.reverse.it/ | File and URL reputation; IOC Gathering | Workstation Intrusion; DSR (multiple) | N/A | |
| N/A | Malwr | https://malwr.com | File and URL reputation; IOC Gathering | Workstation Intrusion; DSR (multiple) | N/A | |
| N/A | UrlQuery | https://urlquery.net/ | File and URL reputation; IOC Gathering | Workstation Intrusion; DSR (multiple) | N/A | |
| N/A | Netcraft - Report | http://toolbar.netcraft.com/report_url | Used to submit phishing pages to Netcraft | Employee Phishing | N/A | |
| N/A | Anti-Phishing Work Group (APWG) - Report | https://antiphishing.org/report-phishing/ | Used to submit phishing pages to APWG | Employee Phishing | N/A | |
| N/A | Trend Site Safety Center - WRS | https://global.sitesafety.trendmicro.com/index.php | URL Reputation; Automated review by Trend | Employee Phishing; Workstation Intrusion | N/A | |
| N/A | Trend Micro Threat Encyclopedia | https://www.trendmicro.com/vinfo/us/threat-encyclopedia/ | AV identifier review | Workstation Intrusion; DSR (AV) | N/A | |

old HaveIBeenPwnd (Draft)

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [General Outline](#)
 - [Process Details](#)
 - [Active Directory Check](#)
 - [LockoutStatus verification](#)
 - [Process FAQs](#)
 - [What other ways can we verify user accounts?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)
 - [Communication Templates](#)

General Information

| | |
|-----------------------|--|
| Responsible Team | infosec-response |
| Process Owner | Anthony Crisostomo |
| Last Review Date | |
| Escalation Contact(s) | Anthony Crisostomo Juan Bustamante David Downs |

Process Summary

This document serves as a guide for credentials that have been reported in HaveIBeenPwnd breaches.

Process Workflow

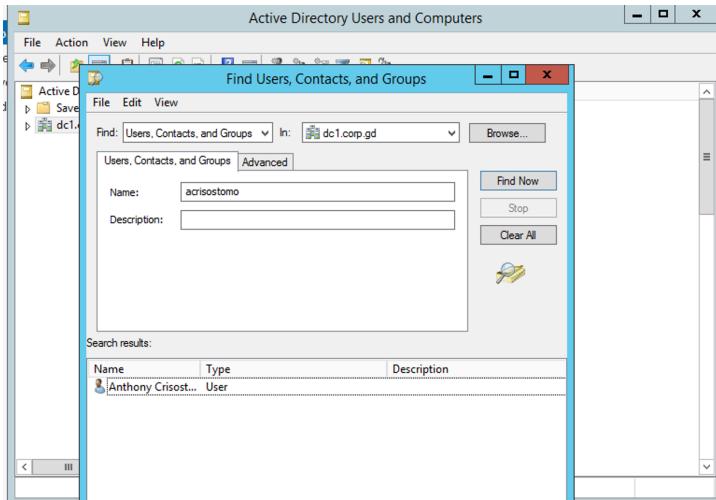
Process Outline and Details

General Outline

1. HaveIBeenPwd ServiceNow ticket received.
2. Check date of reported Breach.
3. Check user accounts in Active Directory to verify if accounts are still active.
 - a. If accounts are active move on to step 4
 - b. Note inactive accounts or close ticket if only a single user was reported.
4. Verify for recent password change using the LockoutStatus tool.
 - a. Password change within 90 days after breach?
 - i. If YES close out ticket
 - ii. If NO reach out to user.
5. Reach out to user to perform a manual password reset by EOD to rotate.
 - a. If user responds verify using the LockoutStatus tool.
 - b. No response from user rotate their credentials following the [Credential Mitigation](#) process.

Process Details

Active Directory Check



LockoutStatus verification

| DC Name | Site | User State | Bad Pwd Count | Last Bad Pwd | Pwd Last Set | Lockout Time | Orig Loc |
|-----------------|-------------|----------------|---------------|-----------------------|---------------------|--------------|----------|
| ASPWDC1DC001 | DC1A2 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| ASPWDC1DC002 | DC1A2 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| A2PWDC1DC003 | DC1A2MGT | Not Locked | 0 | 7/9/2020 9:32:53 AM | 6/4/2020 2:57:28 PM | N/A | N/A |
| A2PWDC1DC004 | DC1A2MGT | Not Locked | 0 | 6/4/2020 3:10:10 PM | 6/4/2020 2:57:28 PM | N/A | N/A |
| A2PWDC1SSDC001 | DC1A2S5 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| B1PWDC1SSDC002 | DC1B0S1 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| B1PWDC1DC001 | DC1B0S1 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| C1PWDC1DC002 | DC1C9S1 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| C1PWDC1DC001 | DC1C9S1 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| C1PWDC1DC002 | DC1C9R1 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| D1PWDC1DC003 | DC1C9R1 | Not Locked | 0 | 12/5/2018 2:48:08 PM | 6/4/2020 2:57:28 PM | N/A | N/A |
| D1PWDC1DC004 | DC1C9T1 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| N1PWDC1SSDC001 | DC1N1S5 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| N1PWDC1SSDC002 | DC1N1S5 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| P3PWDC1DC003 | DC1PHK3 | Not Locked | 0 | 8/18/2020 3:31:38 PM | 6/4/2020 2:57:28 PM | N/A | N/A |
| P3PWDC1DC004 | DC1PHK3 | Not Locked | 0 | 7/10/2020 10:29:13 AM | 6/4/2020 2:57:28 PM | N/A | N/A |
| P3PWDC1DC005 | DC1PHK3 | Not Locked | 0 | 7/20/2020 11:54:05 AM | 6/4/2020 2:57:28 PM | N/A | N/A |
| P3PWDC1DC006 | DC1PHK3 | Not Locked | 5 | 7/23/2020 11:37:07 AM | 6/4/2020 2:57:28 PM | N/A | N/A |
| P3PWDC1DC007 | DC1PHK3E3NT | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| P3PWDC1DC008 | DC1PHK3E3NT | Not Locked | 0 | 6/19/2017 10:38:48 PM | 6/4/2020 2:57:28 PM | N/A | N/A |
| P3PWDC1IMGT001 | DC1PHK3MGT | Not Locked | 1 | 8/18/2020 3:24:30 PM | 6/4/2020 2:57:28 PM | N/A | N/A |
| P3PWDC1IMGT002 | DC1PHK3MGT | Not Locked | 0 | 6/14/2018 9:48:53 AM | 6/4/2020 2:57:28 PM | N/A | N/A |
| P3PWDC1SRBD001 | DC1PSS8 | DC Unavailable | - | - | - | - | - |
| P3PWDC1SRBD004 | DC1PSS8 | DC Unavailable | - | - | - | - | - |
| P3PWDC1SSDC001 | DC1PHK3SS | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| P3PWDC1SSDC002 | DC1PHK3SS | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| P3PWDC1DC001 | DC1S0L1 | Not Locked | 0 | 6/15/2017 2:12:49 AM | 6/4/2020 2:57:28 PM | N/A | N/A |
| S1PWDC1DC001 | DC1S0L1 | Not Locked | 0 | 12/8/2017 12:33:28 PM | 6/4/2020 2:57:28 PM | N/A | N/A |
| S1PWDC1DC001 | DC1S1E1 | DC Unavailable | - | - | - | - | - |
| S1PWDC1DC002 | DC1S1E1 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| S2GPWDC1DC001 | DC1S1E1 | Not Locked | 0 | 9/23/2016 10:38:23 AM | 6/4/2020 2:57:28 PM | N/A | N/A |
| S2GPWDC1DC002 | DC1S1E1 | Not Locked | 0 | 8/18/2016 10:32:05 AM | 6/4/2020 2:57:28 PM | N/A | N/A |
| S3B1PWDC1MGT001 | DC1S8H1MGT | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| S3B1PWDC1MGT002 | DC1S8H1MGT | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| T2PWDC1DC001 | DC1T12 | Not Locked | 0 | None | 6/4/2020 2:57:28 PM | N/A | N/A |
| T2PWDC1DC002 | DC1T2 | Not Locked | 0 | 11/8/2017 1:35:05 PM | 6/4/2020 2:57:28 PM | N/A | N/A |

Process FAQs

What other ways can we verify user accounts?

1. Verify via the address book in Outlook.
2. Verify in Slack.
3. Verify in the [Planet Directory](#).
4. Verify in Okta Admin.

Resources and Definitions

Internal Resources

External Resources

Communication Templates

| Communication Name |
|--|
| <p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean libero risus, tristique viverra tortor eu, VARIABLE accumsan pellentesque dolor. Maecenas euismod, tellus ac vestibulum viverra, nulla ligula fermentum turpis, ut blandit dui sapien ac purus. Mauris ut nunc ante. Fusce nec arcu magna. Proin eget mattis quam.</p> |

old HIVE Incident Testing

| Key | Summary | T | Created | Updated | Due | Assignee | Reporter | P | Status | Resolution |
|---|---------|---|---------|---------|-----|----------|----------|---|--------|------------|
| No issues found  Refresh | | | | | | | | | | |

GCSO-417 – IsItBad Test Case

<http://hansolo-test.cloud.phx3.gdg:9000/index.html#!/case/AXIVVzVhWjNnOtieVfu3/details>

Comparison:

- Similar to SIR you can generate a set of tasks to track work and allow multiple analysts to work on a single case.
- IOC tracking exists and is better presented than in our custom SNOW table. Is comparable to the SIR Observables table.
- Navigation can be somewhat unintuitive, but could be overcome over time.

Gaps:

- HIVE has a worse display of activity log (if that's even possible) and is nearly impossible to follow on the main case.
 - Individual tasks have a log which is a bit easier to follow.
 - Cases only display "Live Stream" which do not have timestamps, but rather have a calculated time (NOW-CurrentTime).
 - There is no unified timeline from tasks to Cases.
- Text formatting in this platform is AWFUL - I spent more time trying to make things legible than it would have taken to do the sample work being recorded.
 - The platform uses GitHub style markup, but the editor seems to have trouble handling basic line breaks.
 - The text editor by default converts text into hyperlinks where possible which is a TERRIBLE idea for an IR platform.
- Basic timestamps, incident status, etc are not present in the platform and would require custom configuration (if possible)
 - Statuses are only OPEN or CLOSED
 - Validity is tracked ONLY on Close and is not otherwise immediately visible.
 - No timestamps.

GCSO-419 – Server Intrusion Test Case

<http://hansolo-test.cloud.phx3.gdg:9000/index.html#!/case/AXIVTibpWjNnOtieVfVo/details>

Comparison:

- Can create a set of tasks to track work
- IOC tracking works OK

Gaps:

- IOCs are only tracked – no place to provide an analysis of an IOC except as a worklog entry in a task. Won't be available for review of the IOC in later cases
- Unable to output a final report of the case itself
- No sense of an incident timeline
- Need to track affected systems/users as observable to track them across alerts/cases. Easy to accidentally mark as an IOC

GCSO-421 - User Interactions (User Malware Report)

<http://hansolo-test.cloud.phx3.gdg:9000/index.html#!/case/AXIaXOMLWjNnOtieWZWt/details>

Comparison:

- Create a set of tasks to track work
- IOC tracking works OK

Gaps:

- Not aware of CI/Users (such as SNOW)

GCSO-418 – Major Incident (Social Engineering)

<http://hansolo-test.cloud.phx3.gdg:9000/index.html#!/case/AXIZ7-XAWjNnOtieWUdr/tasks>

old Incident Prioritization

Incident priority is determined by a combination of two key elements: Impact and Urgency.

- **Urgency** refers to the expected timeframe in which a task or incident should be reasonably expected to need to be resolved. This is generally driven by the level of sensitivity of the affected environment/user, the level of potential public exposure, and/or the sophistication of the threat actor.
- **Impact** refers to either the level of damage can be done when an incident occurs or the level of damage already resultant by an incident.
- **Priority** provides a general expectation for the speed and care needed when reviewing an incident.

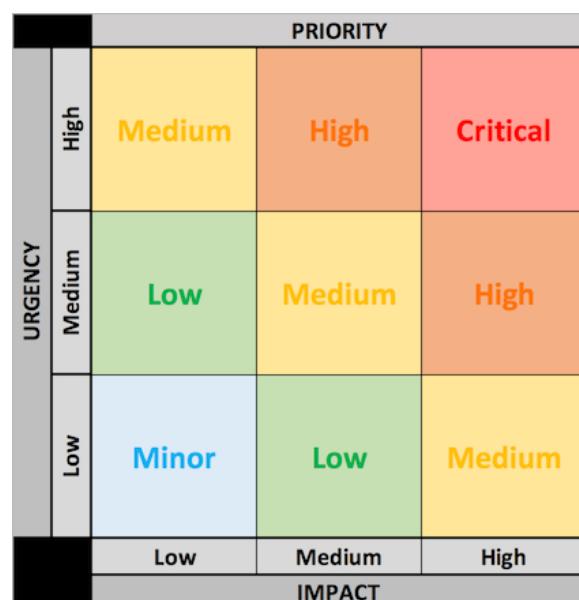
Impact & Urgency Guidelines

These guidelines provide a general outline for the uses of the Urgency and Impact levels to generate the appropriate priority for incidents. These should be reviewed on a per-process basis to determine the individual priority for each type of incident.

| | Urgency | Impact |
|--------|--|--|
| High | <ul style="list-style-type: none"> • Externally Reported • PCI/PKI Targeted • Targeted Attack/APT • Large Target Group | <ul style="list-style-type: none"> • Suspected Data Loss • Business Disruption • Expected Wide-Scale Impact • Sensitive Access |
| Medium | <ul style="list-style-type: none"> • Medium/Small Target Group • Higher-Risk Targets • Risk of Public Exposure • Sophisticated Actor • High Fidelity Reporter | <ul style="list-style-type: none"> • SLT / XLT Affected • Semi-Sensitive Systems |
| Low | <ul style="list-style-type: none"> • Audit Only • Individual Target • Policy Violation | <ul style="list-style-type: none"> • General Systems • False Positive • Non-Malicious |

Prioritization Matrix

The Priority of an incident is determined by a cross reference between the determined Urgency and Impact. Generally everyday incidents should fall within the Low and Medium categories. Adjustments to the urgency and impact guidelines should be considered in cases where common incidents frequently fall outside of these norms.



Process-Specific Priority Matrix - Employee Phishing Incidents

| | Urgency | Impact |
|--------|--|--|
| High | <ul style="list-style-type: none"> • SLT/XLT Spoof (BEC Attempt) • Targeted Attack (HR, Finance, SLT, PR) • Large Non-Targeted Attempt (t>50) • Internal Sender | <ul style="list-style-type: none"> • Suspected Data Loss • SLT/XLT Compromise • Medium to Large Remediation (6+ Users) • Sensitive System Accessed (Ex: Workday, GitHub) • Credentials Verified or Used by TA |
| Medium | <ul style="list-style-type: none"> • Individual High-Risk Target • Medium Non-Targeted Attempt (t<=50) | <ul style="list-style-type: none"> • Small Remediation (Up to 5 Users) • No Indications of Credential Use |
| Low | <ul style="list-style-type: none"> • Individual Target • Small Non-Targeted Attempt (t<=10) | <ul style="list-style-type: none"> • No Remediation of Users • No Indications of Credential Use • False Positive; Non-Malicious; Spam / Scam Message |

Process-Specific Priority Matrix - Daily Endpoint Anti-Virus Report

| | IMPACT | URGENCY |
|-----|--|--|
| LOW | <ul style="list-style-type: none"> • Detections of non-malicious items such as: <ul style="list-style-type: none"> • Adware (ADW) • Potentially Unwanted Applications (PUA/PUP) • Tracking Cookies (COOKIE) | <ul style="list-style-type: none"> • Realtime Deletions • Scheduled Deletions on Low-Priority Systems <ul style="list-style-type: none"> • Virtual Machines • IT Security Devices |

| | IMPACT | URGENCY |
|---------------|---|---|
| | <ul style="list-style-type: none"> • Joke programs (JOKE) • Browser Helper (BHO) • Detections of low-risk malicious items: <ul style="list-style-type: none"> • Non-native executables on machines (ex. EXE files on Mac; ELF files on Windows) | <ul style="list-style-type: none"> • Fraud (FR) Devices |
| MEDIUM | <ul style="list-style-type: none"> • Detections of medium-risk malicious items such as: <ul style="list-style-type: none"> • Non-executable phishing documents (HTML, JS) • Files with macros (W2KM) • Hack tools (HKTL/CRCK) • Spyware (SPYW) • Trojans (TROJ) | <ul style="list-style-type: none"> • Realtime deletions on Medium-Priority systems <ul style="list-style-type: none"> • Marketing (MK) • Public Relations (PR) • Scheduled Deletions |
| HIGH | <ul style="list-style-type: none"> • Detections of high-risk malicious items such as: <ul style="list-style-type: none"> • Batch files (BAT) • IRC • Remote Access (RAP/RAT) • Rootkit (RTKT) • Backdoor (BKDR) • Malicious Spyware (TSPY) • Worms (WORM) • Virtual Basic (VBS) • Ransomware | <ul style="list-style-type: none"> • All deletions on High-Priority Systems <ul style="list-style-type: none"> • Legal (LG) • Human Resources (HR) • Executives (EX) • Payroll (PY) • Accounting (AC) • Registration Authority (RA) |

Process-Specific Priority Matrix - IWSaaS/URL Reclassification Requests

| | Urgency | Impact |
|---------------|----------------|---------------|
| High | | |
| Medium | | |
| Low | | |

old Major Incident Workflow

Table of Contents

- Pre-Existing IRP Documentation
- Incident Response Docs Template
- Defining Major Incidents
 - What is a Major Incident?
 - How do I identify a Major Incident?
 - Who handles Major Incidents?
- Handling Major Incidents
 - Incident Handler Priorities
 - Major Incident Workflow
 - Major Incident Communications

Pre-Existing IRP Documentation

- CSIRP - GoDaddy
- Incident Response Plan.docx
- Incident Handoff Process
- Incident Coordinator Communication
- Incident Response Resources
- V-Team Program Setup
- Documentation Cleanup List
- Incident Management Process Alignment.pptx
- Initial Incident Engagement Process
- IR Team 3 year plan
- Incident Coordinator Communication
- ISP-20

Incident Response Docs Template

Unable to render {include} | The included page could not be found.

Defining Major Incidents

What is a Major Incident?

A **Major Incident** is an instance in which an incident has reached a severity level that requires the following to occur:

1. Management must be notified.
2. Escalation to Level 2 must occur.
3. An Incident Handler must be assigned.

How do I identify a Major Incident?

An important part of handling a Major Incident is being able to define how to first determine if a major incident has occurred. Often the first indication of this is overall **Priority** of the incident. Any incident which has a **High** or **Critical Priority** is likely a Major Incident. Within each of the processes it will be important to define what specific thresholds exist to identify when a Major Incident has occurred if identification cannot be driven by Priority.

Who handles Major Incidents?

Once a Major Incident has been confirmed it is the responsibility of the owning team to identify an **Incident Handler**. This individual plays a crucial role in the operational management of a Major Incident, not limited to the following:

- Direct individual contributors over the course of the incident.
- Define and monitor action items throughout the life of the incident.
- Manage communication of the incident to management and external teams.
- Engage resources needed to resolve the incident.
- Ensure containment of the incident is prioritized.

Handling Major Incidents

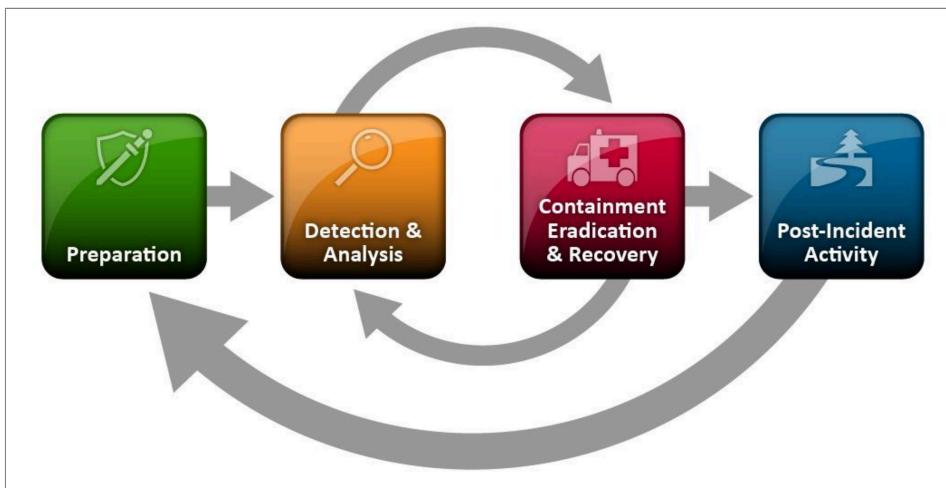
Incident Handler Priorities

It is important to note that the duty of the Incident Handler is not to perform the technical tasks associated with the incident, although they may also participate in these tasks. In general, the Incident Handler is there to ensure that the following priorities are met:

1. **Direction** - Ensure that resources are performing appropriate action items.
2. **Containment** - Ensure that containment of a major incident is reached as quickly as possible; drive all ongoing tasks toward containment.
3. **Scoping** - Scope the impact of the incident by identifying pivot points from gathered IOCs, providing knowledge of the environment, and understanding common TTPs.
4. **Communication** - Communicate to various stakeholders about the incident status; gather resources from external teams as needed.
5. **Resolution** - Identify current path to resolution; Outline appropriate action items to complete any after-containment investigation.

Major Incident Workflow

In general, the high-level lifecycle of Major Incidents should follow the Incident Response Lifecycle:



For the Incident Handler, the primary goals are **Detection** and **Containment** with a focus on scoping of the incident and prevention of continued damage to the company. It is also important to identify short-term and long-term remediation strategies, which will be used for Post-Activity and feedback into the Prevention phase. It is important that the Incident Handler be able to maintain focus on their priorities to attain the desired outcome and reach resolution quickly and effectively. In general, the workflow for an Incident Handler should be similar to the following:



Major Incident Communications

An important aspect for the Incident Handler to consider is maintaining proper communication with stakeholders and impacted groups. Ultimately it is the Incident Handler who should determine who is included in communications outside of active resources and key stakeholders, however some general standards can help to clarify what the basic expectation is. In general, the following should be considered when determining what type of communication is required and which groups to include:

1. What is the potential impact of the incident?
2. What groups could be impacted?
3. What level of communication is needed?
4. What is the urgency of communication to these groups?

Some basic examples of which groups to communicate incidents to and how are as follows:

| Situation 1 - Employee Compromise | | | |
|-----------------------------------|--|--|--|
| | | | |
| | | | |

old Monthly ASV Audit Scans (PCI)

Table of Contents

General Information

| | |
|------------------------------|---|
| Responsible Team | Security Risks & Assessments (SRA) - Slack: vulnerability_mgmt - Email: sra@godaddy.com |
| Process Owner | Warren Harris |
| Last Review Date | 2020-03-03 |
| Escalation Contact(s) | Bindi Davé |
| Requests for Updates | Security Risks & Assessments |

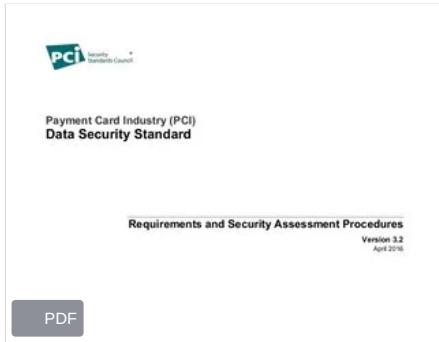
Process Summary

This process provides direction for the detection, analysis and remediation of <X> event types and outlines the general process guidelines to be followed by Incident Response analysts. A summary of applicable use cases for this process are as follows:

- PCI DSS 3.2.1 includes requirement 11.2.2 to "Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC)." To meet this requirement we engage the services of an Approved Scanning Vendor (ASV) to perform regular scans. The vendor may change due to the regular vendor issues (quality, responsiveness, cost) but it will always be an ASV verified with the PCI Council list.
- PCI 11.2.2 requires scans to be performed a minimum of quarterly. In practice, the card processors expect to see a report within 90 days of the previous report.

Process-Specific Definitions Supporting Documentation

- PCI
 - [Section 11.2.2 PCI DSS...](#)



Process Workflow

- [Process Diagram...](#)

Process Outline and Details

Summary

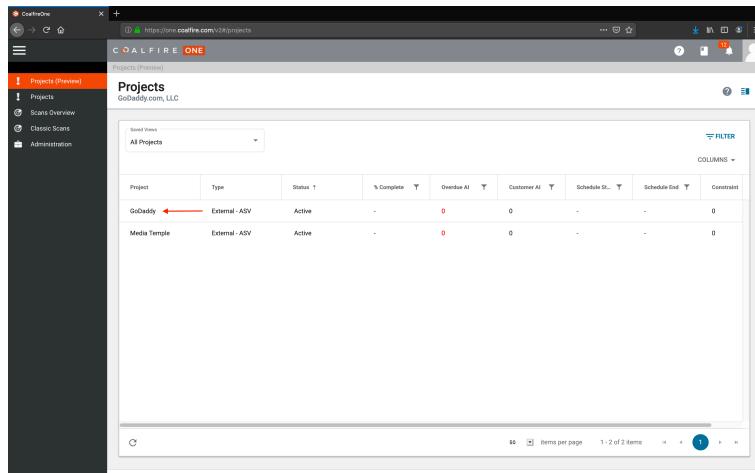
The Monthly ASV Vulnerability scans are performed by third-party scanning vendors. Once per month scans are automatically started. Upon completion, the scan reports are retrieved from the vendors via a web GUI. The results are parsed for findings and tickets are created in the ticketing system - currently ServiceNOW. After ticketing is complete and the issues remediated, the reports are attached to the JIRA stories (currently on the ESA board) and links to the stories are added to the [Audit Calendar](#). The PCI ASV currently being used is Coalfire.

Scope

| Coalfire ASV Configuration | |
|---------------------------------|---------------------------|
| GoDaddy | Media Temple |
| 64.202.161.46 | 64.207.129.30 |
| 64.202.184.1 | 64.207.129.182 |
| 64.202.185.1 | 64.207.129.252 |
| 72.167.70.1 | 208.109.6.238 |
| 72.167.198.1 | 216.69.191.208 |
| 97.74.96.1 | 216.70.122.213 |
| 208.109.6.2 | 216.70.122.217 |
| 208.109.6.14 | 72.10.62.12 - 72.10.62.15 |
| 208.109.147.1 | |
| 208.109.151.1 | |
| 104.238.65.147 - 104.238.65.148 | |
| 208.109.7.1 - 208.109.7.6 | |
| 208.109.7.8 - 208.109.7.63 | |

Schedule

The scan schedule is set on the Coalfire system via the web GUI. The PCI ASV scans for GoDaddy and Media Temple are set to run at 2am on the 1st of every month. This can be edited via the Projects (Preview) Tab on the main Coalfire page:



| Project | Type | Status | % Complete | Overdue AI | Customer AI | Schedule Start | Schedule End | Constraint |
|--------------|----------------|--------|------------|------------|-------------|----------------|--------------|------------|
| GoDaddy | External - ASV | Active | - | 0 | 0 | - | - | 0 |
| Media Temple | External - ASV | Active | - | 0 | 0 | - | - | 0 |

- Click on the name of the Project – in this case "GoDaddy" – to bring up the External ASV main page for the GoDaddy Project

- Click on the "Setup" tab to open up the various setup related tabs and sections. By default, the "Schedule" tab is selected

- Click on the schedule name – in this case "GoDaddy" – to open the Edit Schedule page

- In the two highlighted red boxes are the settings for the scan itself. You can see that it is set to run at 2:00am GMT-7 (Phoenix time) every month on the 1st day of the month

General Outline

Must be completed for both the GoDaddy Project and the Media Temple Project that have been setup in the Coalfire system. (Note: There used to be two different login accounts, one for GoDaddy and one for Media Temple. Due to Coalfire licensing changes, this is no longer the case. Rather, there is one login account and each of these two entities is set up as a separate project)

- After the 1st of each month, log on to the Coalfire console at <https://one.coalfire.com>:
-

- The first screen you will see is the Coalfire Home Screen:
-
- Click on the Project name – in this case "GoDaddy" – to get to the External ASV screen for the Project:
-
- The "Current Quarter" tile will say one of two things – either "PASSING" (which is what we want) or "FAILING" (which means we have scan findings that need addressing). In this case, we have a "FAILING" status and can see in the "Top 10 Failing Vulnerabilities" tile that we have a High "X.509 Certificate Subject CN Does Not Match the Entity Name" issue. To address this finding, we need to click on the "Analyze" tab to get to the Analyze screen for the project:
-

Handling disputes

We can see on this screen that the X.509 vulnerability is the only one that we need to address. Click on the "Hosts" tab to bring up the Hosts screen:

Only one host is failing compliance due to this finding, so click on the row next to the IP address to highlight it (it turns a dark gray), then click on the three dots above and to the right of the list of rows (where the red arrow is pointing):

A drop-down menu opens, and the "Add dispute" option will allow us to dispute this particular finding (because this particular finding should be disputed as it is not a configuration or vulnerability issue). Click on the "Add dispute" option to open the Create Dispute screen:

Click on the "Category" line to open the dispute category drop-down:

In this case, the finding is a false positive because Coalfire is scanning for the IP address, and the certificate's "Subject CN" is correctly set to the actual site name rather than its IP address. Coalfire does not know the site name and does not scan for it that way. Therefore, select "False Positive" from the category drop-down:

Next, in the Reason box, enter in the following language for this particular vulnerability (if different, then provide the correct reason): "The server does not serve websites under its IP address. The certificate CN matches the name of the website being served, as it should." Then click the "Submit For Review" button in the top right-hand corner of the screen. (NOTE: If the finding had been valid, then the proper procedure is to generate a ServiceNOW Problem ticket for the server owner to get the vulnerability remediated)

After submitting the dispute for review, you will be taken back to the "Hosts" screen. Click on the "Disputes" tab to examine the state of the dispute that was just filed:

You can see that a previously submitted False Positive dispute was "APPROVED", and the one that was just submitted is "PENDING REVIEW". After the dispute is reviewed, the system will email the submitter a status of the dispute. Once the dispute is approved, log back into the Coalfire interface and navigate to the Project → External ASV tab as was done previously:

If a dispute is "REJECTED" you can view comments by clicking on the dispute section, clicking in to the dispute, and clicking the arrow to see the "Comments" section.

You can see in the "Current Quarter" tile that the scan status is now "PASSING". Click on the "Analyze" tab to navigate to the Analyze screen:

We can see multiple findings on the right

Click on the legitimate finding on the right, you should see a page that looks like the following:

Find the owning group of the IP address using CMDB, IPPlan, or simply searching it in Confluence.

Create a Problem ticket

Assignment group: The group that owns the box.

Root cause: Security.Vulnerability

Vulnerability type: PCI

Vulnerability Criticality: Pull from the Vulnerability Details page. In this example, it would be medium.

Impact/urgency: the same rating as the vulnerability finding. In this example, both would be a 2 - Medium to make the priority medium.

Description: paste the Impact and Remediation sections from Coalfire into the ticket. Include the ip address

Title: The title of the Vulnerability. In this example, "Apache default installation/welcome page installed". Append the host name to it, so it would look like "Apache default installation/welcome page installed - 208.109.7.9".

Check the ticket every day to determine if it has been remediated.

Once the ticket has been remediated, rescan the box. There should be no findings. If there are, the box was either not patched or is throwing a false positive.

Generate reports

The next thing we need to do is generate the reports necessary for audit purposes. Click on the "Hosts" tab to navigate to the Hosts screen:

Note that all Addresses listed now have a status of "PASS". To generate reports, click on the "plus" icon near the top right corner of the Hosts list:

This will open the Generate Reports dialog. Click on the light gray "Add" link to specify the reports to be generated:

The drop-down list will open, displaying the top-most report types first:

Use the scroll bar in the drop-down to scroll to the bottom of the list of possible report types:

The three reports that we want are the last three in this list – namely, "AoSC Mod90Day.pdf", "Detailed Report Mod90Day.pdf", and "Summary Report Mod90Day.pdf". Click on the "AoSC Mod90Day.pdf" entry to add it to the list of reports to generate:

Next, click on the "Detailed Report Mod90Day.pdf" and "Summary Report Mod90Day.pdf" entries to add them as well. Then click on the light gray "Generate" button to submit the report generation request:

After the reports are generated, the Coalfire system will email you when each report is done being generated. Once you receive the email, click on the "Reports" tab in the External ASV view of the Project to open the Reports screen:

The Reports screen will show all three generated reports:

Click on the name of the report that you would like to download (it will underline like a hyperlink), then your normal browser download process will occur:

Click on the names of the other two reports that you generated to download them as well, then attach all three downloads to the JIRA story for the GoDaddy ASV PCI Monthly Audit.

Add a link to the JIRA story on the [Audit Calendar](#) where Compliance can fetch it.

Repeat this process for the Media Temple project, and you are all done!

NOTE:

If the result is a Fail, the result MUST be remediated within the current calendar month in one of the following methods:

Dispute the finding via the Coalfire interface

If the Dispute is approved, the Compliance result will automatically update to Pass and the above PDFs can be generated, downloaded and stored.

If the Dispute is denied, follow the steps below for remediation

Create a ServiceNow ticket for the relevant host owner to remediate the finding.

Once the finding has been remediated, contact Coalfire support to repeat the scan so that the results update and the Compliance result is a Pass. After result is Pass, store in JIRA per the above steps and update the Audit Calendar

Administration

User Administration

This describes how to add a new user to the account, and also how to make them an administrator. **This requires that you are already an admin.** If you are not, ask an existing admin to add you. If no admin is available (eg. left the company) then open a ticket with CoalFire support requesting admin status.

1. Navigate to <https://one.coalfire.com/> and login

2. Click Administration

 > [Click here to expand...](#)

3. Click Users

 > [Click here to expand...](#)

4. Click Create New User
 - » [Click here to expand...](#)

5. Fill out all of the required information (red asterisks). To make the user an admin, check the "Administrative Users" security group membership. Otherwise, check "Users".
6. Click "Save and Set Credentials"
 - » [Click here to expand...](#)

7. An email should be sent to the new user for activation.
8. Done!

Resources and Definitions

Internal Resources

Audit Tracking Calendar - [Audit Tracking](#)

External Resources

Coalfire - <https://one.coalfire.com>

Associated Audit Controls / Requirements

| Audit Type | Process Specifics | Requirement | Requirement Label |
|------------|--------------------|---|-------------------|
| PCI | Process - Step 2.1 | <i>Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC)</i> | PCI DSS 3.2.1 |

Table of Contents

General Information

| | |
|-----------------------|---|
| Responsible Team | Security Risks & Assessments (SRA) - Slack: vulnerability_mgmt - Email: sra@godaddy.com |
| Process Owner | Warren Harris |
| Last Review Date | 2020-03-03 |
| Escalation Contact(s) | Bindi Davé |
| Requests for Updates | Security Risks & Assessments |

Process Summary

This process provides direction for the detection, analysis and remediation of <X> event types and outlines the general process guidelines to be followed by Incident Response analysts. A summary of applicable use cases for this process are as follows:

- PCI DSS 3.2.1 includes requirement 11.2.2 to "Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC)."

To meet this requirement we engage the services of an Approved Scanning Vendor (ASV) to perform regular scans. The vendor may change due to the regular vendor issues (quality, responsiveness, cost) but it will always be an ASV verified with the PCI Council list.

- PCI 11.2.2 requires scans to be performed a minimum of quarterly. In practice, the card processors expect to see a report within 90 days of the previous report.

Process-Specific DefinitionsSupporting Documentation

- PCI
 - [Section 11.2.2 PCI DSS...](#)



Process Workflow

- [Process Diagram...](#)

Process Outline and Details

Summary

The Monthly ASV Vulnerability scans are performed by third-party scanning vendors. Once per month scans are automatically started. Upon completion, the scan reports are retrieved from the vendors via a web GUI. The results are parsed for findings and tickets are created in the ticketing system - currently ServiceNOW. After ticketing is complete and

the issues remediated, the reports are attached to the JIRA stories (currently on the ESA board) and links to the stories are added to the [Audit Calendar](#). The PCI ASV currently being used is Coalfire.

Scope

| Coalfire ASV Configuration | |
|---------------------------------|---------------------------|
| GoDaddy | Media Temple |
| 64.202.161.46 | 64.207.129.30 |
| 64.202.184.1 | 64.207.129.182 |
| 64.202.185.1 | 64.207.129.252 |
| 72.167.70.1 | 208.109.6.238 |
| 72.167.198.1 | 216.69.191.208 |
| 97.74.96.1 | 216.70.122.213 |
| 208.109.6.2 | 216.70.122.217 |
| 208.109.6.14 | 72.10.62.12 - 72.10.62.15 |
| 208.109.147.1 | |
| 208.109.151.1 | |
| 104.238.65.147 - 104.238.65.148 | |
| 208.109.7.1 - 208.109.7.6 | |
| 208.109.7.8 - 208.109.7.63 | |

Schedule

The scan schedule is set on the Coalfire system via the web GUI. The PCI ASV scans for GoDaddy and Media Temple are set to run at 2am on the 1st of every month. This can be edited via the Projects (Preview) Tab on the main Coalfire page:

| Project | Type | Status | % Complete | Overdue AI | Customer AI | Schedule Start | Schedule End | Constraint |
|--------------|----------------|--------|------------|------------|-------------|----------------|--------------|------------|
| GoDaddy | External - ASV | Active | - | 0 | 0 | - | - | 0 |
| Media Temple | External - ASV | Active | - | 0 | 0 | - | - | 0 |

- Click on the name of the Project – in this case "GoDaddy" – to bring up the External ASV main page for the GoDaddy Project

Hosts
By passing fail: Passing Hosts 72 Failing Hosts 1

Top 10 Failing Vulnerabilities
By Instances

| Vulnerability | Severity | Instances |
|--|----------|-----------|
| 3.0K Certificate Subject CN Does Not Match the Entity Name | High | 1 |

- Click on the "Setup" tab to open up the various setup related tabs and sections. By default, the "Schedule" tab is selected

- Click on the schedule name – in this case "GoDaddy" – to open the Edit Schedule page

- In the two highlighted red boxes are the settings for the scan itself. You can see that it is set to run at 2:00am GMT-7 (Phoenix time) every month on the 1st day of the month

General Outline

Must be completed for both the GoDaddy Project and the Media Temple Project that have been setup in the Coalfire system. (Note: There used to be two different login accounts, one for GoDaddy and one for Media Temple. Due to Coalfire licensing changes, this is no longer the case. Rather, there is one login account and each of these two entities is set up as a separate project)

- After the 1st of each month, log on to the Coalfire console at <https://one.coalfire.com>:
- The first screen you will see is the Coalfire Home Screen:
- Click on the Project name – in this case "GoDaddy" – to get to the External ASV screen for the Project:
- The "Current Quarter" tile will say one of two things – either "PASSING" (which is what we want) or "FAILING" (which means we have scan findings that need addressing). In this case, we have a "FAILING" status and can see in the "Top 10 Failing Vulnerabilities" tile that we have a High "X.509 Certificate Subject CN Does Not Match the Entity Name" issue. To address this finding, we need to click on the "Analyze" tab to get to the Analyze screen for the project:
- False positive findings**
 - We can see on this screen that the X.509 vulnerability is the only one that we need to address. Click on the "Hosts" tab to bring up the Hosts screen:
 - Only one host is failing compliance due to this finding, so click on the row next to the IP address to highlight it (it turns a dark gray), then click on the three dots above and to the right of the list of rows (where the red arrow is pointing):

- A drop-down menu opens, and the "Add dispute" option will allow us to dispute this particular finding (because this particular finding should be disputed as it is not a configuration or vulnerability issue). Click on the "Add dispute" option to open the Create Dispute screen:
 - Click on the "Category" line to open the dispute category drop-down:
 - In this case, the finding is a false positive because Coalfire is scanning for the IP address, and the certificate's "Subject CN" is correctly set to the actual site name rather than its IP address. Coalfire does not know the site name and does not scan for it that way. Therefore, select "False Positive" from the category drop-down:
- Next, in the Reason box, enter in the following language: "The server does not serve websites under its IP address. The certificate CN matches the name of the website being served, as it should." Then click the "Submit For Review" button in the top right-hand corner of the screen. (NOTE: If the finding had been valid, then the proper procedure is to generate a ServiceNOW Problem ticket for the server owner to get the vulnerability remediated)
- After submitting the dispute for review, you will be taken back to the "Hosts" screen. Click on the "Disputes" tab to examine the state of the dispute that was just filed:
 - You can see that a previously submitted False Positive dispute was "APPROVED", and the one that was just submitted is "PENDING REVIEW". After the dispute is reviewed, the system will email the submitter a status of the dispute. Once the dispute is approved, log back into the Coalfire interface and navigate to the Project→External ASV tab as was done previously:
- You can see in the "Current Quarter" tile that the scan status is now "PASSING". Click on the "Analyze" tab to navigate to the Analyze screen:

› [Legitimate findings](#)

We can see multiple findings on the right

Click on the legitimate finding on the right, you should see a page that looks like the following:

Find the owning group of the IP address using CMDB, IPPlan, or simply searching it in Confluence

Create a Problem ticket

Assignment group: The group that owns the box.

Root cause: Security.Vulnerability

Vulnerability type: PCI

Vulnerability Criticality: Pull from the Vulnerability Details page. In this example, it would be medium.

Impact/urgency: the same rating as the vulnerability finding. In this example, both would be a 2 - Medium to make the priority medium.

Description: paste the Impact and Remediation sections from Coalfire into the ticket. Include the ip address
Title: The title of the Vulnerability. In this example, "Apache default installation/welcome page installed". Append the host name to it, so it would look like "

Apache default installation/welcome page installed

The next thing we need to do is generate the reports necessary for audit purposes. Click on the "Hosts" tab to navigate to the Hosts screen:

Note that all Addresses listed now have a status of "PASS". To generate reports, click on the "plus" icon near the top right corner of the Hosts list:

This will open the Generate Reports dialog. Click on the light gray "Add" link to specify the reports to be generated:

The drop-down list will open, displaying the top-most report types first:

Use the scroll bar in the drop-down to scroll to the bottom of the list of possible report types:

The three reports that we want are the last three in this list – namely, "AoSC Mod90Day.pdf", "Detailed Report Mod90Day.pdf", and "Summary Report Mod90Day.pdf". Click on the "AoSC Mod90Day.pdf" entry to add it to the list of reports to generate:

Next, click on the "Detailed Report Mod90Day.pdf" and "Summary Report Mod90Day.pdf" entries to add them as well. Then click on the light gray "Generate" button to submit the report generation request:

After the reports are generated, the Coalfire system will email you when each report is done being generated. Once you receive the email, click on the "Reports" tab in the External ASV view of the Project to open the Reports screen:

The Reports screen will show all three generated reports:

Click on the name of the report that you would like to download (it will underline like a hyperlink), then your normal browser download process will occur:

Click on the names of the other two reports that you generated to download them as well, then attach all three downloads to the JIRA story for the GoDaddy ASV PCI Monthly Audit.

Add a link to the JIRA story on the [Audit Calendar](#) where Compliance can fetch it.

Repeat this process for the Media Temple project, and you are all done!

NOTE:

If the result is a Fail, the result MUST be remediated within the current calendar month in one of the following methods:

Dispute the finding via the Coalfire interface

If the Dispute is approved, the Compliance result will automatically update to Pass and the above PDFs can be generated, downloaded and stored.

If the Dispute is denied, follow the steps below for remediation

Create a ServiceNow ticket for the relevant host owner to remediate the finding.

Once the finding has been remediated, contact Coalfire support to repeat the scan so that the results update and the Compliance result is a Pass. After result is Pass, store in JIRA per the above steps and update the Audit Calendar

Administration

User Administration

This describes how to add a new user to the account, and also how to make them an administrator. **This requires that you are already an admin.** If you are not, ask an existing admin to add you. If no admin is available (eg. left the company) then open a ticket with CoalFire support requesting admin status.

1. Navigate to <https://one.coalfire.com/> and login

2. Click Administration

› [Click here to expand...](#)

3. Click Users

› [Click here to expand...](#)

4. Click Create New User

› [Click here to expand...](#)

5. Fill out all of the required information (red asterisks). To make the user an admin, check the "Administrative Users" security group membership. Otherwise, check "Users".

6. Click "Save and Set Credentials"

› [Click here to expand...](#)

7. An email should be sent to the new user for activation.

8. Done!

Resources and Definitions

Internal Resources

Audit Tracking Calendar - [Audit Tracking](#)

External Resources

Coalfire - <https://one.coalfire.com>

Associated Audit Controls / Requirements

| Audit Type | Process Specifics | Requirement | Requirement Label |
|------------|--------------------|---|-------------------|
| PCI | Process - Step 2.1 | <i>Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC)</i> | PCI DSS 3.2.1 |

old Monthly External Vulnerability ASV Audit Scans-Qualys (PCI and PKI)

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [Summary](#)
 - [Audit Requirements](#)
 - [Process-Specific Definitions](#)
 - [PKI Critical Vulnerability - 96 hour rule](#)
 - [Supporting Documentation](#)
 - [PKI](#)
 - [PCI](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Ticket Recording Guide](#)
 - [Process-Specific Priority Matrix](#)
 - [General Outline](#)
 - [Captured Metrics - N/A](#)
 - [Process FAQs](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)
 - [Associated Audit Controls / Requirements](#)

General Information

| | |
|-----------------------|---|
| Responsible Team | Security Risks and Assessments (SRA) - Slack: vulnerability_mgmt - Email: sra@godaddy.com |
| Process Owner | SRA |
| Last Review Date | 2020-03-30 |
| Escalation Contact(s) | Bindi Davé |
| Requests for Updates | Security Risks & Assessments (SRA) |

Process Summary

Summary

This process provides direction for how to execute on the monthly external ASV audit scans. A summary of this process is as follows:

1. The External monthly scans are performed by third-party scanning vendors.
2. Once per month scans are automatically started.
3. Once complete, the scan reports are retrieved from the vendors via a web GUI.
4. The results are parsed for findings and tickets are created in the ticketing system - currently ServiceNOW.
5. Once ticketing is complete, the reports are attached to and linked in the [Audit Calendar](#).

Audit Requirements

- PCI DSS 3.2 includes requirement 11.2 to "*11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).*"
 - We currently scan two PCI sites, [payments.madmimi.com](#) and [checkout.afternic.com](#) with an independent external scan vendor, that targets web vulnerabilities rather than the more general ASV scan. This provides better results in addition to our ASV scan, and while not a requirement of PCI DSS 3.2, Compliance has asked that we continue these scans, and pull the report as a separate item in the Audit Calendar as auditors do occasionally request these scans.
- PKI WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Version 2.2, Principle 4: Section 4.3 requires "*The CA maintains controls to provide reasonable assurance that a Vulnerability Scan is performed on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following:*"
 - *Within one week of receiving a request from the CA/Browser Forum;*
 - *After any system or network changes that the CA determines are significant; and*
 - *At least once per quarter "*

Process-Specific Definitions

PKI Critical Vulnerability - 96 hour rule

- GoDaddy has 96 hours from when the scan has completed and a critical vulnerability has been found, to re-mediate the vulnerability

| | |
|------------------|--|
| Procedure | <ol style="list-style-type: none"> ServiceNow ticket is created for server owner Server owner is notified via communication channels (slack or email, or other official form of communication sanctioned by GoDaddy) Server owner has to implement one of the following actions |
| Actions | <ol style="list-style-type: none"> Remediate the vulnerability. If remediation is not possible within 96 hours, implement a formal written plan (can be in ticket) to mitigate and track such remediation within the ticket. Identify the item as a false positive, document this is a false positive and why in the ticket, and follow the exceptions process to acquire an exception for this finding. Then notify ESA at esa@godaddy.com so they can issue the false positive to the ASV. |

Supporting Documentation

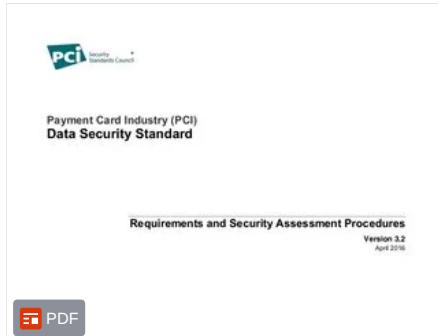
PKI

- [Principle 4: Section 4.3...](#)



PCI

- [Section 11.2 PCI DSS...](#)



Process Workflow

- [Click here to see process workflow...](#)

Process Outline and Details

Ticket Recording Guide

| Problem Ticket | |
|----------------------------------|--|
| Root Cause | Security.Vulnerability |
| Vulnerability Type | Env that the hosts are in (PKI, PCI, SOX, etc) |
| Vulnerability Criticality | Set to the severity of the report's finding |

Process-Specific Priority Matrix

The priority is set by the severity of the finding provided in the report.

Criticals found in PKI must follow the 96-hour PKI critical process.

General Outline

1. The External monthly scans are performed by third-party scanning vendors. Once per month scans are automatically started. Once complete, the scan reports are retrieved from the vendors via a web GUI. The results are parsed for findings and tickets are created in the ticketing system – currently ServiceNOW. Once ticketing is complete, the reports are filed and linked in the [Audit Calendar](#).
2. The scheduling is set on the Vendor system via the web GUI. Currently scans are set to run between 2am and 10am on the 1st of every month. Make sure to change the schedule for each target that needs it. This typically can be left alone unless audit requirement changes dictate otherwise.
 - › [Click here to see schedule UI...](#)

Schedule Vulnerability Scan Edit: api.pkl.starfieldtech.com

Turn help tips: On | Off | Launch help X

Edit Mode

Configure task start date and occurrence

Task details >

Target >

Settings >

Scheduling > (1 REQUIRED FIELDS)

Notification >

Action Log >

Recurrence

Mode* **Monthly** Recurrence

Ends after occurrences

Day of every month

The of every month

Launch Information

Start Date **Sun 01 Dec 2013** Time* **03:00**

Time Zone* **(GMT -06:00) Mountain Standard Time (MDT America/Bois)**

Duration

Cancel Option **Do not Cancel Scan**

Cancel Download as iCalendar Save As... Save

3. After the 1st of each month, log on to the [Qualys console](#):

› [Click here to see login screen...](#)



4. Select the WAS (Web Application Scanning) Service

› [Click here to expand image...](#)

Qualys. Express

Vulnerability Management | Help | Scott Neville (gtdadd2s) | Logout

Welcome to QualysGuard Express

Your subscription includes the following applications.

Click one to get started.

VM

Vulnerability Management

1 Total IPs

PCI

PCI Compliance

WAS

Web Application Scanning

25 Web Applications

5. Select the "Web Applications" tab to get the list of apps that are being scanned, and check the "Scanned" column to confirm that it was scanned on the first of the month:

› [Click here to expand image...](#)

6. Select the "Reports" tab and click the "New Report" button:
 > Click here to expand image...

7. Ensure that both drop-down boxes are set to "Web Application Report" and click "Continue":
 > Click here to expand image...

8. Use the "Select Web Applications" drop-down to find the site you wish to include in the report. Once selected, it will show in the area directly below the drop-down. If you wish to add multiple sites to one report (as we do with the multiple PKI websites), repeat the process until all are showing below the drop-down. The report will generate and display on the screen. Review it to confirm that it contains everything you need (all expected sites are listed, etc). Then

click "Finish".

For PCI, the applications are: payments.madmimi.com and checkout.afternic.com (AfterNIC cart)

For PKI, the applications are: certs.godaddy.com, whs.pki.godaddy.com, api.pki.starfieldtech.com, certs.starfieldtech.com, evbeacon.starfieldtech.com, evbeacon.godaddy.com, seal.starfieldtech.com, seal.godaddy.com, and tsa.starfieldtech.com

› [Click here to expand images...](#)

Scan targets as of 2020-03-30:

The screenshot shows the Qualys Web Application Management interface. The left sidebar has sections for Filter Results, Tags, Scan Information, Schedule Information, and Scanner Appliance. The main area displays a table of scanned web applications with columns for Name, # Pages, # Vuls, Severity, MDS Severity, Scanned, and Updated. The table lists various domains including payments.madmimi.com, AfterNIC cart, certs.godaddy.com, whs.pki.godaddy.com, api.pki.starfieldtech.com, certs.starfieldtech.com, evbeacon.starfieldtech.com, evbeacon.godaddy.com, seal.starfieldtech.com, seal.godaddy.com, and tsa.starfieldtech.com.

Create report:

The screenshot shows the "Report Creation" step 2 target selection interface. It has two tabs: "Details" (selected) and "Target". Under "Target", there are sections for "Select target of your report", "Select Tags", and "Select Web Applications". The "Select Web Applications" section lists "api.pki.starfieldtech.com", "certs.godaddy.com", and "certs.starfieldtech.com". A red arrow points from the "Finish" button at the bottom right to the "Save" button in the next screenshot.

9. Click the "Download" button to export a report. Confirm that the format is "Portable Document Format (PDF)" and the Timezone is "(GMT -07:00) Mountain Standard Time (MST America/Phoenix)". Click "Save"

› [Click here to expand image...](#)

The screenshot shows the "Save report" configuration interface. It has fields for "Report Format" (set to "Portable Document Format (PDF)", indicated by a red arrow), "Timezone used for dates in report" (set to "(GMT -07:00) Mountain Standard Time (MST America/Phoenix)", indicated by a red arrow), and "Add tags to the report" (with a "Select" button). A red arrow points from the "Save" button at the bottom right to the "Save" button in the final screenshot.

- The PCI scans are processed as a convenience to the Compliance team, we do not generate tickets from the PCI scan report at this time.
- Any findings on the PKI report of **High** or **Critical** must be ticketed with a ServiceNow Problem ticket. Set the "Root Cause" field to "Security.Vulnerability", the "Vulnerability Type" to whichever environment the hosts are in (PCI/PKI/SOX/etc) and the "Vulnerability Criticality" to the severity of the finding from the report.
- If there are any **PKI Critical** findings, immediately begin the **96 Hour PKI Critical workflow**.
- Attach the reports to the **Audit Calendar** and create a link to it in the appropriate cell.

Captured Metrics - N/A

- Currently, the metrics are the reports themselves, which are on the [Audit Calendar](#).

Process FAQs

This is a link to view the tutorials for PKI/PCI Monthly External Audit reporting, currently hosted on in I-Drive:

- <smb://jomax.paholdings.com/data/itsecurity/Audits/HowTo/External Pentest Audits/>

Resources and Definitions

Internal Resources

All audit documentation is logged and tracked to the [Audit Calendar](#).

External Resources

Qualys Console - <https://qualysguard.qg2.apps.qualys.com>

Associated Audit Controls / Requirements

| Audit Type | Process Specifics | Requirement | Requirement Label |
|------------|-------------------|---|-------------------|
| PCI | Process - Step 2A | <i>Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).</i> | PCI DSS 3.2 |
| PKI | Full Process | <i>The CA maintains controls to provide reasonable assurance that a Vulnerability Scan is performed on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following:</i> <ul style="list-style-type: none">• Within one week of receiving a request from the CA/Browser Forum;• After any system or network changes that the CA determines are significant; and• At least once per quarter " | PKI WebTrust 4.6 |

old Monthly Internal Audit Scan

Process Workflow

Table of Contents

- [Process Workflow](#)
- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [Process-Specific Definitions](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [General Outline](#)
 - [Process Details - Covered above or do we need to port everything hyperlinked from other Confluence pages?](#)
 - [Step A](#)
 - [Step B](#)
 - [Captured Metrics - N/A](#)
 - [Process FAQs - N/A](#)
 - [What happens if "X"?](#)
 - [How can I determine if "Y"?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)
 - [Associated Audit Controls / Requirements](#)

General Information

| | |
|------------------------------|---|
| Responsible Team | Vulnerability Management (VM) - Slack: vulnerability_mgmt - Email: vulnerabilitymgmt@godaddy.com |
| Process Owner | Security Risk & Assessments team (sra@godaddy.com) |
| Last Review Date | 2020-04-08 |
| Escalation Contact(s) | sra@godaddy.com |
| Requests for Updates | sra@godaddy.com |

Process Summary

The policy at GoDaddy is to scan the PCI/SBE, PKI, and SOX environments on a monthly basis to adhere to the below PKI and PCI requirements.. A summary of applicable use cases for this process are as follows:

- **PKI Critical Vulnerability - 96 hour rule** - GoDaddy has 96 hours from when the scan has completed and a critical vulnerability has been found, to remediate the vulnerability
- **PKI Compliance Controls**
 - [Section 4.6 WebTrust...](#)
Error rendering macro 'viewpdf' : Failed to find attachment with Name pki_webtrust_requirements.pdf
- **PCI Compliance Controls**
 - [Section 11.2 PCI DSS...](#)
Error rendering macro 'viewpdf' : Failed to find attachment with Name pci_dss_v3-2.pdf

For the above use cases, GoDaddy administers monthly vulnerability scans for assets in scope for the above compliance definitions.

Process-Specific Definitions

- **Process-Specific:** Pertains only to this process. May have a different definition in other process flows.

Process Workflow

➢ [Click here to view process diagram...](#)



Process Outline and Details

General Outline

1. The following scans are configured in Tenable.io for the **2nd Monday of each month**:
 - a. **PKI** - These are handled by the Vulnerability Response Module in ServiceNow, so you don't need to worry about these for this process.
 - i. Monthly P3 PKI
 - ii. Monthly S2 PKI
 - iii. Monthly SG2 Perseus Nodes
 - iv. Monthly N1 Perseus Nodes
 - v. Monthly CH4 Perseus Nodes
 - vi. Monthly P3 Perseus Nodes
 - vii. Monthly A1 Perseus Nodes
 - b. **PCI** - These get grouped into one report
 - i. Monthly PCI
 - ii. Monthly PCI-Domain Controllers
 - c. **SBE**
 - i. Monthly SBE
 - d. **GFN**
 - i. Monthly GFN
2. Create a ServiceNow Change Request on the **Friday prior to each monthly scan**
 - a. > [Click here to see CHG ticket details...](#)
On the Friday prior to each monthly scan, a Change (CHG) ticket shall be created with the information listed below. Notification of this CHG shall be an email to the SRE_GPD@godaddy.com distro on the Friday before the scan by 12:00 Noon.

CHG Ticket information:

- **Risk:** Low
- **Impact:** Medium
- **Assignment Group:** ENG-VulnerabilityMgmt
- **Assigned To:** <Person that will be running the monthly scan>
- **Title:** "Monthly Internal Audit Scan - <Month>-<Date>-<Year>"
- **Description:** "Monthly Internal Audit for <Month>-<Date>-<Year>. Script located here: https://github.secureserver.net/ContinuousSecurity/monthlyvuln_report/. Supporting documentation here: Monthly Internal Audit Scan (<https://godaddy-corp.atlassian.net/wiki/display/IRKB/Monthly+Internal+Audit+Scan>)."
- **Type:** Manual
- **Approval:** Approved
- **JIRA Issue Key:** If a JIRA is created for this, then provide the key here
- **Change Plan:** "A Tenable.io scan will be automatically performed for PCI, PKI, SBE, and Perseus nodes on the second Monday of this month starting at 00:00 Monday morning."
- **Backout Plan:** "N/A because no actual changes will occur on the systems. Performance degradation may occur but is not expected."
- **Test Plan:** "Scan target owners will contact the Security Risk & Assessments team either via email (sra@godaddy.com) or on Slack (#vulnerability_mgmt)."
- **Planned Start Date:** <Date of second Monday of the month at 00:00>
- **Planned End Date:** <Date of second Monday of the month at 07:00>

Email notification format, sent to SRE_GPD@godaddy.com:

Good Morning,

This is an advance notification that Monthly Internal Audit scans will take place on Monday <Month>-<Date> @ 12:00am. All scans should be complete before 7:00am the same morning.

If you have any questions, please contact our team at sra@godaddy.com or on Slack at #vulnerability_mgmt.

Thanks for your attention,

Security Risks & Assessments, Information Security

3. On the day of scheduled scans, check for completed results for each scan - Download a copy of each in CSV format
 - a. If scans are stuck or taking overly long, a support case should be logged with Tenable.IO
4. Follow the instructions in the GitHub readme.md to create the tickets and process the reports: [ContinuousSecurity/monthlyvuln_report](https://github.secureserver.net/ContinuousSecurity/monthlyvuln_report)
 - a. This will require the following
 - i. Workstation with Docker and Python runtime
 1. Month-Int-Audit.cloud.phx3.gdg is created for this purpose
 - ii. Access to Vulntron and snow service account credentials hosted at I:\ITSecurity\Password Safe\soc (2).kdbx
 1. Vulntron MySQL production database
 2. vulnmgmt_snow_prod
5. Process the results by audit/compliance scope according to the following steps
 - a. PKI

- i. Tickets for PKI related vulnerabilities are automatically created in ServiceNow via the Vulnerability Response module. There is no longer a need to process the results downloaded as CSV from Tenable
- ii. The audit report for PKI can be found in ServiceNow at [VRM - PKI Audit Report](#)
 - 1. An easier report to export can be found in the [Vulnerability Management dashboard under the PKI Monthly Audit tab](#)
- b. PCI
 - i. Import results to the Vulntron Database - [Link](#)
 1. Combine the PCI and Domain Controllers reports under the same vulntron scanid (see the github readme for details)
 - ii. Attach the Audit Report CSV results to the audit page
 - iii. Update the Audit Calendar Confluence page with a link to the attachment containing the audit report results
- c. SBE
 - i. Import results to the Vulntron Database - [Link](#)
 - ii. Attach the Audit Report CSV results to the audit page
 - iii. Update the Audit Calendar Confluence page with a link to the attachment containing the audit report results
- d. GFN
 - i. Import results to the Vulntron Database - [Link](#)
 - ii. Attach the Audit Report CSV results to the audit page
 - iii. Update the Audit Calendar Confluence page with a link to the attachment containing the audit report results

Process Details - Covered above or do we need to port everything hyperlinked from other Confluence pages?

Step A

Use tool (0) and capture "M" data.

(Screenshot?)

Step B

Check the following tools: (1), (2) & (3)

Document findings determine if "X"

Captured Metrics - N/A

- Metric A - Captured using E; (Required/Optional); Reporting example (if needed)
- Metric B - Captured using F; (Required/Optional); Reporting example (if needed)
- Metric C - Captured using G; (Required/Optional); Reporting example (if needed)

Process FAQs - N/A

What happens if "X"?

"X" is caused by A,B or C. Can be handled by doing "D".

How can I determine if "Y"?

"Y" is determined by E or F. If "G", then sometimes "H".

Resources and Definitions

Internal Resources

Github - https://github.secureserver.net/ContinuousSecurity/monthlyvuln_report

Audit Tracking Calendar - </wiki/spaces/VULNMGMT/pages/76588626>

External Resources

Docker - <https://www.docker.com/>

Tenable.io - <https://www.tenable.com/products/tenable-io>

ServiceNow - <https://godaddy.service-now.com/navpage.do>

Associated Audit Controls / Requirements

| Audit Type | Process Specifics | Requirement | Requirement Label |
|------------|--------------------|--|-------------------|
| PKI | Process - Step 2.1 | GoDaddy has 96 hours from when the scan has completed and a critical vulnerability has been found, to re-mediate the vulnerability | PKI WebTrust 4.6 |

old Security@ General Inbox (Old)

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [Process-Specific Definitions](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [CVD Specific](#)
 - [Process FAQs](#)
 - What should we do if we receive multiple False Positive reports?
 - What if the message was also sent to the correct team by the reporter?
 - What if the report was sent to a brand other than GoDaddy (e.g. HEG, MediaTemple, etc)?
 - [Captured Metrics](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)
 - [Communication Templates](#)
 - Internal Reporter
 - External Reporter
 - Other Responses

General Information

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• GCSO<ul style="list-style-type: none">• SLACK: #gcso_team |
| Stakeholders | <ul style="list-style-type: none">• SRA• AppSec |
| Process Owner | @David Dubois (Deactivated) |
| Last Review Date | 2020-10-28 by @David Dubois (Deactivated) |
| Escalation Contact(s) | <ul style="list-style-type: none">• Infosec_Response<ul style="list-style-type: none">• Slack: @ir-team• Email: IR@GoDaddy.com |

Process Summary

This process provides direction for the handling of communications to the Security@ general mailbox. This mailbox serves as a common point of contact for most general security requests from both external and internal entities. Some of the specific use-cases which are seen via this communication method are:

- Coordinated Vulnerability Disclosure (CVD) Notifications
- Reports of Impersonation of GoDaddy (Websites, Phishing Attempts, etc.)
- External Reports of Malicious Customer Activity (Malware, Phishing, Spam, etc.)
- Internal Reports of Suspicious Activity (Phishing, Physical Behavior, etc.)
- General Solicitations (Security Vendors, Services, SPAM, etc.)
- General Security-related Inquiries

Process-Specific Definitions

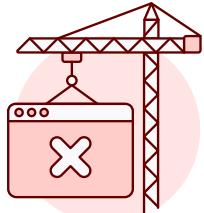
- NONE

Process Workflow



Oops, Diagram Unavailable

This diagram cannot be displayed. It may have been moved, deleted, or you do not have permission to view it.



Oops, Error 500!

Diagram Unavailable

Our system is currently under maintenance. Reach out to your administrator for a fix.

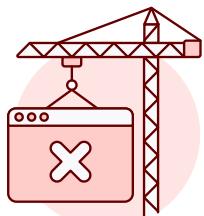


You have an unpublished draft.



Oops, Diagram Unavailable

This diagram cannot be displayed. It may have been moved, deleted, or you do not have permission to view it.



Oops, Error 500!

Diagram Unavailable

Our system is currently under maintenance. Reach out to your administrator for a fix.



You have an unpublished draft.

Process Outline and Details

Incident Recording Guide

| Incident Type | |
|------------------|--|
| Title | <ul style="list-style-type: none"> Created As <ul style="list-style-type: none"> Security@ - <SENDER> - <SUBJECT> Updated To <ul style="list-style-type: none"> Security@<TAG> - <SENDER> - <SUBJECT> <p>Example :</p> <ul style="list-style-type: none"> Ingested: Security@ - myemail@domain.net - i think this is phishing Updated: Security@ABUSE - myemail@domain.net - i think this is phishing |
| Assignment Group | OPS-GCSO |
| Incident Type | <ul style="list-style-type: none"> Incident Category: --NONE-- Incident Subcategory: --NONE-- |

General Outline

- GCSO receives automated SNOW ticket for review.
 - Review the message to identify the communication type
 - Update the Title field with the appropriate tag.
 - Follow the appropriate reporting method.

| Communication Type | Reporting Method | Notified Team | Identification Tag |
|------------------------------------|--|--|--------------------|
| GoDaddy Impersonation | <ul style="list-style-type: none"> If valid, report via FoS Abuse Form If not, Close False Positive | ENG-DCU | GDP |
| Customer Abuse Report | <ul style="list-style-type: none"> Report via FoS Abuse Form <ul style="list-style-type: none"> If this is not possible email to abuse@godaddy.com | ENG-DCU | ABUSE |
| Customer Security Concerns | Close False Positive - No further action | --- | CARE |
| Suspicious Internal Activity | <ul style="list-style-type: none"> If Physical related - Add to Allowed Groups Physical Security Command Center and notify #workplace-services via Slack | <ul style="list-style-type: none"> Physical Security Command Center | EMP |
| Threats or Threat Reports | <ul style="list-style-type: none"> If this is a received threat (not a report from OCEO, WSC, etc.), add to Allowed Groups Physical Security Command Center immediately notify #workplace-services via Slack | Physical Security Command Center | THREAT |
| General Solicitations | Close False Positive - No further action | --- | SPAM |
| Internal Reporter | Forward the email to isitbad@godaddy.com | --- | ISITBAD |
| General Security-Related Inquiries | Assign to @David Dubois (Deactivated) for additional review and notify via Slack/Email | --- | MISC |

CVD Specific

When assessing CVD reports, we should also consider if they align to the report types accepted by the [GoDaddy Coordinated Vulnerability Disclosure policy](#).

› [Excerpt from Policy...](#)

The following actions do not qualify for Coordinated Disclosure and should not be tested by researchers participating in the Program:

- DoS, brute force, user enumeration or DDoS attacks
- Physical attacks
- Phishing attacks
- Any bug that relies on Social engineering
- CRIME/BEAST attacks
- Logout CSRF
- Banner or version disclosures
- Missing SPF records**
- Directory listing (unless sensitive data can be found)
- Blackhat SEO techniques
- Any bug that relies upon an outdated browser

GoDaddy will not accept reports from automated vulnerability scanners.

Specifically, we do not want to route any requests specifically related to **SPF, DKIM or DMARC Configurations** at this time.

| Communication Type | Reporting Method | Notified Team | Identification Tag |
|--------------------|---|---------------|--------------------|
| CVD Notification | <ul style="list-style-type: none"> For any CVD's reported by external/internal security researchers via security@ mailbox, they should submit their vulnerability reports at https://hackerone.com/godaddy-vdp (and the triage will be performed by the H1 team). Communication template added at the bottom to Responsible Disclosure. | ENG-SRA | CVD |

Process FAQs

What should we do if we receive multiple False Positive reports?

Please notify management and/or the process owner if you encounter a situation where we continue to receive unwanted messages. We can review and determine if there is an appropriate method of blocking the sending party if necessary.

What if the message was also sent to the correct team by the reporter?

If the Security@ mailbox was CC'd, BCC'd or otherwise included on a message that was already delivered to the appropriate team we can close the ticket without further action. This will likely be the case only with Abuse-related messages however, and priority items such as CVD notices should still be handled per SOP to ensure they are not missed.

What if the report was sent to a brand other than GoDaddy (e.g. HEG, MediaTemple, etc)?

INTERIM PROCESS: At the moment we do not respond to these directly as our responder mailbox is Security@GoDaddy.com which could cause concerns with brand-differentiation when dealing with customers of GoDaddy sub-brands. These will only come to us if an internal reporter such as a brand-specific team sending it to Security@GoDaddy.com. Please ask the internal contact to respond to the reporter that the message has been routed to the security team for review.

Captured Metrics

- Volumetric Data
- Time In Progress
- Escalated Tickets
- Communication Types

Resources and Definitions

Internal Resources

- [Autoresponse \(HTML\)](#)

External Resources

- NONE

Communication Templates

All communication templates are now vetted and maintained by SRA. Please refer to [Responsible Disclosure#USE_CASES](#)

» Deprecated Templates

Internal Reporter

- » [Direct to IsItBad](#)
<<<EMPLOYEE>>,

Thank you for reporting this to us.

Please be aware that the Security@godaddy.com mailbox is a general communication path with the Security team, however for reports of suspicious/malicious activity please forward the reported email as an attachment to IsItBad@godaddy.com so that we can expedite investigation.

Regards,
GoDaddy Security Team

- » [Direct to Internal Department](#)
<<<EMPLOYEE>>,

Thank you for reporting this to us.

Please be aware that the Security@godaddy.com mailbox is a general communication path with the Security team, however for specific reports and inquiries please contact the appropriate department directly.

Regards,
GoDaddy Security Team

External Reporter

- » [Direct to Customer Support](#)
<<<PERSON>>>,

Thank you for reporting this to us.

We have reviewed your submission and it appears that this matter is best directed to our [Support Team](#). We ask that you contact them for further assistance.

Regards,
GoDaddy Security Team
» [Reply to CVD - Cannot Reproduce](#)
<<<PERSON>>>,

Thank you for reporting this to us.

Unfortunately we were unable to reproduce your report with the information provided and so no further action can be taken at this time. If you believe
Regards,
GoDaddy Security Team

» [Reply to CVD - Request Info](#)
<<<PERSON>>>,

Thank you for reporting this to us.

Unfortunately we were unable to validate your report with the information provided. Please provide us with any steps needed to duplicate as well as a
Regards,
GoDaddy Security Team

» [Reply to CVD - Payout Inquiry \(Need Info\)](#)
<<<PERSON>>>,

Thank you for reporting this to us.

GoDaddy's standard security model is using a Coordinated Vulnerability Policy. While we do not currently operate a formal published bug bounty program
Regards,
GoDaddy Security Team

» [Reply to CVD - Already Reported](#)
<<<PERSON>>>,

Thank you for reporting this to us.

We have reviewed the provided information and confirmed that this issue had been previously reported to us by another party and has already directed

Regards,
GoDaddy Security Team

» [Reply to CVD - Update Requests \(In Progress\)](#)
<<<PERSON>>>,

Your report has been reviewed and directed to the appropriate team(s) for further investigation and remediation. If more information is necessary to

Regards,
GoDaddy Security Team

» [Reply to CVD - Payout Requests \(In Progress\)](#)
<<<PERSON>>>,

Your report has been reviewed and directed to the appropriate team(s) for further investigation and remediation. We are still awaiting updates from t

Regards,
GoDaddy Security Team

» [Reply to CVD - Issue Not Valid](#)
<<<PERSON>>>,

We appreciate you reporting this issue to us. We have directed the provided information to the appropriate team(s) for review and the issue has been

Regards,
GoDaddy Security Team

» [Reply to CVD - Payout \(Request Acceptance\)](#)
<<<PERSON>>>,

While we do not currently operate a formal published bug bounty program, we have been authorized to offer you a reward as a thank you for your effort

Regards,
GoDaddy Security Team

Other Responses

» [External Report - Direct to CVD Path](#)
<<<PERSON>>>,

We appreciate you reaching out and have developed a system for responsible disclosure. To see the details on how to submit a potential issue, please

Thank you,
<<<SENDER>>>

old Server Patching Playbook - Vulnerability Management

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [General Outline](#)
 - [Rebooting Notes for Special Systems](#)
 - [Process Details](#)
 - [Adding custom tags to target endpoints](#)
 - [Create computer group](#)
 - [Create maintenance window](#)
 - [Create and deploy the patch action](#)
 - [Current State \(as of !\[\]\(9d82ecb648168a67037ed08a39027ce0_img.jpg\) 09 Apr 2020 \)](#)
 - [Internal Resources](#)
 - [External Resources](#)
 - [Internal Resources](#)
 - [External Resources](#)

General Information

This playbook describes how to automatically patch the Servers owned by the SRA/ENG-VulnerabilityMgmt teams on a recurring basis.

| | |
|------------------------------|--|
| Responsible Team | #vulnerability_mgmt, sra@godaddy.com, Tier 1 . GSOC: #vm_tier1_priv (must have invite) |
| Process Owner | Security Risks and Assessments (SRA) |
| Last Review Date | 2020-05-22 @Former user (Deleted) |
| Escalation Contact(s) | Security Risks and Assessments |
| Requests for Updates | Contact SRA for process changes or help with Tanium |

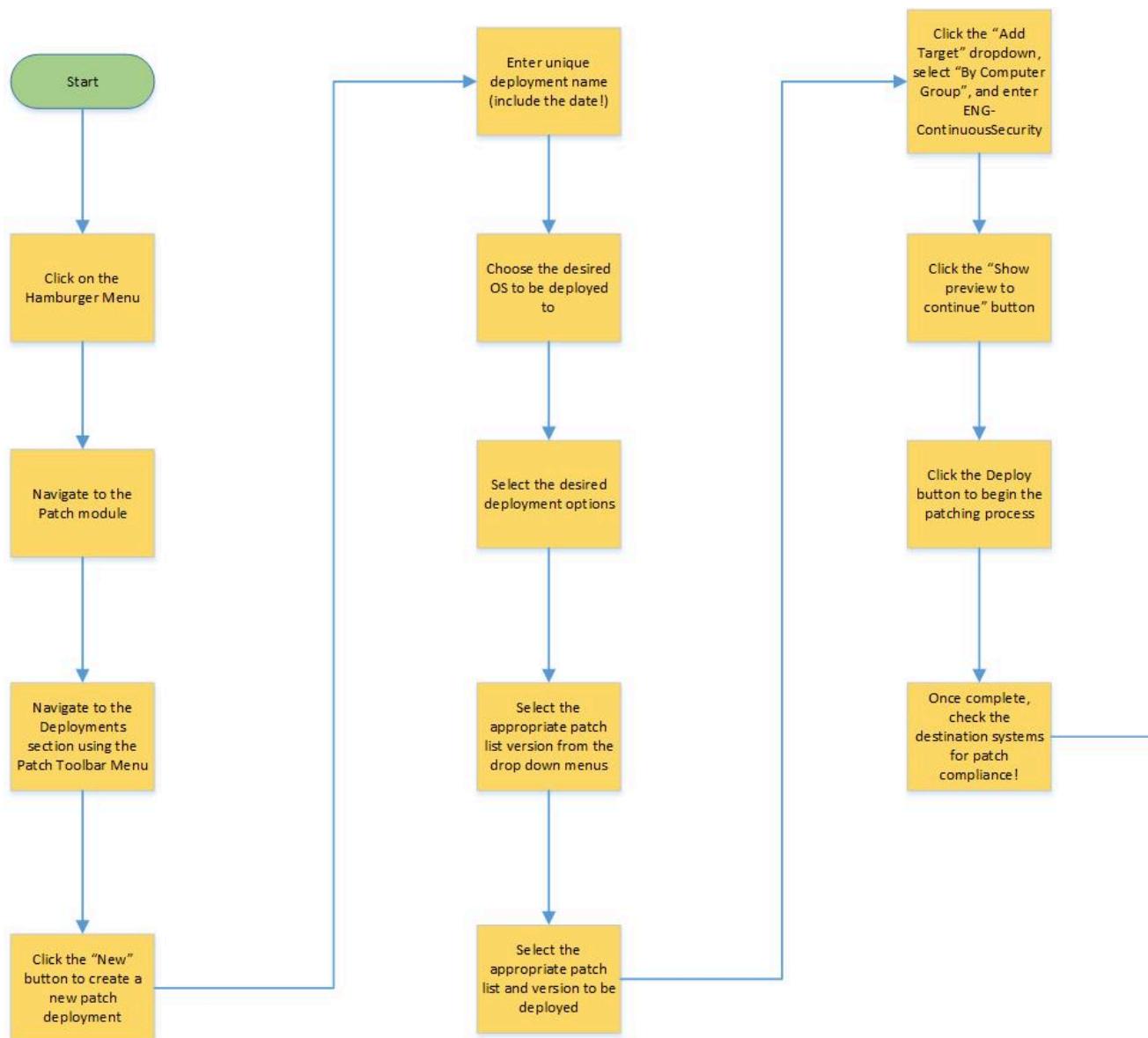
Process Summary

This process provides a methodology to efficiently and automatically patch the Windows and Linux systems owned by the SRA / Vulnerability Management team.

Process Workflow

The work in this diagram is to be done in the [Tanium Console](#).

› [Click here to view the workflow diagram...](#)



Process Outline and Details

General Outline

1. Login to the Tanium Console
2. To add new systems: *Do this whenever new systems are on-boarded*
 - a. Add custom tags to desired endpoints (see Current State section for tag specifics)
 - i. ServiceNOW filter to find all SRA / ENG-VulnerabilityMgmt computers
3. To add a new group of systems (include previous step): *Do this whenever you need a new deployment target set*
 - a. Create a computer group for each custom tag group
4. To create a new patch deployment: *Do this whenever you need a new deployment (ie. if you need one with different options selected)*
 - a. Create a maintenance window for each computer group
 - b. Create and deploy patch actions targeting each computer group
5. Patching: *Do this after every patching cycle*
 - a. After each patching window completes (which means the patch deployment action should have also completed), login to each box that requires a reboot and reboot it (see below for rebooting notes)
 - i. To find SRA/ENG-VulnerabilityMgmt boxes in tanium that have the custom tags discussed in the Current State section, use the [Get all SRA or ENG-VM owned computers](#) saved question
 - ii. **NOTE: Do not reboot any scanners or scan interface computers (eg. AppSpider, ServerScan, Tenable/Nessus scanners) until you have verified that they are not currently running any scans! Failing to do this will cause the systems to drop the scans silently!**

Rebooting Notes for Special Systems

Serverscan

Make sure to gracefully shut down the serverscan docker containers. Make sure there are no scans running in cloud.tenable.com that correspond to scans listed in serverscan.int.godaddy.com first. If so, wait for them to finish.

```
ssh p3plsoctools002.prod.phx3.secureserver.net
sudo docker ps # Check if serverscan is running, should see frontend, scan-runner2, scan-runner,
cd /app/etc/serverscan
sudo ./stop-serverscan-dockers.sh
# Wait for it to complete
sudo reboot
# wait for it to come back up and ssh back into it
ssh p3plsoctools002.prod.phx3.secureserver.net
cd /app/etc/serverscan/
sudo ./start-serverscan-dockers.sh
# Done!
```

p3plsbecsscan01.prod.phx3.gdg

Use the SBE bastion server located on the [Scan Servers](#) page. Use your RSA token and Jomax pw to log in to the bastion, and your Jomax pw for the scan box.

p3plpkicsscan01.pki.gdg

Use the linux PKI bastion on the [Scan Servers](#) page.

a2plpkiten001.pki.gdg

Use this bastion: [p3plpkibhnet01.pki.gdg](#) - 10.6.214.70 (from [this page](#)).

Process Details

Adding custom tags to target endpoints

Do this whenever you need to on-board new systems.

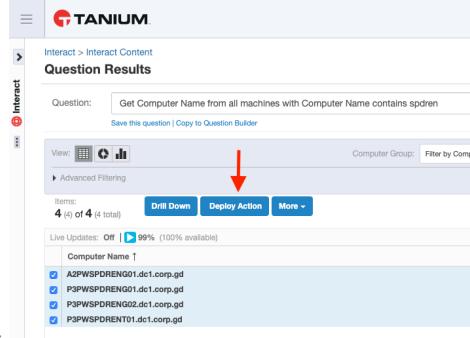
› [Click here to view the steps to prep boxes for patch inclusion...](#)

The endpoints must have a [custom tag](#) so that they can be targeted by the [computer group](#) that will be used for the patch action deployment target. This is less dynamic than using a hostname match, but also more reliable in case someone else names a computer something that would match your query.

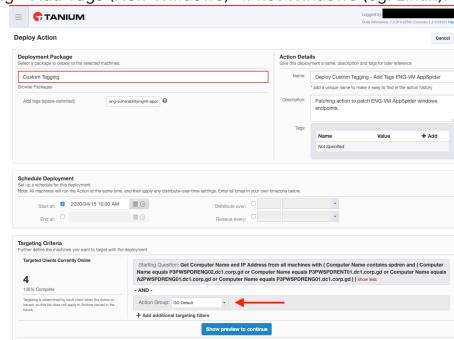
Each time a new endpoint is created, make sure to add the custom tag to it so it gets picked up by the correct computer group.

Steps to add Custom Tags

1. Ask a question in Tanium Interact (can just click the Tanium icon in the upper left corner to get to the question interface) that targets just the endpoints to which you want to add the custom tag. Then select them all and click "Deploy Action" (below image referenced in the following steps)



2. In the Deploy Action interface, under "Deployment Package" search for "Custom Tagging", and add "Custom Tagging - Add Tags" for Windows, or "Custom Tagging - Add Tags (Non-Windows)" if not Windows (eg. Linux).



3. Under Action Details, give the action a descriptive name and description.
4. In "Add Tags (space delimited)", add your desired tags. Ensure that they are unique enough that a collision with other tags is unlikely.
5. Under "Schedule Deployment", select "Start At" and set the date and time that you want the deployment to kick off. Leave it unchecked to run it immediately.
6. Under "Targeting Criteria", notice that the Starting Question is your initial question, plus additions that specifically target the endpoints you selected.
7. Set the "Action Group" to GD-Default.
8. Ensure that the "Targeted Clients Currently Online" matches the count you expect.
9. Click "Show preview to continue" and once the question hits 100% ensure that it returns only and all of the endpoints you expect. If it does not, then start over at step 1 with a more specific initial question. If it does, then click "Deploy Action", and then click "Yes" on the popup.
10. On the next screen you can see the deployment status in real-time. Once the "Completed" bar count matched your expected count, the action is complete.

Action ID: 108508
Source ID: 108508
Status: Queued
Action Group: GD-Default
Start Time: 4/19/2020, 10:45:47 AM
End Time: 4/19/2020, 10:45:47 AM
Comment: cmd.exe /c script.ps1 & /S & /Q & /F & /T 1000 add-tags.ps1
Package Name: Deploy Custom Tagging - Add Tags ENG-VM AppSpider
+ Package Parameters
Add Tags (space delimited): eng-vulnerabilityagent-appspider

a.

11. Your custom tags have been added! To validate, click the Tanium logo, ask the below question, and verify that all and only the machines you targeted show up in the list:
 - a. "Get Computer Name and Custom Tag Exists[your_tag,1]" from all machines with Custom Tag Exists[your_tag,1] contains true", replacing "your_tag" with your tag.

Create computer group

Do this whenever you want to create a new target group, for example if you want different deployment options than the existing ones (eg. to add a linux deployment that auto-reboots).

➤ [Click here to expand...](#)

A computer group should be created for the patch deployment action to target. This way, all you have to do is add the same custom tag to any new endpoints in order to include them in the computer group, which will include them in the patch deployment action.

1. Click the "hamburger button" at the top-left of the interface, then click "Administration", then click "Computer Groups". If you aren't able to do this, then contact a Tanium admin to help you.

New Group New Manual Group

a.

2. Click on "New Group". Note - "New Manual Group" creates a manual group, and those cannot be used for deployment action targeting.

Administration Users User Groups Computer Groups Global Settings Whitelisted URLs System Status Question History

New Group New Manual Group

| Name | Type | Filter Expression |
|----------------|----------|-------------------|
| ENG-VMSERVER01 | Computer | |

a.

3. Enter a unique name for your new group. Click "Filter Builder" and create the filter you'll use to include endpoints in the group. For this case, select "Custom Tag Exists" contains "true", with "Custom Tag" being the tag name you previously created. Then click "Apply" in the filter builder, and finally click "Save".

New Computer Group

Details: Name: ENG-VulnerabilityAgent-AppSpider

Members:

from computers with:

Filter Type: Sensor
Custom Tag Equals: True
Custom Tag Name: eng-vulnerabilityagent-appspider

a.

4. The preview will come up at the bottom. Once it reaches 100%, ensure that all and only the expected endpoints show up. If not, then check your custom tagging (see the "Adding custom tags to target endpoints" section). Once you are satisfied with the preview, click "Save",, and then "Yes" on the popup.
5. To verify that your computer group was created successfully, go back to "Administration" → "Computer Groups" (you should be brought here automatically after the previous step). Use the filter at the top-right to find your computer group. If it is there then it was created successfully.
6. To verify that your computer group is targeting the correct computers, click the Tanium logo, enter the following question (replacing "your_tag" with your tag), and verify that all and only the machines you targeted show up in the list:
 - a. "Get Computer Name and Custom Tag Exists[your_tag,1] from all machines with Custom Tag Exists[your_tag,1] contains true"
7. The computer group has been created and configured! Now all you have to do is add the custom tag to any new endpoints and they will automatically be included in the computer group.

Create maintenance window

Do this whenever you create a new deployment or need to adjust when the deployments occur.

› [Click here to expand...](#)

In order to control when your patch deployment action can run, you must create a **maintenance window**. This is the time during which your action is allowed to occur. Each action target may commence their deployment at any time during this window. Ensure that it is long enough to account for any downloads if the deploy action is not configured to "Download Immediately".

1. Navigate to "Maintenance Windows" and click "Create Window".

| ID | Targeted Computer Groups | Type | Effective Date | Summary (Local Endpoint Time) |
|---|--------------------------|---------|----------------|--|
| ID: 3 - SRE-GPD Group A | Tanium | Windows | 03/18/2019 | Every month on the third Monday from 7:00 PM to 3:00 AM |
| ID: 4 - Non-AZ Business Hours | Tanium | Windows | 03/23/2020 | Every week on Monday, Tuesday, Wednesday, Thursday, Friday from 8:00 AM to 6:00 PM |
| ID: 5 - eng-vulnerabilitymgmt-appspider-patch | Tanium | CentOS | 04/15/2020 | Every week on Wednesday from 10:00 AM to 2:00 PM |

- a.
2. Give your window a unique name and select the correct "Platform OS". This will bring up the rest of the form. Example settings may be (but customize to your needs):
 - a. Window Time: Window Issuer's Browser Time
 - b. Repeats: Weekly (or however often you want it to occur)
 - c. Start Date: When the window will initially start. It will not be open prior to this date/time.
 - d. Duration: Both values must be filled in. This is the length of the window. Ensure it is long enough for your deployment to complete.
 - e. Repeats Every: How often the window repeats
 - f. Repeat On: On which days the window repeats
3. Click "Create" at the bottom once the window is configured to your needs.

- a.
4. On the new window, click "Add Computer Group" under the "Targeted Computer Groups" section. Then select your computer group from the list and click "Add". Note - a window is associated with specific groups, not actions.

- a.
5. The window will then initialize, which may take a few minutes. Once this is done, your maintenance window is complete!

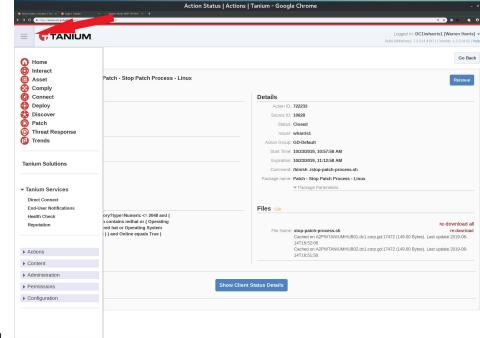
Create and deploy the patch action

This only needs to be done once per deployment. Once deployed, it will run automatically according to the associated maintenance window if set to on-going.

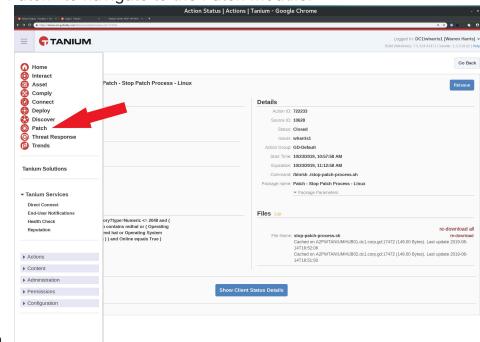
› [Click here to view deployment configuration steps...](#)

Once the computer group has been successfully created, you can create the patching deployment action.

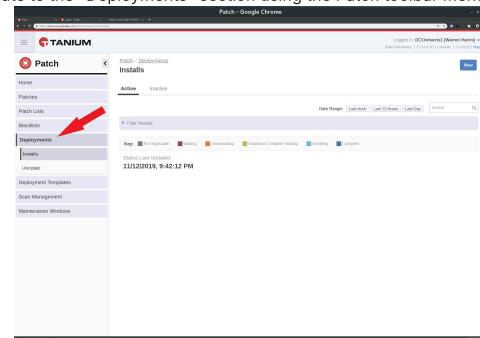
1. Login to the Tanium Console and click on the "hamburger" menu.



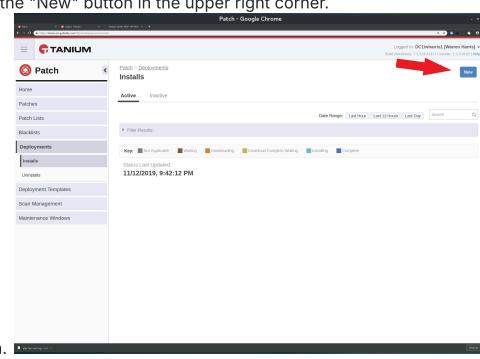
2. Click "Patch" to navigate to the Patch Module.



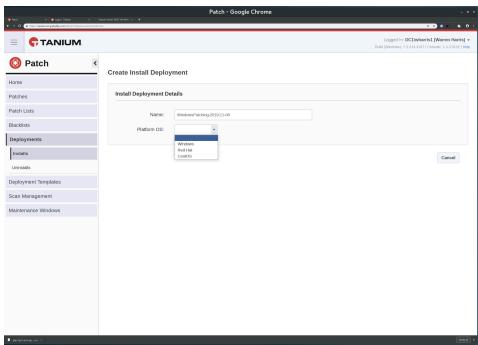
3. Navigate to the "Deployments" section using the Patch toolbar menu and click "Installs"



4. Click the "New" button in the upper right corner.



5. Enter a unique name for the Deployment & Choose the "Platform OS". The OS will determine which options are presented in the rest of the form.



- a.
6. In the newly displayed "Deployment Options, Workflow and Notifications Section", select the desired options.
- Some example settings are:
 - Window Issuer's Browser Time
 - Select from list (choose the correct deployment template, dependent on platform OS)
 - Deployment Template - Select from list → Pick your deployment template.
 - Deployment Type
 - Use Ongoing Deployment to make it always run. Use this for scheduling recurring deployments by also adding a maintenance window to specify the times it can run
 - Use Single Deployment to just run it once at the specified time
 - Download immediately - checked
 - This means that the packages will be downloaded when they become available, but only installed during the maintenance window. This prevents the deployment from failing if the download takes longer than the window allows.
 - Will restart: Depends on if you want the targets to restart once patched
 - For CentOS, typically choose all patches will be installed (could do just security patches too)

b.

- c.
7. Add "Patch List" and "Version options" for Windows (can use "Latest"), or select one of the "Patches" option for Linux

- a.
8. In the "Target" section, select "By Computer Group or Targeting Question", then "Add Target" dropdown. Note, manual computer groups cannot be used for this. Select "By computer group" to use the previously created computer group.

a.

9. Click on the "Show preview to continue" button

a.

10. Click on the Deploy button to begin the deployment if the preview looks good, then click "Yes" in the popup. It should have the expected number of "Targeted Clients Currently Online" (should match your computer group configuration).

a.

11. The following page summarizes the deployment action configuration and initialization status.

12. Complete! Your action is now ready. If you completed the previous sections, then this should only be allowed to run during your maintenance window, starting at the specified time.

Current State (as of  09 Apr 2020)

- A custom tag has been pushed to the known linux boxes called **eng-vulnerabilitymgmt-linux**.
- A custom tag has been pushed to the known Windows AppSpider boxes called **eng-vulnerabilitymgmt-appspider**.
 - Will need to push the custom tag to any new machines to be picked up by the computer group
- The computer groups **ENG-VulnerabilityMgmt-Linux** and **ENG-VulnerabilityMgmt-AppSpider** have been created that pick up any machine with the above custom tags, respectively.
- The patch deployment names are **eng-vulnerabilitymgmt-linux-patch** and **eng-vulnerabilitymgmt-appspider-patch**, and are configured to be **on-going, no reboots, download immediately, and targets the above computer group**
 - This means that we will have to manually reboot the servers after the window closes (see Rebooting Notes section for specifics on special machines)
 - Adding endpoints to the aforementioned computer groups will automatically include them in their respective deployment action
 - **Ensure that no scans are running on the servers before reboot or they will be lost! This includes AppSpider, Tenable, and ServerScan.**
- The maintenance windows, which control the scheduling of the patch deployment, are called **eng-vulnerabilitymgmt-linux-patch** and **eng-vulnerabilitymgmt-appspider-patch**. **Reboots must happen outside of this window.**
- Saved question to find our boxes: "[Get all SRA or ENG-VM owned computers](#)"
 - Get Computer Name and Online and Reboot Required from all machines with (Custom Tag Exists[eng-vulnerabilitymgmt-linux,1] contains true or Custom Tag Exists[eng-vulnerabilitymgmt-appspider,1] contains true)

Internal Resources

- [Tanium Console](#)
- [Tanium Saved Question: Get all SRA or ENG-VM owned computers](#)
- [ServiceNOW filter to find SRA / ENG-VulnerabilityMgmt computers](#)

External Resources

- [AppSpider](#)

- [Tenable](#)
- [ServerScan](#)
- [Tanium Docs - Custom Tags](#)
- [Tanium Docs - Computer groups](#)

Internal Resources

- [Tanium Console](#)
- [Tanium Saved Question: Get all SRA or ENG-VM owned computers](#)
- [ServiceNOW filter to find SRA / ENG-VulnerabilityMgmt computers](#)

External Resources

- [AppSpider](#)
- [Tenable](#)
- [ServerScan](#)
- [Tanium Docs - Custom Tags](#)
- [Tanium Docs - Computer groups](#)

old ServerScans Playbook - On-demand and On-build

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [Process-Specific Definitions](#)
- [Process Workflow](#)
 - [Build/Vuln Scan Handling Process](#)
 - [ServerScan Problem Ticket Handling Process](#)
- [Process Outline and Details](#)
 - [General Outline](#)
 - [Process Details](#)
 - [Vuln Scan Quick Filter Selection in Kanban](#)
 - [Legacy ServerScan Interface](#)
 - [ServerScan Manually Input Hostname & IP checkbox](#)
 - [ServerScan Hostname & IP Interface](#)

General Information

This playbook describes how to respond to JIRA stories generated from the Vulnerability Scan Request Form in Confluence requesting a Nessus scan, as well as how to action ServiceNOW Problem tickets generated by both on-build Server Scans and manually requested Server Scans entered into the legacy ServerScan application interface at <https://serverscan.int.godaddy.com>

| | |
|------------------------------|--|
| Responsible Team | Vulnerability Management: #vulnerability_mgmt, vulnerabilitymgmt@godaddy.com Tier 1. GSOC: #vm_tier1_priv (must have invite) |
| Process Owner | Vulnerability Management |
| Last Review Date | |
| Escalation Contact(s) | Vulnerability Management |
| Requests for Updates | JIRA tickets on the Vulnerability Management Kanban board and backlog with the label "collector-04e7a4af" ServiceNOW Problem tickets with a Root Cause field set to Security.Vulnerability Contact Vulnerability Management for process changes or help interpreting Nessus output results |

Process Summary

This process provides a methodology to handle user requests for on-build and vulnerability scans of systems, as well as how to handle the resulting output of such scans that are not automatically routed to the . The three use cases for these types of Nessus scans are as follows:

- On-build scans requested by SMDB or ServiceNOW server build automation
- Vulnerability scans requested by users via the Confluence based Vulnerability Scan Request form: </wiki/spaces/VM/pages/76585317>
- Vulnerability scans requested by users via the legacy <https://serverscan.int.godaddy.com> application

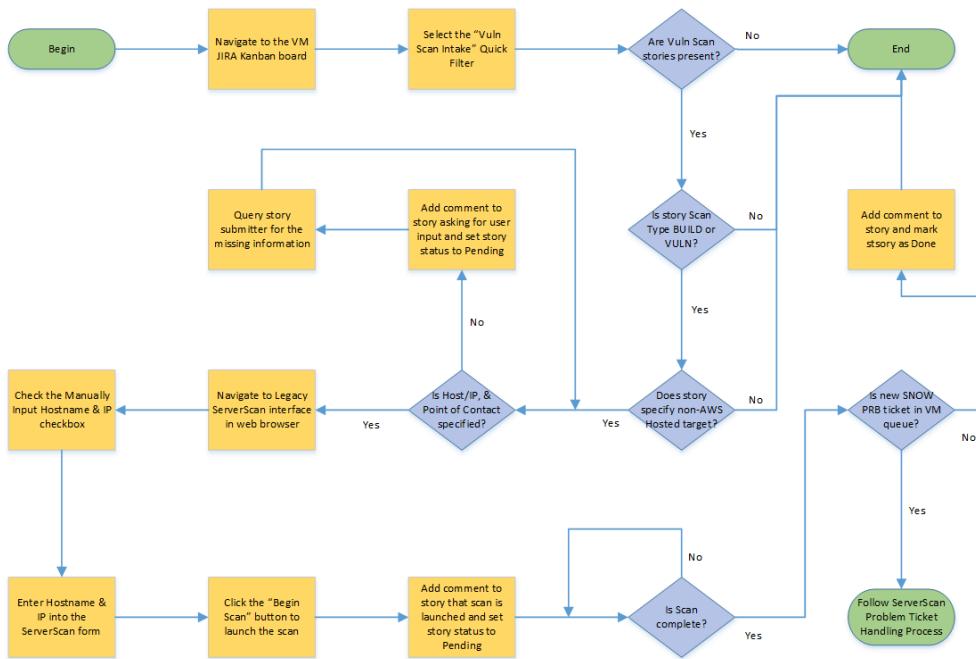
This process should be used for any JIRA tickets found on the Vulnerability Management Kanban board and backlog with the label "collector-04e7a4af" originating from the Vulnerability Scan Request Form, as well as any ServiceNOW Problem tickets with a Root Cause field set to Security.Vulnerability originating from the legacy ServerScan application. The result of following these processes is that ServiceNOW Problem tickets indicating actionable items will be assigned to the appropriate group so that detected vulnerabilities can be mitigated or resolved.

Process-Specific Definitions

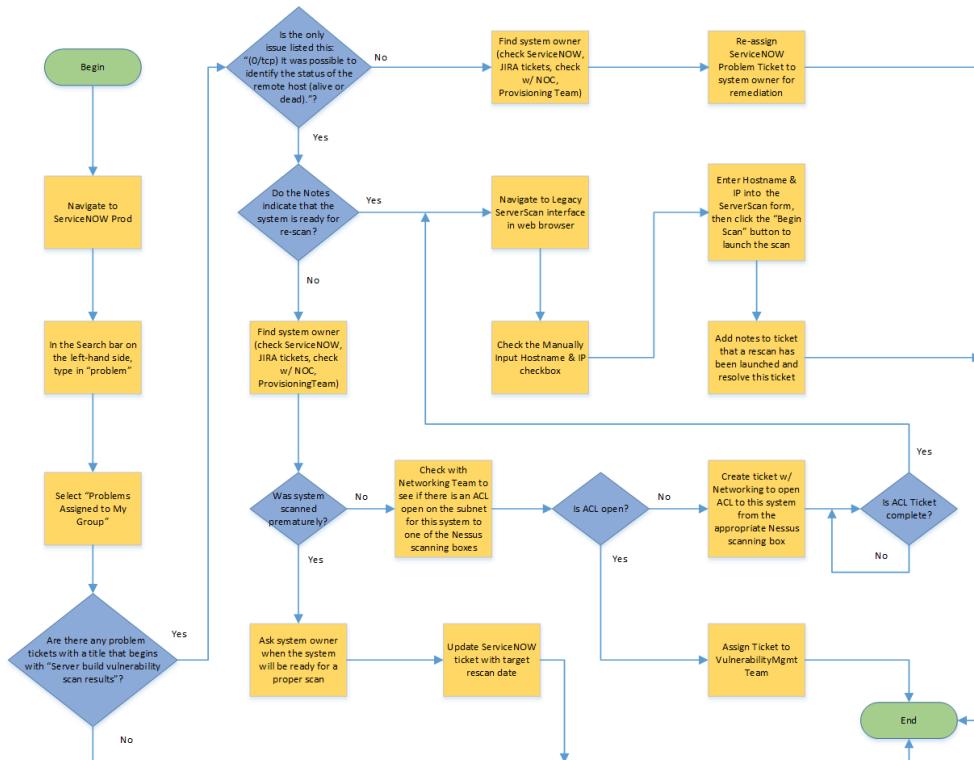
- **Nessus:** The vulnerability scanning software used by Vulnerability Management for Monthly Internal Audits. It attempts to detect known exploits and configuration related issues, and is updated with new exploit plugins on a daily basis.
- **ServerScan:** The legacy application at <https://serverscan.int.godaddy.com> that users can use to input either an SMDB ID or an IP Address/Hostname pair to kick off a Nessus scan of a system
- **Problem Ticket:** A ticket in ServiceNOW that begins with the prefix PRB
- **JIRA Ticket:** A ticket or story to be worked that appears in the Vulnerability Management Kanban board or backlog

Process Workflow

Build/Vuln Scan Handling Process



ServerScan Problem Ticket Handling Process



Process Outline and Details

General Outline

1. Navigate to the [Vulnerability Management Kanban Board in JIRA](#)
2. Select the "Vuln Scan Intake" Quick Filter
3. If Vuln Scan stories are found
 - a. If the Scan Type specified in the story is BUILD or VULN
 - i. If the story is for a system that is not AWS Hosted
 1. If the Hostname, IP address, or Point of Contact is **not** specified then
 - a. Add a comment to the story asking for user input
 - b. Set the JIRA story status to Pending
 - c. Query the story submitter for the missing information
 2. Navigate to the [Legacy ServerScan Interface](#)
 3. Check the "Manually Input Hostname & IP" checkbox
 4. Enter the Hostname and IP Address into the ServerScan Interface
 5. Click the "Begin Scan" button to launch the scan
 6. Add comment to the JIRA story that the scan has been launched
 7. Set the JIRA story status to Pending
 8. Re-check the ServerScan Interface periodically to see if the scan is done. The ServerScan Interface can be refreshed by clicking on the "Server Scans" link in the upper left corner of the form
 9. Navigate to the [ServiceNOW Problem Tickets Assigned to My Group](#) table
 10. If there is **not** a new ServiceNOW Problem Ticket in the Problem Table that was created by ServerScan then
 - a. Add a comment to the JIRA story that the scan is complete
 - b. Let the submitter know that the scan is complete and that they should have results in ServiceNOW if there were any findings
 - c. Mark the JIRA story done
 4. Navigate to the [ServiceNOW Problem Tickets Assigned to My Group](#) table
 5. If there are any open or pending Problem tickets generated by ServerScan in the list (the title begins with "Server build vulnerability scan results") then
 - a. If the only issue listed is the 0/tcp issue then
 - i. If the Notes in the ticket indicate that the system is ready for re-scan then
 1. Navigate to the [Legacy ServerScan Interface](#)
 2. Check the "Manually Input Hostname & IP" checkbox
 3. Enter the Hostname and IP Address into the ServerScan Interface
 4. Click the "Begin Scan" button to launch the scan
 5. Add a Note to the ticket that a rescan has been launched and resolve this ticket
 - ii. If the Notes in the ticket do not indicate that the system is ready for re-scan then
 1. Find the system owner (search ServiceNOW, JIRA Tickets, check with NOC, check with the Provisioning Team)
 2. If the system was scanned prematurely (i.e. before it was finished being setup) then
 - a. Ask the system owner when the system will be ready for a proper scan
 - b. Update the ServiceNOW ticket with the target rescan date
 3. If the system was not scanned prematurely then
 - a. Check with the Networking Team to see if there is an ACL open on the subnet for this system to one of the Nessus scanners
 - b. If an ACL is open then assign the ServiceNOW ticket to the Vulnerability Management Team for further investigation
 - c. If an ACL is not open, then create a ticket w/ Networking to open an ACL to this system from the appropriate Nessus scanner
 - i. After the ACL has been opened, go to step 5.a.i.1
 - b. If there are issues listed other than or in addition to the 0/tcp issue then
 - i. Find the system owner (search ServiceNOW, JIRA Tickets, check with NOC, check with the Provisioning Team)
 - ii. Re-assign the ServiceNOW Problem Ticket to the system owner for remediation

Process Details

Vuln Scan Quick Filter Selection in Kanban

The screenshot shows a Jira Kanban board titled "VM board - Agile Board - GoDaddy Jira - Google Chrome". On the left sidebar, under "PROJECT SHORTCUTS", there is a link to "Legacy ServerScan Interface". The main area displays a Kanban board with columns: "ENDING/BLOCKED 0", "MVR INTAKE 0", and "MVR IN PROGRESS 0 OF 5". At the top of the board, there are "QUICK FILTERS" buttons: "Vuln Scan Intake" (highlighted with a red arrow), "Not MVR", "MVR", "Only My Issues", and "Recently Updated". To the right of the board, a detailed view of a single issue is shown:

- Issue Summary:** New Vulnerability Scan - Kabbage Integration
- Assignee:** Unassigned
- Dates:**
 - Created: 10/02/2019 4:38 PM
 - Updated: 10/28/2019 1:34 PM
- Description:** Please fill out the following information to request a Vulnerability Scan.
- Targets:** (C's, URI's, Hosts, IP's) Anson Tsao?
- Environment:** PROD
- Point Of Contact:** Anson Tsao
- Team Contact:** #kabbage-int-launch
- Notes:** Planning pentest for 10/14 unless it's determined we don't need it

Legacy ServerScan Interface

The screenshot shows the "Server Scan - Google Chrome" interface. At the top, there is a "MANUALLY INPUT" section and a "SEARCH SCAN RESULTS" section. The "SEARCH SCAN RESULTS" section includes fields for "Hostname", "Result Limit" (set to 1000), "Last # Days" (set to 30), and "Order by" (set to "Dateline"). Below these are buttons for "Search" and "Check entries". The main area is a table titled "SERVER SCANS" with columns: Date, Status, Host Name, Host IP, Review, and Scanner. The table lists numerous scan entries, such as:

| Date | Status | Host Name | Host IP | Review | Scanner |
|---------------------|----------|----------------------------|-----------------|--------|---------|
| 2019-11-06 21:46:09 | Complete | AUS3PLESX01N03 | 10.99.33.195 | Nessus | |
| 2019-11-06 21:46:10 | Complete | AUS3PLESX01N02 | 10.99.33.194 | Nessus | |
| 2019-11-06 21:46:31 | Complete | AUS3PLESX01N01 | 10.99.33.193 | Nessus | |
| 2019-11-06 20:29:32 | Complete | P3PLPCDATA0568 | 10.38.129.148 | Nessus | |
| 2019-11-02 00:46:29 | Complete | P3PLPCBCLDHV017-21 | 10.205.76.151 | Nessus | |
| 2019-11-01 23:31:58 | Complete | P3NWLPHLOG09 | 45.40.164.159 | Nessus | |
| 2019-11-01 22:30:47 | Complete | A2PLMMWVWORKER15 | 10.36.72.77 | Nessus | |
| 2019-11-01 20:04:45 | Complete | P3PLPCDATA01 | 10.22.240.19 | Nessus | |
| 2019-11-01 18:13:40 | Complete | salt-master.cloud.phc3.gdg | 10.33.104.126 | Nessus | |
| 2019-11-01 02:06:04 | Complete | P3PLPCDATA01 | 10.22.240.19 | Nessus | |
| 2019-10-31 23:00:03 | Complete | P3PLPCDATA01 | 10.22.240.19 | Nessus | |
| 2019-10-31 21:29:42 | Complete | P3PLPCDATA04 | 10.22.240.26 | Nessus | |
| 2019-10-31 21:29:42 | Complete | P3PLPCDATA03 | 10.22.240.21 | Nessus | |
| 2019-10-31 21:46:46 | Complete | P3PLPCDATA02 | 10.22.240.20 | Nessus | |
| 2019-10-31 20:15:04 | Complete | salt-master.cloud.phc3.gdg | 10.33.104.126 | Nessus | |
| 2019-10-31 07:30:46 | Complete | SXB1P1CPN10007 | 92.204.65.5 | Nessus | |
| 2019-10-30 19:17:55 | Complete | SGB1P1UBCLDNV015-22 | 10.205.62.22 | Nessus | |
| 2019-10-30 19:17:55 | Complete | SGB1P1UBCLDNV015-14 | 10.205.62.14 | Nessus | |
| 2019-10-30 19:17:19 | Complete | SGB1P1UBCLDNV015-11 | 10.205.62.11 | Nessus | |
| 2019-10-30 17:29:38 | Complete | salt-master.cloud.phc3.gdg | 10.33.104.129 | Nessus | |
| 2019-10-30 16:13:41 | Complete | salt-master.cloud.phc3.gdg | 10.33.104.129 | Nessus | |
| 2019-10-30 08:30:27 | Complete | P3PLPCDATA03 | 10.22.240.20 | Nessus | |
| 2019-10-30 09:27:20 | Complete | SGB1P1UBCLDNV015-10 | 10.205.64.19 | Nessus | |
| 2019-10-30 09:27:19 | Complete | SXB1P1CPN10049 | 92.204.65.136 | Nessus | |
| 2019-10-30 09:27:19 | Complete | SXB1P1CPN10033 | 92.204.65.32 | Nessus | |
| 2019-10-30 16:30:42 | Complete | salt-master.cloud.phc3.gdg | 10.33.104.126 | Nessus | |
| 2019-10-29 13:50:19 | Complete | P3PLSEARCHH009 | 10.39.197.130 | Nessus | |
| 2019-10-28 22:14:39 | Complete | P3NWSHICWVS007 | 173.201.136.137 | Nessus | |
| 2019-10-25 21:57:56 | Complete | salt-master.cloud.phc3.gdg | 10.33.104.126 | Nessus | |
| 2019-10-25 21:40:29 | Complete | salt-master.cloud.phc3.gdg | 10.33.104.126 | Nessus | |
| 2019-10-25 01:07:45 | Complete | SXB1P1CPN10065 | 92.204.65.154 | Nessus | |
| 2019-10-25 00:57:41 | Complete | SXB1P1CPN10056 | 92.204.65.149 | Nessus | |

ServerScan Manually Input Hostname & IP checkbox

The screenshot shows the 'SEARCH SCAN RESULTS' section of the Server Scan interface. At the top right, there is a checkbox labeled 'MANUALLY INPUT HOSTNAME & IP'. Below it, there are search fields for 'Hostname' and 'IP Address', and dropdowns for 'Result Limit' (set to 1000), 'Last # Days' (set to 30), and 'Order by' (set to 'Date/time'). A 'Search' button is also present. The main area displays a table of scan results with columns for Date, Status, Host Name, Host IP, Review, and Scanner. The table shows numerous completed scans from November 2019, with Nessus as the scanner. A red arrow points to the 'MANUALLY INPUT HOSTNAME & IP' checkbox.

ServerScan Hostname & IP Interface

This screenshot shows the same 'SEARCH SCAN RESULTS' section as the previous one, but with a different configuration. The 'MANUALLY INPUT HOSTNAME & IP' checkbox is now unchecked. Instead, the 'IP Address' input field is populated with '10.99.33.196'. The rest of the interface elements, including the search fields, result limit, and order by dropdown, are identical to the first screenshot. The table of scan results is also the same, showing completed scans from November 2019 with Nessus as the scanner. A red arrow points to the 'IP Address' input field.

old Suspicious User Behavior - Monitoring and Response

Table of Contents

- 1. General Information
- 2. Dashboard Review
- 3. FAQ
- 4. Internal Resources/ useful links

General Information

| | |
|---------------------|--|
| Responsible Team | <ul style="list-style-type: none">• GCSOEmail : gcso@godaddy.comSlack : #gcs0, @gcs0 |
| Escalation Contacts | <ul style="list-style-type: none">• Infosec_ResponseSlack : @ir-team,On-call |

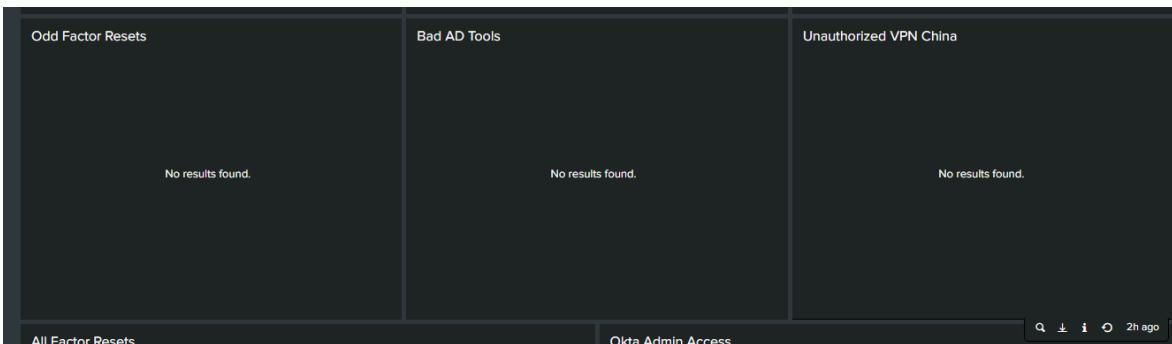
Process Summary

The 'IRT - Temp Daily' [dashboard](#) to be monitored once in 4 every hours
Immediately callout IR Team on-call member if any events displayed on

- > Odd Factor Resets
- > BAD AD Tools
- > Unauthorized China VPN

2a. Dashboard Review

Dashboard : [IRT - Temp Daily](#)



Odd Factor Reset :

Displays users with more than 2 MFA resets within Okta. These are the events of resets, not done by the user himself/herself.

This panel is monitoring for users with excessive MFA Factor Resets within Okta. Because this is a key indicator from our persistent social engineering actor any new values present in this panel require an immediate call-out.

1. If 'No results found', then no actions required.
2. If any results found, then
 - a. Immediately callout IR Team [on-call](#) member.
 - b. Create a Security incident and a private Slack channel if any further actions required.
 - c. For confirmed compromise, remediate user account by following the [Employee Compromise Containment](#) process.

BAD AD Tools :

Displays login attempts on user account using known malicious AD tools

This panel is monitoring for instances of known-bad AD tools being used within our environment. Because this is a key indicator from our persistent social engineering actor any new values present in this panel require an immediate call-out.

1. If 'No results found', then no actions required.
2. If any results found, then
 - a. Immediately callout IR Team [on-call](#) member.
 - b. Create a Security incident and a private Slack channel if any further actions required.
 - c. For confirmed compromise, remediate user account by following the [Employee Compromise Containment](#) process.

Unauthorized China VPN :

This panel is monitoring for users VPN logons from users in the China region. We do not expect to see ANY logons from this group at this time.

1. If 'No results found', then no actions required.
2. If any results found, then
 - a. Remediate the identified user account by following the [Employee Compromise Containment](#) process.
 - b. Notify the IR team per [on-call](#) process.
 - c. Begin review of user's Okta app access.

All Factor Reset

All Factor Resets :
Displays events of MFA resets done other then the user.

1. If no events, no actions required
2. If any events, then determine if it is a legitimate activity.
3. If yes → no further actions required
4. If no → follow [Employee Compromise Containment](#)

2b. Dashboard

| All Factor Resets | Okta Admin Access |
|--------------------------|-------------------|
| No results found. | No results found. |
| Okta Profile Activations | |
| No results found. | |

Okta Profile activations : Displays the events of MFA activations, generally for new hires.

It is legitimate if is done by system@okta.com
> 'Display message' field displays 'Activate Okta user'

The events can be reviewed further in [Okta Logins IRT](#) and [Okta Logs GCSO](#) in case of doubt.

If still unsure about the event, escalate to T2 via #internal_gcsco

Okta Admin Access

Okta Admin Access :
Access events of Okta Admin App

This tab displays the user's :
1. Email Id
2. Title
3. Department

What determines the legitimacy of the event : Title and Department

Example of a Legitimate Event :
Title: Eng - System II
Department : Cloud Infrastructure and IT

Example of a suspicious event :
Title : Sup - Care
Department : C3 Support

Okta Factor Activations

Okta Factor Activations : Displays the events of MFA set up events

Events from 'IRT - Temp Daily' Dashboard:

| Okta Factor Activations | | | | |
|-------------------------|-------------------------|--------------------------|----------------|------------------------|
| _time | actor.alternateId | eventType | outcome.result | outcome.reason |
| 2021-04-11 00:46:31.345 | dhoff@godaddy.com | user.mfa.factor.activate | SUCCESS | User set up Yubikey |
| 2021-04-10 22:20:58.563 | rubi8390@godaddy.com | user.mfa.factor.activate | SUCCESS | User set up Soft Token |
| 2021-04-10 21:13:19.431 | japheth2006@godaddy.com | user.mfa.factor.activate | SUCCESS | User set up Soft Token |
| 2021-04-10 20:18:39.109 | jasmeet9942@godaddy.com | user.mfa.factor.activate | SUCCESS | User set up Yubikey |

Review

1. User's okta logs in [Okta Logins IRT](#) or [Okta Logs GCSO](#)
2. Check users login IP and location.
 - a. If it is not a GoDaddy IP, review the IP in [IP Void](#) for details.
 - b. If the IP is malicious or user having a login events from a different location than expected, escalate to Tier 2 .
Example of an anomalous activity: A user from Germany having logon events from Australia.
3. For confirmed compromises, follow [Employee Compromise Containment](#) process.

More information :

Search Query for 'Okta Factor Activations', if to be reviewed in Splunk apart from the 'IRT - Temp Daily' dashboard or to edit/ modify search :
index="oktalogs" eventType="user.mfa.factor.activate" | dedup _time, eventType | table _time, actor.alternateId, eventType, outcome.result, outcome.reason

> outcome.reason shows the details of type of MFA

- Eg. a. User set up YUBIKEY OTP_FACTOR factor
b. User set up SOFT_TOKEN factor
c. User set up FIDO_WEAUTHN factor

For any user account remediation, follow [Employee Compromise Containment](#) process.

1. Send [Account Locked \(Credentials Only\)](#) communication template

› Communication Template

To: Affected User

CC: Supervisor (**Do NOT CC Director level or above**); Workforce (**Care Agents ONLY**); GCSO; ssit@godaddy.com; engwin@godaddy.com

Subject: Your User Account Has Been Locked : Action Required

The Security team was recently made aware of a <Incident_Type> in which we believe your account credentials may have been compromised. Because you were unavailable at the time of this discovery, we have taken action as a precaution to protect your account from misuse.

You will need to reset your password in order to regain access to your account. This will require you to contact [GetHelp](#) (480-624-2580) for assistance. Please ensure that the following best-practices are also observed for your account:

- Reset any credentials not synchronized to your GoDaddy login - example include SaaS applications, local accounts, etc.
- Ensure that passwords are not reused across any services, accounts, etc.
- Passwords on all company-controlled platforms must conform to GoDaddy password standards.

We will also be ensuring you are enrolled into Okta Multi-Factor Authentication (MFA) as an added layer of protection. If you were not already enrolled in MFA you will be prompted to complete setup when you next sign-on to Okta.

2. Notify #get-itsec via Slack by providing the user id and to follow re-enabling process

3. For this process, GCSO also need to monitor enabling process.

4. Steps to re-enable remediated user

› [Re-enabling process](#)

If remediated users reaches out to GetHelp to be re-enabled, please follow this process to ensure their identity.

1. GetHelp must identify their manager and validate the manager's identity.

a. Do NOT let user initiate with manager.

2. GetHelp initiate a zoom call with their manager.

3. Invite a member of the GCSO team to the zoom (slack #gcsoteam.)

4. Invite user to zoom call.

5. All users must have their cameras on.

6. Manager should identify user.

7. Unless user location is Germany, user must show some sort of picture ID to verify themselves.

8. Match name/picture.

9. GetHelp can then re-enable user.

10. GetHelp should verify and review user's active MFA tokens with the user to ensure they are correct.

a. Disable any additional tokens for user.

If the user cannot comply with the above process, please let them know that they cannot be re-enabled at this time.

Also, please reach out to GCSO (slack #gcsoteam) and alert them if this occurs, or if the user does not comply.

3. FAQ

1. What is the difference between Odd Factor Reset and All Factor Reset

Odd factor is 3 or more resets for a user account

All factor reset includes all the factor reset events on the user account

2. Known Bad AD Tools for this dashboard

- a. passwordcontrol.exe
- b. Hyena_x64
- c. stuc.exe

3. How to determine if the event is legitimate

Legitimate reset : Done by user or concerned team (for example, Get Help)

Non legitimate/ suspicious event : Non authorized user resetting other users' MFA

Example: Aftermarket Sales user resetting other users' MFA

4. What happens when a user account is remediated

- a. Remediation basically auto resets user's password and clears the active okta, O365 and slack sessions

- b. If the remediated user is with in 3 levels from CEO, it requires approval

4. Internal Resources/ Useful Links

Credential Mitigation : <https://godaddy-corp.atlassian.net/wiki/display/IRKB/Credential+Mitigation>

Employee Compromise Containment : <https://godaddy-corp.atlassian.net/wiki/display/IRKB/Employee+Compromise+Containment>

Okta Logs : [Okta Logins IRT and Okta Logs GCSO](#)

IRT- Temp Daily Dashboard : https://godaddy.splunkcloud.com/en-US/app/search/irt_temp_daily?form.timeSelector.earliest=-4h%40h&form.timeSelector.latest=now

old Vendor Advisory Handling Playbook

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [Process-Specific Definitions](#)
- [Process Workflow](#)
 - [Process Flow](#)
 - [Technology Flow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [Process-Specific Priority Matrix](#)
 - [General Outline](#)
 - [Process Details](#)
 - [Captured Metrics](#)
 - [Process FAQs](#)
 - [How can I determine if a VA applies to us?](#)
 - [What happens if the VA doesn't apply to us?](#)
 - [How do I calculate the CVSS score?](#)
 - [What do the various ticket states mean?](#)
 - [What do I put in the Worklog?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)
 - [Communication Templates](#)
 - [VA does not apply to us](#)
 - [VA severity is less than 7.0](#)
 - [Finding responsible teams](#)
 - [Communicate remediation to teams](#)
 - [Other communications](#)
- [Associated Audit Controls / Requirements](#)

General Information

This describes the process for handling vendor advisories (VAs) that come in via the automation created/maintained by [@Former user \(Deleted\)](#).

| | |
|-----------------------|--|
| Responsible Team | GCSO |
| Process Owner | @David Dubois (Deactivated) |
| Last Review Date | 2019-10-01 by @Former user (Deleted) |
| Escalation Contact(s) | ENG-VulnerabilityMgmt vulnerabilitymgmt@godaddy.com #vulnerability_mgmt in Slack |
| Requests for Updates | @David Dubois (Deactivated) |

Process Summary

This process provides direction for the detection, analysis and remediation of incoming Vendor Advisories and outlines the general process guidelines to be followed by Incident Response analysts. A summary of applicable use cases for this process are as follows:

- A new VA is identified by automation and ticketed in SNOW which must be investigated and handled
- New VAs are retrieved and ticketed daily, and should be inspected at least weekly
- Expected outcome is that VA tickets are handled weekly with false positives being noted & closed, and real positives being driven toward remediation with the responsible team(s)

Process-Specific Definitions

- **VA:** Vendor Advisory
- **Vendor Advisory Tickets:** https://godaddy.service-now.com/u_physical_security_list.do?sysparm_view=&sysparm_first_row=1&sysparm_query=u_assignment_groupDYNAMICd6435e965f510100a9ad2572f2b47744%5Eu_stateNOT%20INclosed%5Eu_titl

Process Workflow

Process Flow

Technology Flow

Process Outline and Details

Incident Recording Guide

| Security Incidents (SEC on the u_physical_security table) | |
|---|--|
| The below rows refer to fields in the SEC VA tickets | |
| Worklog | Enter validation, communications log, and resolution |
| Assignee | Assign this to whomever performed the analysis on the ticket |
| Incident Category | Risk |
| Sub-Category | other |
| Detection Method | External Report |
| Title | Always starts with "[VENDOR ADVISORY]" |
| DSR | Checked |
| Contained Summary | Resolution notes |
| Contain Time | The date/time when the ticket is closed |

Process-Specific Priority Matrix

N/A - The priority of VA evaluation is to do it at a minimum frequency of weekly, and each ticket's criticality depends on its evaluated CVSS (base CVSS & GD CVSS)

General Outline

1. Navigate to the vendor advisory table ([u_physical_security](#))
2. Find the VA tickets (filter on → Title starts with "[Vendor Advisory]" **and** State is not Closed)
3. Evaluate each ticket's applicability and severity
 - a. If it does not apply to our environment then close the ticket noting that in the Contained Summary
 - i. For example, if it is an RPM package that we don't support and isn't in our repos
 - b. If the GD CVSS score is less than 7 (that is, Medium or lower) then close the ticket noting the CVSS in the Contained Summary
 - i. The base CVSS score is usually in the RHEL vendor advisory, which you can typically find by searching for the RHEL VA ID, found in the ticket title
 - ii. [Here](#) is supporting documentation on how to adjust for the GD score.
 - iii. You may contact Vulnerability Management for help with determining the GoDaddy CVSS score if necessary
4. Determine responsible team(s) (GSOC or NOC should be able to assist here) and add them to the "Allowed Groups" field so they can see the ticket
5. At this point, the VA has been determined to be a High or Critical, so start the MVR process. **TODO: Add link to MVR Playbook**
6. Once vulnerability is remediated, note resolution in the Contained Summary and set the Contained Time to the current date/time
7. Close the ticket
8. Done!

Process Details

Entire process is described in the general outline, above.

Captured Metrics

Note that dashboards are not yet created.

- **Number of open tickets** - Can be a dashboard report, provides info on current state of VA list
- **Closed VAs over time** - Can be a dashboard report, provides info on closure velocity
- Maybe others? Unknown at this time, feedback should be solicited from leadership to find out what other metrics are desired

Process FAQs

How can I determine if a VA applies to us?

- If a Linux VA, then look in our [CentOS repo](#) for the package. If it is not present, then it is not supported. (Must be on VPN to access repos)
 - Make sure to check with EMEA as well because they have different repos (#emea_vst)
- If a Windows (or windows application) VA, then inquire with Desktop (Adam Brown or Michael Goodman)
- Check with Al Fama in Hosting
- Check in #emea_vst to see if it affects EMEA (you may need an invite to the channel - request from Flemming Riis)

What happens if the VA doesn't apply to us?

- Close the ticket after noting that in the Contained Summary field

How do I calculate the CVSS score?

- First find the base CVSS score (typically in the RHEL advisory, which is where the vast majority of the VAs come from)
- Use the [NIST CVSS Calculator](#) to determine CVSS. Replicate the base CVSS factors, then [adjust for GD](#)

What do the various ticket states mean?

- Open: Initial ticket state, not yet evaluated
- In Progress: Currently being evaluated
- Pending Internal: Waiting on remediating team(s)
- Pending External: Waiting for remediation availability (eg. patch release)
- Closed: Final state of ticket

What do I put in the Worklog?

- Investigation/analysis conclusions (CVSS scoring, applicability, etc)
- Remediation plans and estimated completion dates (obtain from remediating team)
- Notes if VA does not apply or does not meet the severity threshold (severity >= 7.0)
- Notes on VA applicability to our environment, including compliance area (PKI, PCI, etc) and business area (Hosting, OpenStack, EMEA, etc)
- Any other interesting or useful information

Resources and Definitions

- Vulnerability Management or Threat Intelligence
 - Can escalate if help is required to evaluate tickets
- #noc or GSOC can help determine responsible groups
- [Vendor Advisory Table](#)
 - Must filter this (Title starts with "[Vendor Advisory]" **and** State is not Closed)
 - May need to request access to this table - you will only get access to your or your team's tickets, so make sure they are assigned appropriately
- [NIST CVSS calculator](#)
- [CVSS Determination Guide](#)
- [Vendor Advisory automation script](#)

Internal Resources

See "Resources and Definitions" section, above.

External Resources

See "Resources and Definitions" section, above.

Communication Templates

| Communication Name |
|---|
| VA does not apply to us In the Contained Summary: "The packages listed in this advisory do not apply to our environments." |
| VA severity is less than 7.0 In the Contained Summary: "This has a CVSS score of <insert GD CVSS score here> and does not meet our severity thresholds." |
| Finding responsible teams Check in the #noc channel in Slack: "Hello! We are trying to determine the owning team for <insert affected nodes/tech/systems/environment here>. Can you assist or point us to someone who can? Thank you!" |
| Communicate remediation to teams "Hello. We have received a vendor advisory that may affect your systems. The affected package(s) is/are <insert package name(s) here>, and the updated package(s) is/are <insert updated package name(s) here>. You can find more information here: <insert link to ticket - note that their group must be in the "Allowed Groups" field>. Please investigate and remediate by <insert SLA breach time here>. Thank you, and please reach out to us for guidance at <insert your contact details here>." |
| Other communications Feel free to reach out to the VM team if you are unsure of other communications. |

Associated Audit Controls / Requirements

N/A

old Employee Phishing Incidents

Table of Contents

- Table of Contents
- General Information
 - Process Summary
 - Process-Specific Definitions
- Process Workflow
- Process Outline and Details
 - Incident Recording Guide as per SIR Module
 - General Outline
 - Reviewing Malicious URLs
 - Reviewing Business Email Compromise (BEC) Attempts
 - Process Details
 - Finding a Domain's Registrar and Host
 - Reviewing for URL Visits
 - Process FAQs
 - What if a C3 Rep Reports a Phish Targeting a Customer?
 - What is a Business Email Compromise (BEC) attempt?
- Resources and Definitions
 - Internal Resources
 - External Resources
 - Communication Templates

General Information

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Employee Cyber Security Incident Response• SLACK: #employee_security #internal-gcso• EMAIL: EmployeeSecurity@GoDaddy.com Infosec_Response@GoDaddy.com |
| Process Owner | @David Dubois (Deactivated) |
| Last Review Date | 2020-04-28 by @Former user (Deleted)downs |
| Escalation Contact(s) | <ul style="list-style-type: none">• @Juan Bustamante• @Former user (Deleted)crisostomo• @David Downs |
| Requests for Updates | By Email - EmployeeSecurity@GoDaddy.com Infosec_Response@GoDaddy.com |

Process Summary

This process provides direction for the analysis and remediation of user reported employee-targeted phishing attempts and outlines the general process guidelines to be followed by Incident Response analysts. A summary of applicable use cases for this process are as follows:

- Phishing reports generated by user-initiated emails to IsItBad@GoDaddy.com

Process-Specific Definitions

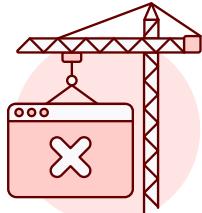
- **Impersonated Individual/Group:** Impersonated Individual or Group refers to who the phishing email is pretending to be. This can be a company, an organization, or a single user.
- **Targeted Group (if specific):** Targeted group is an optional field that refers to the GoDaddy group that received the emails, often grouped by department.
- **Type of Attack:** Type of Attack refers to what classification the malicious email falls under, as not all malicious and actionable emails that get reported to IsItBad@GoDaddy.com are strictly phishing emails—some may contain a malicious script or be impersonating an SLT/XLT member.

Process Workflow



Oops, Diagram Unavailable

This diagram cannot be displayed. It may have been moved, deleted, or you do not have permission to view it.



Oops, Error 500!

Diagram Unavailable

Our system is currently under maintenance. Reach out to your administrator for a fix.

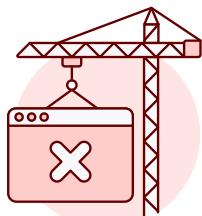


You have an unpublished draft.



Oops, Diagram Unavailable

This diagram cannot be displayed. It may have been moved, deleted, or you do not have permission to view it.



Oops, Error 500!

Diagram Unavailable

Our system is currently under maintenance. Reach out to your administrator for a fix.



You have an unpublished draft.

Process Outline and Details

Incident Recording Guide as per SIR Module

| Employee-Targeted Phishing | |
|----------------------------|--|
| Assignment Group | OPS-GCSO |
| Source | Email |
| Category | Phishing(Auto filled) |
| Title | User Reported Phishing : <i>Here comes the subject of the reported email</i> |
| State | Analysis |
| Business Impact | 3 - Non - critical(Auto filled) |
| Severity | 2 - Medium(Auto filled) |
| Priority | Low |
| Alert Sensor | User Reported Phish |

General Outline

1. Report is received:
 - a. Via IsItBad@GoDaddy.com, ticket is generated by automation, and the reporter is automatically thanked.
 - b. Via other means and ticket is created using the Incident Recording Guide
2. Review Message Headers and Body to determine if malicious
 - a. Analyze Return Path, Sender IP, Spam Confidence Level(SCL), SPF to determine if its a Spoofed email or not.
 - b. Review the email body, follow the below steps about reviewing malicious url's and attachments.
 - c. If NOT, respond to reporter using [Response to Reporter - Not Malicious](#) and close as False Positive.
3. For malicious messages:
 - a. If the message targets GoDaddy-brand (i.e. impersonates GoDaddy) and/or targets GoDaddy customers (not employees):
 - i. Report the Malicious URL to the [Front of Site form](#)
 - ii. Respond to the user with the template [GoDaddy Customer Phish](#)
 - b. If the message has been generated from an **internal sender** (GoDaddy.com, MediaTemple.net, Heg.com, etc.) → [Escalate to InfoSec Response Team](#)
4. Perform a [Message Trace](#) to determine the number of emails seen in the environment.
5. Review the [Content Search](#).
 - i. If required, update Content Search to match properties to capture the malicious messages.
 - b. Reported via other means - Create a new Content Search using the ticket # as the name and matching properties to capture the malicious messages.
6. If necessary, download a sample of the message and attach to the ticket.
7. Using the SIR module Search & Delete option initiate Purge request for the Content Search.
8. Determine next actions based on the type of malicious content in the message.

Reviewing Malicious URLs

1. Trace path URL takes to final landing page via appropriate methods and record findings in the Ticket.
 - a. Use external sites like [URL Scan](#), Virus Total and other Security sites to review the URL.
 - b. Using CURL via Virtual Machine or Sandbox.
 - c. From a browser in a Virtual Machine or Sandbox like browserling.com.
 - i. Check and verify url's under Network options in Browser Developer mode.
2. Capture a screenshot of the landing page and attach to the ticket.
3. Report to phishing URL to external sites:
 - a. [Netcraft Toolbar](#)
 - b. [Google Safe Browsing \(Firefox, Chrome & Safari\)](#)
 - c. [Anti-Phishing Work Group \(APWG\)](#)
 - d. [Trend Site Safety Center \(WRS\)](#)
4. Determine where the landing page and any intermediate URL(s) are hosted:
 - a. If Hosted at GoDaddy; Report to the [Front of Site Abuse Form](#).
 - b. If Hosted elsewhere:
 - i. Use Security@godaddy.com mailbox to report malicious URL's to respective abuse teams.
 - ii. Domain Host & Registrar ([See Process Details](#))
5. Determine if any visits occurred ([See Process Details](#)).
 - a. If unblocked visits exist, remediate by following the [Employee Compromise Containment](#) process for each user.
6. Once any necessary containment is completed, close the Ticket.

Reviewing Malicious Attachments

1. Review file to collect potential Indicators of Compromise.
 - a. Submit the file to our internal [ThreatAPI](#) platform. Use resultant hash with "threatbot test" slack app. Message the bot with "getreport <hash>" and the report will display when it has finished running.
 - b. Alternatively we also submit the file in [Cuckoo](#) for analysis.
 - c. Using [VirusTotal](#), [Reverse.it](#), or other virus-analysis site to look up a particular file by Hash. (NOTE: Do not submit files to these sites)
2. Determine if the url contains any redirects.
 - a. If YES, follow the process to handle **Malicious URLs** above.

3. Review using Tanium to determine if the file has been downloaded to any machines
 - a. If YES, determine if the activity was blocked in Real-Time by Antivirus.
4. Is there evidence of unblocked downloads of the file?
 - a. If YES, follow [System Investigation](#) process.
 - b. Include your IOCs in the ticket for use by the next analyst.
5. If there is no evidence of download, or once any necessary containment is completed, close the Ticket.

Reviewing Business Email Compromise (BEC) Attempts

1. Perform a Message Trace both To and From and Reply-To addresses of the message.
2. Determine if any replies have been sent to the Sender:
 - a. If any replies have been seen, take action based on the email content and check with InfoSec Response Team if required
 - b. if NOT, document and close the Ticket

Process Details

Finding a Domain's Registrar and Host

Domain Host & Registrar requires some external checks to find. In general, three steps are needed:

1. WHOIS Lookup on the Domain.
2. A Record DNS Dig on the Domain.
3. WHOIS Lookup on the A Record IP.

There are several tools available to do these lookups, including command line utilities. Here are a few preferred methods:

- Via Command Line using *whois* and *dig* commands.
 - › [Commandline Examples](#)

Domain Whois Example

```
LMIT-DAVIDD:~ ddubois$ whois davedubois.com | grep -Ei 'Registrar|Abuse'
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
registrar's sponsorship of the domain name registration in the registry is
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
Registrars.
```

Domain Dig Example

```
LMIT-DAVIDD:~ ddubois$ dig davedubois.com A | grep -A1 'ANSWER SECTION'
;; ANSWER SECTION:
davedubois.com.    497 IN  A   184.168.221.63
```

IP Whois Example

```
LMIT-DAVIDD:~ ddubois$ whois 184.168.221.63 | grep -Ei 'Organization|Abuse'
Organization: GoDaddy.com, LLC (GODAD)
Comment: Please send abuse complaints to abuse@godaddy.com
Comment: Please send abuse complaints to abuse@godaddy.com
OrgAbuseHandle: ABUSE51-ARIN
OrgAbuseName: Abuse Department
OrgAbusePhone: +1-480-624-2505
OrgAbuseEmail: abuse@godaddy.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE51-ARIN
RAbuseHandle: ABUSE51-ARIN
RAbuseName: Abuse Department
RAbusePhone: +1-480-624-2505
RAbuseEmail: abuse@godaddy.com
RAbuseRef: https://rdap.arin.net/registry/entity/ABUSE51-ARIN
```

- Using external lookups. Some of the preferred sites are:
 - GeekTools [WHOIS](#) and [Dig Tools](#).
 - › [GeekTools Examples](#)

The screenshot shows the Geektools Whois Proxy interface. At the top, there's a promotional banner for Squarespace. Below it, a cartoon character with a magnifying glass is holding a sign that says "Geektools Whois Proxy". The main area displays the WHOIS information for the domain davedubois.com.

```

Whois: davedubois.com Whois >>
Checking server [whois.crsnic.net]
Checking server [whois.godaddy.com]
Results:
Domain Name: DAVEDUBOIS.COM
Registry Domain ID: 1520400829_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2018-01-26T16:54:20Z
Creation Date: 2008-09-20T06:59:38Z
Registrar Registration Expiration Date: 2019-02-01T11:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505

```


The next part of the screenshot shows the results of a DIG command. It includes the query, answer section (IP 184.168.221.53), and some metadata like the query time and server details.

```

; <>> DiG 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.1 <>> 64.2.2.1 davedubois.com A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 19067
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;davedubois.com. IN A
;; ANSWER SECTION:
davedubois.com. 600 IN A 184.168.221.53
;; Query time: 21 msec
;; SERVER: 4.2.2.1#53(4.2.2.1)
;; WHEN: Tue Oct 16 18:37:44 2018
;; MSG SIZE rcvd: 48

Your host (64.202.160.88) has visited 4 times today.

dig again

```

Copyright Centergate® Research Group, LLC 1998 - 2017

The final part of the screenshot shows the ARIN WHOIS results for the IP address 184.168.221.53. It includes the NetRange, CIDR, and various network parameters.

```

Whois: 184.168.221.53 Whois >>
Final results obtained from whois.arin.net.
Results:
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/whois_reporting/index.html
#
# Copyright 1997-2018, American Registry for Internet Numbers, Ltd.
#
NetRange: 184.168.0.0 - 184.168.255.255
CIDR: 184.168.0.0/16
NetName: ARIN-AS12-COM-LC
NetHandle: NET-184-168-0-0-1
Parent: NET184 (NET-184-0-0-0-0)
NetType: Direct Allocation
OrgName: ARIN
Organization: GoDaddy.com, LLC (GODAD)
RegDate: 2010-09-21
Updated: 2014-02-23
Comment: Please send abuse complaints to abuse@godaddy.com
Ref: https://dap.arin.net/registry/ip/184.168.0.0

```

- MxToolbox WHOIS, DNS Lookup (Dig) and ARIN Lookup (IP WHOIS)
 - › [MxToolbox Examples](#)

The image contains three separate screenshots of the MX Toolbox interface, each showing a different type of lookup for the domain davedubois.com.

- Whois Lookup:** Shows the Whois details for davedubois.com. Key information includes:

| Name | Value |
|-------------|------------------------|
| Registrar | GoDaddy.com, LLC |
| Name Server | NS29.DOMAINCONTROL.COM |
| Name Server | NS30.DOMAINCONTROL.COM |

 and

| Name | Value |
|-------------------------------|----------------------------|
| Domain Name | DAVEDUBOIS.COM |
| Registry Domain ID | 1520400829_DOMAIN_COM-VRSN |
| Registrar WHOIS Server | whois.godaddy.com |
| Registrar URL | http://www.godaddy.com |
| Updated Date | 2018-01-26T16:54:21Z |
| Creation Date | 2008-09-20T06:59:38Z |
| Registry Expiry Date | 2019-02-01T11:59:59Z |
| Registrar | GoDaddy.com, LLC |
| Registrar IANA ID | 146 |
| Registrar Abuse Contact Email | abuse@godaddy.com |
| Registrar Abuse Contact Phone | 480-624-2505 |
- DNS Lookup:** Shows the DNS record for the A record of davedubois.com, which points to the IP address 50.63.202.36.
- ARIN Lookup:** Shows the ARIN WHOIS record for the IP address 50.63.202.36. The record details include:

| Type | Domain Name | IP Address |
|------|----------------|--|
| A | davedubois.com | 50.63.202.36 GoDaddy.com, LLC (AS26496) |

 and the full ARIN WHOIS text:


```
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/whois_reporting/index.html
#
# Copyright 1997-2018, American Registry for Internet Numbers, Ltd.
#
NetRange: 50.62.0.0 - 50.63.255.255
CIDR: 50.62.0.0/15
NetName: GO-DADDY-COM-LLC
NetHandle: NET-50-62-0-0-1
Parent: NET50 (NET-50-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS26496
Organization: GoDaddy.com, LLC (GODAD)
RegDate: 2011-02-02
Updated: 2014-02-25
Comment: Please send abuse complaints to abuse@godaddy.com
Ref: https://rdap.arin.net/registry/ip/50.62.0.0
```

Reviewing for URL Visits

The primary method for reviewing URL access is via [Tanium's Trace DNS Queries](#).

- Either run: "Trace DNS Queries[3 days,1536785672356|1536782073356,1,0,10,0,,(?)[**SUBDOMAIN** if applicable].[**DOMAIN**].[**TLD**]*,*]" where **DOMAIN** is the website domain, **SUBDOMAIN** is the url before the domain, and **TLD** is the ending piece of the url, the top-level domain, before any /
- Example:** Get Trace DNS Queries[3 days,1551803153252|1551799554252,1,0,1,"","","","(?){smile.amazon.com.*}","",""] from all machines

or

- Use Question Builder to fill out the fields as follows:
 - Time Range:** 3 days
 - Absolute Time Range:** Leave untouched
 - Treat Inputs as Regular Expressions:** Check
 - Output only Yes or No:** Uncheck
 - Max Results Per Host:** 10
 - Make Stackable / Skip Unique:** Uncheck
 - Process Path:** Leave blank
 - Username:** Leave blank

- **Query:** (?i)[subdomain if applicable].[domain].[suffix].* (**Example:** (?i)smile.amazon.com.*)
- **Response:** Leave Blank
- **Operation:** Leave blank
- Attach the Tanium hits to respective SIR incidents.
- When found hits in Tanium, contact the user to get info if he input his credentials.
 - If yes, follow the [Employee Compromise Containment](#) process.

Process FAQs

What if a C3 Rep Reports a Phish Targeting a Customer?

Occasionally, C3 reps will send phishing emails targeting customers, especially those impersonating GoDaddy, to IsItBad@GoDaddy. IsItBad@GoDaddy is reserved solely for suspicious emails targeting GoDaddy employees. Phishing reports targeting customers are handled by a different team. To report those, submit a ticket using the [Front of Site form](#).

What is a Business Email Compromise (BEC) attempt?

Business Email Compromise (BEC) refers to a body of social engineering attempts in which the Threat Actor (TA) attempts to impersonate a member of the targeted company/organization in order to either obtain sensitive data or, most often, convince the target to perform a transfer of funds to an account controlled by the TA. Most often these are initiated with a communication to the user that will not include a malicious hyperlink or attachment, but rather will appear as an urgent request from the spoofed member. Although the origins of this type of attack refer to the compromise of an internal account to send this mail, many recent cases use a spoofed (non-internal) address. Some additional resources for understanding BEC can be found here:

- [https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-\(bec\)](https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec))
- <https://info.phishlabs.com/blog/phishing-attack-breakdown-1-bec-scams>

Resources and Definitions

Internal Resources

- Content Search - <https://protection.office.com/?ContentOnly=1#/contentsearchbeta>
- Message Trace - <https://protection.office.com/#/messagetrace>
- Tanium - <https://tanium.int.godaddy.com>
- Front of Site Abuse Form - <https://supportcenter.godaddy.com/AbuseReport>

DCU Contacts

Digital Crime Unit (DCU-ENG)

- SLACK: #dcueng
- Internal Email: DCUEng@GoDaddy.com
- Public Email: Abuse@GoDaddy.com

External Resources

- Netcraft Toolbar - http://toolbar.netcraft.com/report_url
- Google Safe Browsing (Firefox, Chrome & Safari) - https://safebrowsing.google.com/safebrowsing/report_phish?hl=en
- Anti-Phishing Work Group (APWG) - <https://antiphishing.org/report-phishing/>
- Trend Site Safety Center (WRS) - <https://global.sitesafety.trendmicro.com/index.php>
- URLQuery - <https://urlquery.net/>

Communication Templates

Response to Reporter - Not Malicious

Thank you for reporting this to us. We have investigated the email and determined that it is not malicious as it does not contain any malicious links or attachments. If you were not expecting this email, feel free to delete it from your inbox. No further actions are required from you at this time.

Response to Reporter - GoDaddy Customer Phish

Thank you for reporting this to us. We have reviewed the message and determine that this was a phishing message reported by a customer. Please be aware that the IsItBad@GoDaddy.com address is intended for the purpose of reviewing suspicious messages directed at GoDaddy employees. We have reported this to the appropriate team at this time, however in the future customers who believe they have received a phishing message that is either from GoDaddy services or intended to impersonate GoDaddy should do so via our Abuse Form located here: <https://supportcenter.godaddy.com/AbuseReport>

old Retired - IsItBad Process

Table of Contents

- General Workflow
 - Investigation Process
 - Initial Steps
 - Message Removal
 - Malicious Attachment
 - Closing Steps
 - Other Information
 - What types of reports does IsItBad handle?
 - What if I don't know if a message is malicious?
 - What happens to purged messages?
 - Additional Resources
 - - Templates -
 - - Associated Documents -
 - - External Sites -
-

General Workflow

› [Click here to expand...](#)

Investigation Process

Initial Steps

1. Create a new ServiceNow Incident.
 - a. **Title:** IsItBad - <MessageSubject>
 - b. **Assignment Group:** Eng-Gess
2. Download the original reported message.
 - a. If the reporter did not forward the message as an attachment, create a **Content Search** to obtain a copy.
3. Review any relevant Message Header information for indications of suspicious/malicious intent.
› [Example...](#)

↑ LIMIT-DAVIDD:Downloads dduboisi\$ cat jason@godaddy.com is\ no\ longer\ active.eml

```

Received: from DM5PRO2MB3366.namprd02.prod.outlook.com (10.164.152.158) by
CY4PRO2MB3366.namprd02.prod.outlook.com (10.165.89.149) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
15.1.1143.10 via Mailbox Transport; Fri, 9 Jun 2017 03:41:58 +0000
Received: from BY2PR02MB329.namprd02.prod.outlook.com (10.141.140.142) by
DM5PRO2MB3370.namprd02.prod.outlook.com (10.164.152.158) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
15.1.1143.10; Fri, 9 Jun 2017 03:41:56 +0000
Received: from MWBPR02CA0016.namprd02.prod.outlook.com (10.168.209.154) by
BY2PR02MB329.namprd02.prod.outlook.com (10.141.140.142) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
15.1.1143.10; Fri, 9 Jun 2017 03:41:55 +0000
Received: from SNINAM01FT002.eop-nam01.prod.protection.outlook.com
(2a01:111:f400:7e40::203) by MWBPR02CA0016.outlook.office365.com
(2603:10b6:300:4b::26) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.1157.12 via
Frontend Transport; Fri, 9 Jun 2017 03:41:55 +0000
Authentication-Results: spf=pass (sender IP is 104.47.1.99)
smtp.mailfrom=unicef.org; godaddy.com; dkim=pass (signature was verified)
header.d=Unicef.onmicrosoft.com;godaddy.com; dmarc=bestguesspass action=none
header.from=unicef.org;
Received-SPF: Pass (protection.outlook.com: domain of unicef.org designates
104.47.1.99 as permitted sender) receiver=protection.outlook.com;
client-ip=104.47.1.99; helo=EUR01-VEL-obe.outbound.protection.outlook.com;
Received: from EUR01-VEL-obe.outbound.protection.outlook.com (104.47.1.99) by
SNINAM01FT002.mail.protection.outlook.com (10.152.64.63) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id
15.1.1143.11 via Frontend Transport; Fri, 9 Jun 2017 03:41:54 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=Unicef.onmicrosoft.com; s=selector1-unicef-org;
h=From;Date:Subject:Message-ID:Content-Type:MIME-Version;
bh=5ol162oJ26chvKRwp3MmJNSUirz/fYRR9uxGfJbZ0BY=;
b=OTU4IOfct+qoYrKkBuÜvaKRYv7XdhgUkrx6CT84D86/DD9KUWCC3+rm2RKRV7fa6eoQCQq4+yYLy8dk7BLY9jdp8u1y1ju1
Authentication-Results: godaddy.com; dkim=none (message not signed)
header.d=none;godaddy.com; dmarc=none action=none header.from=unicef.org;
Received: from unicef.org (45.76.118.22) by
HE1PR0502MB3033.eurprd05.prod.outlook.com (2603:10a6:3:d9::10) with Microsoft
SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.1157.12; Fri, 9
Jun 2017 03:41:51 +0000
From: team Microsoft <ediab@unicef.org>
To: <jason@godaddy.com>
Subject: jason@godaddy.com is no longer active
Date: 09 Jun 2017 03:41:33 -0700
Message-ID: <>20170609034132.D55F74187E135B22@unicef.org>
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
X-Originating-IP: [45.76.118.22]
X-ClientProxiedBy: SG2PR0401CA0024.apcprd04.prod.outlook.com
(2603:1096:3:1::34) To HE1PR0502MB3033.eurprd05.prod.outlook.com
(2603:10a6:3:d9::10)
Return-Path: ediab@unicef.org Message Return-Path
X-MS-PublicTrafficType: Email
X-MS-TrafficTypeDiagnostic: HE1PR0502MB3033:|BY2PR02MB329:|DM5PRO2MB3370:
X-MS-Office365-Filtering-Correlation-Id: 22588682-2ffb-4380-5533-08d4aee97949
X-MS-Office365-Filtering-HT: Tenant

```

MTA Paths are written from bottom to top

Message Authentication Results

Received by Outlook

Initial MTA Details

4. Review the Message Body for indications of suspicious/malicious intent.

› Example...

What makes a message suspicious? Phishing attempts are a form of social engineering. The attacker relies on basic queues to convince a target that a message is legitimate and that they should take whatever action that attacker has directed them to. In the case of most phishing messages, the primary queues are:

- A sense of urgency: The attacker uses language or words that invoke a need to quickly address a situation. This reduces the amount of time a user will spend scrutinizing the message.
- A sense of legitimacy: By including language, images, etc. that parody a legitimate message attackers play off queues that a legitimate message uses to identify itself to users.

One method most attackers use to hide the intent of their phishing messages is to avoid any specifics which may identify their message as fake. One benefit to this is that means messages are often lacking in things which the true message would not, such as Account Numbers, Names, etc. In addition, messages are often from non-English speaking users are drafted in such a way as to contain odd wording or grammar which can flag the email as suspicious. Below is an example of a phishing attempt sent to one of our users with some key indicators marked:

Dropbox Reminder - Casey Smith has shared a document with you.

Microsoft Corporation [US] | <https://outlook.office.com/owa/projection.aspx>

Reply all | Delete Not junk | ...

Who is the Sender? Why am I receiving this?

Dropbox Reminder - **Casey Smith** has shared a document with you.

D Dropbox <dropbox@veintrain.com>

Thu 06/08, 11:01
David R. DuBois

Odd Sender

Reply all | ...

Junk Email Delivered to Junk

This message was identified as spam. It's not spam

Notice: This email is from an external sender.

Dropbox Sense of Legitimacy

Hello,

This is a reminder that Casey Smith shared with you document called "[Payment Invoice 864834721](#)" and left you this message:

Sense of Urgency

"Please let me know if you have any questions about the invoice 864834721. ... Thank you in advance for your prompt payment." Casey

[View file](#)

Contact

Have questions or concerns about Dropbox, our Services and privacy? Contact us at privacy@dropbox.com.

Spelling & Grammar Mistakes

Message is Strangely Formatted

Linked URL is Suspicious

bucksinvestmentgroup.com/viewdoc/file.php?document=ZGR1Ym9pc0Bnb2RhZGR5LmNvbQ==

5. Determine if the message is malicious

a. If the message is malicious

- i. Record the related Message Header details in the SECINC ticket.
 - The following Header must be included in ServiceNow: *Recipient, Sender, Subject, Date, Message-ID*
 - Other valuable items include: *Reply-To, Return-Path, Authentication-Results, X-Originating-IP, X-MS-Exchange-Organization-SCL*
- ii. Attach the email to the SECINC ticket in an encrypted zip.
(password: *infected*)
- iii. Perform Message Removal.
- iv. Address Malicious Hyperlink or Malicious Attachment
- v. Complete Closing Steps. Incident is **Confirmed**.

b. If the message is not malicious

- i. Skip to Closing Steps. Incident is **False Positive**.

Message Removal

1. Perform a **Content Search** to locate any offending messages in our system.
 - a. **Name:** < Incident# > (Example: SEC0012345)
 - b. **Location:** Search Everywhere > Exchange
 - c. **Query:** Depends; Generally Subject and/or Sender
(You may have to adjust the parameters multiple times to catch all senders/versions of the message)
2. Once the Content Search is completed, use **Powershell** to:
 - a. Run Search Results and obtain a list of Unique Recipients. Record the number in the Incident.
 - b. Submit a Purge and monitor using Purge Status. Once it completes record the job details in the ServiceNow Incident.
3. Depending on what type of malicious content is in the message:
Continue on to address the Malicious Hyperlink or Malicious Attachment.

Malicious Hyperlink

1. Determine where the URL leads, who the domain is registered through, who hosts it, whether it redirects/downloads a payload, or if it is no longer live.

a. Record the destination URLs in the Incident (be sure to modify the URL to prevent clickthrough)

< Example – hxxp://domain[.com]/path/file.ext >

b. If possible, include a screenshot of the final phishing destination page.

› [Curl to Check Headers...](#)

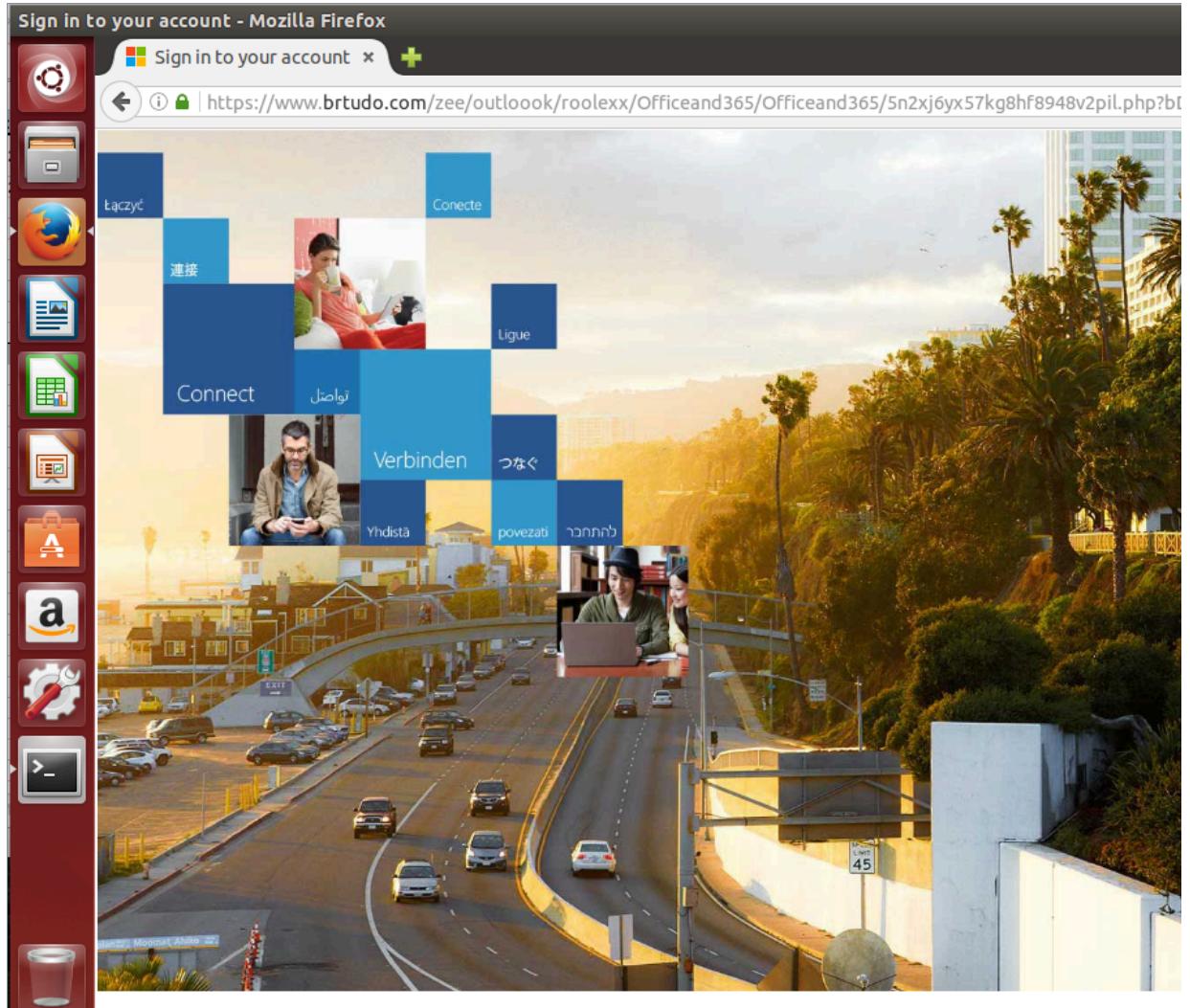
```
LIMIT-DAVIDD:Downloads ddubois$ curl -I google.com
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/ URL Redirects
Content-Type: text/html; charset=UTF-8
Date: Tue, 13 Jun 2017 18:00:12 GMT
Expires: Thu, 13 Jul 2017 18:00:12 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219 Hyperlink
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN

LIMIT-DAVIDD:Downloads ddubois$ curl -I http://www.google.com/
HTTP/1.1 200 OK HTTP Response Code
Date: Tue, 13 Jun 2017 18:00:20 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1 Destination Content Type
P3P: CP="This is not a P3P policy! See https://www.google.com/support/accounts/answer/151657?hl=en for more info
Server: gws
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Set-Cookie: NID=105=Y74PXzvZTOOPQlaAgYlnbiUYlOMboaIBEl6olwRKNk7gEZy5FzwGEnoC58YAnOx1-6gyDP0gL6RkiScMM9dC6dAO00v
cUzCf2wUiw; expires=Wed, 13-Dec-2017 18:00:20 GMT; path=/; domain=.google.com; HttpOnly
Transfer-Encoding: chunked
Accept-Ranges: none
Vary: Accept-Encoding
```

Watch for URL Redirects.
Find the final destination.

› [URL Destination...](#)

◆ You should be using a sandbox or virtual machine for this. Just in case.



› [Whois Checks...](#)

===== Domain Registration Whois =====

```
>LMIT-DAVIDD:Downloads ddubois$ whois google.com
Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: GOOGLE.COM
Registrar: MARKMONITOR INC. Registrar
Sponsoring Registrar IANA ID: 292
Whois Server: whois.markmonitor.com
Referral URL: http://www.markmonitor.com
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNS Nameservers

Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Updated Date: 20-jul-2011
Creation Date: 15-sep-1997
Expiration Date: 14-sep-2020

>>> Last update of whois database: Tue, 13 Jun 2017 17:47:42 GMT <<<
```

===== Domain DNS Information =====

```
>LMIT-DAVIDD:Downloads ddubois$ dig google.com
; <>> DiG 9.8.3-P1 <>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26438
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;google.com.           IN      A
;; ANSWER SECTION:
google.com.        46      IN      A      216.58.193.206
DNS A Record - Hosting IP

;; Query time: 13 msec
;; SERVER: 172.31.250.11#53(172.31.250.11)
;; WHEN: Tue Jun 13 10:48:38 2017
;; MSG SIZE rcvd: 44
```

===== IP Whois =====

```
>LMIT-DAVIDD:Downloads ddubois$ whois 216.58.193.206
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/public/whoisinaccuracy/index.xhtml
#

#
# The following results may also be obtained via:
# https://whois.arin.net/rest/nets;q=216.58.193.206?showDetails=true&showARIN=false&showNonArinTopLevelNet=false&ext=netref2
#
NetRange:      216.58.192.0 - 216.58.223.255
CIDR:          216.58.192.0/19
Network Range and Name
NetName:       GOOGLE
NetHandle:     NET-216-58-192-0-1
Parent:        NET216 (NET-216-0-0-0-0)
NetType:       Direct Allocation
OriginAS:     AS15169
Organization: Google Inc. (GOGL)
ASN and Owner
RegDate:      2012-01-27
Updated:       2012-01-27
Ref:          https://whois.arin.net/rest/net/NET-216-58-192-0-1

OrgName:       Google Inc.
OrgId:         GOGL
Address:       1600 Amphitheatre Parkway
City:          Mountain View
StateProv:    CA
PostalCode:   94043
Country:      US
RegDate:      2000-03-30
Updated:       2017-01-28
Ref:          https://whois.arin.net/rest/org/GOGL
Registered Organization & Location
```

2. Report the URL to instigate takedown:

- If the domain IS NOT hosted with GoDaddy:
 - Netcraft - [Report a Phishing URL](#)
 - Google Safebrowsing - [Report Phishing Page](#)
- If the domain IS hosted with GoDaddy and the phishing page is live:
 - Report to DCU via Front of Site and notify in #dcuong. Be sure to provide the URL, Registrar and Hosting provider.
 - › [Example...](#)

http://angiestoy[.com]/file.php?d=
Registrar: GoDaddy.com, LLC
angiestoy[.com]. 600 IN A 185.104.248.16
angiestoy[.com]. 600 IN A 194.87.94.1

3. Review access to the URL and any redirect points via [Websense](#) to determine:
 - a. What the **current Category** for each URL is. If the URL is not in a blocked Category, [move it to one](#).
 - b. Determine if any users have accessed the URL and when.
 - c. Record any visitations in the Incident.
 - d. Continue on to [Closing Steps](#)

Malicious Attachment

⚠ Be VERY careful when downloading files from messages. If you have a Virtual Machine or Sandbox make sure to use that location to download and store any malicious files.
DO NOT handle files via Windows Explorer. Once you have the file downloaded any review of it should be done via Command Line to avoid accidental execution.

1. Obtain a copy of the file from the message.
 - a. If AV deletes/quarantines the downloaded file:
 - i. Record this in the Incident for locating other machines that download the file.
 - ii. Re-download the file to your H: drive.
2. Review the file to determine if it is known-malicious.
 - a. Hash the file (MD5/SHA1) and search for it and the file name using [VirusTotal](#) or [Malwr](#)
Do NOT submit the file itself to these sites.
 - b. Use other tools to review the file, if possible.
 - c. Record your findings in the Incident.
3. Check for users who have downloaded and/or executed the file via [Tanium](#)
([Trace Executed Processes](#) and [Index Query File Exists](#))
 - a. Record any potential compromises in the Incident.
 - b. Continue on to [Closing Steps](#)

Closing Steps

1. If any potential compromises were detected:
 - a. Create a new Incident to investigate each user/workstation.
2. Record any final information in the Incident:
 - a. **Event Time:** When the message was received by the reporter.
 - b. **Detect Time:** When the report was received by GESS.
 - c. **Contain Time:** When the messages were purged and URL(s)/attachment(s) blocked.
(Contain Time is not required for False Positive Incidents)
 - d. **Resolve Time:** The time at which all actions have been taken to complete the investigation process and the ticket is Closed.
 - e. Determine the appropriate **Priority** using the [Incident Priority Matrices](#).
3. Close the Incident with the proper type:
 - a. **False Positive:** The message was not malicious and/or no action was required.
(Example: valid message, scam message w/o links or attachments, advertisements, customer reports, etc.)
 - b. **Confirmed:** The message was malicious and/or required investigation.
4. If the Incident was **Confirmed**:
 - a. Report detected IOCs to EMEA using the below template.
 - › [Template...](#)
 - To: mail-admin-emea@godaddy.com
 - CC: security-emea@godaddy.com; isitbad@godaddy.com;
 - Subject: IsItBad IOC - <SEC Incident #>
- URL(s):
Potential EMEA Recipients:
General message details:
 - > Subject:
 - > Sender:
 - > Message-ID:
- File Hashes:
Virus Total Info:
5. Respond to the individual(s) who reported the message.
 - a. If **False Positive** the response should contain:
 - i. Thank the user for their report
 - ii. Identify the message as false positive and briefly explain why
 - iii. Identify further action to take (if any)
 - iv. Direct them to proper reporting channels (if any)
 - b. If **Confirmed** the response should contain:
 - i. Thank the user for their report
 - ii. Confirm the message was malicious and briefly explain why
 - iii. Verify that we've taken action

› Examples...

!! These are only for use as an example. We want to make sure to personalize responses to ensure continued engagement. !!

--- False Positive (Customer Report) ---

Thank you for reporting to this message to us. The message which your customer provided is an advertisement and, while unsolicited, it is not malicious.

Please note that IsItBad is the reserved address for reporting suspicious emails which are received by GoDaddy employees. If a customer is reporting an abuse of GoDaddy services or a message which they believe is impersonating GoDaddy they should be directed to send their report to Abuse@GoDaddy.com

--- False Positive (Scam Message) ---

Thank you for your report. Upon review it appears that this is generic scam message. These types of activities usually rely on you replying to the message and do not contain a malicious attachment or URL that we can further investigate. We would recommend that you flag the message as Junk and/or purge it from your inbox.

--- Confirmed Positive (Generic Phish) ---

Thank you for reporting this to us. As suspected this is a phishing message targeting email credentials. We have taken action to block the malicious URL and prevent further impact to users.

--- Confirmed Positive (Wire Transfer) ---

Thanks for notifying us of this. As you suspected the message which you received is not legitimate; the actual sender is xxxxx. We've taken action to remove any instances of this message from our system. These types of social engineering have become more common recently and it pays to be extra vigilant. A good method to prevent being fooled by messages of this type is to perform a secondary confirmation of any requests of this nature over any trusted communication path such as by Phone or via Slack.

Other Information

What types of reports does IsItBad handle?

IsItBad is the primary reporting path for ANY suspicious messages which a GoDaddy employee receives. Although our primary focus is to address messages which contain phishing or malware, we should also assist users to identify scams or other generic malicious messages. That being the case, please be sure that we direct users to the appropriate point of contact if one other than IsItBad exists.

What if I don't know if a message is malicious?

If ever in doubt, be sure to escalate the message to a senior member for investigation. This is especially important if the message is potentially targeted directly at GoDaddy and/or executive staff (spear phishing).

What happens to purged messages?

The Powershell tool referenced in this process uses the SoftDelete option provided by Microsoft. This removes messages from a user's primary mailbox paths and places it in a hidden Recoverable Items folder. Users can technically still recover items from this folder using the Recover Deleted Items function within Outlook/OWA, however the level of extra steps between a user and a malicious message is sufficient for our use case.

Additional Resources

- Templates -

› [TEMPLATE - IsItBad Incident Summary](#)

 Unknown macro: 'multiexcerpt'

- Associated Documents -

[Incident Priority Matrices](#)

- External Sites -

[Phishing.org](#)

[Malwarebytes - How to Detect Phishing](#)

[DecentSecurity - Report Phishing and Malware](#)

old Incident Escalation Procedures

Table of Contents

- General Incident Escalations
 - How is incident escalation handled?
 - When should I escalate an incident?
 - How do I know who to escalate to?
- Escalation Contacts

General Incident Escalations

How is incident escalation handled?

Escalation of incidents to the various Information Security groups is accomplished by assigning ServiceNow tickets to the appropriate groups and/or individuals based on the process in question. In addition, there may be call-out requirements based on the severity of the incident. In general, the process for escalation should be as follows:



- ⓘ When updating the Assignment Group for a ticket it is important to ensure that you **add your current group to the Allowed Groups list**. If you fail to do so you will be unable to view the ticket after the Assignment Group update is completed.

When should I escalate an incident?

Each process can have custom definitions of when to escalate to the process owners, however in general the deciding factor is the **Priority** of the incident. Any incident with a **High** or **Critical** priority should, at the very least, be communicated the appropriate escalation contacts. In addition, it is important that we escalate **any undocumented situations** to the appropriate stakeholders. This allows us to ensure anything not currently defined in a playbook is handled by the owner of the associated space as well as provide a chance for new playbooks to be considered and implemented.

How do I know who to escalate to?

Each process will have a list of defined **Escalation Contacts** who are the individuals that are the first-line of contact for any escalations or questions about the need to escalate an incident during business hours. In the case that the escalation contact(s) are not available analysts should use the contacts listed as the **Responsible Team** for the process.

Outside of business hours the **Global Operations Center** can be engaged to reach out to the on-call contacts for the appropriate team.

Escalation Contacts

When an on-call group is required, the process requires that call-out requests are filtered through our Global Operations Center (GOC). Initial contact should be made via Slack to request assistance to identify the on-call members of the team owning the process in question. The GOC can also be reached via phone in cases that require high urgency.

| Global Operations Center |
|---|
| <ul style="list-style-type: none">• SLACK: #noc• PHONE: 480-505-8809 |

The on-call group for the *Infosec_Response* team are also available directly in ServiceNow via <https://godaddy.servicenow.com/oncall>

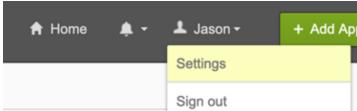
old Removing Old Okta Factors - Steps and FAQ

Purpose

The purpose of this document is to provide the steps needed to remove all but 1 factor in Okta, as well as address any questions/answers employees may have.

Steps to remove old factors

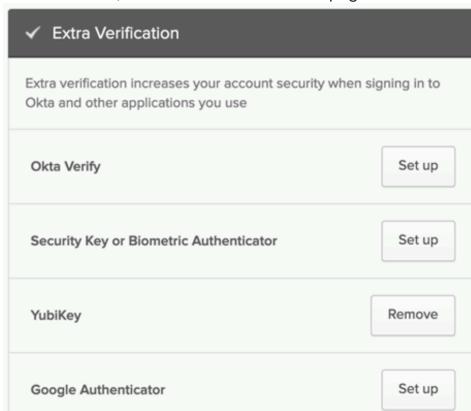
1. Open <https://godaddy.okta.com>.
2. Click your profile name drop down, and click Settings.



3. Click "Edit Profile" at the top of this page.



4. This step should require you to re-enter your password, and multi-factor code to proceed.
5. Once validated, scroll to the bottom of the page. Go to the section labeled "Extra Verification."



6. Click the "Remove" button next to the factors that you no longer use.
 - a. Okta Verify is currently preferred, unless you happen to have a physical Yubikey already set up. If so, please remove the others.
7. Once this is done, and you only see 1 "Remove" button, meaning only 1 factor enabled, please let me know.

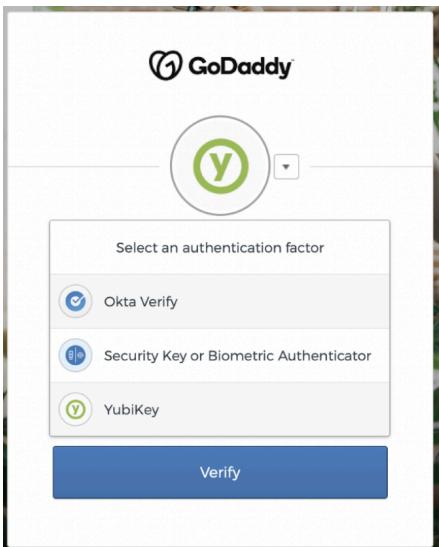
FAQ

Q: I have Okta Verify and Google Authenticator enabled. Which one should I disable?

A: Okta Verify is currently the preferred over Google Authenticator.

Q: I have a Yubikey, but I can't use it with Global Protect VPN, I need to keep Okta Verify.

A: Yubikeys are compatible with Global Protect VPN. When connecting, you should be able to click the drop down, and select Yubikey. Once you have used the Yubikey to authenticate Global Protect, then you can use the steps above to remove Okta Verify.



If you question is not in this document, please reach out to us with your questions via slack at #employee_security, or email us at employeesecurity@godaddy.com

old ServiceNow Create Trend AV (EMEA) Incident From SEC Incident

Description: This process uses a Security Incident OfficeScan child ticket to create an Incident (INC) and assign it to GetHelp. Currently used for generating EMEA INC tickets for further investigations, it has been genericized, and does not contain any specific EMEA info except any that is in the Title/Summary.

To see the new Action UI button, the SEC ticket has to have the following criteria:

1. Category=Intrusion
2. Sub-Category=Workstation
3. Detection Method=Trend AV
4. Parent Ticket is not empty
5. Parent Incident IS empty

When this criteria is met, the Action UI button will appear.

When clicked it will generate an Incident (INC) ticket. It will copy these existing SEC ticket fields and info:

1. Title
2. Summary → Description
3. Affected CIs → Affected CIs (if possible)
 - a. Grab the location off of the CI if possible and → INC Location field
4. Assign to GetHelp team.
5. Request Type=Other
6. Secondary Criteria=AV Troubleshooting
7. Impact/Urgency

It will also update SEC "Parent Incident" field with newly created INC.

The activity log will also be updated on both the SEC and INC tickets referencing each other.

NOTES: This is meant as a one-time-use button. When the SEC field Parent Incident is filled with the newly created INC number, this button disappears. If the INC number is removed from the SEC record, and saved, the button will reappear. If clicked, it will create a NEW INC. Please do **NOT** do this.

Also, this process copies all text from the Title and Summary fields. If data is set incorrectly in the SEC ticket, the resulting INC will also be incorrect.

If no Affected CI is on the SEC ticket, the resulting INC ticket will select "Remote" as the location. EMEA GetHelp is aware of this.

| | | |
|----------|--------|---------------------------------|
| Location | Remote | <input type="button" value=""/> |
|----------|--------|---------------------------------|

old InfoSec/CMDB/SNOW Support

Meeting Agenda

Weekly meet to discuss the Tier1 support for Tanium GAP/Tanium related issues handled by GCSO along with the SNOW/CMDB/IR and TSA team.

Respective Team Involved: GCSO, IR, TSA, CMDB, SNOW

| GCSO | SNOW | CMDB | TSA |
|---|---------------------------------|--|--|
| Syed Nayeem (Manager - GCSO) Sarfaraz Nawaz (Team Lead) Uday Sheshu Snehittha Chintapanti Masood Mohammed Durga Alluri Vijay Adiveni Sai Khorpoina Dakshayani Guraggari | Cindy Hoskins Veera Ayyagari | Austin Miller Kevin Loes David Koopman | Randy Thompson (Tech Lead) Andrea Gray Nathan Grandbois Vincent J. Koski Benjamin Smith Michael Pronchick |

| Slack to monitor | Slack for support assistance |
|---|------------------------------|
| #tanium #patchviz #secviz #tanium-emea | #infosec-support |

Intakes from meeting:

Discussing on the issues handled by GCSO with TSA/SNOW/CMDB and operationalize support for various InfoSec needs including Tanium Gap.

| Team | Next Step |
|--|-----------|
| CMDB | |
| SNOW | |
| TSA | |
| GCSO | |
| CMDB Playbooks | |
| <ul style="list-style-type: none">• Channels• Notes | |

CMDB Playbooks

- How to

SNOW Playbook

- Channels
- Notes
- How to

old CMDB - Check for Placeholder CI

Why: Sometimes Assets accidentally get put into a Live status which also puts the Placeholder "temporary" CI into a Installed status and that generates a tanium/patch ticket.

Typically Placeholder CIs have names that contain the Asset Name.

If the Name contains the Asset Name please create a ticket for the CMDB team to review.

The screenshot shows a CMDB asset creation interface. At the top, it says 'All Trustworthiness Validations Passed.' Below that is a table of asset fields:

| | |
|-----------------------------|---|
| Name | Supermicro AS -1123US-TN10RT |
| Fully qualified domain name | |
| Serial number | A438631X1804567 |
| Location | BOM1/Mumbai |
| Asset | A5082304 - Supermicro AS -1123US-TN10RT |
| Rack | BOM1SB01.04 |
| Rack U | 23 |
| Slot | |
| Rack Position | — None — |

Below the table is a tabbed section labeled 'Configuration' with tabs for Software, Networking, Meta, Reporting, Security, Maintenance, and Notes. Under Configuration, there are three fields:

- Asset tag: A5082304
- RFID Tag: A5082304
- Bios Version: (empty)

Two specific fields are highlighted with red arrows: the 'Name' field and the 'Asset' field in the Location row. Both fields contain the string 'Supermicro AS -1123US-TN10RT'.

old CMDB - Duplicate CI check

SOP to troubleshoot Tanium/Patch tickets when the CIs do not show a recent Tanium discovery.

1. Pull up CI in question and check for the name using this [QUERY](#).1.1 Click Show Filters
- 1.2 Enter the server name 1.3 Click Run
2. If there are multiple Results that are Live there is a strong chance that Tanium Is updating one record and not the other causing Tanium/patch ticketing problems.
- 2.1 Create a CMDB ticket for resolution of the Duplicate CI issue.
3. If only one result is present then continue to troubleshoot with the SRA team.

The screenshot shows a web-based CMDB search interface. At the top, there's a navigation bar with links like 'GOC - Global Oper...', 'Post Attendee - Zo...', 'Hosting Admins - H...', 'Mail - Austin J Mille...', 'CMDB - Ramp up P...', 'Global Process Man...', and 'Foundations eLearn...'. Below the navigation is a search bar with dropdown menus for 'Computers' and 'New', and a 'Search' button. A 'Name' field is populated with 'starts with Enter Server Name Here > Status = Installed'. Below the search bar is a toolbar with buttons for 'Run', 'Save', 'AND', 'OR', 'Add Sort', and a refresh icon. Red numbers 1, 2, and 3 are overlaid on this toolbar. Red box 1 points to the 'Run' button. Red box 2 points to the 'AND' button. Red box 3 points to the 'Status' dropdown menu. Below the toolbar, a message says 'All of these conditions must be met'. There are two main condition sections. The first section has a 'Name' dropdown set to 'starts with' and a text input 'Enter Server Name Here'. To its right are 'AND', 'OR', and a close ('X') button. The second section has a 'Status' dropdown set to 'is' and a text input 'Installed'. To its right are 'AND', 'OR', and a close ('X') button. At the bottom of the search interface are various filter buttons: 'Name', 'Asset', 'Assignment Group', 'Support group', 'Service Group', 'Fully qualified domain name', 'Environment', 'Status', and 'Primary Busin'. There are also icons for a gear and a magnifying glass.

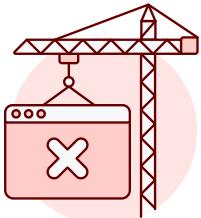
old HackerOne Process

When we receive reports in HackerOne, a severity rating is assigned and a problem ticket is created by SRA's process. If that severity is labeled as a High or Critical, then a SIR ticket is created. We run the ticket as a "Pre-incident" to close the vulnerability.



Oops, Diagram Unavailable

This diagram cannot be displayed. It may have been moved, deleted, or you do not have permission to view it.



Oops, Error 500!

Diagram Unavailable

Our system is currently under maintenance. Reach out to your administrator for a fix.



You have an unpublished draft.

1. Open the SIR incident and validate the Vulnerability.
2. Within the SIR ticket, the problem ticket is identified.

The application at <https://payments.click.godaddy.com> suffers from arbitrary content and injects resources such as iframes to the web page.

All Steps to reproduce:

1. Visit <https://payments.click.godaddy.com>
2. Click on the link in the email.
3. Observe the content being served. In case the browser is blocking content due to invalid certificate error, one can click anywhere in the page in Chrome browser and type "Rununsafe" and press Enter to see the site being injected.

All Impact statement:

- Filter input on arrival. At the point where user input is received ("Candidate"), filter as strictly as possible based on what is expected or valid input.
- Content Security Policy: As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

All Impact statement:

Nothing, attack vector is legitimate domain

If you would like to coordinate with SIA, please file for an exception at [a.ztEAC5d4tmt](#).
For any questions, please reach out on the [Vizir slack channel](#).

Hypothesis:

2023-04-29 09:44:52 - HackerOne
Phone Analytics
2023-04-29 09:44:52 - [HackerOne Work Name]
magi posted a comment on [a.ztEAC5d4tmt](#).
Hey @magi, the domain is yours and is being used to host your Phone analytics links, you point it with a cname.

- b. Open the problem ticket in a new tab and identify the owning team of the product under the assignment group. The "Assignment Group" is the team's product owner. You can click on the "information" button to get the manager of the team.

Urgency: 2 - Medium Root Cause: SecurityVulnerable

* Assignment Group: DEV-Web-Sales Vulnerability Type: BugBounty

Group

| | |
|---|--------------------|
| Name: DEV-Web-Sales | Parent: |
| Manager: Chris Bergstrom | Group Email: |
| Active: <input checked="" type="checkbox"/> | Active Members: 73 |
| 24x7: <input type="checkbox"/> | |
| Description: Developer Group | |
| Trustworthiness: Access granted is missing information | |
| Group Scope: In Scope | |
| Access Granted: | |
| Compliance: Not Compliant | |
| CI Assignable: <input checked="" type="checkbox"/> | |
| Group Trust Scope Reason: Has onCall Rota or is marked 24x7 | |

Open Record

3. Once a slack channel is created, invite the manager of the product team to the channel and provide the details of the problem ticket and an explanation of the vulnerability. Explain the severity and explain that we are running it as an incident and validating that it has not been exploited.
4. Run "Pre-incident" the same way that an incident is normally run, including assigning the severity of the SIR ticket according to IR standards, even if differing from the severity of the problem ticket.
5. Once an incident is closed, report to SRA that the incident has been closed and let them know IR's severity rating and the reasoning. This will help the SRA team to assess future HackerOne incoming reports.

old MVR Playbook

Table of Contents

- Table of Contents
- General Information
 - Process Summary
 - Process-Specific Definitions
- Process Workflow
 - MVR Admin Automation Workflow
 - MVR User Workflow
 - MVR User SLA Workflow
- Process Outline and Details
 - Incident Recording Guide
 - Process-Specific Priority Matrix
 - General Outline
 - Process Details
 - Captured Metrics
 - Process FAQs
 - What happens if I don't know how to calculate the GoDaddy CVSS score?
 - Where is the MVR form?
 - Why can't I see the MVR form?
 - Where can I point users to if they don't know how to work their tickets?
 - Where can I find more information about how the underlying process works?
 - What do I do if a team's remediation SLA has breached?
- Resources and Definitions
 - Internal Resources
 - External Resources
 - Communication Templates
 - Acknowledge new potential vulnerability intake
 - SLA breach escalation to CSM
 - Associated Audit Controls / Requirements

General Information

This playbook describes how to execute the Major Vulnerability Report (MVR) process. This process is invoked when the team is made aware of a new potential vulnerability. The vulnerability must be evaluated, scored, and then the appropriate actions must be taken depending on the score.

| | |
|-----------------------|--|
| Responsible Team | Vulnerability Management: #vulnerability_mgmt, vulnerabilitymgmt@godaddy.com Tier 1 / GSOC: #vm_tier1_priv (must have invite) |
| Process Owner | Vulnerability Management |
| Last Review Date | 2019-10-03 |
| Escalation Contact(s) | Vulnerability Management |
| Requests for Updates | ServiceNOW service portal to submit MVRs, contact Vulnerability Management for process changes |

Process Summary

This process provides a way for GoDaddy to proactively find and evaluate potential vulnerabilities in our environments and drive patching and remediation in order to maintain good security hygiene. Some of the applicable use cases for this process are as follows:

- Zero-day vulnerabilities
- Independent researcher disclosure
- Internal reports (eg. articles in slack)

Process-Specific Definitions

- **MVR:** Major Vulnerability Report
- **Submit MVR Form:** The form that is used to submit MVRs, located in the GD Service Portal under *My Digital Experience → Compliance → Submit MVR*
 - Note: The Submit MVR form is only available to those with the ***u_vulnerability_mgmt_admin*** ServiceNOW role
- **Admin / Admin Team:** People/team responsible for administering and using the MVR system
- **User:** People/team responsible for following the user doc to remediate systems
- **VM Team:** Vulnerability Management Team

- **Tier 1:** Tier 1 team/GSOC/Genpact

Process Workflow

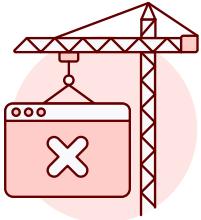
MVR Admin Automation Workflow

See [here](#) for the full admin document, which has details supporting the below workflow. If there is a discrepancy between this document and the admin document, the admin document shall be considered the primary source of truth.



Oops, Diagram Unavailable

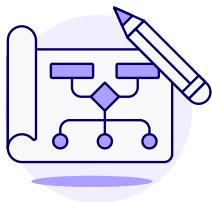
This diagram cannot be displayed. It may have been moved, deleted, or you do not have permission to view it.



Oops, Error 500!

Diagram Unavailable

Our system is currently under maintenance. Reach out to your administrator for a fix.



You have an unpublished draft.

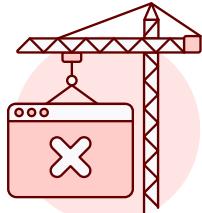
MVR User Workflow

See [here](#) for the full user document, which has details supporting the below workflow. If there is a discrepancy between this document and the user document, the user document shall be considered the primary source of truth.



Oops, Diagram Unavailable

This diagram cannot be displayed. It may have been moved, deleted, or you do not have permission to view it.



Oops, Error 500!

Diagram Unavailable

Our system is currently under maintenance. Reach out to your administrator for a fix.



You have an unpublished draft.

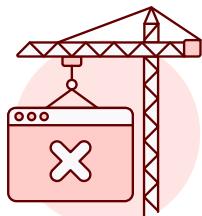
MVR User SLA Workflow

See [here](#) for the full user document, which has details supporting the below workflow. If there is a discrepancy between this document and the user document, the user document shall be considered the primary source of truth.



Oops, Diagram Unavailable

This diagram cannot be displayed. It may have been moved, deleted, or you do not have permission to view it.



Oops, Error 500!

Diagram Unavailable

Our system is currently under maintenance. Reach out to your administrator for a fix.



You have an unpublished draft.

Process Outline and Details

Incident Recording Guide

| Submit MVR Form Required Fields | |
|---------------------------------|---|
| Short title | A short description of the vulnerability, typically the vuln name |
| Description | A full description of the vulnerability, often obtained from the vendor or reporter |
| Remediate / Mitigate | Enter the steps to remediate or mitigate the vulnerability |
| Base CVSS | The base CVSS score, usually obtained from the vendor or reporter |
| GoDaddy CVSS | The GoDaddy-adjusted CVSS, which takes into account our environment and other factors. This field is what the MVR automation workflow keys off of. See the admin workflow above for automation details. |

The form itself has some short descriptions for many of the input fields. The [admin doc](#) has more details on the Submit MVR form fields. The [user doc](#) has more details on the MVR child ticket fields.

Process-Specific Priority Matrix

| CVSS Rating | Action |
|-------------|--|
| Critical | Fill out form, automation creates tickets and starts the Critical MVR SLA |
| High | Fill out form, automation creates tickets and starts the High MVR SLA |
| Medium | Fill out form, automation creates and auto-closes ticket with notifications. Expectation is that remediation will occur as part of the normal patching cycle |
| Low | Fill out form, automation creates and auto-closes ticket with notifications. Expectation is that remediation will occur as part of the normal patching cycle |

General Outline

1. Receive a new potential vulnerability (via email, slack, web article, vendor advisory, etc)
2. Research vulnerability and [score using CVSS](#)
 - a. Escalate to the VM team for help if needed
3. Fill out Submit MVR form in the GDSP
4. Communication blast automatically sent (email & slack) with information about the vulnerability (title, cves, cvss, description, etc)
5. One of three automated things happens, depending on CVSS score:
 - a. Critical, High: MVR RITM is created; MVR child tickets are created, associated with the parent MVR RITM, and are assigned to the people and teams in the [u_vm_ops_contacts](#) table in SNow; SLAs start
 - b. Medium, Low, or lower: MVR RITM is created, annotated, and automatically closed
 - c. Unknown: System awaits a change to the CVSS Variable field in the MVR RITM. VM & Tier 1 are notified a total of 4 times over the Unknown CVSS SLA period as a reminder to reinvestigate. Once the CVSS score is updated, then the automation goes back to the email/slack blast step
6. Be available for questions from remediating teams, can escalate to VM team as needed for guidance
7. Monitor for notifications of MVR tickets that have breached their SLA and follow up as needed, informing assignees that they must present their reasons to leadership at the CSM meeting
8. Once all child tickets are closed, close the MVR RITM ticket
9. Done!

Process Details

More process details may be found in the [Admin Document](#) and in the [User Document](#).

Captured Metrics

All metrics are captured in ServiceNOW. There is a [dashboard](#) (*Vulnerability Management Dashboard → MVR in SNow tab*) in SNow that captures and presents many metrics. This dashboard may change as leadership provides additional requirements.

Process FAQs

What happens if I don't know how to calculate the GoDaddy CVSS score?

- Follow [this guide](#) at first
- Reach out to the VM team for further guidance

Where is the MVR form?

- [GoDaddy Service Portal](#) → My Digital Experience → [Compliance](#) → Submit MVR

Why can't I see the MVR form?

- You must have the **u_vulnerability_mgmt_admin** role in ServiceNOW to view or submit the form. Contact the VM team if you need this role

Where can I point users to if they don't know how to work their tickets?

- Point them to the [User Documentation](#)
- If they have reviewed the user doc and still need help, send them to the VM team

Where can I find more information about how the underlying process works?

- See the [Admin documentation](#) for more details, including how to make changes to the process technology
- If you have reviewed the admin doc and still need help, contact the VM team

What do I do if a team's remediation SLA has breached?

- Follow up with the ticket assignee and their manager via email and inform them that they must attend the weekly CSM meeting to explain why they have not remediated yet

Resources and Definitions

Internal Resources

- Security Risks and Assessments (formerly Vulnerability Management) team:
 - Slack: #vulnerability_mgmt (or #vm_tier1_priv for non-public questions)
 - Email: sra@godaddy.com
- [User documentation](#) (includes tutorial video as an attachment)
- [Admin documentation](#)
- [Help calculating CVSS scores](#)
- [GDSP landing page](#)
 - My Digital Experience → [Compliance](#) → Submit MVR
- [MVR SNow Dashboard](#)

External Resources

- These are typically articles, NIST/Mitre or vendor reports, etc, and are unique to each MVR effort. This is usually what comes in as intake, often in Slack

Communication Templates

| Communication Name |
|--|
| Acknowledge new potential vulnerability intake <i>Usually via slack, but this can be used via whatever communication format the initial report comes in as:</i> Thank you for reporting this potential vulnerability. We will be investigating this and the results of the investigation will be posted to #vulnerability_mgmt in Slack. You or your leadership will be notified if action is required. SLA breach escalation to CSM <i>This should be an email, and a note should be put into the associated ticket that this email has been sent:</i> Hello. You are receiving this email because your remediation SLA has breached for the <MVR title> MVR remediation effort. Please review your ticket, <ticket # & link>, and be prepared to report to leadership at the weekly CSM meeting to explain why you have not met your remediation SLA. The meeting is on <meeting date/time> and you may attend by zoom using this link: <zoom link for the meeting>. If you have any questions, please reply to this email or reach out to our team in Slack in the <your team's slack channel> channel. Thank you. |

Associated Audit Controls / Requirements

N/A

old IWSaaS/URL Reclassification Requests

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [Rules of Engagement for Whitelists](#)
 - [Process-Specific Definitions](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [Process Details](#)
 - [Reviewing Malicious URLs](#)
 - [Captured Metrics](#)
 - [Process FAQs](#)
 - [What happens if "X"?](#)
 - [How can I determine if "Y"?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)
 - [Communication Templates](#)
 - [Associated Audit Controls / Requirements](#)

General Information

| | |
|-----------------------|---|
| Responsible Team | Global Cyber Security Operations (GCSO) |
| Process Owner | David DuBois |
| Last Review Date | 2020-02-14 |
| Escalation Contact(s) | @Juan Bustamante |

Process Summary

The flows in this section outline the general process to follow for routine processes for web filtering maintenance. Governing these flows are rules of engagement to follow as a set of guidelines.

Rules of Engagement for Whitelists

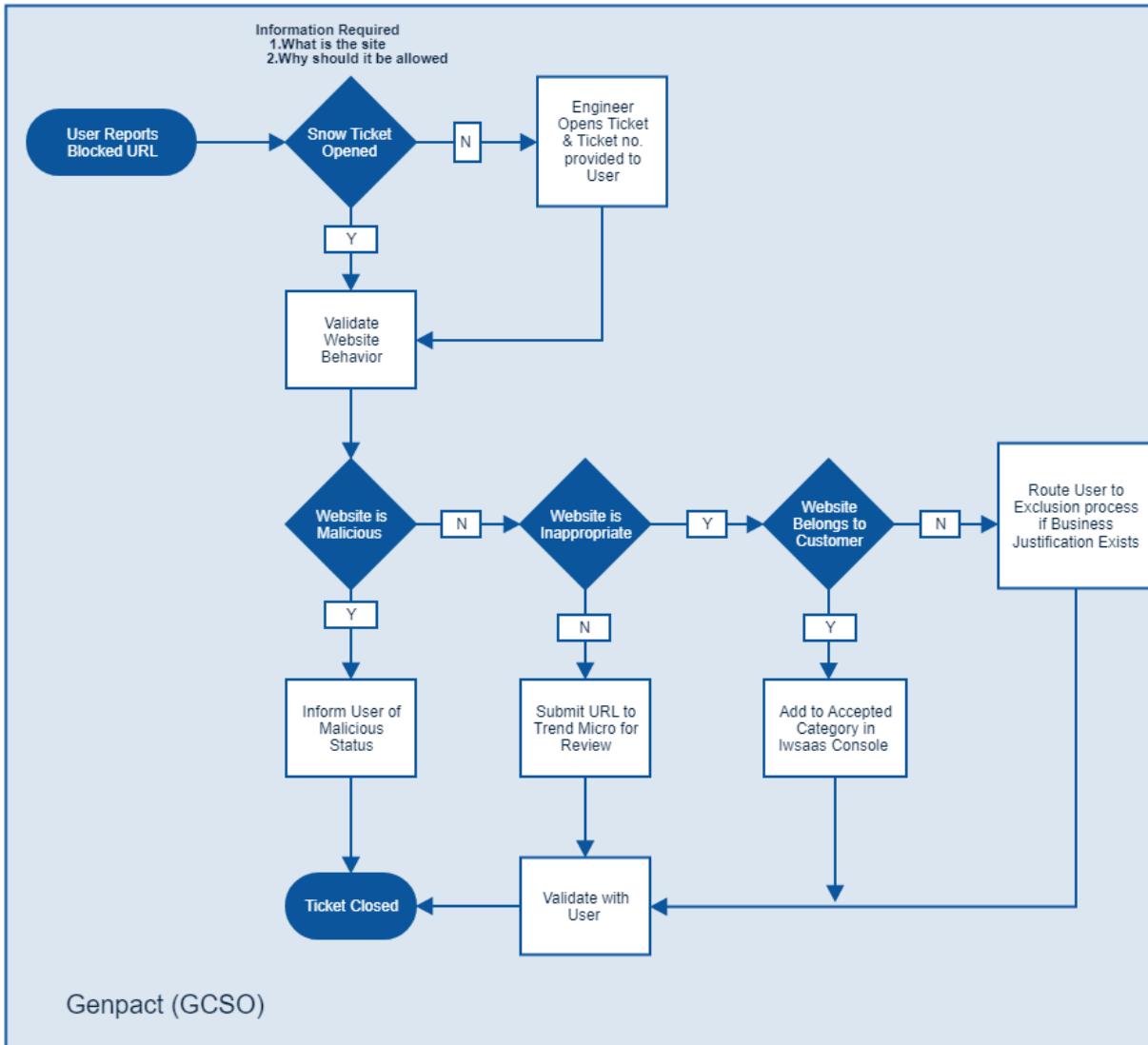
Rules of engagement are defined to serve as guideposts for the use of white/blacklists. The intent is to establish a structure without introducing unnecessary burdens. These are defined below:

1. Immediately following any addition to the whitelist , the URL will be submitted to Trend Micro for reclassification
2. Whitelist requests require a valid business justification and are subject to management approval
3. Whitelists will be pertinent to the most specific user set within reason

Process-Specific Definitions

- **Process-Specific:** Pertains only to this process. May have a different definition in other process flows.

Process Workflow



Process Outline and Details

Incident Recording Guide

General Outline

1. Perform Step A and document
2. Perform Step B
 - a. If "X" then do C
 - i. If "D" then do E
 1. Perform Step F (Tier 2)
 2. Perform Step G (Tier 2)
 - ii. If "not D" then do Z
 - b. If "not X" then do Z

Process Details

Reviewing Malicious URLs

1. Trace path URL takes to final landing page via appropriate methods and record findings in the Ticket.
 - a. Use [URL Scan](#), [VirusTotal](#) and other URL scanners to review the URL

- b. Using CURL via Virtual Machine or Sandbox.
 - c. From a browser in a Virtual Machine or Sandbox.
2. Capture a screenshot of the landing page and attach to the ticket.

Captured Metrics

- **Metric A** - Captured using E; (Required/Optional); Reporting example (if needed)
- **Metric B** - Captured using F; (Required/Optional); Reporting example (if needed)
- **Metric C** - Captured using G; (Required/Optional); Reporting example (if needed)

Process FAQs

What happens if "X"?

"X" is caused by A,B or C. Can be handled by doing "D".

How can I determine if "Y"?

"Y" is determined by E or F. If "G", then sometimes "H".

Resources and Definitions

Internal Resources

External Resources

Communication Templates

| Communication Name |
|--|
| <p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean libero risus, tristique viverra tortor eu, VARIABLE accumsan pellentesque dolor. Maecenas euismod, tellus ac vestibulum viverra, nulla ligula fermentum turpis, ut blandit dui sapien ac purus. Mauris ut nunc ante. Fusce nec arcu magna. Proin eget mattis quam.</p> |

Associated Audit Controls / Requirements

| Audit Type | Process Specifics | Requirement | Requirement Label |
|------------|-------------------|---|-------------------|
| PCI | Process - Step 2A | Immediately revoke access for any terminated users. | PCI DSS 8.1.3 |
| | | | |
| | | | |
| | | | |
| CIS | Full Process | Maintain Contact Information For Reporting Security Incidents | CIS 19.5 |

old OnCall Escalation Procedure

OnCall Escalation Process for GCSO

In the event a Security Event needs to be escalated to Incident Response please follow the following escalation path.

1. When GCSO identifies a confirmed threat, they will perform the following
 - a. During US/UK Business Hours
 - i. Notify @ir-team in the #internal-gcso slack channel.
 - ii. If No Response within 15m - Contact GOC to Notify On-Call
 - iii. If No response is received from Primary On-Call, Please request GOC to notify secondary On-Call
 - iv. If no response is received. Please request GOC to engage On-Call manager.
 - b. After US/UK Business Hours
 - i. Contact GOC to notify on-call.
 - ii. If No Response within 15m - Contact GOC to Notify On-Call
 - iii. If No response is received from Primary On-Call, Please request GOC to notify secondary On-Call
 - iv. If no response is received. Please request GOC to engage On-Call manager.
2. When GCSO needs assistance with an alert or request, they will perform the following
 - a. During US/UK Business Hours
 - i. Notify @sec_mon and @ir-team in the #internal-gcso slack channel.
 - ii. Communication must be clear and concise. Such as: <Teams> We need your assistance with the following alert as we can't determine XYZ
 - iii. Do not engage On-call
3. Acknowledgement
 - a. GCSO shall not consider the incident escalated until IR Acknowledges the Escalation
 - i. Expect to have IR or other teams state, one of the following statements, but not limited too: "I acknowledge", "I am taking a look", "working on it", "I will be there in X minutes"
4. Escalation Details
 - a. For all escalations, it is imperative that as many details known are provided.
 - i. What have you done?
 - b. [Splunk Events WorkFlow#Escalation](#)

Expectations for IR

1. Each IR member is responsible for being available during their On-Call period.
 - a. The Incident Response team on-call schedule can be viewed at <http://x.co/oncall>
2. Per the [Time Off Requests](#) process - if time out of office overlaps with OnCall responsibilities coverage must be coordinated.
3. All IR members should have the GOC Phone Numbers whitelisted in their phone to prevent filtering calls. This includes overriding Do Not Disturb settings.
 - a. GOC On-Call Procedures can be viewed at [Incident Management On-Call Policy](#)
 - b. A list of applicable phone numbers can be viewed at [GOC/SNOW Numbers](#)

Data Loss Reporting

To ensure proper reporting should data lost occur in incidents involving sensitive data we need to follow these guidelines when sensitive data loss has occurred. Some special requirements are provided here:

- **Credit Card Info:** Incidents involving credit card information should be reported to a manager or above in Technology Risk immediately (techrisk@godaddy.com for general notification). If it involves data on a hosting customer's server, also include Abuse.
 - Technology Risk will review to determine whether to file an incident report with the payment brands or credit card processors, following [Visa's What to Do if Compromised](#) document.
 - Technology Risk is also responsible for approving communications to customers or public posts regarding these types of incidents.
- **Amazon Marketplace Web Services (MWS):** Incidents involving products for sale on MWS should be reported to a Director or above on the appropriate product team.
 - The product team will review to determine whether to file an incident report with MWS.
 - Contact Amazon (via email to 3p-security@amazon.com) within 24 hours of detecting the incident

Additional reporting requirements can be found in </wiki/spaces/GDSP/pages/449741148>

Disable Employee Access

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [Process-Specific Definitions](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [Process Details](#)
 - [Disabling Active Directory Accounts](#)
 - [Process FAQs](#)
 - [What happens if the user is not available to select for remediation on the SNOW Tile?](#)

General Information

Process Summary

Occasionally we will need to provide support in removing an employee from the network. These are normally initiated by our HR, Legal, or Employee Relations (ER) teams and often come from management or through coordination with our Workplace Services Center (WSC). The following are a few cases where we may need to remove employee access:

- High-risk terminations being carried out in partnership with HR.
- An employee is being placed on administrative leave.
- Management or Incident Response has identified a potential internal threat actor.

Process-Specific Definitions

- N/A

Process Workflow



Process Outline and Details

Incident Recording Guide

| Incident Type | |
|---------------|--|
| Title | <Department> Request - <Reason> <ul style="list-style-type: none">• ER Request - Admin Leave• ER Request - High Risk Termination• IR Request - Internal Threat |
| Summary | Requesting Party: Request Reason: Requesting Party: David DuBois Request Reason: User is being placed on Admin Leave |
| Allowed Group | Requestor Group (When applicable) |
| Parent Ticket | Ticket# provided by Requestor (When applicable) |

General Outline

1. Request is received from authorized group:
 - a. Employee Relations (ER)

- b. Human Resources (HR)
 - c. Workplace Services at the behest of ER/HR (WSC)
2. Confirm the affected user with the requestor:
 - a. Verify the correct username is provided
 - b. Cross-reference by department/email/etc to confirm
 - i. If only a full name is provided we can verify via Workday lookup of user.
 - ii. If user is entered into the Affected Users field in SNOW the user record can be cross-referenced.
 3. Complete automated remediation of the affected user via the [Credential Mitigation](#) tile.
 4. Update the generated SNOW ticket:
 - a. Title & Summary
 - b. Child Ticket of Request Ticket (provided by requestor)
 - c. Allowed Groups includes Requestor's Group
 5. Disable Logic Access via the [Disable or Enable users in AD and Emp. Master](#) tile.
 6. Notify requestor when actions are completed.
 7. Document actions and close ticket.

Process Details

Disabling Active Directory Accounts

Active Directory accounts should only be disabled via the provided [Disable or Enable users in AD and Emp. Master](#) tile. If disabled directly in Active Directory the user will not be disabled immediately in the Employee Master legacy system. More importantly, if not enabled through this method the Employee Master account will remain disabled and the user will be unable to perform job duties tied to this account (mainly functions relating to customer calls or CRM).

Process FAQs

What happens if the user is not available to select for remediation on the SNOW Tile?

This usually would be caused by the user already being in a disabled status in Active Directory. When a user is terminated this should be updated in Workday and there is automation which will attempt to perform these actions as well. Generally our involvement is only needed if there is a risk the user may cause issues during the time that it takes for this automation to complete (approx. 1hr). If this issue occurs, check to see if the user's Jomax account is already in disabled status.

Reviewing Call Recording in ORECX

1. Table of Contents

- 1. Table of Contents
- 2. Requirements
- 3. Locating ORECX Recordings
- 4. Exporting ORECX Calls

2. Requirements

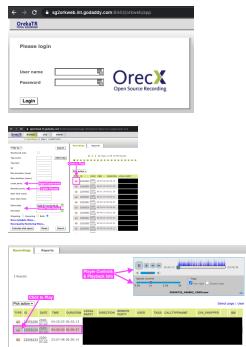
- You must have been granted access to the ORECX platform(s) you intend to query: [OrecX Recording System Access](#)
- You must be on VPN or internal-network to access the recording platforms.

3. Locating ORECX Recordings

Call recordings are stored in one of three location-dependent platforms indicated here:

| Recording Platform | Call Regions | Departments | Recording Retention |
|---|------------------------|--------------------------|---------------------|
| https://x.co/listenus >> https://p3plorkweb01.prod.phx3.gdg:8443/orkweb/app | • US | • Care • GetHelp (US) | • 1 year |
| https://x.co/listenin >> https://sg2orkweb.int.godaddy.com:8443/orkweb/app | • India • Singapore | • Care • GetHelp (IN) | • 90 days |
| https://x.co/listenbe >> https://n3plorkweb01.prod.ams3.gdg:8443/orkweb/app | • Sofia | • Care | • 90 days |

1. Log into the appropriate Recording Platform (see above).
2. Once in the console, you can search for the appropriate call. Make sure to set a reasonable timeframe if you know the period within which the call would have been made. Common identifiers to use are:
 - a. **ID** - The **ORECX Call ID** which is unique within the platform (but not across platforms).
 - b. **Local party** - The **username** of the agent who received the call.
 - c. **Remote party** - The **phone number** of the caller.
3. Once the call is located, you can click on the Speaker Icon to listen to the call.



⚠ The above list is not exhaustive for what is recorded in each location. When attempting to identify a call recording it may be necessary to review all of the systems. In addition, if we are certain a call should be recorded but cannot be found we will need to engage Telecom for assistance.

4. Exporting ORECX Calls

For privacy, security, and compliance reasons the exporting of calls cannot be performed by standard ORECX users. If a calls must be exported as part of evidence collection for a Security Incident we must do so via the available request path: [Recording Export Request](#)

- **Reason for Request?** - These calls are being requested as evidence for security incident #####. The Response team needs to obtain recordings for security retention & review.
- **Legal Case ID** - Use the Security Incident number.

Security@ Archive

General Information

- › [Reply to CVD - Cannot Reproduce](#)
<<<PERSON>>,

Thank you for reporting this to us.

Unfortunately we were unable to reproduce your report with the information provided and so no further action can be taken at this time. If you believe this is a valid issue, please provide us with any steps needed to duplicate as well as any additional information you may have.

Regards,
GoDaddy Security Team

- › [Reply to CVD - Request Info](#)
<<<PERSON>>,

Thank you for reporting this to us.

Unfortunately we were unable to validate your report with the information provided. Please provide us with any steps needed to duplicate as well as any additional information you may have.

Regards,
GoDaddy Security Team

- › [Reply to CVD - Payout Inquiry \(Need Info\)](#)
<<<PERSON>>,

Thank you for reporting this to us.

GoDaddy's standard security model is using a Coordinated Vulnerability Policy. While we do not currently operate a formal published bug bounty program, we are always open to reviewing reports and addressing them as appropriate.

Regards,
GoDaddy Security Team

- › [Reply to CVD - Already Reported](#)
<<<PERSON>>,

Thank you for reporting this to us.

We have reviewed the provided information and confirmed that this issue had been previously reported to us by another party and has already directed to the appropriate team(s) for investigation and remediation.

Regards,
GoDaddy Security Team

- › [Reply to CVD - Update Requests \(In Progress\)](#)
<<<PERSON>>,

Your report has been reviewed and directed to the appropriate team(s) for further investigation and remediation. If more information is necessary to resolve this issue, we will reach out to you directly.

Regards,
GoDaddy Security Team

- › [Reply to CVD - Payout Requests \(In Progress\)](#)
<<<PERSON>>,

Your report has been reviewed and directed to the appropriate team(s) for further investigation and remediation. We are still awaiting updates from the reporter.

Regards,
GoDaddy Security Team

- › [Reply to CVD - Issue Not Valid](#)
<<<PERSON>>,

We appreciate you reporting this issue to us. We have directed the provided information to the appropriate team(s) for review and the issue has been closed.

Regards,
GoDaddy Security Team

- › [Reply to CVD - Payout \(Request Acceptance\)](#)
<<<PERSON>>,

While we do not currently operate a formal published bug bounty program, we have been authorized to offer you a reward as a thank you for your effort and assistance.

Regards,
GoDaddy Security Team

Security@ General Inbox

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [Process-Specific Definitions](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [Captured Metrics](#)
 - [Process FAQs](#)
 - What should we do if we receive multiple False Positive reports?
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)
 - [Communication Templates](#)
 - [Internal Reporter](#)
 - [External Reporter](#)
 - [Other Responses](#)

General Information

 Unknown macro: 'metadata-list'

Process Summary

This process provides direction for the handling of communications to the Security@ general mailbox. This mailbox serves as a common point of contact for most general security requests from both external and internal entities. Some of the specific use-cases which are seen via this communication method are:

- [Coordinated Vulnerability Disclosure \(CVD\) Notifications](#)
- Reports of Impersonation of GoDaddy (Websites, Phishing Attempts, etc.)
- External Reports of Malicious Customer Activity (Malware, Phishing, Spam, etc.)
- Internal Reports of Suspicious Activity (Phishing, Physical Behavior, etc.)
- General Solicitations (Security Vendors, Services, SPAM, etc.)
- General Security-related Inquiries

Process-Specific Definitions

- [NONE](#)

Process Workflow



Process Outline and Details

Incident Recording Guide

Incident Type

| | |
|------------------|--|
| Title | <ul style="list-style-type: none"> Created As <ul style="list-style-type: none"> Security@ - <SENDER> - <SUBJECT> Updated To <ul style="list-style-type: none"> Security@<TAG> - <SENDER> - <SUBJECT> <p>Example :</p> <ul style="list-style-type: none"> Ingested: Security@ - myemail@domain.net - i think this is phishing Updated: Security@ABUSE - myemail@domain.net - i think this is phishing |
| Assignment Group | OPS-GCSO |
| Incident Type | <ul style="list-style-type: none"> Incident Category: --NONE-- Incident Subcategory: --NONE-- |

General Outline

1. GCSO receives automated SNOW ticket for review.
 - a. Review the message to identify the communication type
 - i. Update the Title field with the appropriate tag.
 - ii. Follow the appropriate reporting method.
2. Escalate to Tier 2:
 - a. Server related compromise
 - b. Social Engineering attempt
 - c. Data breach

ⓘ What if the message was also sent to the correct team by the reporter?

If the Security@ mailbox was CC'd, BCC'd or otherwise included on a message that was already delivered to the appropriate team we can close the ticket without further action. This will likely be the case only with Abuse-related messages however, and priority items such as CVD notices should still be handled per SOP to ensure they are not missed.

| Communication Type | Reporting Method | Notified Team | Identification Tag |
|------------------------------------|--|--|--------------------|
| CVD Notification | <ul style="list-style-type: none"> Child ticket created & assigned to DEV-AppSecurity Set to Pending - Internal until resolution is confirmed. | Dev-AppSecurity | CVD |
| GoDaddy Impersonation | <ul style="list-style-type: none"> If valid, report via FoS Abuse Form If not, Close False Positive | ENG-DCU | GDP |
| Customer Abuse Report | <ul style="list-style-type: none"> Report via FoS Abuse Form <ul style="list-style-type: none"> If this is not possible email to abuse@godaddy.com | ENG-DCU | ABUSE |
| Customer Security Concerns | Close False Positive - No further action | --- | CARE |
| Suspicious Internal Activity | <ul style="list-style-type: none"> If Cyber related - Add to Allowed Groups infosec_response and notify security@godaddy.com If Physical related - Add to Allowed Groups Physical Security Command Center and notify scc@godaddy.com via email. | <ul style="list-style-type: none"> infosec_response Physical Security Command Center | EMP |
| Threats or Threat Reports | <ul style="list-style-type: none"> If this is a received threat (not a report from OCEO, WSC, etc.), add to Allowed Groups Physical Security Command Center immediately notify #workplace-services via Slack If this is a Threat Report (from OCEO, WSC, etc.), verify scc@godaddy.com was included in the recipients and Close | Physical Security Command Center | THREAT |
| General Solicitations | Close False Positive - No further action | --- | SPAM |
| General Security-Related Inquiries | Assign to infocsec_response for additional review and notify via Slack/Email | --- | MISC |

Captured Metrics

- Volumetric Data
- Time In Progress
- Escalated Tickets
- Communication Types

Process FAQs

What should we do if we receive multiple False Positive reports?

Please notify management and/or the process owner if you encounter a situation where we continue to receive unwanted messages. We can review and determine if there is an appropriate method of blocking the sending party if necessary.

Resources and Definitions

Internal Resources

- NONE

External Resources

- NONE

Communication Templates

Internal Reporter

- [Direct to IsItBad](#)
<<<EMPLOYEE>>,

Thank you for reporting this to us.

Please be aware that the Security@godaddy.com mailbox is a general communication path with the Security team, however for reports of suspicious/malicious activity please forward the reported email as an attachment to IsItBad@godaddy.com so that we can expedite investigation.

Regards,
GoDaddy Security Team

- [Direct to Internal Department](#)
<<<EMPLOYEE>>,

Thank you for reporting this to us.

Please be aware that the Security@godaddy.com mailbox is a general communication path with the Security team, however for specific reports and inquiries

Regards,
GoDaddy Security Team

External Reporter

Other Responses

- [External Report - Direct to CVD Path](#)
<<<PERSON>>,

We appreciate you reaching out and have developed a system for responsible disclosure. To see the details on how to submit a potential issue, please visit:

Thank you,
<<<SENDER>>>

Revoke Compromised Certificate

1. Table of Contents

- [1. Table of Contents](#)
 - [1.1 Process Summary](#)
- [2. Process Workflow](#)
- [3. Process Outline and Details](#)
 - [3.1 General Outline](#)
- [4. Additional Documentation](#)
 - [4.1 Other Resources](#)

1.1 Process Summary

This process provides direction for revoking and retiring Internal and External certificates as instructed by the Cert-API team. The process can be used, but not limited to the following scenarios:

- Stolen Certificates
- Retired Domains
- Rogue Certificates
- Sub-domain Takeovers

| | |
|-----------------------|----------------------------------|
| Responsible Team | Cert-API Team |
| Process Owner | David Hernandez |
| Last Review Date | 2022-06-30 |
| Escalation Contact(s) | Ryanne Fox or Manager Mark Henry |

2. Process Workflow

3. Process Outline and Details

3.1 General Outline

1. Identify the certificate owners
 - a. Search for the certificate and owner [here](#). Note: Certificates and owners will not be found using the standard CMDB search process. Use the Certificate table listed here
 - b. Notify, The owner with the reason why the certificate needs to be revoked.
 - c. If the certificate is not compromised you may ask the owner to retire it using the "[Cloud-UI](#)" Portal.
Note: Cert owners can only Retire Certificates in "[Cloud-UI](#)". If the certificate has been compromised continue to the following step
2. To Revoke a Certificate
 - a. You will need to request help in the #cert-api channel using their automation. Hint: It's the Plus sign at the bottom left of where the text bar would normally be at.
They are the only people that can revoke the certificate. Once you have someone assigned to you, add them to the incident channel if one has been created.
 - b. In a rare case that you are not able to find help from #cert-api you may need to reach out to Ryanne Fox or the Manager Mark Henry.
3. Confirm the certificate is no longer active
 - a. Search for the certificate [here](#). If it is no longer active you will have zero results.

4. Additional Documentation

4.1 Other Resources

[Revoke process as followed by the Cert-API team](#)
[Revoke script as followed by the Cert-API team](#)

ServiceNow General Usage

Table of Contents

- General Information
- High-Level Design
- General Usage Workflow
- Field Definitions
 - State
 - Timestamps & Timeframes
 - Priority, Impact & Urgency
 - Data Type & Detection Method
 - Other

General Information

GoDaddy Cyber Incident Response teams currently utilize a custom ServiceNow table which provides a number of custom metrics and functions. However, as a result this also means it is necessary to understand the context behind the various fields and the workflow in which incidents are currently handled within ServiceNow. This page provides guidance surrounding the current ServiceNow table and the generally accepted usage.

High-Level Design

Our current ServiceNow structure utilized Incident Category and Subcategory to differentiate between incident types and determine the types of information we collect from these incidents. Below is a chart showing the division of categories and subcategories within our incident space as well as outlines the various collection fields that are included in these sections.

› [Excel Document with Field Outline](#)

| Primary Incident Category | Primary Category Fields | Required to Close? | Sub-Category | Sub-Cate |
|---------------------------|---|----------------------------|-----------------|--------------------|
| Intrusion | Affected CI's [SNOW] | X | Server | Applicat |
| | AffectedCI.Count [Dynamic, Int] | X | | User(s)Impa |
| | Contain Time [Date/Time] | If [!FalsePositive = True] | Workstation | WorkstationTy |
| | Contained? [Check] | If [!FalsePositive = True] | | User(s)Impa |
| | Contained.Summary [Dynamic, Text] | If [Contained = True] | | User(s)Impacted.C |
| | DSR [Check] | | | UserLocation(s) [N |
| | Environment [Dynamic, CMDB] | if [!Affected CI's == 0] | | UsersJobRole(|
| | Owner Notified? [Check] | | Networking Devi | User(s)Impa |
| | Owner(s) [Multi-Select, SNOW] | X | | SystemID |
| | PrimaryBusinessService [Dynamic, CMI] | if [!Affected CI's == 0] | Mobile Device | MobileDeviceI |
| | Root Cause [Dropdown] | | | User(s)Impacted.C |
| SocialEng | AssociatedCustomer# [INT] | | | UserLocation(s) [N |
| | Contain Time [Date/Time] | If [!FalsePositive = True] | | UsersJobRole(|
| | Contained? [Check] | If [!FalsePositive = True] | Email | Sender [Text] |
| | Contained.Summary [Dynamic, Text] | If [Contained = True] | | Subject [Text] |
| | User(s)Impacted [SNOW] | | | Reply-To Address |
| | User(s)Impacted.Count [Dynamic, Int] | | | MessageID [Text] |
| | UserLocation(s) [Multi-Select, SNOW, JI] [VE] | | | SearchName [Text] |
| | UsersJobRole(s) [Multi-Select] | | | SearchQuery [Text] |
| | | | Phone Call | Recipients [Int] |
| | | | | Reports [Int] |
| | | | | URLVisits [Int] |
| | | | | URLVisitsBlocked |
| | | | | URLVisitsReporte |
| | | | | FileDownloads [In |
| | | | | ConfirmedCompro |
| | | | | Re-Images [Int] |
| | | | | CallerPhone# [Tex |
| | | | | StatedName [Text] |

Sheet1

General Usage Workflow



Field Definitions

State

- **New** : A ticket that has not had any user activity performed. These will often be auto-generated by internal systems.
- **In Progress** : A ticket that is being actively worked by an analyst before it reaches any state of resolution.
- **Pending - Internal** : A ticket that is awaiting action from a group internal to the IT Security organization.
- **Pending - External** : A ticket that is awaiting action from another external team or service (Example: Internal IT, GETHelp, Development or Product Teams, Vendors, etc.)
- **Closed** : A ticket that needs no further action and is therefore resolved.

Timestamps & Timeframes

- **Event Time** : The time at which an event takes place. If unknown, best estimation or match detect time.
- **Detect Time** : The time at which the appropriate team/individual is made aware of an incident, through reporting or organic discovery.
 - **Time to Detect** : The time from the occurrence of an event or incident to the time that the appropriate team/individual is made aware of the occurrence.
- **Contain Time** : The time at which a TA can no longer continue malicious activity and/or adversely impact systems within the network. See [Containment](#)
 - **Time to Contain** : The time from the detection of an event or incident to the time that the appropriate steps have been taken to contain.
- **Resolve Time** : The time at which any and all follow-up actions are completed and the ticket is closed.
 - **Time to Resolve** : The time from the containment for an event or incident to the completion of all steps needed to resolve a ticket.
- **Time to Process** : The time it takes to process an event or incident in its entirety.
- **Dwell Time**: The amount of time in which a Threat Actor was able to gain unauthorized access or continue malicious activity.



- **Time in Progress**: This field is calculated as the total amount of time that a ticket is set to In Progress. This calculation occurs when a ticket is changed from "In Progress" to any other status.



Priority, Impact & Urgency

- **Impact** : The damage potential of a specific incident or event.
- **Urgency** : The need to address an incident or event to prevent occurrence of damage. The likelihood that an unresolved incident will lead to further damage.
- **Priority** : A combined scoring which accounts for both Impact and Urgency.

| | | PRIORITY | | |
|---------|--------|----------|--------|----------|
| | | High | Medium | High |
| URGENCY | High | Medium | High | Critical |
| | Medium | Low | Medium | High |
| | Low | Minor | Low | Medium |
| | | Low | Medium | High |
| IMPACT | | | | |

Data Type & Detection Method

- **Data Type** : Used to specify the type of data targeted or impacted by the event or incident.
- **Detection Method** : The path by which detection of an incident or event occurs.

Other

- **Business Impacted** : Signifies an incident or event which has caused widespread outages to either employees or customers.
- **Contained** : Signifies that the threat actor(s) have been prevented from continuing malicious actions.
- **Data Loss** : Signifies that data of the identified Data Type was confirmed to have been lost to the Threat Actor.
- **DSR** : Signifies that an incident or event is to be included in the Daily Security Report, and therefore is an audit compliance requirement.
- **False Positive** : Signifies that a reported event or incident was not a valid occurrence.
- **SLT Affected** : Signifies that a reported event or incident directly targeted or impacted an SLT member.

old Email Un-Quarantine Requests

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [Process-Specific Definitions](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [General Outline](#)
 - [Process FAQs](#)
 - [What types of business justifications are appropriate for releasing a malicious email to the requestor?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)

General Information

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Employee Cyber Security• SLACK: #employee_security• EMAIL: EmployeeSecurity@GoDaddy.com |
| Process Owner | @Former user (Deleted) |
| Last Review Date | 2018-11-09 by @David Dubois (Deactivated) |
| Escalation Contact(s) | @Juan Bustamante @Former user (Deleted) |
| Requests for Updates | Via Email - EmployeeSecurity@GoDaddy.com |

Process Summary

This process provides direction for the handling of un-quarantine requests generated by users who believe that a message has been incorrectly flagged and covers the following use cases:

- User requests assistance with a quarantined message via direct communication.
- User submits a request for assistance with a quarantined message.

Process-Specific Definitions

- **CAS (Cloud App Security):** A Trend Micro product currently providing security filtering to the GoDaddy Office365 tenant.

Process Workflow



Process Outline and Details

General Outline

1. User requests an email be un-quarantined.
2. Does a ticket exist?
 - a. If NO, direct to the [Cloud App Security](#) form.
3. Log into the [CAS Console](#) and navigate to the [Quarantine](#) tab.
 - a. Locate the email using the provided quarantine details. Generally the best filters are Sender, Recipient or Subject.
4. Does the quarantined email still exist?
 - a. If NO, close the ticket using the Close Skipped option. Record any findings.
5. Download the email for review by checking the box and selecting Download.
 - a. You may need to select encrypted zip if prompted to prevent AV detection of the downloaded document.
6. Review the email to determine if it is malicious.
 - a. If YES, did the user provide an appropriate business justification to obtain the message?
 - i. If YES, continue to Step 7.
 - ii. If NO, close the ticket using the Close Incomplete option. Record any findings.
7. If appropriate, use the Restore option to un-quarantine the email.
 - a. If multiple CAS requests were raised for the same URL which is safe to access, then [IT Security - Reclassify URL](#) request can be raised to reclassify the URL.
 - b. If the email was quarantined due to a non malicious link, then submit URL to 'RECLASSIFY REQUEST' at [Trend Micro Site Safety](#)
8. Close the ticket using the Close Complete option. Record any findings.

Process FAQs

What types of business justifications are appropriate for releasing a malicious email to the requestor?

In general, we will release malicious messages if the requestor has a job role or function that requires them to view malicious messages AND they are unable to use a centralized mailbox for this purpose. Some examples are:

1. Users who review malicious content reported by customers only on an occasional basis.
2. Users who receive reports that occasionally contain references to malicious content.
3. Users who are investigating a one-time occurrence.

NOTE: Users who have a role which would allow for a centralized mailbox (Abuse, Security, etc.) should not be using their personal mail accounts for this purpose.

Resources and Definitions

Internal Resources

- Cloud App Security (CAS) Console - <https://admin.tmcas.trendmicro.com/#!/login>
- ServiceNow Requests - https://godaddy.service-now.com/sc_req_item_list.do?sysparm_query=assignment_groupDYNAMICd6435e965f510100a9ad2572f2b47744%5Eactive%3Dtrue%5Ecat_item%3Dce126c833753d380eb8163d2b3990e59

Tanium Useful queries

DNS

Get Trace DNS Queries[1 week,1610976909262|1610973310262,0,0,1,","","(?i)domainhere.com.*","",""] from all machines

DNS for GCSO

Get Trace DNS Queries[3 days,1610979325902|1610975726902,1,0,10,0,"(?i)domainhere.ru.*","","","",""] from all machines

File/hash search

Get Index Query File Exists[0,*filename,*hashmd5,sha1hash,sha256hash,*] from all machines (* where no hash entry)

Network connections

Get Trace Network Connections[3 days,1610976608897|1610980207897,0,0,1,0,local ip,"",remote ip,"","","","",""] from all machines

How to enter a Vertigo child VM

1. Download a time limited certificate from [here](#)
2. Sync password via User Access Management [here](#) (required for first login)
3. Confirm IP address as a Vertigo IP [here](#)
4. SSH into the host IP.
5. Go to [Vertigo](#) and search for {CONTAINER_ID}

| Containers 1 | | | | | | | | | |
|--------------|--|-------------|------|---------------|--------|-------------------|-----|------|-------------------------|
| VE | | Primary IP | Vlan | Friendly Name | Status | OS | RAM | Disk | Created |
| 28882 | | 50.62.57.27 | 828 | wheelie | Live | CentOS 6 + cPanel | 3GB | 90GB | Feb. 5, 2015, 4:59 p.m. |

6. Sudo /usr/sbin/vzctl enter {CONTAINER_ID}
7. ## {CONTAINER_ID} can be found as Container ID in ToolZilla, or as Server ID in VAT
8. To exit press <ctrl>d

Using HUE to Query Hadoop

Table of Contents

- HUE - Hadoop Queries
- HUE - Viewing Table Details
- HUE - Querying JSON

HUE - Hadoop Queries

To query against Hadoop the easiest method, assuming that the necessary table is configured, is to utilize HUE.

1. Go to <https://hue.p3.int.godaddy.com/>.
2. Using the navigation on the left select HIVE and locate the correct Database.
3. Once you have located the table you wish to query can use the Query editor to build your query. This uses **SQL syntax**.
4. Click the play button to run your query.

The figure consists of four screenshots of the HUE interface, illustrating the steps to query a Hive database:

- Screenshot 1: Sources Selection**
Shows the "Sources" sidebar with "Hive" selected. A purple arrow points from the "Select Hive" button to the "Hive" entry in the list.
- Screenshot 2: Database Selection**
Shows the "Hive" database page. A purple arrow points from the "Search for DB" input field to the "cauth" database entry. Another purple arrow points from the "Click to Select" button to the "cauth_login" table entry.
- Screenshot 3: Table Selection**
Shows the "cauth_login" table page. A purple arrow points from the "Available Tables" link to the "cauth_login" table entry.
- Screenshot 4: Query Editor**
Shows the "My Query" section of the Query Editor. A purple arrow points from the "Click to Run" button to the SQL query text area, which contains:

```
1 SELECT * FROM cauth_login
2 WHERE year=2020
3 AND month=5
4 AND (get_json_object(cauth_login.json, '$.user_ip')='149.154.159.36'
5 OR get_json_object(cauth_login.json, '$.user_ip')='151.236.14.67')
6 LIMIT 10|
```

⚠️ In your Query, where possible make sure to select for the Year, Month, and Day to limit the number of records checked. This will allow for better performance. You can also use LIMIT when testing a query to reduce the number of results needed for the query to complete.

HUE - Viewing Table Details

You may find this difficult as there are many similar tables in Hadoop. You can use the Table Browser to view table details to help identify the correct one to use:

1. Select Show Details for the table.
2. Go to Table Browser
3. This shows what columns are present, gives some examples of the data in the table, along with other various bits of information.

| Column (4) | Type | Description | Sample |
|------------|--------|---|---|
| json | string | { "imp_realm": null, "imp_user": null, "de.realm": null, "de.user": null, ... } | {"realm": "pass", "app": "o365", "user_ip": "111.235.89.119", "year": 2020, "month": 6, "day": 7} |
| year | int | 2020 | 2020 |
| month | int | 6 | 6 |
| day | int | 7 | 7 |

HUE - Querying JSON

If your table data is stored in a single JSON blob instead of separated columns, you cannot use the JSON items as column names without using a JSON parse string in your query.

Format:
get_json_object(<TABLE>.json, '\$.<FIELD>') = "<VALUE>"

Example:

```
Table=myTable
JSON={"valueA": 0, "valueB": "Yes", "valueC": "mayB", ....}
Desired FIELD= valueC
VALUE contains B OR VALUE = "maybe"
```

Query:
SELECT * FROM myTable
WHERE year=2020 AND month=7 AND day=7
AND get_json_object(myTable.json,'\$.valueC') LIKE "%B%"
OR get_json_object(myTable.json,'\$.valueC')="maybe"

KnowBe4 PhishER

Table of contents

- Table of contents
- Purpose
- Workflow
- Threat Category
- Clean/Spam Category
- Unknown Category
- Other Alert Types
- Closure
- Other Acknowledgements
- General Documentation

Purpose

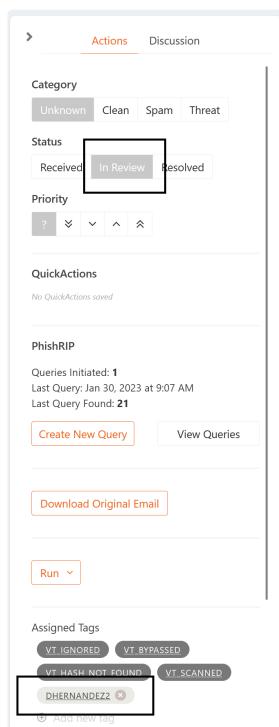
| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | 2023-03-07 by @David Hernandez |
| Escalation Contact(s) | <ul style="list-style-type: none">• @Benny Boham (Deactivated) • @David Dubois (Deactivated) |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @David Hernandez 02/21/2023 |

Workflow

Under the “Inbox” tab find oldest event without an assignee



Upon opening the alert, place it “In Review” if not done so already and add your AD-ID in the TAGs section.



Next, using all the PhishER features, use the [Phishing Playbook](#) to determine the appropriate category for this email.

If you have determined the email category is “Threat”, follow the Phishing playbook at the containment stage [Employee Phishing Incidents | EmployeePhishingIncidents Containment](#)

Remember to block IOCs, escalate phishing Campaigns, and quarantine all emails

Threat Category

1. Review any malicious URL delivery to other recipients
2. Review sender IP for other malicious deliveries
3. Review subject in question for deliveries sent to other recipients
4. Review malicious attachment hashes for deliveries in other emails
5. Run quarantine. Include the Incident ID in your soft delete
“<https://phisher.knowbe4.com/inbox/be7a284d-6363-4a8a-a676-8a5850dd9a33>”

Clean/Spam Category

Briefly review the email for any questions by the reporter or miss-classifications

Unknown Category

Follow the [Phishing Playbook](#)

Other Alert Types

Okta Alerts:

1. Users may report Okta sign-ins email notifications. When done so please review Okta logins for any anomalies or logins from non-standard locations.
2. Work with the user to make sure this was not something they unknowingly triggered.
3. Escalate if needed.

Closure

1. Apply the correct category



2. Send a closure email to the appropriate user.

Send Custom Email

GoDaddy Malicious ▾

- Report Received
- GoDaddy Malicious**
- GoDaddy Non-Malicious
- GoDaddy Spam
- Custom Email Template

Specify Recipients

| | |
|--|----------------------|
| From | From Name |
| no-reply@phisher.knowbe4.com | IsItBad |
| Reply To | Reply To Name |
| no-reply@phisher.knowbe4.com | Security@godaddy.com |
| Subject | |
| IsItBad Report - Classification: Malicious | |

Format | **I** U **S** **x_a** **x^b** **T_X** **i_≡** **i_≡** **A₊** **A₋** **[** **]** **∞** **∞** Placeholder | Source

Thank you for your most recent isitbad submission.

Email Reported:
Subject: {{subject}}

Our automation has reviewed the message submitted and determined it is **malicious**. If you forwarded the email to IsItBad@godaddy.com, please delete the original email. If you believe this classification is incorrect, please respond to this email with your concern.

Thanks again for being vigilant in reporting suspicious emails.

– Global Cyber Security Operations

Include original email at the bottom of body
 Attach original email
 Include PhishER links and tag information ⓘ

3. Write your findings and actions under the discussion tab

- Did you respond to the user?
- Did you quarantine all emails as needed?
- Did you block any IOCs?
- Were any users impacted, if so which actions did you take?

4. Finally, set the alert status to “Resolved”

> Actions Discussion

Category

Unknown Clean Spam Threat

Status

Received In Review Resolved

Other Acknowledgements

Phish Machine Learning (PML):

The Phish Machine Learning score is proprietary and thus we don't know how it truly works, but do know a few things.

- The more times an item is reported, the higher confidence score it will get.
- An item reported via the Phish Button will get a higher confidence score than an item which is forwarded.

General Documentation

Product Manual [!\[\]\(34e027debe573630395ee97bb4f591b9_img.jpg\) PhishER Product Manual](#)

OnCall Escalation Procedure Old

Table of contents

- Table of contents
- Purpose
 - GCSO Identifies a Confirmed Threat
 - During US/UK Business Hours
 - After US/UK Business Hours
 - GCSO Analyst needs assistance with an alert or request
 - During US/UK Business Hours
 - Acknowledgement From Escalation
 - GCSO shall not consider the incident escalated until IR or higher Tier acknowledges the escalation
- Escalation
 - The Analyst may escalate an alert/incident to IR for several reasons
- Expectations for IR

Purpose

| | |
|----------------------|--|
| Responsible Team | <ul style="list-style-type: none">• Detection and Monitoring• SLACK: #internal-gcso• EMAIL: GCSO@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | 09/12/2023 by @David Hernandez @Ivan Avilla |
| Requests for Updates | By Email - GCSO@godaddy.com |
| Training Log | By: @David Hernandez 09/12/2023 |

GCSO Identifies a Confirmed Threat

During US/UK Business Hours

1. Notify **@ir-team** in the **#internal-gcso** slack channel.
2. If No Response within 15m - Contact GOC to Notify On-Call

3. If No response is received from Primary On-Call, Please request GOC to notify secondary On-Call
4. If no response is received. Please request GOC to engage On-Call manager.

After US/UK Business Hours

1. Contact GOC to notify on-call.
2. If No Response within 15m - Contact GOC to Notify On-Call
3. If No response is received from Primary On-Call, Please request GOC to notify secondary On-Call
4. If no response is received. Please request GOC to engage On-Call manager.

i IR US Business Hours : 1700 - 0500 UTC for US M-F

IR UK/India Business Hours : 0500 - 1700 UTC for UK/India M-F

i Monitoring Team US/Colombia Business Hours

Monitoring Team Serbia Business Hours

GCSO Analyst needs assistance with an alert or request

During US/UK Business Hours

1. Notify **@sec_mon** and **@ir-team** in the **#internal-gcso** slack channel.
2. Communication must be clear and concise. Such as: <Teams> We need your assistance with the following alert as we can't determine XYZ
3. ONLY engage On-call if you believe this is most likely a threat.

Acknowledgement From Escalation

GCSO shall not consider the incident escalated until IR or higher Tier acknowledges the escalation

1. Expect to have IR or other teams state one of the following statements, but not limited too: "I acknowledge", "I am taking a look", "working on it", "I will be there in X minutes"
2. If you believe your escalation was not acknowledged, please request the recipient to acknowledge.

Escalation

The Analyst may escalate an alert/incident to IR for several reasons

- In the event the analyst is not able to determine a verdict, the analyst will seek peer assistance. After peer assistance has been sought with no verdict, the analyst will engage IR for assistance.
- Confirmed Activities: Ransomware, Privileged Escalation, Lateral Movement, Persistence, TA Interactive Sessions, Campaigns, Persistent TA Efforts.

When an escalation is engaged, please be prepared to answer the following

Who:

- If an employee is impacted
 - Who are they?
 - Which Department do they work in?
 - Are other employees impacted?
- If a customer is impacted
 - What is their shopper id?

What:

- What happened (include link to event and description of the event)?
- Are there other instances of malware on the server?
- If a server/workstation is impacted:
 - What is the server name?
 - What environment is it in?
 - What team owns it?
 - What purpose does the server serve?
 - Are other servers impacted
- What IOCs are available if any?

Where:

- Where in the environment did this occur? (Customer, Employee, Server)

Attention to:

- If you have already performed some analysis, please share those details as well.
- If there are details that you think are important to this alert/incident, please note them here.

Expectations for IR

1. Each IR member is responsible for being available during their On-Call period.

- a. The Incident Response team on-call schedule can be viewed at <http://x.co/oncall>
2. Per the [Time Off Requests](#) process - if time out of office overlaps with OnCall responsibilities coverage must be coordinated.
3. All IR members should have the GOC Phone Numbers whitelisted in their phone to prevent filtering calls. This includes overriding Do Not Disturb settings.
 - a. GOC On-Call Procedures can be viewed at [Incident Management On-Call Policy](#)
 - b. A list of applicable phone numbers can be viewed at [GOC/SNOW Numbers](#)

Alert Tuning Request

Process

1. Go to <https://godaddy-corp.atlassian.net/secure/CreateIssue.jspa?pid=32819&issuetype=8>
2. Provide a short summary that describes your request in the **Summary** section.
3. In the **Description** please answer the following to the best of your abilities
 - a. Why are you submitting this request?
 - b. What kind of event is it generating, Examples:
 - i. False Positive Incorrect Analytic Logic
 - ii. False Positive Inaccurate Data
 - iii. Generating too many alerts
 - iv. Alert is unclear or requires better description
4. Make sure you are listed as the **Reporter**.
5. Click **Create**
6. You will then be contacted by someone in the Detections team to complete your request.

Urgent Requests

For urgent requests please engage #security for assistance.

For GCSO members please engage @detections in dedicated collab channels.

DSR Failed Logons Review

Table of Contents

- Table of Contents
- General Information
 - Process Summary
- Process Workflow
- Process Outline and Details
 - Incident Recording Guide
 - General Outline
 - Daily Report Review
 - Daily Event Investigation.
 - Process Details
 - Event Source Dashboards & Thresholds
 - Blackholing IPs via Protect
 - Brute-force Attempts
 - Viewing Reset Actions for Passwords
 - Option 1: Using the Lockout Tool
 - Option 2: Using ADUC
 - Process FAQs
 - What is an acceptable cause?
 - What is an urgent reason for reset?
- Resources and Definitions
 - Internal Resources
 - External Resources
 - Communication Templates

General Information

 Unknown macro: 'metadata-list'

Process Summary

This process serves as a guideline for reviewing Linux and Windows failed logon events within PCI and PKI scoped environments. In addition, this process provides steps for handling of action items generated as a result of these reviews.

Process Workflow



Process Outline and Details

Incident Recording Guide

› [Click here to expand...](#)

| | |
|-------------------|---|
| Assignment Group | OPS-GCSO |
| Incident Category | Intrusion |
| Sub Category | Server |
| Title | (Based on Event Source) <ul style="list-style-type: none">• PCI Windows Logons - <USERNAME>• PCI Linux Logons - <IP>• PKI Windows Logons - <USERNAME>• PKI Linux Logons - <USERNAME> |
| Summary | Number of Failed Logons: Username(s) Affected: Source (Hostname/IP): Destination (Hostname/IP): Sample Event URL: Summary of Events: |

| | |
|-------------------------|--|
| | <p>Example</p> <p>Number of Failed Logons: 177 Username(s) Affected: pallen Source (Hostname/IP): p3plextjss001 / 184.168.130.204 Destination (Hostname/IP): p3pwjmxdc007 / 172.17.158.24 Sample Event URL: https://secstack-rproxy.cloud.dev.phx3.gdg/kibana/?#/doc/[dcr-corporate-windows-security-]YYYY.MM.DD/dcr-corporate-windows-security-2019.07.29/corporate-windows-security/?id=7_78870337416_0 Summary of Events: User pallen had 177 failed logon attempts originating from p3plextjss001 on 2019-07-28 at around 19:30 with a Logon Type 3 (Network).</p> |
| Data Type | Employee-Credential |
| Detection Method | Log Review - Kibana |

General Outline

Daily Report Review

1. Review Elastic Dashboard for each Event Source (see [Event Source Table](#))
2. Determine if any activity meets or exceeds the set thresholds.
 - a. If NO, close and note ticket
3. For each unique set of events above threshold, create a child ticket (limit 10 per event source).
 - a. Child tickets should be created using the information provided in the Incident Recording Guide.

Daily Event Investigation.

For each open child ticket you must follow next steps:

1. Verify if there is **evidence of Bruteforce** (this should only occur for PCI Linux in most cases)
 - a. If YES, was the source a GoDaddy or Internal IP Address?
 - i. If YES, **Escalate to Incident Response (Infosec_response)**
 - ii. If NO, block source IP using Protect
 - b. Verify if there are any correlated successful logons.
 - i. If YES, **Escalate to Incident Response (Infosec_response)**
 - ii. If NO, note and close the ticket.
2. Verify if there have been any recent credential rotations (within 24 hour).
 - a. If YES, set **Pending - Internal** for 24-hour review.
3. If there has been no credential change, has there been an **acceptable cause** been provided?
 - a. If YES, close ticket as resolved.
4. Verify if urgent reset is necessary.
 - a. If YES, then remediate user account, notify user and close ticket.
5. Has the user been notified?
 - a. If NO, set **Pending - Internal** for 24-hour review.
6. Has the supervisor been notified?
 - a. If NO, set **Pending - Internal** for 24-hour review.
 - b. If YES, then disable the account and notify user, and close ticket

Process Details

Event Source Dashboards & Thresholds

| Event Source / Dashboard | Thresholds | |
|--------------------------|---|--------------------------|
| PCI Windows | (100 Failed Logons OR 5 Unique Destinations) PER Username | fig. 1.1 |
| PCI Linux | (50+ Failed Logons) PER IP Address | fig. 1.2 |
| PKI Windows | (10 Failed Logons OR 5 Unique Destinations) PER Username | fig. 1.3 |
| PKI Linux | (10 Failed Logons) PER Username | fig. 1.4 |

Blackholing IPs via Protect

1. Navigate to [Protect](#) and perform a search for the IP address. If found, skip.
2. In the Protect UI select the Green "+" button and fill in the following:
 - a. Name should be the Name of the SNOW ticket you created the type of activity and the IP address being blackholed (Ex: SEC0030661_SSH_Brute_58.218.92.47)
 - b. Network should be the IP address as a /32
 - i. 58.218.92.47/32
 - c. TTL should be set for 1 day
 - d. Click Submit

Bruteforce Attempts

In general, these processes look at internal to internal logon attempts and will not include bruteforce activity. The caveat to this is the PCI Linux source which sees mostly external to internal traffic and therefore is prone to having bruteforce attempts.

When reviewing these items it is important to verify if the activity matches the expected patterns of a bruteforce attempt:

1. Bruteforce attempts often target privileged users (root, admin, administrator, etc.) but can also target individual accounts.
2. Bruteforce attempts generally have a large volume of events over a short period of time.
3. Bruteforce attempts may be from a single or multiple IP sources.

Matching these patterns does not always indicate a bruteforce has occurred, and it is up to the analyst to make this determination. Bursts of short-period failures can also result from things such as automation that has not been updated, systems with sessions that have old passwords, etc.

Viewing Reset Actions for Passwords

Option 1: Using the Lockout Tool

The LockoutStatus.exe tool is provided by [Windows](#) and allows quick access to review. A copy of this tool can also be found in the legacy SOC drive (<smb://jomax.paholdings.com/data/ITSecurity/tools/unlocker/LockoutStatus.exe>)

Option 2: Using ADUC

1. Select the proper domain:
 - a. [pki](#) for WIN PKI
 - b. [jomax.paholdings.com](#) OR [dc1.corp.gd](#) for WIN PCI
2. Right click "domain", select "find" & search for user.
3. Look in "Member Of" to see where they are members.
4. compare their member groups against the assignment/support group of the server itself
5. Review members of Assignment Group to determine if affected username is a member

Through this process you can verify if user belongs to the group to where they were trying to login, or if they did not have access to it. As well as reviewing if the user had recently changed their password.

Process FAQs

What is an acceptable cause?

Is there enough information that has been obtained in order to justify a reasonable explanation for the failed logons. i.e. Change of logon info. that synchronized after another successful logon. Or user responded, that they were having difficulties with their logon.

What is an urgent reason for reset?

Is there a reason to believe that the account needs to be reset? What is the cause for that?
i.e. An SLT/XLT member seems to have evidence of Brute-force being attempted against his account, and it only happens when he is out of the office.
Please remember to note it on the ticket.

Resources and Definitions

Internal Resources

- Team-Email Distro List(IPE Maintained): [List of Team E-mail Distros](#)
- CMDB Search – <https://x.co/cmdbsearch>

External Resources

- ADUC: <https://www.microsoft.com/en-us/download/details.aspx?id=28972>
- Abuse IP Database – <https://www.abuseipdb.com/>
- Talos Reputation Center – https://www.talosintelligence.com/reputation_center

Communication Templates

Service Logon Failures

During our daily review of logon activity we observed the username **USERNAME** failing a significant number of logon attempts against **SYSTEM**. Based on our review of available data this appears to be due to a mis-configuration local to the system. We ask that you review the configuration of services present on the server to correct this issue. Alternatively if the service or system is no longer necessary we ask that you either disable the service or work to retire the system. If you have any questions please respond to this message or reach out to us on Slack via #intrusion_prevention.

User Logon Failures

During our daily review of logon activity we observed the username **USERNAME** failing a significant number of logon attempts against **SYSTEM**. Based on our review of available data this appears to be due to a recent password change where you did not then log out and back in. In the future please log out and back in after password changes to ensure your system is not generating failed logons due to old cached credentials. If you have any questions please respond to this message.

DSR - FIM Review Procedure

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [Process Details](#)
 - [Dashboard Review](#)
 - [Process FAQs](#)
 - [How can I lookup File change history on a system or exclude noisy systems?](#)
 - [What are we monitoring?](#)
 - [I'm now sure what this file is or what it does!](#)
 - [How can you tell a system is being patched?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)

General Information

| | |
|-----------------------|---|
| Responsible Team | InfoSec Response Team Slack: #internal-gcso Email: infosec-response@secureservernet.onmicrosoft.com |
| Process Owner | @Former user (Deleted) |
| Last Review Date | 2018-12-13 |
| Escalation Contact(s) | @Former user (Deleted) @Former user (Deleted) @Former user (Deleted) |
| Requests for Updates | @Former user (Deleted) @Former user (Deleted) Slack or Email |

Process Summary

This process provides direction for the review of Trend Deep Security File Integrity monitoring events, particularly within the PCI and PKI environment to meet audit requirements and detect anomalies to prevent intrusion.

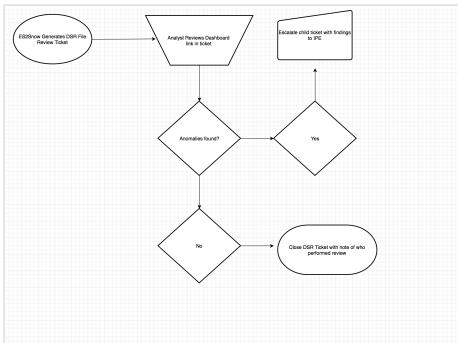
Reviewing these events require that you have basic understanding of:

1. Windows System Files
 - a. DLL or EXE Files
 - b. Windows System Directories
2. Linux System Files
 - a. Linux critical system paths
 - b. Commonly updated files
3. How to research unknown(s)
 - a. Google
 - b. VirusTotal - [Link](#)
 - c. man pages, etc

Process-Specific Definitions

- **Process-Specific:** Pertains only to this process. May have a different definition in other process flows.

Process Workflow



Process Outline and Details

Incident Recording Guide

| Incident Type wrt SIR Module | |
|------------------------------|---|
| Assignment Group | OPS-GCSO |
| Category | No Incident |
| Sub Category | None |
| Title | DSR - [PKI]/[PCI] File Changes (FIM) - #Hostname : Reason |
| Summary | Include link to sample Splunk Event |
| Priority | Low |
| Severity | Medium |
| Source | SIEM |

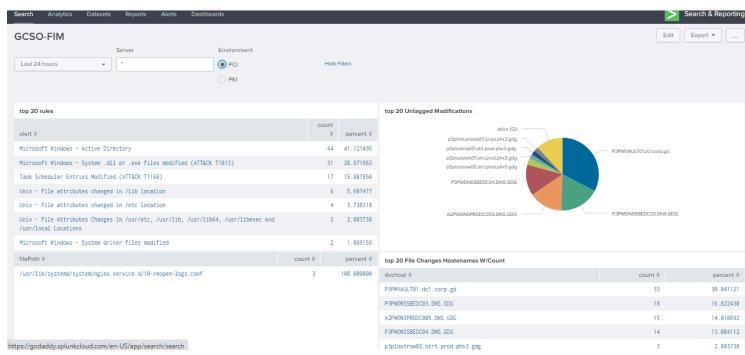
General Outline

1. 12:00AM MST DSR FIM Review Ticket Created
2. Follow dashboard review steps
3. Escalate any child tickets created

Process Details

Dashboard Review

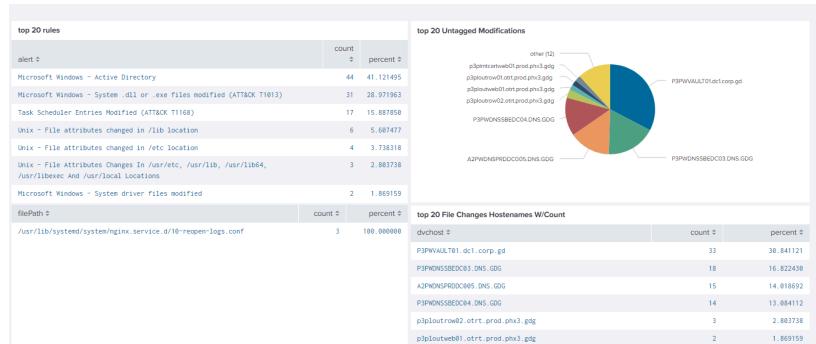
1. Review Deep Security Manager - File Integrity Dashboard: [Here](#)
2. Create child SECINC ticket if an anomaly is found.
 - a. Please provide link to example Anomaly event.
 - b. Anomalies could be:
 - i. Interesting or non-standard named files
 - ii. Unknown file hashes in critical directories (Can use VirusTotal or MalShare, etc)
 - iii. File change oddities(Odd file location or Odd modification pattern)
3. Goal of review is to review all changes for anomalies, this at times will mean you may need to exclude systems from your search.
 - a. EX: Dev Team patches 100 Servers, all with hostnames like: P3PWDEVBOX0[5-99]
 - i. We can quickly exclude these from our search in Splunk.
 - ii. We can easily determine patching by quickly seeing all the similarly named systems having similar files updated en masse
4. Child tickets should be created based on CI(s) found. If changes are found to be across multiple CI's with similar naming conventions like: P3PWDEVBOX0[5-99] , a single child ticket is acceptable



Process FAQs

How can I lookup File change history on a system or exclude noisy systems?

- Using the [Splunk Dashboard](#) which will redirect to GCSO FIM Splunk page. Need to select PCI/PKI and can view the top 20 rules and File changes based on the hostnames.
- You can look for the file changes based on the rules and the file paths.



What are we monitoring?

- TrendMicro rule names included below. These can be looked up within the Trend DSM or Encyclopedia(TBD)
 - Both OS -

1008720 - Users and Groups - Create and Delete Activity

1003533 - Application - OpenSSH

- Windows -

Customized Microsoft Windows - Active Directory for GoDaddy

1008257 - Microsoft Windows - USB Storage Device Detected

1006076 - Task Scheduler Entries Modified

1005042 - Malware - Suspicious Microsoft Windows Registry Entries Detected

1005041 - Malware - Suspicious Microsoft Windows Files Detected

1002860 - Microsoft Windows - SAM Domain Account Users Modified

1002859 - Microsoft Windows - Local Security Authority (LSA) Notification/Authentication Packages modified

1002787 - Microsoft Windows - Event Log settings changed

1002779 - Microsoft Windows - System file modified

1002778 - Microsoft Windows - System .dll or .exe files modified

1002777 - Microsoft Windows - System configuration file modified

1002774 - Microsoft Windows - Microsoft HTML Viewer dll file modified

1002773 - Microsoft Windows - 'Hosts' file modified

1002767 - Microsoft Windows - System directory attributes changed

- Linux -

1008464 - Unix - File Attributes Changes In /usr/etc, /usr/lib, /usr/lib64, /usr/libexec And /usr/local Locations

1003587 - Unix - Directory attributes changed for /bin

1003574 - Unix - File attributes changed in /sbin location

1003573 - Unix - File attributes changed in /bin location
1003514 - Unix - File attributes changed in /lib location
1003513 - Unix - File attributes changed in /etc location
1002770 - Unix - File Attributes Changes In /usr/bin And /usr/sbin Locations
1002766 - Unix - Directory attributes changed for /sbin

I'm now sure what this file is or what it does!

- Take the file name, with or without the path and dump it into your favorite search engine
 - Google
 - Bing
 - DuckDuckGo
 - etc..
- Take the file hash from the event and search in VirusTotal
 - When in doubt, copy a sample event and escalate!

How can you tell a system is being patched?

This can be determined based on context clues around the other FIM event data that we have.
Are there similar systems getting the same file updates en masse?
Are the systems similarly named?
Are the systems owned by the same team?
When in doubt, escalate a sample to IPE and follow for results.

Resources and Definitions

Internal Resources

<https://godaddy.splunkcloud.com/en-US/app/search/gcsofim>
HIPS - Deep Security Console - <https://hips.int.godaddy.com/SignIn.screen>

External Resources

Virus Total - <https://www.virustotal.com/#/home/upload>
MalShare - <https://malshare.com/>
- Look up file hash reputations or information

DSR - PCI Cloud Review Procedure

1. Table of Contents

Table of Contents

- General Information
 - Process Summary
- Process Workflow
- Process Outline and Details
 - Incident Recording Guide
 - General Outline
 - Process Details
 - Dashboard Review
 - Process FAQs

2. General Information

| | |
|------------------|---|
| Responsible Team | Global Cyber Security Operations (GCSO) |
| Process Owner | David DuBois |
| Last Review Date | 2020-02-14 |

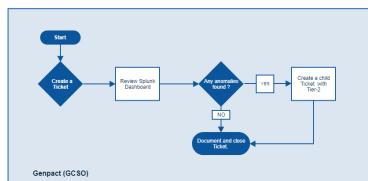
2.1. Process Summary

The below is the process needed for reviewing AWS PCI Cloud Events. This process will provide direction for the review of a PCI cloud Guard Duty, PCI Cloud Security Login & PCI Cloud FIM Review on the Elastic Dashboard.

2.2. Process Ingestions

| Event type | Event Source |
|--------------------------|--------------|
| PCI Cloud FIM | Elastic |
| PCI Cloud Security Logon | Elastic |
| PCI Guard Duty | Elastic |

3. Process Workflow



4. Process Outline and Details

4.1. Incident Recording Guide

| PCI Cloud Review Tickets | |
|--------------------------|---|
| Assignment Group | OPS-GCSO |
| Incident Category | Intrusion |
| Sub-Category | Server |
| Title | <ul style="list-style-type: none">• DSR - PCI Cloud Guard Duty Review• DSR - PCI Cloud Security Login• DSR - PCI Cloud FIM Review |
| Summary | DSR - PCI Cloud Guard Duty Review ; DSR - PCI Cloud Security Login ; DSR - PCI Cloud FIM Review ; Elastic Dashboard: https://security-prod.kibana.int.gdcorp.tools/app/dashboards#/view/54416fa0-794d-11ec-9d1e-5b56ec0d9762?_g=(filters:!(),refreshInterval:(pause:0,value:0),time:(from:now-1d%2Fd,to:now-1d%2Fd)) Process: https://confluence.godaddy.com/display/IRKB/DSR++PCI+Cloud+Review+Procedure |
| Impact / Urgency | (SEE MATRIX) |
| Detection Method | Log Review- Other |
| DSR | True |

4.2. General Outline

4.3.

Process Details

4.4. PCI FIM Review

Reviewing the FIM events, you will need to log into the [Elastic FIM Dashboard](#) for events, this defaults to the **Yesterday** view so change as needed.

1. Once logged in, review the SSH Login Panel
 - a. none = Good
2. Review that Product/Environments Panel area is reporting in the Prod Environment
3. Review the File Integrity Monitoring Events Panel
 - a. Nothing = Good
 - b. Something = escalate
 - i. /etc/motd is a false positive but a good heart beat check
 - ii. /etc/resolve is typically a false positive as cloudformation team may update DNS on systems, need to investigate
4. Export the page as a PDF (may not be needed later)
5. Create the ServiceNOW Ticket (DSR - PCI Cloud FIM Events) and attach the PDF

4.5. PCI Logon Events

1. Log on to the [PCI Compliance Review](#) dashboard
2. Select the eComm Payments and Prod environment to review logins
 - a. only one service account with a deploy role should access
 - i. 02d735y7bq14A - is the service account role attached to the payments prod account
 - b. may see a readonly role - not able to make any actions or changes in the account
 - c. master security should only be [@Brian Gosch \(Deactivated\)](#) or [@Jason Berry \(Deactivated\)](#) or [@Former user \(Deleted\)](#) accessing
 - d. may see a security read only account access at times - again a read only role
 - e. Events of the role GD-AWS-P-Global-Audit-Admin can be ignored. It is used for audit checks.

4.6. Guard Duty Events

Guard Duty monitors suspicious activity network wise notifying of suspicious activities. These logs have not yet been introduced to Elastic at this time so a manual review will have to be done inside of the account. Will need to update once inside of Elastic. DSR - PCI Cloud Guard Duty Review

1. Log into the [Guard Duty Dashboard](#)
2. Product=payments - Environment=Prod
3. If no alerts show up then close ticket out as reviewed
4. A port scan alert may show up, this account requires monthly pen testing so this alert may show up as a false positive, below is an example of the FP

Guard Duty EC2 Instance Findings

| product | environment | type | description | region | inst |
|----------|-------------|--------------------|--|-----------|---|
| payments | prod | Recon:EC2/Portscan | EC2 instance i-0faaf701b4c958959 is performing outbound port scans against remote host 10.114.6.198. | us-west-2 | arn:aws:lambda:us-west-2:123456789012:function:GD-AWS-Security-Tenable-EC2InstanceProfile |

- a.
 - i. The InstanceProfileArn of GD-AWS-Security-Tenable-EC2InstanceProfile is going to be done internally and a false positive
 - b. Anything other than listed above, reach out to [@Jason Berry \(Deactivated\)](#)

DSR - SQL Failed Login Reports

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [SQL Failed Login Reports](#)
 - [Templated Communication](#)
 - [Template](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)

General Information

| | |
|-----------------------|---|
| Responsible Team | InfoSec Response Team(IR) Slack: #internal-gcso Email: infosec-response@secureservernet.onmicrosoft.com |
| Process Owner | @Former user (Deleted) |
| Last Review Date | 2018-09-06 by @Former user (Deleted) |
| Escalation Contact(s) | @Former user (Deleted) @Logan Zahn (Deactivated) @Former user (Deleted) |
| Requests for Updates | @Former user (Deleted) infosec-response@secureservernet.onmicrosoft.com |

Process Summary

- This process provides direction for the detection, analysis and remediation of SQL Failed Logins for PCI events generated by Windows Logging and outlines the general process guidelines to be followed by Incident Response analysts. This process includes a portion dedicated to the review of a Splunk Dashboard as well as a general guideline for handling SQL Failed Login events. A summary of applicable use cases for this process are as follows:
 - Review of the SQL Failed Logins Dashboard

Process Workflow



Click to Edit

Process Outline and Details

Incident Recording Guide

| Escalation to Tier 2 | | Escalation to IR | |
|----------------------|--|-------------------|--|
| Assignment Group | TO ADD | Assignment Group | Infosec_response |
| Incident Category | Intrusion | Incident Category | Intrusion |
| Sub-Category | Server | Sub-Category | Server |
| Title | PCI SQL Failed Logons – #Hostname | Title | PCI SQL Failed Logons – #Hostname |
| Summary | Hostname: Ex. p3pwtanijummod01 Account Name: Ex. DC1\jcarter1 Account Owner: Ex. jcarter1 | Summary | Hostname: Ex. p3pwtanijummod01 Account Name: Ex. DC1\jcarter1 Account Owner: Ex. jcarter1 |
| Impact | 3 | Impact | Owner Confirmed that the activity was unknown: 2 Owner Unreachable: 3 |
| Urgency | 3 | Urgency | Owner Confirmed that the activity was unknown: 2 Owner Unreachable: 3 |
| Data Type | Other | Data Type | Other |
| Detection Method | Other | Detection Method | Other |

General Outline

SQL Failed Login Reports

LEVEL 1

1. Review Dashboard Link in Ticket
2. Review all events on [Dashboard](#)
 - a. If events found create a [Child Ticket](#) and escalate to Tier 2
 - i. Each ticket should be per Account Name failing logins
 - b. If no events found Close out main ticket

LEVEL 2

1. Lookup user account in ADUC (Active Directory Users and Computers) if it is a Service Account. If it is a user account reach out to user.
 - a. Install ADUC from External Resources (if needed)
 - b. Open ADUC
 - c. Select the proper domain:
 - i. dc1.corp.gd
 - ii. jomax.paholdings.com
 - d. Right click on domain and select find
 - e. Search for Service Account
 - f. Look in the Description and seen which group owns the account
 - i. Should look like: "Internal\Application\OPS-Security Operations\A"
 - ii. The one you would want to select is "OPS-Security Operations"
 - g. Lookup that account in Service Now using the search option and review results under "People and Places"
2. Reach out to Owning Manager of the account in Service Now via Slack and if no response in 5 minutes send follow-up email using template
3. If no response from Account Owner in 1 hour
 - a. Note that no response was received.
 - b. Escalate to **InfoSec Response** using Incident Reporting Guide above.
4. If response is received from owner and the login failure is known. Note in ticket and close
5. If response is received from owner and the login failure is unknown. Note in ticket and escalate to **InfoSec Response** using Incident Reporting Guide above.

Templated Communication

Template

Greetings **USER**, We have recently detected failed login attempts from account **ACCOUNTNAME** against the SQL Database on **FQDN**. According to our research you are listed as the current owner for this account. Is this account expected to be attempting logins to the SQL Database on **FQDN**?

Resources and Definitions

Internal Resources

Splunk: [https://security-prod.kibana.int.gdcorp.tools/app/dashboards#/view/813ce0e0-5691-11ec-9cfc-af15db683ef5?_g=\(filters:!\(\),refreshInterval:\(pause:!t,value:0\),time:\(from:now-1d%2Fd,to:now-1d%2Fd\)\)](https://security-prod.kibana.int.gdcorp.tools/app/dashboards#/view/813ce0e0-5691-11ec-9cfc-af15db683ef5?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-1d%2Fd,to:now-1d%2Fd)))

External Resources

ADUC: <https://www.microsoft.com/en-us/download/details.aspx?id=28972>

Device Environment

End user devices ([source](#)):

- Windows devices joined to Jomax Domain
- Windows devices joined to Azure\Intune
- Windows VDI instances
- Windows AWS Workspaces
- MacOS device managed by JAMF

Employee Workstation Intrusion Incidents

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [Process-Specific Definitions](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [Process Details](#)
 - [AV Incident Review > Level 2 - Step 1](#)
 - [Captured Metrics](#)
 - [Process FAQs](#)
 - [What is "Malicious"?](#)
 - [What is "Actionable"?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)

General Information

 Unknown macro: 'metadata-list'

Process Summary

This process provides direction for the detection, analysis and remediation of workstation intrusion events (such as AV events, user virus reports, etc.) and outlines the general process guidelines to be followed by Incident Response analysts. A summary of applicable use cases for this process are as follows:

- Review of Incident generated through the Daily AV Report.
- Review of suspicious/malicious events reported by end-users or detected via other means.

Process-Specific Definitions

- **Malicious:** Malicious items are or are part of a group of items specifically targeted at gaining unwanted access, visibility and/or control over a system.
- **Actionable:** Items that are actionable meet the criteria for the GESS team to be required to take action to remediate the effects of said item upon a system.

Process Workflow



Process Outline and Details

Incident Recording Guide

| AV Incident Review Tickets | |
|------------------------------------|---|
| Assignment Group | OPS-GCSO |
| Incident Category | Intrusion |
| Sub-Category | Workstation |
| Title | <ul style="list-style-type: none">• Tickets Associated with the Daily Report: ApexOne AV Report - US• Tickets Reported through Other Means: Intrusion - EndpointName |
| Description(To be update manually) | <p>— AV Summary —</p> <p>Type of Malware: [Ex. Adware Installer, Banking Trojan, Malicious Web-based Script,</p> |

| | |
|---|--|
| <p>etc.]</p> <p>Malware Type Summary: [Ex. "This type of malware generally does...." "This is (not) a(n) inherently malicious file/script."]</p> <p>Additional Details: On YYYY-MM-DD OfficeScan detected EVENT which was determined to be (not) malicious because REASON. ACTIONS TAKEN.</p> | <p>Example:</p> <p>— AV Summary —</p> <p>Type of Malware: Potentially Unwanted Application (PUA) / Yahoo! Toolbar</p> <p>Malware Type Summary: This application provides users with a browser-based toolbar that allows access to Yahoo! services.</p> <p>Additional Details: On 2018-09-04 OfficeScan detected download of a PUA known as Yahoo! Toolbar which was determined to be not malicious because this applications poses a small amount of risk, does not perform malicious actions on the system, and was intentionally installed by the user. No additional action was required.</p> |
| Priority | Low |
| Severity | Medium |
| Source | SIEM |
| DSR | <input checked="" type="checkbox"/> |

General Outline

1. If no ticket exists, create a ticket using the Incident Recording Guide.
2. Determine if activity is **Malicious** and **Actionable** and document (**warning** if the machine is a VDI do not let the user log off until after artifacts are collected):
 - a. If NOT, close ticket as **False Positive**. Document findings and reasoning for closing.
3. Using Tanium, determine potentials Indicators of Compromise and review system to determine if compromise may have occurred. Items to review include:
 - a. Was the file executed?
 - b. Were there any suspicious connections?
 - c. Were any other files created?
 - d. Were any scheduled tasks, cron jobs, or similar created?
 - e. What other processes were run associated to this file?
 - f. Are there signs of malicious user logon access? If yes, what was accessed?
4. From the prior review, can we confirm that there was compromised? If not, is there reasonable evidence an un-confirmed compromise still exists?
 - a. If NOT, then close as False Positive
5. Complete **Employee Compromise Containment**
6. Create the required re-image request.
7. Communicate to Internal IT and Users as appropriate
8. Set ticket to **Pending - Internal**.

Process Details

AV Incident Review > Level 2 - Step 1

Checking for Indicators of Compromise relies on both identifying potential identifiers based on the reputation of the file(s) in question and reviewing the activity on the machine for behavioral anomalies. Reputation information is generally found using OSINT to determine if the activity has been seen before and what types of indicators were associated with it when it was. Some common method to gather these indicators include:

- Using [VirusTotal](#), [Reverse.it](#), or other virus-analysis site to look up a particular file by Hash. (NOTE: Do not submit files to these sites).
 - Look for related files, associated network connections, and/or associated domains.
- Submit the file to our internal [ThreatAPI](#). Use resultant hash with "threatbot-test" slack app. Message the bot with "getreport <hash>" and the report will display when it has finished running.

In addition to this, we need to be aware of file activity that has occurred on the machine that may indicate that malicious activity has or is occurring. Generally this will be obtained by reviewing the file activity in [Tanium](#) to search activity associated to or occurring around when the file was seen executed on the machine. Some things to look for are:

- Network connections to suspicious IP space.
- Suspicious DNS queries.
- Suspicious files created or modified.
- Suspicious processes started or touched.

The primary method of reviewing logon activity is via our SSO provider, [Okta](#). Common items to look for are:

- Logons from high-risk regions (Africa, China, Russia) that are not in-line with normal user activity.
- Logons outside of a reasonable geolocation as would be expected by their primary work location.
- Logons outside of normal times.
- Increased numbers of failed logon attempts.

Captured Metrics

Most fields associated to metrics will be required by default in order to close the ticket. Below is a brief summary of metrics specific to this process which should be captured:

- **Intrusion Metrics** - Found under the Intrusion Tab on *Intrusion - Workstation* tickets.
 - **Malware Delivery:** Identifies how the malicious file(s) was delivered to the target machine.
 - **Malware Family:** Identifies if malicious file(s) are of a known family. Leave blank if unknown.

- **Malware Type:** Identified general subtypes of malicious files.
- **Root Cause:** Identifies the exploitation that occurred to allow the file(s) to be present on the machine.
- **Workstation Type:** Identifies the general subcategory of workstation impacted by the incident.

Process FAQs

What is "Malicious"?

In many cases the difference between malicious and non-malicious activity is the intention behind said activity. Threat Actors tend to utilize the same functions and tools as valid users, and it is the responsibility of the analyst to differentiate between these when reviewing an event. Malicious activity will generally present with one or more of the following:

- Attempts to modify the system in a way to capture sensitive information.
- Attempts to hide itself from the user either by:
 - Subverting system protections (AV, UAC, Authentication, etc.)
 - Attempts to masquerade as other benign file (system files, other software, etc.)
- Attempts to gain persistence to prevent removal of software.
- Attempts to communicate with a C2 or similar.

What is "Actionable"?

There are often cases where reported activity could be classified as malicious under some circumstances but not in others. It is up to the analyst to determine if an event requires further action, and is therefore "Actionable". In general, Actionable activity will meet the following criteria:

- Falls outside the scope of accepted use of a user workstation.
- Represents a reasonable risk to a workstation. Some items that are **NOT** a risk include:
 - PUA/Adware installations that are not likely to include malicious functions (Toolbars, Ad-Supported Apps, etc.)
 - Files that cannot natively run on a workstation (ex. EXE on Mac/Linux systems; PHP files on Windows; etc.)
 - Intentional activities related to investigations or testing (generally refers to alerts on IT Security workstations)
 - Attempts by the user/threat were successfully mitigated by existing security controls (Antivirus, Web-based Filtering, etc.)

Resources and Definitions

Internal Resources

- Threat Slack Bot - threatbot-test
- Tanium - <https://tanium.int.godaddy.com/>
- OfficeScan Console - (Via Okta - Trend Micro Control Manager: US)

External Resources

- VirusTotal - <https://www.virustotal.com/>
- Reverse.it - <https://www.reverse.it/>
- UrlQuery - <https://urlquery.net/>
- Trend Threat Encyclopedia - <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/>

IDS Alerts Procedure

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [General Outline](#)
 - [Daily Event Investigation.](#)
 - [Process Details](#)
 - [Blackholing IPs via Protect](#)
 - [Internal Resources](#)

General Information

IDS alerts for PCI/PKI are reviewed in [GCSO-IDS - Elastic \(gdcorp.tools\)](#). When investigating an alert, analysts will need to determine if the alert is a false positive or not to determine if the alert needs to be tuned or disabled.

| | |
|-----------------------|--|
| Responsible Team | Response Team Slack: #gcsco_team |
| Process Owner | Anthony Crisostomo |
| Escalation Contact(s) | @Former user (Deleted) @Juan Bustamante @David Downs |

Process Summary

This process serves as a guideline for reviewing the IDS alerts within PCI and PKI scoped environments. In addition, this process provides steps for handling of action items generated as a result of these reviews.

General Outline

1. Review alerts in [GCSO-IDS - Elastic \(gdcorp.tools\)](#) for top 10 IPs in the last 24hrs.
2. Determine if any activity legitimate or false positive.
 - a. If YES, close and note ticket
3. For each unique set of events for the GoDaddy IPs that can be actioned on create a child ticket.

Daily Event Investigation.

For each open child ticket you must follow next steps:

1. Verifying Bruteforce alerts
 - a. If YES, was the source a GoDaddy or Internal IP Address?
 - i. If YES, determine if IP is customer related or not
 - ii. If customer related hand-off to DCU for further investigation (pending step)
 - iii. If NO, escalate to Tier 2
 - iv. If External IP Address, Blackhole for 24hrs in Protect.
2. Verifying other rules
 - a. Majority of the rules are related to Bruteforce activity. Rules that seem unfamiliar need to be escalated to Tier 2 or Netdef for review for tuning or to be disabled.

Process Details

Blackholing IPs via Protect

1. Navigate to [Protect](#) and perform a search for the IP address. If found, skip.
2. In the Protect UI select the Green "+" button and fill in the following:
 - a. Name should be the Name of the SNOW ticket you created the type of activity and the IP address being blackholed (Ex:)
 - i. SIR<number>_SSH_Brute_IPAddress
 - b. Network should be the IP address as a /32
 - i. IPAddress/32

- c. TTL should be set for 24hrs.
- d. Click Submit

Internal Resources

<https://protect.int.godaddy.com/blackholes>

Windows Log Clear Event Procedure

- What
- Where
- How
- False Positives

What

Windows Log Clear is an alert that watches for [EventID:1102](#) which is the clearing of the Windows audit log (Security). We care about this because this is a technique used by attackers in an attempt to hide their activities and has historically been a very good indicator of compromise.

Where

SNOW tickets are generated within the SEC space from log data within our Elastic. The SNOW ticket will contain a link to a Elastic dashboard with the log clear event(s).

Sample ticket details:

```
Dashboard - Windows Event 1102 Log Clear: https://security-prod.kibana.int.gdcorp.tools/app/dashboards#/view/868c0a70-bd9a-11eb-8d62-f725f3c7ec37
Process - https://godaddy-corp.atlassian.net/wiki/display/IRK8/Windows+Log+Clear+Procedure
Threshold - None
```

How

Reviewing the alerts is pretty straight forward:

- Review [Elastic dashboard](#) to determine target systems.
- Inspect event to determine if part of known automation which causes false positives
 - If false positive appears to be a new type of false-positive, create a new JIRA spike story to determine best method to tune this new false-positive type. Add the JIRA story number to the security incident ticket.
- If not a known false positive, investigate it, update the existing incident and escalate to IR if required.

False Positives

There is currently one known scenario which will create false positives. The #inf-mgt-auth-support team (formerly #compute) have automation which creates a nightly build of a Windows Openstack image. The end of this build process clears all logs on the system prior to saving the image. All of these alerts will have a similar naming scheme for the system and will ultimately be sourced from p3plcldimg00[1-2].

To confirm if false positive:

- Review event data in Elastic dashboard

| Windows Log Clear Events | | | | | | | | | |
|--------------------------|---------|-------------|---------|------------|-------------|--------|---------|----------|-------|
| EventId | Summary | MachineName | LogName | SecurityID | AccountName | Domain | LogonID | Keywords | _time |
| No Results to display | | | | | | | | | |

- Check hostname (system.Computer) to see if it starts with **WINDOWS-**, if so it is likely part of automation.
- Take the hostname from Elastic, search it in Tanium to confirm it's source IP
 - Tanium → Administration → System Status → Search hostname → Set check in time to last 1 day

| | Host Name | Network Location (from client) | Network Location (from server) |
|-------------------------------------|-----------------|--------------------------------|--------------------------------|
| <input checked="" type="checkbox"/> | windows-ijbmuvb | 192.168.122.165 | 10.22.240.127 |

- Get hostname associated with IP (Network Location)

```
$ host 10.22.240.127
127.240.22.10.in-addr.arpa domain name pointer p3plcldimg001.prod.phx3.gdg.
```

- If associated with p3plcldimg00[1-2], close ticket as false positive.
- It's possible that the hostname will not appear in Tanium. In that case as long as the hostname matches the pattern WINDOWS-[A-Z0-9]{7} (and does not exist in CMDB, does not have any AV alerts) it is safe to consider the alert a False Positive

User Altered the Windows System Clock

- [What](#)
- [Where](#)
- [How](#)

What

User Altered the Windows System Clock is an alert that watches for [EventID:4616](#). This event indicates the old and new system time as well as who did it as specified in the Subject: section. Process information shows the program that was used to change the time. We care about this because this is a technique used by attackers in an attempt to hide their activities and has historically been a very good indicator of compromise.

Where

SNOW tickets are generated within the SEC space from log data within our Elastic. The SNOW ticket will contain a link to the Elastic Alert along with time stamps to review.

Sample ticket details:

```
A Windows system had its time changed by a user.

@timestamp: 2022-07-14T22:13:29.996Z
EventCode: 4616
SubjectUserName: cfields
Hostname: cpdcw1656625421.dc1.corp.gd

@timestamp: 2022-07-14T22:13:29.998Z
EventCode: 4616
SubjectUserName: cfields
Hostname: cpdcw1656625421.dc1.corp.gd

@timestamp: 2022-07-14T20:12:41.999Z
EventCode: 4616
SubjectUserName: cfields
Hostname: cpdcw1656625421.dc1.corp.gd

@timestamp: 2022-07-14T20:12:41.999Z
EventCode: 4616
SubjectUserName: cfields
Hostname: cpdcw1656625421.dc1.corp.gd

Link to results: https://security-prod.kibana.int.gdcorp.tools/app/security/detections/rules/id/f67b0f30-3828-11ec-bf42-87570b8f4ed7?timerange=(global:(15m))
```

How

Reviewing the alerts is pretty straight forward:

- Review the ticket to determine target systems and user who initiated the time change.
- Look in Service Now to see if there is a CO (Change Order) for the server in question.
 - If no CO is present reach out to the user and to confirm they made the change, if yes ask them for a CO for the work they have preformed on the server.
 - Example of a Change Order

The screenshot shows a Service Now Change ticket interface. The ticket number is CHG0680915. The fields visible include:

- Risk: 3 - Low
- Impact: 3 - Low
- Assignment Group: DEV-CRM
- Assigned To: Clinton Fields
- Location: (empty)
- Number: CHG0680915
- Approval: Approved
- State: Closed Complete
- Type: Manual
- Category: Other
- Sub-Category: - None -
- Brand: GoDaddy
- Title: Change server time for testing
- Description: The time on the server cpdcw1656625421 will be updated to an incorrect time for testing purposes. It will then be updated back to the correct time.

A tooltip is displayed over the Type field, providing a detailed explanation of the three types of changes:

- Manual - These changes are those that do not move through a CI/CD pipeline. They require approvals and planning documentation.
- Automated - Automated changes require a CI/CD pipeline and can only be created through the API.
- Emergency - Emergency changes are for documenting fixes after they have been applied while resolving an incident.

- If you can confirm that the user did do this activity from the user, notate the ticket with the notes from the user and where possible the Change Order it self.
- If not a known false positive, investigate it, update the existing incident and escalate to IR if required.

System Activity Investigations

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
 - [Process Ingestion](#)
 - [Process-Specific Definitions](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [General Outline](#)
 - [Process Details](#)
 - [Checking for Indicators of Compromise \(IOCs\)](#)
 - [Process FAQs](#)
 - [What is "Malicious"?](#)
 - [What is "Actionable"?](#)
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)

General Information

| | |
|------------------------------|---------------------------------------|
| Responsible Team | OPS-GCSO |
| Process Owner | @David Dubois (Deactivated) |
| Last Updated | 2023-03-22 |
| Escalation Contact(s) | Incident Response (@ir-team in Slack) |

Process Summary

This process provides direction for the analysis and remediation of suspicious/malicious detections across our workstation and server environments and outlines the general process guidelines to be followed by Incident Response analysts. A summary of applicable use cases for this process are as follows:

- Detections of potentially malicious files on workstations or servers. Some examples of these detections are:
 - Antivirus Events
 - Network Activity Events
 - Behavioral or Advanced Detections (SIEM)
- Reports of suspicious processes on workstations or servers.
 - Reports of odd activity on a machine with clear indications of associated processes or files.

Process Ingestion

| Event type | Event Source |
|------------|--------------|
|------------|--------------|

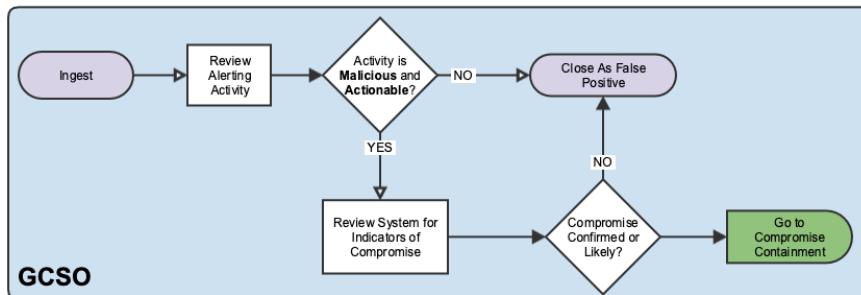
| | |
|----------------|-----------------------------|
| Workstation AV | SentinelOne |
| Server AV | Deep Security / SentinelOne |

Process-Specific Definitions

- **Malicious:** Malicious items are or are part of a group of items specifically targeted at gaining unwanted access, visibility and/or control over a system.
- **Actionable:** Items that are actionable meet the criteria for the GESS team to be required to take action to remediate the effects of said item upon a system.

Process Workflow

System Investigations



Process Outline and Details

Incident Recording Guide

▼ Click here to expand...

| | |
|-------------|--|
| Description | <p>Type of Malware: [Ex. Adware Installer, Banking Trojan, Malicious Web-based Script, etc.]</p> <p>Malware Type Summary: [Ex. “This type of malware generally does....” “This is (not) a(n) inherently malicious file/script.”]</p> <p>Additional Details: On YYYY-MM-DD OfficeScan detected EVENT which was determined to be (not) malicious because REASON.</p> <p>ACTIONS TAKEN.</p> <p>Example:</p> |
|-------------|--|

Type of Malware: Potentially Unwanted Application (PUA) /

Yahoo! Toolbar

Malware Type Summary: This application provides users with a browser-based toolbar that allows access to Yahoo! services.

Additional Details: On 2018-09-04 OfficeScan detected download of a PUA known as Yahoo! Toolbar which was determined to be not malicious because this applications poses a small amount of risk, does not perform malicious actions on the system, and was intentionally installed by the user. No additional action was required.

General Outline

1. Determine if activity is **Malicious** and **Actionable** and document:
 - a. If NOT, close ticket as **False Positive**. Document findings and reasoning for closing using Description template in the Incident Recording Guide.
2. Determine potentials Indicators of Compromise and review system to determine if compromise may have occurred. Items to review include:
 - a. Was the file executed?
 - b. Were there any suspicious connections?
 - c. Were any other files created?
 - d. Were any scheduled tasks, cron jobs, or similar created?
 - e. What other processes were run associated to this file?
 - f. Are there signs of malicious user logon access? If yes, what was accessed?
3. From the prior review, can we determine if a compromise of the system has occurred? If not, is there reasonable evidence an un-confirmed compromise still exists?
 - a. If NOT, then close as False Positive
 - b. If YES, escalate to InfoSec Response.

Process Details

Checking for Indicators of Compromise (IOCs)

Checking for Indicators of Compromise relies on both identifying potential identifiers based on the reputation of the file(s) in question and reviewing the activity on the machine for behavioral anomalies. Reputation information is generally found using OSINT to determine if the activity has been seen before and what types of indicators were associated with it when it was. Some common method to gather these indicators include:

- Using [VirusTotal](#), [Reverse.it](#), or other virus-analysis site to look up a particular file by Hash. (NOTE: Do not submit files to these sites).
 - Look for related files, associated network connections, and/or associated domains.
- Submit files to [JoeSandbox](#)

In addition to this, we need to be aware of file activity that has occurred on the machine that may indicate that malicious activity has or is occurring. Generally this will be obtained by reviewing the file activity in [Tanium](#) to search activity associated to or

occurring around when the file was seen executed on the machine. Some things to look for are:

- Network connections to suspicious IP space.
- Suspicious DNS queries.
- Suspicious files created or modified.
- Suspicious processes started or touched.

Review [Okta Logs](#) for suspicious activity. Common items to look for are:

- Logons from high-risk regions (Africa, China, Russia) that are not in-line with normal user activity.
- Logons outside of a reasonable geolocation as would be expected by their primary work location.
- Logons outside of normal times.
- Increased numbers of failed logon attempts.

Process FAQs

What is "Malicious"?

In many cases the difference between malicious and non-malicious activity is the intention behind said activity. Threat Actors tend to utilize the same functions and tools as valid users, and it is the responsibility of the analyst to differentiate between these when reviewing an event. Malicious activity will generally present with one or more of the following:

- Attempts to modify the system in a way to capture sensitive information.
- Attempts to hide itself from the user either by:
 - Subverting system protections (AV, UAC, Authentication, etc.)
 - Attempts to masquerade as other benign file (system files, other software, etc.)
- Attempts to gain persistence to prevent removal of software.
- Attempts to communicate with a C2 or similar.
- Attempt to escalate permissions to root or administrative levels.

What is "Actionable"?

There are often cases where reported activity could be classified as malicious under some circumstances but not in others. It is up to the analyst to determine if an event requires further action, and is therefore "Actionable". In general, Actionable activity will meet the following criteria:

- Falls outside the scope of accepted use of the system in question:
 - Activity represents a significant risk.
 - Activity appears to be utilizing the system in a way not related to work tasks.
- Represents a reasonable risk to the affected system. Some items that are **NOT** a risk include:
 - Internal Servers
 - Activities known to be carried out by administrators as part of troubleshooting or maintenance (Uncommon Executables; Powershell; etc.)
 - Hosting Servers
 - Files stored in customer-level directories which do not have the capability to escalation permissions (Webshells; BlackhatSEO; Malicious Javascript; etc.)
 - Files that cannot natively run on the affected server (ex. EXE on Mac/Linux systems; ELF files on Windows; etc.)
 - Actions initiated and followed by IUSR's.
 - Workstations
 - PUA/Adware installations that are not likely to include malicious functions (Toolbars, Ad-Supported Apps, etc.)
 - Files that cannot natively run on a workstation (ex. EXE on Mac/Linux systems; PHP files on Windows; etc.)

- Intentional activities related to investigations or testing (generally refers to alerts on IT Security workstations)
- Attempts by the user/threat were successfully mitigated by existing security controls (Antivirus, Web-based Filtering, etc.)

Resources and Definitions

Internal Resources

- Threat Slack Bot - [threatbot test](#)
- Tanium - <https://tanium.int.godaddy.com/>
- OfficeScan Console - (Via Okta - Trend Micro Control Manager: US)
- SentinelOne Console - <https://usea1-godaddy.sentinelone.net/>

External Resources

- VirusTotal - <https://www.virustotal.com/>
- Reverse.it - <https://www.reverse.it/>
- UrlQuery - <https://urlquery.net/>
- Trend Threat Encyclopedia - <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/>

Endpoint Intrusion Incidents v2 Draft

1. Table of Contents

- 1. Table of Contents
- 2. General Information
 - 2.1. Process Summary
 - 2.2. Definitions
- 3. Process Workflow
- 4. Process Outline and Details
 - 4.1. Incident Recording Guide
 - 4.2. General Outline
- 5. Identification
 - 5.1. Identification
 - 5.2. Identification Part 2: IOC Discovery and Expanding Scope
- 6. Containment
 - 6.1. Containment
- 7. Eradication
 - 7.1. Eradication
- 8. Recovery
 - 8.1. Recovery
- 9. Lessons learned
 - 9.1. Lessons learned
 - 9.2. ~~Captured Metrics~~-(Discuss with threat team)
- 10. Process FAQs
 - 10.1. Process FAQs
 - 10.1.1. What is "Malicious"?
 - 10.1.2. What is "Actionable"?
- 11. Resources and Definitions
 - 11.1. Internal Resources
 - 11.2. External Resources

2. General Information

2.1. Process Summary

This process provides direction for the detection, analysis and remediation of an endpoint intrusion event (such as AV/EDR events, user virus reports, etc.) and outlines the general process guidelines to be followed by Incident Response analyst. The process closely aligns with the PICERL Framework. A summary of applicable use cases for this process are as follows:

- Review of Incident generated through the Daily AV Report.
- Review of suspicious/malicious events reported by end-users or detected via other means.
- Alerts reported in the SIEM

2.2. Definitions

- **Malicious:** Malicious items are or are part of a group of items specifically targeted at gaining unwanted access, visibility and/or control over a system.
- **Actionable:** Items that are actionable meet the criteria for the security teams to take action and remediate the effects of said item upon a system.
- **Incident Handler (IH):** Leader and guide for the technical investigation of an ongoing incident.

3. Process Workflow

Workflows pending upon Q/A

4. Process Outline and Details

4.1. Incident Recording Guide

| AV Incident Review Tickets | |
|--|---|
| Assignment Group | OPS-GCSO |
| Incident Category | Malware |
| Sub-Category | N/A |
| Title | <ul style="list-style-type: none"> Tickets Associated with the Daily Report: ApexOne AV Report - US Tickets Reported through Other Means: Intrusion - <Endpoint Name> |
| Description (To be update manually) | <p>— AV Summary — Type of Malware: [Ex. Adware Installer, Banking Trojan, Malicious Web-based Script, Suspicious Process etc.] Additional Details: On YYYY-MM-DD OfficeScan detected EVENT which was determined to be (not) malicious because REASON. ACTIONS TAKEN.</p> <div style="border: 1px solid black; padding: 5px;"> <p>Example:</p> <p>— AV Summary — Type of Malware: Potentially Unwanted Application (PUA) / Yahoo! Toolbar Additional Details: On 2018-09-04 OfficeScan detected download of a PUA known as Yahoo! Toolbar which was determined to be not malicious because this application poses a small amount of risk, does not perform malicious actions on the system, and was intentionally installed by the user. No additional action was required.</p> </div> |
| Priority | Low |
| Severity | Low |
| Source | SIEM |
| DSR | ✓ |

4.2. General Outline

- If no ticket exists, create a ticket using the Incident Recording Guide.
- Identification: Can we confirm that there is/was a compromise?
 - If NOT, then close as False Positive
- Contain: Isolate the intrusion
- Eradicate: Reimage, Patch, Restore-From-Backup
- Recovery: Validate and return to BAU
- Lessons Learned: Retro and Procedure changes
- Captured Metrics

5. Identification

? Unknown Attachment

5.1. Identification

Identification will be the most time consuming task. Understand that you can't rush things and do your best to keep stress levels low. Reach out to your peers for assistance if needed.

Whether it's a user reported incident or alert, we need to validate the compromise and collect all possible IOCs.

Review the following for any malicious/suspicious activity:

- Abnormal process execution
- Network connections to suspicious IP space from non-standard apps
- Suspicious DNS queries.
- Suspicious files created or modified.
- Suspicious processes started or manipulated.
- Suspicious Scheduled tasks, registry entries (Windows), Plists (macOS), Cron jobs (UNIX)

- Local users created
- Privilege escalation
- Firewall modification ie, open ports

If there is any findings of the items above, review user login activity of users who have logged in during the expected time of compromise.

- Compare historical logins with present ones.
 - Are logins using different or abnormal user agents? (Normal: Chrome/Safari/Firefox)
 - Are logins from a VPS or Cloud Provider?
 - Are present logins from an a geolocation? ----- (SRA blacklisted location) (consider VPN gateway locations)
 - constructive location logins

If you are unable to validate malicious activity by completing the items above, use the following tools to reduce your risk gap. Some common method to compare and validate IOCs include:

- Submit your IOCs to our internal [Threat UI tool](#).
- Google: It is likely that someone else on the internet has already found the malware name or hash. Use google dork commands to identify write-ups or anything else relating to the suspected compromise.
- Using [Joe's Sandbox](#), or other virus-analysis site to look up a particular file by Hash. (**NOTE:** Do not submit files to these sites).
 - Look for related files, associated network connections, and/or associated domains

Malware Type Identification

To assist in containment, try to find an analysis report on the malware type you are working with. Use what you find as a reference and not an absolute guide.

5.2. Identification Part 2: IOC Discovery and Expanding Scope

Using all collected IOCs, search for all relevant IOCs within the company using all security resources.

Perform the following actions that are relevant to you incident:

- Search for domains
- Search for IPs
- Search Hashes
- Search files names (Purpose is to find different hashes with the same name)
- Search for registry keys in Tanium and Defender or other EDR/Asset-Discovery tools

If there are any hits on other endpoints repeat this cycle at the Identification step.

6. Containment

6.1. Containment

1. Take a snapshot of the impacted device using capable security tools. (deep data collection)
2. If possible isolate the device. **Criteria?**
3. Based on your findings determine if credential mitigation should be performed before or after eradication.
4. Block IPs/Domains

7. Eradication

Unknown Attachment

7.1. Eradication

During the Eradication phase you will identify root cause and remove all traces of malware.

- If isolation was not possible, it is imperative that the incident responder eliminates all trace of malware as soon as possible.
- Eradicate malware in the following order
 - a. Capture and kill all malicious services
 - b. Capture and eliminate persistence artifacts ie: registry keys, scheduled tasks, cron jobs, plists etc
 - c. Capture and eliminate all malware artifacts. Examples include but not limited to: exe's, carrier files, payloads, other created files.
 - d. Capture and remove recently created accounts
 - e. Capture, review, and restore modified files
- Regardless of the malware type/scope, perform a [credential mitigation](#) for all users who have logged into the endpoint with-in the suspected compromise

time.

8. Recovery

8.1. Recovery

Your goal is to return to business as usual (BAU)

- Re-image or restore-from-backup.
- Restore services back to BAU.
- Test mitigations and/or patches are in place?
- The incident responder is confident in the endpoint status?

9. Lessons learned

9.1. Lessons learned

The following should be answered during an Incident Retro if one is held, if not, make note of the questions below and escalate to the appropriate teams if needed.

- Are there new siem rules that we should create?
- Are there additional security measures that should be implemented?

9.2. Captured Metrics-(Discuss with threat team)

Most fields associated to metrics will be required by default in order to close the ticket. Below is a brief summary of metrics specific to this process which should be captured:

- **Intrusion Metrics** - Found under the Intrusion Tab on *Intrusion - Workstation* tickets.
 - **Malware Delivery:** Identifies how the malicious file(s) was delivered to the target machine.
 - **Malware Family:** Identifies if malicious file(s) are of a known family. Leave blank if unknown.
 - **Malware Type:** Identified general subtypes of malicious files.
 - **Root Cause:** Identifies the exploitation that occurred to allow the file(s) to be present on the machine.
- **Workstation Type:** Identifies the general subcategory of workstation impacted by the incident.

10. Process FAQs

10.1. Process FAQs

10.1.1. What is "Malicious"?

In many cases the difference between malicious and non-malicious activity is the intention behind said activity. Threat Actors tend to utilize the same functions and tools as valid users, and it is the responsibility of the analyst to differentiate between these when reviewing an event. Malicious activity will generally present with one or more of the following:

- Attempts to modify the system in a way to steal or manipulate sensitive information.
- Attempts to hide itself from the user either by:
 - Subverting system protections (AV, UAC, Authentication, etc.)
 - Attempts to masquerade as other benign file (system files, other software, etc.)
- Attempts to gain persistence
- Attempts to prevent removal of software.
- Attempts to communicate with a C2 or similar.
- Attempts to delete or encrypt data
- Attempts to execute code from no standard locations
- Attempts to evade or bypass security controls

10.1.2. What is "Actionable"?

There are often cases where reported activity could be classified as malicious under some circumstances but not in others. It is up to the analyst to determine if an event requires further action, and is therefore "Actionable". In general, Actionable activity will meet the following criteria:

- Falls outside the scope of accepted use of a user workstation.

- Represents a reasonable risk to a workstation. Some items that are **NOT** a risk include:
 - PUA/Adware installations that are not likely to include malicious functions (Toolbars, Ad-Supported Apps, etc.) To monitored
 - Files that cannot natively run on a workstation (ex. EXE on Mac/Linux systems; PHP files on Windows; etc.)—Should still be remediated and reviewed for IOC.
 - Intentional activities related to investigations or testing (generally refers to alerts on IT Security workstations)—Activities should still be validated, and ensure accidental detonation is not triggered.
 - Attempts by the user/threat were successfully mitigated by existing security controls (Antivirus, Web-based Filtering, etc.)—Ensure carrier file was remediated and not just payload.

11. Resources and Definitions

11.1. Internal Resources

- Tanium - <https://tanium.int.godaddy.com/>
- Defender - security.microsoft.com
- Threat UI - <https://ui.threat.int.gdcorp.tools/>

11.2. External Resources

- VirusTotal - <https://www.virustotal.com/>
- Joe's Sandbox - <https://joxim.org/joesandbox/>
- UrlQuery - <https://urlquery.net/>
- Trend Threat Encyclopedia - <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/>
- PICERL - <https://www.sans.org/media/score/504-incident-response-cycle.pdf>

Event Comments Standard

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Purpose](#)
- [Comments Standard](#)
- [Comments might contain the following](#)
 - [Who:](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: GCSO@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | 2023-12-14 by @David Hernandez @Darko Zecic |
| Escalation Contact(s) | |
| Requests for Updates | By Email - GCSO@godaddy.com |
| Training Log | By: @David Hernandez 12/14/2023 |

Purpose

Coming Soon

Comments Standard

Comments must contain

- Reason for chosen disposition

- Actions that were taken
- Hypotheses
- Recommended steps/actions

Comments might contain the following

Who:

- If an employee is impacted
 - Who are they?
 - Which Department do they work in?
 - Are other employees impacted?
- If a customer is impacted
 - What is their shopper id?

What:

- What happened (include link to event and description of the event)?
- Are there other instances of malware on the server?
- If a server/workstation is impacted:
 - What is the server name?
 - What environment is it in?
 - What team owns it?
 - What purpose does the server serve?
 - Are other servers impacted
- What IOCs are available if any?

Where:

- Where in the environment did this occur? (Customer, Employee, Server)

Attention to:

- If you have already performed some analysis, please share those details as well.
- If there are details that you think are important to this alert/incident, please note them here.

Quarterly Control Audit (WIP)

Table of Contents

- Quick Links
- Submitting Control Evidence
 - Evidence Formats
 - Evidence Submissions
- Submitting Control Samples
 - Sample Formats
 - Sample Collection Process
- IR/GCSO Audit Items
- ServiceNow (SIR) Configuration
- ServiceNow Report Configuration

Quick Links

All Controls Owned by IR/GCSO

- ServiceNow Controls

Audit SNOW Reports

- CyberSec Ops Dashboard > Audit
 - CTRL0024286 - PCI Daily Security Alert/Log Review
 - CTRL0026472 - PCI IDS Events
 - CTRL0026474 - HIPS Control Review

TechRisk Audit Requests

- CTRL0024286 Requests
- CTRL0026472 Requests
- CTRL0026474 Requests

IR Control Evidence Sharepoint

- Documents > Audits > CtrlEvidence

Submitting Control Evidence

Each submission of evidence for a Control will need to be collected from ServiceNow and then attached to the Sharepoint request page.

Evidence Formats

› Screenshots

- Should include the System Time/Date
 - Windows: Lower-left corner of the screen (Startbar must be displayed)
 - Mac: Upper-right corner of the screen (needs to be turned on in the Menubar)

› List Exports

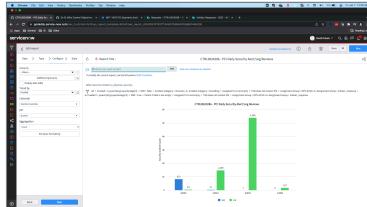
- Should be exported in CSV Format
- Included fields:
 - SIR
 - Control Objective
 - Task
 - Task.Title
 - Task.Assignment Group
 - Task.Assigned To
 - Task.State
 - SEC
 - TBD

Evidence Collection Process

The process for collecting the Control evidence is as follows:

1. Open the report associated with the Control in question.
 - a. CTRL0024286 - PCI Daily Security Alert/Log Review
 - b. CTRL0026472 - PCI IDS Events
 - c. CTRL0026474 - HIPS Control Review
2. **Screenshot** the report view.

a. Save it as QuarterYear_SNOWReport_CTRL (example: Q42021_SNOWReport_CTRL0024286.png).

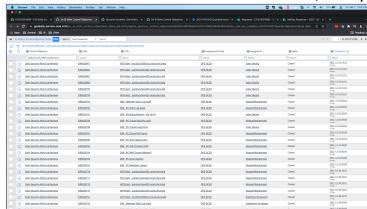


3. Click on the graph bar for the Quarter in question (generally previous). This will load a list-view of the associated tickets.

a. If multiple datasets existing (SEC & SIR) you will need to click both.

4. **Screenshot** the list view(s) of the ServiceNow tickets.

a. Save it as QuarterYear_Table_List_CTRL (example: Q42021_SIR_List_CTRL0024286.png).



5. At the top of the list view, click the menu button for any of the columns (≡), and select **Export > CSV**.

a. Save the CSV as QuarterYear_Table_Export_CTRL (example: Q42021_SIR_Export_CTRL0024286)

Once done, should have:

- 2-3 screenshots
- 1-2 exported CSVs

Evidence Submissions

Once the evidence is collected, it needs to be uploaded to the appropriate Request in the TechRisk Sharepoint:

1. Compress all of the collected evidence into a ZIP file named QuarterYear_CTRL (example: Q42021_CTRL0024286.zip)

2. Open the evidence request in the TechRisk Sharepoint:

- a. [CTRL0024286 Requests](#)
- b. [CTRL0026472 Requests](#)
- c. [CTRL0026474 Requests](#)

3. Locate the request for the collection period (usually the one in Status "Not Started").

4. Attach the created ZIP file to the open request, and set the Status to "Checked In".

5. Also save a copy to the [IR CtrlEvidence](#) folder in the IR Sharepoint for backup and reference.

Submitting Control Samples

Sample Formats

› [PDF Exports](#)

- (COMING SOON)

Sample Collection Process

(COMING SOON)

IR/GCSO Audit Items

The GCSO/IR teams currently own 3 controls which are tracked by the Tech Risk team.

| Control ID | Control Objective | Description | SNOW Control Ticket | SNOW Control Report |
|-----------------------------|----------------------------------|---|-----------------------------|---|
| CTRL0024286 | Daily Security Alert/Log Reviews | <p>The following critical security alerts and related logs are reviewed on at least a daily basis. Evidence of reviews is tracked within ServiceNow tickets.</p> <ul style="list-style-type: none"> • All individual user accesses to cardholder data • All actions taken by any individual with root or administrative privileges • Access to all audit trails • Invalid logical access attempts • Use of and changes to identification and authentication mechanisms including but not limited to creation of new accounts and elevation of privileges and all changes, additions, or deletions to accounts with root or administrative privileges • Initialization, stopping, or pausing of the audit logs • Creation and deletion of system-level objects (FIM) • Web Application Firewall (WAF) alerts | CTRL0024286 | CTRL0024286 - PCI Daily Security Alert/Log Review |

| Control ID | Control Objective | Description | SNOW Control Ticket | SNOW Control Report |
|-------------|--------------------------|---|---------------------|-----------------------------------|
| | | <ul style="list-style-type: none"> Anti-Virus events | | |
| CTRL0026472 | IDS - Alert Review | Intrusion detection (IDS) alerts are reviewed by responsible personnel on an as needed basis. | CTRL0026472 | CTRL0026472 - PCI IDS Events |
| CTRL0026474 | Server AV - Alert Review | Malware detection alert tickets are reviewed by responsible personnel as identified. | CTRL0026474 | CTRL0026474 - HIPS Control Review |

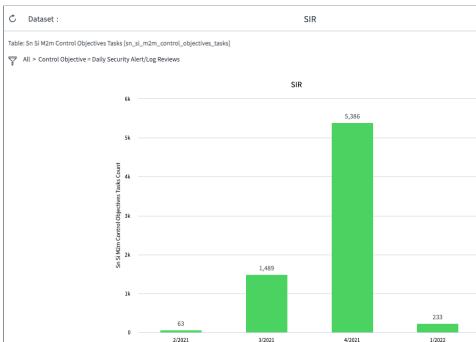
ServiceNow (SIR) Configuration

See [DSR - Development](#) for additional details.

Tickets generated in ServiceNow SIR automatically receive Control Objective assignments on generation that map to the above. These are stored in the custom table [sn_si_m2m_control_objectives_tasks](#).

| Control Objective | Task | Title | Assignment Group |
|----------------------------------|------------|--------------------------------------|------------------|
| Daily Security Alert/Log Reviews | SIR0030353 | DSR - Defender Daily Log Audit | OPS-GCSO |
| IDS - Alert Review | SIR0030352 | DSR - IDS Alerts Review - Top 10 IPs | OPS-GCSO |
| Daily Security Alert/Log Reviews | SIR0030352 | DSR - IDS Alerts Review - Top 10 IPs | OPS-GCSO |
| Daily Security Alert/Log Reviews | SIR0030351 | DSR - PCI Daily Log Audit | OPS-GCSO |
| Daily Security Alert/Log Reviews | SIR0030350 | DSR - PCI Cloud Security Login | OPS-GCSO |
| Daily Security Alert/Log Reviews | SIR0030349 | DSR - PCI Cloud Guard Duty | OPS-GCSO |

All of the ServiceNow reports for SIR utilize the data from this table to generate reports rather than data from the SIR table ([sn_si_incident](#)) directly.



ServiceNow Report Configuration

› CTRL0024286 - PCI Daily Security Alert/Log Review - Report Configuration Report

- Primary Dataset: SEC (see below)
- Secondary Dataset: SIR (see below)

Queries

- SIR
 - Control Objective = Daily Security Alert/Log Reviews
- SEC Table (DEPRECATED)
 - Created >= javascript:gs.quartersAgo(3)
 - DSR = false
 - Incident Category = Intrusion .or. Incident Category = SocialEng
 - Assigned To is not empty
 - Title does not contain PKI
 - Assignment Group = OPS-GCSO .or. Assignment Group = infosec_response
 - OR Created >= javascript:gs.quartersAgo(3)
 - DSR = true
 - Parent Ticket is not empty
 - Assigned To is not empty
 - Title does not contain PKI
 - Assignment Group = OPS-GCSO .or. Assignment Group = infosec_response

Catalog of Investigation Data / commands

Table of contents

- [Purpose](#)
- [Cheat Sheets](#)
- [Indicator Of Compromise](#)
 - [Where to look](#)
 - [Commands to use - Linux](#)
 - [Logs - Linux](#)
- [References and Additional Reading](#)

Purpose

This document serves as a guide in aiding incident responders on identifying Indicators of Compromise (IOC) on a system. This includes where to look for IOCs, commands that will aid in the identification of malicious activity, and logs or events that will support the Incident Handling process.

Additionally, system configuration items listed in this document can prove helpful in comparing the system being investigated against a normal baseline configuration and determining where a deviation has occurred.

Cheat Sheets

| Link | Contents |
|--------------------------------------|--|
| EventID Encyclopedia | Encyclopedia of Windows Security Log events by ID with references to older Windows OS IDs, |

| | |
|--|---|
| | example logs, and detailed information of each line item in log. |
| <u>Windows Forensics</u> | Artifact discovery including File Downloads, Program Execution, Deleted Files and File Knowledge, Network Activity, File\Folder Opening, Account Usage, External Device\USB Usage, and Browser Usage |
| <u>Hunt for Process, Lat Movement, Remote Execution in Windows</u> | Normal Processes and their expected behavior, identifying lateral movement, identifying remote execution, and evidence of program execution. |
| <u>Windows ATT&CK Logging Cheat Sheet</u> | This “Windows ATT&CK Logging Cheat Sheet” is intended to help you map the tactics and techniques of the Mitre ATT&CK framework to Windows audit log event IDs in order to know what to collect and harvest, and also what you could hunt for using Windows logging Event IDs. |
| <u>Linux Logs</u> | Definition of what you can find in each type of |

| | |
|--|---|
| | Linux log |
| <u>Linux Example</u> | Quick Example of Identifying and killing malicious activity. |
| <u>Linux Artifacts</u> | Locations to look for intrusion, logs to look through and what to search, persistence mechanisms, user activity to look for, timestamps to look at, and process execution to look at. |
| <u>Investigating Suspected Break In, in Linux</u> | Using aureport, checking logs for suspicious authentication and logged in users, privileged use, and SSH brute force attempts. |
| <u>Linux Mitre ATT&CK Matrix</u> <u>Windows Mitre ATT&CK Matrix</u> | Mitre matrices for Windows and Linux OS, use this to identify tactics and techniques at different stages the attack chain. |
| <u>Malware Archaeology Cheat Sheets</u> <u>SANS Cheat Sheets</u> | Additional cheat sheets to check out. |

Indicator Of Compromise

Where to look

| Location | What to look for | Reference |
|--|---|--|
| Linux /tmp /var/tmp /etc /usr/bin /usr/local/Jenkins - For a Jenkins box | <p>Common locations where malware will be running from or dropped on the system. Look for files with pseudo-random looking names, files that seem out of place, and 1 letter files or directories. Consider doing a recursive directory listing of these locations and comparing timestamps of when files landed on the system compared to the time the incident took place.</p> <p>NOTE: There is a possibility that malicious files have been time stomped and the timestamps will look similar to benign system files. In this case it is useful to check all timestamps, Modified/Access/Changed(\$MFT modified)/Birth(file creation time), for a comparison.</p> | T1036 - Masquerading |
| Windows C:\users\<NAME>\AppData\Local\LocalLow/Roaming esp temp dir in each> C:\ProgramData\ C:\Windows\Temp C:\Temp C:\Windows\Microsoft.NET\Framework\<Versoin #>\Temporary ASP.NET Files\ | | |
| /home/<user>/.bash_history | <p>Used to extract commands that have been executed by Linux users in all the previous sessions.</p> | T1070/003 |
| Scheduled Tasks- Linux /etc/crontab - System wide cron jobs. /etc/cron.d/ - where some applications install cron files. | <p>Scheduled tasks can be used for persistence and if found will point you to the file establishing persistence where you can potentially find other malicious executables used in the malicious activity.</p> <p>Look at cron jobs for scheduled tasks that look suspicious. This requires elevated permissions, to</p> | T1053 - This covers Linux and Windo |

| | | |
|---|---|--|
| /etc/cron.daily - scripts that run daily | view a specific user's cronjobs use "crontab -u username -l" | ws systems with Event IDs to look for in Windows. |
| /etc/cron.hourly - scripts that run hourly | An example of this is /etc/cron.hourly/gcc.sh used by the BillGates botnet. | |
| /etc/cron.weekly - scripts that run weekly | | |
| /etc/cron.monthly - scripts that run monthly | Check scheduled task for persistence and if found will point you to the file establishing persistence where you can potentially find other malicious executables used in the malicious activity. | |
| Scheduled Task Viewer- Windows Sysinternal's Autoruns HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Task Cache %systemroot%\System32\Tasks | If you can use SysInternal's Autoruns the time it takes to identify and verify these would be drastically reduced. | |
| /proc/<Process ID>/ | Information relevant to the associated Process ID(PID) ; "environ" includes the values of environment variables, "cwd" current working directory of the executable that started the process, "cmdline" arguments used when it ran, "exe" shows a link to the executable of the PID and various other information. | |
| Autorun on Startup - windows Sysinternal's Autoruns HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVers | For Windows Programs/Executables the registry keys listed are set to run on system start or when a user logs in. If you can use Sysinternal's Autoruns the time it takes to identify and verify these would be drastically reduced. Check for suspicious or randomly generated looking names. | T1547 - Boot or Logon Autostart Execution |

| | | |
|--|--|---|
| ion\RunOnce | | |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce | | |
| Event Triggered Execution WMI event subscriptions can be used to establish persistence on Windows machines. These can be scheduled to run daily, hourly, when a user logs on, or when a machine has been up for a certain amount of time, basically however you want them to trigger. Sysinternal's Autoruns This has been seen before in the "Plesk+NWVPMINER" incident | Get-WMIOObject -Namespace root\Subscription -Class __EventFilter Get-WMIOObject -Namespace root\Subscription -Class CommandLineEventConsumer Get-WMIOObject -Namespace root\Subscription -Class __FilterToConsumerBinding **Note: Check additional namespaces if using Sysinternals, the Subscription could be setup elsewhere from where Sysinternals checks, namely "root" | T1546 - execution to look for including WMI Event Subscription |

Commands to use - Linux

| Command | What it does |
|--|--|
| lsof -Pni lsof -p <PID> | For displaying open files. An open file may be a regular file, a directory, a block special file, a character special file, an executing text reference, a library, a stream or a network file (Internet socket, NFS file or UNIX domain socket.) List files opened by process using PID. Can be helpful in identifying any network connections the process is making and odd shared objects it is using, |
| Sysinternal's ProcExp Get-Process -ID <#> Select-Object -ExpandProperty modules | List Module Name and File Name. List of DLLs open by PID. List of Network Connections. |

| | |
|--|--|
| Get-NetTCPConnection Where-Object -Property OwningProcess -EQ <#> | |
| top Task Manager or Process Explorer | show system resource utilization. Pay attention to resource intensive processes, uncommon process names, amount of time it's been running, user who it is running under, and command and process ID. |
| ps -aux | List running processes; looking for uncommon processes running, uncommon processes by users that shouldn't have any running, and processes that should be running on the type of system you are on. Process in square brackets indicate a kernel or zombie process. |
| grep <pattern to search for> <FILENAME or STDIN> | Use grep to find a word or part of a word in a human readable file. This can aid in narrowing down results from large output. |
| head or tail | Use head or tail to view the first part or last part of files |
| less or more | Use less or more to view output 1 screenful at a time. "Less" is the preferred tool to use between the two. |
| ls -lartch | List directory contents. With the options listed you will use a long listing format, include hidden files, reverse order while sorting, sort by modification time, sort by and show c time, and print file sizes in human readable format. Use the options that work best for you. |
| Net user net localgroup administrators lslogins cat /etc/passwd file to find newly added users and check what group they are apart of | Look for any new users added to host or ones that are not normal when compared to default installation and other systems in the environment. |
| netstat -pan (For Windows or Linux) Get-NetTCPConnection (Windows) | Utilities to investigate sockets. Netstat has been deprecated and replaced by ss but netstat should still be available in the event you need to check connections consider comparing the results of both. Switches included, -pan, with -p list the process |

| | |
|---|---|
| ss -pan (Linux) | associated with the connection, -a list all connections, -n will not resolve port to service name. |
| yum history list all yum history info <ID> yum history summary <ID> | To review information about a timeline of Yum transaction IDs, the dates and times they occurred, the number of packages affected, whether transactions succeeded or were aborted, and if the RPM database was changed between transactions. Without the all option you will be limited to the most recent 20 IDs. Info and summary will give you more information on the specific transaction ID. Reference: T1547 |
| rpm -qa rpm -qi <package name> rpm -qa --qf '%{INSTALLTIME:date}: %{NAME}-%{VERSION}\n' | List installed packages. Query information on a specific package. List rpm packages installed with their installed time. Reference: S0377 |
| stats | Use to find Access, Modify, Change times. |
| fuser | Use to find processes that have a file open. |

Logs - Linux

| Log/Event ID | What it captures |
|--|--|
| /var/log/auth.log (Debian/Ubuntu) /var/log/secure (RedHat/CentOS) | System authorization information is included in this file, along with user logins and the authentication mechanism that were used. |
| /var/log/btmp "last -f /var/log/btmp" | This file contains information about failed login attempts. Use the last command and the file name to view the btmp file. The file contains username, IP, and time user logged in and out. |
| /var/log/cron | Whenever cron daemon (or anacron) starts a cron job, it logs the information about the cron job in this file. For historical cron information look at |

| | |
|-------------------------------|---|
| /var/log/cron-{yyyyMMdd} | /var/log/cron-{yyyyMMdd} file. |
| /var/log/lastlog "lastlog" | Displays the recent login information for all the users. This is not an ASCII file. An admin can use the lastlog command to view the content of this file. |
| var/log/message | This file has all the global system messages located inside, including the messages that are logged during system startup. Depending on how the Syslog config file is sent up, there are several things that are logged in this file including mail, cron, daemon, kern, auth, etc. |
| /var/log/utmp | This file contains information about the users who are currently logged onto the system. |
| /var/log/wtmp "last" | This file is like history for utmp file, i.e. it maintains the logs of all logged in and logged out users (in the past). The last command uses this file to display a listing of last logged in users. |
| /var/log/yum.log | Contains information that is logged when a package is installed using yum. This file can be referenced in the event a package is removed that has dependencies. |

References and Additional Reading

| Incident | Indicators | Mitre TTPs used |
|---|---|-----------------|
| /wiki/spaces/SECINC/pages/477135529 | Linux cron job which had apparent malicious intent with wgets/curls to onion and tor addresses, authorized_keys file had access removed for GD root and replaced with TA key, resource intensive process, port 25 being unavailable which was unusual, disabling FW, disabling SE Linux, Exim being exploited, service manipulation of "dnsadmin" and "NTP" service config files. | |

| | | |
|---|---|--|
| /wiki/spaces/SE CINC/pages/47 7135322 | Scheduled task created from malware that was executed from roaming profile of a user that was previously infected. | |
| /wiki/spaces/SE CINC/pages/47 7135188 | Exposed API via floating IP, crypto miner setup with high resource utilization. | |
| /wiki/spaces/SE CINC/pages/47 7135236 | IPtables not restored, exploited Redis, cronjob used for persistence, crypto mining setup, /tmp and /root dir used for malware locations. | |
| /wiki/spaces/SE CINC/pages/47 7150328 | User account creation on system after compromise and additional software installed and users created after initial access. | T1136 - Create Account |
| /wiki/spaces/SE CINC/pages/47 7134896 | Cron jobs for persistence, packages updated, setup socks proxy, /etc/host file updated, crypto miner setup, /lib/systemd/ and /etc/cron.d/ used for malware locations. | T1053 - Cron |
| /wiki/spaces/SE CINC/pages/47 7135221 | Modified "games" user to obtain root-level access, crypto miner setup, log tampering. | |
| /wiki/spaces/SE CINC/pages/47 7150397 | net.exe executable in odd location C:\Windows\Temp\, one letter executable on system "1.exe" at D:\temp\1.exe. | |
| /wiki/spaces/SE CINC/pages/47 7135467 | C:\Windows\Tasks\ and C:\Program Files (x86)\Common Files used for malware location, reg key "sethc" modified to malware in C:\Windows\Tasks\ to provide persistence, service installed to provide another means of persistence, service communicates with various IP for C2 and to query DNS, event logs cleared, psexec found and associated with service, local user "iis_uses" created, and keylogger used. | |
| /wiki/spaces/SE CINC/pages/47 7135019 | exploited using JuicyPotato to gain SYSTEM level permission, used mimikatz for creds, used creds and service account to distribute malware and gain access to more systems, c:\windows\temp and C:\temp used for malware location, vulnerable IIS web users used to execute malware. | |

| | | |
|---|--|--|
| /wiki/spaces/SECINC/pages/477135444 | WMI event consumer persistence, powershell used to download Powersploit tools, new user creation, event logs cleared, firewall turned off, wmic remote code execution, location used to store malicious files C:\windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files\, 1 character directory and executables i.e. "x" directory and "1.exe", cmd.exe in abnormal location, scheduled tasks to remove event logs, and executing custom DLLs using regsvr32.exe. | |
| /wiki/spaces/SECINC/pages/477134945 | High CPU usage, port 25 unavailable, process running as root, cronjob for persistence, exim exploited, wget used to download malicious file. | |
| /wiki/spaces/SECINC/pages/477135294 | Malicious scheduled tasks installed using "at" and user account compromised. | |
| /wiki/spaces/SECINC/pages/477150324 | Keylogger, VPN access, lateral movement, location used when malware ran %APPDATA%\Roaming\ggupdate.exe, location keylogger stored info %APPDATA%\Roaming\GLogs. | |
| Stopped at Completed Investigations | Continue to add when available. | |

Employee Compromise Containment

Table of Contents

- Table of Contents
- General Information
 - Process Summary
- Process Workflow
- Process Outline and Details
 - General Outline
 - Process FAQ
 - What Remediations require approval?
 - What if I'm remediating users at the request of an Incident Handler?
- Resources and Definitions
 - Internal Resources
 - Communication Templates

General Information

Review Notes

- Update team contact info
- Update Process Owner
- Update Escalation Contacts

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Employee Cyber Security• SLACK: #employee_security• EMAIL: EmployeeSecurity@GoDaddy.com |
| Process Owner | @Former user (Deleted) |
| Last Review Date | 2018-11-09 by @David Dubois (Deactivated) |
| Escalation Contact(s) | <ul style="list-style-type: none">• @Former user (Deleted)• @Juan Bustamante |
| Requests for Updates | By Email - EmployeeSecurity@GoDaddy.com |

Process Summary

This process provides direction for the remediation of employee-related compromises.

- An employee is suspected to have entered credential information into a phishing page.
- A workstation was found running malicious software.
- An employee account was found engaged in malicious activity.

Process Workflow





Process Outline and Details

General Outline

1. Ingress from Original Process.
2. Determine if Approval is required - [ServiceNow List](#)
 - a. If YES; Escalate to Tier 2.
3. Does the remediation involve more than 5 individuals?
 - a. If YES; Escalate to Tier 2.
4. Are the affected users online at the time of remediation?
 - a. If YES; Contact user via Slack/Skype to provide them with the appropriate steps to take and coordinate an appropriate time to perform the remediation (within reason).
5. Run the [Credential Mitigation](#) for users within the associated SNOW ticket(s)
 - a. Send email communication as per the below template.
 - b. Notify in [#get-itsec](#) channel to assist user in resetting password.
6. Is there a compromise of a workstation involved or suspected?
 - a. Send a notification to the Manager and the Workstation owner of your intended actions.
 - b. If YES; submit a [Re-Image Request](#) for the workstation.
7. Is a notification to the user required?
 - a. If YES; send the appropriate notification.
8. Egress to Original Process.

Process FAQ

What Remediations require approval?

Remediations involving upper-management must be approved and attempting to remediate a user at this level will trigger an approval process within ServiceNow. This is accomplished within the automation by determining if a user is within 3-levels of separate from the CEO.

Analysts can review the list of users who require approval within ServiceNow to manually verify before submitting an remediation via the automation - [ServiceNow List](#)



All > Manager = Aman Bhutani .or. Manager Manager = Aman Bhutani .or. Manager Manager Manager = Aman Bhutani >

What if I'm remediating users at the request of an Incident Handler?

This process is intended specifically to provide a process for low-impact remediations associated with day-to-day tasks. If this is remediation is related to an ongoing Major Incident then it is the responsibility of the Analyst and Incident Handler to coordinate on the appropriate process for remediation. However, in general it is best practice to involve the GetHelp and User Admin teams on any incident which may impact a significant number of users.

Resources and Definitions

Internal Resources

- Okta Admin - <https://godaddy-admin.okta.com/admin/dashboard>
- Office 365 Admin - <https://admin.microsoft.com/AdminPortal/Home#/homepage>
- Re-Image Request - https://godaddy.service-now.com/gdsp?id=gd_sc_cat_item&sys_id=db5b84dc4f4cdf804a92e3414210c78d
- Credential Mitigation Documentation - [Credential Mitigation](#)

Communication Templates

- ⓘ Please ensure that any custom communications follow the Communication Guidelines listed here.

➤ [Communication Guidelines](#)

Initial Contact

- Analysts should utilize the template included on this page, revising as necessary.

- Provide general details to support our actions:
 - Do not provide in-depth analysis (logs, file evaluations, hashes, etc.)
 - Indicate general risk/threat associated ("may have gained access to X", "could be used to monitor Y", etc.)
- Use common language ("malware", "malicious activity/process/file")
- Avoid using acronyms; If necessary define them on first use ("you will be required to enroll in Multi-Factor Authentication (MFA)")
- Be sure to convey the appropriate urgency ("please do X as soon as convenient", "Y must be done ASAP", "we must immediately perform Z to remediate", etc.)
- Ensure the right parties are included for awareness:
 - CC the EmployeeSecurity group for visibility.
 - For jobs that monitor daily performance (primarily C3 report), ensure direct supervisors are CC'd on the communication for awareness.

Follow-Up

- Answer any question as straight-forward as possible:
 - Use this as a chance to educate users if possible.
- If users have concerns with steps taken or to take we can:
 - Offer alternatives, if possible.
 - Re-state our reasoning and express the urgency/risk of the situation.

➤ Account Locked (Credentials Only)

Communication templates#Account-Locked-(Credentials-Only)

➤ Account Locked + Workstation Re-Image

Communication templates#Account-Locked--Workstation-Re-Image

➤ Communicate Major Phish to Everyone@

To: Everyone@ <everyone@godaddy.com>; Everyone-EMEA <Everyone-EMEA@godaddy.com>; DL-allbelgrade <allbelgrade@godaddy.com>

CC: EmployeeSecurity

Subject: Security Alert - Spear Phishing Email - <SUBJECTLINE_OF_PHISHING_EMAIL>

Team –

We are seeing a round of phishing emails from <"an internal Go Daddy employee" OR EMAILADDRESS> with the subject line "<SUBJECTLINE>". This email contains a link to a fake <BRAND> login page.

This email is a spear phishing attempt to get you to fill out the login page and steal your credentials. If you have received this email, immediately delete it. If you have visited the fake website from the link in the email, please immediately change your password. If you are not sure, check your browsing history for any URL containing <PHISH_DOMAIN>. If you have issues resetting your password, please reach out to the GetHelp team for assistance.

Here is what the email may look like for your reference:

<SCREENCAP> NOTE: Partial redaction for internal emails.



Here's what the login page looks like, if you clicked through the link in the email:

<SCREENCAP>

Please reach out to our employee security team at #employee_security or isitbad@godaddy.com if you have any additional questions!

To learn more about phishing, please see: <https://godaddy.jiveon.com/community/security/safety-security/phishing>

Credential Mitigation

Table of contents

- Table of contents
 - Automated Credential Remediation Process Workflow
 - >>> Process Link <<<
 - Contact Impacted User and Manager
 - Inform #get-itsec
 - Validate Credential Mitigation
 - Assign Security Awareness Training
 - Existing Gaps

Automated Credential Remediation Process Workflow

>>> Process Link <<<

When a user's credentials are suspected of being compromised, Credential Mitigation can be kicked off from our tickets in the Security Incident table in SNOW. It will perform the following on each user selected:

1. Expires and resets password - Okta, which means JOMAX and DC1 will also be reset
 - a. <https://developer.okta.com/docs/reference/api/users/#expire-password>
 - b. This call "expires" the user's password, and sets a temporary password, which is not saved/logged.
 - c. This does NOT disable the user's account.
2. Clear Okta sessions
3. Clear O365 sessions, both OWA and OneDrive
4. Clear Slack session

Contact Impacted User and Manager

 To: Affected User

CC: Supervisor (**Do NOT CC Director level or above**); Workforce (**Care Agents ONLY**);

GCSO; ssit@godaddy.com; engwin@godaddy.com

Subject: Your User Account Has Been Locked : Action Required

The Security team was recently made aware of <**Incident_Type**> in which we believe your account credentials may have been compromised. Because you were unavailable at the time of this discovery, we have taken action as a precaution to protect your account from misuse.

You will need to reset your password in order to regain access to your account. This will require you to contact [GetHelp](#) (480-624-2580) for assistance. Please ensure that the following best-practices are also observed for your account:

- Reset any credentials not synchronized to your GoDaddy login - example include SaaS applications, local accounts, etc.
- Ensure that passwords are not reused across any services, accounts, etc.
- Passwords on all company-controlled platforms must conform to GoDaddy password standards.

We will also be ensuring you are enrolled into Okta Multi-Factor Authentication (MFA) as an added layer of protection. If you were not already enrolled in MFA you will be prompted to complete setup when you next sign-on to Okta.

⚠ Please make necessary change while sending the above communication as per the scenario.

Inform #get-itsec

Using one of the two message templates, please inform #get-itsec of the remediation performed.

[Communication templates | Credential Mitigation](#)

Validate Credential Mitigation

Using Splunk **ES**, find the user's Okta actor ID, below is a quick way to find it.

```
1 index=oktalogs email=<email>
```

Then search for the all logs containing the actor ID.

1 Example: index=oktalogs TERM(00u8j7c99UBV5Tvcc0y6)

You want to make sure the targetUserID is the ID of the user you remediated and not any other. As shown below, the top two logs are what we are looking for validation. "Clear user session" and "Perform user password reset by AD agent"

| outcome.result | debugContext.debugData.risk | displayMessage | client.userAgent.rawUserAgent | debugContext.debugData.requestUrl | targetAppUserAlternateId | targetUserId | actor.id |
|----------------|-----------------------------|---|---|--|--------------------------|----------------------|----------------------|
| SUCCESS | | Clear user session | ServiceNow/1.0 | /api/v1/users/00u8j7c99UBV5Tvcc0y6/sessions | | 00u8j7c99UBV5Tvcc0y6 | 00uiruhny5C9sBC7s0x7 |
| SUCCESS | | Perform user password reset by AD agent | ServiceNow/1.0 | /api/v1/users/00u8j7c99UBV5Tvcc0y6/lifecycle/expire_password | cthornton@godaddy.com | 0ua8f9lxck4m3OHj0y6 | 00uiruhny5C9sBC7s0x7 |
| SUCCESS | | User single sign on to app | Windows-AzureAD-Authentication-Provider/1.0 | /app/office365/exk3c5qbbpJ0B61dF0x7/sso/wsfed/username13 | cthornton@godaddy.com | 0ua3hkcoj94trVza0x7 | 00u8j7c99UBV5Tvcc0y6 |
| ALLOW | | Evaluation of sign-on policy | Windows-AzureAD-Authentication-Provider/1.0 | /app/office365/exk3c5qbbpJ0B61dF0x7/sso/wsfed/username13 | | | 00u8j7c99UBV5Tvcc0y6 |
| SUCCESS | | Authentication of user via MFA | Windows-AzureAD-Authentication-Provider/1.0 | /app/office365/exk3c5qbbpJ0B61dF0x7/sso/wsfed/username13 | | 00u8j7c99UBV5Tvcc0y6 | 00u8j7c99UBV5Tvcc0y6 |
| SUCCESS | | Authenticate user with AD agent | Windows-AzureAD-Authentication-Provider/1.0 | /app/office365/exk3c5qbbpJ0B61dF0x7/sso/wsfed/username13 | cthornton@godaddy.com | 0ua8f9lxck4m3OHj0y6 | 0007824oHOx6Q3YW0y6 |

Assign Security Awareness Training

After confirming that the user has successfully clicked on a phishing link (by checking DNS logs) we should submit the user for security awareness training following these steps:

1. Check the users position in the company (Do not submit VP's for training!)
2. Submit the training request on this SN link https://godaddy.service-now.com/gdep?id=sc_cat_item&sys_id=c33ce096dba1e454bb5a4a28139619de&sysparm_category=1b9c0e8fdb28d4d0bb5a4a2813961922

★

Cornerstone Support

Request support with Cornerstone, GoDaddy's learning management system

Complete the form to submit a request for Cornerstone Support. Please select the correct category and add any necessary attachments or screenshots of issues by clicking on the paperclip icon.

* Requester

* Employee's Involved

* Topic

Title

* Description of Issue

 Add attachments

Submit

Existing Gaps

1. An unlock email can be sent to [@godaddy.com](#) email addresses. If a TA has more than one account, they could, theoretically, send an unlock email for a mitigated account, to another account, use the unlock email to answer the security question, assuming of course that they have changed the security question, and unlock the locked account.
 - a. Suggestion: disable all self-service unlocking capabilities from Okta. This way any user has to go through GetHelp to regain access.
2. Still unknown, needs confirmation: When a user is set to "User must change password at next logon" in AD, Okta will allow the previous, non-temporary password set, and it allows for the same self-service unlock process.
 - a. Again, if we can disable self-service unlocking, this would solve this gap as well.
3. This automation utilizes the Dynamic Workflow Engine which does all onboarding and offboarding. At 2pm AZ time daily, all onboarding is done. The queue will fill up around this time, and cause a delay in mitigation processing. i.e. We kicked off a mitigation at 2:54pm on a heavy onboarding day, and it did not get processed until 3:22pm, a total of 28 minutes later.
 NOTE: This was a known gap, and hasn't been in issue while the Credential Mitigation automation has existed.
 - a. There currently isn't a way to fix this using the DWE for processing.

4. Communications/coordination between Security/HR/IAM/GetHelp so that user's mitigated by security are scrutinized more. - Raised by Rob Schrafel during our meeting.

Security@ and SecurityBreach Mailbox Process

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Workflow](#)
- [Security@ Scenarios](#)
- [SecurityBreach@ Scenarios](#)

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | 2023-03-30 by @David Hernandez |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @David Hernandez 03/30/2023 |

Purpose

This process provides direction for the handling of communications to the Security@ general mailbox. This mailbox serves as a common point of contact for most general security requests from internal entities. Some of the specific use-cases which are seen via this communication method are:

- [Coordinated Vulnerability Disclosure \(CVD\) Notifications](#)
- Reports of Impersonation of GoDaddy (Websites, Phishing Attempts, etc.)
- External Reports of Malicious Customer Activity (Malware, Phishing, Spam, etc.)
- Internal Reports of Suspicious Activity (Phishing, Physical Behavior, etc.)
- General Solicitations (Security Vendors, Services, SPAM, etc.)
- General Security-related Inquiries

Workflow

1. GCSO receives a message from Security@ mailbox. A ticket has been created on SNOW with the same subject too.
2. Review the message to identify the communication type and/or scenario.
3. Escalate to Tier 2:
 - a. Server related compromise
 - b. Social Engineering attempt
 - c. Data breach

Security@ Scenarios

| | | | |
|------------------------------|--|---|-------|
| GoDaddy Impersonation | <ul style="list-style-type: none">• If valid, report via FoS Abuse Form• If not, Close False Positive | ENG-DCU | GDP |
| Customer Abuse Report | <ul style="list-style-type: none">• Report via FoS Abuse Form<ul style="list-style-type: none">◦ If this is not possible email to abuse@godaddy.com | ENG-DCU | ABUSE |
| Customer Security Concerns | Close False Positive - No further action | --- | CARE |
| Suspicious Internal Activity | <ul style="list-style-type: none">• If Cyber related - Review and determine if event can be taken care of by GCSO. If not, Escalate to IR• If Physical related - Notify | <ul style="list-style-type: none">• infosec_response• Physical Security Command Center | EMP |

| | | | |
|------------------------------------|--|----------------------------------|--------|
| | scc@godaddy.com via email. | | |
| Threats or Threat Reports | <ul style="list-style-type: none"> If this is a received threat (not a report from OCEO, WSC, etc.), immediately notify #workplace-services via Slack If this is a Threat Report (from OCEO, WSC, etc.), verify scc@godaddy.com was included in the recipients and report during standup | Physical Security Command Center | THREAT |
| General Solicitations OR SPAM | Close False Positive - No further action | --- | SPAM |
| General Security-Related Inquiries | <ul style="list-style-type: none"> Review and determine if event can be taken care of by GCSO. If not, notify Incident Response via Slack/Email | --- | MISC |

SecurityBreach@ Scenarios

| | | | |
|-------------------------------------|--|-----|--------|
| Vendor Security Breach Notification | <ul style="list-style-type: none"> Review and determine if event can be taken care of | --- | THREAT |
|-------------------------------------|--|-----|--------|

| | | | |
|------------------------------------|---|--|------|
| | by GCSO and immediately notify Incident Response via Slack/Email | | |
| Suspicious Internal Activity | <ul style="list-style-type: none"> If Cyber related - Review and determine if event can be taken care of by GCSO. If not, Escalate to IR If Physical related - Notify scc@godaddy.com via email. | <ul style="list-style-type: none"> infosec_response Physical Security Command Center | EMP |
| General Solicitations OR SPAM | Close False Positive - No further action | --- | SPAM |
| General Security-Related Inquiries | <ul style="list-style-type: none"> Review and determine if event can be taken care of by GCSO. If not, notify Incident Response via Slack/Email | --- | MISC |

How-To Guides

- [Hostname Conventions and Machine Information](#)
- [How to use Kentik](#)
- [Convert shopperIDs to CustomerIDs](#)
- [Custom Assessment and Remediation Scanning and Reporting](#)
- [AWS Account Investigations](#)
- [Hosting VS Non-Hosting Content](#)
- [Common Customer Environments](#)

Hostname Conventions and Machine Information

Table of Contents

- [Reading Hostnames](#)
 - [Workstations](#)
 - [Hostname Information](#)
 - [Hostname Structure](#)
 - [Servers](#)
 - [Hostname Information](#)
 - [Hostname Structure](#)
- [Finding Devices](#)
 - [ServiceNow Configuration Management Database \(CMDB\)](#)
 - [Absolute](#)

Reading Hostnames

Workstations

Hostname Information

The Hostname of a workstation can generally provide the following pieces of information:

- Machine Type (and Operating System)
- User Role

In some cases it can also provide:

- User Location / Office
- Username

Hostname Structure

Workstation hostnames have a general format which provides insight into the Device Type, User Role and often the Username of the assigned user.

The format for most hostnames is `<Office><MachineType> <UserRole> - <Username/OfficeLocation>`

While this is not true of all systems, this provides a general method for identifying workstation types and ownerships. Some examples:

- An IT user's Windows laptop: `LT IT - DDUBOIS`
- A Tempe-based C3 Workstation (Desktop PC): `T1 WS C3 - C131`
- A Virtual Machine on an IT user's Mac laptop: `VM - LM IT - DAVIDD`

Some items to note are:

- i. Usernames (when present) are not always complete.
- ii. In some cases the username is not used, instead there may be an identifier (UM764H9) or a modified username (DAVID).

The naming codes generally used to identify workstations are as follows:

| Office | Machine Type | User Roles |
|--|---|--|
| <ul style="list-style-type: none">• T1/T2 - Tempe• S1 - Scottsdale• G1 - Gilbert• SE1 - Seattle• C1 - Hiawatha• SJ1 - San Jose• P3 - Phoenix• C3WFH - C3 Remote | <ul style="list-style-type: none">• LM - Laptop (Mac)• WS - Workstation (Desktop, Windows)• LT - Laptop (Windows)• VM - Virtual Machine• TB - Tablet | <ul style="list-style-type: none">• WC - Website Creation (GD Web Design)• AC - Accounting• C3 - C3 (Customer Care Center)• CM - C3 Management (Customer Care Center)• CP - Corporate (General Use - Corp)• DS - Domain Services• DV - Developer• EA - Executive Assistant• EX - Executive• FA - Facilities• FR - Fraud• GS - Guest Services (ISS)• HA - Hosting Admin (SRO/HOC)• HR - Human Resources <ul style="list-style-type: none">• IT - Information Technology (General Use - IT)• LG - Legal• MK - Marketing• OP - Office of the President (OCEO)• PD - Professional Development (ProDev)• PS - Physical Security (WSC)• PY - Payroll (Accounting)• QA - Quality Assurance (C3 QA)• QM - Quality Management (C3 QA)• RA - Registration Authority (SSL Support)• TC - Technical Corporate (General Use - TC) |

- **TR** - Training (C3 Training Class)
- **TV** - Television (Wallboards)
- **WF** - Workforce

Servers

Hostname Information

The Hostname of a server can generally provide the following pieces of information:

- Machine Type (and Operating System)
- User Role

In some cases it can also provide:

- User Location / Office
- Username

Hostname Structure

Good Luck!

| Environment | Rexgex |
|-------------|--------------|
| vps3 | .*PLPCS.* |
| vps4_os | .*ztncldhv.* |
| vps4_vm | .*plvzvmn.* |
| vps4_kvm | .*plohvnmn.* |
| vps4_ct | .*plvzctn.* |

Finding Devices

ServiceNow Configuration Management Database (CMDB)

ⓘ Used for Servers, Network Devices, Appliances & Windows Workstations

CMDB is the source of truth for most GoDaddy devices and can provide the following pieces of information:

- System User (Assigned To)
- Operating System
- Serial Number

When using CMDB the primary method of finding machines is via the Quick Search function:

1. Using the **CMDB Quick Search** enter the identifying portion of the Hostname into the **Hostname / FQDN** field and click **OK**. (NOTE: Results will not immediately show)
2. When results are found the **CI Results** or **Asset Results** section at the bottom will update to show the number of records returned.
 - a. Click the Results type to expand the list.
 - b. Click on the Hostname to review.
3. On the Record you can the Assigned To to determine the machine user.
4. Hovering on the Information ⓘ Icon will display more details about the user.

The screenshot shows two main windows from the GoDaddy Absolute console.

Search Results: A modal window titled "Search Results [1 results]" displays a single result for "LTIT-DDUBOIS". The table includes columns: Device Name, IP, Owner, Model, Serial, RMAC, Rack, and Slot. The entry shows "LTIT-DDUBOIS" in all columns.

Device Details: The main window shows the device "Computer - LTIT-DDUBOIS" with the following details:

| Name | LTIT-DDUBOIS | Status | Installed |
|---------------|--|--------------------------|-----------------------|
| Asset tag | | CHDB C Status | Live |
| Manufacturer | Hewlett-Packard | Primary Business Service | Employee Workstations |
| Model ID | Hewlett-Packard HP EliteBook Folio 9470m | Assigned to | David Dubois |
| Asset | Hewlett-Packard HP EliteBook Folio 9470m | Assignment group | |
| Serial number | CNU4019HQM | Most Recent Login User | |

Below the main table, there are tabs for Configuration, Meta, Reporting, and Activity. The Configuration tab is selected. Under Configuration, there are fields for Is Virtual, GS Domain (jomax.jaholdings.com), Operating System (Windows 8.1 Enterprise), GS Version (6.3.3600), GS Service Pack, and Disk space (0B).

On the right side, there are sections for Chassis Type (Notebook), RAM (16.0GB), CPU manufacturer (GenuineIntel), CPU type (GenuineIntel), CPU speed (MHz) (2.80), CPU count (1), and CPU core count (4). At the bottom right of the main window is a "Save" button.

Absolute

Used for Workstations

Absolute is GoDaddy's device management solution and can provide the following piece of information:

- Last Check In Time
- Serial Number
- Username
- Operating System
- Local & Public IP

Absolute is a cloud solution which is access through their external site:

1. Sign into the **Absolute console**.
2. From the menu on the left, select **Find Devices**.
3. Under **Active Devices** search for the hostname in question.
4. Click the listed **Identifier** to view device details.

The screenshot shows the Absolute Find Devices interface.

Left Sidebar: Shows navigation links including Active Devices (selected), Reports, Devices with Active Policies, Device Analytics, Full-Disk Encryption Status, SCCM Status, Anti-Malware, Event History, Android Vulnerability, and Application Persistence.

Search Results: A table titled "Active Devices" lists one item: "LTIT-DDUBOIS". The table columns are Identifier, Last Connected (UTC), Username, Serial Number, Device Name, Make, Model, and OS. The entry shows "LTIT-DDUBOIS" in all columns.

Details View: A modal window titled "LTIT-DDUBOIS" displays the following details:

| Identifier | Last Connected (UTC) | Username | Serial Number | Device Name | Make | Model | OS |
|---------------------|----------------------|---------------|---------------|--------------|-----------------|--------------------------|---------|
| 2Q0XF1SDHAA19FX1273 | Oct 20, 2017 3:33 AM | JOMAX\ddubois | CNU4019HQM | LTIT-DDUBOIS | Hewlett-Packard | HP EliteBook Folio 9470m | Windows |

At the bottom of the details view is a "Report Options" button.

How to use Kentik

Kentik Over View

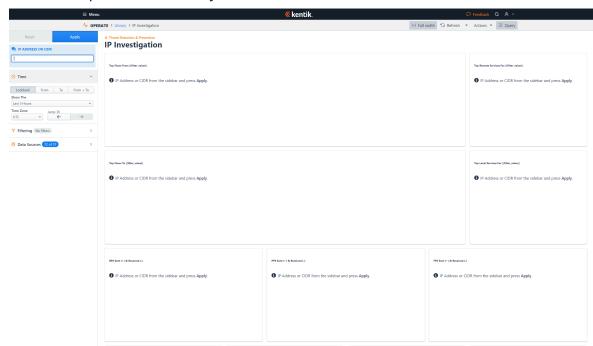
Kentik is a tool owned by our networking team to help monitor Netflow Data and is made up of Multiple sensors placed around GoDaddy's environment capturing data from 1 in 2000 packets and shipping that data Kentik's data store.

Kentik Library

Objective: To review TA IP using the saved IP Investigation Dashboard in the Kentik Library, doing this will allow you to review the Netflow Data of the TA IP in our network.

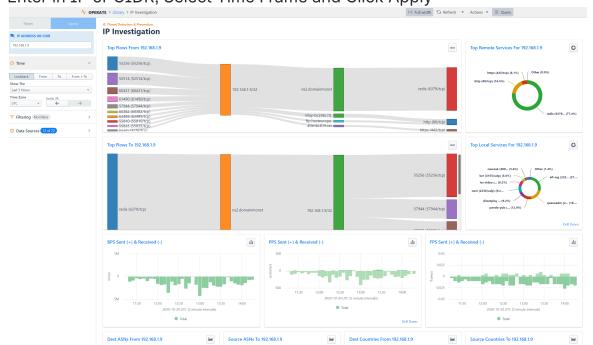
1. Log into Kentik and navigate to the Dashboards

- Menu → Operate → Library → Threat and Detection & Prevention – IP Investigation



2. Enter in TA IP to pull Netflow Data based on the saved search.

- Enter in IP or CIDR, Select Time Frame and Click Apply



Data Explorer

Objective: To review the TA IP's Net Flow Data in Kentik

1. Log into Kentik's Data Explorer function
- a. Menu → Operate → Data Explorer
2. Select the Visualization type you would like (defaults to *Stacked Area Chart*).
3. Select Data Sources

a. This defaults to All Data Sources but can be broken down by Site, Labeled Groups or Individual Data Sources.

4. Select Dimensions

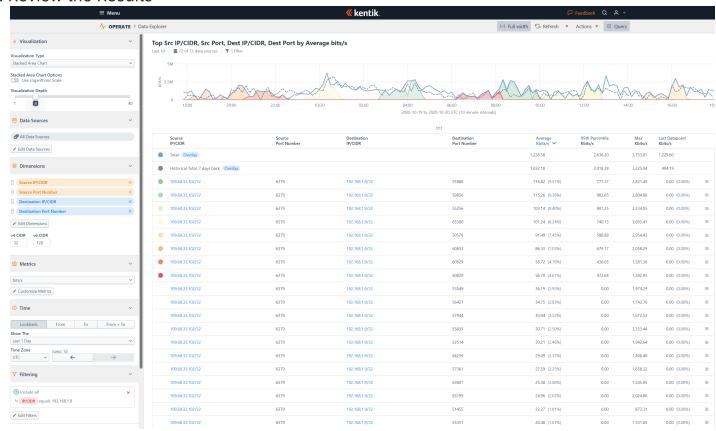
5. Select the time frame in which you want review the Net Flow data (Defaults to UTC).

6. Select the Metrics you want to collect (IP's, Bits, Packets, ect).

7. Select the filter which can be multiple items.

a. Edit Filters → Add Ad Hoc Filters

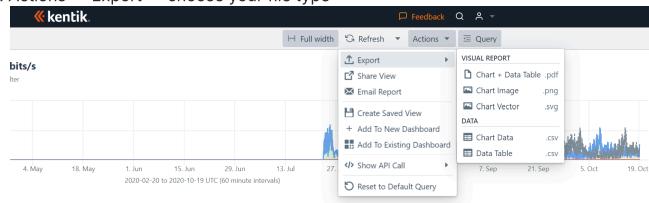
8. Review the Results



How to Export out of Kentik

Objective: To share info with leadership or fellow team mates you can export the data or share the view.

1. To export the data you can choose a pdf, png or csv file.
 - a. Actions → Export → choose your file type



2. To share your search you can choose *Share View* under *Actions* as well.

Convert shopperIDs to CustomerIDs

General Information

If the IR team needs to convert shopperIDs to CustomerIDs or CustomerIDs to shopperIDs to facilitate analysis during an incident this will guide them on how to do it.

Steps to convert IDs

1. Log into the Production AWS Storage Account via Okta and ensure you are in the **Oregon (us-west-2)** region.
 - a. **gd-aws-usa-gd-respstorag-prod (710249649903)**
2. If you are interested in running an ID conversion for a large batch of IDs then continue to **Step 3**, if you are interested in running a small set of ID conversions then go to **Step 7**
3. Navigate to the **S3** service, then the s3 bucket **gd-respstorag-prod-athena**, then the folder **idsToLookup**, and upload the CSV file containing the IDs you need to convert into this folder.
 - a. The CSV file should have all the IDs you need to convert in the 1st column and should all be the same type of ID i.e. either all **shopperID** or all **CustomerID**.
 - b. NOTE: If you plan on running more than one query, the CSV file should be named the same each time to convert only the IDs needed. Otherwise, Athena will query against and return values for all CSV files in the **idsToLookup** folder.
4. Navigate to the **Athena** service, and select **Launch query editor** under Get Started. This should take you to a page where you can run queries.



- a.
5. Here you will be able to run a query against the CSV file previously uploaded. The following query can be used to perform this operation.

```
1 WITH a AS  
2  
3     (SELECT ids
```

```
4      FROM "shopperid-to-customerid".shopperids),
5  b as
6      (SELECT *
7       FROM "customer-id-mapping".customer_id_mapping_snapshot)
8
9  SELECT * FROM b
10 JOIN a ON a.ids=b.id
```

6. Once the query is complete the results will be dropped in the S3 bucket **gd-respstorag-prod-athena** where you can download the CSV and retrieve the IDs needed. The results will be placed in nested folders with names based on the date of the query i.e. for results for a query ran on **28/Jun/2023** the location of the CSV would look like the following:

a. **gd-respstorag-prod-athena/Unsaved/2023/06/28/<queryResults.csv>**

7. If you only need to perform a query against 1 ID or a small amount of IDs the following query can be used instead of uploading a CSV.

a. 1 #Use this query to return all results about the shopperID 1234567
2 SELECT * FROM customer_id_mapping_snapshot
3 WHERE id = '1234567'

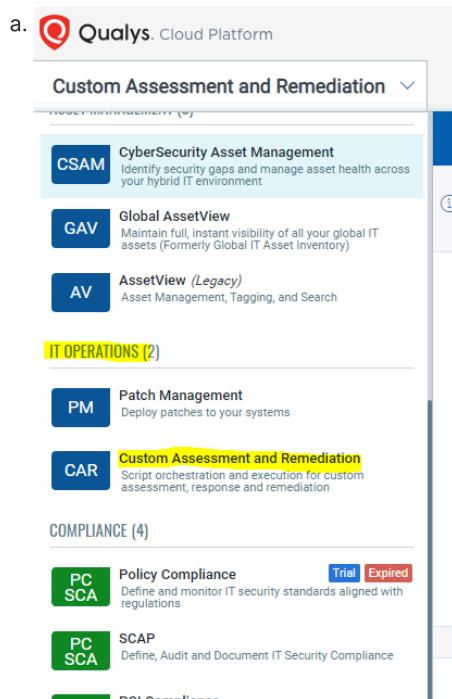
b. 1 #Use this query to return all results about the CustomerID '12345678-1234-1234-1234-12345678901234'
2 SELECT * FROM customer_id_mapping_snapshot
3 WHERE customerid = '12345678-1234-1234-1234-12345678901234'

Custom Assessment and Remediation Scanning and Reporting General Information

If the IR team needs to collect data from an endpoint this will guide an IR member on how to do this using Qualys. All Incident Response members should have the permissions required to perform these operations, if not then reach out to the **#qualys** channel for guidance on how to obtain the required permissions.

Steps to run a scan in Qualys

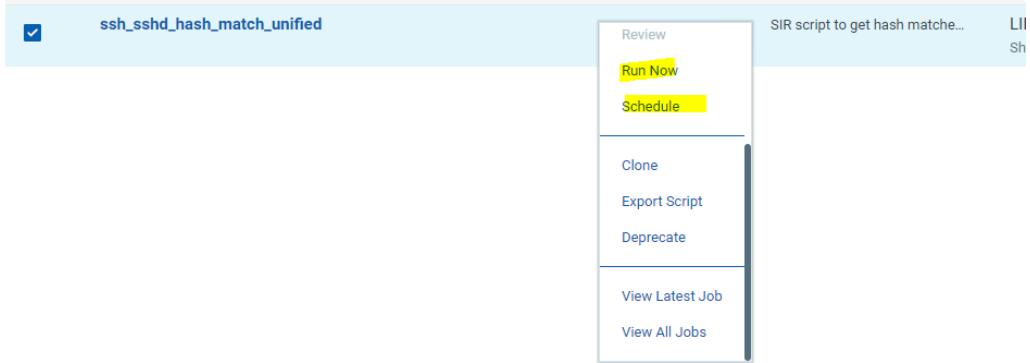
1. Log into Qualys via Okta
2. Navigate to the drop-down menu in the top left of the screen and select “Custom Assessment and Remediation” under the “IT Operations” section.



3. Select “Scripts” from the list of tabs at the top



- a. Select the drop-down menu next to the script you would like to run and Select either Run or Schedule dependent on if you want to run the scan once now or schedule it to run on a schedule.



a.

5. Next, you will either select the Assets you want to run the scan against by adding them to the list individually OR adding assets based on Asset Tags where you can run one or multiple Asset tags at a time.
6. Finally, select Execute Script, and under the Jobs tab you will see the progress of your scan.

a.

7. If you are running a scan against a large number of assets at a time, instead of using the GUI to review details from the scan it is better to pull the results down using Qualys CAR Reporting Tool (QCRT).

Steps to pull Qualys scan reports with QCRT

In order to pull reports back from Qualys you will need to install QCRT and retrieve credentials for API access from the AWS Forensic Analysis account's Secrets Manager (`gd-aws-usa-gd-respforens-prod` (accountID `238324709343`))

1. Install QCRT
 - a. Follow the guidance here for how to install QCRT: <https://github.com/gdcorp-infosec/qcrt>
2. Retrieve the `Qualys-API` credentials from the AWS Forensic Analysis account's Secrets Manager (`gd-aws-usa-gd-respforens-prod` (accountID `238324709343`))
 - a. In order to retrieve Secrets in this account you have to Elevate permissions via Public Cloud Portal <https://pcp.int.gdcorp.tools>. This can be accomplished following this guide [Elevate Permissions in AWS Accounts through Public Cloud Portal \(PCP\)](#).
3. Identify the Job ID you want to pull a report for. To find this in Qualys select the link for the Job Name corresponding to the scan you ran and in the URL the Job ID is listed after

asset-jobs

- a. Example Job ID below is **238826**
- i. [https://qualysguard.qg4.apps.qualys.com/sm/#/jobmanagement/asset-jobs/238826?
search=&source=&pageSize=50&pageNumber=0](https://qualysguard.qg4.apps.qualys.com/sm/#/jobmanagement/asset-jobs/238826?search=&source=&pageSize=50&pageNumber=0)
 4. Next, you will need to identify the delimiter and CSV headers for the script you ran, these should be listed in the script's comment section. The delimiter should match the delimiter used when the script writes output from the commands.

Summary

 fileInfoAdditionalIOC
Created By Carlos Lopez, May 3, 2023 12:32 PM

Script Details

| | | |
|--------------|---|--|
| Script Id | Platform | Type |
| 173429 | LINUX | Shell |
| Severity | Category | Last updated |
| 5 | Data Collection | Updated By Carlos Lopez, May 3, 2023 12:39 PM |
| Threshold | Last job run | |
| 3600 seconds | May 3, 2023 12:39 PM | |
| Description | Scanning for IOCs from malicious mod_dir.so and libkeyutils | |

Script

```
#!/bin/bash
# csv headers here
# ensure your echo statements match this format, using a cell seperator that does not show up as a part of the output of commands
# you're running
# host_name file_path size blocks io_block file_type device inode links perms uid gid access modify change birth md5 sha1 sha256
host_name=$(hostname -f)
```

a.

5. Now in your terminal where QCRT is installed run the following command to pull your report

- a. qcrt --delimiter <DELIMITER> --user <USERNAME> --password <PASSWORD> <JOBID> <FIELDS>
- b. qcrt --delimiter \| --user foo --password bar 123456 hypervisor "host/vm" uuid server_name file_path size blocks io_block file_type device inode links perms uid gid access modify change birth md5 sha1 sha256

AWS Account Investigations

- [AWS Overview](#)
- [AWS Logs](#)
- [Using Athena to Search Historical Logs](#)

AWS Overview

- [Architecture Overview](#)
- [Glossary](#)

At GoDaddy, teams use Amazon Web Services (AWS) extensively. As such, it is required that members of the Incident Response team understand and be able to respond to incidents in AWS. This is **not** a comprehensive overview, just the main points that may be useful as far as the IR team is concerned.

Architecture Overview

In each AWS Organization, there exists:

- one Logging Account:
 - Collects the logs from all LoB accounts and
 - Replicates the collected logs to the Organization's Security Account
- one Security Account:
 - Stores the replicated logs.
 - Administrator account for AWS GuardDuty in the Organization
 - Administrator account for AWS WAF's FMS
 - Administrator account for AWS Shield
 - Extra Notes:
 - the Non-PCI Security Account also aggregates logs from On-Prem and other Non-AWS sources, such as SaaS applications
- multiple LoB Accounts:
 - any team may own any number of LoB Accounts (or sets of LoB Accounts)

An overview of the Security Logging architecture can be found here: <https://github.com/gdco/rp-infosec/security-logging-aws-infra/tree/develop/docs> Connect your Github account

You do not need to concern yourself with the EKS cluster(s), ECR, Alerting, or SQS Queues.

Glossary

Note: some terms may be GoDaddy-specific.

- **AWS:** Amazon Web Services

- **Environment:** sometimes referred to internally as an "**AWS Environment**" (or, rarely, a **Stage**). This refers to one AWS Account used for a specific part in the development process. The [CTO Guidelines page](#) explains this in more depth.

- note that **CICD** is also considered an **Environment**, though it is not listed in the CTO Guidelines (at the time of writing)
- the **CICD** account is special in that it assumes the Deploy Role in any of the other **Environments** associated with the same **Project**

- **FMS:** Firewall Management Service; a component of AWS WAF. This is used to enforce a baseline set of WAF Rules managed by the Organization's Security account. These rules are enforced by default against Application Load Balancers and API Gateway Stages. However, teams may choose to be disassociated (excluded) from this default policy if they attach a WAFv2Regional to all resources that would otherwise be protected.
- **GuardDuty:** an AWS service that monitors for threats and/or malicious activity originating from or targeted against an account's resources.
- **LoB:** Line of Business; often used to refer to a specific GoDaddy product or service. An LoB Account refers to one specific Environment or Stage
- **Organization:** A collection of AWS Accounts that may share resources or trust relationships.

At GoDaddy, we have the following Organizations:

- Non-PCI: "GEN", where most projects/accounts live. These accounts do not store or process PCI data
- PCI: Payment Card Industry. These accounts/projects are in-scope for PCI compliance and have higher data security requirements
- Registry: For the Registry org. Few accounts live here, but they likely have higher data security requirements
- C3PO: Nobody knows what this stands for. But probably something along the lines of "Centralized Cloud Control Plane Organization". This is the newest organization, which is trusted by all other AWS Organizations' accounts and the final resting place for a lot of shared assets. This may include, but is not limited to:
 - Ingest of Security logs from every other Organizations' Security Accounts
 - company-wide IAM roles' access roles (e.g., `SecurityReadOnlyAccessRole` , `SecurityAdminAccessRole`)
 - Lambda functions S3 bucket for Service Catalog
 - Golden Container Registry

- MNA: Mergers and Acquisitions. This organization is where AWS Accounts from acquired companies gets placed under before they are transitioned to a GoDaddy standard account (also sometimes known as a TLZ - Trusted Landing Zone). This allows GoDaddy to place some default security controls (e.g., logging, IAM roles for management, GuardDuty, WAF)
 - Hackathon: For company hackathons; usually contains only temporary accounts or otherwise short-term resources. Usually this is not utilized.
 - Dev1GD: Usually reserved for Cloud Platform Engineering/Cloud Automation team to test changes before applying them to all other AWS Organizations. Requires a separate `@dev1.gdg` Okta account (`dev1gd.oktapreview.com`) to log in through the "front door"
- **Project:** a Public Cloud Portal (PCP) Project, which is a means to associate resources (such as Budgets, AWS Accounts, OpenStack Projects) for a specific **LoB**.
 - **Shield:** an AWS managed service that provides DDoS protection
 - **WAF:** Web Application Firewall.

AWS Logs

- [Log Types](#)
 - [App Security](#)
 - [CloudTrail](#)
 - [Config](#)
 - [EKS](#)
 - [GuardDuty](#)
 - [Syslog](#)
 - [VPC Flow](#)
 - [WAF](#)
- [Accessing the Logs](#)
 - [Splunk](#)
 - [Prerequisites](#)
 - [Procedure](#)
 - [AWS Security Account](#)

Log Types

App Security

```
1 index IN (
2     "app_security",
3     "pci_app_security",
4     "registry_app_security",
5     "mna_app_security",
6     "c3po_app_security",
7     "testingscripts_app_security"
8 )
```

These logs are generated by each teams' applications running their AWS Accounts. These generally follow the [AppSecLog standard](#), but may not provide the same level of fidelity across

CloudTrail

```
1 index IN (
2     "aws_cloudtrail",
3     "pci_aws_cloudtrail",
4     "registry_aws_cloudtrail",
5     "mna_aws_cloudtrail",
6     "c3po_aws_cloudtrail",
7     "testingscripts_aws_cloudtrail"
8 )
```

These logs contain data for (almost) all API calls invoked by (almost) every entity in AWS. This has the effect of tracking an entities' actions in AWS.

Config

```
1 index IN (
2     "aws_config",
3     "pci_aws_config",
4     "registry_aws_config",
5     "mna_aws_config",
6     "c3po_aws_config",
7     "testingscripts_aws_config"
8 )
```

These logs contain a snapshot of all resources in the account. To find a specific resource, you can use the `resourceType` field (to get the class of resource, such as

`AWS::IAM::Role` or

`AWS::ServiceCatalog::CloudFormationProvisionedProduct`) and/or the `object_path` (e.g., `arn:aws:iam::123456789012:role/example-role` or `arn:aws:catalog:us-west-2:123456789012:product/prod-abc1234567890`).

Depending on the resource, there may be more or less fields that further describe the connections between any given resource(s).

EKS

```
1 index IN (
2     "aws_eks",
3     "pci_aws_eks",
4     "registry_aws_eks",
5     "mna_aws_eks",
6     "c3po_aws_eks",
7     "testingscripts_aws_eks"
8 )
```

These logs contain EKS logs. These are generally not used

GuardDuty

```
1 index IN (
2     "aws_guarddduty",
3     "pci_aws_guarddduty",
4     "registry_aws_guarddduty",
5     "mna_aws_guarddduty",
6     "c3po_aws_guarddduty",
7     "testingscripts_aws_guarddduty"
8 )
```

These logs are a mirror of the findings in the production Security account's GuardDuty interface. These findings are created every time the GuardDuty service detects a threat.

Syslog

```
1 index IN (
2     "aws_syslog",
3     "pci_aws_syslog",
4     "registry_aws_syslog",
5     "mna_aws_syslog",
6     "c3po_aws_syslog",
7     "testingscripts_aws_syslog"
8 )
```

These logs are created by the syslog service running in a GoDaddy AWS Accounts' EC2 instances, including those running as a part of an EKS cluster.

VPC Flow

```
1 index IN (
2     "aws_vpc_flowlogs",
3     "pci_aws_vpc_flowlogs",
4     "registry_aws_vpc_flowlogs",
5     "mna_aws_vpc_flowlogs",
6     "c3po_aws_vpc_flowlogs",
7     "testingscripts_aws_vpc_flowlogs"
8 )
```

These are network metadata logs (like NetFlow). At the time of writing, the 14 fields are:

```
1 scheme_version account_id interface_id src_ip dst_ip src_port dst_port proto packets duration
  start_time_unix end_time_unix vpcflow_action log_status
```

[AWS Documentation here](#)

WAF

```
1 index IN (
2     "aws_waf",
3     "pci_aws_waf",
4     "registry_aws_waf",
5     "mna_aws_waf",
6     "c3po_aws_waf",
7     "testingscripts_aws_waf"
8 )
```

These logs contain data logged by the Web Application Firewall (WAF) that protects certain resources in the AWS Account. The default protected resources are API Gateways and Load Balancers. This includes the default policies set by the Firewall Management Service (FMS), and custom rules set by each teams using WAFV2Regional.

Accessing the Logs

Splunk

Only the most recent 90 days of logs are stored in Splunk

Prerequisites

- Access to either
 - [Splunk Core](#) or
 - [Splunk Enterprise Security \(ES\)](#)
- SPL knowledge

Procedure

0. Log in to a Splunk Instance
1. Search the appropriate index query above

AWS Security Account

Data is stored in the Security account(s) are stored for a maximum of two (2) years unless directed otherwise by regulatory/compliance requirements.

See [Using Athena](#) for the procedure

Using Athena to Search Historical Logs

- [Background](#)
- [Prerequisites](#)
- [Procedure](#)
- [Support](#)

Background

Sometimes, it is required to search longer than the past 90 days of data (which is the default retention period for logs in Splunk).

The easiest* way to do this is using AWS Athena, a service that allows us to search logs stored in S3 (up to two (2) years, unless directed otherwise by policy or regulatory requirements).

Prerequisites

- Access to either:
 - `global-security` account in each AWS Organization (Ops or higher privileged role)
 - `MasterSecurity` role in each AWS Organization's Management Account
 - One of the following roles in the GoDaddy C3PO Organization Management Account
(`GoDaddy AWS - C3PO` Okta chiclet; account ID `146929684086`)
 - `GD-SecurityAdminAccessRole`
 - `GD-SecurityReadOnlyAccessRole`
- A working understanding of SQL (structured query language)

Procedure

0. Log in to the appropriate Security account
1. Navigate to the AWS Athena console in the `us-west-2` region (or wherever the log data is being stored – Athena can only search S3 buckets in the same region. At the time of writing, this is `us-west-2`)
2. Select the `manual_audit` WorkGroup (or create a new WorkGroup for the Incident, if required)

The screenshot shows the Amazon Athena Query Editor interface. At the top, a green banner indicates "Workgroup switched to manual_audit." The "Workgroup" dropdown menu on the right shows "manual_audit" is selected. The main area displays the "Data" tab with "AwsDataCatalog" as the data source and "default" as the database. Under "Tables and views", there is a list of tables and views, including "cloudtrail_logs_godaddy_aws_logs_nonprod" and "compliancetrails". The "Results" section below shows a search bar and a message: "No results Run a query to view results".

3. Select the **manual** database

The screenshot shows the Amazon Athena Query Editor interface. The "Database" dropdown menu in the "Data" tab has "manual" selected. The list of tables and views now includes "all_appseclogs", "appseclog_o655_post_cutover", "appseclog_onprem", "aws_config_configuration_snapshot", "cloudtrail_audit_productsec_3062", "onprem_all", "ssocloudprod_manual", "ssoprod_manual", "vpc_flow_logs", and "vpc_flow_logs_14". The "Results" section remains empty with the message: "No results Run a query to view results".

4. To determine which partitions and columns are available for the Table, use the “Generate table DDL” option in the pop-up menu (click on the three dots to the right of the Table name):

The screenshot shows the AWS Management Console with the Athena service selected. In the main area, a context menu is open over a table named 'all_appseclogs'. The 'Generate table DDL' option is highlighted. Other options visible in the menu include 'Run Query', 'Preview Table', 'Load partitions', 'Insert', 'Insert into editor', 'Manage', and 'Delete table'. The left sidebar shows a list of tables under the 'manual' database, including 'all_appseclogs', 'appseclog_o365_post_cutover', 'appseclog_onprem', 'aws_config_configuration_snapshot', 'cloudtrail_audit_productsec_3062', 'onprem_all', 'ssocloudprod_manual', 'ssoprod_manual', 'vpc_flow_logs', and 'vpc_flow_logs_14'. The bottom right corner of the screen displays the copyright notice '© 2023, Amazon Web Services, Inc. or its affiliates.' and links for 'Privacy', 'Terms', and 'Cookie preferences'.

a. The result will be the DDL (Data Description Language) Query used to create the table

The screenshot shows the same Athena Query editor interface. The query results pane now displays the generated DDL code for the 'all_appseclogs' table:

```

1 SHOW CREATE TABLE `all_appseclogs`;
SQL Ln 1, Col 1
Run again Explain Cancel Clear Create
Query results | Query stats
Completed
CREATE EXTERNAL TABLE `all_appseclogs` (
    `date` string COMMENT 'from deserializer'
)
PARTITIONED BY (
    `product` string,
    `env` string,
    `year` int,
    `month` int,
    `day` int,
    `hour` int
)
ROW FORMAT SERDE
    'com.amazonaws.glue.serde.GrokSerDe'
WITH SERDEPROPERTIES (
    'input.format'='%(GREEDYDATA)log'
)
STORED AS INPUTFORMAT
    'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
    'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
    's3://godaddy-aws-logs-replica-non-pci-us-west-2/appseclogs/$({platform})/${env}/${year}/${month}/${day}/${hour}'
TBLPROPERTIES (
    'compression.type'='gzip',
    'projection.day.digits'='2',
    'projection.month.digits'='2',
    'projection.day.range'='01,31',
    'projection.day.type'='integer',
    'projection.enabled'='true',
    'projection.year.digits'='4',
    'projection.env.values'='dev,dev-private,test,staging,qa,prod,clio',
    'projection.hour.digits'='2',
    'projection.hour.interval'='1',
    'projection.year.interval'='3',
    'projection.year.type'='Integer',
    'projection.month.digits'='2',
    'projection.month.interval'='1',
    'projection.month.range'='01,12',
    'projection.month.type'='Integer',
    'projection.product.type'='Injected',
    'projection.year.digits'='4',
    'projection.year.interval'='1',
    'projection.year.range'='2020,9999'
);
  
```

The status bar at the bottom indicates 'Time in queue: 294 ms' and 'Run time: 685 ms'.

b. The partitions available are listed under the **PARTITIONED BY** block. The data columns are specified by in the **TABLE** block (in the above example, the lines between the parentheses immediately following **CREATE EXTERNAL TABLE** ``all_appseclogs``)

- While it is usually the case that the partition names are self-explanatory, you may also need to consult the **TBLPROPERTIES** section to determine which values are valid for the partition.

- ii. If that is still not clear, or the type `projection.<partition_name>.type` is **injected** (such as for partition `product` in the above example), you will need to consult the S3 bucket and S3 prefix specified in the `LOCATION` field to determine valid values.
5. If the required table is not present, log in to a higher-privileged account, if necessary, and use the following guide(s) to create it:
- Notes:
 - not all AWS logs are queriable using Athena
 - syntax for AWS Athena: [DML queries, functions, and operators - Amazon Athena](#)
 - AWS Service Logs:
 - CloudTrail: [Query AWS CloudTrail logs - Amazon Athena](#)
 - WAF: [Query AWS WAF logs - Amazon Athena](#)
 - VPC Flow: [Query Amazon VPC flow logs - Amazon Athena](#)
 - GuardDuty: [Query Amazon GuardDuty findings - Amazon Athena](#)

Support

Please contact [@Kedwin Chen](#) if you have questions.

Hosting VS Non-Hosting Content

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Purpose](#)
- [Hosting Servers](#)
- [Hosting Content](#)
- [Endpoints Non-Hosting Servers](#)
- [Non-Hosting Servers](#)
- [Team Responsibilities](#)

Purpose

| | |
|----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Detections and Monitoring• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | 2023-08-31 by @David Hernandez |
| Requests for Updates | By Email - ir@godaddy.com |

Purpose

This document was created to assist in understanding how different security units handle and segregate customer vs non-customer alerts.

Most importantly, GCSO will respond to Hosting servers events but not Hosting Content. For example:

If the threat is found in a hosting server and the following directory

/vz/root/29aba240-5ff2-42ad-971f-

113ba75954f4/home/customer/malware GCSO will not respond to the event

If the threat is found on a hosting server and the following directory

/home/employeename/malware GCSO will respond to the threat.

Hosting Servers

For the purposes of security operations, a hosting server will be a server containing **active** customer content in following GoDaddy services: cPanel, VPS (Virtuzzo), Managed Word Press (MWP). Below are some hosting server groups that can quickly determine customer hosting servers.

| Server Group | Business Unit/Service |
|--------------------|-----------------------|
| VZ-CLOUD | Virtuozzo |
| SRE-Hosting | cPanel & MWP |
| org-gpe-uk-north | Heart Internet |
| SRE-cPanel | cPanel |
| org-gpe-emea-cloud | Host Europe |
| DEV-Plesk Platform | Plesk |
| org-gpe-de-south | Domain Factory |
| org-gpe-uk-south | TSOHOST |
| org-sre-emea | Host Europe? |
| org-gpe-de-west | Host Europe |

Hosting Content

Hosting content are server directories or spaces which customers have access to modify.

Hosting content also includes customer backups even if the customer is not able to access the backup.

Below are Regex rules used to filter for customer content. You may also find the most up to date rules in the splunk macro “isHostedContent”.

| | |
|---|--|
| ^/home/\w*/public_html | cPanel HTML Root Paths |
| ^/home/\w*/mail | cPanel Mail Paths |
| ^/home/\w*/(\w*\.\{1,\}\w*/ | cPanel Alias Domains Paths |
| ^/home/\w*/domains/([\w\-\"]*\.\{1,\}\w*/ | cPanel Alias Domains Alternate Paths |
| ^/home/\w*.*?/public_html/ | Other HTML Doc Roots |
| ^/home/[a-zA-Z0-9]\{12\}/.+ | cPanel HTML Root Paths |
| ^/vz/root/[\w\-\"]*/ | Virtuozzo Container Paths |
| ^/home/.*/wp-(content includes)/ | WordPress Content |
| ^/var/lib/docker/volumes/.+/html/.+ | MWP HTML Root Paths |
| ^/home/sites/\d/w/[\w\.\"]*/public_html | 123Reg Customer NAS Paths |
| ^/mnt/nas/tmp/mailapiAttachments/* | Customer Email Attachments |
| \Device\HarddiskVolume\d\PleskVhosts\.\.+ | Customer Plesk Content |
| ^/data/kunden/.+ | Domain Factory Customer Space |
| ^/var/backups/even/.+ | Heart Internet and 123 Reg Shared Hosting Customer Backups |
| ^/var/backups/odd/.+ | Heart Internet and 123 Reg Shared Hosting Customer Backups |
| ^/data/tarifchange/.+ | Customer Email Files Transfer |
| ^/kunden/[0-9]\{6\}_[0-9]\{5\}/.+ | Customer Environment Heart Internet |
| ^/kunden/.+/wp-content/.+ | Customer Environment Heart Internet |
| ^/data/temp/[0-9]\{5,6\}/u[0-9]\{5,6\}/.+ | Customer Environment Heart Internet |
| /var/is/attachments/[0-9]\{5\}/[0-9]\{9\} | Customer Email |
| /home/cluster-sites/[0-9]\{1\}/.+./public_html/.+ | Customer sites |
| /home/cluster-sites/[0-9]\{2\}/.+./public_html/.+ | Customer sites |

| | |
|---|------------------|
| /backup/tapes/raid001/restore_temp_data/[0-9]{6}/.+www/wp/.+ | Customer Backups |
| /mnt/nas/tmp/webmailAttachments/[a-z]{1}/[a-z]{1}/[a-z]{1}/.+ | Customer Backups |

Endpoints Non-Hosting Servers

Endpoints are nodes with the group name “ENG-Desktop Engineering”.

Non-Hosting Servers

Non-Hosting Servers all remaining servers that do not meet the criteria above.

Team Responsibilities

GCSO is responsible for triaging security alerts in all spaces possible except customers'. To segregate the two places we have created a couple definitions to assist with understanding each team's responsibilities.

| Alert Space | Responsible Team |
|---|------------------|
| Alert triggered on Hosting Server but not Hosting Content | GCSO |
| Alert triggered on Hosting Server AND Hosting Content | CSOC |
| Alert triggered on Non-Hosting Server | GCSO |
| Alert triggered on Endpoints | GCSO |

Common Customer Environments

Table of Contents

- [Table of Contents](#)
- [cPanel](#)
- [VPS 10](#)
- [Managed WordPress \(MWP\)](#)
- [Plesk](#)

cPanel

cPanel uses CaigFS to contain Customers, Customer should not be able to write to directories outside of their own.

`^/home/\w*/public_html`

VPS 10

VPS10 is Heart's Internet (EMEA Brand) managed VPS platform running Plesk web hosting

Managed WordPress (MWP)

Plesk

Plesk does not have a Cage this you might find customer writing to directories outside of their own. Customers should NOT be writing system directories or other customer directories. You might find customers writing to the temp directories

Defender for O365: Email Un-Quarantine Requests

1. Table of Contents

- 1. Table of Contents
 - 1.1. Process Summary
 - 1.2. Process-Specific Definitions
- 2. Process Workflow
- 3. Process Outline and Details
 - 3.1. General Outline
 - 3.2. Process FAQs
 - 3.2.1. What types of business justifications are appropriate for releasing a malicious email to the requestor?
- 4. Resources and Definitions
 - 4.1. Internal Resources

1.1. Process Summary

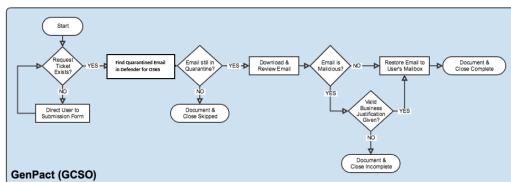
This process provides direction for the handling of un-quarantine requests generated by users who believe that a message has been incorrectly flagged and covers the following use cases:

- User requests assistance with a quarantined message via direct communication.
- User submits a request for assistance with a quarantined message.

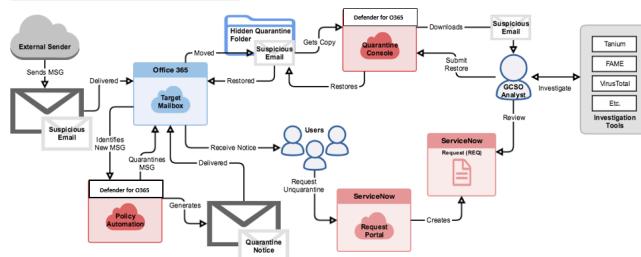
1.2. Process-Specific Definitions

- **Microsoft 365 Defender:** A Microsoft product currently providing security filtering to the GoDaddy Office365 tenant.

2. Process Workflow



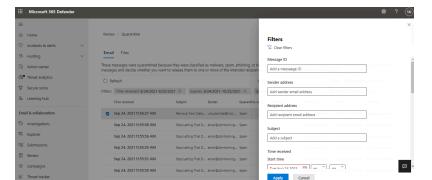
UnQuarantine - Basic Architecture



3. Process Outline and Details

3.1. General Outline

1. User requests an email to be un-quarantined.
2. Does a ticket exist?
 - a. If NO, direct to the [Defender for O365](#) form.
3. Log into the [Microsoft 365 Defender](#) and navigate to the [Quarantine](#) tab.
 - a. Locate the email using the provided quarantine details. Generally the best filters are Sender, Recipient or Subject.

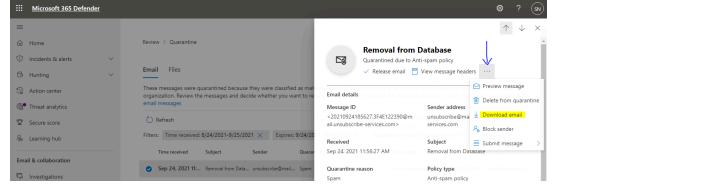


b. Make sure while searching for emails, Time received Start time window should be increase to fetch the email.

4. Does the quarantined email still exist?

a. If NO, close the ticket using the Close Skipped option. Record any findings.

5. Select the email, click on the three dots and select "Download email" option.



6. Review the email to determine if it is malicious.

a. If YES, did the user provide an appropriate business justification to obtain the message?

i. If YES, continue to Step 7.

ii. If NO, close the ticket using the Close Incomplete option. Record any findings.

7. If appropriate, use the "Release email" option to un-quarantine the email.

8. Close the ticket using the Close Complete option. Record any findings.

Note: The Exchange Admin group will handle issues related to **Defender for O365**. To engage O365 Admins they require a Jira intake process. Any such request that came up via Slack channel, GCSO needs to create Jira issue on behalf of the requestor until further update from O365 Admins as they are still working on their official way to engage. Also no SNOW incident needed at this moment.

Example:

- Release an email that we can't find.
- Adding email sender to allow list so it doesn't get flagged as SPAM.
- Create block for specific URL/Site.
- Primary contacts for Defender for O365 Admins are:
 - **Jason Liu**
 - **Ross Sheridan**

Additional Info: Any Spam emails which gets quarantined, it stays in quarantine folder for 30 days and can only be retrieve/restore within 30days of window. Any email which gets quarantined due to suspicious attachments, it can only be retrieve/restore within 15 days.

3.2. Process FAQs

3.2.1. What types of business justifications are appropriate for releasing a malicious email to the requestor?

In general, we will release malicious messages if the requestor has a job role or function that requires them to view malicious messages AND they are unable to use a centralized mailbox for this purpose. Some examples are:

1. Users who review malicious content reported by customers only on an occasional basis.
2. Users who receive reports that occasionally contain references to malicious content.
3. Users who are investigating a one-time occurrence.

NOTE: Users who have a role which would allow for a centralized mailbox (Abuse, Security, etc.) should not be using their personal mail accounts for this purpose.

4. Resources and Definitions

4.1. Internal Resources

- Microsoft 365 Defender Console - <https://security.microsoft.com/quarantine?viewid=Email>
- ServiceNow Requests - https://godaddy.service-now.com/gdsp?id=gd_sc_cat_item&sys_id=ce126c833753d380eb8163d2b3990e59

Email DLP Incident

1. Table of Contents

- [1. Table of Contents](#)
 - [1.1 Process Summary](#)
- [2. Process Workflow](#)
- [3. Process Outline and Details](#)
 - [General Outline](#)
- [3. Troubleshooting](#)
 - [Permissions](#)

1.1 Process Summary

This process provides direction for handling Email DLP Incidents. The process can be used, but not limited to the following scenarios:

- Insider threat: A malicious actor with intent to exfiltrate confidential data.

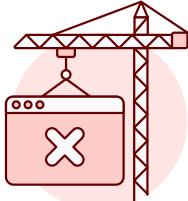
| | |
|-----------------------|----------------------------|
| Responsible Team | Enterprise Security |
| Process Owner | David Hernandez |
| Last Review Date | 2022-07-06 |
| Escalation Contact(s) | Paul Mueller & Dave Allmon |

2. Process Workflow



Oops, Diagram Unavailable

This diagram cannot be displayed. It may have been moved, deleted, or you do not have permission to view it.



Oops, Error 500!

Diagram Unavailable

Our system is currently under maintenance. Reach out to your administrator for a fix.



You have an unpublished draft.

3. Process Outline and Details

| Outbound Email DLP | |
|-------------------------|--|
| Assignment Group | OPS-GCSO |
| Source | O365 Compliance |
| Category | Confidential Personal Identity Data Exposure |
| Title | Email DLP : <i>Subject of the reported email</i> |
| State | Analysis |
| Business Impact | 3 - Non - critical(Auto filled) |
| Severity | 2 - Medium(Auto filled) |
| Priority | Critical |
| Alert Sensor | Microsoft Email DLP Compliance |

General Outline

1. Alert is received via:
 - a. Via employee/customer/SIEM.
 - b. Microsoft DLP Alert, ticket is automatically created in the SIEM.
2. Review Email
 - a. Proceed to the following link <https://security.microsoft.com/>
 - b. Click the "Incident & alerts" →"Alerts" tab.
 - c. Add the filters "Service/detection sources: Microsoft Data Loss Prevention" and "Policy: PCI Data Security Standard (PCI DSS) IR"
 - d. Select "Open alert page" (A new tab will open)
 - e. Select "Events", The will open a panel which contains details about the alert. Most importantly, it will contain the location of the sensitivity info.
 - f. At the bottom of the details panel, select "Actions" then "Download email" for a full analysis. (If the actions button is not visible, you will need to maximize the details pane.)

The screenshot shows the Microsoft Defender Alerts interface. On the left, a navigation sidebar includes Home, Incidents & alerts (selected), Hunting, Actions & submissions, Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, Overview, and Attack surface. The main area is titled 'Alerts' and displays a list of detected incidents. A filter bar at the top allows for export, search, and alert management. The alert list shows entries from Aug 21, 2024, to Jul 30, 2024, all categorized as 'New'. Each entry includes a timestamp, status (New), detection source (DLP policy), and tags (External user risk). A specific alert for Aug 21, 2024, is highlighted with a red lightning bolt icon and the subject 'Airfare Data Actuals - June - (07/23/2024 - 08/20/2024)'. To the right of this alert, there are options to 'Open alert page', 'Manage alert', 'Link alert to another incident', and 'Classify alert'. Below the alert list, there is an 'INSIGHT' section with a link to 'Quickly classify this alert' and a note about improving alert accuracy. At the bottom of the alert list, there is a link to 'View incident page'.

Alerts

Status: New, In progress | Service/detection sources: Microsoft: Data Loss Prevention | Policy: PCI Data Security Standard (PCI DSS) IR

Filter set:

- First activity
- Status
- Alert name
- Detection source
- Tags

| Date | Status | Detection source | Tags |
|-----------------------|--------|--|--------------------|
| Aug 21, 2024 10:44 AM | New | DLP policy (PCI Data Security Standard (PCI DSS) IR matched) | External user risk |
| Aug 20, 2024 9:46 AM | New | DLP policy (PCI Data Security Standard (PCI DSS) IR matched) | External user risk |
| Aug 16, 2024 10:40 AM | New | DLP policy (PCI Data Security Standard (PCI DSS) IR matched) | External user risk |
| Aug 14, 2024 5:59 PM | New | DLP policy (PCI Data Security Standard (PCI DSS) IR matched) | External user risk |
| Aug 12, 2024 10:52 AM | New | DLP policy (PCI Data Security Standard (PCI DSS) IR matched) | External user risk |
| Aug 2, 2024 11:00 AM | New | DLP policy (PCI Data Security Standard (PCI DSS) IR matched) | External user risk |
| Jul 31, 2024 1:20 AM | New | DLP policy (PCI Data Security Standard (PCI DSS) IR matched) | External user risk |
| Jul 30, 2024 3:57 PM | New | DLP policy (PCI Data Security Standard (PCI DSS) IR matched) | External user risk |

Alerts > DLP policy (PCI Data Security Standard (PCI DSS) IR matched for email with subject (Airfare Data Actuals - June - (07/23/2024 - 08/20/2024))

Part of incident: DLP policy (PCI Data Security Standard (PCI DSS) IR matched for email with subject (Airfare Data Actuals - June - (07/23/2024 - 08/20/2024)) involving one user. [View incident page](#)

Alert story

What Happened

Manoj A. Venkat (Vendor) sent an email with subject "Airfare Data Actuals - June - (07/23/2024 - 08/20/2024)" with sensitive content.

Policy description

Helps detect the presence of information subject to PCI Data Security Standard (PCI DSS), including information like credit card or debit card numbers.

[View policy \(tab out\)](#)

Related events

| Event | User | Time detected | Location |
|--|--------------------|------------------------|----------|
| Sensitive info in email with subject 'Airfare Data Actuals - June - (07/23/2024 - 08/20/2024)' | mvenkat@godaddy... | Aug 21, 2024 10:44 ... | Exchange |

Sensitive info in email with subject 'Airfare Data Actuals - June - (07/23/2024 - 08/20/2024)'

External user risk

Full Screen | Go Hunt | Actions | Download email F

Details **Sensitive info types**

Event details

ID: 16f87b71-b4cd-4723-8ee7-d61feb9d06ad | Location: Exchange

Time of activity

Aug 21, 2024 10:44 AM

Impacted entities

3. Determine which category the DLP Incident falls under

- Business:** Employee is performing business operations such as: Corporate payments or Business Travel.
- Non-GoDaddy Originating:** The employee is replying to an email which contains PANs in the first email sent.
- Corporate Payments:** Employee is paying for catering or business venue
- Testing:** Developer shares code which contains a test credit card.
- Training:** Training documentation is sent personal email, Will usually contain test emails
- Personal Use:** Employee paying for personal item/services with GoDaddy Email
- SPAM/IsItBad:** Email sent to "junk@office365.microsoft.com" or "isitbad@godaddy.com" (Handle isisbad emails using the phishing process)
- DLP Blocked:** Email was blocked by a different DLP policy as part of a pilot program (6/20/23), contact [@ Paul Cox](#) to confirm.
- No subject or Context:** An email containing no relevant information other than PANs
- Clear Malicious Intent:** Email indicating corporate retaliation or other Malicious Intent
- Personal Note:** Email sent to suspected personal email such as a gmail/outlook which contains first or last name in the address.

① Important

Under no circumstance is GCSO to engage the user to validate this activity. If GCSO is not able to determine the classification for the email, they shall escalate this alert to Monitoring or IR.

4. Escalate or Close

- a. (GCSO) Close the ticket as a false positive for categories 3a-h and escalate ticket to IR for 3i-k.
- b. Make sure to delete the email from your computer after categorization.

3. Troubleshooting

Permissions

1. If you are unable to download the email, you will need to create a content search to retrieve the email manually from the users mailbox.
<https://compliance.microsoft.com/contentsearchv2>
2. Unable to download email error: "You require the role 'Preview' to download the email. Please contact your administrator"
To resolve this issue, you will need to be in the appropriate group for your team. Please see your team's on-boarding page for details.

Employee Phishing Incidents

Table of Contents

- Table of Contents
- General Information
 - Process Summary
 - Process-Specific Definitions
- Process Workflow
- Process Outline and Details
 - Incident Response Guide
 - General Outline
- Analysis
 - Review basic visible headers
 -
 - Review Message Body
 - Reviewing Attachments
 - Reviewing URLs
 - Malicious URL Clicks
 - Raw Headers
 - IOC Discovery and Expanding Scope
- Parameters For A Safe Email
- Containment
- Eradicate
- Recovery
- Post-Incident Activity
- Process Details
 - Finding a Domain's Registrar and Host
 - Defender
 -
 - Advance Phish URL Detection
 - IOC Containment Process
 - Eradicate
- Process FAQs
 - What if a C3 Rep Reports a Phish Targeting a Customer?
 - What is a Business Email Compromise (BEC) attempt?
- Resources and Definitions

General Information

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @David Dubois (Deactivated) |
| Last Review Date | 2022-11-01 by @David Hernandez |
| Escalation Contact(s) | <ul style="list-style-type: none">• @Juan Bustamante• @David Downs• @David Hernandez |
| Requests for Updates | By Email - ir@godaddy.com |

Process Summary

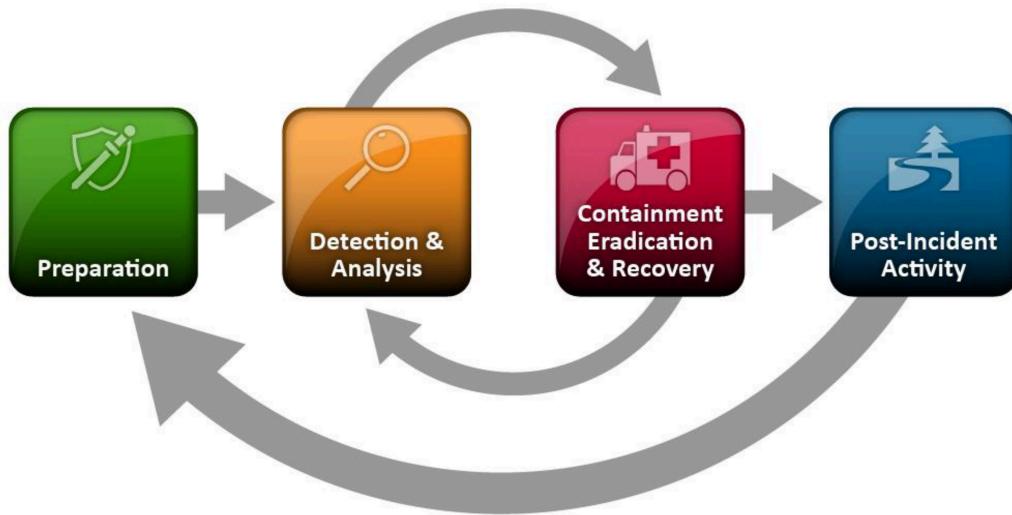
This process provides direction for the analysis and remediation of user reported employee-targeted phishing attempts and outlines the general process guidelines to be followed by Incident Response analysts. A summary of applicable use cases for this process are as follows:

- Phishing reports generated by user-initiated emails to IsItBad@GoDaddy.com
- Phishing reports submitted with the Report Phish Button

Process-Specific Definitions

- **Impersonated Individual/Group:** Impersonated Individual or Group refers to who the phishing email is pretending to be. This can be a company, an organization, or a single user.
- **Targeted Group (if specific):** Targeted group is an optional field that refers to the GoDaddy group that received the emails, often grouped by department.
- **Type of Attack:** Type of Attack refers to what classification the malicious email falls under, as not all malicious and actionable emails that get reported to IsItBad@GoDaddy.com are strictly phishing emails—some may contain a malicious script or be impersonating an SLT/XLT member.

Process Workflow



Process Outline and Details

Incident Response Guide

| Employee-Targeted Phishing | |
|----------------------------|--|
| Assignment Group | OPS-GCSO |
| Source | Email |
| Category | Phishing(Auto filled) |
| Title | User Reported Phishing : <i>Here comes the subject of the reported email</i> |
| State | Analysis |
| Business Impact | 3 - Non - critical(Auto filled) |
| Severity | 2 - Medium(Auto filled) |
| Priority | Low |
| Alert Sensor | User Reported Phish |

General Outline

As a general guideline, the goal of a phishing report is to prove it is malicious until it no longer can be proved.

1. Report is received:
 - a. Via IsItBad@GoDaddy.com, ticket is generated by automation, and the reporter is automatically thanked.
 - b. Phishing reports submitted with the Report Phish Button
2. Review Visible Headers
3. Review Body
4. Review URLs
5. Review Attachments
6. Review Raw Headers
7. Expanding IOC scope
8. Block IOCs
9. Search and Destroy
10. Recover and Post Review

Analysis

In the analysis phase, we will attempt to identify malicious emails using the following techniques.

Review basic visible headers

1. Review header from address
 - a. Assuming the domain is not spoofed (Discussed later), you may check sender domain email reputation here "https://talosintelligence.com/reputation_center/email_rep"
2. GoDaddy Banners.
 - a. GoDaddy adds a tag to all external emails. It is important to know as internal emails and authorized will not have this tag.
"Caution: This email is from an external sender. Please do not click links or open attachments unless you recognize the sender and know the content is safe. Forward suspicious emails to isitbad@."
3. Typosquatting
 - a. Take a close look at the sender from domain, be sure that this is not made to look like any other site.

Review Message Body

- Is the body related to anything in GoDaddy's Business line?
- Is the email sent with high urgency?
- Subject: Contains suspicious titles such as: "Remittance Advice"
- Are non-conventional financial terms used such as gift cards, bitcoin, or lottery?
- Email contains password protected compressed file ie .zip and password in the body?
- Email imitates shipping solutions UPS, Fedex, DHL, Costco shipping center
- Email imitates common phishing brands such as IRS, PayPal, Apple, DocuSign
- Email is non-personal such as "dear user"
- Email starts conversation as if they have spoken before such as, "followup with our previous conversation...".
- Email contains suspicious phone number, (typically represented as support number)

Reviewing Attachments

1. Hash file to review reputation.
 - a. Use [VirusTotal](#), Joe's Sandbox or other virus-analysis site to look up a particular file by Hash. (NOTE: Do not submit files to these sites, unless approved by peer review)
2. Review attachment,
 - a. Using a sandbox, review the email using the same analysis techniques as in the "Review Message Body" section.
 - b. If any urls are present, review the attachment using the same techniques found in the "Reviewing URLs" section.
3. Use corporate tools such as Defender/Tanium/EDR to determine if the file has been downloaded to any machines
 - a. If YES, determine if the activity was blocked.
 - i. If NOT and executed (exe), escalate to IR.
 - ii. If NOT and not an executable, follow [System Investigation](#) process.
 - b. Include your IOCs in the ticket for use by the next analyst or future review if not included already.

Reviewing URLs

1. If the URL is using the TLD "<nam10.safelinks.protection.outlook.com>", decode the URL using <https://www.o365atp.com/>
2. Review URL reputation and Whois
 - a. [Virustotal](#) can also provide a quick url reputation, but lacks whois information.
 - b. <https://www.urlvoid.com> is an alternative to virustotal
3. Review URL Behavior
 - a. Use [UrlScan.io](#) to detect redirects, scripts, active content, and executable downloads
 - b. <https://urlquery.net> Is an alternative. Some Phishing sites, block urlscan.io searches and thus the site may appear as down or clean.
 - c. For documentation purposes, collect a screenshot of the page, regardless of what you believe at this point.
4. Do email url links contain password reset links with no token or extremely short token? View "[Advance Phish URL Detection](#)" for more info.
5. As a last resort, you may add the url to Joe's Sandbox or other sandbox for additional analysis.
6. Determine URL Origin
 - a. Determine where the landing page and any intermediate URL(s) are hosted :
 - i. If hosted at GoDaddy; Report to the [Front of Site Abuse Form](#).
 - ii. If Hosted elsewhere:
 1. Use Security@godaddy.com mailbox to report malicious URL's to respective abuse teams.
 2. Domain Host & Registrar ([whois](#))
 - b. If the message targets GoDaddy-brand (i.e. impersonates GoDaddy) and/or targets GoDaddy customers (not employees):
 - i. Report the Malicious URL to the [Front of Site form](#)
 - ii. Use Phishlabs if its targeting GoDaddy customers or brand
 - iii. Respond to the user with the template [gdphish](#)
 - c. If the message has been generated from an **internal sender** ([GoDaddy.com](#), [MediaTemple.net](#), [Heg.com](#), etc.) → **Escalate to InfoSec Response Team**
7. Exclusions: If the user impacted belongs to the "Fraud Detection" team and the originating process is a web browser, please disregard the alert as this process is part of their daily job duties.

Malicious URL Clicks

- Use [Defender Advance Hunting](#) to Identify users that may have clicked the URL.
- Alternatively, use any other tools at your dispose to search web traffic such as Tanium.
- See [urlvisits](#) for process information.

Raw Headers

1. Review message headers to determine if it's of malicious origin or spoofed.
 - a. Analyze Return Path, Sender IP, Spam Confidence Level(SCL), and DMARC.

IOC Discovery and Expanding Scope

Using the IOCs collected, search for the following globally at least within the last 14 days.

- Sender
- Attachment hash
- Attachment name, if unique
- Subject
- Sender IP
- Determine if any replies have been sent to the sender/reply-to.
 1. If any replies have been seen, take action based on the email content and check with InfoSec Response Team if required

Determine if the email is targeted or a campaign and document in your ticket.

Parameters For A Safe Email

If the analysis techniques above yield no malicious activity, respond to the user with the Not Malicious Template.

- ⓘ If you are unable to classify the email, escalate to a peer or IR.

Containment

Using [Defender Tenant Block/Allow list](#), block available IOCs with a 30 expiration. Only block the IOCs if they are confirmed malicious. **DO NOT** block domains or urls such as godaddy.com or google.com

If the IOC can't be blocked due to business impact, check with IR for advice on how to proceed.

- ⓘ **Identify any potential impact to business before blocking, by searching the IOCs collected globally. Review the IOC Containment Process before continuing.**

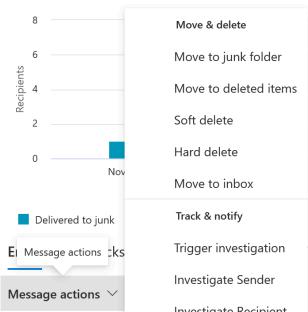
- Block URLs
 - Block Sender or Domain
 - Block Attachment Hash
1. If any malicious URL clicks occurred ([urlvisits](#)).
 - a. If unblocked visits exist, remediate by following the [Employee Compromise Containment](#) process for each user.

- ⓘ **Defender Tenant Block/Allow list**

This list only blocks traffic for email traffic and **not** web traffic.

Eradicate

1. Using the SIR module Search & Delete option, initiate a Purge request for the Content Search.
2. Alternatively, use [Threat Explorer](#) to quarantine the emails in question.
 - a. Search for the relevant emails **without** impacting legitimate ones.
 - b. After a successful search, select all emails in your search.
 - c. Click "Message actions" then "Soft delete"



3. If either solution is not safely possible, reach out to IR for guidance.

Recovery

1. Review the incident in detail to make sure no steps were missed
2. Using the appropriate `nm`, respond to the user with your analysis.

Post-Incident Activity

1. Escalate any process/technical changes that you believe should be made to IR
2. Escalate any interesting or targeted artifacts to IR.

Process Details

Finding a Domain's Registrar and Host

Domain Host & Registrar requires some external checks to find. In general, three steps are needed:

1. WHOIS Lookup on the Domain.
2. A Record DNS Dig on the Domain.
3. WHOIS Lookup on the A Record IP.

There are several tools available to do these lookups, including command line utilities. Here are a few preferred methods:

- Via Command Line using `whois` and `dig` commands.
 - » [Commandline Examples](#)

Domain Whois Example

```
LMIT-DAVIDD:~ ddubois$ whois davedubois.com | grep -Ei 'Registrar|Abuse'
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
registrar's sponsorship of the domain name registration in the registry is
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
Registrars.
```

Domain Dig Example

```
LMIT-DAVIDD:~ ddubois$ dig davedubois.com A | grep -A1 'ANSWER SECTION'
;; ANSWER SECTION:
davedubois.com.      497 IN  A   184.168.221.63
```

IP Whois Example

```
LMIT-DAVIDD:~ ddubois$ whois 184.168.221.63 | grep -Ei 'Organization|Abuse'
Organization:  GoDaddy.com, LLC (GODAD)
Comment:      Please send abuse complaints to abuse@godaddy.com
Comment:      Please send abuse complaints to abuse@godaddy.com
OrgAbuseHandle: ABUSE51-ARIN
OrgAbuseName:  Abuse Department
OrgAbusePhone: +1-480-624-2505
OrgAbuseEmail: abuse@godaddy.com
OrgAbuseRef:   https://rdap.arin.net/registry/entity/ABUSE51-ARIN
RAbuseHandle: ABUSE51-ARIN
RAbuseName:  Abuse Department
RAbusePhone: +1-480-624-2505
RAbuseEmail: abuse@godaddy.com
RAbuseRef:   https://rdap.arin.net/registry/entity/ABUSE51-ARIN
```

Reviewing URL Visits

Defender

- Navigate to [Defender Advance Hunting](#) and paste the code below into your query builder.
- Replace "godaddy.com" with the malicious URL in question

Defender Advance Hunting

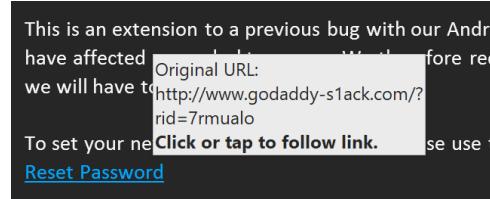
```
let url = "godaddy.com";
search in (EmailUrlInfo,DeviceNetworkEvents,DeviceFileEvents,DeviceEvents, UrlClickEvents)
Timestamp between (ago(30d) .. now())
and (RemoteUrl contains url
or FileOriginUrl contains url
or FileOriginReferrerUrl contains url
or Url contains url
)
```

- Use Question Builder to fill out the fields as follows:
 - **Time Range:** 3 days
 - **Absolute Time Range:** Leave untouched
 - **Treat Inputs as Regular Expressions:** Check
 - **Output only Yes or No:** Uncheck
 - **Max Results Per Host:** 10
 - **Make Stackable / Skip Unique:** Uncheck
 - **Process Path:** Leave blank
 - **Username:** Leave blank
 - **Query:** (?i)[subdomain if applicable].[domain].[suffix].* (Example: (?i)smile.amazon.com.*)
 - **Response:** Leave Blank
 - **Operation:** Leave blank
- When found hits in Tanium, contact the user to get info if he input his credentials.
 - If yes, follow the [Employee Compromise Containment](#) process.

Advance Phish URL Detection

A quick and dirty, phishing URLs can be spotted at times when there is a very short query token. The query token is used to associate a user to an internal account and are commonly only temporary. Due to their dynamic nature, legitimate URLs tend to be extremely long. Be advised, this method is best used for password reset emails and can be easily confused by spam URLs which include trackers as well.

Below is an example of a short query token as well as typo-squatting.



Below is a legitimate and secure password reset or account activation that makes use of a JWT token determined by the "ey" at the end of the final query.

https://falcon.crowdstrike.com/login/activate/eyJhbGciOiJSUzI1NiIsImtpZCI6Ikp2amttQ3qwdjlpYUw5cmx6ODIVb3hzUVZGYmVYdHlWEVtQ1ktN3lQVuILCJ0eXAiOiJKV1QiQ.eyJpc3MiOiJzbGF5ZXJuYmV0YS5iYXJiLmV5cmllLmNs3VkiIwic3ViIjoiYkdpODJnamZDbUdhc2NoRm9hQ0tDbTjnTxdrPSIsImF1ZCI6WyJjb25maXJtI0sImV4cCI6MTY2NTA5NjE5OSwibmJmIjoxNjY1MDA5Nzk5LCJpYXQiOjE2NjUwMDk3OTksImp0aSI6IjQ5ZGM3YmI2LTJiZTkNGEwNy04MjZlThiNjk0OWY2MmQyZiJ9.MyjpGyZSUA2N_onrqORnLk1nNEO7wOUANoWzN-kzwCUUI704czWNMN7QRaSmuYrWTzgNk1sSNPSREzHNuOBzdrj2cTPWxjtIEJFYtoXHkc8J-4xeWPiZ-HD-TJs-IkwxQkMiTxtWO0fDqU74bC0PrJeSJ1AAOYXRUqb5OHHWLycg9glpgtTMvO09tfQAW05_HYvmYdj2MrMyGQSbmbNotarR_g1fG3gM3dTWzEFFd-zNmQgIj3QyLLZbHm-kdmgRmKXD3bb1kYpUchBnAtP7apMQioUVZd0kDlrtPHurCAzC13edDYrPM0m7iaKRsa9nMOBuF2TjhTqE-5NTg?session_source=slayer

IOC Containment Process

Before you continue, use [Threat Explorer](#) to search for the IOC you are about to block within the last 30 days. Be sure that all results are malicious and no business will be impacted upon containment.

1. Navigate to the [Tenant Allow/Block List](#) site
2. Select the appropriate IOC Tab (ie:Domains,URLs,Files)
3. Click the "Block" button
4. Enter the IOC details
5. Select Remove block after 30 days
6. Enter INC # in the "optional note" section
7. Click "Add"

Tenant Allow/Block List

Domains & addresses Spoofed senders UR

Block external email addresses or domains to prevent com

+ Block

Block domains & addresses

Domains & addresses

Maliciousdomain.com

Remove block entry after

30 days

Optional note (100 characters max)

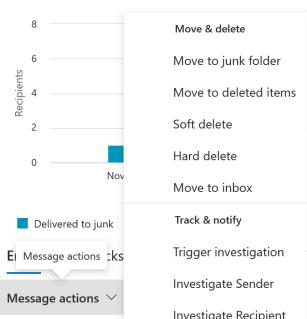
<Enter Incident Number>

77 characters left

Add Cancel

Eradicate

1. Using the SIR module Search & Delete option, initiate a Purge request for the Content Search.
2. Alternatively, use [Threat Explorer](#) to quarantine the emails in question.
 - a. Search for the relevant emails **without** impacting legitimate ones.
 - b. After a successful search, select all emails in your search.
 - c. Click "Message actions" then "Soft delete"



Process FAQs

What if a C3 Rep Reports a Phish Targeting a Customer?

Occasionally, C3 reps will send phishing emails targeting customers, especially those impersonating GoDaddy, to IsItBad@GoDaddy. IsItBad@GoDaddy is reserved solely for suspicious emails targeting GoDaddy employees. Phishing reports targeting customers are handled by a different team. To report those, submit a ticket using the [Front of Site form](#).

What is a Business Email Compromise (BEC) attempt?

Business Email Compromise (BEC) refers to a body of social engineering attempts in which the Threat Actor (TA) attempts to impersonate a member of the targeted company/organization in order to either obtain sensitive data or, most often, convince the target to perform a transfer of funds to an account controlled by the TA. Most often these are initiated with a communication to the user that will not include a malicious hyperlink or attachment, but rather will appear as an urgent request from the spoofed member. Although the origins of this type of attack refer to the compromise of an internal account to send this mail, many recent cases use a spoofed (non-internal) address. Some additional resources for understanding BEC can be found here:

- [https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-\(bec\)](https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec))
- <https://info.phishlabs.com/blog/phishing-attack-breakdown-1-bec-scams>

Resources and Definitions

Internal Resources

- Content Search - <https://protection.office.com/?ContentOnly=1#/contentsearchbeta>
- Block/Allow Tenant list <https://security.microsoft.com/tenantAllowBlockList?viewid=Sender&tid=d5f1622b-14a3-45a6-b069-003f8dc4851f>
- Defender Advance Hunting
- [Threat Explorer](#)
- Message Trace - <https://protection.office.com/#/messagetrace>
- Tanium - <https://tanium.int.godaddy.com>
- Front of Site Abuse Form - <https://supportcenter.godaddy.com/AbuseReport>

DCU Contacts

Digital Crime Unit (DCU-ENG)

• SLACK: #dcueng

- Internal Email: DCUEng@GoDaddy.com
- Public Email: Abuse@GoDaddy.com

External Resources

- Google Safe Browsing (Firefox, Chrome & Safari) - https://safebrowsing.google.com/safebrowsing/report_phish/?hl=en
- Anti-Phishing Work Group (APWG) - <https://antiphishing.org/report-phishing/>
- Trend Site Safety Center (WRS) - <https://global.sitesafety.trendmicro.com/index.php>
- URLQuery - <https://urlquery.net/>
- https://talosintelligence.com/reputation_center/email_rep
- <https://www.o365atp.com/>

Communication Templates

Standard Templates

Response to Reporter - IsItBad Report - Classification: Smishing

<https://godaddy-corp.atlassian.net/wiki/spaces/DETECTMON/pages/edit-v2/3708991102#Response-to-Reporter---IsItBad-Report---Classification%3A-Smishing>

Response to Reporter - IsItBad Report - Classification: Not Malicious

<https://godaddy-corp.atlassian.net/wiki/spaces/DETECTMON/pages/edit-v2/3708991102#Response-to-Reporter---IsItBad-Report---Classification%3A-Not-Malicious>

Response to Reporter - IsItBad Report - Classification: SPAM

<https://godaddy-corp.atlassian.net/wiki/spaces/DETECTMON/pages/edit-v2/3708991102#Response-to-Reporter---IsItBad-Report---Classification%3A-SPAM>

Response to Reporter - IsItBad Report - Classification: Phish

<https://godaddy-corp.atlassian.net/wiki/spaces/DETECTMON/pages/edit-v2/3708991102#Response-to-Reporter---IsItBad-Report---Classification%3A-Phish>

Response to Reporter - IsItBad Report - Classification: Legit Communications

<https://godaddy-corp.atlassian.net/wiki/spaces/DETECTMON/pages/edit-v2/3708991102#Response-to-Reporter---IsItBad-Report---Classification%3A-Legit-Communications>

Response to Reporter - IsItBad Report - Classification: Malware

<https://godaddy-corp.atlassian.net/wiki/spaces/DETECTMON/pages/edit-v2/3708991102#Response-to-Reporter---IsItBad-Report---Classification%3A-Malware>

Automation Template

Automated Response to Reporter - Not Malicious

Thank you for your recent isitbad submission.

Email Reported:

Subject: ([[subject]])

We have investigated the email and determined that it is not malicious as it does not contain any malicious content. If you were not expecting this email, please delete it from your inbox. No further actions are required from you at this time. If you believe this classification is incorrect, please respond to this email with your concern.

Thanks again for being vigilant in reporting suspicious emails.

- Global Cyber Security Operations

Automated Response to Reporter - GoDaddy Customer Malicious

Thank you for your recent isitbad submission.

Email Reported:

Subject: ([[subject]])

Our automation has reviewed the message submitted and determined it is **malicious**. In the near future, this message will be deleted from your mailbox. No further actions are required from you at this time. If you believe this classification is incorrect, please respond to this email with your concern.

Thanks again for being vigilant in reporting suspicious emails.

- Global Cyber Security Operations

Automated Response to Reporter - GoDaddy Customer Spam

Thank you for your recent isitbad submission.

Email Reported:

Subject: ([[subject]])

Thank you for your most recent isitbad submission. Our automation has reviewed the message submitted and determined it is spam and non-malicious. No further actions are required from you at this time. If you believe this classification is incorrect, please respond to this email with your concern.

Thanks again for being vigilant in reporting suspicious emails.

- Global Cyber Security Operations

Automated Response to Reporter - GoDaddy Report Received

Thank you for your recent isitbad submission.

Email Reported:

Subject: ([[subject]])

If you are sure this email is malicious, or not something you expected or handle, please delete it from your inbox. We will investigate and take the appropriate action for all affected users.

If you are unsure if the email is malicious, do not delete it from your inbox at this time. We will contact you within 24 hours if the email is not malicious.

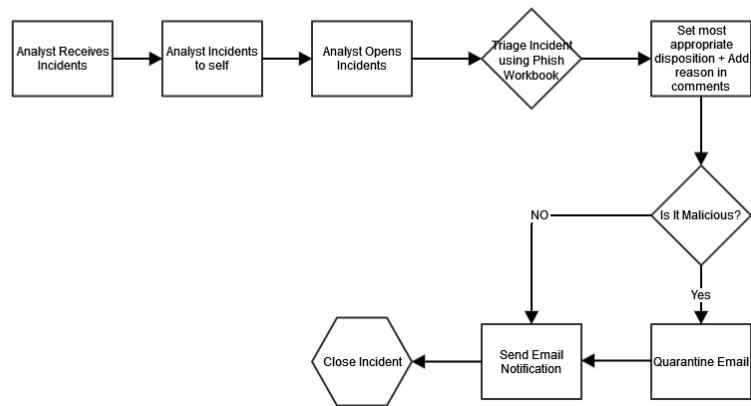
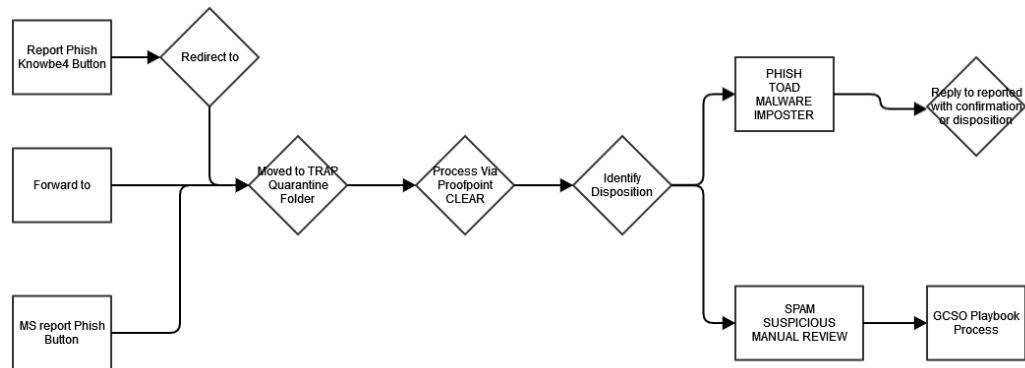
If you have any questions or want to check the status or later find your reported message is legitimate, feel free to contact #gcso_team via Slack or email at security@godaddy.com

- Global Cyber Security Operations

Phishing Reporting Architecture

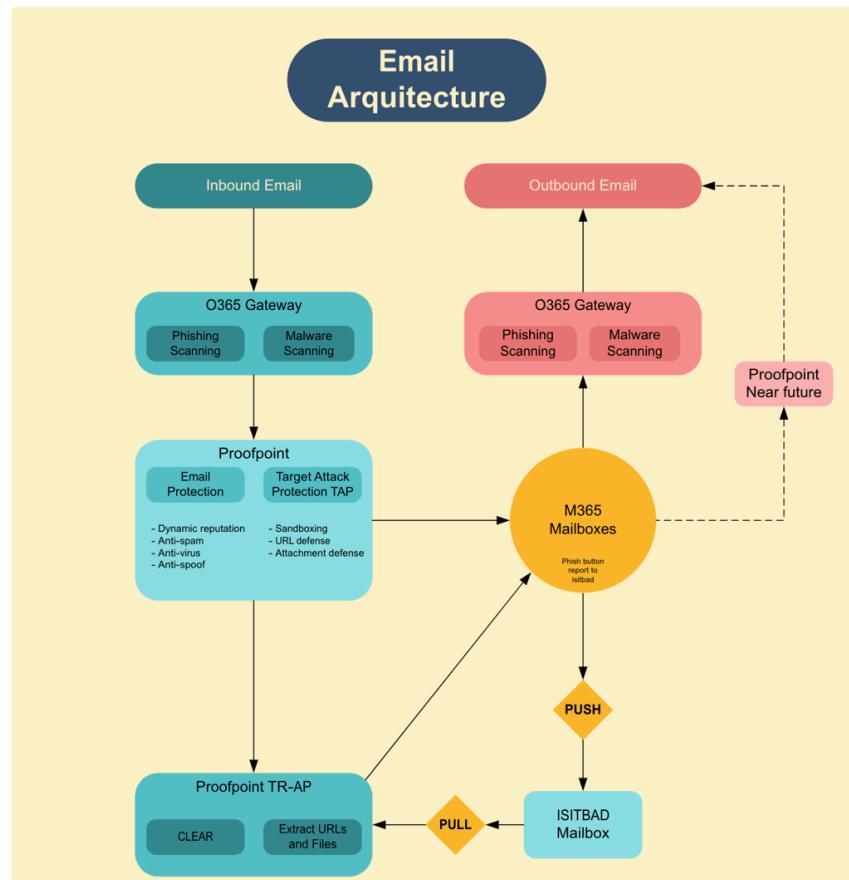
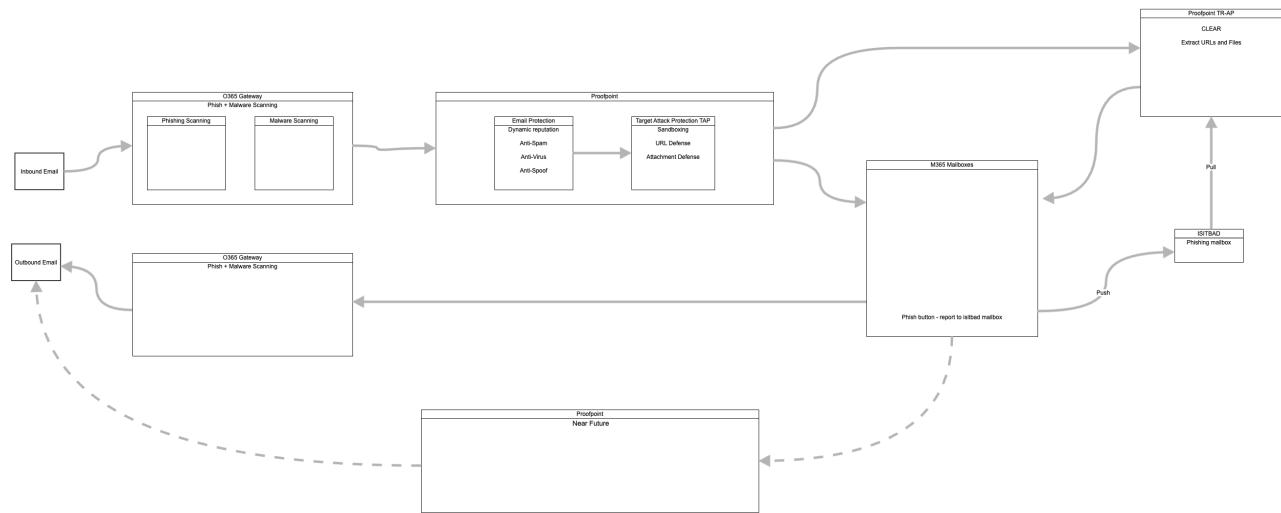
orwar

Proofpoint TRAP Workflows



Email Architecture

Network Diagram



Investigating SentinelOne Hologram (Attivo) Activity

Table of Contents

- Table of Contents
- General Information
 - Process Summary
 - Process-Specific Definitions
- Process Workflow
- Process Outline and Details
 - Incident Response Guide
 - General Outline
 - BOTsink detects the following example Attacks. Full list can be found under Internal Resources:
- Analysis
 - Review Attack Details
 - IOC Discovery and Expanding Scope
 - Using the IOCs collected, search for any correlated activity that could be indicative of potential coordinated attacks
 - Parameters For Potentially Safe Activity
 - If the analysis techniques above yield no malicious activity;
- Containment
- Eradicate
- Recovery
- Post-Incident Activity
 - Process FAQs
 - How does Singularity Hologram deception work?
 - What outcomes does Singularity Hologram provide?
 - What type of data do the decoys capture?
 - How do I get access to SentinelOne Hologram (Attivo)?
- Resources
 - Internal Resources
 - External Resources

General Information

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcs0• EMAIL: ir@godaddy.com• EMAIL: netsec@godaddy.com |
| Process Owner | Emilio Granda |
| Last Review Date | 2023-09-20 by Emilio Granda |
| Escalation Contact(s) | @Randy Thompson @Ivan Avilla |
| Requests for Updates | By Email - ir@godaddy.com By Email - netsec@godaddy.com |

Process Summary

This process provides direction for the analysis and remediation of **SentinelOne Hologram (Attivo)** detections and outlines the general process guidelines to be followed by Security Operations Center & Incident Response analysts. A summary of applicable use cases for this process are as follows:

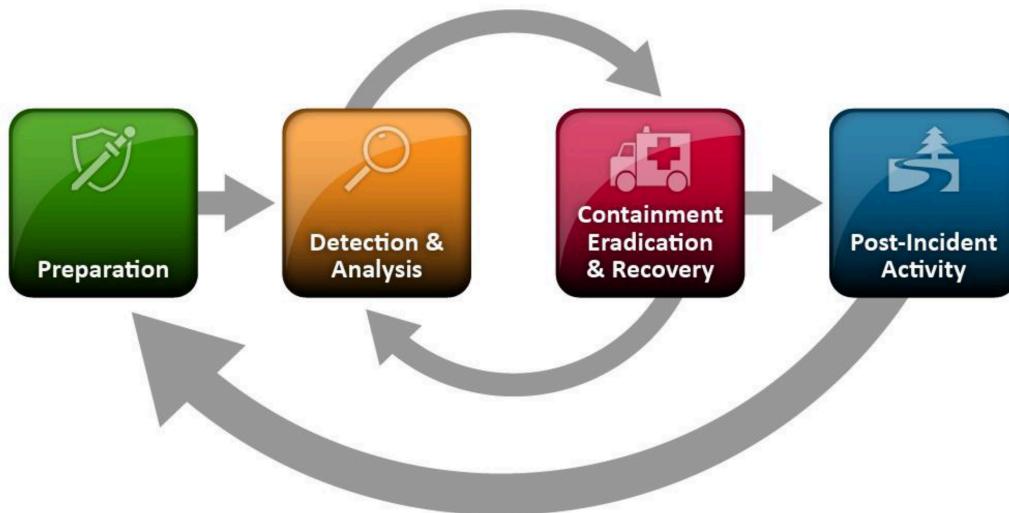
- Network_SentinelOne_Hologram_Activity

Process-Specific Definitions

- **Singularity Hologram** - Network-based threat deception that lures covert threat actors and insiders into engaging and revealing themselves.
- **Attivo** - Attivo Networks was recently acquired by SentinelOne and has now rebranded to Singularity Hologram
- **BOTSink** - system consists of BOTsink and its embedded software. Physical and virtual BOTsink appliances are available.

- **Decoy** - These virtual machines are the server and client hosts to detect breaches in your network. The decoy VMs pose as targets for BOTs and APTs. The decoy VMs engage compromised endpoints when they attempt lateral movement on your network. This enables you to identify and track the actions of these malicious endpoints as well as to prevent data exfiltration.
- **ThreatStrike** - Attivo's ThreatStrike is an endpoint feature, which enables you to complete these critical stages of your deception campaign - customize the decoy VMs with deceptive content as well as create the deceptive tokens.
- **Sinkhole VM** - All traffic originating from the decoy VMs are sent to a Linux-based sinkhole VM. This prevents a compromised decoy VM from sending any malicious traffic to your production network. Optionally, you can configure the sinkhole VM as an Internet proxy for the decoy VMs.
- **Deception content** - Deception content is the data on the decoy VMs, which attackers can access through services such as SMB, FTP, and HTTP. Deception content can include logon credentials, web pages, files in shared folders, and so on.

Process Workflow



Process Outline and Details

Incident Response Guide

| Investigating SentinelOne Hologram (Attivo) Activity | |
|--|---|
| Assignment Group | OPS-GCSO |
| Source | SentinelOne Hologram - Splunk Notable Event |
| Category | Network Attacks |
| Title | Network_SentinelOne_Hologram_Activity |
| State | Analysis |
| Business Impact | 3 - Non - critical(Auto filled) |
| Severity | 2 - Medium(Auto filled) |
| Priority | Low |
| Alert Sensor | SentinelOne Hologram (Attivo) |

General Outline

As a general guideline, the goal of **SentinelOne Hologram (Attivo)** alerts is to detect and lure **in-network attackers and insider threat actors into engaging and revealing themselves**. By mimicking production OSes, applications, data, and more, Singularity Hologram uncovers covert adversary activity, and collects high-fidelity telemetry. **Please keep in mind that these activities insinuate that adversaries with an established foothold in the environment will at some point attempt lateral movement.** Similarly, employees with privileged access and a motive for misuse may pose an insider threat.

1. Alert is received
2. Review alert details
 - a. botsink_dest - BOTSink appliance
 - b. botsink_ip - BOTSink ip address
 - c. user - User
 - d. src - Source Hostname
 - e. src_dns - Source FQDN

- f. dest - Decoy
 - g. dest_ip - Decoy ip address
 - h. app - SentinelOne Hologram (Attivo)
 - i. category - Category of alert
 - j. signature - Rule signature name
 - k. service - Service or protocol
 - l. severity - Severity of alert
 - m. mitre_tactic - MITRE Tactic
 - n. mitre_technique - MITRE Technique
 - o. body - Body of alert message
3. Determine what the source of the attack is
 4. Review signature and determine attack vector
 5. Determine if activity is potentially malicious or expected
 6. Review additional or correlated risk indicators
 7. Appropriately block or quarantine IOCs
 8. Recover and Post Review

BOTsink detects the following example Attacks. Full list can be found under Internal Resources:

Port scan: A port scan is a recon attack, wherein attackers probe the ports that are open on a computer.

Note: For port scan attacks, BOTsink event displays the attacking endpoint, the targeted decoy IP address, and the list of ports scanned.

BOTsink detects the following port scan attacks:

- TCP half open scan: This is also called as SYN scan. This is a commonly used port scan attack. The attacker sends a crafted SYN packet to specific or all the ports of a server. If the server returns a SYN-ACK, the attacker knows that the corresponding port is open. However, the attacker does not send the ACK to complete the TCP handshake. If the server returns a RST, the attacker knows that the port is closed. If there is no response or if an ICMP port unreachable message is received for a particular SYN, then that port is filtered by the firewall. Because no time is spent on creating or tearing down the TCP handshake, the TCP half open scan enables the attacker to scan more ports in less time.
- TCP full connect scan: This is also called as TCP connect scan. The attacker attempts to complete the three-way handshake for each port scanned on a server.
- UDP port scan: A UDP packet is sent to specific or all the ports. If the server returns an ICMP port unreachable error message then the corresponding port is likely to be closed.

Port sweep: In a port sweep, the attacker tries to see in which servers a particular port is open. For example, to exploit an SMB vulnerability, the attacker attempts to see the servers which listen for SMB connections.

Note: For port sweep attacks, the BOTsink event displays the attacking endpoint, the targeted port, and the targeted servers.

- TCP SYN port sweep: The attacker sends a crafted TCP SYN for a particular port to multiple servers. Based on the response, the attacker can identify the servers on which the ports are open.
- TCP ACK port sweep: The attacker sends just the TCP ACK (without the prior SYN) to multiple servers. If a server responds with TCP RST, the attacker can know that there is no firewall filtering on that server. If there is no response from the server, the probability of firewall filtering is high.
- UDP port sweep: The attacker targets a UDP port on multiple servers.

Host sweep: This could be an extensive recon attack, wherein the attacker probes for different ports across servers.

Note: For host sweep attacks, the BOTsink event displays the attacking endpoint and the targeted servers.

- TCP Host sweep: From the same source, the attacker targets multiple TCP ports on different servers.
- UDP Host sweep: From the same source, the attacker targets multiple UDP ports on different servers.
- ICMP host sweep: From the same source, the attacker sends ICMP echo to identify the active endpoints.

ARP scans: When attackers attempt lateral movement, it generally results in too many ARP requests. When there are excessive number of ARP requests from a specific endpoint, you can suspect an ARP scan attack. When attacking endpoints send the ARP requests, the BOTsink too receives these packets. Based on the threshold values you set, BOTsink raises an event with the details if an ARP scan attack is suspected.

ARP floods: Attackers might attempt to bring your network down by saturating your network with ARP requests (broadcasts) from multiple compromised endpoints.

Man In The Middle (MITM): attackers in your local networks who launch NBNS/LLMNR poisoning, SMB relay attacks, and ARP cache poisoning attacks. For example, when attempting to connect to an SMB server, a user might misspell the server name in the path due to which the DNS server fails to resolve the host. Then, the user's Windows endpoint attempts to resolve the server name through NetBIOS Name Service (NBNS) and Link-Local Multicast Name Resolution (LLMNR) broadcasts. A man-in-the-middle (MITM) attacker in the same subnet might respond to these broadcasts pretending to be the requested server. Subsequently, the attacker can force the user for NTLM authentication and harvest the credentials. The attacker can also use the password hashes using pass-the-hash technique to compromise.

- **MITM attacks involving name service protocols** - BOTsink first detects an MITM attacker and then makes an attempt to provide deceptive credentials to the attacker. The attacker eventually uses these deceptive credentials on a decoy VM or a production server.
- **MITM attacks involving ARP** - An attacker inside your network might attempt ARP cache poisoning attacks. For example, the attacker can send an ARP reply in which the IP address of the default gateway is spoofed. In addition to ARP cache poisoning, attackers might also attempt to steal the ARP entries to forward the threat.
- **MITM attacks involving DHCP** - Attackers can launch crippling attacks from within your network using rogue DHCP servers.
- **MITM attacks involving DHCPv6** - An attacker might target a network where IPv6 is enabled and replies to DHCPv6 solicits. The attacker provides his own IPv6 as the DNS server IP.

Credential Deception: In credential deception object is a list of user names. Each user name has an associated password and other details such as first name, last name, and phone number, email address, and so on. All the features, which involve fake credentials make use of the user name and password. The other details are used only for the AD Deception feature.

Domain Deception: A domain deception object contains the decoy domain names, which the Manager uses to create Local Security Authority Subsystem Service (LSASS) lures. Therefore, domain deception objects are required only if you plan to create LSASS tokens through ThreatStrike.

Email Deception: An email deception object is a collection of fake email addresses and passwords. The Central Manager uses these email and passwords to create ThreatStrike tokens for Outlook and Thunderbird email clients. To construct these tokens, the Central Manager chooses a decoy from the corresponding decoy server deception object as the SMTP server.

Scripts & Files Deception: Scripts & Files deception objects contain decoy documents, scripts, files, and fake file paths which the Central Manager uses to create deceptive tokens for scripts & files. Using this deception object, you can add your own fake content in any plain text file or use the required header code and customize any plain text file before you upload the file to the Central Manager.

*Please note that it is possible that NOT all of the fields will populate with results. This could be intentional given the alert category. Additional ThreatStrike & BOTsink detections can be found under Internal Resources

Analysis

In the analysis phase, we will attempt to identify malicious activity using the following techniques.

Review Attack Details

1. Determine whether or not the source of the attack is from a nefarious or expected source
 - a. Can the source be identified using IPAM, CMDB, and/or other asset management available tools?
 - i. Is the source of the attack a known vulnerability scanner, or asset manager, pentesters, or known business app/tool?
 - b. Who are the user?
 - i. Are the users potentially compromised accounts as opposed to the user's themselves?
 - ii. Are the users potentially compromised service accounts?
 - c. What type of attack is this?
 - i. What are the TTPs?
2. Determine potential correlated events
 - a. Are there multiple alerts for the same activity?
 - b. Has this activity been seen recently? In the past?

IOC Discovery and Expanding Scope

Using the IOCs collected, search for any correlated activity that could be indicative of potential coordinated attacks

- Source IPs
- Source Hostnames
- Destination IPs
- Destination Hostnames
- Users
- MITRE Tactics
- MITRE Techniques
- Additional alerts triggered during a relevant timeframe

Parameters For Potentially Safe Activity

If the analysis techniques above yield no malicious activity;

1. confirm that the source of the attack is legitimate
2. Document confirmation of legitimate activity
3. Request tuning and/or whitelisting

Know false positives include legitimate IPAM, SCCM, NETBOX, Qualys, and other network discovery tools and applications.

ⓘ If you are unable to determine source of attack, escalate to a peer or IR.

Containment

Follow quarantine procedures to network segment source from rest of corporate network

Eradicate

Identify additional TTPs and/or IOCs that may indicate widespread or coordinated attack. This alert insinuates that an attacker has an established foothold but may be causing a divergence for actual actions on objectives

Recovery

Segment network zones to enforce least privilege

Reduce access to only needed privileges

- Recommend Zero Trust Model

Post-Incident Activity

How did the attacker gain access?
How long was the attacker's persistence?
Are there additional TTPs or Actions on Objectives?

Process FAQs

How does Singularity Hologram deception work?

Singularity Hologram deception technology deploys decoy systems, credentials, and data to lure in-network attackers and insiders into revealing themselves. The decoy systems mimic production assets and engage with attackers, recording their every action while feeding them fake data. Misdirections present fake results to AD queries. Hologram deception deploys lures to endpoints that lead attackers to the decoy systems, misdirecting them away from production systems.

What outcomes does Singularity Hologram provide?

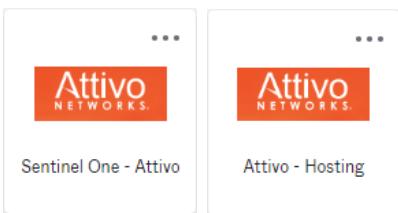
Singularity Hologram detects, misdirects, and isolates external and insider threats that have established a foothold inside the network. Singularity Hologram operates in on-premises networks, in the cloud, and at remote sites to detect lateral movement attack activity that can evade detection from other security controls.

What type of data do the decoys capture?

Singularity Hologram decoys record all attacker interaction they experience in-memory, on disk, and in network traffic, making them available for download or export. The endpoint agent can also capture in-memory activity on hosts that engage with the decoys and lures. For example, decoy documents will provide the full host information for internal systems or the geo-IP of any external system that opens them, and attempts to access concealed credentials will generate alerts.

How do I get access to SentinelOne Hologram (Attivo)?

Request access to the following group **Okta_Attivo_ROAnalysis**. You should see two available tiles: **Sentinel One - Attivo & Attivo - Hosting** where one is for non-hosting environments and the other is, respectively.



Resources

Internal Resources

- https://holomgr.gcn.phx3.netsec.int.gd3p.tools:8443/help/help_files/index.htm (Requires already being logged into Attivo console)

External Resources

- <https://www.sentinelone.com/platform/singularity-hologram/>
- <https://assets.sentinelone.com/eagers-automotive/singularity-hologram-ds>

SentinelOne Deep Visibility Log Headers

| Column n # | Value Name |
|---------------|---|
| 1 | OS Source Process Integrity level |
| 2 | OS Indicator Post Exploitation Count |
| 3 | Cross Process Out of Storyline Count |
| 4 | OS Source Parent Process Image path |
| 5 | OS DNS Requests Count |
| 6 | K8s Node Name |
| 7 | Source Process Login Username |
| 8 | Driver Load Verdict |
| 9 | Logins User Name |
| 10 | Source Process Parent Image MD5 |
| 11 | Target File Extension |
| 12 | Source Process Parent Real Username |
| 13 | Target Process Display name |
| 14 | OS Source Process Parent Reason Signature Invalid |
| 15 | Endpoint Machine Type |
| 16 | Target Process Publisher |
| 17 | Session ID |
| 18 | Named Pipe Read Mode |
| 19 | Task Path |
| 20 | Event Time |

| | |
|----|---|
| 21 | Named Pipe Connection Type |
| 22 | Named Pipe Security Descriptor Group |
| 23 | OS Source Process Start Time |
| 24 | Cross Process Thread Create Count |
| 25 | Driver Certificate Thumbprint Algorithm |
| 26 | OS Cross Process Duplicate Process Handle Count |
| 27 | Target File Created At |
| 28 | Source Process Thread ID |
| 29 | Named Pipe is First Instance |
| 30 | Source Process Signed Status |
| 31 | Source Process Parent Integrity level |
| 32 | OS Source Parent OS ID |
| 33 | TI Indicator UID |
| 34 | Source Process Active Content File ID |
| 35 | Source Process Publisher |
| 36 | Container Name |
| 37 | OS Source Process Storyline Id |
| 38 | Target File Is Executable |
| 39 | Target Process Command Line |
| 40 | Target Process Image SHA256 |
| 41 | OS Network Connections Count |
| 42 | OS Indicator Exploitation Count |
| 43 | Registry Value is Complete |
| 44 | Driver PE SHA1 |
| 45 | Network Connections Count |

| | |
|----|--|
| 46 | Target File Old SHA256 |
| 47 | Source Process Display name |
| 48 | Source Process Command Script Original Size |
| 49 | Source Process Parent StoryLine ID |
| 50 | TI Indicator Description |
| 51 | Child Process Count |
| 52 | Source Process Parent Signed Status |
| 53 | OS Source Process Command Line |
| 54 | OS Source Process Parent Active Content Hash |
| 55 | OS Source Process Active Content Signed Status |
| 56 | Source Process Image MD5 |
| 57 | URL |
| 58 | Target File Convicted by |
| 59 | TI Indicator Type |
| 60 | Named Pipe Name |
| 61 | Indicator Exploitation Count |
| 62 | K8s Controller Name |
| 63 | Target Process Name |
| 64 | Target Process Verified Status |
| 65 | Source Process Effective Username |
| 66 | OS Target File Modification Count |
| 67 | Source Process Parent Unique ID |
| 68 | Network Event Direction |
| 69 | OS Source Process Publisher |
| 70 | Indicator Ransomware Count |

| | |
|----|---------------------------------------|
| 71 | Source Process Parent Is Native 64Bit |
| 72 | Target Process Active Content File ID |
| 73 | Source Process Parent Image SHA256 |
| 74 | Target Process Active Content Path |
| 75 | Target Process Unique ID |
| 76 | Is administrator equivalent |
| 77 | Endpoint Name |
| 78 | Target Process Effective Username |
| 79 | OS Source Process Parent Is OS Root |
| 80 | OS Source Process Active Content Type |
| 81 | OS Source Process Parent Publisher |
| 82 | Source Process Parent Session ID |
| 83 | Module Count |
| 84 | Site Name |
| 85 | K8s Cluster Name |
| 86 | OS Source Process Signed Status |
| 87 | Named Pipe Wait Mode |
| 88 | Target Process Binary is Executable |
| 89 | Target Process Real Username |
| 90 | Source Process Parent Start Time |
| 91 | Task name |
| 92 | Named Pipe Remote Clients Mode |
| 93 | OS Source Parent Process Image SHA1 |
| 94 | TI Indicator MITRE tactics |
| 95 | OS Source Process Parent Command Line |

| | |
|-----|---|
| 96 | Container Image |
| 97 | OS Target File Creation Count |
| 98 | Source Process Image SHA1 |
| 99 | Source Process Active Content Path |
| 100 | Source Process Parent Active Content File ID |
| 101 | OS Source Process Is Native 64Bit |
| 102 | Registry Change Count |
| 103 | Source Process Unique ID |
| 104 | Target Process Access Rights |
| 105 | URL Action |
| 106 | Source Process Is Native 64Bit |
| 107 | Module Path |
| 108 | K8s Controller Type |
| 109 | Registry Old Value Type |
| 110 | OS Indicator Injection Count |
| 111 | OS Source Process Image MD5 |
| 112 | OS Source Process Parent Process |
| 113 | TI Indicator Upload Time |
| 114 | Source Process Parent Account RUID |
| 115 | TI Indicator Categories |
| 116 | Source Process Parent Command Line |
| 117 | OS Source Process Parent Active Content Signed Status |
| 118 | Event type |
| 119 | Target File Old MD5 |
| 120 | OS Indicator Evasion Count |

| | |
|-----|--|
| 121 | Target File size |
| 122 | Cross Process Open Process Count |
| 123 | TI Indicator Modification Time |
| 124 | Driver Certificate Thumbprint |
| 125 | K8s Pod Labels |
| 126 | Target Process Image MD5 |
| 127 | OS Cross Process Out of Storyline Count |
| 128 | OS Source Process Active Content Hash |
| 129 | Registry Value Type |
| 130 | Target Process Account EUID |
| 131 | Indicator General Count |
| 132 | Source Process Account RUID |
| 133 | Target File Internal Name |
| 134 | Source Process StoryLine ID |
| 135 | Target Process Is Redirected Command Processor |
| 136 | Source Process RPID |
| 137 | Target Process Active Content Hash |
| 138 | Target Process Is Native 64Bit |
| 139 | OS Cross Process Thread Create Count |
| 140 | Source Machine IP |
| 141 | Failure Reason |
| 142 | Endpoint OS |
| 143 | OS Indicator Infostealer Count |
| 144 | Indicator Description |
| 145 | OS Source Process Parent Is Redirected Command Processor |

| | |
|-----|--|
| 146 | Container Image Sha256 |
| 147 | Target Process Account LUID |
| 148 | Source Process Parent Active Content Path |
| 149 | Source Process Account EUID |
| 150 | Target File Path |
| 151 | Source Process Session ID |
| 152 | Source Process Is Redirected Command Processor |
| 153 | Network Connection Status |
| 154 | Source Process Command Script SHA256 |
| 155 | DNS Request |
| 156 | OS Source Process Image SHA1 |
| 157 | Target File Modification Count |
| 158 | Source Process Parent Active Content Type |
| 159 | Source Process Start Time |
| 160 | Target File MD5 |
| 161 | Registry Key Unique ID |
| 162 | Source Process Binary is Executable |
| 163 | Source Process Command Script Is Complete |
| 164 | Source Process Parent User |
| 165 | Source Process Parent Reason Signature Invalid |
| 166 | OS Source Process Binary is Executable |
| 167 | Target Process Integrity level |
| 168 | Indicator Category |
| 169 | Container Labels |
| 170 | Source Process Reason Signature Invalid |

| | |
|-----|---|
| 171 | OS Source Process Is Redirected Command Processor |
| 172 | Source Process Name |
| 173 | Named Pipe Max Instances |
| 174 | OS Source Process Parent Active Content Type |
| 175 | Source IP |
| 176 | OS Source Process Display name |
| 177 | TI Indicator intrusion sets |
| 178 | Target File Creation Count |
| 179 | OS Target File Deletion Count |
| 180 | Source Process Parent Image path |
| 181 | Network Connection Outgoing Count |
| 182 | Target File Old SHA1 |
| 183 | Target File Description |
| 184 | Target Process Image path |
| 185 | Indicator Post Exploitation Count |
| 186 | Named Pipe Overlapped |
| 187 | Named Pipe Access Mode |
| 188 | Module Image SHA1 |
| 189 | OS Source Process Active Content Path |
| 190 | Site ID |
| 191 | Account SID |
| 192 | TI Source |
| 193 | Source Process Active Content Hash |
| 194 | OS Source Parent PID |
| 195 | OS Source Process Parent User |

| | |
|-----|---|
| 196 | OS Network Connection Incoming Count |
| 197 | OS Indicator Ransomware Count |
| 198 | OS Source Parent Process Image MD5 |
| 199 | TI Indicator Name |
| 200 | Cross Process Duplicate Thread Handle Count |
| 201 | Source Process Parent Account EUID |
| 202 | OS Source Process Image SHA256 |
| 203 | Account Name |
| 204 | K8s Namespace Labels |
| 205 | Registry Old Value |
| 206 | Target Process StoryLine ID |
| 207 | TI Indicator Creation Time |
| 208 | Source Process Parent Effective Username |
| 209 | Target Process Is Storyline Root |
| 210 | OS Source Process Parent Signed Status |
| 211 | Target Process Active Content Signed Status |
| 212 | Source Process Parent Active Content Hash |
| 213 | Agent UUID |
| 214 | Type |
| 215 | Target File Old File Path |
| 216 | Source Process Is Storyline Root |
| 217 | DNS Response |
| 218 | Target Process Login Username |
| 219 | K8s Pod Name |
| 220 | Indicator Boot Configuration Update Count |

| | |
|-----|--|
| 221 | Target Process Start Time |
| 222 | Source Process Real Username |
| 223 | OS Cross Process Open Process Count |
| 224 | Target Process Image SHA1 |
| 225 | OS Indicator Boot Configuration Update Count |
| 226 | Registry Value |
| 227 | Source Port |
| 228 | OS Source Process Name |
| 229 | Source Process Parent Login Username |
| 230 | OS Source Process Reason Signature Invalid |
| 231 | Source Process Parent Is Storyline Root |
| 232 | Source Process Image path |
| 233 | TI Indicator Valid Until |
| 234 | OS Source Process Parent Is Native 64Bit |
| 235 | OS Source Process Unique ID |
| 236 | OS Source Process Subsystem |
| 237 | Registry Old Value Full Size |
| 238 | Target File SHA1 |
| 239 | Target File Deletion Count |
| 240 | TI Indicator added by |
| 241 | Source Process User |
| 242 | OS Module Count |
| 243 | Target Process Session ID |
| 244 | OS Cross Process Count |
| 245 | Driver Load Start Type |

| | |
|-----|---|
| 246 | Source Process Subsystem |
| 247 | TI Indicator reference |
| 248 | Network Protocol Name |
| 249 | Event ID |
| 250 | OS Source Process Is OS Root |
| 251 | Target File location |
| 252 | OS Source Process Parent Active Content File ID |
| 253 | Destination IP |
| 254 | Source Process Command Script |
| 255 | K8s Namespace |
| 256 | OS Source Parent Process UID |
| 257 | Driver PE SHA256 |
| 258 | Account ID |
| 259 | Source Process Parent Image SHA1 |
| 260 | Indicator Name |
| 261 | Source Process Parent Account LUID |
| 262 | Indicator Persistence Count |
| 263 | OS Source Parent Process Image SHA256 |
| 264 | OS Indicator Reconnaissance Count |
| 265 | Source Process Account LUID |
| 266 | TI Indicator External ID |
| 267 | Source Process Active Content Signed Status |
| 268 | OS Source Process Parent Display name |
| 269 | Source Process Verified Status |
| 270 | Container ID |

| | |
|-----|--|
| 271 | Network Connection Incoming Count |
| 272 | OS Registry Change Count |
| 273 | Target File Modified At |
| 274 | OS Source Process User |
| 275 | Target Process ID (PID) |
| 276 | Target File Id |
| 277 | Cross Process Duplicate Process Handle Count |
| 278 | Named Pipe is Write-through |
| 279 | Source Process Integrity level |
| 280 | Object Type |
| 281 | OS Source Process Active Content File ID |
| 282 | Source Process Parent Publisher |
| 283 | Target Process Signed Status |
| 284 | OS Source Process Image path |
| 285 | Named Pipe Type Mode |
| 286 | Logins Base type |
| 287 | Account Domain |
| 288 | Indicator Metadata |
| 289 | Named Pipe Security Descriptor Owner |
| 290 | OS Network Connection Outgoing Count |
| 291 | Source Process Parent Name |
| 292 | Indicator Infostealer Count |
| 293 | Source Process Parent Display name |
| 294 | Source Process Parent Active Content Signed Status |
| 295 | OS Source Process Parent Active Content Path |

| | |
|-----|---|
| 296 | Source Process Active Content Type |
| 297 | Target File Type |
| 298 | Destination Port |
| 299 | Source Process Image SHA256 |
| 300 | OS Source Process ID (PID) |
| 301 | Registry Key Path |
| 302 | Target File Is Signed |
| 303 | Source Process ID (PID) |
| 304 | OS Source Process Parent Integrity level |
| 305 | Indicator Evasion Count |
| 306 | TI Indicator Metadata |
| 307 | Target Process Relation |
| 308 | Login is Successful |
| 309 | Agent Version |
| 310 | Source Process Parent Is Redirected Command Processor |
| 311 | Target Process Subsystem |
| 312 | Cross Process Count |
| 313 | OS Cross Process Duplicate Thread Handle Count |
| 314 | OS Indicator General Count |
| 315 | Registry Value Full Size |
| 316 | TI Indicator comparison method |
| 317 | Target Process Account RUID |
| 318 | Target Process Active Content Type |
| 319 | Source Process Command Script Application Name |
| 320 | Source Process Command Line |

| | |
|-----|--|
| 321 | DNS Requests Count |
| 322 | Registry Old Value Is Complete |
| 323 | OS Source Process Session ID |
| 324 | OS Source Process Verified Status |
| 325 | Target File SHA256 |
| 326 | OS Child Process Count |
| 327 | Target Process User |
| 328 | K8s Controller Labels |
| 329 | TI Indicator Value |
| 330 | TI Indicator threat actors |
| 331 | Target Process Reason Signature Invalid |
| 332 | Driver Is Loaded Before Monitor |
| 333 | Source Process Parent PID |
| 334 | OS Source Process Parent Session ID |
| 335 | Indicator Injection Count |
| 336 | Indicator Reconnaissance Count |
| 337 | OS Indicator Persistence Count |
| 338 | Module Image MD5 |
| 339 | OS Source Parent Process Start TimeOS Source Process Integrity level |
| 340 | OS Indicator Post Exploitation Count |
| 341 | Cross Process Out of Storyline Count |
| 342 | OS Source Parent Process Image path |
| 343 | OS DNS Requests Count |
| 344 | K8s Node Name |

| | |
|-----|---|
| 345 | Source Process Login Username |
| 346 | Driver Load Verdict |
| 347 | Logins User Name |
| 348 | Source Process Parent Image MD5 |
| 349 | Target File Extension |
| 350 | Source Process Parent Real Username |
| 351 | Target Process Display name |
| 352 | OS Source Process Parent Reason Signature Invalid |
| 353 | Endpoint Machine Type |
| 354 | Target Process Publisher |
| 355 | Session ID |
| 356 | Named Pipe Read Mode |
| 357 | Task Path |
| 358 | Event Time |
| 359 | Named Pipe Connection Type |
| 360 | Named Pipe Security Descriptor Group |
| 361 | OS Source Process Start Time |
| 362 | Cross Process Thread Create Count |
| 363 | Driver Certificate Thumbprint Algorithm |
| 364 | OS Cross Process Duplicate Process Handle Count |
| 365 | Target File Created At |
| 366 | Source Process Thread ID |
| 367 | Named Pipe is First Instance |
| 368 | Source Process Signed Status |
| 369 | Source Process Parent Integrity level |

| | |
|-----|--|
| 370 | OS Source Parent OS ID |
| 371 | TI Indicator UID |
| 372 | Source Process Active Content File ID |
| 373 | Source Process Publisher |
| 374 | Container Name |
| 375 | OS Source Process Storyline Id |
| 376 | Target File Is Executable |
| 377 | Target Process Command Line |
| 378 | Target Process Image SHA256 |
| 379 | OS Network Connections Count |
| 380 | OS Indicator Exploitation Count |
| 381 | Registry Value is Complete |
| 382 | Driver PE SHA1 |
| 383 | Network Connections Count |
| 384 | Target File Old SHA256 |
| 385 | Source Process Display name |
| 386 | Source Process Command Script Original Size |
| 387 | Source Process Parent StoryLine ID |
| 388 | TI Indicator Description |
| 389 | Child Process Count |
| 390 | Source Process Parent Signed Status |
| 391 | OS Source Process Command Line |
| 392 | OS Source Process Parent Active Content Hash |
| 393 | OS Source Process Active Content Signed Status |
| 394 | Source Process Image MD5 |

| | |
|-----|---------------------------------------|
| 395 | URL |
| 396 | Target File Convicted by |
| 397 | TI Indicator Type |
| 398 | Named Pipe Name |
| 399 | Indicator Exploitation Count |
| 400 | K8s Controller Name |
| 401 | Target Process Name |
| 402 | Target Process Verified Status |
| 403 | Source Process Effective Username |
| 404 | OS Target File Modification Count |
| 405 | Source Process Parent Unique ID |
| 406 | Network Event Direction |
| 407 | OS Source Process Publisher |
| 408 | Indicator Ransomware Count |
| 409 | Source Process Parent Is Native 64Bit |
| 410 | Target Process Active Content File ID |
| 411 | Source Process Parent Image SHA256 |
| 412 | Target Process Active Content Path |
| 413 | Target Process Unique ID |
| 414 | Is administrator equivalent |
| 415 | Endpoint Name |
| 416 | Target Process Effective Username |
| 417 | OS Source Process Parent Is OS Root |
| 418 | OS Source Process Active Content Type |
| 419 | OS Source Process Parent Publisher |

| | |
|-----|--|
| 420 | Source Process Parent Session ID |
| 421 | Module Count |
| 422 | Site Name |
| 423 | K8s Cluster Name |
| 424 | OS Source Process Signed Status |
| 425 | Named Pipe Wait Mode |
| 426 | Target Process Binary is Executable |
| 427 | Target Process Real Username |
| 428 | Source Process Parent Start Time |
| 429 | Task name |
| 430 | Named Pipe Remote Clients Mode |
| 431 | OS Source Parent Process Image SHA1 |
| 432 | TI Indicator MITRE tactics |
| 433 | OS Source Process Parent Command Line |
| 434 | Container Image |
| 435 | OS Target File Creation Count |
| 436 | Source Process Image SHA1 |
| 437 | Source Process Active Content Path |
| 438 | Source Process Parent Active Content File ID |
| 439 | OS Source Process Is Native 64Bit |
| 440 | Registry Change Count |
| 441 | Source Process Unique ID |
| 442 | Target Process Access Rights |
| 443 | URL Action |
| 444 | Source Process Is Native 64Bit |

| | |
|-----|---|
| 445 | Module Path |
| 446 | K8s Controller Type |
| 447 | Registry Old Value Type |
| 448 | OS Indicator Injection Count |
| 449 | OS Source Process Image MD5 |
| 450 | OS Source Process Parent Process |
| 451 | TI Indicator Upload Time |
| 452 | Source Process Parent Account RUID |
| 453 | TI Indicator Categories |
| 454 | Source Process Parent Command Line |
| 455 | OS Source Process Parent Active Content Signed Status |
| 456 | Event type |
| 457 | Target File Old MD5 |
| 458 | OS Indicator Evasion Count |
| 459 | Target File size |
| 460 | Cross Process Open Process Count |
| 461 | TI Indicator Modification Time |
| 462 | Driver Certificate Thumbprint |
| 463 | K8s Pod Labels |
| 464 | Target Process Image MD5 |
| 465 | OS Cross Process Out of Storyline Count |
| 466 | OS Source Process Active Content Hash |
| 467 | Registry Value Type |
| 468 | Target Process Account EUID |
| 469 | Indicator General Count |

| | |
|-----|--|
| 470 | Source Process Account RUID |
| 471 | Target File Internal Name |
| 472 | Source Process StoryLine ID |
| 473 | Target Process Is Redirected Command Processor |
| 474 | Source Process RPID |
| 475 | Target Process Active Content Hash |
| 476 | Target Process Is Native 64Bit |
| 477 | OS Cross Process Thread Create Count |
| 478 | Source Machine IP |
| 479 | Failure Reason |
| 480 | Endpoint OS |
| 481 | OS Indicator Infostealer Count |
| 482 | Indicator Description |
| 483 | OS Source Process Parent Is Redirected Command Processor |
| 484 | Container Image Sha256 |
| 485 | Target Process Account LUID |
| 486 | Source Process Parent Active Content Path |
| 487 | Source Process Account EUID |
| 488 | Target File Path |
| 489 | Source Process Session ID |
| 490 | Source Process Is Redirected Command Processor |
| 491 | Network Connection Status |
| 492 | Source Process Command Script SHA256 |
| 493 | DNS Request |
| 494 | OS Source Process Image SHA1 |

| | |
|-----|---|
| 495 | Target File Modification Count |
| 496 | Source Process Parent Active Content Type |
| 497 | Source Process Start Time |
| 498 | Target File MD5 |
| 499 | Registry Key Unique ID |
| 500 | Source Process Binary is Executable |
| 501 | Source Process Command Script Is Complete |
| 502 | Source Process Parent User |
| 503 | Source Process Parent Reason Signature Invalid |
| 504 | OS Source Process Binary is Executable |
| 505 | Target Process Integrity level |
| 506 | Indicator Category |
| 507 | Container Labels |
| 508 | Source Process Reason Signature Invalid |
| 509 | OS Source Process Is Redirected Command Processor |
| 510 | Source Process Name |
| 511 | Named Pipe Max Instances |
| 512 | OS Source Process Parent Active Content Type |
| 513 | Source IP |
| 514 | OS Source Process Display name |
| 515 | TI Indicator intrusion sets |
| 516 | Target File Creation Count |
| 517 | OS Target File Deletion Count |
| 518 | Source Process Parent Image path |
| 519 | Network Connection Outgoing Count |

| | |
|-----|---|
| 520 | Target File Old SHA1 |
| 521 | Target File Description |
| 522 | Target Process Image path |
| 523 | Indicator Post Exploitation Count |
| 524 | Named Pipe Overlapped |
| 525 | Named Pipe Access Mode |
| 526 | Module Image SHA1 |
| 527 | OS Source Process Active Content Path |
| 528 | Site ID |
| 529 | Account SID |
| 530 | TI Source |
| 531 | Source Process Active Content Hash |
| 532 | OS Source Parent PID |
| 533 | OS Source Process Parent User |
| 534 | OS Network Connection Incoming Count |
| 535 | OS Indicator Ransomware Count |
| 536 | OS Source Parent Process Image MD5 |
| 537 | TI Indicator Name |
| 538 | Cross Process Duplicate Thread Handle Count |
| 539 | Source Process Parent Account EUID |
| 540 | OS Source Process Image SHA256 |
| 541 | Account Name |
| 542 | K8s Namespace Labels |
| 543 | Registry Old Value |
| 544 | Target Process StoryLine ID |

| | |
|-----|--|
| 545 | TI Indicator Creation Time |
| 546 | Source Process Parent Effective Username |
| 547 | Target Process Is Storyline Root |
| 548 | OS Source Process Parent Signed Status |
| 549 | Target Process Active Content Signed Status |
| 550 | Source Process Parent Active Content Hash |
| 551 | Agent UUID |
| 552 | Type |
| 553 | Target File Old File Path |
| 554 | Source Process Is Storyline Root |
| 555 | DNS Response |
| 556 | Target Process Login Username |
| 557 | K8s Pod Name |
| 558 | Indicator Boot Configuration Update Count |
| 559 | Target Process Start Time |
| 560 | Source Process Real Username |
| 561 | OS Cross Process Open Process Count |
| 562 | Target Process Image SHA1 |
| 563 | OS Indicator Boot Configuration Update Count |
| 564 | Registry Value |
| 565 | Source Port |
| 566 | OS Source Process Name |
| 567 | Source Process Parent Login Username |
| 568 | OS Source Process Reason Signature Invalid |
| 569 | Source Process Parent Is Storyline Root |

| | |
|-----|---|
| 570 | Source Process Image path |
| 571 | TI Indicator Valid Until |
| 572 | OS Source Process Parent Is Native 64Bit |
| 573 | OS Source Process Unique ID |
| 574 | OS Source Process Subsystem |
| 575 | Registry Old Value Full Size |
| 576 | Target File SHA1 |
| 577 | Target File Deletion Count |
| 578 | TI Indicator added by |
| 579 | Source Process User |
| 580 | OS Module Count |
| 581 | Target Process Session ID |
| 582 | OS Cross Process Count |
| 583 | Driver Load Start Type |
| 584 | Source Process Subsystem |
| 585 | TI Indicator reference |
| 586 | Network Protocol Name |
| 587 | Event ID |
| 588 | OS Source Process Is OS Root |
| 589 | Target File location |
| 590 | OS Source Process Parent Active Content File ID |
| 591 | Destination IP |
| 592 | Source Process Command Script |
| 593 | K8s Namespace |
| 594 | OS Source Parent Process UID |

| | |
|-----|--|
| 595 | Driver PE SHA256 |
| 596 | Account ID |
| 597 | Source Process Parent Image SHA1 |
| 598 | Indicator Name |
| 599 | Source Process Parent Account LUID |
| 600 | Indicator Persistence Count |
| 601 | OS Source Parent Process Image SHA256 |
| 602 | OS Indicator Reconnaissance Count |
| 603 | Source Process Account LUID |
| 604 | TI Indicator External ID |
| 605 | Source Process Active Content Signed Status |
| 606 | OS Source Process Parent Display name |
| 607 | Source Process Verified Status |
| 608 | Container ID |
| 609 | Network Connection Incoming Count |
| 610 | OS Registry Change Count |
| 611 | Target File Modified At |
| 612 | OS Source Process User |
| 613 | Target Process ID (PID) |
| 614 | Target File Id |
| 615 | Cross Process Duplicate Process Handle Count |
| 616 | Named Pipe is Write-through |
| 617 | Source Process Integrity level |
| 618 | Object Type |
| 619 | OS Source Process Active Content File ID |

| | |
|-----|--|
| 620 | Source Process Parent Publisher |
| 621 | Target Process Signed Status |
| 622 | OS Source Process Image path |
| 623 | Named Pipe Type Mode |
| 624 | Logins Base type |
| 625 | Account Domain |
| 626 | Indicator Metadata |
| 627 | Named Pipe Security Descriptor Owner |
| 628 | OS Network Connection Outgoing Count |
| 629 | Source Process Parent Name |
| 630 | Indicator Infostealer Count |
| 631 | Source Process Parent Display name |
| 632 | Source Process Parent Active Content Signed Status |
| 633 | OS Source Process Parent Active Content Path |
| 634 | Source Process Active Content Type |
| 635 | Target File Type |
| 636 | Destination Port |
| 637 | Source Process Image SHA256 |
| 638 | OS Source Process ID (PID) |
| 639 | Registry Key Path |
| 640 | Target File Is Signed |
| 641 | Source Process ID (PID) |
| 642 | OS Source Process Parent Integrity level |
| 643 | Indicator Evasion Count |
| 644 | TI Indicator Metadata |

| | |
|-----|---|
| 645 | Target Process Relation |
| 646 | Login is Successful |
| 647 | Agent Version |
| 648 | Source Process Parent Is Redirected Command Processor |
| 649 | Target Process Subsystem |
| 650 | Cross Process Count |
| 651 | OS Cross Process Duplicate Thread Handle Count |
| 652 | OS Indicator General Count |
| 653 | Registry Value Full Size |
| 654 | TI Indicator comparison method |
| 655 | Target Process Account RUID |
| 656 | Target Process Active Content Type |
| 657 | Source Process Command Script Application Name |
| 658 | Source Process Command Line |
| 659 | DNS Requests Count |
| 660 | Registry Old Value Is Complete |
| 661 | OS Source Process Session ID |
| 662 | OS Source Process Verified Status |
| 663 | Target File SHA256 |
| 664 | OS Child Process Count |
| 665 | Target Process User |
| 666 | K8s Controller Labels |
| 667 | TI Indicator Value |
| 668 | TI Indicator threat actors |
| 669 | Target Process Reason Signature Invalid |

| | |
|-----|-------------------------------------|
| 670 | Driver Is Loaded Before Monitor |
| 671 | Source Process Parent PID |
| 672 | OS Source Process Parent Session ID |
| 673 | Indicator Injection Count |
| 674 | Indicator Reconnaissance Count |
| 675 | OS Indicator Persistence Count |
| 676 | Module Image MD5 |
| 677 | OS Source Parent Process Start Time |

Monitoring Standup Procedure - needs to be redone!

Table of Contents

Purpose

The purpose of this procedure is to demonstrate which items should be covered during a daily standup.

Structure

| | |
|----------------------|----------------------|
| Analyst/Host: | GCSO Member |
| Customer | Monitoring/IR Leader |

Procedure

1. The analyst will begin standup by shows the SOC dashboard. The dashboard should include KPIs since the last standup was held.
2. The analyst who ran the most recent shift shall present notable activities which have occurred since the last standup.
3. The analyst will present any blockers or existing struggles.
4. The analyst will present tuning opportunities if necessary.

Alert Analysis Playbook

1. Table of contents

- 1. Table of contents
- 2. Purpose
- 3. Intro
- 4. Understanding the alert
- 5. Analyze and Correlate the Data
- 6. Example
- 7. Improvements
- 8. General Documentation

2. Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic |

3. Intro

As our security detection capabilities continue to advance, we find ourselves encountering an increasing number of new and unfamiliar alerts. With many of these alerts lacking dedicated playbooks, it becomes imperative to establish a structured approach for their analysis. This playbook serves as your comprehensive guide, outlining the essential steps to ensure a thorough and effective alert analysis process.

4. Understanding the alert

Upon receiving a security alert that you've never encountered before, it's crucial to understand it thoroughly. Begin by asking yourself two essential questions: What is the purpose of this security alert, and why did it trigger in the first place?

1. Start by reading the Rule Description provided in the alert itself. This initial step often provides enough context to begin investigating the alert.
2. Next, inspect the rule query located on the top right side of the alert under 'Correlation Search.' Understand what this query is searching for.
3. Examine the logs that the rule has triggered. Using the same timeframe as the alert, copy and execute the search query to access full logs that may contain additional information about the event.
4. Check the **ESCU alerts info dashboard** for any supplementary information about the specific rule that the alert relates to. Sometimes, this dashboard contains further explanations about the rule.
5. Conduct online research about the rule and its detection. Feel free to explore online resources for articles and information that can enhance your understanding of the detection.

5. Analyze and Correlate the Data

Analyze and Correlate the Data

Now that you've gathered all the information about the rule, use this newfound knowledge to analyze the data from the logs effectively.

1. Search the Logs: Begin by utilizing a Rule search query as a starting point. Modify the search parameters to retrieve the specific information you require.
2. Find out more information about the data that was collected from the logs (example - Source IP - Where is IP from? What is the reputation? If internal, what is the hostname? What is internal IP? Who is the owner? What does it do?...etc)
3. Experiment with the Search: Often, searches involve filters and macros. Take the time to understand these filters and their use cases. Experiment with different search configurations to extract the most relevant information.
4. Correlate the Data: As you experiment with different searches, you'll accumulate various pieces of information related to this alert. Correlate these data points to draw meaningful conclusions.

5. Reach a Conclusion: With a clear understanding of the rule, comprehensive data collection, and data correlation, you should now have a more precise picture of what the rule is designed to detect. Evaluate the rule's significance from a security perspective and assess whether the observed behavior aligns with the data you've gathered and correlated.

6. Example

We have received a new alert, never seen before in our environment.

What information did we get in the alert?

1. Brief explanation what this rule observes
2. Timestamp - We got a timestamp when this behavior was observed
3. Source IP - We got a public source IP (what is it?) - I've did a whois search and found out it's godaddys IP. Checked CMDB and found hostname of internal IP and the owner. Searched more info on it in Sentinel one, Qualys, Confluence and Slack and found out it's a proxy server.

So far we know that there were attempts to log in from the IP that were unsuccessful and successful which could indicate a successful brute force attack coming from Source IP.

Gathering information

We know a source IP. Lets check additional information on Whois .

IP Information for 208.109.194.17

Quick Stats

| | |
|---------------|---|
| IP Location | United States Tempe Godaddy.com LLC |
| ASN | AS26496 AS-26496-GO-DADDY-COM-LLC, US (registered Oct 01, 2002) |
| Resolve Host | 17.194.109.208.host.secureserver.net |
| Whois Server | whois.arin.net |
| IP Address | 208.109.194.17 |
| NetRange: | 208.109.0.0 - 208.109.255.255 |
| CIDR: | 208.109.0.0/16 |
| NetName: | GO-DADDY-COM-LLC |
| NetHandle: | NET-208-109-0-0-1 |
| Parent: | NET208 (NET-208-0-0-0-0) |
| NetType: | Direct Allocation |
| OriginAS: | AS26496 |
| Organization: | GoDaddy.com, LLC (GODAD) |
| RegDate: | 2006-04-12 |
| Updated: | 2014-02-25 |
| Comment: | Please send abuse complaints to abuse@godaddy.com |
| Ref: | https://rdap.arin.net/registry/ip/208.109.0.0 |
| OrgName: | GoDaddy.com, LLC |
| OrgId: | GODAD |
| Address: | 2155 E GoDaddy Way |
| City: | Tempe |
| StateProv: | AZ |
| PostalCode: | 85284 |
| Country: | US |
| RegDate: | 2007-06-01 |
| Updated: | 2022-08-02 |
| Comment: | Please send abuse complaints to abuse@godaddy.com |
| Ref: | https://rdap.arin.net/registry/entity/GODAD |

Looks like it belongs to Godaddy.

Searching on S1

| Action | Endpoint Name | Endpoint Tags | Account | Site | Last Logged In User | Group | Domain | Console Visible IP | Agent Version |
|---------|------------------------------|--------------------------------|--------------|-------------------------|---------------------|---------------|----------------|--------------------|---------------|
| Actions | p3plsaproxy02.cloud.phx3.gdg | FIM-Test Network-Security-Z... | GoDaddy Inc. | Eng-TSA | N/A | Default Group | cloud.phx3.gdg | 208.109.194.171 | 22.3.3.11 |
| Actions | p3vmjim005 | Network-Security-Z... | GoDaddy Inc. | ENG-Desktop Engineering | N/A | Default Group | DC1 | 208.109.194.17 | 22.2.2.394 |

GENERAL

| | | | |
|---------------------|--------------------------|----------------------|-------------------------|
| Last active | Last 4 minutes | Disk encryption | Off |
| Health status | Healthy | UUID | b372919a5c344676bbc... |
| Last logged in | N/A | Console connectivity | Online |
| Agent version | 22.2.2.394 UPDATED | Network status | Connected |
| Full Disk Scan | N/A | Configurable Netw... | Disabled |
| Memory | 8.00 GB | Domain | DC1 |
| CPU | 4 X AMD EPYC-Rome Pro... | Subscribed on | May 11, 2023 01:09 |
| Core count | 4 | Last Reboot | Sep 21, 2023 01:32 |
| Customer identifier | N/A | Console visible IP | 208.109.194.17 |
| Ranger Version | 21.11.0.75 | IP Address | 10.36.161.247 |
| Installer Type | MSI | Locations | fallback |
| Firewall status | Disabled | Serial Number | 2db7dc9e-41b6-4801-9... |

Looks like we have two hosts on that public IP, with internal IP

Checking CMDB

CMDB Search

Quickly search for CIs or Assets with commonly used filters. Searches are limited to 400 results.

| | | |
|---|---|---|
| Name | <input type="text"/> Starts With | <input type="text"/> Enter a host name, or portion |
| FQDN | <input type="text"/> Starts With | <input type="text"/> Enter a fully qualified domain name, or port |
| IPv4 Address | <input type="text"/> 208.109.194.17 | |
| Serial Number | <input type="text"/> Enter an exact serial number | |
| Asset / RFID Tag | <input type="text"/> Enter an exact asset or RFID tag | |
| Assignment Group | <input type="text"/> | |
| Support Group | <input type="text"/> | |
| Security Service Group | <input type="text"/> | |
| Product Line | <input type="text"/> | |
| Product | <input type="text"/> | |
| Business Service | <input type="text"/> | |
| Model | <input type="text"/> | |
| Operating System | <input type="text"/> | |
| Security Zone | <input type="text"/> | |
| Location | <input type="text"/> | |
| Reporting Realm | <input type="text"/> | |
| Search Type | <input type="text"/> CI | |
| <input type="checkbox"/> GoDaddy Managed CIs <input type="checkbox"/> Appliance CIs <input checked="" type="checkbox"/> Exclude Retired | | |
| <input type="button" value="Clear"/> <input type="button" value="OK"/> | | |
| Feedback | | |

IPv4 Address Details (9)

| Table | Items Found | | | |
|--|------------------|---------------------------------------|-----------------|-------------------------------|
| Configuration Items (cmdb_ci_hardware) | CI | Serial Number | Reporting Realm | Status |
| | p3vmjim005 | 2db7dc9e-41b6-4801-98e2-f2b65bb6d2709 | GoDaddy Core | Installed |
| IP Addresses (cmdb_ci_ip_address) | IP | CI | Reporting Realm | CI Status |
| | 208.109.194.17 | p3vmjim005 | GoDaddy Core | Installed |
| IPAM Cache (u_ipam_cache) | CIDR | Type | Sub Type | Reporting Realm Security Zone |
| | 208.109.0.0/16 | Aggregate | | GoDaddy Core |
| | 208.109.0.0/16 | Prefix | Container | GoDaddy Core |
| | 208.109.192.0/22 | Prefix | Container | GoDaddy Core PRD |
| | 208.109.194.0/23 | Prefix | Active | GoDaddy Core |
| | 208.109.194.0/24 | Prefix | Active | GoDaddy Core None |

Looks like we have our hostname, it belongs to JAMF Cloud in Engineering Team Group, but there is no info what does it do...

Checking Slack

← → ⏪ Search: p3vmjim005

Search results for “p3vmjim005”

Messages 7 Files 0 Channels 0 People 0

From In With Date Only my channels Exclude automations More filters

Sort: Newest message Show: 20 results per page

openstackng – Feb 22nd

 **Igor Malevanny** 11:50 PM
JIM proxy server on VM p3vmjim008.jamfdev.godaddy.com
We created an A record for it using old openstack.
Has a floating IP assigned:
208.109.194.73 (edited)

We have the info it's JIM Proxy server.

Now that we know it's a proxy server , we should expect a lot of logins from that IP.

Lets check the rule search query:

Correlation Search

| | |
|-------------|---|
| Search Name | Authentication_Windows_Suspicious_Logons_by_Source |
| App | Enterprise Security |
| App Context | Enterprise Security |
| Description | Malicious actors attempting broad authentications often will generate a significant number of failures which can be used as an indicator of their activity. This detection focuses on identifying sources from which at least 35% of authentication attempts are failing. This is a strong indicator of a potential authentication attack (bruteforce, password spray, etc.) or of a significant misconfiguration at the source of the events. |
| Mode | Guided |
| Search | <pre> index=windows_events sourcetype="XmlWinEventLog:Security" EventCode IN ("4624","4625") IPAddress!="-" IPAddress!="127.0.0.1" TargetUserName!="SYSTEM" TargetUserName!="*\$" fields _time IPAddress Computer action dest user app sourcetype ``` ... Align to Logic Requirements ... rename IPAddress as src ``` ... Remove Hosting ... eval gd_event_domain=mvindex(split(Computer,"."),-2) search NOT gd_event_domain IN ("gdhosting","hostingtest","hostingdev") ``` ... Alert Logic ... `gd_bruteforce_custom_alert_logic` ``` ... Output Results ... table _time action app description mitre_technique_id severity signature signature_id sourcetype src src_type src_zone type user_count dest_count gd_attempts </pre> |

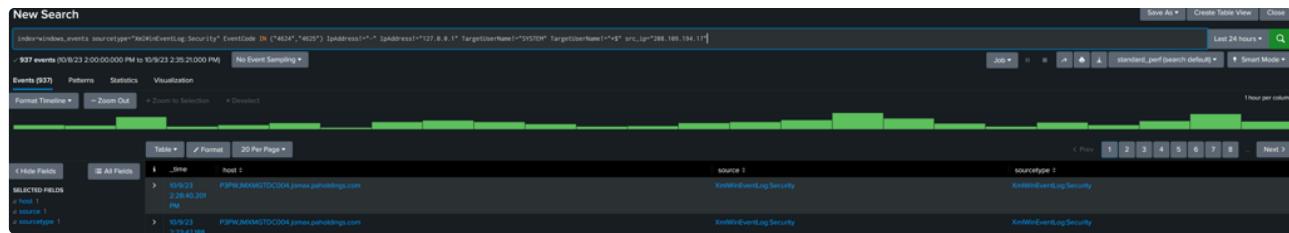
What can we see by checking Rule search query?

1. It searches Windows events
2. Sourcetype are windows security events
3. It searches for Event code 4624 and 4625 (Google searched them and it's successful and unsuccessful logon events)
4. It filters for specific fields (which means it doesn't show us all the data from the log)
5. It applies some hosting environment filters
6. It applies bruteforce macro (maybe we should check what this macro do?)
7. It outputs specific tables (which means it doesn't show us all the data from the log)

Lets now do the search from this rule query our self to get all of the info that are collected:

I will remove all unnecessary tables and macros and manually enter the source IP to see all the login attempts from the IP.

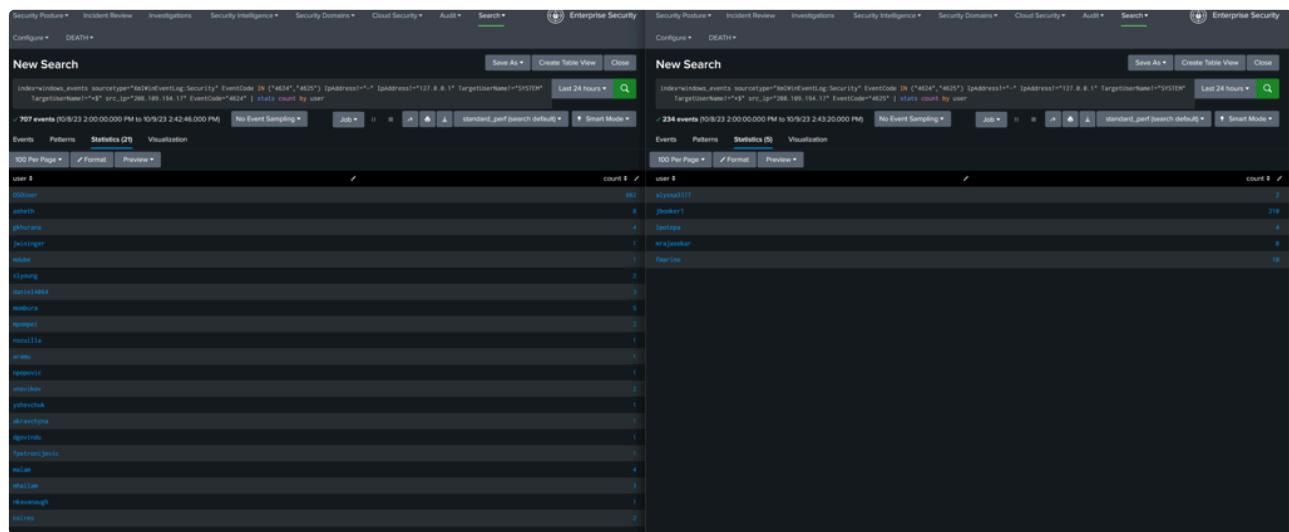
Search for the last 24h to see when this behavior started.



Correlation search

My theory - this alert is detecting a successful brute force attack with event codes, so a TP for this event would look like this: Many unsuccessful attempts followed with successful attempt on a single user.

Lets modify the search to show us successful and unsuccessful logins per user.



So, following the results only one username stands out as a potential bruteforce victim, as there are many unsuccessful attempts (4625) ran on his username- jbooker1

Checking the successful logins, we can not see his name, which brings me to the conclusion that this is unsuccessful bruteforce attempt.

Conclusion

Correlating the data from the alert showed us that there is potential bruteforce attack going on for the user jbooker1 but there was no successful login happened.

This could be running bruteforce attack or broken automation script running for that user.

7. Improvements

Add all possible improvements here:

8. General Documentation

Coming Soon

Identity Identification Playbook

1. Table of contents

- 1. Table of contents
- 2. Purpose
- 3. Intro
- 4. Sentinel One logs
- 5. Splunk Investigations
- 6. Windows Events
- 7. Okta logs
- 8. M365 logs
- 9. Microsoft Defender for Office 365 (MDO) Logs
- 10. CyberArk logs
- 11. Linux Logs
- 12. MS Defender
- 13. Improvements
- 14. General Documentation

2. Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic |

3. Intro

When analyzing alerts, it is sometimes unclear who was the user that initiated this event. In such cases, further investigation into the logs is necessary. There are several ways to find out who the user that logged on the machine is, and this process is gonna be explained in this playbook.

4. Sentinel One logs

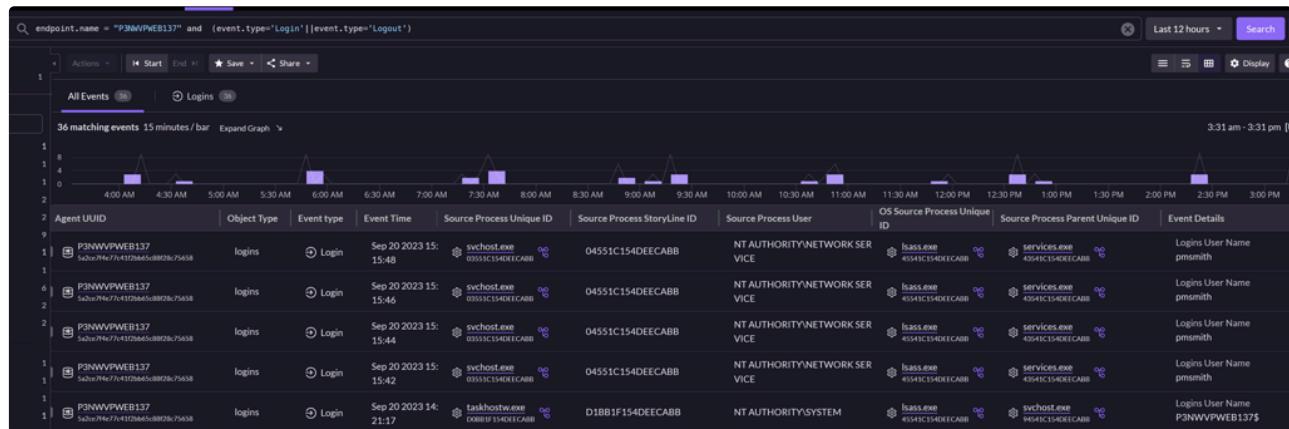
To find out what is the username that logged in to the host go to Sentinel One Deep Visibility and use this search query:

ertainly, here's your provided condition integrated into the context:

```
1 endpoint.name = "hostnameThat'sInvestigated" and (event.type='Login'||event.type='Logout')
```

This condition can be used for filtering and querying logs or data related to the specified endpoint ("hostnameThat'sInvestigated") and events of type 'Login' or 'Logout.' This can be helpful when investigating user activities and access on a specific machine or endpoint.

Just be sure to always set up time frame of interest.



5. Splunk Investigations

Splunk provides valuable information about events on the machine, with more data and various logs than Sentinel One. Understanding where and how to find this information is crucial. We will list indexes of interest and explain the information they store.

6. Windows Events

In Windows event logs, you can typically find user login and logout events using Event IDs. Here are some common Windows event IDs that indicate user login and logout activities:

- Successful User Login:
 - Event ID 4624: This event ID is generated when an account successfully logs on.
- Failed User Login:
 - Event ID 4625: This event ID is generated when a login attempt fails. It provides information about the reason for the failure.
- User Logout (Interactive Logoff):
 - Event ID 4647: This event ID is generated when a user logs off interactively (e.g., through the Windows GUI).
- Remote Desktop Services (RDS) Session Logon/Logoff:
 - Event ID 4624: For successful RDS session logon.
 - Event ID 4647: For RDS session logoff.
- Remote Desktop Services (RDS) Disconnected Session:
 - Event ID 4779: This event ID is generated when an RDS session is disconnected.
- Lock and Unlock Events:
 - Event ID 4800: Generated when a user locks the computer.
 - Event ID 4801: Generated when a user unlocks the computer.

This event codes can be used in search query to determine the username that logged in/out:

```
1 index=windows_events host="TargetedHoast*" (EventCode="4624" OR EventCode="4625") | table
 _time TargetUserName EventCode
```

Always ensure that you adjust the search time interval to align with the specific investigation case, as the presented data volume can be substantial.

7. Okta logs

Okta logs, also referred to as Okta event logs or Okta audit logs, serve as comprehensive records documenting activities and events occurring within the Okta Identity Cloud platform. Okta, an Identity and Access Management (IAM) solution, plays a pivotal role in helping organizations manage user authentication, authorization, and access to a wide range of applications and services. Okta logs are of significant importance in the realms of security, compliance, and monitoring as they provide detailed insights into user and system interactions within the Okta platform.

Search Query for Okta Logs:

To access Okta logs, leverage the following search query:

```
1 index=oktalogs sourcetype="OktaIM2:log" email=InvestigatedUser@godaddy.com
```

Be sure to remain vigilant in adjusting the search parameters to align with the specific requirements of your investigation, as the data volume may exhibit variability.

8. M365 logs

Microsoft 365 (M365) is a versatile cloud-based productivity suite encompassing a wide range of applications and services, including Microsoft Exchange, SharePoint, OneDrive, Teams, and more. Within this dynamic environment, a wealth of logs holds crucial information about activities and events. Monitoring and thorough analysis of M365 logs are essential for a comprehensive approach to security, compliance, and effective issue resolution. Below, we present a playbook outlining common types of information that M365 logs can contain.

Search Query:

To access M365 logs, employ the following search query:

```
1 index=m365 sourcetype="o365:management:activity" UserId="InvestigatedUser@godaddy.com"
```

Always adapt the search parameters to align with the specific needs of your investigation, as the volume and nature of data may vary.

9. Microsoft Defender for Office 365 (MDO) Logs

Microsoft Defender for Office 365, formerly known as Office 365 Advanced Threat Protection, stands as a formidable security service provided by Microsoft. Its mission is to safeguard organizations using Microsoft 365 (formerly Office 365) from a spectrum of email-based threats, encompassing malware, phishing, and various malicious activities. Within its purview of logs and auditing, Microsoft Defender for Office 365 generates a diverse range of logs and reports. These invaluable resources offer keen insights into security-related events and activities situated within the email and threat protection domain.

Search Query:

To access MDO logs for user activity, employ the following search query:

```
1 index="mdologs" UserId=userthatisinvestigated@godaddy.com
```

Always tailor your search parameters to suit your specific investigative needs, as the nature and quantity of data may fluctuate.

10. CyberArk logs

CyberArk, a renowned provider of Privileged Access Management (PAM) solutions, empowers organizations to secure and manage privileged accounts and access to critical systems and data. In the context of CyberArk's PAM solution, "CyberArk logs" encompass the logs and audit data generated by CyberArk components and services. These logs play a pivotal role in monitoring and auditing privileged access activities, facilitating the maintenance of a secure and compliant IT environment.

CyberArk Logs:

1. Search Query for CyberArk Logs:

```
1 index="cyberark" user="*UserNameThatIsInvestigated*"
```

Note: While we may not gather extensive information from CyberArk logs, they can prove invaluable in scenarios where the determination of hosts from IP addresses or vice versa is required.

11. Linux Logs

Linux logs can be a valuable source of information, especially for monitoring user access and system activity. However, it's essential to note that the format and content of Linux logs can be diverse and may not always follow strict standardization. This playbook provides guidance on investigating Linux logs, particularly focusing on user logins and activity.

Investigating Linux Logs:

There are several fields that could be of our interest. This example will count them all in, but you can delete the ones that you are not interested at

1. Search Query for Linux auth logs:

- **Purpose:** To access Linux logs and gather information about user logins and system activity.
- **Search Query:**

```
1 index="linux_secure" (eventtype="useradd" OR eventtype=failed_login OR  
eventtype=sshd_authentication OR eventtype=su_root_session OR eventtype=ssh_open OR  
eventtype=ssh_disconnect OR eventtype=ssh_close) username="*InvestigatedUser*"
```

- Note: The "linux_secure" sourcetype indicates logs related to security and user access on Linux machines.

• Identify Available gd_fluentId_name:

- **Purpose:** Linux logs may vary in their content and format, and the gd_fluentId_name used for specific log types can be diverse. It's essential to identify the relevant

gd_fluentId_name for your specific investigation.

- **Search Query to Identify gd_fluentId_name:**

```
1 | tstats values(sourcetype) values(gd_fluentd_name) where index=on_prem by sourcetype
```

•

Note: This query helps you identify the sourcetype and gd_fluentd_name associations within the logs, enabling you to specify the correct gd_fluentId_name in your subsequent searches.

- **Customized Search Queries:**

- **Purpose:** Based on the identified gd_fluentId_name, create customized search queries to investigate specific aspects of Linux logs, such as user logins, system events, or other relevant activities.

- **Example Customized Search Query:**

```
1 index="on_prem" sourcetype="[sourcetype]" gd_fluentd_name="[gd_fluentd_name]"  
[additional_search_parameters]
```

Note: Replace "[sourcetype]" and "[gd_fluentd_name]" with the relevant sourcetype and gd_fluentd_name values you identified in the previous step. Add any additional search parameters to focus on specific aspects of Linux logs.

12. MS Defender

Microsoft Defender is in process of decommission in the company, but there are still some instances that are using it.

To search User logon events on the machine navigate to [Defender](#) > Hunting > Advanced Hunting

You can use this query to filter Auth logs:

```
1 DeviceLogonEvents  
2 | where DeviceName contains "" and AccountName contains ""
```

The screenshot shows the Microsoft 365 Defender Advanced hunting interface. The left sidebar contains navigation links for Home, Incidents & alerts, Hunting (Advanced hunting selected), Custom detection rules, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets (Devices, Identities), Endpoints (Vulnerability management, Partners and APIs, Evaluation & tutorials, Configuration management). The main area has tabs for Schema, Functions, Queries (selected), and Detection Rules. A search bar at the top right says 'Search'. Below it, a 'Run query' button is highlighted. The 'Query' section shows a Kusto query: 1 DeviceLogonEvents | where DeviceName contains "" and AccountName contains ""'. The 'Results' tab is selected, showing a table with columns: Timestamp, DeviceId, DeviceName, ActionType, LogonType, AccountDomain, AccountName. There are two rows of data:

| Timestamp | DeviceId | DeviceName | ActionType | LogonType | AccountDomain | AccountName |
|------------------------|----------------------|-----------------------|----------------|-----------|----------------------|----------------|
| Sep 2, 2023 2:13:21 PM | 00802c1ecd12595e1... | p3vmit-anune.jomax... | LogonAttempted | Unknown | jomax.paholdings.com | p3vmit-anune\$ |
| Sep 2, 2023 2:13:21 PM | 00802c1ecd12595e1... | p3vmit-anune.jomax... | LogonAttempted | Unknown | jomax.paholdings.com | p3vmit-anune\$ |

13. Improvements

Add all possible improvements here:

14. General Documentation

Coming Soon

AWS Defense Evasion Delete Cloudtrail

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description:](#)
- [Detection Rule](#)
- [Resources](#)
- [Investigation Process](#)
- [Improvements](#)
- [Common False Positives](#)
- [General Documentation](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic |

Description:

The following playbook provides a step-by-step guide for investigating an alert related to AWS Defense Evasion via DeleteTrail events within CloudTrail logs. Adversaries often attempt to evade detection by impairing their target's defenses, which includes deleting CloudTrail logs to hide their malicious activities. When the adversary gains the necessary permissions in the compromised AWS environment, they may delete the entire CloudTrail, which logs activities in the environment.

Detection Rule

```
1 cloudtrail eventName=DeleteTrail eventSource=cloudtrail.amazonaws.com
  userAgent!=console.amazonaws.com errorCode=success
2 | stats count min(_time) as firstTime max(_time) as lastTime values(requestParameters.name)
  as deleted_cloudtrail_name by src region eventName userAgent user_arn aws_account_id
3 | security_content_ctime(firstTime)
4 | security_content_ctime(lastTime)
5 | aws_defense_evasion_delete_cloudtrail_filter
```

Resources

- Splunk Research: [🔗 Detection: AWS Defense Evasion Delete Cloudtrail](#)

Investigation Process

Step 1: Review the Alert Details

- Retrieve the specific event details of the alert to understand the context and scope of the DeleteTrail activity.
- Ensure you have the relevant time frame and other event-specific information.

Step 2: Search for Related Events

- Use the following search query in the CloudTrail logs for the time frame when the alert occurred:

```
1 cloudtrail eventName=DeleteTrail eventSource=cloudtrail.amazonaws.com
  userAgent!=console.amazonaws.com errorCode=success
```

- Examine the results and check the `userIdentity.accountId` field to find the User ID associated with the event.

Step 3: Identify Associated Group

- Examine the `requestParameters.name` field to identify which group the deleted account belongs to.

Throughout the investigation, document all findings, and ensure proper collaboration with other team members if needed. The playbook aims to help analysts in comprehensively investigating and mitigating the impact of AWS Defense Evasion Delete CloudTrail incidents.

Step 4: Investigate Slack History

- Copy the User ID from the previous step and search for it in Slack to check if there were any recent mentions related to requests to delete the account.
- Look for discussions or any other activity related to this user's actions.
- If there are no recent mentions in Slack history, seek assistance from the **#secrets-management** group to determine if anyone has knowledge of the account deletion activity.

Improvements

Add all possible improvements here:

Common False Positives

This Alert will trigger if the account has been deleted on purpose. If you can't prove that this account was deleted on purpose, this might be TP detection of malicious behavior.

Search results for "318604403082"

Messages 66 Files 0 Channels 0 People 0

From In With Date Only my channels Exclude apps and workflows More filters

Sort: Newest message Show: 20 results per page

aws-onboarding – Aug 2nd

 **Tyler Kroymann** 10:43 PM
Hello! can somebody please delete the following AWS accounts? There are no longer plans to continue ... on the cicd account and don't believe there's anything left we setup on the dev account.

[318604403082 GD-AWS-USA-GD-CaretechAC-Dev-Private](#)
and
[152304653728 GD-AWS-USA-GD-CaretechAC-CI_CD](#) (edited)

2 replies

General Documentation

Coming Soon

Delete ShadowCopy With PowerShell Playbook

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description:](#)
- [Detection Rule](#)
- [Resources](#)
- [Investigation Process](#)
- [Improvements](#)
- [Common False Positives](#)
- [General Documentation](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic |

Description:

This following analytic detects PowerShell command to delete shadow copy using the WMIC PowerShell module. This technique was seen used by a recent adversary to deploy DarkSide Ransomware where it executed a child process of PowerShell to execute a hex encoded command to delete shadow copy. This hex encoded command was able to be decrypted by PowerShell log.

Detection Rule

```
1 powershell EventCode=4104 ScriptBlockText="*ShadowCopy*" (ScriptBlockText="*Delete*" OR
ScriptBlockText="*Remove*")
2 | stats count min(_time) as firstTime max(_time) as lastTime by Opcode Computer UserID
EventCode ScriptBlockText
3 | security_content_ctime(firstTime)
4 | security_content_ctime(lastTime)
5 | delete_shadowcopy_with_powershell_filter
```

Resources

- Splunk Research: [Detection: Delete ShadowCopy With PowerShell](#)

Investigation Process

Step 1: Review the Alert Details

- Obtain the specific event details of the alert to understand the context and scope of the PowerShell script attempting to delete shadow copies.
- Gather the time frame and other relevant event-specific information.

Step 2: Investigate PowerShell Code and Decrypt if Encrypted

- Analyze the PowerShell code to understand its purpose and potential implications.
- If the script contains any encryption, attempt to decrypt the encrypted part to gain insight into its functionality and verify if it involves the deletion of shadow copies.

Step 3: Check for Shadow Copy Creation and Deletion

- Look for evidence of shadow copy creation and deletion activities in the system logs.
- Verify if the PowerShell script executed a command related to shadow copy deletion or removal.
- Assess whether the process was fully executed or if it was interrupted, as an incomplete process might lead to a false positive alert.

Step 4: Correlate with Other Indicators

- Correlate the PowerShell script's execution with other indicators of compromise (IOCs) or suspicious activities observed in the environment.

- Cross-reference the findings with threat intelligence sources to identify any known patterns associated with DarkSide Ransomware or other similar threats.

Throughout the investigation, document all findings, and ensure proper collaboration with other team members if needed. The playbook aims to assist analysts in effectively investigating and responding to incidents involving PowerShell commands attempting to delete shadow copies using the WMIC PowerShell module.

Improvements

Add all possible improvements here:

Common False Positives

Sometimes Shadowcopy is not deleted, but the block contains ***Delete***" OR
"*Remove* for some other command.

General Documentation

Coming Soon

Mission Control Events WorkFlow

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Workflow](#)
- [Alert Ownership](#)
- [NIST Incident Response Life Cycle](#)
- [Escalation](#)
- [Closure Comments](#)
- [Alert Closure](#)
 - [Disposition](#)
- [Improvements](#)
- [Common False Positives](#)
- [Out of Scope Events as of 04/24/2023](#)
 - [Customer Hosting](#)
- [General Documentation](#)

Purpose

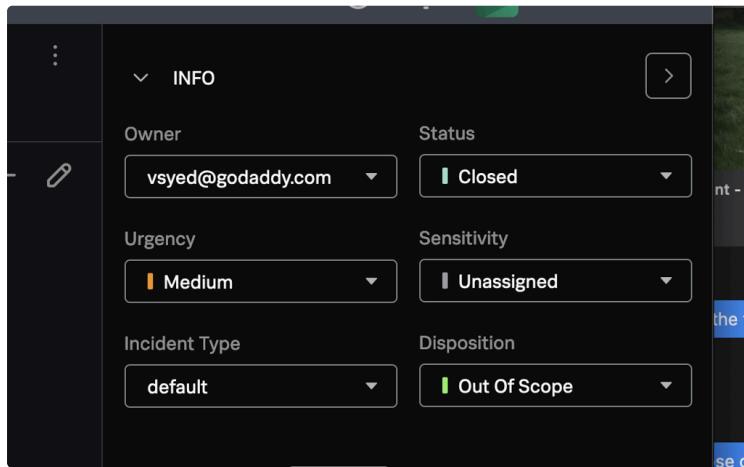
| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | 2023-12-14 by @Thomas Whipple |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @David Hernandez 03/30/2023 |

Workflow

Coming Soon

Alert Ownership

1. once an event is opened, on the right hand plane there is a drop down box for alert ownership and status fields.



2. update notes section on the right hand plane as well when any action is preformed on an event.

Incident ID MC-516988

Description The following analytic identifies the use of PowerShell downloading a file using `DownloadString` method. This particular method is utilized in many different PowerShell frameworks to download files and output to disk. Identify the s... [show more](#)

Created Dec 14th, 2023 5:42 AM

Last updated Dec 14th, 2023 5:48 AM

Incident origin ES Notable Event

Reference ID dfd93d74-c194-4836-a5fa-fa96a104a928

SLA • Dec 14th, 2023 5:48 AM

History [View all review activity for this Notable Event](#)

Splunk Enterprise Security Splunk SOAR [View notable event](#) [View container](#)

NOTES 0

Enter title

T B I U H J K L M N P C G O

Enter note

Save

This screenshot shows the details of an incident in a Splunk interface. It includes fields for Incident ID, Description (with a truncated analytic), Creation and Last Update times, and various incident origins. Below this is a 'NOTES' section with a count of 0, containing input fields for a title and note, along with a rich text editor toolbar. A prominent blue 'Save' button is located at the bottom right of the notes area.

NIST Incident Response Life Cycle

1. Open the alert to review the details. Note, EDR alerts will be best reviewed by opening the alert link.

Incidents | MC-516988 | Any Powershell DownloadString

Overview Response Events Search Automation

Summary

| | | | |
|----------------------|--|--------------------|---|
| Resolution Action | Select... | Original file name | unknown |
| Intrusion Type | Select... | Parent Process | C:\Program Files (x86)\Parallels\Plesk\admin\bin\plesksrv.exe |
| Detection Source | Select... | Parent Process ID | 0xee4 |
| Assessed Severity | Select... | Process | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "(new-object system.net.webclient).downloadsring('http://elite.com/members/site_stats/MemberFollowup.aspx') |
| Annotation Framework | analytic_story context kill_chain_phases mitre_attack | | |
| Annotations | Exploitation HAFNIUM Group Hermetic Wiper Ingress Tool Transfer Malicious PowerShell Source:Endpoint Stage:Execution T1059 T1059.001 T1105 | Process Name | powershell.exe |
| | | Process Id | 0xf40 |
| | | Risk Score | 1336 |
| | | Rule name | ESCU - Any Powershell DownloadString - Rule |
| | | Search name | ESCU - Any Powershell DownloadString - Rule |
| | | Security Domain | endpoint |

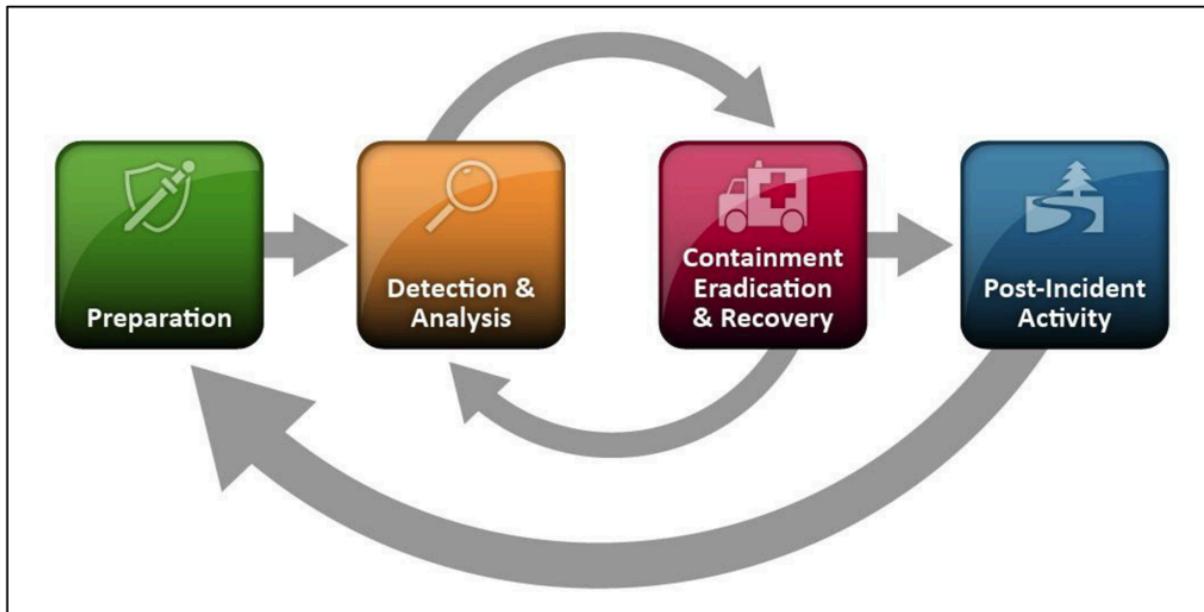
Incident ID: MC-516988
 Description: The following analytic identifies the use of PowerShell downloading a file using 'DownloadString' method. This particular method is utilized in many different PowerShell frameworks to download files and output to disk. Identify the s...
 Created: Dec 14th, 2023 5:42 AM
 Last updated: Dec 14th, 2023 5:48 AM
 Incident origin: ES Notable Event
 Reference ID: dfd93d74-c194-4836-a5fa-fa96a104a928
 SLA: Dec 14th, 2023 5:48 AM
 History: View all review activity for this Notable Event
 Splunk Enterprise Security Splunk SOAR: View notable event | View container

NOTES 0

Enter title
 Enter note

Save

2. Upon opening the alert, your standard process should be to follow the IRP which aligns to the NIST Incident Response Lifecycle



Escalation

The Analyst may escalate an alert/incident to IR for several reasons

- In the event the analyst is not able to determine a verdict, the analyst will seek peer assistance. After peer assistance has been sought with no verdict, the analyst will engage IR for assistance.
- Confirmed Activities: Ransomware, Privileged Escalation, Lateral Movement, Persistence, TA Interactive Sessions, Campaigns, Persistent TA Efforts.

When an escalation is engaged, please be prepared to answer the following

Who:

- If an employee is impacted
 - Who are they?
 - Which Department do they work in?
 - Are other employees impacted?
- If a customer is impacted
 - What is their shopper id?

What:

- What happened (include link to event and description of the event)?
- Are there other instances of malware on the server?
- If a server/workstation is impacted:
 - What is the server name?
 - What environment is it in?
 - What team owns it?
 - What purpose does the server serve?
 - Are other servers impacted
- What IOCs are available if any?

Where:

- Where in the environment did this occur? (Customer, Employee, Server)

Attention to:

- If there are details that you think are important to this alert/incident, please note them here.

Closure Comments

Upon closing the alert, you will be asked for comments. All closure comments should include the following:

What is the hypothesis

Why was the disposition chosen

What analysis was completed to come up with the disposition

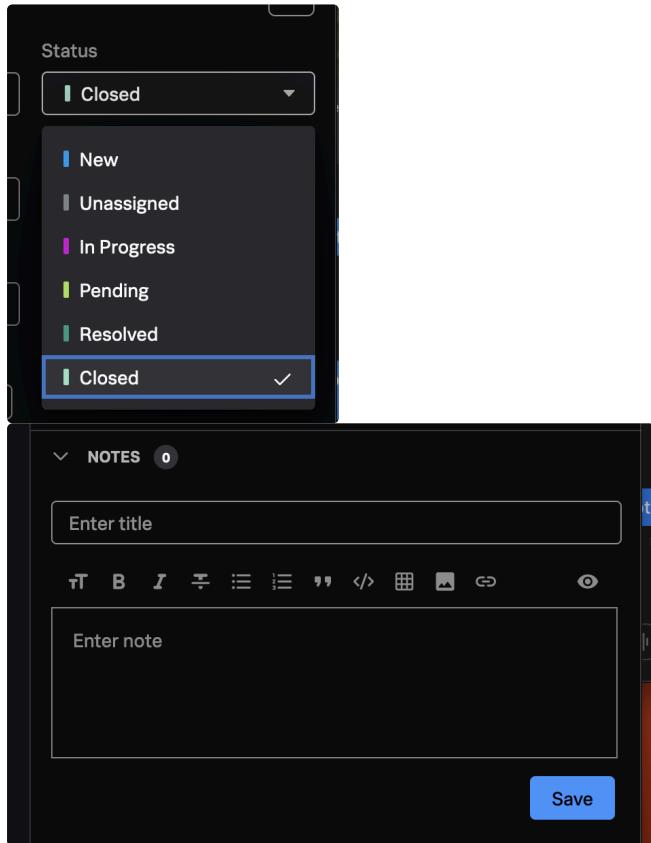
Alert Closure

Disposition

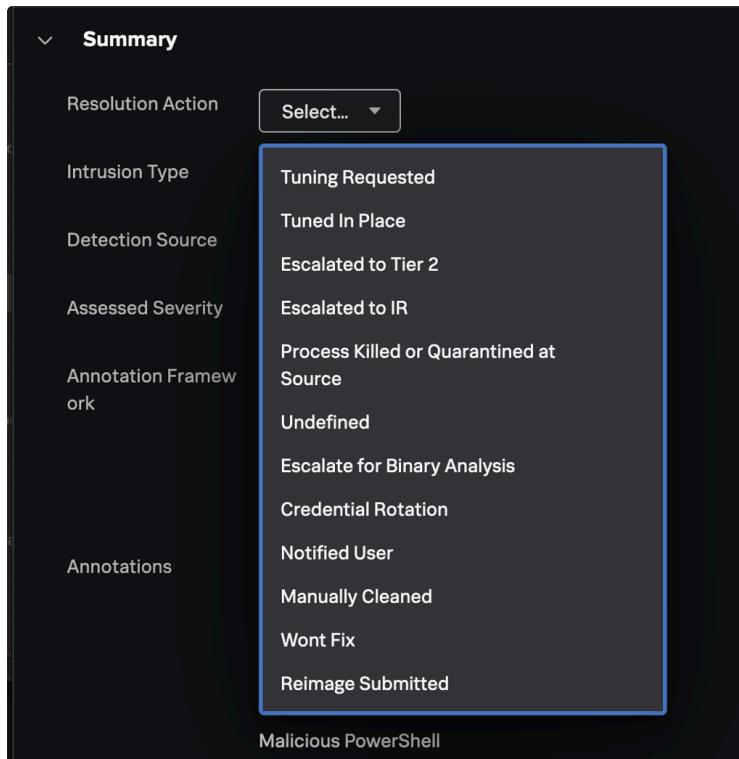
| Label | Description | Example |
|---|--|---|
| Benign Positive - Suspicious But Expected | Issue has been classified as benign. Not Malicious | Hack Tool used by security team to test POC or Web Security Team Downloads Malware for Analysis |
| False Positive - Inaccurate Data | Issue has been classified as a false positive due to inaccurate data. | Search is not flawed but outputting incorrect data. Data is not what has been requested, Log is Giberish, logs, says IP but shows MAC address |
| False Positive - Incorrect Analytic Logic | Issue has been classified as a false positive due to incorrect analytic logic. | Search is flawed, and outputting incorrect data |
| Other | Issue has been classified as other. | |
| Out Of Scope | An event outside the defined roles set to review. | Customer Environment or Outside of Team duties |
| True Positive - Escalated | Event has been escalated to IR | Malicious executable persistent in the environment |
| True Positive - Suspicious Activity | Malicious activity has been detected. (No further Escalation is needed) | Malicious file attempted to run but blocked by security tools, or taken care of by GCSO and not escalated |

Undetermined (**default**)

2. Apply your closing fields and comments



3. Note, there is a field on the top right of each alert to select what action was taken to resolve the event



Improvements

Add all possible improvements here:

Common False Positives

If you believe an alert is a false positive, but not completely sure, take a look at our alert history in splunk or in S1.

Out of Scope Events as of 04/24/2023

Customer Hosting

- The majority of out of scope events and noise will come from the customer hosting environment. We have done our best to tune most of the noise out, but there is still some items that get through.
- Below are some examples of false positives
 - **Alert in Home directory**

For cPanel servers, the customer username will be a random generated 12 character string.

In Legacy spaces, the user

Threat Path /home/ckke3p6gp7op/data/restore/2015-05-20-21-44/files/domains/sherbetbirdie.com/html/wp-includes2/fonts/configseparator.php ▾

Secondly, the sever impacted is a hosting server such as cpanel as shown below.

Affected Host p3plzcpnl494303.prod.phx3.secureserver.net

- In Regex format, Below are the common Customer Hosting Environments

"^/home/\w*/public_html" cPanel HTML Root Paths

"^/home/\w*/mail" cPanel Mail Paths

"^/home/\w*/(\w*\.).{1,}\w*/*" cPanel Alias Domains Paths

"^/home/\w*/domains/([\w-]).{1,}\w/*" cPanel Alias Domains Alternate Paths

"^/home/\w*./?/public_html/*" Other HTML Doc Roots

"^/vz/root/[\w-]/*" Virtuozzo Container Paths

"^/home/.wp-(content/includes)/*" WordPress Content

"^/var/lib/docker/volumes//html/*" MWP HTML Root Paths

"^/home/sites/\d/\w/[\w\.]/public_html" 123Reg Customer NAS Paths

"^/mnt/nas/tmp/mailapiAttachments/*" Customer Email Attachments

"^\\Device\\\\\\HarddiskVolume\\d\\\\PleskVhosts\\\\.+/*" Customer Plesk Content

"^/data/kunden/.+" Domain Factory Customer Space

"^/var/backups/even/.+" Heart Internet and 123 Reg Shared Hosting Customer Backups

"^/var/backups/odd/.+" Heart Internet and 123 Reg Shared Hosting Customer Backups

"^/data/tarifchange/.+" Customer Email Files Transfer

General Documentation

Coming Soon

Powershell Creating Thread Mutex Playbook

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description:](#)
- [Detection Rule](#)
- [Resources](#)
- [Investigation Process](#)
- [Improvements](#)
- [Common False Positives](#)
- [General Documentation](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic |

Description:

The following analytic identifies suspicious PowerShell script execution via EventCode 4104 that is using the mutex function. This function is commonly seen in some obfuscated PowerShell scripts to make sure that only one instance of the process is running on a compromise machine. During triage, review parallel processes within the same timeframe. Review the full script block to identify other related artifacts.

Detection Rule

```
1 powershell EventCode=4104 ScriptBlockText = "*Threading.Mutex*"
2 | stats count min(_time) as firstTime max(_time) as lastTime by EventCode ScriptBlockText
Computer UserID
3 | security_content_ctime(firstTime)
4 | security_content_ctime(lastTime)
5 | powershell_creating_thread_mutex_filter
```

Resources

- Splunk Research: [Detection: Powershell Creating Thread Mutex](#)

Investigation Process

Step 1: Review the Alert Details

- Obtain the specific event details of the alert to understand the context and scope of the PowerShell script using the mutex function.
- Collect the time frame and other relevant event-specific information.

Step 2: Investigate the Mutex Usage in PowerShell Script

- Analyze the PowerShell script's **ScriptBlock** field to identify any mutex commands.
- Try to understand the purpose and implications of using the mutex in the script.

Step 3: Check Windows Event Logs in the Timeframe

- Investigate the Windows event logs for the time frame 5 minutes before and 5 minutes after the alerted event to determine what exactly happened on the machine.
- Examine the process tree to identify any suspicious or unusual activity.
- For machines covered by S1 (Security Information and Event Management system), check the process tree in the S1.

Step 4: If S1 is Unavailable, Use Splunk Search for Windows Event Logs

- For machines not covered by S1, use Splunk's search capability to review the Windows event logs.
- Conduct a Splunk search using the following query: `index="windows_events" host="HostFromTheAlert*" earliest=-5m latest=+5m`

- Analyze the results to gain insights into the events occurring on the machine during the specified timeframe.

Throughout the investigation, document all findings, and ensure proper collaboration with other team members if needed. The playbook aims to assist analysts in comprehensively investigating and responding to incidents involving PowerShell scripts using the mutex function.

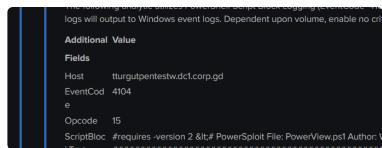
Improvements

Add all possible improvements here:

Common False Positives

There are no False Positives detected so far for this particular alert.

Common indicator that this alert has been generated by internal pentest activity is the hostname of the device. In this example we can see that this machine belongs to tturgut who is our Security Penetration Testing Engineer.



General Documentation

Coming Soon

Powershell Fileless Process Injection via GetProcAddress

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description:](#)
- [Detection Rule](#)
- [Resources](#)
- [Investigation Process](#)
- [Improvements](#)
- [Common False Positives](#)
- [General Documentation](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic |

Description:

The following playbook provides guidelines for analyzing an event related to PowerShell fileless process injection via GetProcAddress. It utilizes PowerShell Script Block Logging (EventCode=4104) to identify suspicious PowerShell execution. Script Block Logging captures the command sent to PowerShell, providing a full view of the command to be executed. Logs generated from this feature will output to Windows event logs. Depending on the volume of logs, consider enabling it on either critical endpoints or all endpoints. The primary objective of this

analytic is to identify instances of `GetProcAddress` in the script block, as this is an uncommon behavior in most legitimate PowerShell scripts and is typically associated with unsafe/malicious activities. Many attack toolkits exploit `GetProcAddress` to achieve code execution. The script utilizes the variable `$var_gpa = $var_unsafe_native_methods.GetMethod(GetProcAddress)` and may be referenced or executed elsewhere. During the investigation, it is essential to review parallel processes using an EDR product or 4688 events to gain a comprehensive understanding of the timeline of events surrounding this activity. The entire logged PowerShell script block should be carefully reviewed.

Detection Rule

```
'powershell' EventCode=4104 ScriptBlockText=*getprocaddress*
| stats count min(_time) as firstTime max(_time) as lastTime by Opcode Computer UserID
EventCode ScriptBlockText
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `powershell_fileless_process_injection_via_getprocaddress_filter`
```

Resources

- Splunk Research: [Detection: Powershell Fileless Process Injection via GetProcAddress](#)
- Picus Security Blog: [MITRE ATT&CK T1055 Process Injection](#)

Investigation Process

Step 1: Review the PowerShell Block

- Gather all alerts from the same host within a close timeframe to the event.
- Since the rule is searching for Windows Event Code 4104 and occurrences of "GetProcAddress" in the script block, locate those specific entries in the PowerShell block.
- Analyze the PowerShell code to understand the script's purpose and potential implications.

Step 2: Review Parallel Processes using EDR

- To gain a comprehensive understanding of what occurred on the affected machine, investigate parallel processes using an Endpoint Detection and Response (EDR) tool.
- Adjust the timeline to include processes that occurred 5 minutes before and after the event.
- Focus on examining the processes on the host with the following characteristics:
src.process.name matches '**.**' + and **endpoint.name** contains '**HOSTNAME**' .
- By analyzing these processes, you can gain insights into what triggered the suspicious PowerShell script and determine if it executed successfully.
- If the environment does not have an EDR solution with process visibility on the host (s1), resort to using Splunk's **index=windows_events** to review the process tree.

Remember to document your findings throughout the investigation and collaborate with other security analysts if necessary. Continuous improvement of this playbook based on real-world experiences will enhance the effectiveness of future incident responses.

Improvements

Add all possible improvements here:

Common False Positives

There are no False Positives detected so far for this particular alert.

Common indicator that this alert has been generated by internal pentest activity is the hostname of the device. In this example we can see that this machine belongs to tturgut who is our [Security Penetration Testing Engineer](#).

```
The following analytic utilizes the Windows endpoint logging to check for logs that output to Windows event logs. Dependent upon volume, enable no crlf
Additional Value
Fields
Host tturgutpentestw.dcl.corp.gd
EventCod 4104
e
Opcode 15
ScriptBloc #requires -version 2 &# PowerSploit File:PowerView.ps1 Author:V
er-
```

General Documentation

Coming Soon

Slack Reports Workflow

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Purpose](#)
- [Process](#)
- [Escalation](#)
 -

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: gcso@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | 2023-12-18 by @David Hernandez |
| Escalation Contact(s) | |
| Requests for Updates | By Email - gcso@godaddy.com |
| Training Log | By: @David Hernandez 12/18/2023 |

Purpose

GCSO will monitor the channel #security-private for the purpose of triaging security concerns or events reported by GoDaddy employees. To accomplish this, GCSO will monitor and respond to the channel 24/7.

Process

1. GCSO will at all times monitor the channel #security-private.

2. When a request is reported, gcs0 will be provided the the person who made the report and a brief description.
 3. Upon working the report, GCSO will add the Emoji [working-on-it] to alert other channel members that it is being responded too
- 
4. The GCSO Analyst will then engage the employee for more details or to provide them and answer for their request.
 5. GCSO will comments details such as, but not limited to:
 - a. Where was the employee directed
 - b. Was GCSO able to answer their question
 - c. Any important conversation details
 6. To close the alert, GCSO will add in all their closing comments and add the [done] emoji



Escalation

If GCSO, needs to escalate a notification:

1. Tag [ir-team] on the alert and include if you need help answering a question or if you are escalating.
2. Then proceed to share any of the details you may have. Below are some examples of items you might include.

The Analyst may escalate an alert/incident to IR for several reasons

- In the event the analyst is not able to determine a verdict, the analyst will seek peer assistance. After peer assistance has been sought with no verdict, the analyst will engage IR for assistance.
- Confirmed Activities: Ransomware, Privileged Escalation, Lateral Movement, Persistence, TA Interactive Sessions, Campaigns, Persistent TA Efforts.

When an escalation is engaged, please be prepared to answer the following

Who:

- If an employee is impacted
 - Who are they?
 - Which Department do they work in?
 - Are other employees impacted?
- If a customer is impacted
 - What is their shopper id?

What:

- What happened (include link to event and description of the event)?
- Are there other instances of malware on the server?
- If a server/workstation is impacted:
 - What is the server name?
 - What environment is it in?
 - What team owns it?
 - What purpose does the server serve?
 - Are other servers impacted
- What IOCs are available if any?

Where:

- Where in the environment did this occur? (Customer, Employee, Server)

Attention to:

- If there are details that you think are important to this alert/incident, please note them in bold.

Splunk Events WorkFlow

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Workflow](#)
- [Alert Ownership](#)
- [NIST Incident Response Life Cycle](#)
- [Escalation](#)
- [Closure](#)
 - [Disposition](#)
- [Improvements](#)
- [Common False Positives](#)
- [Out of Scope Events as of 04/24/2023](#)
 - [Customer Hosting](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | 2023-03-30 by @David Hernandez |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @David Hernandez 03/30/2023 |

Workflow

Coming Soon

Alert Ownership

1. Select an event to analyze and click “Edit Selected”

The screenshot shows a dark-themed user interface for managing 'Notables'. At the top, it displays '2684 Notables' with options to 'Unselect all' or 'Edit Selected'. Below this is a toolbar with icons for search, title sorting, and filtering. A message '1 event was selected' is shown. A single event is expanded, revealing details: 'SentinelOne Threat: Malware on host sg3plcpnl0025.prod.sin3.secureserver.net (malicious)'. The checkbox next to the event name is checked.

2. Update Event with the appropriate fields and assign to yourself.

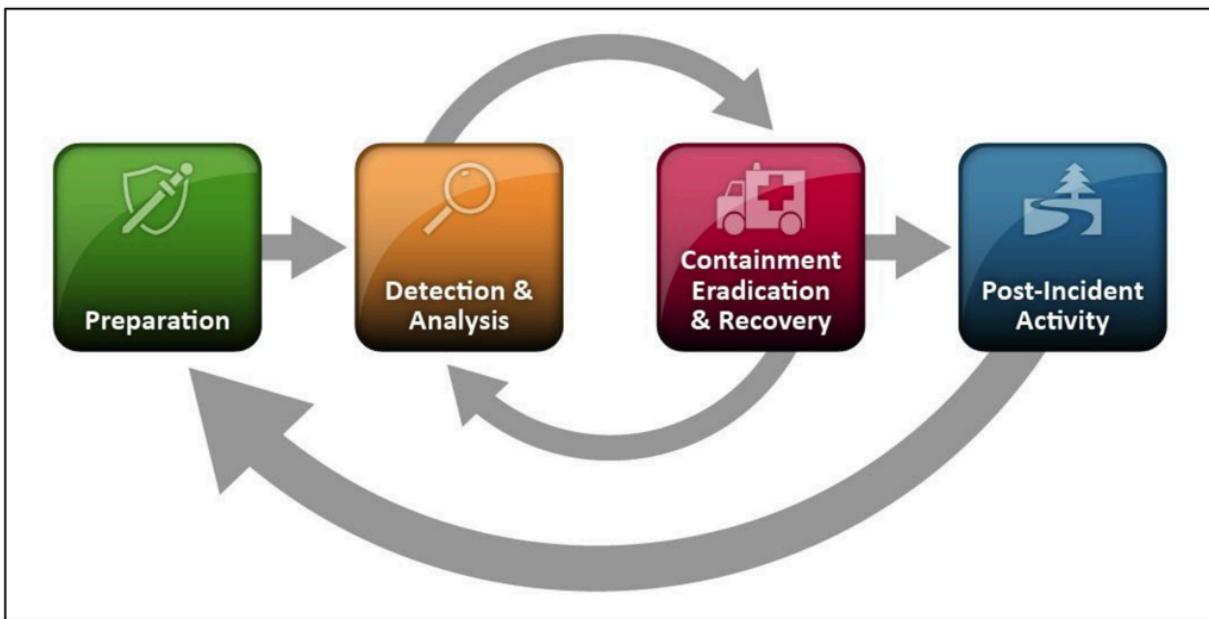
The screenshot shows a modal dialog titled 'Edit Events'. It contains a message '1 event(s) selected. You are editing selected events.' followed by five input fields: Status (set to 'In Progress'), Urgency (dropdown menu), Owner (set to 'David Hernandez'), Disposition (dropdown menu), and Comment (text area containing 'Initial Analysis'). Below the comment area is a link 'Assign to me'. At the bottom are 'Close' and 'Save changes' buttons, with 'Save changes' being highlighted in blue.

NIST Incident Response Life Cycle

1. Expand the alert to review the details. Note, EDR alerts will be best reviewed but opening the alert link.

| Title | Status | Owner | Risk Object | Risk Score | Type | Time | Disposition | Security Domain | Urgency | Actions |
|---|---|------------|-------------|------------|---------|--------------------|--------------|-----------------|---------|---------|
| SentinelOne Threat: Malware on host sg3lcpnl0025.prod.sin3.secureserver.net (malicious) | New | unassigned | -- | -- | Notable | Yesterday, 5:39 PM | Undetermined | Threat | Medium | |
| Description: | | | | | | | | | | |
| This is the IR-specific search for SentinelOne Threats. This search filters SentinelOne events to (1) exclude alerts contained to Customer-managed content as identified by threat paths, and (2) exclude only Static AI type detections which are to be handled by GCSO. | | | | | | | | | | |
| Additional Fields | Value | | | | Action | | | | | |
| Affected Host | sg3lcpnl0025.prod.sin3.secureserver.net | | | | | | | | | |
| Affected Host OS | Linux | | | | | | | | | |
| SentinelOne Agent UUID | 32a9bc1a-4c96-9839-9ecb-84e1dc964bf6 | | | | | | | | | |
| SentinelOne Incident URL | https://use1-godaddy.senteleone.net/analyze/threats/165179373778294520 | | | | | | | | | |
| Threat Classification | Malware | | | | | | | | | |
| SentinelOne Confidence | malicious | | | | | | | | | |
| SentinelOne Detection Engines | SentinelOne Cloud | | | | | | | | | |
| Threat Path | /home/indiatakeone/India Take One Back up/currency/xt/index.php | | | | | | | | | |
| Affected Host Policy Group | cPanel - PROTECT | | | | | | | | | |
| SentinelOne Incident State | unresolved | | | | | | | | | |
| Threat Command | null | | | | | | | | | |
| Threat File SHA1 | 1692688aaea50d20cf65a16d6f0fc13b1a88baed | | | | | | | | | |
| SentinelOne Storyline ID | 510324e6-6995-bd48-9c8e-2ff9dfe5027d | | | | | | | | | |
| SentinelOne Threat ID | 165179373778294520 | | | | | | | | | |
| Severity | high | | | | | | | | | |
| tag | modification_result | | | | | | | | | |
| Short ID | Create Short ID | | | | | | | | | |
| Event Details: | | | | | | | | | | |
| event_id | 816743E2-622A-4B22-89F2-5F86701A3FE5@notable@cd48ea2bba8eda977e2e6a325f270652 | | | | | | | | | |
| event_hash | d48ea2bba8eda977e2e6a325f270652 | | | | | | | | | |
| eventtype | modnotable_results | | | | | | | | | |
| | notable | | | | | | | | | |

2. Upon opening the alert, your standard process should be to follow the IRP which aligns to the NIST Incident Response Lifecycle



Escalation

The Analyst may escalate an alert/incident to IR for several reasons

- In the event the analyst is not able to determine a verdict, the analyst will seek peer assistance. After peer assistance has been sought with no verdict, the analyst will engage IR for assistance.
- Confirmed Activities: Ransomware, Privileged Escalation, Lateral Movement, Persistence, TA Interactive Sessions, Campaigns, Persistent TA Efforts.

When an escalation is engaged, please be prepared to answer the following

Who:

- If an employee is impacted
 - Who are they?
 - Which Department do they work in?
 - Are other employees impacted?
- If a customer is impacted
 - What is their shopper id?

What:

- What happened (include link to event and description of the event)?
- Are there other instances of malware on the server?
- If a server/workstation is impacted:
 - What is the server name?
 - What environment is it in?
 - What team owns it?
 - What purpose does the server serve?
 - Are other servers impacted
- What IOCs are available if any?

Where:

- Where in the environment did this occur? (Customer, Employee, Server)

Attention to:

- If there are details that you think are important to this alert/incident, please note them here.

Closure

Disposition

| Label | Description | Example | Note |
|-------------------|-----------------------|-----------------------|-----------------------------------|
| Benign Positive - | Issue has been | Hack Tool used by | Event used for |
| Suspicious But | classified as benign. | security team to test | pentest/red team |
| Expected | Not Malicious | POC or Web Security | activity or otherwise potentially |

| | | | |
|--|--|---|--|
| | | Team Downloads Malware for Analysis | suspicious/malicious activity that appears to be benign or legitimate given additional context. High degree of confidence where the rule alerted correctly but may not need tuning. |
| Benign Positive - Legitimate Business Activity | Issue has been classified as not suspicious | Non-suspicious or non-malicious activity that is part of normal business operations | Event when there is no evidence of any suspicious or malicious activity and activity appears to be legitimate. This could indicate a high degree of confidence for a tuning opportunity. |
| False Positive - Inaccurate Data | Issue has been classified as a false positive due to inaccurate data. | Search is not flawed but outputting incorrect data. Data is not what has been requested, Log is Giberish, logs, says IP but shows MAC address | Rare event where data is not properly being parsed or data is inaccurate. This could indicate a high degree of confidence for a tuning opportunity. |
| False Positive - Incorrect Analytic Logic | Issue has been classified as a false positive due to incorrect analytic logic. | Search is flawed, and outputting incorrect data | Rare event where the rule logic is not working as the objective intends and/or is not fulfilling its intended purpose. This could indicate a high degree of |

| | | | |
|-------------------------------------|---|--|--|
| | | | confidence for a tuning opportunity. |
| Other | Issue has been classified as other. | A test alert was generated while a rule was being tested | Rare event where the rule logic may have triggered incorrectly due to ongoing testing or an alert does not have a response objective |
| Out Of Scope | An event outside the defined roles set to review. | Customer Environment or Outside of Team duties | Out of scope events |
| True Positive - Escalated | Event has been escalated to IR | Malicious executable persistent in the environment | Event is suspicious or malicious and needs further investigation/remediation from Incident Response |
| True Positive - Suspicious Activity | Malicious activity has been detected. (No further Escalation is needed outside of our team) | Malicious file attempted to run but blocked by security tools, taken care of by GCSO, and not escalated. Suspicious activity investigated in collaboration with Security Monitoring but not escalated to IR | Event is suspicious or malicious but remediation can be or was handled without needing to escalate to Incident Response and/or outside of our direct teams |
| Undetermined (default) | Event disposition has not been set. | Default disposition | Default disposition that should be changed after |

investigation has concluded

2. Apply your closing fields and comments

Edit Events X

1 event(s) selected. You are editing selected events.

| | |
|--------------|--|
| Status | Resolved |
| Urgency | Select... |
| Owner | David Hernandez |
| Assign to me | |
| Disposition | True Positive - Suspicious Activity |
| Comment | The file was confirmed malicious. All IOCs were searched, and all impacted remediated. |

Close **Save changes**

Improvements

Add all possible improvements here:

Common False Positives

If you believe an alert is a false positive, but not completely sure, take a look at our alert history in splunk or in S1.

Out of Scope Events as of 04/24/2023

Customer Hosting

- The majority of out of scope events and noise will come from the customer hosting environment. We have done our best to tune most of the noise out, but there is still some

items that get through.

- Below are some examples of false positives

- **Alert in Home directory**

For cPanel servers, the customer username will be a random generated 12 character string.

In Legacy spaces, the user

| | |
|-------------|--|
| Threat Path | /home/ckke3p6gp7op/data/restore/2015-05-20-21-44/files/domains/sherbetbirdie.com/html/wp-includes2/fonts/configseparator.php |
|-------------|--|

Secondly, the sever impacted is a hosting server such as cpanel as shown below.

| | |
|---------------|--|
| Affected Host | p3plzcpnl494303.prod.phx3.secureserver.net |
|---------------|--|

- In Regex format, Below are the common Customer Hosting Environments

"^/home/\w*/public_html" cPanel HTML Root Paths

"^/home/\w*/mail" cPanel Mail Paths

"^/home/\w*/(\w*\.).{1,}\w*/*" cPanel Alias Domains Paths

"^/home/\w*/domains/([\w-]).{1,}\w/*" cPanel Alias Domains Alternate Paths

"^/home/\w*./?public_html/" Other HTML Doc Roots

"^/vz/root/[\w-]/*" Virtuozzo Container Paths

"^/home/.wp-(content|includes)/*" WordPress Content

"^/var/lib/docker/volumes//html/*" MWP HTML Root Paths

"^/home/sites/\d/\w/[\w\.]/public_html/*" 123Reg Customer NAS Paths

"^/mnt/nas/tmp/mailapiAttachments/*" Customer Email Attachments

"^\\Device\\\\HarddiskVolume\d\\\\PleskVhosts*.+" Customer Plesk Content

"^/data/kunden/.+" Domain Factory Customer Space

"^/var/backups/even/.+" Heart Internet and 123 Reg Shared Hosting Customer Backups

"^/var/backups/odd/.+" Heart Internet and 123 Reg Shared Hosting Customer Backups

"^/data/tarifchange/.+" Customer Email Files Transfer

SentinelOne IOC Block Playbook

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [Incident Recording Guide](#)
 - [Process-Specific Priority Matrix](#)
 - [General Outline](#)
 - [For Domains](#)
 - [For IPs](#)
 - The Process Details section is where depth can be provided for the various steps within your process. Not all steps may require this. Be sure to provide concise direction where possible. Examples are permitted if necessary.
 - [For File Hashes](#)
 - [Captured Metrics](#)
 - [Process FAQs](#)
 - Q: How do I verify which related detections will be blocked in my File Hash block?
 - A: Click on the Threats option, right next to the SHA1 box.
 - Q: How do I verify how common this SHA1 hash is in our environment?
 - A: Click on the Deep Visibility option, right next to the SHA1 box
- [Resources and Definitions](#)
 - [Internal Resources](#)
 - [External Resources](#)
 - [Communication Templates](#)
 - [Associated Audit Controls / Requirements](#)

General Information

| | |
|-----------------------|----------------------------------|
| Responsible Team | Incident Response |
| Process Owner | Incident Response |
| Last Review Date | 2023-05-10 |
| Escalation Contact(s) | @Juan Bustamante |
| Requests for Updates | Slack Jira |

Process Summary

In order to provide more coverage on machines and better data over to Splunk, the IOCs found should also be blocked in SentinelOne.

- Blocking Domains
- Blocking IPs
- Blocking File Hashes

Process Workflow

Process Outline and Details

Incident Recording Guide

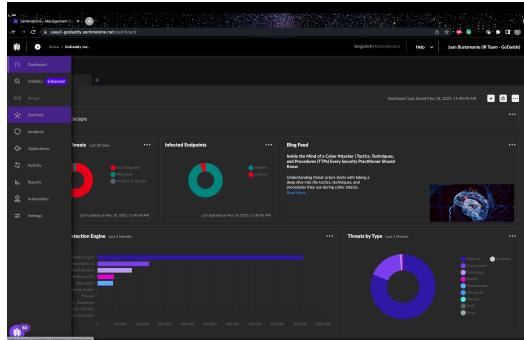
| Incident Type | |
|----------------|--|
| Splunk Field A | |
| Splunk Field B | |
| Splunk Field C | |

Process-Specific Priority Matrix

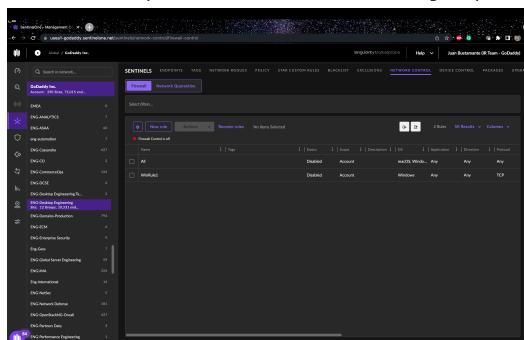
| | Urgency | Impact |
|--------|---------|--------|
| High | | |
| Medium | | |
| Low | | |

General Outline

1. Login into [SentinelOne](#).
2. Go to the **Sentinels** Tab on the left side.



3. Click on the Top Left where it says **Global/GoDaddy Inc.** /
Note: Only Eng-Desktop Engineering has **Network Control** enabled.
4. Go back to **GoDaddy Global** for All Machines including Servers and Workstations.
Note: Make sure you choose the specific group that you want to apply the different blocks for, as that would limit the impact on these different groups/zones.



5. For blocking IPs and Domains choose **Network Control**

6.

For blocking **File Hashes** choose **Blacklist**

For Domains

1. Verify that you're in the **Network Control** tab

2.

Make sure you're on the **Firewall Category** then click on **New Rule**

3. For **Rule Name**: add the **SIR Ticket Number - Malicious URIs**

4. For **OS Type**: On the drop-down choose what Operating System this needs to be applied to. Default is Windows.

5. For **Tag As**: Use **SIR Ticket Number** then click on **Create New Tag**

6. For **Description**: Add the **SIR Ticket Number - Malicious URLs**

7. For **Action**: Choose **Block**

8. Click **Next**

9.

Navigate and click on the **Remote Hosts** option

10. Click on the **Address** dropdown and click on **FQDN**

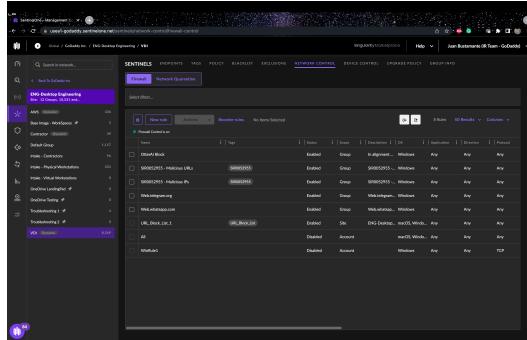
11. Once you have clicked on **FQDN** proceed to add the malicious domains

12. Click on the **Enable rule immediately after saving**

13. Finally, click on **Save**

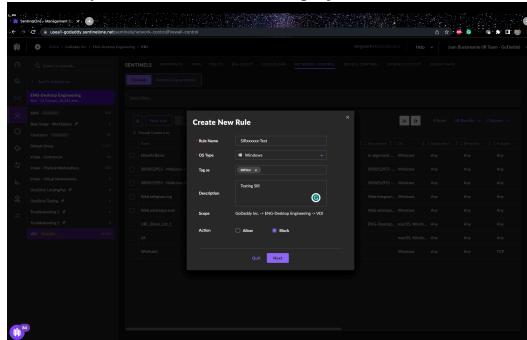
For IPs

- Verify you're in the **Network Control** tab



2.

- Make sure you're on the **Firewall Category** then click on 'New Rule'



3. For Rule Name: add the **'SIR Ticket Number - Malicious IPs'**

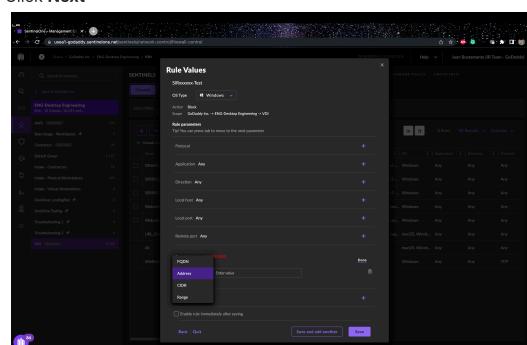
4. For OS Type: On the drop-down choose what Operating System this needs to be applied to. Default is Windows.

5. For Tag As: Use '**SIR Ticket Number**' then click on **Create New Tag**

6. For Description: Add the **SIR Ticket Number - Malicious IPs**

7. For Action: Choose **Block**

8. Click **Next**



9.

- Navigate and click on the **Remote Hosts** option

10. Click on the **Address** dropdown and click on **Addresses**

11. Once you have clicked on **Addresses** proceed to add the malicious domains

12. Click on the **Enable rule immediately after saving**

13. Finally, click on **Save**

The Process Details section is where depth can be provided for the various steps within your process. Not all steps may require this. Be sure to provide concise direction where possible. Examples are permitted if necessary.

For File Hashes

1. Verify that you are in the **Blacklist tab.**

2. Click on **Add New**.

A screenshot of the Microsoft Sentinel interface showing the 'Add to Blacklist' dialog box. The dialog box is centered over a list of log entries. It contains fields for 'Name' (set to 'evil'), 'Description' (set to 'Evil example'), and a 'Comment' field which is empty. At the bottom right of the dialog box is a 'Save and ADD Another' button.

3. For **OS**: On the drop-down choose what Operating System this needs to be applied to.

Note: If you want to block the file hashes on multiple OS you have to add them individually by creating a new entry`.

4. Add your hash in the **SHA1** box.

Note: Blacklist only accepts SHA1 Hashes.

5. Verify the impact of what you will be blocking before you continue.

- a. To view which related detections will be blocked, click on the **Threats** option.
 - b. To view how common this is in our environment, click on the **Deep Visibility** option.

6. For Description: Add the SIR Ticket Number - Malicious Hash.

7 Click Save

Note: If you have a duplicate in the same environment and same OS, you will receive the following error: "Hash 'insert hash' already exists".

Hash '39fcbadcdb2708c0aef13776eca6cccd7370cf644' already exists X

Captured Metrics

Process FAQs

Q: How do I verify which related detections will be blocked in my **File Hash** block?

A: Click on the **Threats** option, right next to the **SHA1** box.

Q. How do I verify how common this **SHA1** hash is in our environment?

A: Click on the **Deep Visibility** option, right next to the **SHA1** box.

Resources and Definitions

Internal Resources

External Resources

Communication Templates

Communication Name

Associated Audit Controls / Requirements

| Audit Type | Process Specifics | Requirement | Requirement Label |
|------------|-------------------|-------------|-------------------|
|------------|-------------------|-------------|-------------------|

| | | | |
|-----|-------------------|---|---------------|
| PCI | Process - Step 2A | Immediately revoke access for any terminated users. | PCI DSS 8.1.3 |
| | | | |
| CIS | Full Process | Maintain Contact Information For Reporting Security Incidents | CIS 19.5 |

Workstation Quarantine (Draft)

Table of Contents

- [Table of Contents](#)
- [General Information](#)
 - [Process Summary](#)
- [Process Workflow](#)
- [Process Outline and Details](#)
 - [General Outline](#)
 - [Process FAQs](#)

General Information

| | |
|-----------------------|--|
| Responsible Team | Incident Response |
| Process Owner | Incident Response |
| Last Review Date | 2023-05-24 |
| Escalation Contact(s) | @ Benny Boham (Deactivated) |
| Requests for Updates | Slack By Email: ir@godaddy.com |

Process Summary

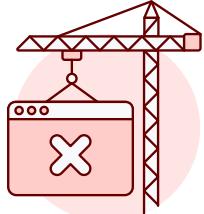
Quarantining workstations / servers using MS 365 Defender/Sentinel One is an important step in containing potential security threats to GoDaddy's network. Below is a playbook to guide you through the process:

Process Workflow



Oops, Diagram Unavailable

This diagram cannot be displayed. It may have been moved, deleted, or you do not have permission to view it.



Oops, Error 500!

Diagram Unavailable

Our system is currently under maintenance. Reach out to your administrator for a fix.



You have an unpublished draft.

Process Outline and Details

| Workstation Quarantine | |
|------------------------|-------------------|
| Assignment Group | response_internal |
| Source | O365 / S1 |
| Category | TBD |
| Title | TBD |
| State | Analysis |
| Business Impact | TBD |
| Severity | TBD |
| Priority | TBD |
| Alert Sensor | |

General Outline

1. An alert is received via mission control and escalated to IR for investigation.
2. **Check the Alerts**
 - a. Prior to taking any action, it is essential to evaluate the generated alerts and determine the scope of the incident. The incident responder must determine whether the compromised system is a server or a personal computer. In the case of a server, the Business Owner must be involved in the decision to isolate the server. Activities that could necessitate isolating a system include:
 - Phishing attacks
 - Security policy violations
 - Suspicious network traffic
 - Malware or virus infections

It is important to note that there should be a plan in place before this system is isolated as this will prevent a user from going about their normal business activities or a business from functioning appropriately.

3. Identify the Infected Device(s)

Once you have reviewed the alerts, identify the infected devices. Check the device's status, operating system, and other relevant information. This will help you to determine the appropriate action to take and where to implement the isolation.

4. Quarantine the Device:

Quarantining a device will isolate it from the network, preventing it from accessing any other devices or resources. This will give you time to investigate the threat and take appropriate action. To quarantine a device using MS 365 Defender, follow these steps:

- Log in to the **Microsoft 365 Defender** portal.
- Click on Devices in the left-hand menu.
- Select the device that you want to quarantine or search for the hostname.
- Click on the hamburger on the right hand side of the screen next to "Manage Tags" and select isolate device.
- Confirm that you want to quarantine the device.

The image shows two screenshots of Microsoft 365 Defender and Sentinel One interfaces.

Microsoft 365 Defender Device Inventory:

- Top Bar:** Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Partner catalog.
- Device Inventory Summary:**
 - Total: 34k
 - High risk: 278
 - High exposure: 410
 - Not onboarded: 14.1k
 - Internet facing: 15
- Table Headers:** Name, Domain, Risk level, Exposure level, OS platform, Windows version, Sensor health state, Onboarding status, Last device update, Tags.
- Table Data:** A list of devices including wsc3-jdly513, vdfc3-78ly503, itc-cbxzq3, wsc3-191tg63, SBXIVMTC-7F3.jonmax.paholdin..., SBXIVMTC-7F5.jonmax.paholdin..., GOLD-CONTRACTOR, LM-C0DFR9HZMD6R, and LM-C0DFR9HZMD6R.

Sentinel One Device Details (wsc3-jdly513):

- Overview:** Device details (Domain: AAD joined, OS: Windows 10 64-bit, IP addresses: 192.168.1.72, Last seen: 24 May 2023 03:15:20), Active alerts (Last 180 days: No active alerts or incidents), Security assessments (Exposure level: Medium, 62 active security recommendations, 62 discovered vulnerabilities (23)), and Health status (Active).
- Incidents and alerts:** 1 logged on user (Most logins: 11, Latest logins: 11, Newest login: 11).
- Timeline:** Logged on users (Last 30 days).
- Security recommendations:** View all recommendations.
- Software inventory:** View all recommendations.
- Discovered vulnerabilities:** View all recommendations.
- Missing KBs:** View all recommendations.
- Advanced features:** Device value, Manage tags, Device value, Manage tags, Report device inaccuracy, Run Antivirus Scan, Collect Investigation Package, Initiate Automated Investigation, Initiate Isolate Device Session, Isolate Device, Ask Defender Expertise, Exclude, Go Hunt, Turn on troubleshooting mode, Policy sync.

a. To create a quarantine policy in **Sentinel One**, follow these steps:

- Log into Sentinel One.
- Click on sentinels and ensure the Endpoints tab is selected in the navigation menu.
- Identify the devices that need to be quarantined.
- If the hostname is known, it can be used to narrow the search to the system of interest.
- Click on the Endpoint Name to open a dialogue box
- In the newly opened box, select Actions, navigate to response and the select Disconnect from network

LM-YTHGYV19MD

GENERAL APP INVENTORY TASKS TAGS Actions

Endpoint Details:

- Last active: Last 4 minutes
- Health status: Healthy
- Last logged in: mpronchick
- Agent version: 22.3.3.6466 (UPDATED)
- Full Disk Scan: Completed (May 03, 2023)
- Memory: 32.00 GB
- CPU: 1 X Apple M1 Pro
- Core count: 10
- Customer identifier: N/A
- Ranger Version: 21.11.0.66
- Installer Type: PKG
- Firewall status: Disabled
- Disk encryption: On
- UUID: DF0B9BD1-BF2C-58C...
- Console connectivity: Online
- Network status: Connected
- Configurable Network: Disabled
- Domain: ptd.net
- Subscribed on: Oct 04, 2022 22:19
- Last Reboot: Apr 26, 2023 19:00
- Console visible IP: 75.97.114.217
- IP Address: 10.39.77.113, 192.168...
- Locations: fallback
- Serial Number: YTHGYV19MD

Actions

LM-YTHGYV19MD

GENERAL APP INVENTORY TASKS TAGS Actions

Endpoint Details:

- Last active: Last 4 minutes
- Health status: Healthy
- Last logged in: mpronchick
- Agent version: 22.3.3.6466 (UPDATED)
- Full Disk Scan: Completed (May 03, 2023)
- Memory: 32.00 GB
- CPU: 1 X Apple M1 Pro
- Core count: 10
- Customer identifier: N/A
- Ranger Version: 21.11.0.66
- Installer Type: PKG
- Firewall status: Disabled
- Disk encryption: On
- UUID: DF0B9BD1-BF2C-58C...
- Console connectivity: Online
- Network status: Connected
- Configurable Network: Disabled
- Domain: ptd.net
- Subscribed on: Oct 04, 2022 22:19
- Last Reboot: Apr 26, 2023 19:00
- Console visible IP: 75.97.114.217
- IP Address: 10.39.77.113, 192.168...
- Locations: fallback
- Serial Number: YTHGYV19MD

Actions

Search...

Recently Used

- Agent Actions
- Endpoint Actions
- Response
- Agent Version Changes
- Shortcuts
- Full Disk Scan
- Troubleshooting
- Configuration
- Tech Support

5. Notify the appropriate parties:

After isolating the devices, you should notify the appropriate parties. This may include the incident channel, security team, or other relevant stakeholders providing a clear explanation of why the device(s) were quarantined, where it has been quarantined (S1/ Defender) what actions were taken, and what steps are being taken to address the issue.

6. Investigate the Threat:

Develop a plan to restore the quarantined endpoint to a trusted state: Perform a comprehensive scan using up-to-date antivirus/antimalware software to detect and remove any malicious software or artifacts. While the device is in quarantine, investigate the threat to determine the appropriate course of action. Using MS 365 Defender portal/ S1:

- Review the alerts, identify the source of the threat determine the scope of the infection. This can also be done using Splunk.
- Assess the potential impact of the incident GoDaddy's critical assets, data, and operations.
- Determine whether the incident is isolated or part of a larger-scale attack. Evaluate the potential for data exfiltration or compromise.
- Implement the required security patches and configurations to address identified vulnerabilities and validate the endpoint's integrity before rejoining it to the network.
- Ensure a thorough investigation is conducted to identify the root cause and attack vectors that led to the endpoint quarantine.

Blocking Velia Brand IPs Procedure

Table of contents

Error loading the extension!

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: gcso@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | 2023-12-19 by @David Hernandez |
| Escalation Contact(s) | |
| Requests for Updates | By Email - gcso@godaddy.com |
| Training Log | By: @David Hernandez 12/19/2023 |

Purpose

In an effort to reduce business outages while successfully remediating threats from the Velia IP space, GCSO will follow procedure below.

Process

1. GCSO will look up IP address in [netbox](#) or whois and determines it belongs to Velia
2. GCSO will craft an email to abuse@velia.net and post in [#godaddy-velia-support](#)
 - a. The email should include the source IP and details about the situation such as the alert type and number of impacted resources
3. Follow up in [#godaddy-velia-support](#) after 24-hours to get status update from Velia

4. If malicious activity is severe enough, there is inherent risk to GD resources, and no response from Velia, #GOC can be engaged to disable port

Email Template

✓ Email Template Example

Hi Velia team,

We have received a security alert which indicates a password spray attack is originating from X.X.X.X. The IP has password sprayed over XX cPanel servers. As this is a Velia IP we are unable to block the IP and require your assistance to mitigate the threat.

Compromised Workstation Playbook

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description:](#)
 - [Validation](#)
 - [Alert Types](#)
 - [Escalation](#)
 - [Isolation](#)
 -  Only isolate a device if it is under “ENG-Desktop Engineering” S1 site. If you need to isolate outside this site you have to engage SEC-MON or IR team.
 -  After isolation is made please notify in the #get-itsec channel
 - [Mitigation](#)
- [Note](#)
- [General Documentation](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic |

Description:

This playbook is a guide on how to respond to compromised workstations found in Godaddy environment.

This playbook only leads you on how to respond to compromised WORKSTATION and not servers, as those are more sensitive.

Validation

Ensure the system in question is a workstation to avoid disrupting business operations. **Do not isolate an operational server.**

- **Naming Convention:** Workstations have different naming conventions than servers. This can be your first hint.
- **CMDB and Snow:** Check the system name in CMDB and Snow for additional information, such as the system owner.

Alert Types

There are two types of alerts that can detect potential malicious behavior on workstations:

- **Sentinel One Alerts:** These are the most common way to detect potentially malicious behavior on endpoints. There are two types of detection:
 - **Static:** Detects known malicious file hashes.
 - **Dynamic:** Behavioral type of detection which identifies potentially malicious behavioral patterns.
- **Splunk Behavioral Alerts:** Every week, new alerts are created by the Detection team to identify potentially malicious behavior. Investigate the alert by checking Splunk search or SentinelOne logs.

Escalation

Once you've confirmed that the system is a workstation and it's been compromised, follow these escalation steps:

- **L2:** Escalate to L2 to assist with your investigation.
- **Monitoring Team:** Escalate to the monitoring team if they are online.
- **IR:** Escalate to IR for further in-depth analysis and remediation.

Isolation

Only isolate a device if it is under “ENG-Desktop Engineering” S1 site. If you need to isolate outside this site you have to engage SEC-MON or IR team.

If the machine is compromised, attackers may use it to move laterally through the network. To prevent or disrupt their actions, isolate the machine. The method of isolation depends on the system type:

- **Windows:** Use Sentinel One. Navigate to SentinelOne start page > Sentinels > Choose Free text search and search by Endpoint Name > paste the Hostname > Click on the hostname > General > actions > Response > Disconnect from the network. This will disconnect the machine from the network but not from the S1 agent.

The screenshot shows the SentinelOne web interface. The left sidebar has a 'Sentinels' section selected. In the main area, the 'ENDPOINTS' tab is active. A search bar at the top shows 'Endpoint name: LTTC-DZ0X2T3'. Below it, there's a 'Free text search' field with 'Endpoint Name' selected, containing 'LTTC-DZ0X2T3'. To the right is a 'Search by Tag' section with 'Has Tag' selected, showing 'Windows' with a count of 1. A dropdown menu for 'Select a key' and 'Select a value' is open. At the bottom of this section is a '+ Add to Filter' button. Further down, there are 'Actions' and 'Group' buttons, and a message 'No Items Selected'. Below these are sections for 'Endpoint Name' and 'Tags', with 'LTTC-DZ0X2T3' listed under Tags. The bottom part of the screenshot shows a detailed view for the endpoint 'LTTC-DZ0X2T3'. It includes tabs for 'GENERAL', 'APP INVENTORY', 'TASKS', 'UPDATES', and 'TAGS'. Under 'GENERAL', there's a 'Disconnect from Network' button. On the right, a 'Actions' menu is open, listing options like 'Recently Used', 'Agent Actions', 'Endpoint Actions', 'Response', 'Agent Version Changes', 'Shortcuts', 'Full Disk Scan', 'Troubleshooting', and 'Configuration'. The 'Response' option is highlighted.

- **MAC:** Use Microsoft Defender. Navigate to Microsoft Defender > Assets – Devices > Search for the hostname > Click on the hostname > ... on the right top side > Isolate Device.

i After isolation is made please notify in the #get-itsec channel

✉ Workstation isolation message template

[Communication templates | Compromised Workstation Playbook](#)

Mitigation

For less concerning TP events (cryptominer or Adware), you can try to mitigate the problem by running a full scan:

- **Windows:** Go to SentinelOne start page > Sentinels > Choose Free text search and search by Endpoint Name > paste the Hostname > Click on the hostname > General > actions > Full Disk Scan > Initiate scan.

If this doesn't work, you can always go to Response > Remote Shell and try to remove the threat manually.

The screenshot shows the Microsoft Defender interface for a device named LTTC-DZ0X2T3. The device is listed as 'Windows 11 Enterprise' from 'GoDaddy Inc. / ENG/Desktop Engineering'. The 'GENERAL' tab is selected, displaying various system metrics: Last active (Last 4 minutes), Health status (Healthy), Last logged in (dzeic), Agent version (23.2.3.358), Full Disk Scan (N/A), Memory (31.68 GB), CPU (Core count), and Customer ID. A context menu is open over the CPU section, with 'Initiate Scan' highlighted in purple. Other options in the menu include 'Abort Scan', 'Full Disk Scan', 'Troubleshooting', and 'Configuration'. The bottom of the screen shows the device version (21.11.0.123) and a timestamp (ID A).

- **Mac:** Go to Microsoft Defender > Assets – Devices > Search for the hostname > Click on the hostname > ... on the right top side > Run Antivirus Scan. If nothing is found, you can try to do it manually by running Initiate live Response Session.

The screenshot shows the Microsoft Defender interface for a device. The 'Security assessments' section indicates an 'Exposure level: Medium'. It shows 11 active security recommendations, with a breakdown: High (10), Medium (4), and Low (3). Below this, it shows 'Logged on users (Last 30 day)' and '0 logged on users'. There were no logged on users. Action buttons include 'Run Antivirus Scan', 'Collect Investigation Package', 'Isolate Device', 'Ask Defender Experts', 'Exclude', 'Go Hunt', and 'Turn on troubleshooting mode'.

Note

These processes might disrupt users' ability to perform business, so always check the user's position in the company before proceeding.

General Documentation

Coming Soon

Lateral movement investigation - in progress

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description:](#)
 - [Validation](#)
 - [Alert Types](#)
 - [Escalation](#)
 - [Isolation](#)
 - [Mitigation](#)
- [Note](#)
- [General Documentation](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic |

Description:

Splunk: In Splunk, lateral movement detection involves identifying processes connecting remotely into a host. This can be done by looking for authentication events over the network from rare or unusual hosts or users¹. Here's an example of a Splunk search that could be used:

```
index=windows_events (EventCode=4624 OR EventCode=4672) Logon_Type=3 NOT user="*\$\" NOT user="ANONYMOUS LOGON"
```

```
| stats count BY dest src_ip dest_nt_domain user EventCode  
| sort count
```

This search uses Windows security logs, looking for successful Windows logon events (EventCode 4624), network connections (LogonType 3), and privilege escalation events (EventCode 4672). It excludes computer logons (*\$) and unauthenticated sessions (ANONYMOUS LOGON).

SentinelOne: In SentinelOne, lateral movement detection is part of the platform's low-level monitoring capabilities. It builds execution context in real time and applies Behavior AI to identify the anomalies of various techniques used to move around in the network².

For example, SentinelOne can detect lateral movement attacks in real time, preventing the spread of malware, or the “roaming around” attacker². It can detect techniques like Pass-the-hash and Pass-the-ticket, where an attacker steals the password hash or a Kerberos ticket from a system and then uses that to authenticate to other systems on the network³.

Remember, these are just examples. The specific methods and searches you use may vary depending on your specific environment and the data you have available. Always ensure to tailor your searches and investigations to your specific needs

Validation

Ensure the system in question is a workstation to avoid disrupting business operations. **Do not isolate an operational server.**

- **Naming Convention:** Workstations have different naming conventions than servers. This can be your first hint.
- **CMDB and Snow:** Check the system name in CMDB and Snow for additional information, such as the system owner.

Alert Types

There are two types of alerts that can detect potential malicious behavior on workstations:

- **Sentinel One Alerts:** These are the most common way to detect potentially malicious behavior on endpoints. There are two types of detection:
 - **Static:** Detects known malicious file hashes.
 - **Dynamic:** Behavioral type of detection which identifies potentially malicious behavioral patterns.

- **Splunk Behavioral Alerts:** Every week, new alerts are created by the Detection team to identify potentially malicious behavior. Investigate the alert by checking Splunk search or SentinelOne logs.

Escalation

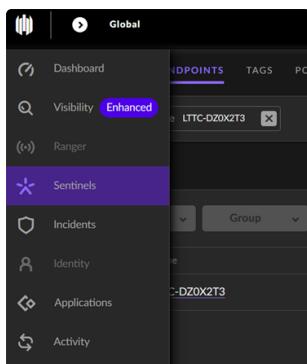
Once you've confirmed that the system is a workstation and it's been compromised, follow these escalation steps:

- **L2:** Escalate to L2 to assist with your investigation.
- **Monitoring Team:** Escalate to the monitoring team if they are online.
- **IR:** Escalate to IR for further in-depth analysis and remediation.

Isolation

If the machine is compromised, attackers may use it to move laterally through the network. To prevent or disrupt their actions, isolate the machine. The method of isolation depends on the system type:

- **Windows:** Use Sentinel One. Navigate to SentinelOne start page > Sentinels > Choose Free text search and search by Endpoint Name > paste the Hostname > Click on the hostname > General > actions > Response > Disconnect from the network. This will disconnect the machine from the network but not from the S1 agent.



The screenshot shows the SentinelOne interface under the 'SENTINELS' tab. In the search bar, 'Endpoint name LTTC-DZ0X2T3' is entered. Below the search bar, there are filters for 'OS' set to 'Windows'. The search results table shows one item: 'LTTC-DZ0X2T3 (1)'. The table has columns for 'Endpoint Name' and 'Endpoint Tags'. A single row is selected, showing 'LTTC-DZ0X2T3' and 'Network-Security-Z...' with a '+1' badge.

The screenshot shows the 'Actions' dropdown menu for endpoint 'LTTC-DZ0X2T3'. The menu includes options like 'Disconnect from Network', 'Reconnect to Network', 'File Fetch', 'Remote Shell', 'Clear Remote Shell Session', 'Run Script', and several system status indicators (Last active, Health status, Last logged in, Agent version, Full Disk Scan, Memory, CPU, Core count, Customer id, Report View).

- **MAC:** Use Microsoft Defender. Navigate to Microsoft Defender > Assets – Devices > Search for the hostname > Click on the hostname > ... on the right top side > Isolate Device.

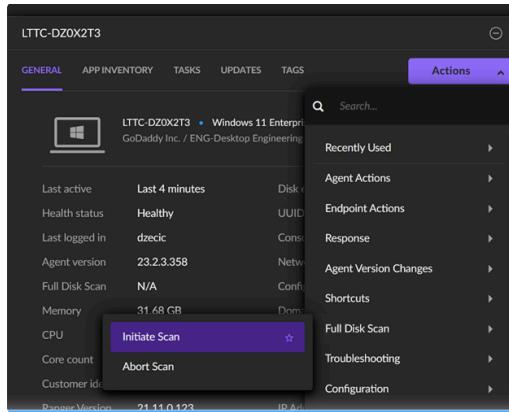
The screenshot shows the Microsoft Defender Device Inventory page. It displays a list of devices, including 'LM-CQ2PT7XMDR' which is highlighted. The device details show it's an 'Unprotected' device with '0' vulnerabilities. The page also includes sections for 'Device Details', 'Security Assessments', and 'Logs'.

The screenshot shows the Microsoft Defender Device Details page for endpoint 'LM-CQ2PT7XMDR'. It provides a detailed view of the device, including its name ('LM-CQ2PT7XMDR'), group ('No active alerts or incidents'), and security status ('Exposure level: Medium'). The page also includes tabs for 'Overview', 'Incidents and alerts', 'Timeline', 'Security recommendations', 'Inventories', 'Discovered vulnerabilities', 'Security policies', and 'Advanced features'.

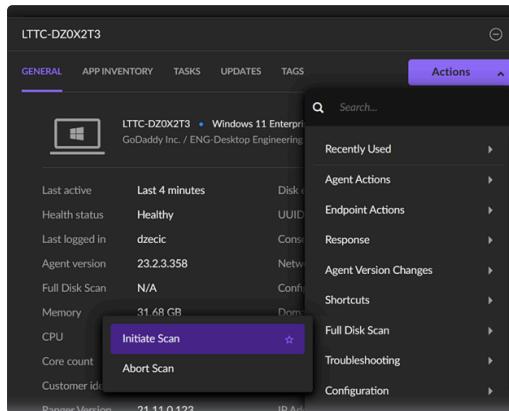
Mitigation

For less concerning TP events (cryptominer or Adware), you can try to mitigate the problem by running a full scan:

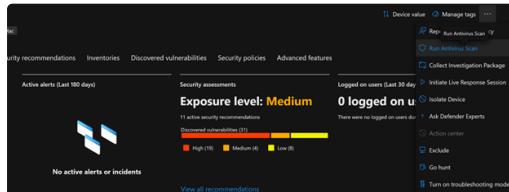
- **Windows:** Go to SentinelOne start page > Sentinels > Choose Free text search and search by Endpoint Name > paste the Hostname > Click on the hostname > General > actions > Full Disk Scan > Initiate scan.



If this doesn't work, you can always go to Response > Remote Shell and try to remove the threat manually.



- **Mac:** Go to Microsoft Defender > Assets – Devices > Search for the hostname > Click on the hostname > ... on the right top side > Run Antivirus Scan. If nothing is found, you can try to do it manually by running Initiate live Response Session.



Note

These processes might disrupt users' ability to perform business, so always check the user's position in the company before proceeding.

General Documentation

Coming Soon

SentinelOne URL blocking

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description:](#)
- [URL blocking procedure](#)
- [Improvements](#)
- [General Documentation](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic |

Description:

The following playbook outlines guidelines for blocking Indicators of Compromise (IOCs) in SentinelOne (S1). As part of our investigations, we often encounter malicious IPs, URLs, file hashes, and other indicators that need to be blocked to enhance GoDaddy's security environment.

This playbook provides step-by-step instructions on how to block these malicious URL's in S1.

WARNING: Exercise caution when using S1's blocking capabilities. Irresponsible use could result in significant disruptions to company operations. Follow each step precisely as outlined in

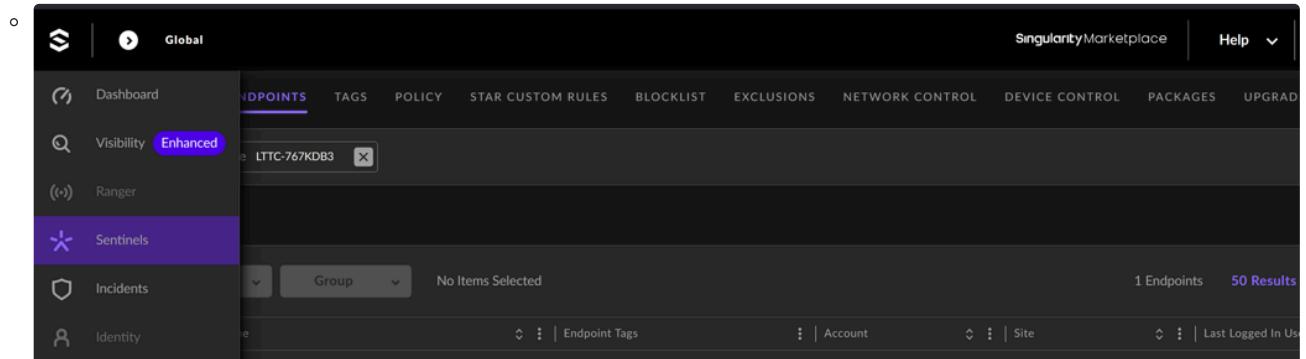
this playbook.

URL blocking procedure

NOTE: When handling potentially malicious URLs, exercise caution. Follow best practices to prevent others from inadvertently clicking on the link, which could potentially compromise their security. To achieve this, use square brackets around dots in the domain. For example: mail[.]google[.]com

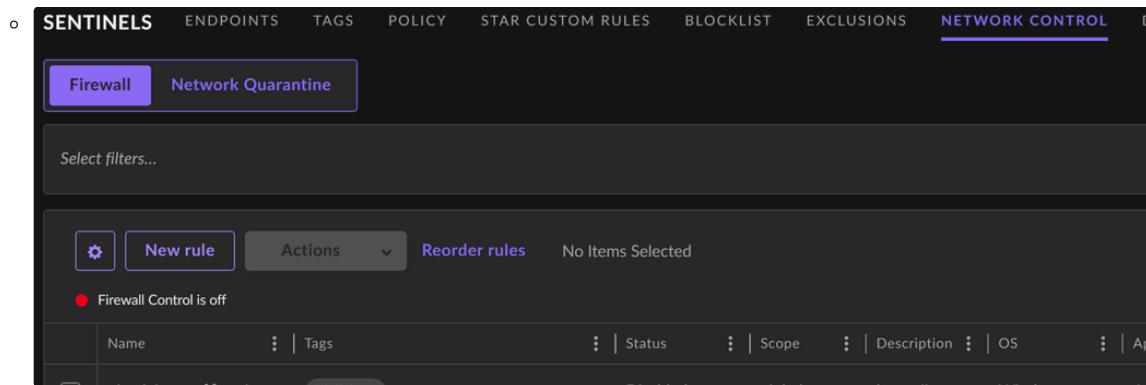
1. Log in to the S1 Console:

- On the left side, click on the “Sentinels” tab.



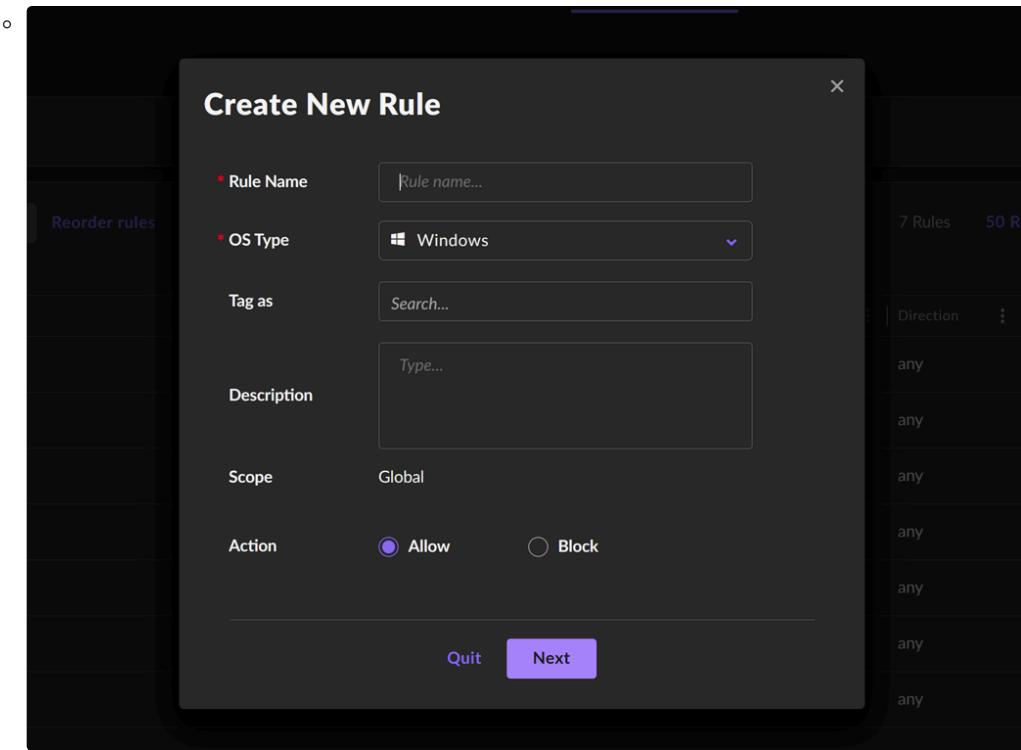
2. Navigate to Network Control:

- Click on the “NETWORK CONTROL” tab.



3. Create a New Rule:

- Ensure that the “Firewall” category is selected.
- Click on “New Rule.”



4. Configure the Rule:

- **Rule Name:** Use safe practices to name the blocked URL. Consider the type of attack and where it was detected. Example: “URL[.]com CredHarvester Defender.”
- **OS Type:** Choose the OS type to which this rule should apply.
- **Tag:** Create a tag (e.g., “Malicious,” “Spam,” etc.).
- **Description:** Explain the details of the incident and why this URL is blocked.
- **Action:** Select “Block” to block the URL.
- Click “Next” to continue the process.

5. Specify the Malicious Domain:

- Navigate to and click on the “Remote Hosts” option.
- Click on the “Address” dropdown and select “FQDN.”
- Add the malicious domain without using square brackets (e.g., “[Example Domain](#)”).
- Click on “Enable rule immediately after saving.”
- Finally, click “Save.”

Action Allow
Scope Global

Rule parameters
Tip! You can press tab to move to the next parameter

Protocol +

Application Any +

Direction Any +

Local host Any +

Local port Any +

Remote port Any +

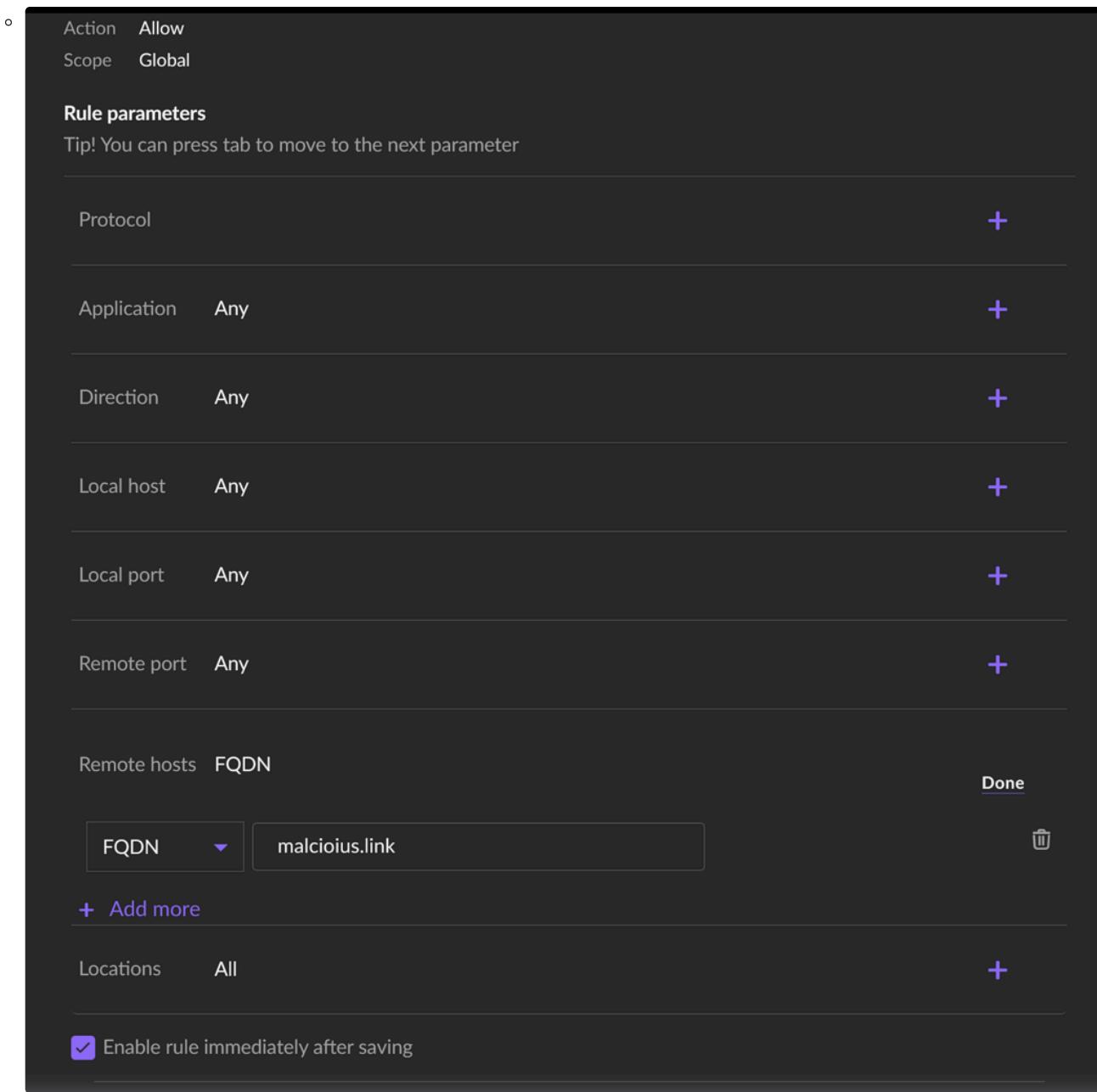
Remote hosts FQDN [Done](#)

FQDN ▾ malcioius.link [Delete](#)

+ Add more

Locations All +

Enable rule immediately after saving



6. Double-Check the Rule:

- Click on the rule you created to confirm that everything is in place.

Remember to exercise caution when using blocking capabilities in SentinelOne, as irresponsible use could disrupt company operations. Follow each step precisely as outlined in this playbook.

Improvements

Add all possible improvements here:

General Documentation

Coming Soon

Forcefield-support : IP Unblock request

Table of contents

Table of contents

Purpose

Description

Note

IP Unblocking

1. Notification sent in the #security-private channel
2. Go to the thread in the #forcefield-support channel
3. Reason for the Block
4. Risk Assessment & Verification
5. Sample work note

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• GCSO• SLACK: sec-mon• EMAIL: gcso@godaddy.com |
| Process Owner | vrajasekharan@godaddy.com |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | |
| Training Log | |

Description

This playbook is a guide on how to unblock an IP which is request to unblock on the channel #forcefield-support.

Note

The procedure is to handle the IP unblock request coming on #forcefield-support channel. The unblock request will be forwarding to Security Private channel. For monitoring we will use the single channel as security Private and the findings will be updated on the #forcefield-support

channel directly. A link will be there in security-private channel directing to concerned IP unblock request.

IP Unblocking

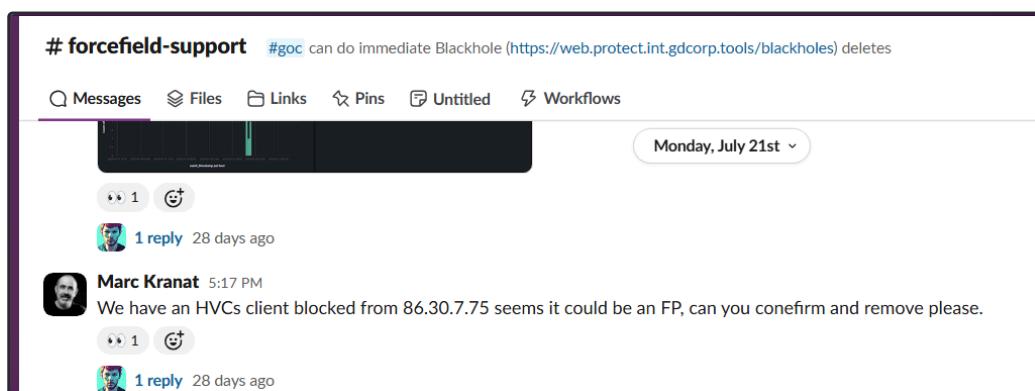
1. Notification sent in the #security-private channel

Once the notification comes in security-Private channel, need to make ensure that GCSO is acknowledging the message. There will be a link which will direct to actual IP unblock request posted by the user on #forcefeild-support channel.

2. Go to the thread in the #forcefield-support channel

Link on security-Private channel will direct to #forcefeild-support channel and the specific IP unblock request. Please give an acknowledgment there as well to keep the reported know that, we are started work on the request.

Sample unblock request in #forcefield-support channel would like below



3. Reason for the Block

Check on the web protect to see when the IP is blocked and any reason for blocking the IP. The web protect can be accessed through <https://web.protect.int.gdcorp.tools/mitigations>. Check on Splunk and verify the IP is part of any security alerts or not. Gather the basic IP information using OSINT tools.

4. Risk Assessment & Verification

Re-assess the risk level of the IP. Check to see if the IP is still exhibiting malicious behavior or not. This can be identified using OSINT tools like AbuseIPDB and check for that last IoA report time.

This IP address has been reported a total of **5** times from 2 distinct sources. 23.90.109.14 was first reported on April 15th 2025, and the most recent report was **4 minutes ago**.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

| Reporter | IoA Timestamp (UTC) | Comment | Categories |
|---------------------|--|---------|------------------------|
| ✓ madeit Belgium | 2025-08-18 08:03:21 (4 minutes ago) | | Email Spam Spoofing |

If the report time is more than 4 weeks , then we are safe to consider to unblock. If it is still part of active threat activity due to latest reports check for the business usecase to identify clearly identify the IP unblock request. Evaluate if the IP is from a trusted source, such as a customer, partner etc. Check and see is there an ongoing business impact due to the block. This can be identified by contacting the reporter.

Check the IP on Splunk to see if we have any recent hits from the IP or not. If we have any hits, then identify the kind of traffic and hitting on which environment (Hosting or non-hosting).

5. Sample work note

A structure of work note that will help to summarize and close the IP block request. The notes should contain the below details.

Who reported the issue or requested the unblock

What service or system was impacted

When was the IP blocked

What was the activity pattern of the IP before it was blocked

Was there any malicious behavior or any repeated offenses.

Phishing email analysis in Proofpoint

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description:](#)
- [Proofpoint access & navigation](#)
 - [Incidents](#)
 - [Messages](#)
- [Investigation Process](#)
 - [Assignment:](#)
 - [Investigation:](#)
 - [Mitigation:](#)
- [Improvements](#)
- [Common False Positives](#)
- [General Documentation](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic |

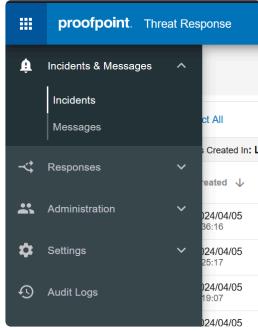
Description:

This playbook is made to explain how to navigate Proofpoint for email analysis and remediation.

Proofpoint access & navigation

To access Proofpoint Threat Response, follow these steps:

1. Visit Proofpoint Threat Response. <https://threatresponse.proofpoint.com>
2. On the left side, navigate to **Incidents & Messages**.



There are two fields you can choose from:

Incidents

This section contains multiple reports and detections grouped by an incident.

A screenshot of the Proofpoint Threat Response interface showing the 'Incidents' list view. The top navigation bar shows 'proofpoint Threat Response'. The left sidebar has a 'Incidents' section expanded. The main area displays a table of incidents with columns: Priority, Created (sorted), State, Incident ID, Incident Title, Team, Assignee, Rep. #, Closed, and Source(s). There are 1-20 of 249 incidents listed, all marked as 'Open'. The table includes rows for various incidents with details like 'INC-258' for an abuse report from 'lisa@prodidyl.com' and 'INC-259' for another abuse report from 'lisa@prodidyl.com'. A 'Create Incident' button is visible at the top right of the table area.

The grouping is done by Proofpoint and can be based on the same sender, subject, etc. Inside each incident, you can find several fields:

- **Messages:** Displays alerts that have been bundled in the same incident

| Received by Thread | Disposition | Source | Association | Recipient | Message Status | Remediation Status | Sender | Subject |
|---------------------|-------------|---------------|-----------------|-----------------------------------|-------------------|--|-----------------------|---------|
| 2024/04/05 18:23:01 | Low Risk | Abuse Mailbox | Initial Message | tdw@godaddy.com First Reporter | Message read | Quarantine Not Attempted Low Risk Message | ayanimail@personal... | Payment |
| 2024/04/05 18:23:01 | Low Risk | Abuse Mailbox | Same Message ID | ayanimail@personal... | Message delivered | Quarantine Not Attempted Low Risk Message | ayanimail@personal... | Payment |

- **Summary:** Provides more details about the incident and allows you to assign it to yourself.

| Total Messages | Message Sources | Reported False Positive |
|----------------|-----------------|-------------------------|
| 2 | Abuse Mailbox | 0 |

Created: 2024/04/05 15:23:02
Last updated: 2024/04/05 15:26:50
Closed: -
Reopened: -

- **Activities:** Shows the steps that Proofpoint or analysts have taken so far.

| | |
|---------------------|---|
| 2024/04/05 15:23:02 | System created this incident with title "tdw@godaddy.com reported a message "Payment" |
| 2024/04/05 15:26:50 | System updated the priority to "Medium" Priority was previously used |

- **Comments:** Allows you to leave a comment and see what other comments have been left.

[Incidents](#) Incident ID: INC-266

tdw[@godaddy].com reported a message "Payment"
Created: 2024/04/05, 15:23 • Last updated: a few seconds ago • Assignee: Unassigned • Priority: Medium • State: Open

[Close Incident](#)

| Messages | Summary | Activities | Comments |
|-----------|---------|------------|----------|
| 1 Comment | | | |
| | | | |

Add a comment

+ New Comment

Darko Zoric
Test
a few seconds ago

Messages

This section displays individual alerts with more details such as Disposition, Recipient, Sender, Remediation Status, etc.

By selecting a checkbox on the left of the alert, you can select the alert to automate tasks by clicking on **Run Workflow**.

This will ease your remediation steps.

| Messages | | | | | | | |
|---------------------------------|---------------|-------------------------------|--|-------------------------|-------------|-------------------|----------------------------------|
| 1-20 of 451 Messages Select All | | | | | | | |
| Messages Received in Last week | | | | | | | |
| Received by Thread... | Disposition | Recipient | Remediation Status | Sender | Incident(s) | Message Status | Subject |
| 2024/04/05 15:23:01 | Low Risk | ayimail@personalizedemail.com | Quarantine Not Attempted Low Risk Message | ayimail@personalized... | INC-286 | Message delivered | Payment |
| 2024/04/05 15:23:01 | Low Risk | mbg@godaddy.com | Quarantine Not Attempted Low Risk Message | ayimail@personalized... | INC-286 | Message read | Payment |
| 2024/04/05 15:01:32 | Spam | coinger@godaddy.com | Message Not Found | microsoftexchange329... | INC-285 | Message unread | Undeliverable: For your oe... |
| 2024/04/05 15:01:32 | Spam | clint@godaddy.com | Quarantine Successful | microsoftexchange329... | INC-285 | Message unread | Undeliverable: For your oe... |
| 2024/04/05 09:36:15 | Low Risk | 056766-ca40-40cb-85fa-70f... | Quarantine Not Attempted Low Risk Message | chr1822@yodality.c... | INC-284 | Message delivered | [Phish Alert] Hey Chris, we'... |
| 2024/04/05 09:36:15 | Low Risk | laffine@godaddy.com | Quarantine Not Attempted Low Risk Message | chr1822@yodality.c... | INC-284 | Message unread | [Phish Alert] Hey Chris, we'... |
| 2024/04/05 09:36:15 | Spam | dzmonr@godaddy.com | Quarantine Successful | dzmonr@eucnserve.net | INC-283 | Message read | For your own safety, I highly... |
| 2024/04/05 09:36:15 | Spam | dzmonr@eucnserve.net | Distribution List Received | dzmonr@eucnserve.net | INC-283 | Message delivered | For your own safety, I highly... |
| 2024/04/05 09:36:15 | Manual Review | bauer797@godaddy.com | Quarantine Not Attempted | murphyb@gmail.com | INC-282 | Message read | Fwd: FW: Important account... |
| 2024/04/05 09:36:15 | Low Risk | newslette@abcjour... | Quarantine Not Attempted Low Risk Message | newslette@abcjour... | INC-281 | Message read | Read All About Emphasis: ... |
| 2024/04/05 04:19 | Manual Review | enroll100@godaddy.com | Quarantine Not Attempted | chf600@gmail.com | INC-280 | Message read | Fwd: Urgent: You'll lose acc... |

If you click on any of the alerts, **Message Details** will pop up on the right side of the screen with more details on the alert such as:

- **Message - Overview:** Provides more information about the email, links, and attachments.

Message Details

Quarantine Not Attempted

Message Forensics Timeline Comments

Headers

| | |
|-----------------------|---|
| Received by user | 2024/04/05 15:12:07 (UTC+02:00) |
| Sender | ayanismail@personalizedcareforall.com |
| Recipient(s) | ayanismail@personalizedcareforall.com |
| Reply-to | |
| Subject | Payment |
| Message ID | <SN4PR16MB486468D40F215DEF6FEC142CB4032@SN4PR16MB4864.namprd16.pod.outlook.com> |
| Via Distribution List | No |
| Message disposition | Low Risk |

2 URLs and 2 Attachments

- https://nam10.safelinks.protection.outlook.com/?url=http... [View link in Proofpoint Browser Isolation](#)
- http://www.personalizedcareforall.com/ [View link in Proofpoint Browser Isolation](#)
- Payment Details.msg [Download](#)
- Outlook-psnqvzf.png [Download](#)

- **Headers:** Displays parsed header details from the examined email.

Message Details

Quarantine Not Attempted

Message Forensics Timeline Comments

Headers

6 Headers

| | Header | Value |
|---|------------------|---|
| ① | Received by user | 2024/04/05 15:12:07 (UTC+02:00) |
| ② | Sender | ayanismail@personalizedcareforall.com |
| ③ | Recipient(s) | ayanismail@personalizedcareforall.com |
| ④ | Reply-to | |
| ⑤ | Subject | Payment |
| ⑥ | Message ID | <SN4PR16MB486468D40F215DEF6FEC142CB4032@SN- |

- **Forensics:** Provides extra details about the email, Sender, Recipient, etc.

Message Details

Quarantine Not Attempted

- Message**
- Forensics** (selected)
- Timeline**
- Comments**

Overview

| | |
|-----------------------------|-------------------------------------|
| Received by Threat Response | 2024/04/05 15:23:01 (UTC+02:00) |
| Disposition | Low Risk |
| Source name | Abuse Mailbox |
| Association | Initial Message |
| Message status | Message delivered |
| Threat name | This threat is not available in TAP |

Sender

| | |
|-----------------|---------------------------------------|
| Envelope Sender | ayanismail@personalizedcareforall.com |
| Header From | |
| Header Reply-to | |
| Sender IP | |

Recipient

| | |
|--------------------|---------------------------------------|
| Envelope Recipient | ayanismail@personalizedcareforall.com |
| Header To | |

- **Timeline:** Shows what steps have been taken by Proofpoint and analysts on this particular alert.

Message Details

Quarantine Not Attempted

- Message**
- Forensics**
- Timeline** (selected)
- Comments**

2024/04/05 15:12:07 User received message

2024/04/05 15:23:01 Message received by Threat Response

2024/04/05 15:23:04 Message submitted to CLEAR
CLEAR ID: b889d9e8-c4f4-48e5-9440-3485b57b4822

2024/04/05 15:26:50 System updated the disposition Low Risk

2024/04/05 15:26:50 Message processed by CLEAR with Verdict Low Risk
CLEAR ID: b889d9e8-c4f4-48e5-9440-3485b57b4822
Confidence: Medium

- **Comments:** Allows you to add a comment or read the existing ones left by analysts.

Investigation Process

Assignment:

- Navigate to **Incidents**.
- Select the checkbox on the unassigned incident and assign it to yourself.
- For **Team**, select the team you belong to.
- For **Assignee**, select yourself (or any other person you want to assign this incident to).
- Leave a comment (for the beginning, it is okay just to inform us that you started to investigate).
- Save changes.

The screenshot shows a Splunk search results page for 'Open, incidents created in: Last week'. A modal dialog box titled 'Assign Incident' is open, overlaid on the main table. The dialog has fields for 'Team' (set to 'GCSO'), 'Assignee' (set to 'Select Assignee'), and 'Add comment' (with the placeholder 'Add comment'). At the bottom right of the dialog is a 'Save Changes' button. The main table lists 12 incidents, each with columns for Priority, Created, State, Incident ID, Incident Title, Team, Assignee, Msg #, Owner, and Source(s). The first incident in the list has a checked checkbox in the Priority column.

Investigation:

- Enter the incident by clicking on the **Incident ID**.
- Click on the individual alert to access more information.
- Use all the information that you gathered to get to a conclusion.

Note: Do not be afraid to use any other services like O365, Splunk, IsItBad mailbox, etc., to help you in your investigations.

Mitigation:

- Once you've done your investigation and concluded that it's malicious, follow these steps:
 - **Quarantine the email:** Select the alert and run “Run Workflow”. From the drop-down menu, choose **Quarantine Messages GoDaddy**.
 - **Inform the user:** For this, you can use automated actions to speed up the process or send it manually by using a template from the Phishing playbook. Select the alert and click on **Run Workflow** and choose one of the automated replies.

- **Check if any other email of this kind has been sent to any other user:** For this, you will have to use **Microsoft Defender - Explore**.

Note: If it turns out that this email is a part of a phishing campaign, escalate the case to a gcso-internal group in Slack

Improvements

Add all possible improvements here:

Common False Positives

General Documentation

Coming Soon

Remediate customer hosting account

This playbook has moved to a new location (Hosting Security SOC Confluence Space): [Remediate customer hosting account](#)

Communication Procedure (Draft)

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[Communication](#)

[Validation of Activities](#)

[Requesting additional information](#)

Purpose

| | |
|------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | David Hernandez |
| Last Review Date | 2/28/25 darko |
| Training Log | |

Description

This playbook is a guide on how to contact employees for additional information or validation of activities.

Communication

In all scenarios of communication, it is important your message is clear and concise. It is also important that you make sure there is no grammar issues.

Please avoid exposing information about the security incident until you know you are talking to someone that can help.

Here are a few guidelines to pay attention to when reaching to the users:

- **Introduce yourself properly** - introduce yourself politely and explain from which team you are reaching them. Just saying GCSO team is not enough as most people don't know what

the acronym stands for.

- **Assume the User is not technical** - Users do not have to be technical and most likely won't understand technical details.
- **Do not share incident details** if you don't absolutely have to - Security Incidents are confidential and analysts job is to protect the confidentiality. Formulate sentences carefully and do not provide any confidential information to the user
- **User word is not an evidence** - even if the user is saying something, take it with a grain of salt. Use users to help you prove a hypothesis or help you make a decision. People are often lying, especially when they need to take a responsibility for their own mistakes.
- **Document the conversation** - Always document the conversation in alert comment to protect yourself from false accusations and to leave evidence to other analysts so they don't have to reach out to the same user multiple times.

You may always use the following templates to start a conversation.

Hi <User>,

I am <GCSO Member>, with GCSO (Information Security).

Validation of Activities

If you ever need to validate a user's activities, please be sure activity is not suspicious or potentially malicious. Additionally, only engage them if you have validated all signs are legit.

Preferably, in situations where a server is involved, reach out to the server owner oncall primary. This can be found in cmdb.

1st message.

I am reviewing a security event on the following <server/workstation>. Is this something you can assist with or do you know someone that can?

2nd message

We noticed the following activities on the machine. Can you please validate if this is expected activity.

include as clear as possible:

The commands or activities you need information on.

Requesting additional information

Responding to Security Reports in Slack

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description](#)
- [Process](#)
- [Improvements](#)
- [General Documentation](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic |

Description

To effectively handle security alerts in Slack channels, it's crucial to approach them with a structured and efficient process akin to technical customer support. Each report should be treated as a ticket with a defined lifecycle, ensuring timely resolution and clear communication with the reporter.

Process

1. Receiving Report:

- When a user submits a security report, it appears in the designated Slack channel.

2. Ticket Assignment:

- View each submitted report as a new customer ticket.
- Assume responsibility for resolving it promptly and informing the submitter of the outcome.

3. User Notification:

- Notify the user that you've initiated work on the report by replying within the Slack thread.

4. Report Understanding:

- Dedicate time to thoroughly understand the reported issue.
- Research unfamiliar terms, problems, bugs, tools, etc., utilizing Slack for collaboration and information gathering.

5. Problem Addressing:

- Utilize acquired knowledge to determine the appropriate course of action.
- Decide whether the issue can be resolved internally or needs escalation to another party.
- Seek guidance from the #security-analyst-collab channel if uncertain about the responsible group.

6. User Communication:

- Update the user on the progress of the report by replying within the thread.
- Communicate your findings and proposed next steps to maintain transparency throughout the process.

7. Follow-Up:

- Monitor the security report until resolution.
- If unable to complete the task, assign it to another team member by tagging them in the thread.

8. Closure Report:

- Document all steps taken and resolutions achieved in detail.
- Compile a closure report summarizing the entire process for future reference.

9. Additional Actions:

- Check with the reporter if any further action is required on the reported case.

Improvements

Add all possible improvements here:

General Documentation

Coming Soon

OnCall Escalation Procedure

Table of contents

- Table of contents
- Purpose
 - GCSO Identifies a Confirmed Threat
 - All Hours
 - GCSO Analyst needs assistance with an alert or request (IR)
 - During US/UK/India Business Hours
 - Acknowledgement From Escalation
 - GCSO shall not consider the incident escalated until the receiving party or higher Tier acknowledges the escalation
 - Escalation Format
 - Escalation Details
 - The Analyst may escalate an alert/incident to IR for several reasons
- Expectations for IR
- Email Template
- SOAR Playbook for Escalating Splunk Alerts

Purpose

| | |
|----------------------|--|
| Responsible Team | <ul style="list-style-type: none">• Detection and Monitoring• SLACK: #internal-gcso• EMAIL: GCSO@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | 06/27/2024 by @David Hernandez |
| Requests for Updates | By Email - GCSO@godaddy.com |
| Training Log | By: @David Hernandez 09/12/2023 |

GCSO Identifies a Confirmed Threat

All Hours

| | IR Escalation | Hosting Escalation | Detections Escalation |
|---|---|--|--|
| 1 | <p>@ir-team in the #internal-gcso slack channel.</p> <p>Communication templates GCSO identifies a confirmed threat</p> | <p>Tag @hsde in #hosting-soc slack channel</p> <p>Communication templates GCSO identifies a confirmed threat</p> | <p>Tag @detections in #security-analyst-collab</p> |
| 2 | <p>On-Call Email template below. You will receive a slack notification if correctly executed.</p> <p>email.b7gfjo5x@gd-response.pagerduty.com</p> | <p>On-Call Email template below. You will receive a slack notification if correctly executed</p> <p>hsde-team-email.q64s92zw@gd-response.pagerduty.com</p> | <p>Engage the GOC and have them engage the on-call for detections_engineering</p> <p>Alternatively you may use the pager duty email below.</p> <p>detections-engineering-email.0utaqem2@gd-response.pagerduty.com</p> |

| | | | |
|---|--|--|--|
| 3 | 30min, If no response, engage the GOC and have them engage the on-call for infosec_response | | |
|---|--|--|--|

ⓘ If step 2 fails to function, please move to step 3.

GCSO Analyst needs assistance with an alert or request (IR)

During US/UK/India Business Hours

| | Security Monitoring (US/India) | IR Request | Hosting Request | Detections request |
|---|---|--|---|---|
| 1 | 1. Notify @sec_mon in ##security-analyst-collab | 1. Notify @ir-team in the #internal-gcsco slack channel. | Notify @hsde in the #hosting-soc slack channel. | Tag @detections in #security-analyst-collab |
| 2 | | | | |
| 3 | | | | |

1. Communication must be clear and concise. Such as: <Teams> We need your assistance with the following alert as we can't determine XYZ
2. ONLY engage On-call if you believe this is most likely a threat.

Acknowledgement From Escalation

GCSO shall not consider the incident escalated until the receiving party or higher Tier acknowledges the escalation

1. Expect to have teams state one of the following statements, but not limited too: "I acknowledge", "I am taking a look", "working on it", "I will be there in X minutes"
2. If you believe your escalation was not acknowledged, please request the recipient to acknowledge.

Escalation Format

Please follow the follow Slack Post format

Primary Post:

- 1 Title:
- 2 Request:
- 3 Link:

In the comments section, post your details as referenced below.

This format allows escalations to be clear and concise.

Escalation Details

ⓘ Please prioritize escalating the details from the previous step before organizing the details in the following. This will ensure IR is made aware of an incident escalation as soon as possible.

The Analyst may escalate an alert/incident to IR for several reasons

- In the event the analyst is not able to determine a verdict, the analyst will seek peer assistance. After peer assistance has been sought with no verdict, the analyst will engage IR for assistance.
- Confirmed Activities: Ransomware, Privileged Escalation, Lateral Movement, Persistence, TA Interactive Sessions, Campaigns, Persistent TA Efforts.

When an escalation is engaged, please be prepared to answer the following

Who:

- If an employee is impacted
 - Who are they?
 - Which Department do they work in?
 - Are other employees impacted?
- If a customer is impacted
 - What is their shopper id?

What:

- What happened (include link to event and description of the event)? .
- Are there other instances of malware on the server?
- If a server/workstation is impacted:
 - What is the server name?
 - What environment is it in?
 - What team owns it?
 - What purpose does the server serve?
 - Are other servers impacted
- What IOCs are available if any?

Where:

- Where in the environment did this occur? (Customer, Employee, Server)

Attention to:

- If you have already performed some analysis, please share those details as well.
- If there are details that you think are important to this alert/incident, please note them here.

Expectations for IR

1. Each IR member is responsible for being available during their On-Call period.
 - a. The Incident Response team on-call schedule can be viewed at <http://x.co/oncall>
2. Per the [Time Off Requests](#) process - if time out of office overlaps with OnCall responsibilities coverage must be coordinated.
3. All IR members should have the GOC Phone Numbers whitelisted in their phone to prevent filtering calls. This includes overriding Do Not Disturb settings.
 - a. GOC On-Call Procedures can be viewed at [Incident Management On-Call Policy](#)
 - b. A list of applicable phone numbers can be viewed at [GOC/SNOW Numbers](#)

Email Template

 Communication templates | If No Response within 5m Escalate using one of the following:

SOAR Playbook for Escalating Splunk Alerts

OnCall Escalation Procedure - MC Playbook

By Luis Fernando Garcia Yepes In progress 2 min Add a reaction

Powered by Confluence

Alert Tuning/Changes Request

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[General Documentation](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">DetectionsSLACK: #internal-gcsoEMAIL: detectmon@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | 08/21/2024 |
| Escalation Contact(s) | |
| Requests for Updates | |
| Training Log | |

Description

This playbook is a guide on how to request one or more of the following:

- New Alert
- Tuning Request
- Modifications to an alert or Dashboard
- Modifications or changes to a playbook

General Documentation

1. To request submit a request, head over to [错误 - GoDaddy Jira Cloud](#) and fill the request with the following details.

```
1 Summary: Enter a short title for your request
2
3 Description:
4   - Item impacted: Alert Name or Playbook name.
5   - What would you like accomplished. (Tuning the following alert)
6   - What platform is this for? S1/Splunk/other etc
```

2. Then hit submit

Someone will be assigned your ticket within the SLA. You may have someone reach out to you for more questions.

- i If this request is urgent please be sure to initiate detections On-call and share in #internal-gcso channel

VDI Login via User Impersonation

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[Process](#)

[Step 1 Analysis:](#)

[Step 2 Containment:](#)

[Step 3 Expanding Analysis:](#)

[Step 4 Eradication/Recovery:](#)

[Email Template](#)

Purpose

| | |
|-----------------------|--|
| Responsible Team | <ul style="list-style-type: none">DetectionsSLACK: #internal-gcsoEMAIL: detectmon@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | Sep 25, 2024 |
| Escalation Contact(s) | IR@godaddy.com |
| Requests for Updates | |
| Training Log | |

Description

This playbook is a guide on how to handle the alert “VDI Login via User Impersonation”

Process

Step 1 Analysis:

Identify the *Source* and *Target* users. The alert will represent these fields as:

- “Source User” for the user who authenticated into the VDI environment via Okta

- “Target User” for the user that is opening the Windows session.

Step 2 Containment:

1. Follow the credential mitigation process found [here](#), and inform getitsec **NOT** to assist the user with access until the investigation is complete.
2. Send an [email notification](#) to appropriate team to assist with your investigation

i Do not use the email templates found in the credential mitigation playbook. Use the ones found in the [Email Template](#) section below.

Step 3 Expanding Analysis:

Investigate the root cause of the alert.

1. Was there malicious intent?
2. Was the *Source* user assisting the *Target* user in any manner?

To investigate:

1. Review the user's okta sign-in logs for any suspicious logins or new devices.
2. Review all authentication logs for the *Target/Source* user for suspicious sign-ins or activities.
3. Identify if these two users have recently been found in any notable index=notable or risk events index=risk which may indicate malicious intent or compromise.
4. If possible, review all security alerts including S1 alerts for the source and destination devices.

Step 4 Eradication/Recovery:

- If no malicious intent is found, work with the BPO/Care Team to collect a justification. Once a valid justification is provided, you may ask #get-itsec assist the users impacted in gaining access to their accounts.
- If there is any signs of malicious intent or compromise continue with the incident lifecycle or escalate to the next tier for further analysis.

Email Template

i User details are found in Workday.

 Edit   Share 

Communication templates

 By Thomas Whipple  5 min  Add a reaction

Powered by  Confluence

Spoofed Emails analysis

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Purpose](#)
- [Comments Standard](#)
- [Comments might contain the following](#)
 - [How to Spot a Spoofed Email](#)
 - [Step 1: Check the 'From' Address](#)
 - [Step 2: Examine the 'Reply-To' Field](#)
 - [Step 3: Look for 'Mailed-By' and 'Signed-By' Fields](#)
 - [Step 4: Check Email Headers](#)
 - [Step 5: Use Tools for Verification](#)
 - [Step 6: Critical Thinking](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: GCSO@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - GCSO@godaddy.com |
| Training Log | By: @Darko Zecic 10/14/2024 |

Purpose

Coming Soon

Comments Standard

Some things to pay attention when analyzing emails that might be spoofed.

Comments might contain the following

How to Spot a Spoofed Email

Step 1: Check the ‘From’ Address

1. Verify the Domain:

- Ensure the domain in the ‘from’ address is exactly what you expect. For example, if the email claims to be from PayPal, the domain should be “ Pay, Send and Save Money with P
ayPal” and not something similar like “paypal-mail-server.com”.
- Be cautious of free email services (e.g., Gmail, Hotmail) used in the ‘from’ address, as legitimate companies typically use their own domains.

2. Look for Similar Domains:

- Scammers often register domains that look similar to legitimate ones. For example, “ Pay,
Send and Save Money with PayPal” (with a number 1 instead of an L) or “rnicrosoft.com” (with an RN instead of an M).
- Check for subdomains that might be misleading, such as “paypal.example.com” where “ Example Domain” is the actual domain.

3. Foreign Characters:

- Be aware that domains can include foreign characters that look like standard Latin characters. For example, a Cyrillic ‘A’ can look identical to a Latin ‘A’.
- Use tools like ‘Unicode Inspector’ or ‘ASCII Validator’ to check for non-standard characters.

Step 2: Examine the ‘Reply-To’ Field

1. Different ‘Reply-To’ Address:

- Check if the ‘reply-to’ address is different from the ‘from’ address. Scammers often use a different reply-to address because they don’t have access to the fake ‘from’ address.
- If the reply-to address is a free email service or looks suspicious, it’s likely a scam.

2. Similar Looking ‘Reply-To’ Address:

- Sometimes scammers use a reply-to address that looks similar to the ‘from’ address to make it seem less suspicious.

3. Body of the Email:

- Scammers might include a different reply address in the body of the email, asking you to respond to that instead of the ‘from’ address.

Step 3: Look for ‘Mailed-By’ and ‘Signed-By’ Fields

1. Indicators:

- Check the ‘mailed-by’ and ‘signed-by’ fields. These indicate if the email was sent by an authorized server.
- Major companies should have these fields matching their official domains.

2. ‘Via’ Indicator:

- If it has ‘via’, it means the domain sending the email doesn’t match the ‘from’ address. This can be legitimate for newsletters and other services but can also indicate spoofing.

Step 4: Check Email Headers

1. SPF (Sender Policy Framework):

- SPF verifies if the server sending the email is authorized to do so. A pass means the server is authorized, while a fail indicates it is not.
- Look for terms like ‘pass’, ‘fail’, ‘neutral’, or ‘softfail’ in the SPF results.

2. DKIM (DomainKeys Identified Mail):

- DKIM ensures the email content hasn’t been altered and verifies the sender. A pass indicates the email was not altered and was sent by the claimed domain.
- Check if the DKIM signature matches the ‘from’ domain.

3. DMARC (Domain-based Message Authentication, Reporting & Conformance):

- DMARC combines SPF and DKIM to ensure the email is from the domain it claims to be. A pass means both SPF and DKIM checks align with the ‘from’ domain.
- If DMARC fails, it indicates a potential spoofing attempt.

Step 5: Use Tools for Verification

1. Unicode Inspector:

- Use tools like ‘Unicode Inspector’ to identify individual text characters and check for foreign characters that look like standard ones.

2. ASCII Validator:

- Use an ASCII validator to check for non-ASCII characters. Standard ASCII only includes basic characters, so any deviation can indicate spoofing.

Step 6: Critical Thinking

1. Assess the Content:

- Even if all technical checks pass, use critical thinking to assess the email’s content and context. Scammers can still use legitimate-looking domains to send fraudulent emails.

- Look for signs of phishing, such as urgent language, requests for personal information, or suspicious links.

2. Compare with Previous Emails:

- Compare the suspicious email with previous legitimate emails from the same sender. Look for inconsistencies in the email format, language, and sender information.

Device Intrusion Incidents

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[Incident Life Cycle](#)

[Analysis](#)

[Documentation](#)

[Decomposition and Externalization](#)

[Timeline](#)

[IOC/TTPs](#)

[Below are some high level activities to search for that may indicate a compromise.](#)

[Recon](#)

[Persistence](#)

[Privileged Escalation](#)

[Credential Harvesting](#)

[Lateral Movement](#)

[Exfiltration](#)

[Containment](#)

[Eradication](#)

[Eradicate malware in the following order](#)

[Recovery](#)

[Post-Incident Activity](#)

[Improvements](#)

[Approved and Reviewed by](#)

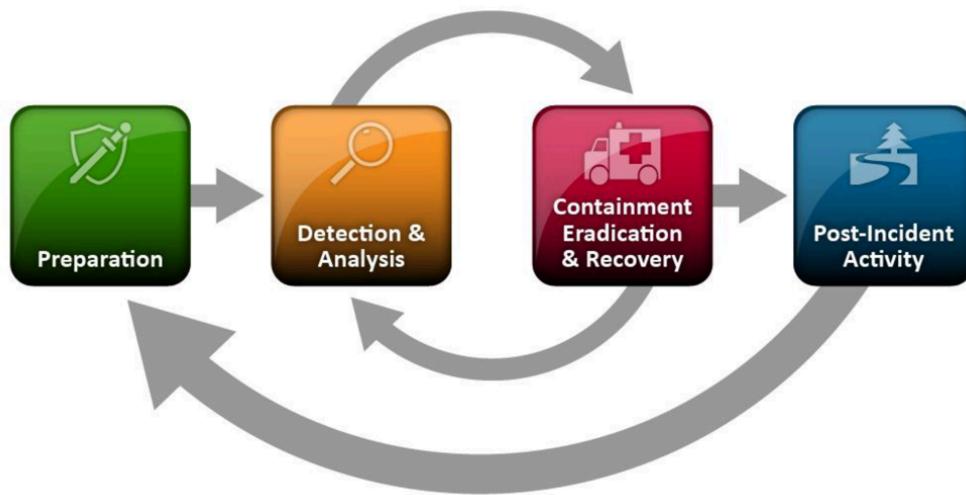
Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Monitoring Team• SLACK: #internal-gcso• EMAIL: GCSO@godaddy.com |
| Process Owner | David Hernandez |
| Last Review Date | |
| Escalation Contact(s) | Darko Zecic, David Hernandez |
| Requests for Updates | |
| Training Log | |

Description

This process provides direction for the analysis and remediation of an endpoint intrusion event (such as AV/EDR events, user virus reports, etc.) and outlines the general process guidelines to be followed by the responding analyst. The process will follow the NIST incident lifecycle.

Incident Life Cycle



Analysis

Analysis will be the most time consuming task, but understand that you can't rush things and do your best to keep stress levels low. Reach out to your peers for assistance if needed. Whether its a user reported incident or alert, we need to validate the compromise and collect all possible IOCs.

Pace yourself and write down information as you find out. in other words get it out of your head before you forget it

1. Understand what you are working with. Type of alert/malware. Rootkit, Trojan, Infostealer, Ransomware, Unauthorized access etc.
2. Was the activity automatically blocked or allowed?
3. Is it a known bad process (bad reputation or commonly known for malicious use)
 - a. use reputation signature to help you find common IOCs
4. Review the process tree if one is available
5. What type of device/scope is impacted? (server, workstation, pci, etc)
6. Who was the activity performed by and was it legitimate?
7. Are there any other alerts for the machine in question?

8. Are there other machines impacted by this malicious/suspicious activity
9. Review the process tree if one is available for other activities performed by the malware
10. Review the raw storyline in detail if available.

Documentation

Decomposition and Externalization

The human mind can only hold approx. 7 items in their head unlike Hernandez who can only hold 2. As such, Decomposition and Externalization techniques should be used to overcome this barrier.

Decomposition: Break things down into bite size pieces. This is to help understand individual pieces before assembling them into a bigger picture.

Externalization: Get data out of your head as soon as you can onto a physical or digital form. This will help you track your progress, but will assist when sharing details with peers. Be sure to do this in an organized manner as a bunch of random thoughts will only make sense **to you** the day you write them.

Timeline

Remember to track the information collected and formulate a timeline of events.

IOC/TTPs

Keep track of IOCs and TTPs in manner that can be searched and used by other teams.

In many cases, TTPs will be used by the detections teams so be sure track where,when,how, and what you found.

- i** If you plan to use live response for your analysis, note that you may be contaminating the scene as simply listing directories could be considered tampering with evidence. As such, be sure to execute a forensics capture when deemed necessary.

Below are some high level activities to search for that may indicate a compromise.

Recon

Examples but not limited too:

- Whoami
- cat /etc/passwd
- net user /domain

- cat /etc/sudoer

Persistence

Examples but not limited too:

- Cron jobs
- Run Keys
- plists
- Scheduled tasks
- start up process
- Authorized SSH keys
- New accounts
- running processes

Privileged Escalation

Examples but not limited too:

- Policy Modification
- Use of domain or location accounts
- Process Injection

Credential Harvesting

Examples but not limited too:

- SAM dumps
- /etc/shadow access
- token hijacking
- Browser credential harvesting
- password sprays
- Kerberoasting
- bash history
- private key access
- keylogger

Lateral Movement

Examples but not limited too:

- Access from non bastion/cyberark devices to servers or other workstations
- Internal Phishing

- Pass the hash/ticket

Exfill

Examples but not limited too:

- Beaconing
- Excessive file transfers or Large file transfers

Containment

Reaching containment is very critical but it can't be done correctly until a thorough analysis has been performed. For example, it may be pointless to run a credential mitigation and restore access if there is a keylogger still running on a user's machine. It is better to:

1. Disable the user's account
2. Identify root cause of compromise
3. Then continue with the remainder of the incident life cycle

When working with workstations the easiest method of containment is device isolation through EDR, but it is important to note that by doing so you will be killing active connections which could be considered IOCs.

i Do not isolate servers without leadership approval or business owner.

i Do not isolate devices without a secondary approval

If device isolation is not possible, we must contain in other manners such as network isolation through firewalls or blocking all IOCs.

Below are other examples of containment:

- Disable the impacted accounts
- Patching vulnerabilities
- Removing keys or accounts used by the threat actor to maintain persistence
- Null route dns queries
- Moving the machine to an isolated vlan

Eradication

During the Eradication phase you will remove all traces of malware or undoing what the threat actor did.

- Note: If isolation was not possible, it is imperative that the incident responder eliminates all traces of malware as soon as possible.

Eradicate malware in the following order

1. If not done so already, perform a forensic capture of the machine(s) impacted
2. Capture and kill all malicious services/processes
3. Capture and eliminate persistence artifacts ie: registry keys, scheduled tasks, cron jobs, plists etc
4. Capture and eliminate all malware artifacts. Examples include but not limited to: exe's, carrier files, payloads, other created files.
5. Capture and remove recently created accounts. Alternatively, run credential mitigation where removal is not possible
6. Capture and review modified files
7. Run a full disk scan

Below are other examples of Eradication:

- Restoring backdoored source code
- Restoring systems from trusted source
- Reimaging a machine

Recovery

Your goal is to return to business as usual (BAU)

- Bring systems back online
- Restore services back to BAU.
- Test mitigations and/or patches are in place correctly
- The incident responder is confident in the endpoint status?

In many cases you might result to reimagine a machine, but be sure to follow the reimagine process if you this route is chosen.

Post-Incident Activity

1. As soon as possible schedule an after action review or retrospective
 - The following should be answered during an Incident Retro if one is held, if not, make note of the questions below and escalate to the appropriate teams if needed.
 - Are there new siem rules that we should created?
 - Are there additional security measures that should be implemented?
 - What went well
 - What can be improved.
2. Finalize your report and/or summary of the events and insure the timeline is up to date

For all other details regarding lesson's learned, follow the Retrospective process.

Improvements

Here you can suggest any improvements to the document

Approved and Reviewed by

| Approver | Task |
|----------|---|
| Darko | DETCTMON-1048: Review and add Comments to intrusions Playbook DONE |
| Emilio | DETCTMON-1049: Review and add Comments to intrusions Playbook DONE |
| Kedwin | DETCTMON-1050: Review and add Comments to intrusions Playbook DONE |
| Luis | DETCTMON-1051: Review and add Comments to i ntrusions Playbook DONE |

Identifying Persistence (Draft)

1. Table of Contents

- [1. Table of Contents](#)
- [2. General Outline](#)
- [3. Universal Tactics](#)
- [4. Windows](#)
 - [4.1. Registry](#)
 - [4.2. Scheduled Tasks](#)
 - [4.3. Command line](#)
 - [4.4. Startup folders](#)
 - [4.5. Security tools](#)
 - [4.5.1. Defender](#)
- [5. macOS](#)
- [6. UNIX](#)
- [7. References](#)

2. General Outline

This knowledge assists in identifying locations where persistence can be found on GoDaddy's top 3 most popular operating systems.

These are not all the tactics for persistence. These are the most common. WFH looking for workstations assigned public IPs

3. Universal Tactics

New accounts

Reverse Shells ie (meterpreter)
Netstat or netsh

4. Windows

4.1. Registry

These keys may need to be modified depending on the security tools used for the discovery.

These is an example of how it may be displayed

Most common to least

HKEY_CURRENT_USER\Software\Microsoft\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

4.2. Scheduled Tasks

You will commonly find the following parent process to show as below

Parent Command
svchost.exe -k netsvcs -p -s Schedule

For a list of all malware types using Task Scheduler, review the mitre page <https://attack.mitre.org/techniques/T1053/005/>

4.3. Command line

How to absube in EDR

schtasks

Powershell

```
Get-ItemPropertyValue -Path $path_softw -Name <Keyname>
New-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "<Keyname>" -Value 822
"reg.exe" add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
```

```
"reg.exe" add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v Entertainment /t REG_SZ /d "%APPDATA%\Entertainment\Entertainment.exe --vrOz" /f
```

4.4. Startup folders

C:\Users<Username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

4.5. Security tools

4.5.1. Defender

```
where RegistryKey has_any ("\"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run",
"\"\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce")
```

5. macOS

```
/Library/LaunchDaemons/
/System/Library/LaunchDaemons/
/System/Library/LaunchAgents
~/Library/LaunchAgents
/Library/Managed Preferences
/etc/periodic
/var/at/jobs
/private/var/db/monadClients
sudo defaults read com.apple.loginwindow
/Library/Preferences/com.apple.loginwindow.plist
<user-home>/.ssh/authorized_keys or root
```

6. UNIX

```
<user-home>/.ssh/authorized_keys or root
/var/spool/cron/crontabs
```

7. References

The Art of Mac Malware - The Guide to Analyzing Malicious Software by Patrick Wardle

<https://attack.mitre.org/tactics/TA0003/>

<https://www.sentinelone.com/blog/how-malware-persists-on-macos/>

<https://attack.mitre.org/techniques/T1037/002/>

GCSO Ticket standards

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description:](#)
 - [Document purpose](#)
 - [Handling an event in ES](#)
 - [Hypothesis and Next Steps](#)
 - [Ticket Hygiene and analysis:](#)
 - [Artifacts](#)
- [Tuning/Whitelisting](#)
- [Ticket Closure](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | pkumarsridharap@godaddy.com |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: pkumarsridharap@godaddy.com |

Description:

This document outlines the standard and minimum requirements for managing and closing the tickets in splunk enterprise security by GCSO team.

Document purpose

The purpose of this document is to:

- Ensure the tickets are completed in standard format by GCSO team.
- Define the minimum standard of information relating to investigation that ticket must contain.
- Ensures the analysis is accurate, understandable and mitigating actions are taken based on the log investigation.

Handling an event in ES

When a member of the GCSO is working on the ticket, it must be assigned to individual GCSO analyst.

Hypothesis and Next Steps

- All tickets are worked by analysts must have an initial note called "**HYPOTHESIS**".
- Hypothesis is basically a statement of an idea or explanation to the logs data (Splunk, SentinelOne, O365 ..etc.). It is important to clarify that hypothesis is not a copy paste of the event detection (UC Name, event description, raw data etc..)
- Hypothesis & next steps must be reviewed together by the Senior Analyst OR at least by other analyst as a part(4 eye check principal).
- Based on the analyst criteria, The detection artifacts and story will be reviewed to understand the context of the detections.
- If the analyst thinks that the ticket needs further escalation, analyst should post the alert details in the "**security-analyst-collab**" channel for further assistance.

5W's:

All tickets must have a note that include 5 W's.

- o **Who** – Added as user account or email account, It's role and permissions.
- o **What** – Refers to the key indicators of the alert(IOC/IOA).
- o **Where** – Added as a system name, Application, location etc.
- o **When** – Added as a date occurred – Enter time format(In UTC)
- o **Why** – Identify the root cause of the activity performed by the user/Account identified.

Ticket Hygiene and analysis:

Notes must be clearly reflect the analysis and listing all the steps taken that supports the conclusion and activities performed. Notes must mention any finding that pose the risk to GoDaddy.

Full root cause analysis must be completed for every alert even if the threat is blocked by the security controls.

5.1 Notes and analysis:

- Document every information that might affect the confidentiality, Integrity or availability of GoDaddy systems.
- Document every analysis performed and the result is discovered regardless of whether the results are relevant/useful. This documentation helps allows the next shift analysts (or) future readers to know what steps are already undertaken. So that they don't repeat the same analysis.
- Additionally, this document can provide guidance on other tickets, describing what techniques are potentially useful for similar alerts.
- Avoid generic notes which don't provide descriptive value. Context should always made clear. Avoid low-level notes. Such as "User manager responded". A better note should provide a clear information which allows a conclusion such as "User line manager responded that they are aware of the activity & it is approved".

Artifacts

Artifacts relevant to the investigation such as Ip, hostname, URL, Domain, filename, filepath, hash values etc.

Should be mentioned in the ticket notes.

Tuning/Whitelisting

When there is a unusual or repeated triggered alert, Analyst should consider performing the whitelisting or tuning of the UC. A jira ticket should be raised to detections team.

Ticket Closure

Upon investigation, The alerts can be closed with the appropriate categories.

| Label | Description |
|--|---|
| Benign Positive - Suspicious But Expected | Issue has been classified as benign. Not Malicious |
| Benign Positive - Legitimate Business Activity | Issue has been classified as not suspicious |
| False Positive - Inaccurate Data | Issue has been classified as a false positive due to inaccurate data. |
| False Positive - Incorrect Analytic Logic | Issue has been classified as a false positive due to incorrect analytic logic. |
| Other | Issue has been classified as other. |
| Out Of Scope | An event outside the defined roles set to review. |
| True Positive - Escalated | Event has been escalated to IR |
| True Positive - Suspicious Activity | Malicious activity has been detected. (No further Escalation is needed outside of our team) |

Security MailBox Integration with Splunk

Table of Contents

- [Table of Contents](#)
- [Purpose](#)
- [Summary](#)
- [Responding to Notables](#)
- [Security@ Scenarios](#)
- [SecurityBreach@ Scenarios](#)
- [Splunk SOAR - Mailbox Integration](#)
- [Improvements/Suggestions](#)
- [Implemented Improvements](#)

Purpose

This process provides direction for the handling of communications to the Security@ general mailbox. This mailbox serves as a common point of contact for most general security requests from internal entities. Some of the specific use-cases which are seen via this communication method are:

- [Coordinated Vulnerability Disclosure \(CVD\) Notifications](#)
- Reports of Impersonation of GoDaddy (Websites, Phishing Attempts, etc.)
- External Reports of Malicious Customer Activity (Malware, Phishing, Spam, etc.)
- Internal Reports of Suspicious Activity (Phishing, Physical Behavior, etc.)
- General Solicitations (Security Vendors, Services, SPAM, etc.)
- General Security-related Inquiries

Responsible Team

For Splunk Playbook:

- Detections team
- Email: detections@godaddy.com
- Slack: @detections

For Information regarding the notables:

- Incident Response

| | |
|-----------------------|---|
| | <ul style="list-style-type: none"> SLACK: #internal-gcso, #security-analyst-collab EMAIL: ir@godaddy.com |
| Process Owner | detections@godaddy.com |
| Last Review Date | 17 Dec 2024 (Kiran M, Darko Zecic) |
| Escalation Contact(s) | dhernandez2@godaddy.com , twhipple1@godaddy.com |
| Requests for Updates | <p>For Playbook - detections@godaddy.com</p> <p>For Troubleshooting Process: ir@godaddy.com</p> |
| Training Log | |

Summary

- The Article briefs about how to respond to notables created via Splunk SOAR, which are reported to security@godaddy.com or reported as isitbad.
- The Article also briefs about the integration between Splunk SOAR and the security mailbox.

Responding to Notables

- GCSO will receive a Splunk notable with title as “Security@“.
- Follow the link provided in the description of the notable, which is named as “Alert Source Link“ for more information about the reported mail.

| | | | | | | | | | |
|--|--|------------------|--|---|---------|--------------|--|--------|--|
| Security@ - kmanju@godaddy.com - FW: 'Soar Quotes testing' | Closed | ns01@godaddy.com | -- | -- | Notable | Today, 08:33 | Benign Positive - Legitimate Business Activity | Threat | |
| Description | | | | | | | | | |
| Kindly check the security@godaddy.com mailbox for more info on the notable. NOTE: Check the email link url to access the mail chain.--Check this link for a playbook on steps for triaging this notable: https://godaddy-corp.atlassian.net/wiki/x/A55y2w | | | | | | | Related Investigations | | |
| Currently not investigated. | | | | | | | History | | |
| Additional Fields | Value | Action | 17 Dec 2024 08:59 | ns01@g... | | | | | |
| Alert Source Link | https://outlook.office365.com/owa/ | ▼ | Security@ - kmanju@godaddy.com - FW: 'Soar Quotes testing' | | | | | | |
| ItemID=AAMkADQ0ZjIzNTiiLWFIMjYtNDdmMSIiY2QxLTfkNmIwMzQ1NWJmMgBGAAAAAABYptovqV6IS5QnxBy%2Bly5pBwDcSrPHMcwvSLztCKT9J93IAArf743%2FAA%3D&exvsurl=1&viewmodel=ReadMessageItem | | | Description | | | | | | |
| Rule Description | Kindly check the security@godaddy.com mailbox for more info on the notable. NOTE: Check the email link url to access the mail chain.--Check this link for a playbook on steps for triaging this notable: https://godaddy-corp.atlassian.net/wiki/x/A55y2w | ▼ | Kindly check the security@godaddy.com mailbox for more info on the notable. NOTE: Check the email link url to access the mail chain.--Check this link for a playbook on steps for triaging this notable: https://godaddy-corp.atlassian.net/wiki/x/A55y2w | | | | | | |
| Rule Name | Security Mailbox Automated Notable Creator | ▼ | Alert Source Link | https://outlook.office365.com/owa/?ItemID=AAMkADQ0ZjIzNTiiLWFIMjYtNDdmMSIiY2QxLTfkNmIwMzQ1NWJmMgBGAAAAAABYptovqV6IS5QnxBy%2Bly5pBwDcSrPHMcwvSLztCKT9J93IAArf743%2FAA%3D&exvsurl=1&viewmodel=ReadMessageItem | | | | | |
| Sender | kmanju@godaddy.com | ▼ | Rule Description | Kindly check the security@godaddy.com mailbox for more info on the notable. NOTE: Check the email link url to access the mail chain.--Check this link for a playbook on steps for triaging this notable: https://godaddy-corp.atlassian.net/wiki/x/A55y2w | | | | | |
| Severity | high | ▼ | | | | | | | |
| Subject | FW: 'Soar Quotes testing' | ▼ | | | | | | | |
| Event Details | | | | | | | | | |

3. Review the notable to identify the communication type and/or scenario.

4. Escalate to Tier 2:

- a. Server related compromise
- b. Social Engineering attempt
- c. Data breach

Security@ Scenarios

| | | | |
|----------------------------|--|---------|-------|
| GoDaddy Impersonation | <ul style="list-style-type: none"> • If valid, report via FoS Abuse Form • If not, Close False Positive | ENG-DCU | GDP |
| Customer Abuse Report | <ul style="list-style-type: none"> • Report via FoS Abuse Form <ul style="list-style-type: none"> ◦ If this is not possible email to abuse@godaddy.com | ENG-DCU | ABUSE |
| Customer Security Concerns | Close False Positive - No further action | --- | CARE |

| | | | |
|-------------------------------|--|--|--------|
| Suspicious Internal Activity | <ul style="list-style-type: none"> If Cyber related - Review and determine if event can be taken care of by GCSO. If not, escalate to monitoring or L3 in #security-analyst-collab, if analysts are not available or doesn't respond in 15 minutes, then escalate to IR in #internal-gcso If Physical related - Notify scc@godaddy.com via email. | <ul style="list-style-type: none"> infosec_response Physical Security Command Center | EMP |
| Threats or Threat Reports | <ul style="list-style-type: none"> If this is a received threat (not a report from OCEO, WSC, etc.), immediately notify #workplace-services via Slack If this is a Threat Report (from OCEO, WSC, etc.), verify scc@godaddy.com was included in the recipients and report during standup | Physical Security Command Center | THREAT |
| General Solicitations OR SPAM | Close False Positive - No further action | --- | SPAM |

| | | | |
|------------------------------------|--|-----|------|
| General Security-Related Inquiries | <ul style="list-style-type: none"> Review and determine if event can be taken care of by GCSO. If not, Escalate to monitoring or L3 in #security-analyst-collab, if analysts are not available or doesn't respond in 15 minutes, notify Incident Response via Slack/Email | --- | MISC |
|------------------------------------|--|-----|------|

SecurityBreach@ Scenarios

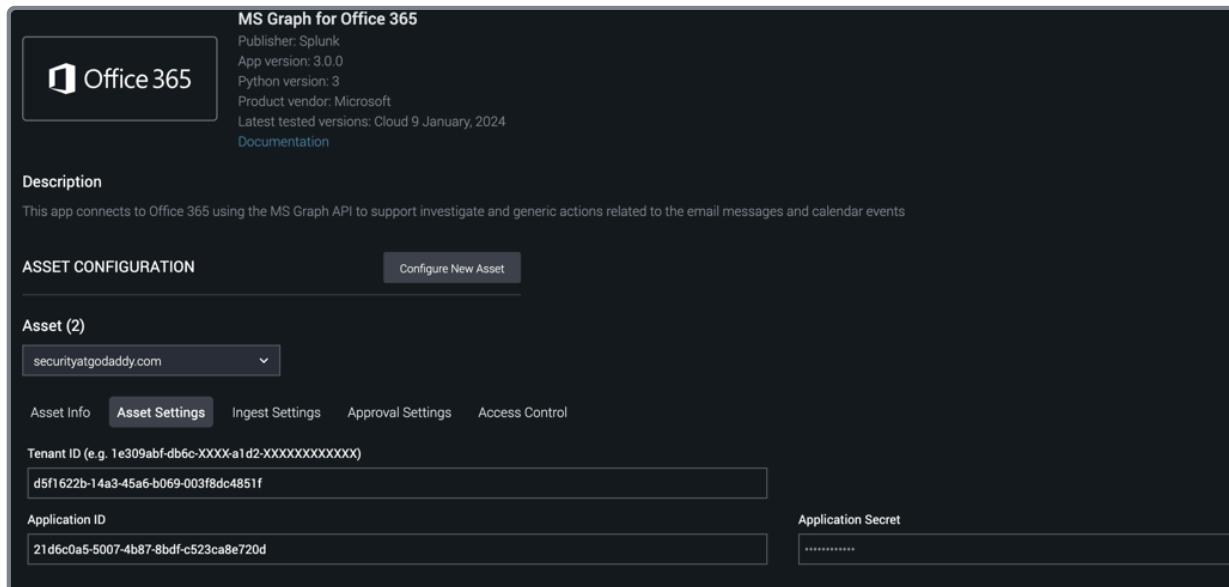
| | | | |
|-------------------------------------|--|--|--------|
| Vendor Security Breach Notification | <ul style="list-style-type: none"> Review and determine if event can be taken care of by GCSO Escalate to monitoring or L3 in #security-analyst-collab, if analysts are not available or doesn't respond in 15 minutes and immediately notify Incident Response via Slack/Email | --- | THREAT |
| Suspicious Internal Activity | <ul style="list-style-type: none"> If Cyber related - Review and determine if event can be taken care of by GCSO. If not, | <ul style="list-style-type: none"> infosec_response Physical Security Command Center | EMP |

| | | | |
|------------------------------------|---|-----|------|
| | <p>Escalate to monitoring or L3 in #security-analyst-collab, if analysts are not available or doesn't respond in 15 minutes then, escalate to IR in #internal-gcso group</p> <ul style="list-style-type: none"> • If Physical related - Notify scc@godaddy.com via email. | | |
| General Solicitations OR SPAM | <p>Close False Positive - No further action</p> | --- | SPAM |
| General Security-Related Inquiries | <ul style="list-style-type: none"> • Review and determine if event can be taken care of by GCSO. If not, Escalate to monitoring or L3 in #security-analyst-collab, if analysts are not available or doesn't respond in 15 minutes then, escalate to IR in #internal-gcso group | --- | MISC |

The Integration is primarily done using Graph API, which grants the read access to security mailbox.

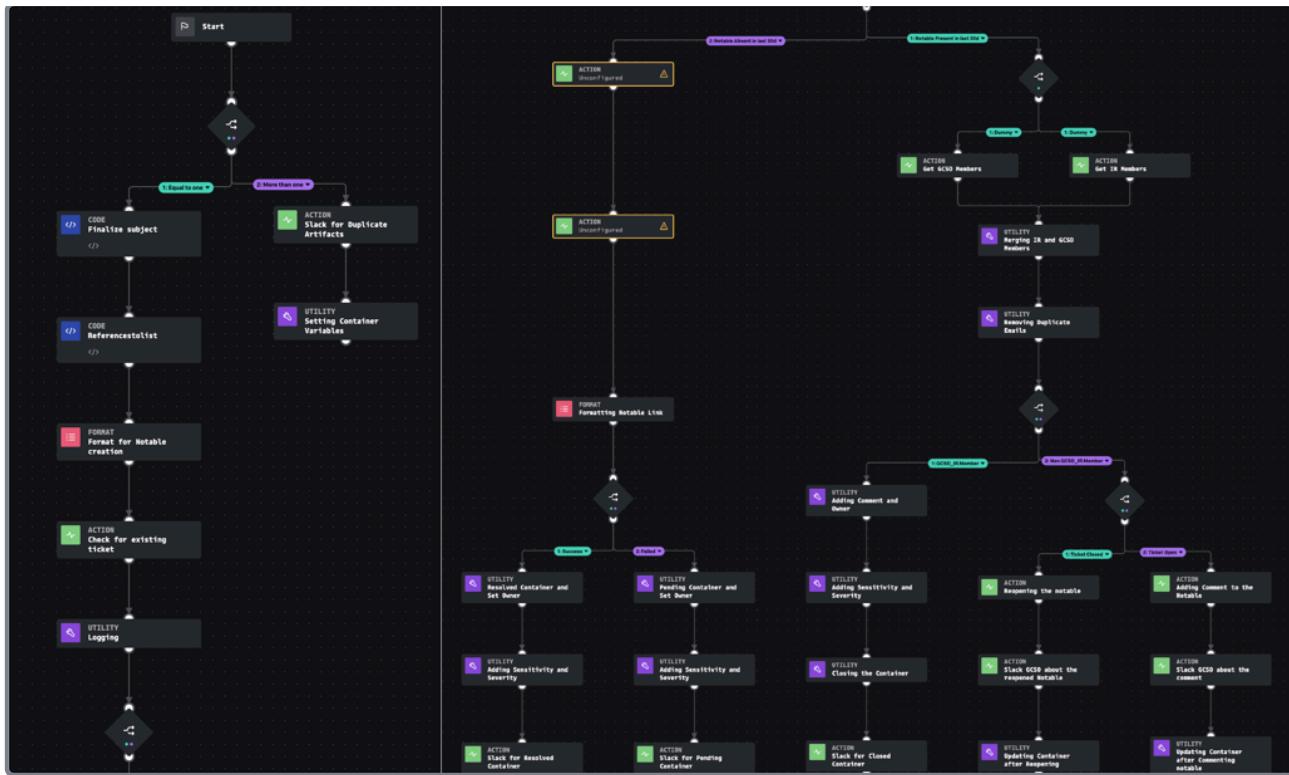
- **Splunk SOAR Asset creation:**

- The below image shows the asset created in splunk soar under the app called “MS Graph for Office 365“.
- The credentials obtained from Azure graph API will be added in the below asset and will be used to integrate Splunk SOAR and Security Mailbox.
- The Asset will execute **every 2 mins** and fetch the latest data from the mailbox and store it under the label “**securitybreachmail**“.
- Based on the label the playbook will automatically execute as soon as the data is ingested in Splunk SOAR.



- **Splunk SOAR Playbook:**

- A SOAR Playbook has been created under the name “Security Mailbox Automation“, which executes only on the data with label “**securitymail**“ and executes as soon as the data is ingested in SOAR.



Working principle:

The Image on the left basically decides the following things in order:

- Based on the number of artifacts in the container, it will decide whether to move ahead to the next blocks or not for further process. Due to the issue of duplicate artifacts in the same container, this check has been provisioned. If there are more than 1 artifact in the container, then the automation stops if not proceeds to next blocks.
- Once there is just 1 artifact, then the playbook moves to “**Finalize subject**“ block and Finalises the subject of the mail. In this block, If the subject has “double quotes“, it will cause the later splunk notable creation to fail, hence “double quotes“ is replaced with “single quote“.
- Once the subject is finalised, then the playbook moves to “**Referencestolist**“ which will fetch references from artifact(references basically contains messageids of the mail previous to the current mail, basically referring this mail as a reply in the mail chain). These references will be made into a list and will be used to suppress duplicate notable further down the playbook.
- Once references are finalised, then playbook moves to “**Format for notable creation**“ block , where the query to create a notable in splunk is created. It will contain rule_name, description, Alert source link etc and all this will be piped to “| **collect index=notable**”, but at this point the notable is not created.
- Once the format is ready, the playbook moves to “**Check for existing tickets**“ block, in this block using the **Referencestolist** output, SOAR will check for duplicate notables for last 30 days. This will fetch the count of events.

- After this block, playbook moves to “**Logging**”, this block is only for troubleshooting which will output several details to make troubleshooting easy.
- The Playbook then moves to a decision block, which will decide whether to create a fresh notable or add a comment to notable or reopen a notable further down the lane based on the no of the events fetched from “**Check for existing tickets**”, if there are no notables then a fresh notable will be created else moves to further checks.

The Image on the right basically decides the following things in order:

- If there are **no notables**(based on the output from **Check for existing tickets** block), then the playbook using the output from “**Format for notable creation**“ block, will create a new notable in the **first** action block on the left.
- Then it proceeds to the fetch the event ids of the created notable in the **second** action block.
- Once eventid is fetched then, the playbook proceeds to create a notable link using the eventid fetched from the **second** block.This will be sent as part of the slack message to kmanju@godaddy.com for reference.
- After this the playbook decides whether the notable creation block, i:e **first** action block is success or failed. If its success, then the playbook will resolve the container, change few container parameter and will send a slack message along with the notable link.If failed, the playbook will send the container to pending state and assign it to kmanju@godaddy.com for troubleshooting.
- If there are Notables then,
 - The playbook will fetch the users from gcco@godaddy.com and ir@godaddy.com and will check whether the mails is from someone who is part of either of these groups.
 - If the mail(reply) is from the group members, then the playbook will close the container and no action is performed.
 - If the mail(reply) is not from the group members then the playbook will check whether the notable is Open or closed
 - If Open, then the playbook will add a comment to the Notable and will send a slack message to #security-analyst-collab channel saying a new reply has been added to the mail chain.
 - If Closed, then playbook will reopen the Notable and will send a slack message to #security-analyst-collab channel saying a notable has been reopened.
 - In either of the above case, the playbook will modify the container to resolved state and modify the sensitivity to Low.

This marks the end of the playbook.

Security@ - kmanju@godaddy.com - FW: [Confluence] Marshall Cahill created 'Untitled whiteboard (257)' Closed kmanju@godaddy.com -- Notable Fri, Dec 13, 2024 3:45 PM Undetermined Threat | Medium

Description
Kindly check the security@godaddy.com mailbox for more info on the notable. NOTE: Check the email link url to access the mail chain.--Check this link for a playbook on steps for triaging this notable: <https://godaddy-corp.atlassian.net/wiki/x/A55y2w>

Additional Fields

| Additional Fields | Value | Action |
|-------------------|--|--------|
| Alert Source Link | https://outlook.office365.com/owa/ | ▼ |
| | ItemID=AAMkADQ0ZjzNTIiWFIMjYtNDdmMS1iY2QxLTFkNmlwMzQ1NWJmMgBGAAAAAAABYptovqV6IS5QnxBy%2BiypBwDcSrPHMcwvSLZtCkT9J93IAArc2kVWA A%3D&exvsurl=1&viewmodel=ReadMessageItem | |
| Rule Description | Kindly check the security@godaddy.com mailbox for more info on the notable. NOTE: Check the email link url to access the mail chain.--Check this link for a playbook on steps for triaging this notable: https://godaddy-corp.atlassian.net/wiki/x/A55y2w | ▼ |
| Rule Name | Security Mailbox Automated Notable Creator | ▼ |
| Sender | kmanju@godaddy.com | ▼ |
| Severity | high | ▼ |
| Subject | FW: [Confluence] Marshall Cahill created 'Untitled whiteboard (257)' | ▼ |

Related Investigations
Currently not investigated.

History

| Date | User |
|----------------------|--------------------|
| Dec 13, 2024 3:49 PM | kmanju@godaddy.com |
| | dcadcaaffadfdaf |

[View all review activity for this Notable Event](#)

Adaptive Responses

| Response | Mode | Time | User | Status |
|-----------------------------|------|------|------|--------|
| No adaptive responses found | | | | |

[View Adaptive Response Invocations](#)

Next Steps

| Step | Description |
|------|-----------------------|
| 1 | No next steps defined |

Sample Notable

27 Jan 2025 07:59
A New reply has been added to the mail below:

Original Mail Subject: SecurityBreach@ - kmanju@godaddy.com - Duplicate artifact trb. Close as BP

Reply Added By: security@godaddy.com

Alert Source Link: <https://outlook.office365.com/owa/?ItemID=AAMkAGMyNDEwNDE4LWMxZGutNGY0OS05YTBlLWExYzk2YzM3MDYwZABGAAAAAA7bSyhsAH%2FSJ8%2FpxbEmdf%2BBwBHSDQPTlwSoQnYMZMT2ynAAAEEAABHSDQPTlwSoQnYMZMT2ynAAKuaIWAAA%3D&exvsurl=1&viewmodel=ReadMessageItem>

Sample for adding a comment to the notable

22 Jan 2025 13:21
A New reply has been added to the mail below,Hence Reopening the notable:

Original Mail Subject: SecurityBreach@ - skarra@godaddy.com - Test Mail- kiran sameer

Reply Added By: skarra@godaddy.com

Alert Source Link: <https://outlook.office365.com/owa/?ItemID=AAMkAGMyNDEwNDE4LWMxZGutNGY0OS05YTBlLWExYzk2YzM3MDYwZABGAAAAAA7bSyhsAH%2FSJ8%2FpxbEmdf%2BBwBHSDQPTlwSoQnYMZMT2ynAAAEEAABHSDQPTlwSoQnYMZMT2ynAAAHjnYoAAA%3D&exvsurl=1&viewmodel=ReadMessageItem>

Sample for reopening a notable

Improvements/Suggestions

For Playbook improvements - detections@godaddy.com or kmanju@godaddy.com

For Troubleshooting Process: ir@godaddy.com

Implemented Improvements

The section will contain any improvements implemented in the Splunk Playbook or in Notable Triaging Process.

1. Dec 12 2024: Updated code to stop duplicate notable being created when a new mail reply was added to the mail chain.
2. Dec 13 2024: Updated code to replace double quotes to single quote in subject, if not updated the notable for such subject with double quotes wasn't creating notables.
3. Jan 11 2024: Added checks for new reply and based on whether the reply is from GCSO or IR member, the containers will be closed, if Non GCSO/IR member replies then reopen notable if closed and add a comment if open.
4. Jan 12 2024: Send slack message to gcs0 if a comment added to notable or a notable is reopened.

Investigation and Response Workflow in ES8 v1

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Introduction](#)
- [Investigation Diagram](#)
- [Investigation workflow](#)
 - [Investigation starts in the Overview tab](#)
 - [Start the Investigation](#)
 - [Notes and Files](#)
 - [Check for Related Incidents](#)
 - [Response Tab](#)
 - [Response Steps](#)
 - [Events](#)
 - [Search](#)
 - [Automation](#)

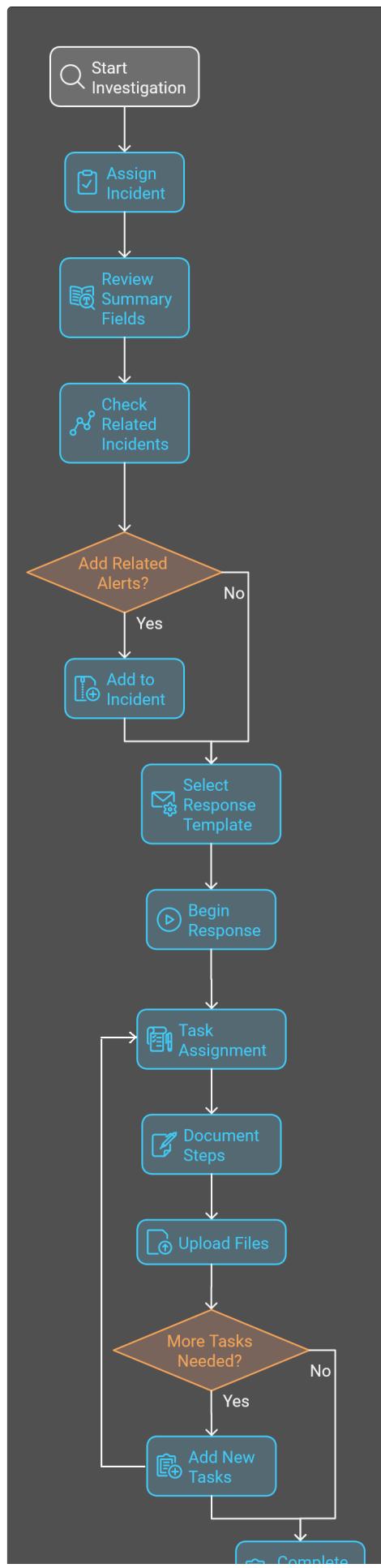
Purpose

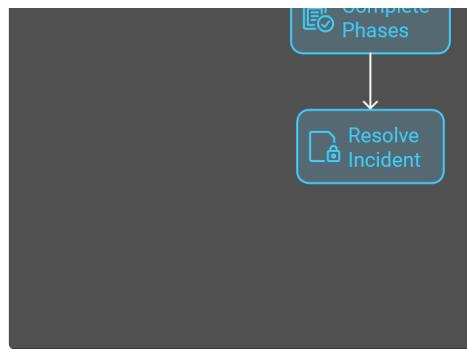
| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: GCSO@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | 12/30/2024 |
| Escalation Contact(s) | |
| Requests for Updates | By Email - GCSO@godaddy.com |
| Training Log | By: @Darko Zecic 12/14/2024 |

Introduction

The purpose of this playbook is to provide a comprehensive guide for security analysts on how to effectively use Splunk Enterprise Security 8.0 for investigating and responding to security incidents.

Investigation Diagram





Investigation workflow

Investigation starts in the Overview tab

Incident review **Search** **Content** **Settings** **SOAR Redirect** **Dashboards** **Mission Control**

← Incidents **MC-872007** **Windows Event Log Cleared**

Overview **Response** **Events** **Search** **Automation**

Summary

| | | | |
|-----------------------|---|--------------------|---|
| Resolution Action | Select... | MITRE Technique | Clear Windows Event Logs |
| Intrusion Type | Select... | Indicator Removal | Indicator Removal |
| Annotation Framework | analytic_story | MITRE Technique ID | T1070 |
| | cis20 | Number of Events | 3 |
| | kill_chain_phases | Result | log file was cleared |
| | mitre_attack_nist | Risk Score | 7624.0 |
| Annotations | CIS 10 | Rule Name | ESCU - Windows Event Log Cleared - Rule |
| | CISA AA22-264A | Security Domain | endpoint |
| | Clop Ransomware | Severity | high |
| | DE.CM | Time | Dec 13th, 2024 2:55 PM |
| | Exploitation | Title | Windows Event Log Cleared |
| | Ransomware | Type | notable |
| | T1070 | User | SYSTEM |
| | T1070.001 | tag | modaction_result |
| Correlation Rule Name | ESCU - Windows Event Log Cleared - Rule | | |
| Destination | jumpjumpdc1.corp.gd | | |
| EPOCH firstTime | 2024-12-13T14:25:22 | | |
| EPOCH lastTime | 2024-12-13T14:33:27 | | |
| Event Code | 104 | | |
| Info search time | 1734101690.548304000 | | |
| MITRE | T1070 | | |
| | T1070.001 | | |
| MITRE Tactic | defense-evasion | | |

INFO

| | | | |
|---------------|--------------------|--|--------------|
| Owner | rbarki@godaddy.com | Status | In Progress |
| Urgency | Medium | Sensitivity | Unassigned |
| Incident Type | default | Disposition | Undetermined |
| Incident ID | MC-872007 | Description | |
| | | The following analytic detects the clearing of Windows event logs by identifying Windows Security Event ID 1102 or System log event 104. This detection leverages Windows event logs to monitor for log clearing activities. Such behav... | |
| | | Created | |
| | | Dec 13th, 2024 2:55 PM | |
| | | Last updated | |
| | | Dec 13th, 2024 3:09 PM | |
| | | Incident origin | |
| | | ES Notable Event | |
| | | Reference ID | |
| | | c60d5751-c8a8-4fc8-a0d3-5595c0a80618 | |
| | | SLA | |
| | | 23 hrs 29 mins | |
| | | History | |
| | | View all review activity for this Notable Event | |
| | | Splunk Enterprise | |
| | | View notable event | |
| | | Security | |
| | | Splunk SOAR | |
| | | View container | |

NOTES

Enter title

Enter note

Save

FILES

Drop your file here or upload file...

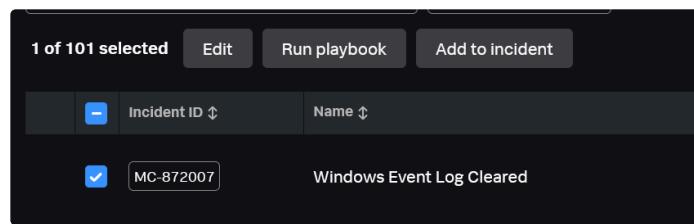
1. **Assign the Incident:** Begin by assigning the incident to yourself so your teammates know you are handling it.
2. **Review Existing Fields in Summary:** Check the existing fields for information about the incident.
3. **Right Side Tab:** This section contains more details about the alert, as well as notes and files related to the investigation.

Notes and Files

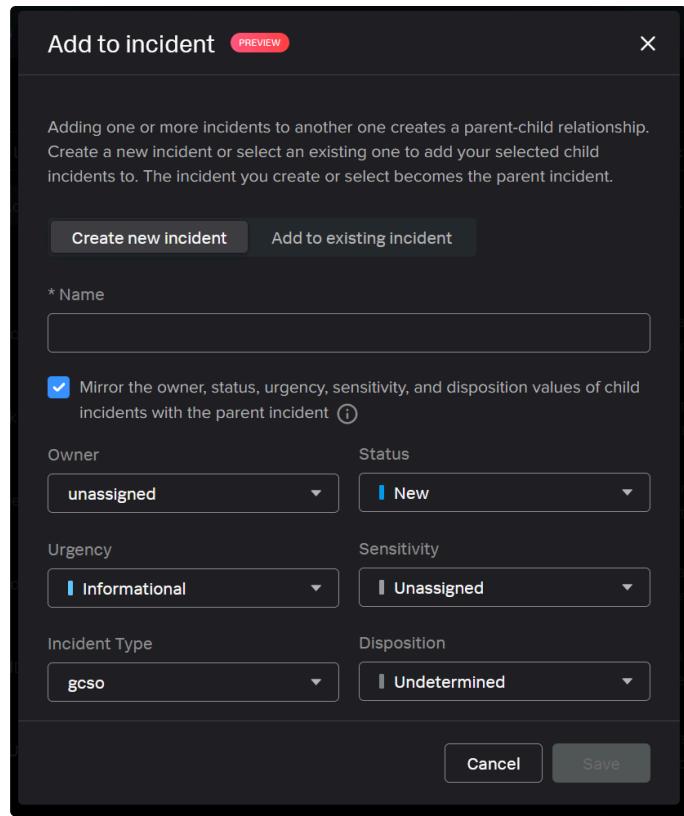
- **Notes:** This field will display every step taken during the investigation.
- **Files:** Here you can find uploaded files such as IoCs, Excel sheets, or pictures.

Check for Related Incidents

1. **Review Existing Fields:** Understanding the incident involves reviewing the populated fields. Go back to the Incident Review tab to check for other alerts that might be part of the same incident.
2. **Add Related Alerts:** If there are related alerts, add them by marking them and clicking on the "Add to Incident" tab. You can add them to a new or existing incident.



From here you can add to a new incident or Add to existing one



Response Tab

1. **Blank Response Tab:** For new incidents, the response tab will be blank.
2. **Select a Response Template:** Click on "+ Response" and choose an appropriate response template. For this playbook, we'll use GoDaddy Incident Life Cycle Template.
3. **Begin Response:** Once a template is selected, you can start the response process.

Windows Event Log Cleared

Overview Response Events Search Automation

Response

No response plan

Add a response plan to this incident to start working through predefined phases and tasks.

+ Response

TIP You can also assign default response templates per incident type. [Assign them here](#)

Add response template

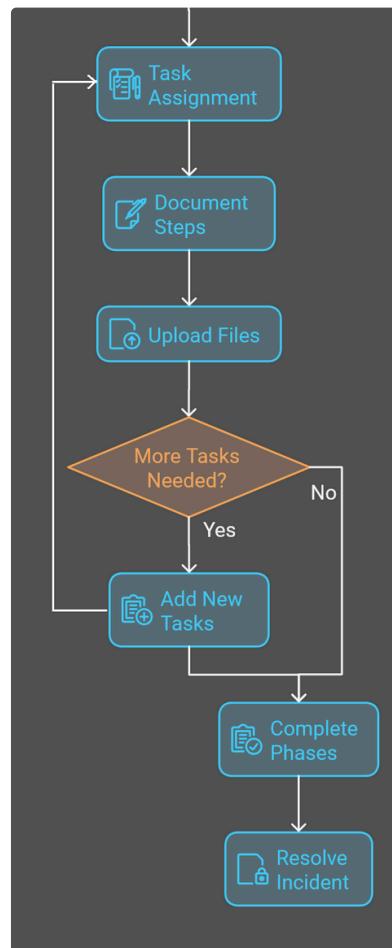
Add response template

Search response templates

| Reference ID | Name | Created by | Created | Last updated | Updated by | Status |
|--------------|--|-------------------|--------------------|--------------------|---------------|-----------|
| ...9835 | GoDaddy Incident Life Cycle Template | David Hernandez | Oct 30th, 05:19 PM | Nov 6th, 03:20 PM | dzeoic@god... | published |
| ...4866 | Notes Only | ddubois@godadd... | Apr 25th, 10:48 PM | Oct 30th, 05:47 PM | David Hern... | published |
| ...6810f | test_basic_info | egranda1@godad... | Sep 11th, 06:27 PM | Sep 11th, 06:29 PM | egranda1@... | published |
| ...c4ef5 | Suspicious Email | Splunk | Apr 5th, 11:50 PM | Apr 5th, 11:50 PM | Splunk | published |
| ...e39fe | NIST 800-61 | Splunk | Apr 5th, 11:50 PM | Apr 5th, 11:50 PM | Splunk | published |
| ...8c1fc | Data Breach | Splunk | Apr 5th, 11:50 PM | Apr 5th, 11:50 PM | Splunk | published |
| ...f184 | Account Compromise | Splunk | Apr 5th, 11:50 PM | Apr 5th, 11:50 PM | Splunk | published |
| ...beeca | This response template defines a response to the potential compromise of one or more system or application accounts. Across the enterprise, user and service accounts are high-value target... | Splunk | Apr 5th, 11:50 PM | Apr 5th, 11:50 PM | Splunk | published |
| ...04fd4 | Generic Incident Response | Splunk | Apr 5th, 11:50 PM | Apr 5th, 11:50 PM | Splunk | published |
| ...50ed | Vulnerability Disclosure | Splunk | Apr 5th, 11:50 PM | Apr 5th, 11:50 PM | Splunk | published |
| ...50ed | Network Indicator Enrichment | Splunk | Apr 5th, 11:50 PM | Apr 5th, 11:50 PM | Splunk | published |
| ...ef5cb | Self-Replicating Malware | Splunk | Apr 5th, 11:50 PM | Apr 5th, 11:50 PM | Splunk | published |

Cancel Submit

Response Steps



1. **Task Assignment:** On the left side, you'll see all the steps needed to resolve the investigation. Each Task in a phase can be assigned to one analyst, but multiple analysts can assign different tasks in a single phase.
2. **Incident Phases:** Incidents have several phases, each requiring specific tasks to be completed.
3. **Start Tasks:** Click "Start" to assign a task to yourself.
4. **Enter Notes:** Document every step taken to resolve each task and phase. You can leave as many notes as needed.
5. **Upload Files:** If you have acquired files from other sources, upload them in the Files field. This way everyone involved in this incident will have access to it.
6. **Add New Tasks:** Some incidents will require more tasks to be done than provided in response template. If more tasks are required, click "+ Task" at the bottom of each phase.
7. **Complete Phases:** A phase is considered finished when all tasks are completed.
8. **Resolve Incident:** The incident is resolved when all phases are completed.

Events

- **Events tab** is a place where logs of all Automation and Search actions ,of the related incident, are stored. It is used to check which search and automation has already been done.

Search

- **Search Bar:** Similar to the Splunk Search, but with added functionality. All searches related to the incident are saved and can be reviewed in Search History.

- **Search History:** Provides insight into what other team members have searched during the investigation.
- **Events Tab:** Search queries will appear here for others to rerun or review.

Automation

- **Current State:** Automation is in its early stages but will grow over time.
- **Available Automation:** Includes tasks like isolation, information enrichment, and file deletion.

Communication templates

Table of contents

Table of contents

Purpose

Description

VIP Communication

Compromised Workstation Playbook

 Inform #get-itsec

Credential Mitigation

 Inform #get-itsec

Employee Compromise Containment

 Account Locked (Credentials Only)

 Account Locked + Workstation Re-Image

Employee Phishing Incidents

 Response to Reporter - IsItBad Report - Classification: Smishing

 Response to Reporter - IsItBad Report - Classification: Not Malicious

 Response to Reporter - IsItBad Report - Classification: SPAM

 Response to Reporter - IsItBad Report - Classification: Phish

 Response to Reporter - IsItBad Report - Classification: Legit Communications

 Response to Reporter - IsItBad Report - Classification: Malware

OnCall Escalation Procedure

 GCSO identifies a confirmed threat

 Escalation format:Please follow the follow Post format.

 If No Response within 5m - Escalate using one of the following:

VDI Login via User Impersonation

 Message template

Note

General Documentation

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic @Luis Fernando Garcia Yepes |
| Last Review Date | |
| Escalation Contact(s) | |

| | |
|----------------------|--|
| Requests for Updates | |
| Training Log | |

Description

This is a guide on how to communicate according to every playbook

⚠ VIP Communication

Whenever communication with VIP users (two levels below the CEO) is required, it should be handled by L2 analyst.

Compromised Workstation Playbook

Inform #get-itsec

Workstation isolation message template :

Hello Team,

We have isolated the machine <machineName> which belongs to <userName>, based on a Security Incident.

The machine will be in isolation till further notice.

Credential Mitigation

Inform #get-itsec

Using one of the two message templates, please inform #get-itsec of the remediation performed.

Hello Team,

Below users have been remediated. Please assist them in resetting the password as they may call GetHelp for assistance.

<Insert AD Names>

If the account needs to remain disabled or contained please use the following template

Hello Team,

Below users have been remediated. Please DO NOT assist them in resetting the password as they may call GetHelp for assistance.

<Insert AD Names>

<Insert alert-red emoji>

Employee Compromise Containment

Account Locked (Credentials Only)

To: Affected User

CC: Supervisor (**Do NOT CC Director level or above**); Workforce (**Care Agents ONLY**); GCSO;
ssit@godaddy.com; engwin@godaddy.com

Subject: Your User Account Has Been Locked : Action Required

The Security team was recently made aware of a <Incident_Type> in which we believe your account credentials may have been compromised. Because you were unavailable at the time of this discovery, we have taken action as a precaution to protect your account from misuse.

You will need to reset your password in order to regain access to your account.

This will require you to contact GetHelp (480-624-2580) for assistance.

Please ensure that the following best-practices are also observed for your account:

Reset any credentials not synchronized to your GoDaddy login - example include SaaS applications, local accounts, etc.

Ensure that passwords are not reused across any services, accounts, etc.

Passwords on all company-controlled platforms must conform to

GoDaddy password standards.

We will also be ensuring you are enrolled into Okta Multi-Factor Authentication (MFA) as an added layer of protection. If you were not already enrolled in MFA you will be prompted to complete setup when you next sign-on to Okta.

NOTE: Please make necessary change while sending the above communication as per the scenario.

Account Locked + Workstation Re-Image

To: Affected User

CC: Supervisor (Do NOT CC Director level or above); Workforce (Care Agents ONLY); GCSO; Ryan Seaman; ssit@godaddy.com; engwin@godaddy.com

Subject: Your User Account Has Been Locked : Action Required

The Security team was recently alerted to potentially malicious activity on <><MachineName>>. During our review we found that a malicious file identified as <><FileName>> (<><MalwareType>>) was downloaded and executed on the machine. This execution may have allowed the malicious software to gain persistence on or gain information from your system.

Due to the risk this poses we must take action to secure the machine and your account. Because you were unavailable at the time of this discovery, we have locked your account as a precaution to prevent any misuse and have requested a re-image for your machine (<><REQ#>>) to ensure that the malicious software is removed.

You will need to reset your password in order to regain access to your account. This will require you to contact GetHelp (480-624-2580) for assistance and to coordinate the re-image of your workstation.

Please ensure that the following best-practices are also observed for your account:

Reset any credentials not synchronized to your GoDaddy login - example include SaaS applications, local accounts, etc.

Ensure that passwords are not reused across any services, accounts, etc. Passwords on all company-controlled platforms must conform to GoDaddy password standards.

We will also be ensuring you are enrolled into Okta Multi-Factor Authentication (MFA) as an added layer of protection. If you were not already enrolled in MFA you will be prompted to complete setup when you next sign-on to Okta.

NOTE: Please make necessary change while sending the above communication as per the scenario.

Employee Phishing Incidents

Response to Reporter - IsItBad Report - Classification: Smishing

Hello \${MESSAGE_REPORTER}

Thank you for reporting this to us.

Subject: \${MESSAGE SUBJECT}

We have reviewed the message and determined it is malicious. Please block the sender and delete the message.

Thanks again for being vigilant in reporting suspicious SMS.

- Global Cyber Security Operations

Response to Reporter - IsItBad Report - Classification: Not Malicious

Hello \${MESSAGE_REPORTER}

Thank you for reporting this to us.

Subject: \${MESSAGE SUBJECT}

We have investigated the email and determined that it is not malicious as it does not contain any malicious content. If you were not expecting this email, please delete it from your inbox. No further actions are required from you at this time.

Thanks again for being vigilant in reporting suspicious emails.

- Global Cyber Security Operations

Response to Reporter - IsItBad Report - Classification: SPAM

Hello \${MESSAGE_REPORTER},

Thank you for reporting this to us.

Subject: \${MESSAGE SUBJECT}

We have reviewed the message and have determined the message to be spam and non-malicious. No further actions are required from you at this time.

Thanks again for being vigilant in reporting suspicious emails.

- Global Cyber Security Operations

Response to Reporter - IsItBad Report - Classification: Phish

Hello \${MESSAGE_REPORTER}

Thank you for reporting this to us.

Subject: \${MESSAGE SUBJECT}

We have reviewed the message and determined it is malicious. The message will now be deleted from your mailbox. No further actions are needed from you at this point in time.

Thanks again for being vigilant in reporting suspicious emails.

- Global Cyber Security Operations

Response to Reporter - IsItBad Report - Classification: Legit Communications

Hello \${MESSAGE_REPORTER}

Thank you for reporting this to us.

Subject: \${MESSAGE SUBJECT}

We have reviewed the email and determined it to be a legitimate communication. Please disregard the email if you are not an intended recipient. No further actions needed from you at this point of time.

- Global Cyber Security Operations

Response to Reporter - IsItBad Report - Classification: Malware

Hello \${MESSAGE_REPORTER}

Thank you for reporting this to us.

Subject: \${MESSAGE SUBJECT}

We have reviewed the message and determined it is malicious. The message will now be deleted from your mailbox. No further actions are needed from you at this point in time.

Thanks again for being vigilant in reporting suspicious emails.

- Global Cyber Security Operations

OnCall Escalation Procedure

GCSO identifies a confirmed threat

Notify @ir-team in the #internal-gcso slack channel.

Escalation format:
Please follow the follow Post format.

Primary Post:

Title:
Request:
Link:

If No Response within 5m - Escalate using one of the following:

The On-Call Email template below. You will receive a slack notification if correctly executed. It is important to note that the

To: oncallemail.b7gfj05x@gd-response.pagerduty.com

Subject: Security Incident Escalation: <ES Alert ID> Your User Account Has Been Locked : Action Required

Please review the following Alert escalation: <Insert Slack Reference Link>
Threat Status : <Insert Status: Contained|Active>
Hosts/Users Impacted: <1-10+>
--GCSO

VDI Login via User Impersonation

Message template

User details are found in Workday.

To: mailto: BPO_Management_Office_XLT@godaddy.com

CC: <mailto:gcsco@godaddy.com>

Subject: Accounts Locked for VDI Policy Violation (Action Required)

Hi Team,

We have disabled the accounts for the users <Source User> and <Target User>.

This was a result of <Source User> authenticating to the VDI environment and signing into the VDI box as <Target User>. Can you please assist us in our investigation and collect a justification from the users in question. Once a justification is provided, get-help will enable the accounts. If the users are unaware of this activity, please inform us as soon as possible.

Source User Details:

<Source User Email>

<Source User Title>

<Source User Department>

<Source User Location>

Target User Details:

<Target User Email>

<Target User Title>

<Target User Department>

<Target User Location>

For more details on our Acceptable Use Policy, please view the policy

[here](#).

-GCSO

Note

These processes might disrupt users' ability to perform business, so always check the user's position in the company before proceeding.

General Documentation

Coming Soon

File collection from OneDrive using S1

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description:](#)
- [File collection](#)
- [Investigation Process](#)
- [Improvements](#)
- [Common False Positives](#)
- [General Documentation](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic |

Description:

There are situations where we need to collect files from users' OneDrive. Outlook Defender often cannot collect the files for us, causing the file collection process to fail. This playbook will guide you through the steps to successfully collect those files

File collection

Standard process for file collection from OneDrive takes a long time. It requires you to contact 0365 team and ask them to collect that file for you. This can take a long time to perform and time is crucial in Incident Response.

Fortunately there is a workaround. You can remotely connect to user machine and access his OneDrive from there. This way you can much faster get to the file.

For this workaround to work User needs to be online and connected to the internet and has connected his shared folder with Windows. This process won't work if user is offline.

This can not be done if the User is using Mac, as user privileges are more secure!!!

Investigation Process

- Navigate to Sentinels
- Enter hostname

The screenshot shows the Sentinel interface with the 'ENDPOINTS' tab selected. A search bar at the top displays 'Endpoint name LTTC-DZ0X2T3'. The main area contains a table of endpoint details and a list of selected endpoints.

Endpoint Details Table:

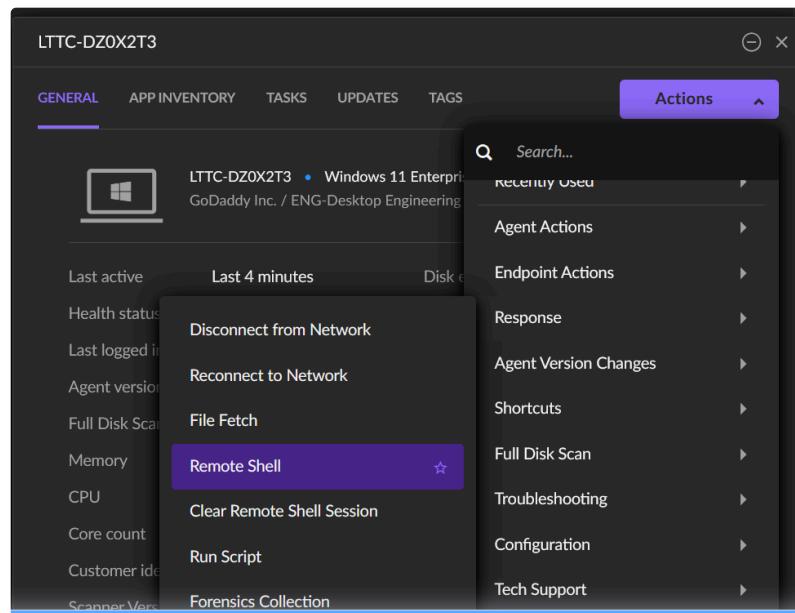
| OS | Version | Type | Domain |
|----------------|------------|-----------------|---------------|
| Windows | 23.4.4.223 | Laptop | WORKGROUP |
| macOS | 22.2.2.394 | Other | N/A |
| Linux | 22.2.4.558 | Desktop | 123.local |
| Windows Legacy | 22.3.3.11 | Server | 123-regional |
| | 22.3.4.612 | Kubernetes Node | 1brands.com |
| | 224.2.4 | Storage | 4-227.private |

Selected Endpoints List:

| Actions | Group | No Items Selected | | | |
|--------------------------|---------------|-------------------|--------------------|-----------------------|----|
| <input type="checkbox"/> | Endpoint Name | LTTC-DZ0X2T3 | Endpoint Tags | Network-Security-Z... | +2 |
| <input type="checkbox"/> | | GoDaddy Inc. | ENG-Desktop Engine | | |

- Actions > Response > Remote Shell

- Click Connect and enter MFA number



- Navigate to sharepoint folder by entering this command: `cd`

```
"C:\Users\username\Go Daddy.com, LLC, A Delaware Company"
```

(replace username with employee account name)

The screenshot shows a terminal window titled 'Remote Shell'. On the left, there is a file listing of a directory. On the right, there is a status bar for the device 'LTTC-DZ0X2T3' showing it is connected. Below the status bar, there is a 'Terminate' button. At the bottom of the terminal window, there is a PowerShell session window showing commands being entered and their results.

```
PS C:\users\dzecic> cd "Go Daddy.com, LLC, A Delaware Company"
PS C:\users\dzecic\Go Daddy.com, LLC, A Delaware Company> dir

Directory: C:\users\dzecic\Go Daddy.com, LLC, A Delaware Company

Mode                LastWriteTime         Length Name
----                -----        ----
da---l      2/27/2025  10:18 AM            2837 Security DEMO - Documents

PS C:\users\dzecic\Go Daddy.com, LLC, A Delaware Company> [ ]
```

You are now accessing files from their Onedrive.

To do a file collection, you can use S1 file collection tool and use the file path that you found using remote shell.

Good luck!

Improvements

Add all possible improvements here:

Common False Positives

General Documentation

Coming Soon

Incident Response mindset and OODA loop

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[OODA loop in IR](#)

Observe

Orient

Decide

Act

Repeat

[Example](#)

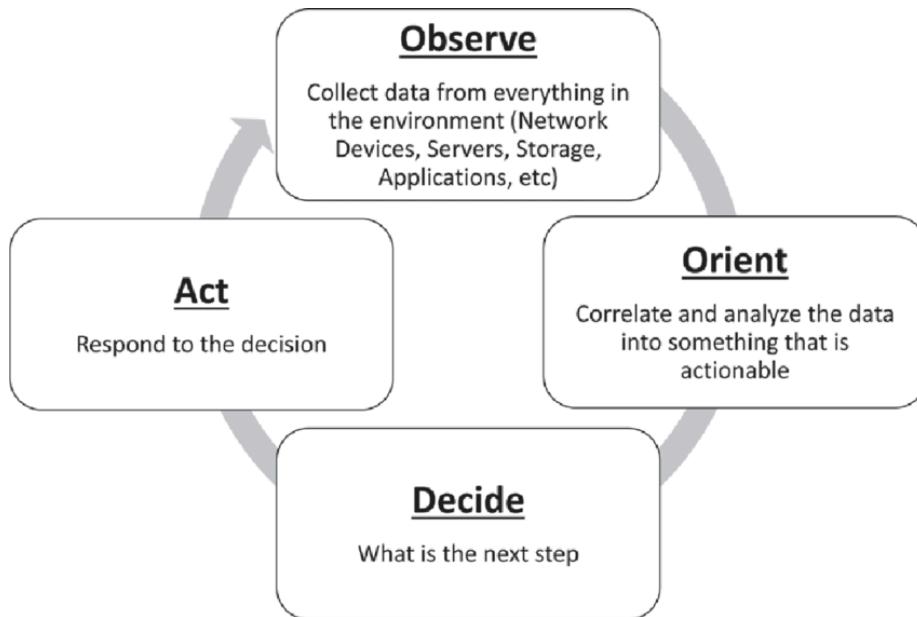
[Requesting additional information](#)

Purpose

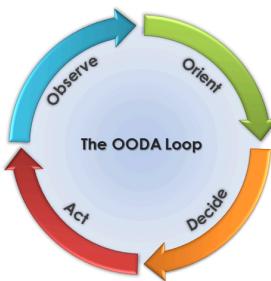
| | |
|------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | David Hernandez |
| Last Review Date | 2/28/25 Darko |
| Training Log | |

Description

The OODA Loop provides a structured approach to incident response, enabling security teams to effectively handle security breaches. By following the Observe, Orient, Decide, and Act phases, analysts can minimize damage and accelerate recovery. It's a decision-making framework that is valuable in incident response.



OODA loop in IR



Observe

This phase begins when you assign an alert to yourself. Start by collecting all the evidence using open-source intelligence platforms and other tools like Splunk search or SentinelOne (S1) to get the best picture of what triggered the alert.

Orient

Now that you have collected all the available data, think through all the possible options to respond to the incident as efficiently as possible. Consider the following questions:

- Can you hypothesize what happened?
- What data is missing?
- Is this data enough to make a decision for your next steps?
- How do you collect the missing data?
- What is the first thing that needs to be done to minimize the impact of this incident?
- What is the scope of the impact?

- What are the priorities?
- What are the possible actions?

Decide

Based on all the data provided and your analysis, make a decision on the next steps to minimize the impact of the incident. Find a balance between urgency of action and lack of information.

Act

Perform the action and execute based on your decision.

Repeat

You may need to repeat these steps multiple times to resolve the incident fully.

Example

Research in progress

Requesting additional information

Blocking Domains using Splunk Playbook

Table of contents

[Table of contents](#)

Purpose

Description

Scope of Affected Clients

Example

WARNINGS

General Documentation

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: @godaddy.com |
| Process Owner | @Kedwin Chen |
| Last Review Date | 2025 May 14 |
| Escalation Contact(s) | @David Hernandez @Kedwin Chen @Kiran Manju |
| Requests for Updates | @Kedwin Chen |
| Training Log | |

Description

This playbook is a guide on how to block a domain using the Splunk Playbook (using Mission Control)

Scope of Affected Clients

⚠ This playbook blocks both URLs and domains. When run against a URL, the domain is also blocked!!

Domains are blocked across ALL on-prem DNS clients using the **Corporate DNS API** AND ALSO **Palo Alto Prisma**. THIS INCLUDES CARE, VDI, AND HOSTING SERVERS.

⚠ URLs blocks are effective against Palo Alto Prisma clients (excludes servers). At the time of writing (2025 May 13), this affects ALL WORKFORCE USERS - BUT ONLY CARE WILL SEE A BLOCK PAGE.

⚠ WARNING: for blocking URLs in Prisma, the Playbook currently (2025 May 14) will strip off ALL URL path elements (e.g., `https://example.com/path/to/resource` will result in all of `example.com` being blocked)

Example

Suppose you deem the URL `https://example.com/url/ex1` to be malicious, and you run the playbook to block the same. After the playbook executes, the following will occur:

- On-Prem Corporate DNS Server clients will no longer be able to resolve `example.com` or `*.example.com`
- Palo Alto Prisma users will no longer be able to access any part of `example.com`

WARNINGS

✖ THE AUTOMATION PLAYBOOK DOES NOT CHECK IF A DOMAIN IS REGISTERED OR HOSTED WITH GODADDY OR A GODADDY-OWNED BRAND. PLEASE CHECK IN CRM FIRST.

⚠ Only L2 or higher should run this playbook after validating domains are:

- actually malicious
- external to GoDaddy, and
- not GoDaddy-registered or hosted domains.

General Documentation

1. Check if the domain is hosted with GoDaddy (or GoDaddy-owned brands) by using CRM. **DO NOT PROCEED IF AN ACCOUNT SHOWS UP WITH dbs:active**

The screenshot shows the 'Customer Search' interface. On the left, there's a sidebar with filters for 'Customer Number', 'Customer name or Shopper ID', 'PHONE NUMBER' (with value '+91 9895058877'), 'EMAIL ADDRESS', 'LOGIN NAME', and 'ORDER NUMBER'. The main area has a search bar with 'SEARCH' and 'RESET' buttons. The results table has columns for 'TYPE', 'DOMAIN STATUS', 'NAME', 'EMAIL', and 'BUSINESS CHANNEL'. A red circle highlights the 'DomainSSL' column. Below the table, a note says '2 - Check "Domain Status" column for any "dbs:active"'. The bottom right shows pagination: 'PAGE 1 OF 1 200 ROWS'.

Example of domain registered with GoDaddy

2. Open the case in Mission Control

3. Open the Automation tab, and select Run Playbook

The screenshot shows the Splunk SOAR Mission Control interface. The top navigation bar includes 'splunk-cloud', 'Apps', 'Messages', 'Settings', 'Activity', 'Find', and 'Mission Control'. The 'Automation' tab is highlighted with a red circle. The main panel shows an incident titled 'TTX01-kchen (2024-10-30T10:11:31-0500)'. The 'Automation' history table lists a single entry: 'New Event Tagger Playbook' by automation on Oct 30, 3:13 PM. To the right, the 'INFO' section displays details like Owner (Kedwin Chen), Status (In Progress), Urgency (Informational), and Incident type (monitoring). The 'Run action' button is circled in red. The 'NOTES' section contains two entries from Kedwin Chen, with the second one being a task note about log search results.

4. Enter **GD-Block-Domain-Manual** into the Search Bar, then select the playbook and click Run playbook

The screenshot shows the 'Run playbook' dialog box. At the top is a search bar with 'GD-Block-Domain-Manual'. Below it is a table with columns: Name, Source, Category, Version, Last Run, and Run Count. A row for 'GD-Block-Domain-Manual' is selected, with a red arrow pointing to its name. At the bottom are 'Scope' dropdowns ('All events') and 'Run playbook' buttons. A red arrow points to the 'Run playbook' button.

5. Open the Prompts tab and select View for prompt_action_and_domain

The screenshot shows the Splunk Cloud interface. At the top, there's a navigation bar with 'splunk>cloud' and various menu items like 'Incident review', 'Search', 'Content', 'Settings', 'Activity', 'Find', and a search bar. Below the navigation is a breadcrumb trail: '← Incidents' and 'TTX01-kchen (2024-10-30T10:11:31-0500)'. The main content area has tabs for 'Overview', 'Response', 'Events', 'Search', 'Automation' (which is selected), and 'Intelligence'. A red arrow points to the 'Automation' tab. In the 'Automation' section, there's a 'Automation history' table with one entry: 'GD-Block-Domain-Manual' by 'kchen@godaddy.com' on Mar 06, 12:43 AM, with 1 action ran. Another entry, 'prompt_action_and_domain', is listed with a status of 'Pending'. Below this is a table for 'Run ID', 'Configuration', 'Name', 'Connector', and 'Status'. A message 'No data found' is displayed. To the right of the history table is a 'Prompts' button, which is circled in red. Below the history table is a 'Prompts' modal window. It has a search bar and a table for 'Unanswered prompts'. One row in the table is highlighted: 'prompt_action_and_domain' by 'Kedwin Chen' with a due date of 'In 29 minutes' and a status of 'Pending'. A 'View' button is also circled in red. At the bottom of the modal are 'Cancel' and 'View' buttons.

6. Complete the Prompts

- Enter the domain to take action on. Only enter one (1) domain.
 - This will also take action on the wildcard subdomains (i.e., if `example.com` is selected, `*.example.com` will also be blocked)
 - URLs are also supported, but please use domains where able
 - There are some restrictions on which domains can be blocked, which are checked automatically. However, **please do your own due diligence to minimize potential business impact**. Currently, the playbook checks the domain is not in one of the following categories of domains:
 - Some GoDaddy corporate domains (such as `godaddy.com`, `gdcorp.tools`, `secureserver.net`)
 - Some non-GoDaddy external resources (such as `godaddy.okta.com`)
 - Top 1 Million domains according to Cisco Umbrella ([Cisco Popularity List](#))
- Select the appropriate action
- Click on **Submit**

d. **prompt_action_and_domain**

MC-862285 TTX01-kchen (2024-10-30T10:11:31-0500) • Playbook: GD-Block-Domain-Manual
Due: In 29 minutes Owner: Kedwin Chen

Message
WARNING This playbook blocks domains across ALL on-prem DNS clients. THIS INCLUDES VDI AND HOSTING SERVERS. THE AUTOMATION PLAYBOOK DOES NOT CHECK IF A DOMAIN IS REGISTERED OR HOSTED WITH GODADDY OR A GODADDY-OWNED BRAND. PLEASE CHECK IN CRM FIRST. Only L2 or higher should run this playbook after validating the domains to be actually malicious, external to GoDaddy, and are not GoDaddy-registered or hosted domains. Check if the domain is hosted with GoDaddy (or GoDaddy-owned brands) by using CRM. DO NOT PROCEED IF AN ACCOUNT SHOWS UP WITH 'dbsactive' # Instructions Please enter the requested parameters

Question
Please enter the domain (or URL) to take action on

Question
Please select the action to take
Select...
 block
 unlock

Cancel Back Submit

7. The playbook will now check if the domain is allowed to be blocked. Open your Prompts view again and look at the Prompt name. If your next prompt is:

- a. **prompt_start_change_settings** - Proceed to Step 8

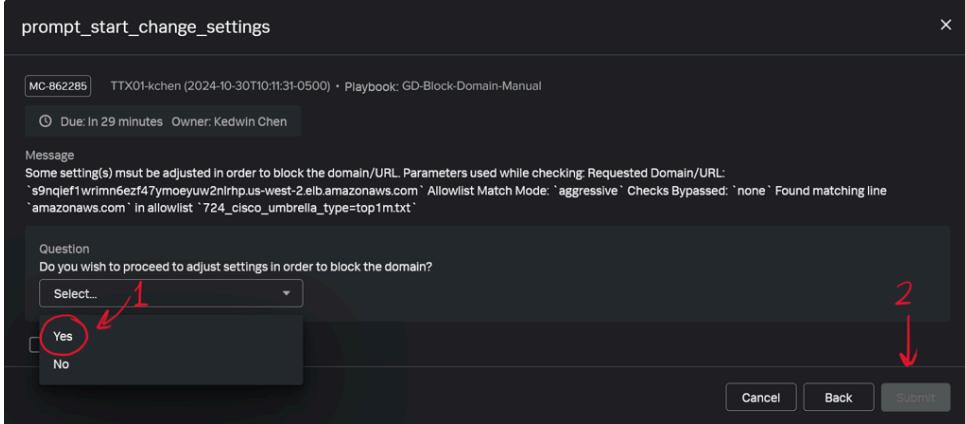
| Prompts | | | | | |
|---|-------------|---------------|---------|----------|-----------------------|
| <input type="text" value="Search prompts"/> Unanswered prompts 1 | | | | | |
| Prompt name | Owner | Due | Status | Response | |
| prompt_start_change_settings | Kedwin Chen | In 29 minutes | Pending | | <button>View</button> |

- b. **prompt_confirm_inputs_for_action_start** - Proceed to Step 9

| Prompts | | | | | |
|---|-------------|---------------|---------|----------|-----------------------|
| <input type="text" value="Search prompts"/> Unanswered prompts 1 | | | | | |
| Prompt name | Owner | Due | Status | Response | |
| prompt_confirm_inputs_for_action_start | Kedwin Chen | In 29 minutes | Pending | | <button>View</button> |

8. **prompt_start_change_settings** - The entered domain was not allowed to be blocked with the default check settings.

- a. You will be prompted if you want to adjust the settings used to run the checks. Often this is the case if the domain is a subdomain of a Top1M domain. Please evaluate again if blocking the domain would have any significant impact to GoDaddy. If little to no impact is expected, select **Yes** to proceed.



b. You should then see a prompt with name `prompt_match_and_bypass_modes`.

If the domain is a subdomain of a Top1M domain, change the **Match Mode** to `strict` and **Bypass Checks** to `none`. You must also enter a **Justification** describing why the check settings needed to be changed.

- i. Note: You should NOT use **Match Mode** of `aggressive` with **Bypass Checks** of `none` - these are the default settings, and doing so will result in a failure message, such as this:

- ii. If using **Match Mode** `strict` still results in a similar message to the above, you may need to select **Bypass Checks** to `top1m` - this will entirely bypass the Top1M domains checks, and **Justification** MUST detail why this check is bypassed.

- iii. Setting of "Bypass Checks" to policy skips ALL checks and should never be used unless directed by L4 or above.

iv.

prompt_match_and_bypass_modes

MC-862285 TTX01-kchen (2024-10-30T10:11:31-0500) • Playbook: GD-Block-Domain-Manual

Due: In 29 minutes Owner: Kedwin Chen

Message
Some setting(s) must be adjusted in order to block the domain/URL. Parameters used while checking: Requested Domain/URL: 's9nqlef1wrimn6ezf47ymoeyuw2nrhp.us-west-2.elb.amazonaws.com' Allowlist Match Mode: 'aggressive' Checks Bypassed: 'none' Found matching line 'amazonaws.com' in allowlist '724_cisco_umbrella_type=top1m.txt'

Question
Match Mode: If you need to block a subdomain of a Top 1M domain, select "strict". Otherwise, select "aggressive"
strict ← 1

Question
Bypass Checks: Select which checks you need to bypass, if any.
none ← 2

Question
Justification required for needing to modify checks.
(Example) Domain hosts credential harvesting page in phishing emails. ← 3

Delegate

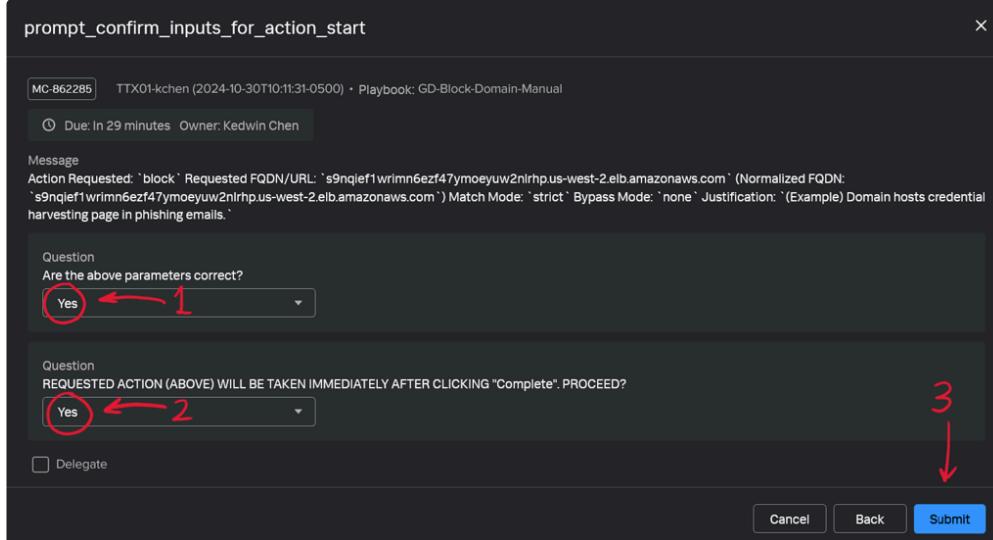
Cancel Back Submit ← 4

- c. Click **Submit**. The playbook will check again to see if the domain can be blocked using the new settings.
- d. Open the Prompt view again. You should see

prompt_confirm_inputs_for_action_start listed. If so, proceed to Step 9 (below). If not, check if there is an error message similar to the above in **#soar-notifications**.

| Prompts | | | | | |
|---|----------------|---------------|---------|----------|-----------------------|
| <input type="text"/> Search prompts Unanswered prompts 1 | | | | | |
| Prompt name | Owner | Due | Status | Response | |
| prompt_match_and_bypass_modes | kc Kedwin Chen | In 29 minutes | Pending | | <button>View</button> |

9. **prompt_confirm_inputs_for_action_start** - The domain is ready to be blocked. This prompt presents the information entered as interpreted by the playbook. **This is your last chance to cancel before the playbook takes action.** If all looks good, select **Yes** to both prompts.



10. Once the playbook completes, you will see a message in the `#soar-notifications` channel from the `InfoSec - SOAR` bot which will look similar to this

InfoSec - SOAR APP 14:45

Playbook Run Summary - GD-Block-Domain-Manual

Playbook Name
GD-Block-Domain-Manual

Launching User
kchen@godaddy.com

Inputs

Requested Domain/URL: `s9nqief1wrimn6ezf47ymoeyuw2nlrhp[.]us-west-2[.]elb[.]amazonaws[.]com`
 (Normalized FQDN: `s9nqief1wrimn6ezf47ymoeyuw2nlrhp[.]us-west-2[.]elb[.]amazonaws[.]com`)
 Requested Action: `block`
 Allowlist Check Mode: `strict`
 Checks Bypassed: `none`
 Check bypass justification: `(Example) Domain hosts credential harvesting page in phishing emails.`

Output

Corporate DNS API

Action Status(es): `success`

Action Message(s):

```
Successfully blocked s9nqief1wrimn6ezf47ymoeyuw2nlrhp[.]us-west-2[.]elb[.]amazonaws[.]com and *.[.]s9nqief1wrimn6ezf47ymoeyuw2nlrhp[.]us-west-2[.]elb[.]amazonaws[.]com
```

DNS Record(s):

```
s9nqief1wrimn6ezf47ymoeyuw2nlrhp.us-west-2.elb.amazonaws.com.security.gdrpz.com|2d8bfcfc-1230-4fc4-aa58-edef350f58c8
*.s9nqief1wrimn6ezf47ymoeyuw2nlrhp.us-west-2.elb.amazonaws.com.security.gdrpz.com|d11cdccb-3b39-43db-8e98-0869c5b55657
```


Forensic collection playbook

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[Forensics Evidence Collection](#)

[File Collection Process](#)

Purpose

| | |
|-----------------------|--|
| Responsible Team | <ul style="list-style-type: none">DetectionsSLACK: #internal-gcsoEMAIL: detectmon@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | Mar 19, 2025 |
| Escalation Contact(s) | IR@godaddy.com |
| Requests for Updates | |
| Training Log | |

Description

This playbook is a guide on how to collect forensics evidences from infected host.

Forensics Evidence Collection

Forensic collection from SentinelOne refers to the process of gathering and analyzing endpoint data to investigate security incidents, understand attack vectors, and uncover malicious activity on endpoints.

The below artifacts can be collected from the “**windows**” machine:

1. Drivers listing

2. Environment Variables

3. Groups Listing

4. Network ports listing

5. Processes

6. Scheduled task listing

7. Services

8. Users Listing

9. Powershell History

The below artifacts can be collected from “Linux” host

1. Environment Variables

2. Network Ports Listing

3. Process and Daemon Listing

4. Shell History

5. Users Listing

Note:

- We strongly recommend to collect Forensics artifacts before the machine isolation.
- We won't be able to run forensics collection if the host is offline.

File Collection Process

- Navigate to Sentinels
- Provide the host name.

The screenshot shows the SentinelOne interface under the 'ENDPOINTS' tab. A search bar at the top contains the endpoint name 'SG2VMSP-11-0022'. Below the search bar, there's a table with one item selected. The table columns include Endpoint Name, Endpoint Tags, Account, Site, Last Logged In User, Group, and a checkbox column. The selected row shows 'SG2VMSP-11-0022' in the Endpoint Name column, 'N/A' in Endpoint Tags, 'GoDaddy Inc.' in Account, 'ENG-Virtual Ephemeral' in Site, 'sbandi' in Last Logged In User, and 'Default Group' in Group. There are also 'Actions' and 'Group' dropdown menus above the table.

- Actions → Response → Forensics Collection

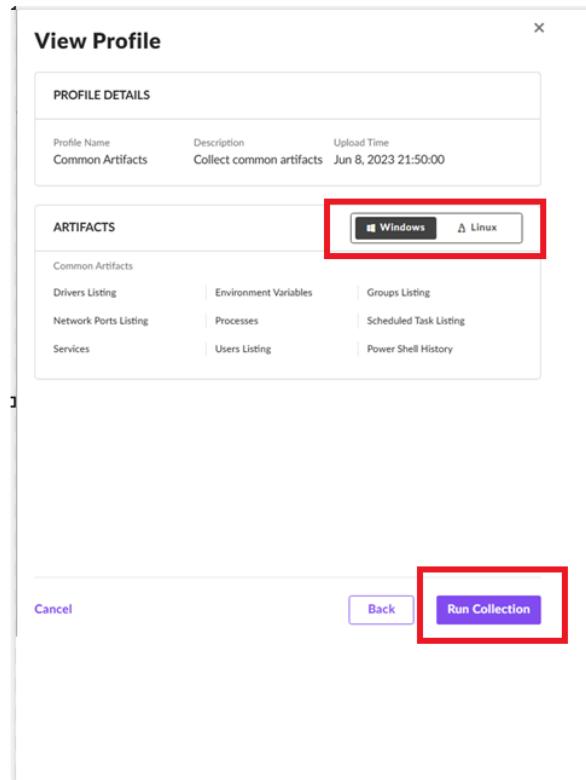
The screenshot shows the SentinelOne interface with the 'ENDPOINTS' tab selected. A search bar at the top contains the endpoint name 'SG2VMSP-11-0022'. Below the search bar, there is a table with columns: Endpoint Tags, Account, Site, Last Logged In User, Group, Domain, and Console. A dropdown menu titled 'Actions' is open, showing various options like 'Recently Used', 'Agent Actions', 'Endpoint Actions', 'Response', 'Agent Version Changes', 'Shortcuts', 'Full Disk Scan', 'Troubleshooting', 'Configuration', and 'Tech Support'. The 'Forensics Collection' option under the 'Response' section is highlighted with a red box.

- Click on Common Artifacts

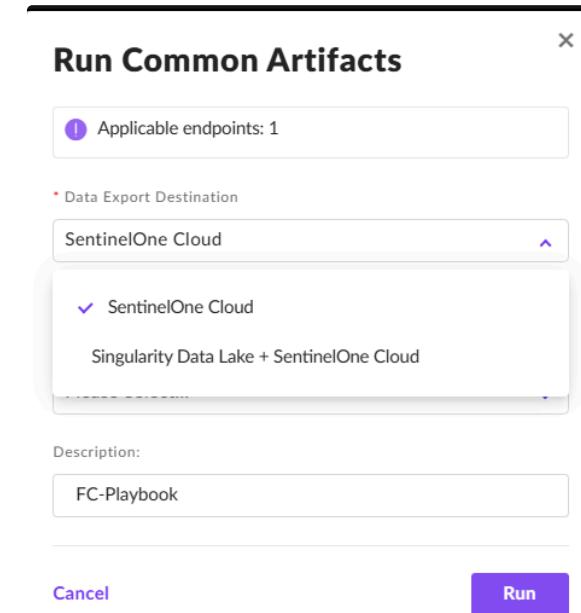
The screenshot shows the 'Forensic Collection' dialog box. At the top, it says 'Forensic Collection'. Below that is a table titled 'Select Profile' with columns: Name, Upload Time, Author, and OS. There are two rows: 'MAC Profile V1- D...' and 'Common Artifacts'. The 'Common Artifacts' row is highlighted with a red box. At the bottom of the dialog box are 'Cancel' and 'Run Collection' buttons.

| Name | Upload Time | Author | OS |
|------------------------|------------------------|----------------------|-------|
| MAC Profile V1- D... | Dec 17, 2024 16:12:... | amahajan@godaddy.... | Apple |
| Common Artifacts | Jun 8, 2023 21:50:00 | SentinelOne | Δ ■■■ |
| Processes and Servi... | Jun 8, 2023 21:50:00 | SentinelOne | ■■■ |

- Select appropriate Operating System → Run Collection



From Data export Destination option, Select any one option preferably “**SentinelOne Cloud**” & then provide random “**Description**” name as shown below.



Once you click on “**Run**”, You need to authenticate with “**okta**”.

⚠ Authentication Required

You must re-authenticate with your SSO Identity Provider to perform protected actions.

The authentication is valid for 30 minutes.

[Cancel](#)

[Authenticate](#)

Post okta validation, Navigate to Automation in S1 and look for the task which you created

| Task Name | Description | Initiated By | Initiated Time | Total In Current Scope | Completed | Failed | Pending | Pending User Action | Expired |
|---------------------|---------------------------------|---------------------------|-----------------------|------------------------|-----------|--------|---------|---------------------|---------|
| Forensic Collection | FC-Playbook | Prasanth Kumar Sridharapu | Mar 19, 2025 15:25:29 | 1 | 1 | 0 | 0 | 0 | 0 |
| Remote Script | Run HSDE remediation script ... | Api_hostingsec | Mar 19, 2025 15:14:25 | 1 | 1 | 0 | 0 | 0 | 0 |
| Remote Script | Run HSDE remediation script ... | Api_hostingsec | Mar 19, 2025 15:09:03 | 1 | 1 | 0 | 0 | 0 | 0 |
| Remote Script | Run HSDE remediation script ... | Api_hostingsec | Mar 19, 2025 15:08:52 | 1 | 1 | 0 | 0 | 0 | 0 |
| Remote Script | Run HSDE remediation script ... | Api_hostingsec | Mar 19, 2025 15:08:40 | 1 | 1 | 0 | 0 | 0 | 0 |
| Remote Script | Run HSDE remediation script ... | Api_hostingsec | Mar 19, 2025 15:05:58 | 1 | 1 | 0 | 0 | 0 | 0 |
| Remote Script | Run HSDE remediation script ... | Api_hostingsec | Mar 19, 2025 15:05:47 | 1 | 1 | 0 | 0 | 0 | 0 |
| Remote Script | Run HSDE remediation script ... | Api_hostingsec | Mar 19, 2025 15:05:33 | 1 | 1 | 0 | 0 | 0 | 0 |
| Remote Script | Run HSDE remediation script ... | Api_hostingsec | Mar 19, 2025 15:05:25 | 1 | 1 | 0 | 0 | 0 | 0 |
| Remote Script | Run HSDE remediation script ... | Api_hostingsec | Mar 19, 2025 14:54:47 | 1 | 1 | 0 | 0 | 0 | 0 |

Click on the task & check the status of it. Once it is completed, You can download the artifacts.

The Artifacts will be downloaded in Zip format & the output evidence files will be in JSON format.

Common Artifacts

TASK DETAILS

| | | |
|----------------------------------|---|-------------------------------|
| Profile Name Common Artifacts | Description FC-Playbook | Tag - |
| Target SG2VMSP-11-0032 | Output Destination SentinelOne Cloud | Status Collection finished |

ARTIFACTS

OS Type Windows

| Common Artifacts | Drivers Listing | Environment Variables | Groups Listing |
|------------------|-----------------|-----------------------|----------------|
| | | | |
| | | | |
| | | | |

Cancel **Download files**

Sample evidence output files:

| Name | Type | Compressed size | Password pr... | Size | Ratio | Date modified |
|---------------------------------|------------------|-----------------|----------------|--------|-------|-------------------|
| PowerShellHistory | File folder | | | | | 3/19/2025 3:26 PM |
| Drivers.json | JSON Source File | 12 KB | No | 116 KB | 90% | 3/19/2025 3:26 PM |
| EnvironmentVariableListing.json | JSON Source File | 1 KB | No | 4 KB | 78% | 3/19/2025 3:26 PM |
| Groups.json | JSON Source File | 2 KB | No | 5 KB | 71% | 3/19/2025 3:26 PM |
| NetworkPorts.json | JSON Source File | 2 KB | No | 15 KB | 92% | 3/19/2025 3:26 PM |
| Processlisting.json | JSON Source File | 61 KB | No | 562 KB | 90% | 3/19/2025 3:27 PM |
| ScheduledTasks.json | JSON Source File | 42 KB | No | 427 KB | 91% | 3/19/2025 3:27 PM |
| Services.json | JSON Source File | 11 KB | No | 94 KB | 89% | 3/19/2025 3:26 PM |
| Users.json | JSON Source File | 1 KB | No | 2 KB | 74% | 3/19/2025 3:26 PM |

How to create a PhishLabs ticket

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[Incident creation](#)

- [1. Create an incident](#)
- [2. Choose an incident type](#)
- [3. Incident type](#)
 - [3.1 Credential Theft](#)
 - [3.2 Domains](#)
 - [3.3 Customer inquiry](#)
- [4. Actions](#)

[5 PhishLabs user guide](#)

Purpose

| | |
|-----------------------|--|
| Responsible Team | <ul style="list-style-type: none">• Detections• SLACK: #internal-gcso• EMAIL: detectmon@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | Mar 28, 2025 |
| Escalation Contact(s) | |
| Requests for Updates | |
| Training Log | |

Description

This playbook is a guide on how to create an incident ticket in PhishLabs platform.

Incident creation

1. Create an incident

For creating a ticket go to Incidents in the left bar then click on the button + Create

The screenshot shows the PhishLabs web interface. On the left, there is a sidebar with the following menu items:

- Dashboard
- Observables
- Incidents** (highlighted with a red box)
- Watchlist
- Create Incident** (highlighted with a red box)
- Reports
- Research

The main content area is titled "Incidents". It features a "Create" button (also highlighted with a red box) and a "Download" button. Below these are sections for "DOMAINS" (with an incident ID: 1454034737) and "MONITORING".

2. Choose an incident type

There are 3 different incident types.

The screenshot shows the "Create Incident" page. The left sidebar is identical to the one in the previous screenshot. The main area is titled "Create Incident". A dropdown menu is open under the heading "Incident Type", with the following options listed:

- Credential Theft
- Customer Inquiry
- Domains

The "Credential Theft" option is highlighted with a blue background and a red border.

3. Incident type

3.1 Credential Theft

Involves cybercriminals creating fake websites that mimic legitimate ones to trick users into entering their login credentials.

- Here you will have to choose a **Brand**.

The screenshot shows the PHISHLABS interface. On the left is a dark sidebar with navigation links: Dashboard, Observables, Incidents, Watchlist, Create Incident (which is highlighted), Reports, and Research. The main area is titled 'Create Incident'. Under 'Incident Type', 'Credential Theft' is selected. In the 'Credential Theft Incident Details' section, there is a dropdown menu for 'Brand *' with two options: 'GoDaddy' (which is highlighted with a red box) and 'Poynt'.

- The incident status and severity will be automatically set.
- Add the URL starting with http or https.
- Browse and attach any evidence you can provide in a properly file extension.
- Click on Submit.

Create Incident

| | | | |
|---|---|--|------|
| Incident Type | Credential Theft | | |
| Brand * | GoDaddy | | |
| Incident Status | New | Severity | High |
| ! Incident Status and Severity are set based on your company's configuration defaults. | | | |
| Vishing | <input checked="" type="radio"/> | | |
| URL * | <input type="text" value="http://example.com"/> <div style="border: 2px solid red; padding: 2px; margin-top: 5px;"> http://example.com </div> | | |
| Comment | <input type="text" value="Enter text here"/> | | |
| | | Drag file here or <input type="button" value="Browse"/> <small>.png .jpg .jpeg .bmp .gif .pdf .doc .docx .xls .xlsx .csv .txt .zip .eml .msg .tiff</small> | |
| <input style="background-color: #E67E22; color: white; border: 1px solid #E67E22; padding: 5px; border-radius: 5px;" type="button" value="Submit"/> | | <input type="checkbox"/> Create another | |

3.2 Domains

PhishLabs monitors and takes down malicious domains that cybercriminals use for various attacks, such as phishing, business email compromise (BEC), and ransomware lures. Their domain monitoring service provides comprehensive visibility into domain threats by continuously tracking new and existing domain registrations and analyzing them for brand-related keywords and variation.

- Choose a brand and a Threat type.

The screenshot shows the PHISHLABS interface. The left sidebar contains navigation links: Dashboard, Observables, Incidents, Watchlist, Create Incident, Reports, and Research. The main area is titled 'Create Incident' and has a sub-section for 'Domains Incident Details'. It includes fields for 'Brand *' (set to 'GoDaddy') and 'Threat Type *' (a dropdown menu with options like 'Adult Content', 'Content Related to your Industry', etc.). A red box highlights the 'Incident Type' field, which is set to 'Domains'. Another red box highlights the 'Brand' field, which is set to 'GoDaddy'. A third red box highlights the 'Threat Type' dropdown menu, specifically the 'Adult Content' option.

- Select a threat type e.g Domain without Content.
- Add the domain and comment.
- Browse and attached a file.
- Finally click on submit.

Create Incident

| | |
|---|--|
| Incident Type | Domains |
| Brand * | GoDaddy |
| Threat Type * | Domain without Content |
| Incident Status | Monitoring |
| Severity | Low |
| <small>! Incident Status and Severity are set based on your company's configuration defaults.</small> | |
| Domain * | Example: https://domain.tld or http://subdomain.domain.tld |
| Comment | Enter text here |
| Drag file here or <input type="button" value="Browse"/> .png .jpg .jpeg .bmp .gif .pdf .doc .docx .xls .xlsx .csv .txt .zip .eml .msg .tiff | |
| <input type="button" value="Submit"/> | <input type="checkbox"/> Create another |

3.3 Customer inquiry

Typically involve users reaching out for support or information. PhishLabs offers 24/7 support via their web application or API integration, and they respond to emergency requests within an hour. This ensures that customers receive timely assistance for any issues they encounter.

4. Actions

After the incident is created you can select any of the 4 actions according to your needs.

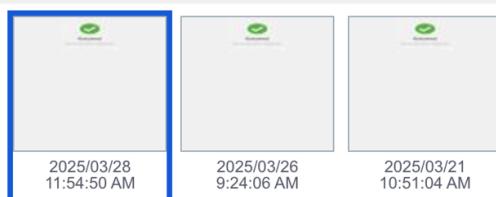
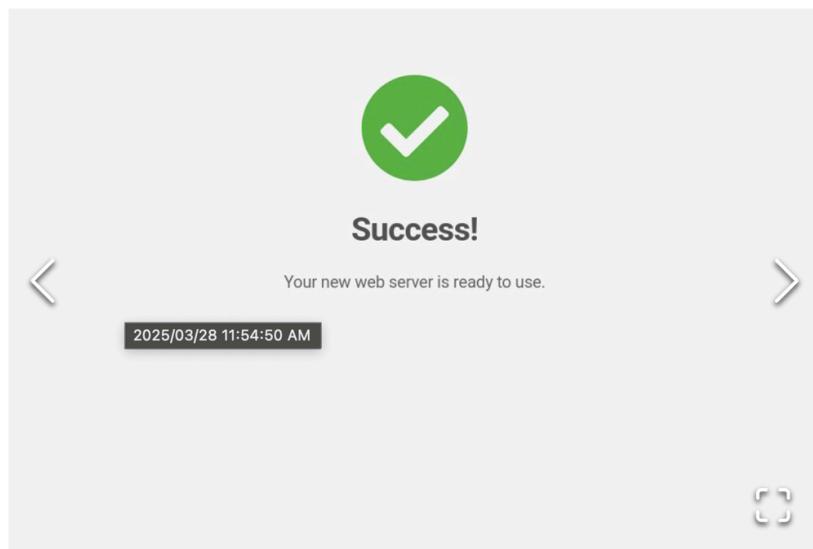
In the following example incident, we have the following parameters; incident type: “Domains” Threat type: “Domain without Content” and action: “Monitor for changes”. Although the site currently has no content, it will remain under monitoring because threat actors might upload content to impersonate the GoDaddy brand.

Incident #1441514545

| | |
|----------------------------|------------------------------|
| INCIDENT STATUS | ACTIONS |
| Monitoring | Select an Action |
| TITLE | Select an Action |
| https://menagewp.com | Add to Safelist |
| INCIDENT TYPE | Close, No Action Required |
| Domains | Monitor for Changes |
| SEVERITY | Start Take Down |
| Low | |
| INCIDENT AGE | LAST MODIFIED |
| 7 days | 2025/03/26 09:23 AM |
| CREATED BY | DATE RESOLVED |
| Luis Garcia | |
| STATUS REASON | BRAND |
| | GoDaddy |
| SOURCE | MITIGATION START DATE |
| Client Submitted (Web App) | 2025/03/21 10:55 AM |

SCREENSHOTS

 Request Screenshot



5 PhishLabs user guide



Prisma URL Filtering Playbook

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[Process Diagram](#)

[Prisma URL Filtering](#)

[1 Notification sent in the #security-private channel](#)

[2 Go to the thread in the #website-block-request channel](#)

[3 Access the URL Filtering Tool:](#)

[4 Analyze if the Site is Compromise or Infected](#)

[5 Is it a GD hosted site?](#)

[Scenarios](#)

[5.1 The site is hosted with GD and it is infected](#)

[5.2 The site is clean and hosted with GD.](#)

[5.3 The site is not hosted with GD](#)

[6 Submit for re-categorization](#)

[Tools](#)

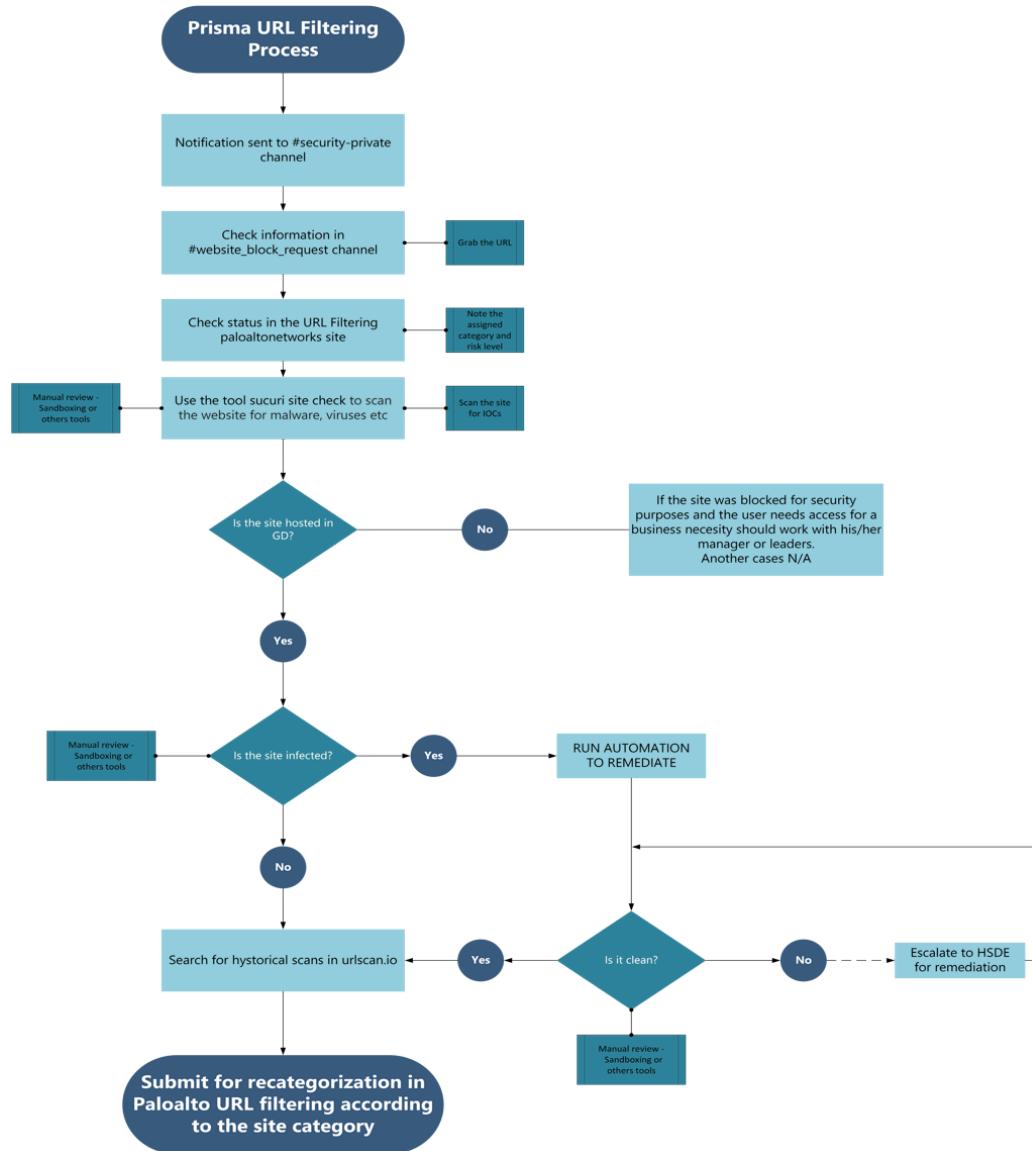
Purpose

| | |
|-----------------------|--|
| Responsible Team | <ul style="list-style-type: none">DetectionsSLACK: #internal-gcsoEMAIL: detectmon@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | Mar 19, 2025 |
| Escalation Contact(s) | @secmon - @hsde |
| Requests for Updates | |
| Training Log | |

Description

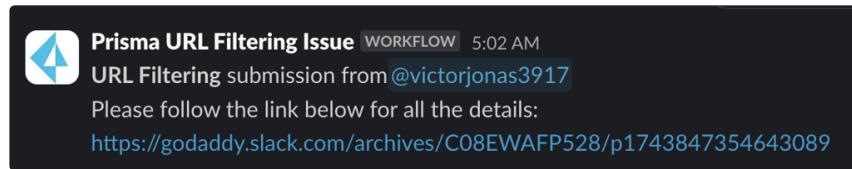
This playbook is a guide on how to analyze the reported URL and provide a solution for remediation and/or re-categorization when needed

Process Diagram



Prisma URL Filtering

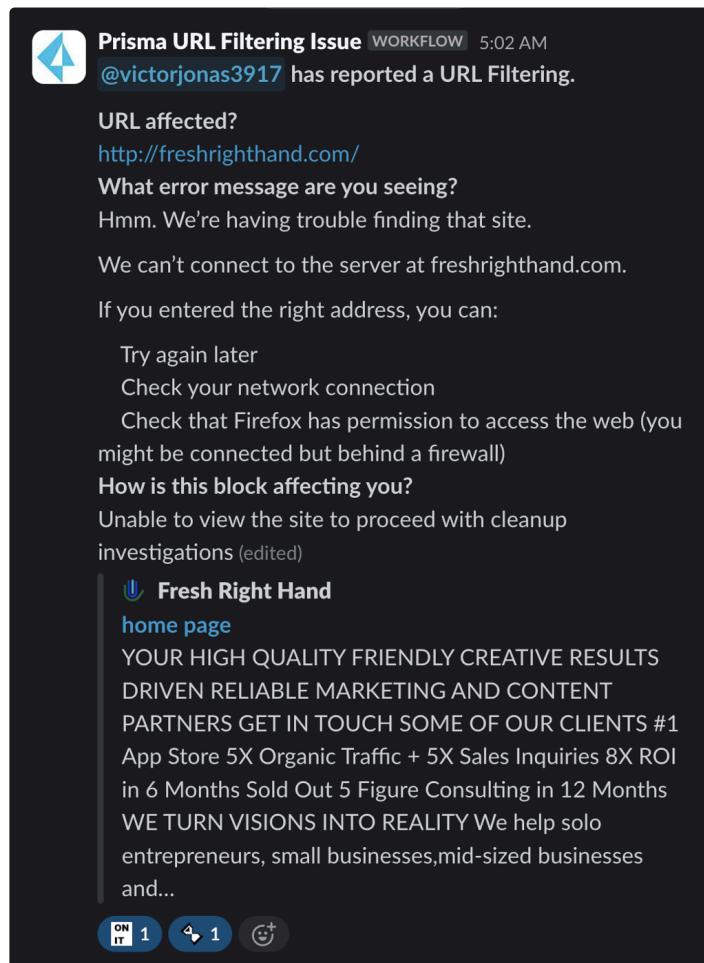
1 Notification sent in the #security-private channel



Prisma URL Filtering Issue WORKFLOW 5:02 AM
URL Filtering submission from @victorjonas3917
Please follow the link below for all the details:
<https://godaddy.slack.com/archives/C08EWAFP528/p1743847354643089>

2 Go to the thread in the #website-block-request channel

- Analyze what is reported by user.
- Grab the URL.
- In this thread, you should demonstrate that you are reviewing it :: and add the responses.



Prisma URL Filtering Issue WORKFLOW 5:02 AM
@victorjonas3917 has reported a URL Filtering.

URL affected?
<http://freshrighthand.com/>

What error message are you seeing?
Hmm. We're having trouble finding that site.
We can't connect to the server at freshrighthand.com.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

How is this block affecting you?
Unable to view the site to proceed with cleanup investigations (edited)

 **Fresh Right Hand**
[home page](#)
YOUR HIGH QUALITY FRIENDLY CREATIVE RESULTS
DRIVEN RELIABLE MARKETING AND CONTENT
PARTNERS GET IN TOUCH SOME OF OUR CLIENTS #1
App Store 5X Organic Traffic + 5X Sales Inquiries 8X ROI
in 6 Months Sold Out 5 Figure Consulting in 12 Months
WE TURN VISIONS INTO REALITY We help solo
entrepreneurs, small businesses,mid-sized businesses
and...

ON IT 1 ↗ 1 😊

3 Access the URL Filtering Tool:

- Use Palo Alto Networks' "Test A Site" tool to check the current category of the website. Enter the URL at Test A Site.

The screenshot shows the URL filtering interface at urlfiltering.paloaltonetworks.com/query/. The top navigation bar includes links for Products, Solutions, Services, Partners, Company, More, a search icon, and a red 'DEMONS AND TRIALS' button. The main content area is titled 'Test A Site' with a sub-section 'Test A Site'. It displays the URL <http://freshrighthand.com/> and its category 'Malware'. Below this, there is a detailed description of what constitutes Malware, mentioning malicious content like executables, scripts, viruses, trojans, and code. A 'Request Change' link is also present.

This screenshot shows the same URL filtering interface at urlfiltering.paloaltonetworks.com/query/. The results for the URL <http://avalsistemas.com/AvalAccount/Index?ReturnUrl=/> show it is categorized as 'Phishing'. The interface provides a detailed description of what constitutes Phishing, noting that it involves harvesting user information such as login credentials and credit card details through various means like social engineering. A 'Request Change' link is also available.

4 Analyze if the Site is Compromised or Infected

- Go to Sucuri SiteCheck to scan the website for malware, viruses, malicious redirects, and other indicators of compromise. You can use a sandbox

sitecheck.sucuri.net/results/gattispizzafranchise.com/wp-admin

SUCURI Website Monitoring Website Firewall Malware Removal Knowledgebase

⌚ **gattispizzafranchise.com/wp-admin**

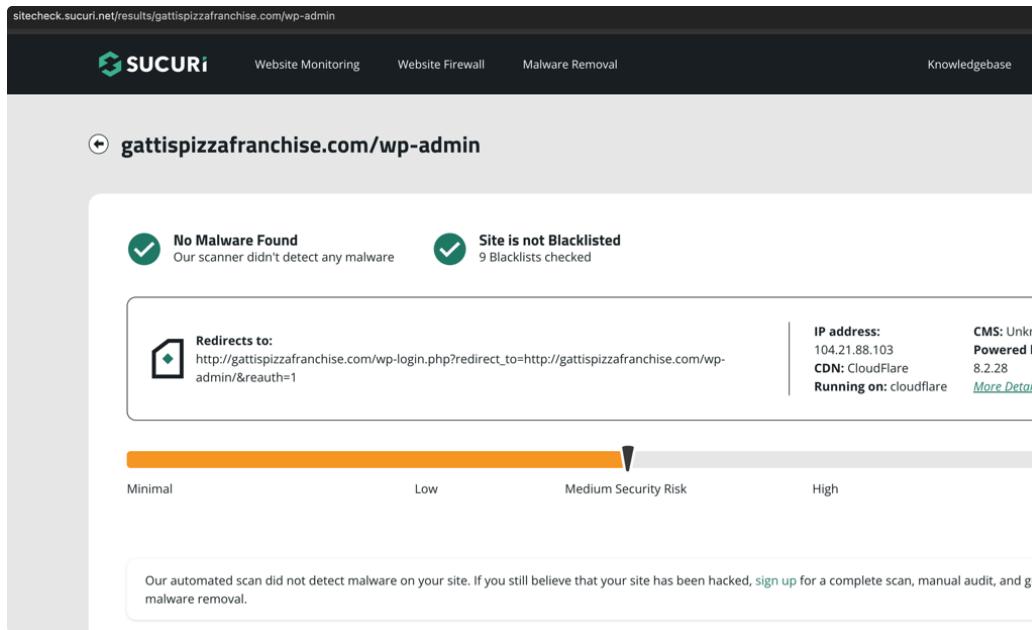
No Malware Found Our scanner didn't detect any malware Site is not Blacklisted 9 Blacklists checked

.Redirects to: http://gattispizzafranchise.com/wp-login.php?redirect_to=http://gattispizzafranchise.com/wp-admin/&reauth=1

IP address: 104.21.88.103 CMS: Unknown
Powered by: 8.2.28 Cloudflare Running on: cloudflare [More Details](#)

Minimal Low Medium Security Risk High

Our automated scan did not detect malware on your site. If you still believe that your site has been hacked, [sign up](#) for a complete scan, manual audit, and guaranteed malware removal.



5 Is it a GD hosted site?

Use CRM or <https://dza.int.secureserver.net/index.php> for checking if it is or not registered with GD

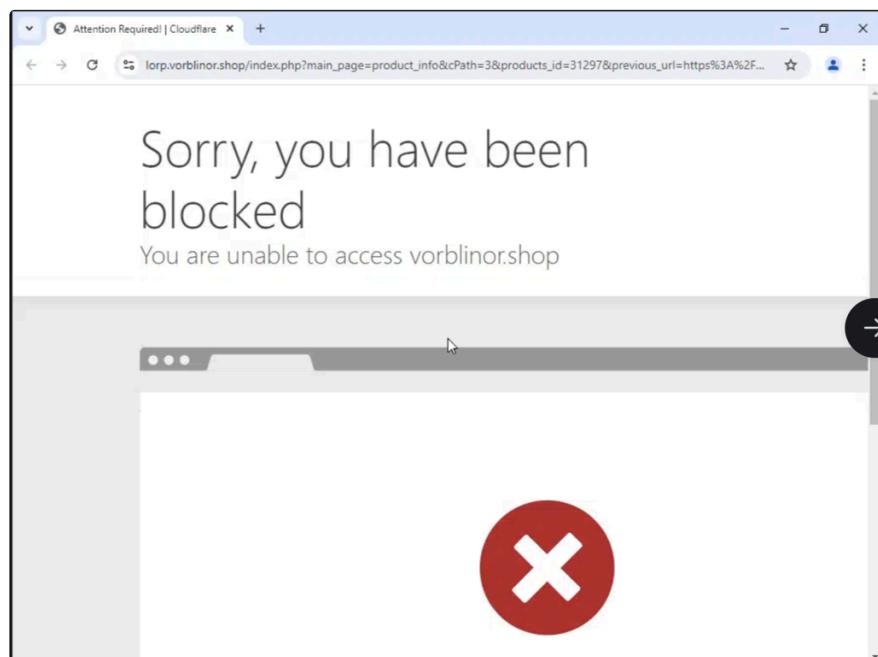
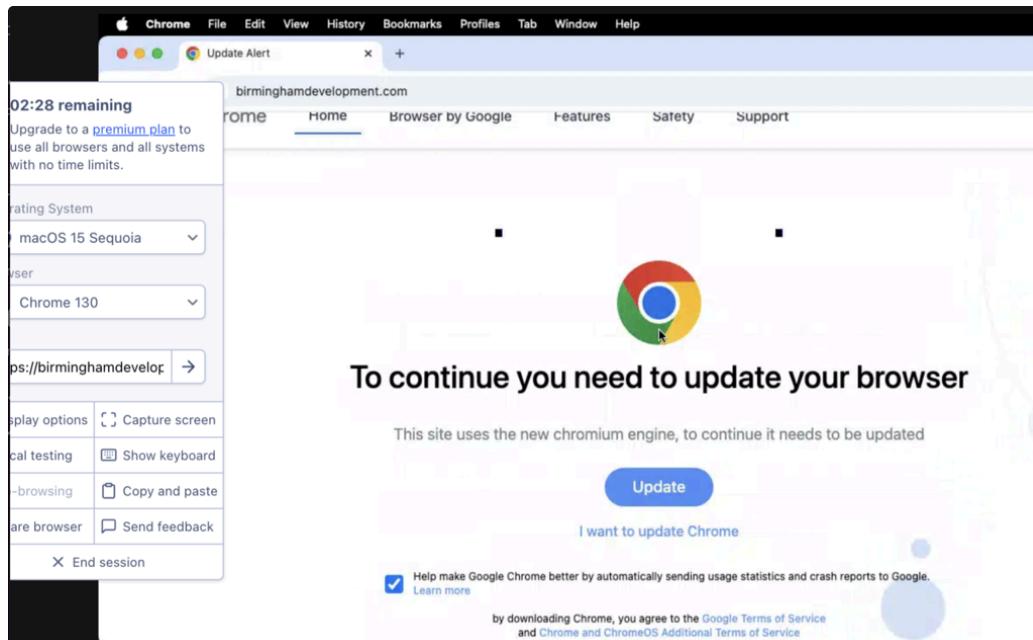
Scenarios

5.1 The site is hosted with GD and it is infected

Run the remediation [playbook](#) then if the site is clean go to step [6](#) submit for re-categorization.

If the infection persists escalate to @hsde for remediation after confirmation that site is clean go to step [6](#).

When using a sandbox, try various configurations such as switching between different browsers and operating systems like macOS, Windows, Android, and Linux.



5.2 The site is clean and hosted with GD.

The site is clean go to step [6](#) submit for recategorization.

The screenshot shows the Sucuri SiteCheck interface. At the top, it displays the URL "sitecheck.sucuri.net/results/adamdesautels.com". The main header features the "SUCURI" logo and navigation links for "Website Monitoring", "Website Firewall", "Malware Removal", and "Knowledgebase". Below the header, the site name "adamdesautels.com" is shown with a back arrow icon. Two green checkmarks indicate "No Malware Found" (scanner didn't detect any malware) and "Site is not Blacklisted" (9 Blacklists checked). A summary box shows the site "Redirects to: https://adamdesautels.com/" and technical details like "IP address: 192.124.249.106", "CDN: Sucuri Firewall", "Powered by: Unknown", and "Running on: Sucuri/Firewall". A "More Details" link is also present. Below this, a horizontal bar indicates "Low Security Risk" (green) between "Minimal" and "High". A note at the bottom states: "Our automated scan did not detect malware on your site. If you still believe that your site has been hacked, sign up for a complete scan, manual audit, and guaranteed malware removal."

The screenshot shows the homepage of Adam DesAutels. The browser title bar reads "Adam DesAutels - Fractional Executive". The page has a blue header with the site's logo and name "Adam DesAutels". The navigation menu includes "Home", "Services", "Adam's Articles", "Experience", and a prominent "SCHEDULE A CALL" button. The main content area features a large white text box with the following message: "Hi, and welcome! I'm a fractional executive, helping startups grow revenue without the cost of a full-time leader." Below this, a smaller text box says "Save money and scale faster with a fractional leader." and contains a "LET'S TALK" button.

5.3 The site is not hosted with GD

If the site is infected we can not address this.

If the site is clean but it is blocked by security purpose, and it is needed by user, he/she should work with her/his leader for getting access.

6 Submit for re-categorization

According to the site category submit a request for reclassify.

Test the site:

urlfiltering.paloaltonetworks.com/query/

The screenshot shows the 'Test A Site' page. At the top, there's a navigation bar with links for Products, Solutions, Services, Partners, Company, More, a search icon, and a 'DEMONS AND TRIALS' button. Below the navigation is a breadcrumb trail: Home / Test A Site. To the right is a 'Log in' link. The main content area has a title 'Test A Site'. Below it, a message says 'Enter a domain or URL into the search engine to view details about its current URL categories. To request recategorization of this website, click Request Change below the search results.' There's a 'URL' input field with 'Enter a URL' placeholder text, a 'SEARCH' button, and a red box highlighting the URL 'http://freshrighthand.com/'. Below the input field, a red box highlights the category 'Malware'. The description states 'Category: Malware' and 'Description: Sites containing or known to host malicious content, executables, scripts, viruses, trojans, and code'. Under 'Example Sites:', there's a 'Request Change' button, which is also highlighted with a red box.

Assigned the corresponding category according to the site:

urlfiltering.paloaltonetworks.com/single_cr?url=http%3A//freshrighthand.com/

The screenshot shows the 'Change A Site' page. At the top, there's a URL input field with 'http://freshrighthand.com/' and a 'Select New Category' dropdown menu. The 'Current Category' is listed as 'Malware'. The 'New Category*' dropdown menu is open, showing 'marketing' and 'Business-and-Economy'. The 'Business-and-Economy' option is selected and highlighted with a red box. Below the dropdown, there's a 'Comment' field with placeholder text about marketing and customer review management. There are also fields for 'Your Email*', 'Confirm Email*', and 'Captcha*'. At the bottom, there are 'Cancel' and 'SUBMIT' buttons.

Use your GoDaddy email account for this submission:

Change A Site

| | |
|---|---|
| URL | http://freshrighthand.com/ |
| Current Category | Malware |
| New Category* | <input type="button" value="Select New Category"/> |
| Comment | Please provide evidence for why this URL needs to be recategorized |
| Your Email* | UserName@godaddy.com |
| Confirm Email* | |
| Captcha* | <input type="checkbox"/> I'm not a robot  reCAPTCHA <small>Privacy - Terms</small> |
| <input type="button" value="Cancel"/> <input type="button" value="SUBMIT"/> | |

Click on submit and you will receive a confirmation message

Thank you for submitting a URL re-categorization request for "ijalu[.]com". We will review the request and notify you via email of our decision usually within one business day.

To prevent notifications from going to your spam folder, please add no-reply-url-feedback@paloaltonetworks.com to your email allow-list.

Url's and hostnames contained in this communication may have been modified for the purposes of security and to ensure delivery to recipients behind mail gateways actively filtering potential malware and phishing attacks.

Note: This is an unmonitored mailbox. Please do not reply to this email, as your response may not be received. If follow-up is required, please contact [Palo Alto Networks support](#).

Regards,
Palo Alto Networks

In one or two hours you will receive an email indicating what is the re-evaluation's result and what is the new category assigned to the site:

Thanks again for your URL re-categorization request. As a result of our re-evaluation, we have made the following changes:

URL: ijalu[.]com
Previous category: command-and-control
You suggested: business-and-economy
New category: shopping

The new categorization is available starting with URL DB version: 20250407.20252

If you disagree with this category change and you'd like to resubmit this request along with additional information that will help with accurate categorization, please visit: https://urldfense.com/v3/_http://urlfiltering.paloaltonetworks.com...;lHj18uoVe_LnxIcznJvn5YddDJDd9yYIPGKbVR5ma9Y8KGjvForOV8sAqYsL9w2TBjXnV5OLQD7qZhd3Bmhva0jaNz3W-YnFGEK72gXGCdOhd4S. Note that you may experience different URL categorizations for a given URL across different PAN-OS versions due to new URL filtering capabilities being introduced to more recent versions of PAN-OS.

Url's and hostnames contained in this communication may have been modified for the purposes of security and to ensure delivery to recipients behind mail gateways actively filtering potential malware and phishing attacks.

Note: This is an unmonitored mailbox. Please do not reply to this email, as your response may not be received. If follow-up is required, please contact [Palo Alto Networks support](#).

Regards,
Palo Alto Networks

Tools

 [Palo Alto Networks URL filtering - Test A Site](#)

 [Sucuri Security](#)

https://crm.int.godaddy.com/app/_/customer/search is it a customer?

<https://sandbox.recordedfuture.com/submit> is the site clean or infected?

<https://web-check.xyz/check> what the site is about? - registrar, metadata, etc.

How to view SQLite raw data in more readable format

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[Using DB Browser for SQLite Files](#)

[DB Browser usage Process](#)

Purpose

| | |
|-----------------------|--|
| Responsible Team | <ul style="list-style-type: none">DetectionsSLACK: #internal-gcsoEMAIL: detectmon@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | Apr 4, 2025 |
| Escalation Contact(s) | IR@godaddy.com |
| Requests for Updates | |
| Training Log | |

Description

This playbook is a guide on how to view SQLite raw data in more readable format.

Using DB Browser for SQLite Files

- 1. Download and Install DB Browser for SQLite.**
- 2. Open Your SQLite File.**
- 3. Browse and Query Data.**

DB Browser usage Process

- Download and install DB Browser for SQLite from the official website. e.g- [Downloads - DB Browser for SQLite](#)
- Download [DB Browser for SQLite - .zip \(no installer\) for 64-bit Windows](#) which does not require any installer to install it

image1



Downloads

(Please consider sponsoring us on Patreon 😊)

Windows

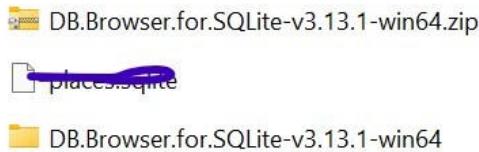
Our latest release (3.13.1) for Windows:

- DB Browser for SQLite – Standard installer for 32-bit Windows
- DB Browser for SQLite – .zip (no installer) for 32-bit Windows
- DB Browser for SQLite – Standard installer for 64-bit Windows
- DB Browser for SQLite – .zip (no installer) for 64-bit Windows

Free code signing provided by SignPath.io, certificate by SignPath Foundation.

- Unzip the downloaded file

image 2



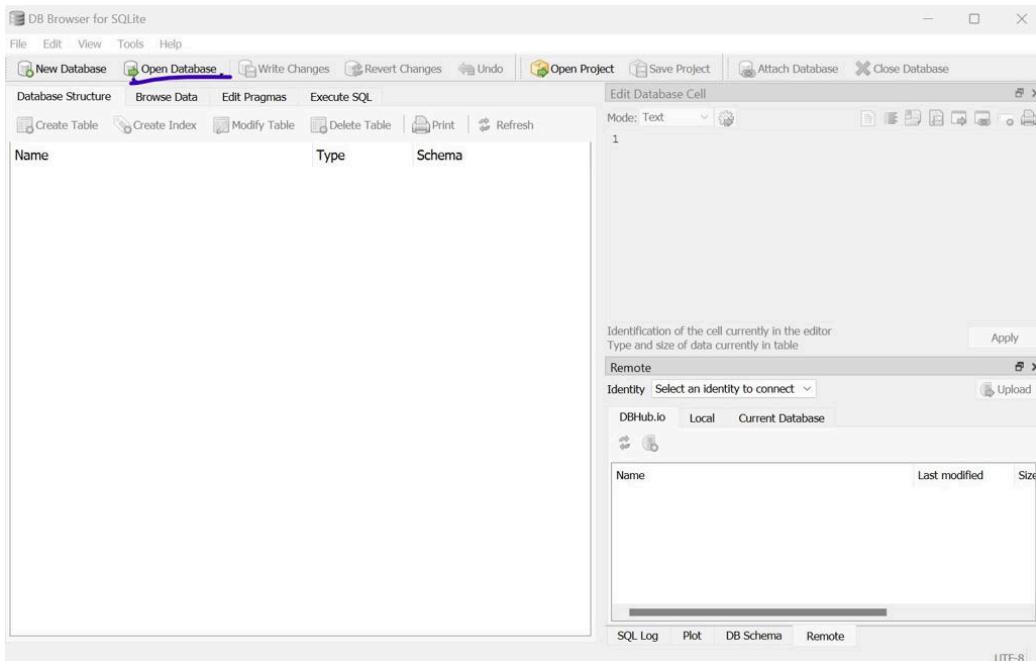
- Open the extracted file and launch DB Browser for sqlite.exe file

image 3

| | | |
|------------------------------|---------------------|--------------------------------|
| 📁 bearer | 4/3/2025 2:51 PM | File folder |
| 📁 extensions | 4/3/2025 2:51 PM | File folder |
| 📁 iconengines | 4/3/2025 2:51 PM | File folder |
| 📁 imageformats | 4/3/2025 2:51 PM | File folder |
| 📁 licenses | 4/3/2025 2:51 PM | File folder |
| 📁 platforms | 4/3/2025 2:51 PM | File folder |
| 📁 printsupport | 4/3/2025 2:51 PM | File folder |
| 📁 styles | 4/3/2025 2:51 PM | File folder |
| ▼ A long time ago | | |
| DB Browser for SQLite.exe | 10/15/2024 7:55 AM | Application 5.962 KB |
| DB Browser for SQLCipher.exe | 10/15/2024 7:55 AM | Application 5.997 KB |
| sqlcipher.dll | 10/15/2024 7:42 AM | Application extension 2,921 KB |
| sqlite3.dll | 10/15/2024 7:41 AM | Application extension 1,784 KB |
| msvcp140.dll | 10/27/2023 12:28 AM | Application extension 555 KB |
| msvcp140_2.dll | 10/27/2023 12:28 AM | Application extension 183 KB |
| concr140.dll | 10/27/2023 12:28 AM | Application extension 311 KB |
| msvcp140_1.dll | 10/27/2023 12:28 AM | Application extension 25 KB |
| msvcp140_atomic_wait.dll | 10/27/2023 12:28 AM | Application extension 57 KB |
| msvcp140_codecvt_ids.dll | 10/27/2023 12:28 AM | Application extension 22 KB |
| vccorlib140.dll | 10/27/2023 12:28 AM | Application extension 328 KB |

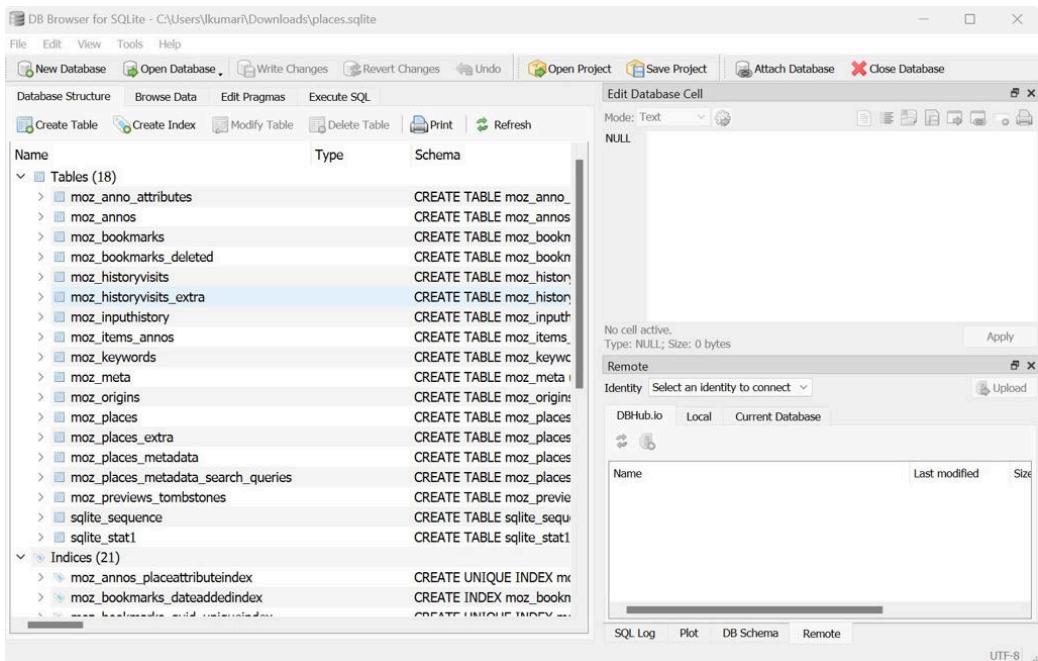
- Open your SQLite database file by clicking on the option Open Database.

image4



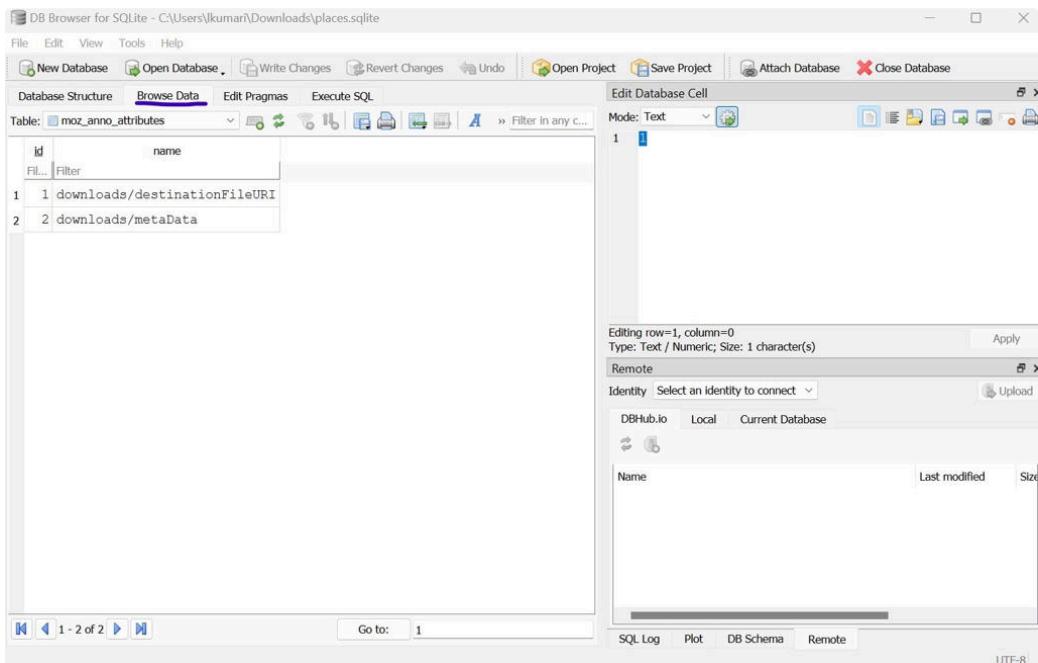
- Your SQLite file will open as shown below

image 5



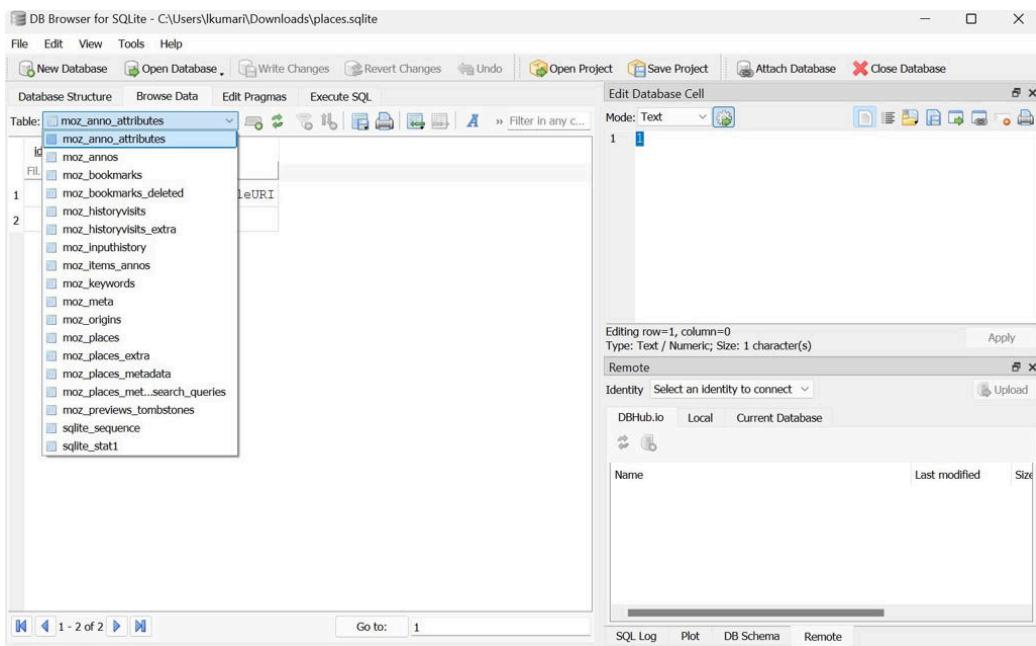
- Use the graphical interface to browse tables, execute SQL queries, and view data by clicking on the Browse Data option.

image 6



- Click on Table option and browse through all the folders to view data.

image 7



- Below is the view of data.

image 8

| | | host | frequency | recalc_frequency | |
|----|----|---|-----------|------------------|--|
| 1 | 1 | https://www.mozilla.org | 1 | | |
| 2 | 2 | https://secureserver.net.sharepoint.com | 24138 | | |
| 3 | 3 | https://support.mozilla.org | 100 | | |
| 4 | 4 | https://login.microsoftonline.com | 5431 | | |
| 5 | 6 | file:/// | 7851 | | |
| 6 | 7 | https://godaddy-corp.atlassian.net | 178183 | | |
| 7 | 8 | https://godaddy.service-now.com | 198552 | | |
| 8 | 9 | https://confluence.godaddy.com | 1 | | |
| 9 | 10 | https://compliance.microsoft.com | 1 | | |
| 10 | 11 | https://jira.godaddy.com | 1 | | |
| 11 | 12 | https://github.secureserver.net | 1 | | |
| 12 | 13 | https://ppc.int.gdcorp.tools | 1 | | |
| 13 | 14 | https://sensei-infosec.netlify.app | 1 | | |
| 14 | 15 | https://www.gorillastack.com | 1 | | |
| 15 | 16 | https://godaddysaas.splunkcloud.com | 1 | | |
| 16 | 17 | https://github.com | 1 | | |

Playbook for GDDY_AWS_Root_Account_Activity_Detected

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[Investigation](#)

Purpose

- Detections
- SLACK: #internal-gcso
- EMAIL: detectmon@godaddy.com

@Darko Zecic @Soumyadeep Basu

Mar 19, 2025

IR@godaddy.com

Description

This playbook is a guide on how to check GDDY_AWS_Root_Account_Activity_Detected alerts.

Investigation

- **Check if snow ticket exists** - Whenever [GDDY_AWS_Root_Account_Activity_Detected](#) alert triggered GCSO should check if snow ticket exists if yes then close the alert.
- **If does not exist** - check API calls for any suspicious or malicious API calls. If suspicious → escalate to IR

Splunk search:

```
'cloudtrail' userIdentity.type="Root" "PUT ACCOUNT ID HERE"
| stats min(_time) as firstTime max(_time) as lastTime values(signature) as
signature values(dest) as dest values(userAgent) as user_agent by
src_user src_ip aws_account_id
```

Examples of suspicious API calls:

1. Unusual API Calls:

- **Listing S3 Buckets:** `ListBuckets` API call from an unfamiliar IP address or region.
- **Accessing DynamoDB Tables:** `Scan` or `Query` API calls targeting tables that are not typically accessed.

2. Excessive API Requests:

- **Multiple Login Attempts:** `AssumeRole` API call repeatedly from different IP addresses, indicating a possible brute force attack.
- **High Volume Data Transfer:** `GetObject` API call on S3 buckets with a large number of requests in a short period.

3. Unauthorized Access Attempts:

- **Modifying S3 Bucket Policies:** `PutBucketPolicy` API call attempting to change permissions without proper authorization.
- **Accessing Secrets Manager:** `GetSecretValue` API call trying to retrieve secrets without the necessary permissions.

4. Privilege Escalation Attempts:

- **Changing IAM Roles:** `UpdateRole` or `AttachRolePolicy` API calls attempting to modify roles to gain higher privileges.
- **Creating New IAM Users:** `CreateUser` API call from an account that typically does not create users.

5. Data Exfiltration:

- **Large Data Transfers:** `PutObject` API call transferring large amounts of data to external destinations.
 - **Unusual Data Access:** `GetObject` API call accessing sensitive data that is not normally accessed.
- **If they are not suspicious** → reach out to account owner for confirmation

<https://pcp.int.gdcorp.tools> - you can find account owner using pcp.

- **If confirmed** → close otherwise escalate to IR

IDS Alert Playbook

Table of contents

Table of contents

Purpose

Description

 Incident Life Cycle

Analysis

Containment

Eradication

Recovery

Post-Incident Activity

Improvements

Approved and Reviewed by

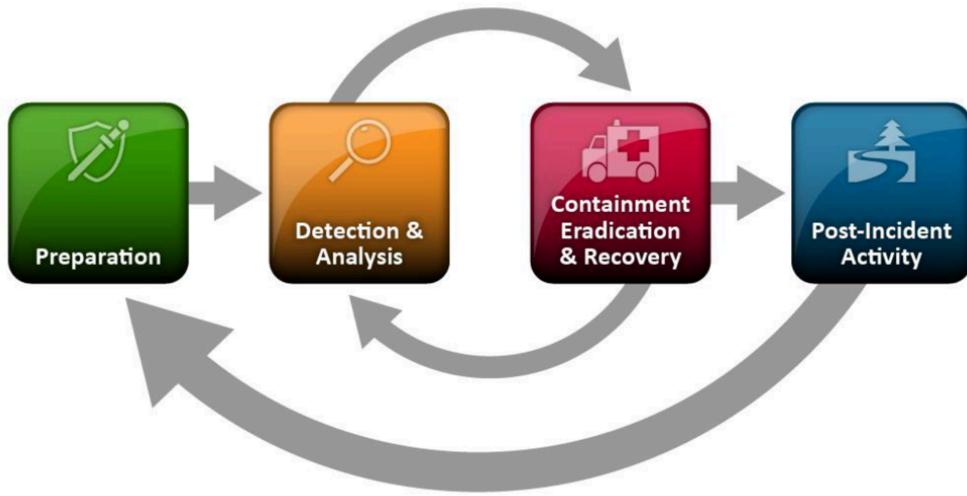
Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Monitoring Team• SLACK: #internal-gcso• EMAIL: GCSO@godaddy.com |
| Process Owner | David Hernandez |
| Last Review Date | |
| Escalation Contact(s) | Darko Zecic, David Hernandez |
| Requests for Updates | |
| Training Log | |

Description

This process provides direction for the analysis and remediation of an IDS alerts (such as IDS - Alerts for suspicious inbound traffic to PCI/PKI env, IDS - Alerts for suspicious outbound traffic from PCI/PKI env, Network_IDS_Suricata_Alert, Network_Inbound_IDS_Threats, Network_Lateral_IDS_Threats) and outlines the general process guidelines to be followed by the responding analyst. The process will follow the NIST incident lifecycle.

Incident Life Cycle



Analysis

1. Gather all the information related to alert:
 - a. Identify Source IP host if external (IP info) otherwise CMDB (if Source IP is GoDaddy owned machine)
 - b. Identify Destination IP host if external (IP info) otherwise CMDB (if Destination IP is GoDaddy owned machine)
 - c. Signature
 - d. Destination ports
 - e. Severity
 - f. Timeline
 - g. Understanding IDS rule
2. Check if there is history of such alerts between Source and Destination IP
3. Evaluate payload parameter in the alert log to understand more context

How to evaluate payload parameter shown with an example of packet captured:

- a. Splunk search query to get payload parameters details:

```
index="ids" src="10.196.80.44" dest="10.128.5.45"
```

```

Apr 24 05:57:57 p3plcorids001 suricata[4126]: {"uuid": "923F75D0651D48F387A687E118C7A9DF", "timestamp": "2025-04-24T05:57:57.574803+0000", "flow_id": 1395577624421166, "in_iface": "bond1", "event_type": "alert", "vlan": [140], "src_ip": "10.196.80.44", "src_port": 42028, "dest_ip": "10.128.5.45", "dest_port": 443, "proto": "TCP", "pkt_src": "stream (flow timeout)", "alert": {"action": "allowed", "gid": 1, "signature_id": 5000979, "rev": 1, "signature": "IPE - MAH RFC1918 -- WEB PORTS", "category": "Information Leak", "severity": 2, "metadata": {"author": "\\\njwade\\", "date-created": "2008-06-30"}, "direction": "to_server", "flow": {"pkts_toserver": 0, "bytes_toserver": 78, "bytes_toclient": 0}, "start": "2025-04-24T05:23:16.062789+0000", "src_ip": "10.196.80.44", "dest_ip": "10.128.5.45", "src_port": 42028, "dest_port": 443, "payload_printable": "", "stream": 0, "packet": "RQAAKAAAAABABhA0CsRQLAqABS2kLAG74stKvAAAAABQAAoAZ9gAA==", "packet_info": {"linktype": 1}}

```

b. Decode the above payload parameter:

"payload_printable\" : \\" - In Suricata, enabling "payload_printable" helps security analysts see the data being transmitted, such as the content of an email or a web page in readable format. Here as the value is showing as Null so there is no data been transmitted here.

The Base64 string

RQAAKAAAAABABhA0CsRQLAqABS2kLAG74stKvAAAAABQAAoAZ9gA

AA== decodes to the following binary data in hexadecimal format:

```

1 4500 0028 0000 0001 4006 1034 0ac4 502c
2 0a80 52da 42c0 06ef 8b2d 2af0 0000 0014
3 000a 0067 d800 0000

```

This data represents a network packet. Here's a breakdown of the decoded packet:

- **4500 0028**: IPv4 header indicating a total length of 40 bytes.
- **0000 0001**: Identification and flags.
- **4006 1034**: TTL (64), Protocol (TCP), Header checksum.
- **0ac4 502c**: Source IP address (10.196.80.44).
- **0a80 52da**: Destination IP address (10.128.82.218).
- **42c0 06ef**: Source port (17152), Destination port (1775).
- **8b2d 2af0**: Sequence number.
- **0000 0014**: Acknowledgment number.
- **000a 0067**: Data offset, Reserved, Flags.
- **d800 0000**: Window size, Checksum, Urgent pointer.

This packet is part of a TCP connection between the source IP **10.196.80.44** and the destination IP **10.128.82.218**, using ports **17152** and **1775** respectively. The packet includes sequence and acknowledgment numbers, which are used to ensure data integrity and order in the TCP stream.

4. Using below query, try to view logs for last 7 days/30 days to see if any pattern can be analyzed basis of timeline:

(index="ids" src="x.x.x.x" dest="x.x.x.x" | table _time, signature, severity, action, ids_type, vendor_product, category, dest, src, dest_port, sourcetype (sort the results basis of time))

5. Use Sentinel one to identify the process that generated the traffic (if Source IP is GoDaddy owned machine) and review suspicious indicators from that process.

Example to evaluate the above statement:

Sentinel query:

```
src.ip.address = '10.196.80.44' dst.port.number=443
```

During the time stamp when the alert triggered, we need to check all the events and processes for source IP in SentinelOne.

| Target | Event Details | Time |
|--------------|---|----------------------|
| 10.196.80.44 | /usr/sbin/squid --foreground ... | 2023-10-10T10:00:00Z |
| 10.196.80.44 | Source Process Parent Command Line: /usr/sbin/httpd -DFOREGRO... Source Process Command Line: /usr/sbin/httpd -DFOREGRO... | 2023-10-10T10:00:00Z |
| 10.196.80.44 | Source Process Parent Command Line: /opt/puppetlabs/puppet/bin/... Source Process Command Line: /usr/bin/python3 -m kcarectl... | 2023-10-10T10:00:00Z |
| 10.196.80.44 | Source Process Parent Command Line: /opt/puppetlabs/puppet/bin/... Source Process Command Line: /usr/bin/python /usr/bin/yum... | 2023-10-10T10:00:00Z |
| 10.196.80.44 | Source Process Parent Command Line: /opt/puppetlabs/puppet/bin/ruby /opt/puppetlabs/puppet/bin/puppet agent --no-daemonize Source Process Command Line: /opt/puppetlabs/puppet/bin/... Source Process Parent Command Line: /opt/puppetlabs/puppet/bin/... Source Process Command Line: /usr/bin/python /usr/bin/yum... | 2023-10-10T10:00:00Z |

As per the above logs, Puppet agent was used to check update and license info and no more suspicious activities have been observed.

6. Correlate Splunk findings with S1 logs to determine which process was making the connection/ any suspicious logins/ any suspicious process behavior/ Possible indicators (Timestamp on SentinelOne and Splunk should be considered carefully as we need to select Time range 10-15 minutes before and after in SentinelOne as per Splunk triggered alert timestamps)
7. Understand if there is a legitimate business reason for this traffic to flow between Source and Destination IP (Note: contact the machine owner - this one should not be used if absolutely necessary)

Containment

1. Servers - if it's confirmed that the server is infected (not customer closed environment) - escalate to IR immediately. Also pay attention on what the server purpose is and how important is it.
2. VDI - if VDI machine is infected and user is not L6 and above, run forensic collection, mitigate user credentials, isolate and if eradication is necessary, restart the VDI (which will create a

- clean VDI environment.)
3. Workstations - check the user position, run forensic collection, isolate the machine(be aware that eradication will not be possible if the workstation is isolated)

A few cents about ISOLATION:

- Running S1 isolation on the machine will make all the existing connections on the machine to drop so it's necessary to finish forensic collection before isolating.
- Doing forensic collection after isolation will not bring any results.
- All the connections will be gone except S1 agent collection.
- If you confirm something is malicious on the machine, but you need more time to investigate, after finishing forensic collection you can do isolation, do your investigation, unisolate and then finish eradication.
- Isolating servers without escalating to IR will make you be yelled at, get you fired and cost this company a lot of money.

Eradication

During the Eradication phase IR/L3 will remove all traces of malware or undoing what the threat actor did.

- **Note: If isolation was not possible, it is imperative that the incident responder/ L3 eliminates all traces of malware as soon as possible or revert machine to the last ShadowCopy saved state.**

Files/Paths that needs to be deleted/removed/checked on a server:

- a. **Temporary Files:** Check and delete suspicious files in `/tmp` , `/var/tmp` etc.
- b. **Log Files:** Review logs in `/var/log` for unusual activity. Delete or archive compromised logs.
- c. **User Directories:** Inspect home directories (`/home/username`) for unauthorized files.
- d. **System Files:** Verify integrity of files in `/etc` , `/bin` , `/sbin` , and `/usr/bin` .
- e. **Startup Scripts:** Check `/etc/init.d`, `/etc/systemd/system`, and `/etc/rc.d` for unauthorized scripts.
- f. **Cron Jobs:** Review and clean up cron jobs in `/etc/cron.d`, `/etc/cron.daily`, `/etc/cron.hourly`, `/etc/cron.weekly`, and `/etc/cron.monthly`.

g. Network Configurations: Inspect /etc/network, /etc/hosts, and /etc/resolv.conf for changes.

h. SSH Keys: Verify SSH keys in /home/username/.ssh and /root/.ssh.

i. Installed Packages: Use package managers (e.g., apt, yum) to check for unauthorized software.

j. Open Ports: Use tools like netstat or ss to identify unusual open ports.

k. User Accounts: Review /etc/passwd and /etc/shadow for unauthorized accounts.

Recovery

Our goal is to return to business as usual (BAU)

- Business owner will bring server back online
- Restore services back to BAU.
- Vulnerability team will test mitigations and/or patches are in place correctly

Post-Incident Activity

1. As soon as possible schedule an after action review or retrospective

- The following should be answered during an Incident Retro if one is held, if not, make note of the questions below and escalate to the appropriate teams if needed.
 - Are there new SIEM rules that we should created?
 - Are there additional security measures that should be implemented?
 - What went well
 - What can be improved.

2. L3/ Manager will finalize report and/or summary of the events and insure the timeline is up to date

For all other details regarding lesson's learned, follow the Retrospective process.

Improvements

Here you can suggest any improvements to the document

Approved and Reviewed by

| Approver | Task |
|----------|------|
| | |

| | |
|-------|---|
| Darko | DETECTMON-1818: Review and add Comments to IDS Alert Playbook DONE |
| | |
| | |
| | |

OnCall Escalation Procedure - MC Playbook

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[OnCall Escalation Procedure](#)

1. Open Mission Control Incident
2. Click on the Automation tab and then click on Run Playbook.
3. Search and select the “BR – SIR – PagerDuty – Manual Escalation for IR/HSDE/Detections” then click on Run playbook.
4. Now, click on Prompts.
5. Select “view” option in the pending prompt list. Please make ensure that you are clicking the “view” option for “questionnaire_for_sir_and_pd_incidents” which is on your name. from the prompt list.
6. Answer the questionnaire and select the team to which you will escalate the issue.
7. You will observe how the tasks are being completed.
8. You can verify how the message will be reflected in Slack according to the group to which you have escalated it.
9. As reply to the below notification getting on Internal-GCSO Channel, we can add the “Ask” and Investigation details.

Purpose

| | |
|-----------------------|--|
| Responsible Team | <ul style="list-style-type: none">• Detections• SLACK: #internal-gcso• EMAIL: detectmon@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | Mar 28, 2025 |
| Escalation Contact(s) | |
| Requests for Updates | |
| Training Log | |

Description

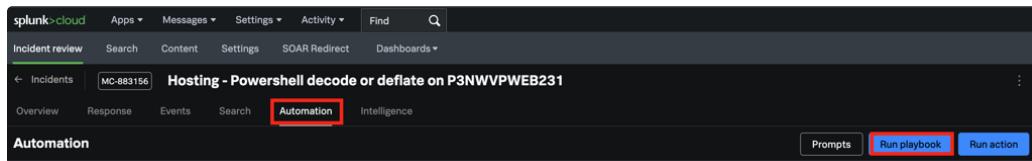
This playbook is a guide on how to escalate an incident to DETECTIONS, HSDE or IR

OnCall Escalation Procedure

1. Open Mission Control Incident

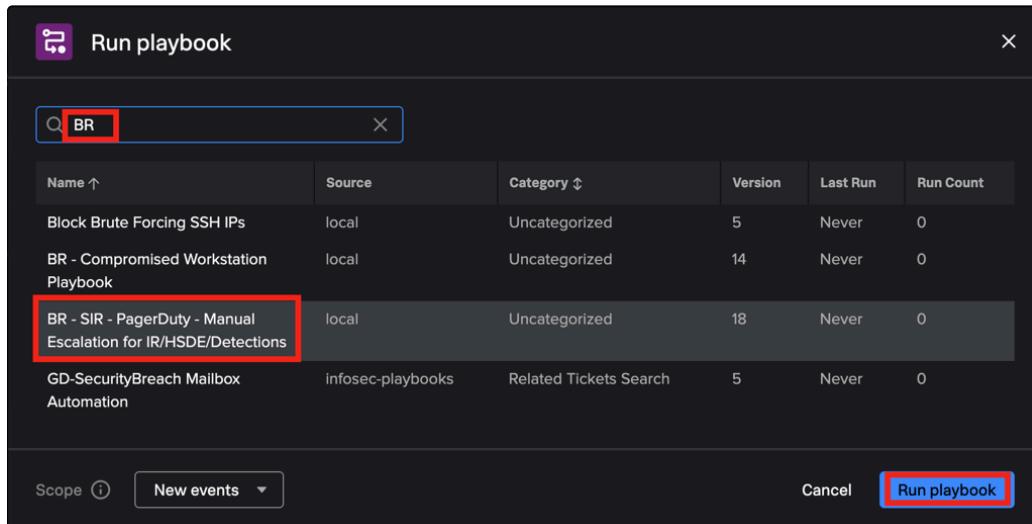
Open the MC ticket to escalate https://es.godaddy.splunkcloud.com/en-US/app/missioncontrol/mc_incident_review,

2. Click on the Automation tab and then click on Run Playbook.



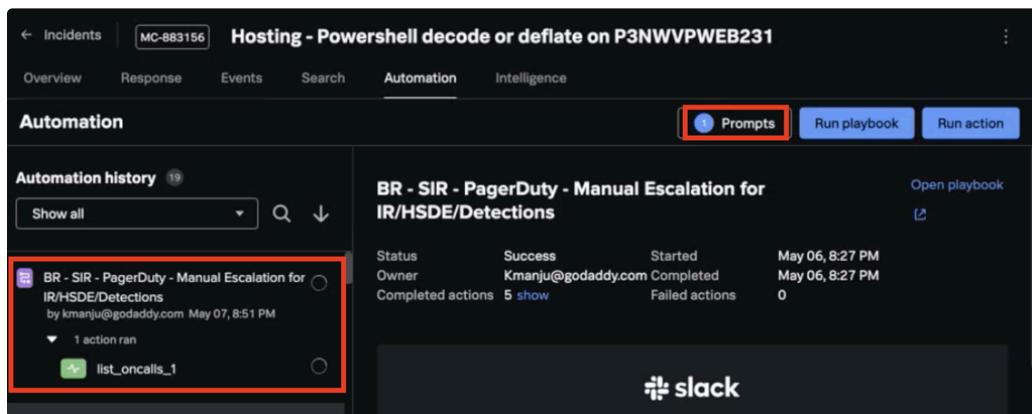
The screenshot shows the Splunk Cloud interface with the 'Automation' tab selected. At the bottom right, there is a prominent 'Run playbook' button with a red box around it.

3. Search and select the “BR - SIR - PagerDuty - Manual Escalation for IR/HSDE/Detections” then click on Run playbook.



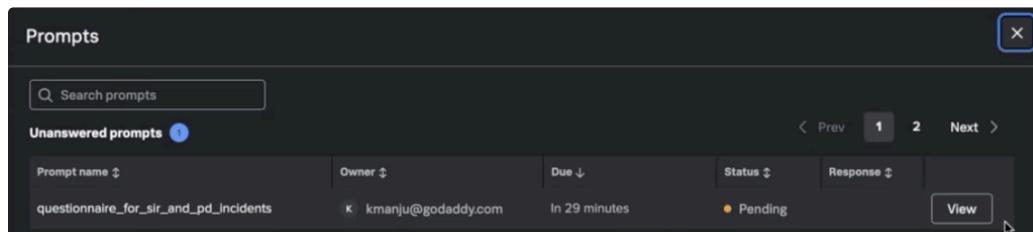
The screenshot shows the 'Run playbook' dialog box. The search bar at the top has 'BR' typed into it. Below the search bar is a table of playbooks. One row is highlighted with a red box, corresponding to the entry: 'BR - SIR - PagerDuty - Manual Escalation for IR/HSDE/Detections'. At the bottom right of the dialog box is another 'Run playbook' button with a red box around it.

4. Now, click on Prompts.



The screenshot shows the Splunk Cloud interface with the 'Automation' tab selected. In the top right corner, there is a 'Prompts' button with a red box around it. On the left side, there is a sidebar titled 'Automation history' with a red box around it. The main area displays a table for the selected automation entry: 'BR - SIR - PagerDuty - Manual Escalation for IR/HSDE/Detections'. The table includes columns for Status, Success, Started, and Completed actions. At the bottom right of the main area is a 'slack' logo.

5. Select “view” option in the pending prompt list. Please make ensure that you are clicking the “view” option for “questionnaire_for_sir_and_pd_incidents” which is on your name. from the prompt list.



The screenshot shows a software interface titled "Prompts". At the top, there is a search bar labeled "Search prompts" and a navigation bar with buttons for "Prev", "1", "2", "Next", and "X". Below this, a table lists "Unanswered prompts". The first row in the table corresponds to the prompt titled "questionnaire_for_sir_and_pd_incidents". The table includes columns for "Prompt name", "Owner", "Due", "Status", and "Response". The "Status" column shows "Pending". To the right of the table, there is a "View" button, which is highlighted with a blue border.

6. Answer the questionnaire and select the team to which you will escalate the issue.

For Hosting team escalation - Option to Select is **HSDE**

For IR team escalation - Option to select is **IR**

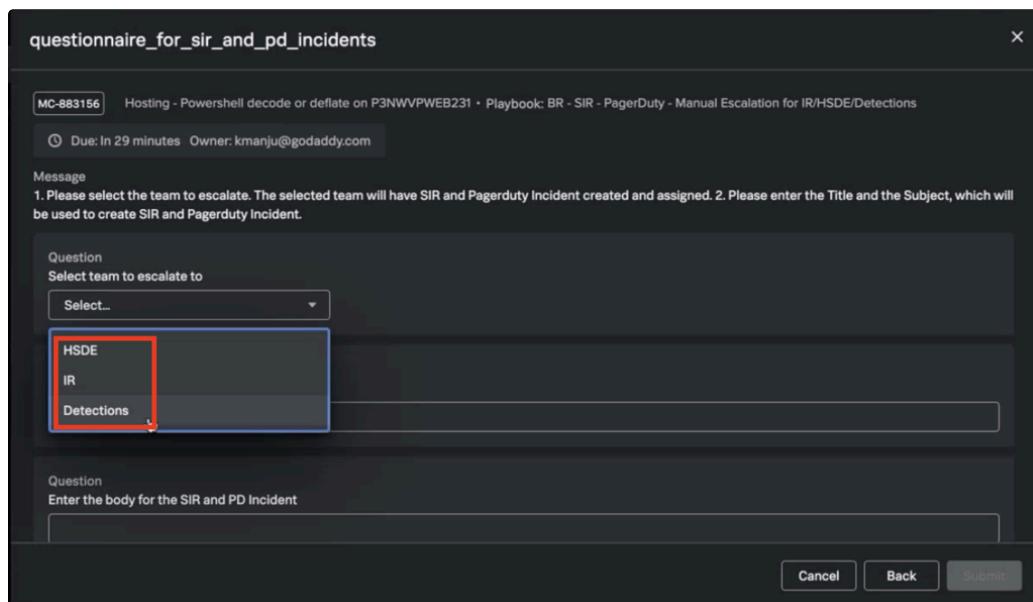
For any escalation detection team - option is **Detections**.

Add the responses to the other two questions as appropriate.

The title input should contain the verbiage as “ Security Incident Escalation" then short ID of the notable / notable title

The next prompt for Body should contain a brief information of Incident. (Should be one or two line). Signature not required to add over here.

Once three questions are answered, click **submit** button.



The screenshot shows a modal dialog box titled "questionnaire_for_sir_and_pd_incidents". At the top, it displays a reference number "MC-883156" and the context "Hosting - Powershell decode or deflate on P3NWVPWEB231 • Playbook: BR - SIR - PagerDuty - Manual Escalation for IR/HSDE/Detections". Below this, it shows the due date "Due: In 29 minutes" and the owner "Owner: kmanju@godaddy.com". The main content area is titled "Message" and contains instructions: "1. Please select the team to escalate. The selected team will have SIR and Pagerduty Incident created and assigned. 2. Please enter the Title and the Subject, which will be used to create SIR and Pagerduty Incident.". There are two sections for "Question". The first section, "Select team to escalate to", has a dropdown menu with three options: "HSDE", "IR", and "Detections". The "HSDE" option is highlighted with a red box. The second section, "Enter the body for the SIR and PD Incident", has a large text input field. At the bottom right, there are "Cancel", "Back", and "Submit" buttons.

questionnaire_for_sir_and_pd_incidents

Due: In 29 minutes Owner: kmanju@godaddy.com

Message

1. Please select the team to escalate. The selected team will have SIR and Pagerduty Incident created and assigned. 2. Please enter the Title and the Subject, which will be used to create SIR and Pagerduty Incident.

Question
Select team to escalate to
Detections

Question
Enter the title for SIR and PD Incident
test

Question
Enter the body for the SIR and PD Incident
Hi team, please ignore

Delegate

Cancel **Back** **Submit**

7. You will observe how the tasks are being completed.

BR - SIR - PagerDuty - Manual Escalation for IR/HSDE/Detections by kmanju@godaddy.com May 07, 8:51 PM

5 actions ran

- slack_to_detections
- create_detections_pd_incident ✓
- get_detections_oncall_user ✓
- questionnaire_for_sir_and_pd_incidents ✓
- list_oncalls_1 ✓

8. You can verify how the message will be reflected in Slack according to the group to which you have escalated it.

InfoSec - SOAR APP 9:35 AM

✓ Playbook Run Summary: "BR - SIR - PagerDuty - Manual Escalation for IR/HSDE/Detections"

@ir-team A SIR has been created and assigned to the Primary Oncall Member bboham@godaddy.com of Infosec_response.
A PagerDuty Incident has been assigned to Response team in PagerDuty.
Below are the details

SIR URL
https://godaddy.service-now.com/nav_to.do?uri=sn_si_incident.do?sys_id=7b99cb963b9da6d0117fa51916e45ae8

PagerDuty Incident Link
<https://gd-response.pagerduty.com/incidents/Q02HI9W0XEX7FA>

SIR and PD Incident Created By
kmanju@godaddy.com

9. As reply to the below notification getting on Internal-GCSO Channel, we can add the “Ask” and Investigation details.

 **PagerDuty** APP 8:05 PM
 **Security Incident Escalation : Test 2**
Business service(s):
 Resolved by Nishant Grover | Today at 6:09 PM

 **InfoSec - SOAR** APP 8:05 PM
 Playbook Run Summary: "BR - SIR - PagerDuty - Manual Escalation for IR/HSDE/Detections"

@ir-team A SIR has been created and assigned to the Primary Oncall Member bboham@godaddy.com of Infosec_response.
A PagerDuty Incident has been assigned to Response team in PagerDuty.
Below are the details

SIR URL
https://godaddy.service-now.com/nav_to.do?uri=sn_si_incident.do&sys_id=7b99cb963b9da6d0117fa51916e45ae8

PagerDuty Incident Link
<https://gd-response.pagerduty.com/incidents/Q02HI9WOXEX7FA>

SIR and PD Incident Created By
kmanju@godaddy.com

Volatility cheat sheet

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[Installation](#)

[Step-by-Step \(No Python install needed\)](#)

[1. Download Volatility Workbench](#)

[Command cheat sheet](#)

[Volatility 3 Plugin Categories and Descriptions](#)

[Common Options:](#)

[1. windows.info](#)

[2. Process and Thread Analysis](#)

[3. DLL and Handle Analysis](#)

[4. Network Analysis](#)

[5. Registry Analysis](#)

[6. File and Module Analysis](#)

[7. Memory Artifacts and Malware Detection](#)

[8. User Session / Credential Analysis](#)

[9. Dumping and Extraction](#)

[10. General / Utility Plugins](#)

[Summary Table](#)

[Example analyzing with Volatility\(Fileless Malware\)](#)

[1. Get System Info](#)

[2. List All Running Processes](#)

[3. Compare with psscan to Find Hidden/Unlinked Processes](#)

[4. Check Process Tree](#)

[5. Check for Memory Injections](#)

[6. List DLLs Loaded in Suspicious Processes](#)

[7. Look at VAD Info \(Process Memory Layout\)](#)

[8. Scan for Files in Memory \(Fileless payloads often live here\)](#)

[9. Dump Suspicious Memory Regions](#)

[10. Look for Credential Theft Signs](#)

[What Fileless Malware Typically Leaves Behind](#)

[Improvements](#)

[Approved and Reviewed by](#)

Purpose

Responsible Team

- Monitoring Team
- SLACK: #internal-gcso
- EMAIL: GCSO@godaddy.com

| | |
|-----------------------|-------------|
| Process Owner | Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | Darko Zecic |
| Requests for Updates | |
| Training Log | |

Description

This playbook provides a structured approach to using **Volatility 3** for memory forensics. It focuses on extracting and analyzing volatile data—such as process memory, loaded modules, kernel structures, network connections, and in-memory logs—that are not available through traditional disk-based analysis.

It includes practical steps for working with memory dumps, identifying malicious or suspicious activity, and using Volatility plugins to extract forensic artifacts. The goal is to support incident response, malware analysis, and post-compromise investigations by leveraging data that only exists in RAM.

Installation

Step-by-Step (No Python install needed)

1. Download Volatility Workbench

- [Volatility Workbench - A GUI for Volatility memory forensics](#)

- Unzip it
- Have fun

Command cheat sheet

Volatility 3 Plugin Categories and Descriptions

Volatility 3 is **modular**, and plugins are grouped by **operating system**, mainly:

- windows.*
- linux.*
- mac.*

- `framework.*` (general)
- `layers.*` (low-level memory layers)

Common Options:

| Option | Purpose |
|---|---------------------------------------|
| <code>-f</code> or <code>--single-location</code> | Path to memory image |
| <code>--pid</code> | Target a specific process |
| <code>--dump</code> | Enable dumping of files or memory |
| <code>--output-dir</code> | Set where dumps/results are stored |
| <code>-V</code> or <code>--verbose</code> | Show debug info |
| <code>--automagic-info</code> | Show what automagic modules are doing |

1. windows.info

- **What it does:** Basic system info.
- **Output:** OS version, build number, architecture, number of CPUs, etc.

2. Process and Thread Analysis

| Plugin | Description | Log/Output |
|---|---|----------------------------------|
| <code>windows.pslist</code> <code>t</code> | Lists active processes by walking the EPROCESS list | PID, name, offset, creation time |
| <code>windows.pstree</code> <code>e</code> | Same as pslist but shows parent/child relationships | Tree of processes |

| | | |
|-----------------------------|--|--|
| <code>windows.pssca</code> | Finds hidden or unlinked processes in memory | PID, name, found by scanning not walking |
| <code>windows.thread</code> | Lists all threads in memory | TID, PID, start time, stack base |

3. DLL and Handle Analysis

| Plugin | Description | Log/Output |
|-----------------------------|-------------------------------------|---|
| <code>windows.dllis</code> | Lists loaded DLLs for each process | PID, DLL name, base address, size |
| <code>windows.handle</code> | Lists open handles for each process | Type (file, event, mutex), handle value |

4. Network Analysis

| Plugin | Description | Log/Output |
|-----------------------------|--|---|
| <code>windows.netsca</code> | Scans for network connections (TCP/UDP) | Local/remote IPs, ports, states |
| <code>windows.netsta</code> | Lists active connections via kernel structures | More reliable but can miss stealthy connections |

5. Registry Analysis

| Plugin | Description | Log/Output |
|--|------------------------------------|---------------------------|
| <code>windows.registry.hivelist</code> | Lists all registry hives in memory | Name and address of hives |

| | | |
|--|---------------------------------|-----------------------------------|
| <code>windows.registry.printkey</code> | Reads keys and values in a hive | Key path, last write time, values |
| <code>windows.registry.userassist</code> | Shows program execution history | Useful for forensics timeline |

6. File and Module Analysis

| Plugin | Description | Log/Output |
|-------------------------------|---|--------------------------------|
| <code>windows.filescan</code> | Scans memory for FILE_OBJECT structures | File paths, types, references |
| <code>windows.moddump</code> | Dumps memory-resident modules (e.g. DLLs) | Can be used to extract malware |
| <code>windows.modules</code> | Lists kernel modules (drivers) | Name, base address, size |

7. Memory Artifacts and Malware Detection

| Plugin | Description | Log/Output |
|--------------------------------|---|--|
| <code>windows.malfind</code> | Finds injected or suspicious memory regions | Virtual address, suspicious regions, can dump code |
| <code>windows.ssdt</code> | Shows System Service Dispatch Table (for syscall hooks) | Hooked functions (potential rootkits) |
| <code>windows.callbacks</code> | Lists kernel-mode callbacks | Can show rootkit persistence |

| | | |
|--------------------------------------|-----------------------------|--------------------------------------|
| <code>windows.device tree</code> | Shows loaded device drivers | Can spot unsigned or unusual drivers |
|--------------------------------------|-----------------------------|--------------------------------------|

8. User Session / Credential Analysis

| Plugin | Description | Log/Output |
|------------------------------------|---|-------------------------------------|
| <code>windows.getsid s</code> | Lists security identifiers for each process | Useful for determining user context |
| <code>windows.hashdu mp</code> | Extracts user password hashes from SAM | Can be cracked offline |
| <code>windows.lsadump p</code> | Dumps credentials from LSA secrets | Passwords, keys (admin-only) |

9. Dumping and Extraction

| Plugin | Description | Log/Output |
|-------------------------------------|---|---------------------------------|
| <code>windows.memdump p</code> | Dumps memory from a process | Raw memory dump file |
| <code>windows.dumpfi les</code> | Extracts file objects from memory | Recover files (config, malware) |
| <code>windows.vadinfo o</code> | Lists process VAD (Virtual Address Descriptors) | Memory layout per process |

10. General / Utility Plugins

| Plugin | Description | Log/Output |
|----------------------------------|--|----------------------|
| <code>framework.inf o</code> | Shows version info for Volatility itself | Useful for debugging |

| | | |
|-----------------------------|------------------------------|-------------------------------|
| <code>layers.physica</code> | Dumps physical memory layout | Advanced usage |
| <code>1</code> | | |
| <code>automagic.*</code> | Auto-detects OS and layers | Usually invoked automatically |

Summary Table

| Category | Example Plugins | Useful For |
|-------------|--|--|
| System Info | <code>windows.info</code> | Confirming memory image type |
| Processes | <code>pslist</code> , <code>pstree</code> | Finding running/hiding malware |
| Modules | <code>dlllist</code> , <code>modules</code> | Identifying injected or unsigned code |
| Registry | <code>printkey</code> , <code>userassist</code> | Timeline and persistence analysis |
| Network | <code>netscan</code> , <code>netstat</code> | C2 and lateral movement detection |
| Malware | <code>malfind</code> , <code>ssdt</code> , <code>callbacks</code> | Detecting stealthy code/memory injection |
| Dumping | <code>memdump</code> , <code>dumpfiles</code> | Extracting suspicious artifacts |
| Users | <code>getsids</code> , <code>hashdump</code> | Mapping user activity and credentials |

Example analyzing with Volatility(Fileless Malware)

1. Get System Info

```
python vol.py -f memdump.raw windows.info
```

Why: Identify the Windows version and architecture to ensure the correct plugin usage.

Output:

```
Kernel Base, Kernel DtB, Is64Bit, Major/Minor Version,  
Build, etc.
```

2. List All Running Processes

```
python vol.py -f memdump.raw windows.pslist
```

Why: Baseline of active processes; look for **suspicious names, unusual parents, odd timestamps**.

Red Flags:

- Processes like `powershell.exe`, `wscript.exe`, `rundll32.exe`, `mshta.exe` with odd parents or start times
- Unknown or obfuscated names

3. Compare with `psscan` to Find Hidden/Unlinked Processes

```
python vol.py -f memdump.raw windows.psscan
```

Why: Scans memory for processes not in the active list — **used by stealthy malware**.

Red Flags:

- A process present in `psscan` but missing from `pslist`

4. Check Process Tree

```
python vol.py -f memdump.raw windows.pstree
```

Why: Shows parent-child relationships. Fileless malware often runs via LOLBins (e.g., powershell spawned from Word).

Red Flags:

- `powershell.exe` → child of `winword.exe`
 - `cmd.exe` or `rundll32.exe` with unknown parent
-

5. Check for Memory Injections

```
python vol.py -f memdump.raw windows.malfind
```

Why: Detects memory regions that look like **injected code** — key for **fileless payloads**.

Expected Output:

- Virtual address
- Protection (e.g. `PAGE_EXECUTE_READWRITE`)
- Suspicious shellcode or PE headers in memory

Red Flags:

- Suspicious memory regions inside legit processes (like `explorer.exe`)
 - Dump and analyze with tools like `strings` or YARA
-

6. List DLLs Loaded in Suspicious Processes

```
python vol.py -f memdump.raw windows.dlllist --pid  
<suspicious_pid>
```

Why: Check if any **non-standard DLLs** were injected or reflectively loaded.

Red Flags:

- DLLs from unusual paths (e.g., `C:\Users\...\Temp`)
 - Missing path information (indicative of reflective injection)
-

7. Look at VAD Info (Process Memory Layout)

```
python vol.py -f memdump.raw windows.vadinfo --pid  
<suspicious_pid>
```

Why: Shows memory regions — **shellcode or scripts** often reside in non-image VADs.

Red Flags:

- Large memory areas with execute permissions and no mapped file
- Regions marked as `Private Memory` with suspicious sizes

8. Scan for Files in Memory (Fileless payloads often live here)

```
python vol.py -f memdump.raw windows.filescan
```

Why: Locates file objects in memory, even if they're not saved to disk.

Red Flags:

- `.ps1`, `.vbs`, `.js`, or unknown file types in temp or user directories
 - Look for files with no backing path
-

9. Dump Suspicious Memory Regions

```
python vol.py -f memdump.raw windows.malfind --pid  
<suspicious_pid> --dump
```

Why: Extracts payloads for offline malware analysis

What to Do Next:

- Run `strings` or `yara` on the dumped files
 - Use a sandbox (like Any.Run or Hybrid Analysis)
-

10. Look for Credential Theft Signs

```
python vol.py -f memdump.raw windows.lsadump
```

Why: Fileless malware often steals credentials from memory (Mimikatz-style)

Red Flags:

- Cleartext passwords
 - NTLM hashes
 - Secret keys
-

What Fileless Malware Typically Leaves Behind

| Indicator | Where Seen | Volatility Plugin |
|---------------------------------|-----------------|----------------------|
| Suspicious parent/child process | Process tree | <code>pstree</code> |
| Memory-only shellcode | Injected region | <code>malfind</code> |

| | | |
|----------------------------|--------------|---|
| Script files not on disk | File objects | <code>filescan</code> , <code>dlllist</code> |
| Memory gaps or RWX VADs | Memory map | <code>vadinfo</code> |
| Stolen credentials | LSA secrets | <code>lsadump</code> |

Improvements

Here you can suggest any improvements to the document

Approved and Reviewed by

| Approver | Task |
|----------|------|
| | |
| | |
| | |

RF Domain Abuse Alert Playbook

Table of contents

[Table of contents](#)

[Purpose](#)

[Description](#)

[Process Diagram](#)

[Domain Abuse Alert](#)

- 1 An alert is triggered in SPLUNK
- 2 Visit the alert source link in the SecurityBreach mailbox
- 3 Get the domain to analyze from the message
- 4 Analyze if the Site is impersonating GoDaddy or any of our brands
- 5 Create a ticket in Phishlabs?

[Tools](#)

Purpose

| | |
|-----------------------|--|
| Responsible Team | <ul style="list-style-type: none">• Detections• SLACK: #internal-gcso• EMAIL: detectmon@godaddy.com |
| Process Owner | @David Hernandez |
| Last Review Date | Mar 19, 2025 |
| Escalation Contact(s) | @secmon - @hsde |
| Requests for Updates | |
| Training Log | |

Description

This playbook is a guide on how to analyze the reported URL and provide a solution for remediation and/or re-categorization when needed

Process Diagram

Domain Abuse Alert

1 An alert is triggered in SPLUNK

“SecurityBreach@ - alert@recordedfuture.com - Updates on Domain Abuse Alert – High Priority – GoDaddy Organization”

2 Visit the alert source link in the SecurityBreach mailbox

| rule_title | status_label | owner_realname | Risk Object |
|--|---|--------------------------|-------------|
| SecurityBreach@ - alert@recordedfuture.com - Updates on Domain Abuse Alert – High Priority – GoDaddy Organization | Pending | hharidas@goda ddy.com | -- |
| Description | | | |
| Kindly check the SecurityBreach@godaddy.com mailbox for more info on the notable. NOTE: Check the email link url to access the mail chain.--Check this link for a playbook on steps for triaging this notable: https://godaddy-corp.atlassian.net/wiki/x/A55y2w | | | |
| Additional Fields | Value | Action | |
| Alert Source Link | https://outlook.office365.com/owa/? ItemID=AAMkAGMyNDEwNDE4LWMxZGUtNGY0OS05YTBlWEYzk2YzM3MDYwZABGA AAAAAA7bSyhsAH%2FSJ8%2FpxbEndF%2BBwBHSdQPThlwSoQnYMZMT2ynAAAAAAE MAABHSdQPThlwSoQnYMZMT2ynAABk4R7AAAA%3D&exvsurl=1&viewmodel=ReadMess ageItem | ▼ | |
| Rule Description | Kindly check the SecurityBreach@godaddy.com mailbox for more info on the notable. NOTE: Check the email link url to access the mail chain.--Check this link for a playbook on steps for triaging this notable: https://godaddy-corp.atlassian.net/wiki/x/A55y2w | ▼ | |
| Rule Name | SecurityBreach Mailbox Automated Notable Creator | ▼ | |
| Sender | alert@recordedfuture.com | ▼ | |
| Severity | high | ▼ | |
| Subject | Updates on Domain Abuse Alert – High Priority – GoDaddy Organization | ▼ | |
| Event Details | | | |
| event_hash | 051941e926aa9b7a790cb7e99daf91be | ▼ | |
| event_id | CFF9F5E8-32D7-4EBF-924C- F9944C822798@@notable@@051941e926aa9b7a790cb7e99daf91be | ▼ | |
| eventtype | notable | ▼ | |
| Short ID | +ZQva5 | ▼ | |

3 Get the domain to analyze from the message

Updates on Domain Abuse Alert – High Priority – GoDaddy Organization

Domain Abuse alerts detect domains impersonating yours, potentially used for phishing or malicious purposes.

www[.]remoto[.]godaddyshop[.]com

Updates

- Priority Updated: **Informational** → High Jun 19, 2025, 00:35 UTC
-  Logotype GoDaddy detected Jun 19, 2025, 00:35 UTC



Has Domain screenshot

Created Jun 18, 2025, 00:32 UTC | Status: Resolved

Comments:

Managed Services - Swimlane, Jun 19, 2025, 01:20 UTC
"Alert processed by Managed Services."

Managed Services - Swimlane, Jun 18, 2025, 01:35 UTC
"Alert processed by Managed Services."

4 Analyze if the Site is impersonating GoDaddy or any of our brands

- You can use a sandbox as RF for visiting the site

5 Create a ticket in Phishlabs?

 [How to create a PhishLabs ticket](#)

Tools

- Recorded future sandbox
<https://sandbox.recordedfuture.com/submit>
- Anomali sandbox
<https://ui.threatstream.com/sandbox>
- Browserling

Abnormal Connection count from hosting to non hosting alert handling playbook- Draft

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description](#)
- [Detection Rule](#)
- [Investigation Process](#)
- [Template for requesting netvio](#)
- [Common False Positives](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Incident Response• SLACK: #internal-gcso• EMAIL: ir@godaddy.com |
| Process Owner | @Soumyadeep Basu @Darko Zecic |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | By Email - ir@godaddy.com |
| Training Log | By: @Darko Zecic @Soumyadeep Basu |

Description

This playbook outlines the approach to identify, investigate, and remediate situations where a machine from hosting environment is generating an unusually high number of connections towards a non-hosting environment machines. Such abnormal connection spikes may indicate underlying issues such as security threats like machine compromise, Customer VPS compromise etc.

By following this playbook, we can effectively detect and respond to abnormal connection patterns, thereby maintaining service reliability, securing network communications, and preventing potential exploitation or resource exhaustion.

Detection Rule

```
1 (pan_network_traffic) OR (index=palo_alto log_type="TRAFFIC")
2 | search NOT
3   [| inputlookup gd_vulnerability_scanners.csv
4     | stats count by prefix
5     | rename prefix as src
6     | fields - count]
7 | lookup u_subnet_nsz.csv u_cidr as src output u_nsz as src_nsz u_location as src_location
8 | lookup u_subnet_nsz.csv u_cidr as dest output u_nsz as dest_nsz u_location as
dest_location
9 | fillnull value="Internet/Unknown" src_nsz dest_nsz
10 #Traffic from hosting to non-hosting
11 | search src_nsz IN ("GoDaddy Cloud Network CMH", "Customer Managed Hosting", "GoDaddy Cloud
Network MAH", "Managed Hosting") NOT dest_nsz IN ("GoDaddy Cloud Network CMH", "Customer
Managed Hosting", "GoDaddy Cloud Network MAH", "Managed Hosting", "Internet/Unknown")
12 #Whitelisting dns lookups
13 | search NOT(dest_port = 53)
14 | stats dc(dest) as dest_ip_count dc(dest_port) as dest_port_count values(action) as action
values(dest_nsz) as dest_nsz values(src_nsz) as src_nsz values(dest_port) as dest_port count
min(_time) as firstTime max(_time) as lastTime by src
15 | eval dest_port = mvjoin(mvsort(dest_port), ", ")
16 | where (dest_ip_count > 200 AND dest_port_count > 2) OR (count > 2000)
```

Investigation Process

Step 1: Validate Involved Systems

Verify the operational status and accessibility of both the source and destination systems. Ensure that logging and monitoring tools are functioning correctly to support further investigation.

Step 2: Collect Supporting Data

Gather all relevant logs, telemetry, and contextual data that can aid in analyzing the suspicious activity. This includes firewall logs, system logs, and network flow data.

Step 3: Identify Source Process

On the source system, determine which specific process or application is initiating outbound connections to the destination IP addresses. Use appropriate diagnostic tools (e.g., netstat, lsof, ss, or system monitoring utilities) to trace the origin.

Step 4: Escalate Customer VPS Traffic

If the traffic originates from a customer VPS, Post a notification in the **#hoc-availability** channel. Include the VPS IP address and a sample of the observed malicious activity. Request that a netvio (network violation) be issued for further action.

Step 5: Assess IP Reputation

Validate the source IP address using “**AbuseIPDB**”. If the confidence score exceeds 50%, consider the IP for blocking in accordance with security policy.

Step 6: Escalate Non-Customer Traffic

If the traffic does not originate from a customer VPS, escalate the incident to the **#hosting-soc** channel. Provide all collected evidence and contextual information to support further investigation and response.

Template for requesting netvio

```
1 Netvio needed for VPS customer - malicious scanning activity
2
3 Customer VPS has been detected performing network scans against our non-hosting IP space and
shows <insert from abuseipdb result> confidence abuse score on AbuseIPDB, indicating
malicious behavior.
4 Account Details:
5 Shopper ID: [INSERT FROM CTK]
6 Domain/VPS: [INSERT DOMAIN/VPS IDENTIFIER]
7
8 Violation Summary: VPS customer engaging in unauthorized network scanning of GoDaddy
internal infrastructure and external networks. High abuse confidence score on AbuseIPDB
confirms malicious activity pattern.
9
10 Action Required:
11 Netvio issued against VPS
12
13 Suspension of VPS to prevent further network abuse Requesting netvio issuance and VPS
suspension due to network abuse
```

Common False Positives

This use case is expected to generate a high volume of true positive tickets, as customers typically have no legitimate need to perform scans on the production environment.

High Volume Data Exfiltration to Cloud Storage services

Table of contents

[Table of contents](#)

[Purpose](#)

[Analysis](#)

Purpose

| | |
|-----------------------|---|
| Responsible Team | <ul style="list-style-type: none">• Monitoring Team• SLACK: #internal-gcso• EMAIL: GCSO@godaddy.com |
| Process Owner | David Hernandez |
| Last Review Date | |
| Escalation Contact(s) | |
| Requests for Updates | |
| Training Log | |

Analysis

Few tips while handling alerts related to - "**High data volume upload to Third-Party Cloud Applications**"

There are two primary methods for uploading data to third-party cloud applications:

1. Via Application Interface
2. Via Web URL Interface

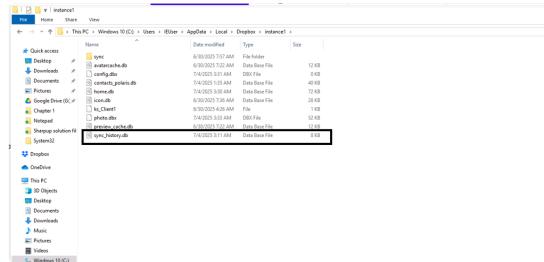
Identifying Data Exfiltration via Application Uploads:

When files are uploaded through a dedicated application, specific system artifacts can help identify potential data exfiltration. Below are key file upload artifacts associated with popular cloud storage applications:

Dropbox application artifacts:

Windows:

C:\Users\<username>\AppData\Local\Dropbox\instance\sync_history.db



C:\Users\<username>\AppData\Local\Dropbox\instance1\config.dbx(Contains the syncing email address)

MAC:

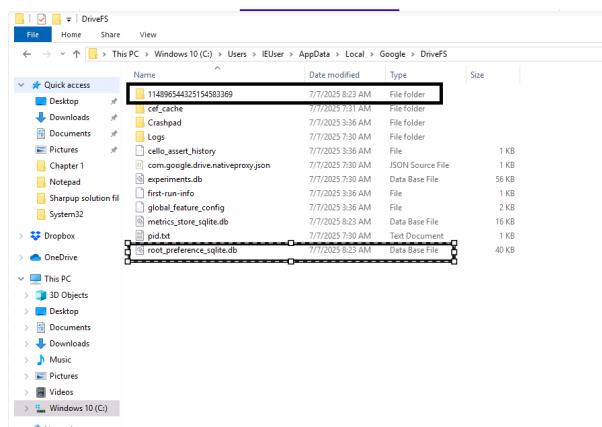
~/Library/Application Support/Dropbox/instance/sync_history.db

~/Library/Application Support/Dropbox/instance1/config.dbx(Contains the syncing email address)

Google-Drive application artifacts:

Windows:

C:\Users\IEUser\AppData\Local\Google\DriveFS\root_prerference_sqlite.db



C:\Users\IEUser\AppData\Local\Google\DriveFS\<RandomProfileID>\metadata_sqlite_db

| | Name | Date modified | Type | Size |
|----------------------|--|------------------|------------------|--------|
| Quick access | | | | |
| Desktop | content_cache | 7/7/2025 8:23 AM | File folder | |
| Downloads | local_folders | 7/7/2025 8:36 AM | File folder | |
| Documents | photos | 7/7/2025 8:23 AM | File folder | |
| Pictures | thumbnails_cache | 7/7/2025 8:23 AM | File folder | |
| Chapter 1 | account_settings | 7/7/2025 8:37 AM | File | 1 KB |
| Notepad | case_inensitivity | 7/7/2025 8:36 AM | File | 0 KB |
| Sharpup solution fil | cello_experiment_token | 7/7/2025 8:36 AM | File | 1 KB |
| System32 | cello_metrics_store_sqlite.db | 7/7/2025 8:23 AM | Data Base File | 24 KB |
| Dropbox | cello_server_token | 7/7/2025 8:36 AM | File | 1 KB |
| OneDrive | content_cache_file_created | 7/7/2025 8:36 AM | File | 0 KB |
| This PC | core_feature_config | 7/7/2025 8:36 AM | File | 4 KB |
| 3D Objects | enabled | 7/7/2025 8:36 AM | File | 0 KB |
| Desktop | experiment_token | 7/7/2025 8:36 AM | File | 1 KB |
| Documents | identifier | 7/7/2025 8:36 AM | File | 1 KB |
| Downloads | metadata.sqlite_db | 7/7/2025 8:23 AM | File | 844 KB |
| Music | metadata.sqlite_db_local_counter | 7/7/2025 8:36 AM | File | 12 KB |
| Pictures | metadata.sqlite_db_local_counter_mmap | 7/7/2025 8:36 AM | File | 1 KB |
| Videos | metadata_update_db | 7/7/2025 8:36 AM | File | 28 KB |
| Windows 10 (C) | metrics_store_sqlite.db | 7/7/2025 8:23 AM | Data Base File | 56 KB |
| Network | mirror_cello_metrics_store_sqlite.db | 7/7/2025 8:23 AM | Data Base File | 48 KB |
| | mirror_metadata_sqlite.db | 7/7/2025 8:23 AM | Data Base File | 968 KB |
| | mirror_metadata_sqlite_db_local_counter | 7/7/2025 8:36 AM | DB_LOCAL_COUN... | 12 KB |
| | mirror_metadata_sqlite_db_local_counter_mmap | 7/7/2025 8:36 AM | DB_LOCAL_COUN... | 1 KB |
| | mirror_metadata_update_db | 7/7/2025 8:36 AM | File | 28 KB |
| | mirror_sqlite.db | 7/7/2025 8:23 AM | Data Base File | 256 KB |
| | server_token | 7/7/2025 8:36 AM | File | 1 KB |
| | shortcuts_items_fetched | 7/7/2025 8:36 AM | File | 0 KB |

MAC:

/Users/<username>/Library/Application Support/Google/DriveFS/root_prerference_sqlite.db

Challenges with Web-Based Uploads:

When files are uploaded via a web browser (Web URL interface), it becomes more difficult to determine the exact files that were exfiltrated.

These uploads typically do not leave behind the same level of forensic artifacts as application-based uploads.

In this case we can check the uploads basis of timeframe in Splunk, whether there is only upload activity or any download activity also performed during same. In most of the cases, if user is downloading some huge data from any public url, so in response that domain will try to sync information like:

- File access logs
- Sync status
- Conflict resolution data

Basis of amount of data downloaded vs uploaded, we can take decision whether any suspicious data uploaded to that storage.

Splunk query to get data download details according to timeframe:

```

1 index=pan URLCategory="online-storage-and-backup" NOT(Application IN ("icloud-base", "ms-
onederive-base")) user=<username>
2 | fillnull value="" URL
3 | search NOT
4   [| inputlookup GoDaddy_IPs.csv
5     | stats count by prefix
6     | rename prefix as dest
7     | fields - count]

```

```

8
9 | eval gbytes_in = bytes_in / (1024.0 * 1024 * 1024)
10 | eval gbytes_out = bytes_out / (1024.0 * 1024 * 1024)
11 | stats count values(URL) as url values(action) as action values(Application) as application by _time user src dest gbytes_in gbytes_out
12
13

```

| _time | user | src | dest | gbytes_in | gbytes_out | count | un | action | application |
|-------------------------|------------|---------------|----------------|--------------|--------------|-------|----|---------|------------------|
| 2025-07-03 06:56:44.831 | jonaxfwang | 10.182.38.194 | 64.233.178.138 | 0.00003954 | 0.00025483 | 1 | | allowed | google-docs-base |
| 2025-07-03 06:55:47.789 | jonaxfwang | 10.182.38.194 | 47.113.23.100 | 0.000020145 | 0.000028043 | 1 | | allowed | ssl |
| 2025-07-03 06:55:47.789 | jonaxfwang | 10.182.38.194 | 47.113.23.100 | 0.000036972 | 0.000039194 | 1 | | allowed | ssl |
| 2025-07-03 07:00:53.481 | jonaxfwang | 10.182.38.194 | 120.24.174.2 | 0.0000065100 | 0.0000034578 | 1 | | allowed | ssl |
| 2025-07-03 07:00:55.942 | jonaxfwang | 10.182.38.194 | 47.113.23.100 | 0.0000075947 | 0.000007825 | 1 | | allowed | web-browsing |
| 2025-07-03 07:10:37.712 | jonaxfwang | 10.182.38.194 | 47.113.23.100 | 0.0000071032 | 0.0000041980 | 1 | | allowed | ssl |
| 2025-07-03 07:14:27.481 | jonaxfwang | 10.182.38.194 | 47.113.23.100 | 0.000085544 | 0.000022562 | 1 | | allowed | ssl |
| 2025-07-03 07:14:35.749 | jonaxfwang | 10.182.38.194 | 47.113.23.100 | 0.000025078 | 0.000041435 | 1 | | allowed | ssl |
| 2025-07-03 07:14:36.749 | jonaxfwang | 10.182.38.194 | 47.113.23.100 | 0.000030889 | 0.000039705 | 1 | | allowed | ssl |
| 2025-07-03 07:42:05.717 | jonaxfwang | 10.182.38.194 | 60.188.138.122 | 6.7727 | 0.28458 | 1 | | allowed | ssl |
| 2025-07-03 07:42:24.749 | jonaxfwang | 10.182.38.194 | 60.188.138.122 | 6.0122 | 0.29254 | 1 | | allowed | ssl |
| 2025-07-03 13:10:43.447 | jonaxfwang | 10.181.39.157 | 47.113.23.100 | 0.000010141 | 0.0000030799 | 1 | | allowed | ssl |
| 2025-07-03 13:11:13.140 | jonaxfwang | 10.181.39.157 | 47.113.23.100 | 0.000011054 | 0.0000031614 | 1 | | allowed | ssl |
| 2025-07-03 13:12:34.886 | jonaxfwang | 10.181.39.157 | 64.233.178.100 | 0.000011578 | 0.0000026496 | 1 | | allowed | google-docs-base |
| 2025-07-03 13:12:34.886 | jonaxfwang | 10.181.39.157 | 64.233.178.138 | 0.000012972 | 0.0000028135 | 1 | | allowed | google-docs-base |

During such cases, If you need further assistance please reach-out to #insider threat detection team for help. (edited)

How to upload Proofpoint Trap logs to Splunk

Table of contents

- [Table of contents](#)
- [Purpose](#)
- [Description](#)
- [Exporting incident and audit logs in PP](#)
 - [Incidents logs](#)
 - [Go to Audit logs](#)
- [Upload logs into Splunk](#)
 - Upload the logs to Splunk index="proofpoint_trap" or index="proofpoint_trap_dev" to practice the process.
- [Splunk Query](#)

Purpose

| | |
|-----------------------|--|
| Responsible Team | <ul style="list-style-type: none">• Detections• SLACK: #demo-internal• EMAIL: detectmon@godaddy.com |
| Process Owner | |
| Last Review Date | |
| Escalation Contact(s) | @secmon |
| Requests for Updates | |
| Training Log | |

Description

This playbook serves as a guide for uploading Proofpoint logs to Splunk, starting with the export of incident and audit logs and concluding with adding the data to the `index=proofpoint_trap`.

Exporting incident and audit logs in PP

Incidents logs

Go to TRAP - Incidents

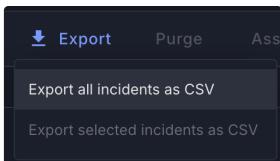
The screenshot shows the Proofpoint Threat Response web interface. The URL in the browser bar is `threatresponse.proofpoint.com/incidents`. On the left, there's a sidebar with a bell icon and two main categories: 'Incidents & Messages' and 'Messages'. Under 'Incidents & Messages', the 'Incidents' link is highlighted with a red box. Below the sidebar, the main content area says 'Select All'.

Filter

This screenshot shows the 'Filters' modal dialog. It has two main sections: 'Incident Attributes' and 'Message Attributes'. In the 'Incident Attributes' section, several filters are applied, each highlighted with a red box: 'User' (dropdown), 'Team (1) GCSO' (dropdown), 'Priority' (dropdown), 'Incident ID' (dropdown), 'Incident State Closed' (dropdown), 'Incidents Created In Custom' (dropdown), and a date range from 'Start: 2025/03/01 13:56:04' to 'End: 2025/08/31 13:56:04'. There's also a 'VAP' toggle switch. In the 'Message Attributes' section, four dropdowns are shown: 'Source', 'Message Disposition', 'CLEAR Confidence', and 'CLEAR Verdict'. At the bottom of the dialog are three buttons: 'Cancel', 'Clear All', and 'Apply'.

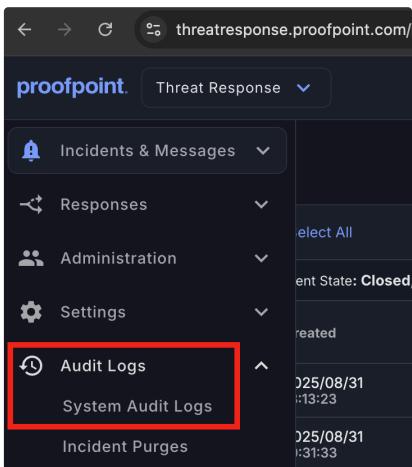
Export the logs to a csv file

This screenshot shows the 'Incidents' list page. The URL in the browser bar is `threatresponse.proofpoint.com/incidents`. The main content area displays '1-500 of 1265 Incidents' and a 'Select All' button. At the top right, there are 'Refresh' and 'Export' buttons, with the 'Export' button highlighted with a red box. A status bar at the bottom of the list area says 'Assigned Team: GCSO, Incident State: Closed, Incidents Created In: 2025/03/01 13:56:04 - 2025/09/01 00:00:00'.

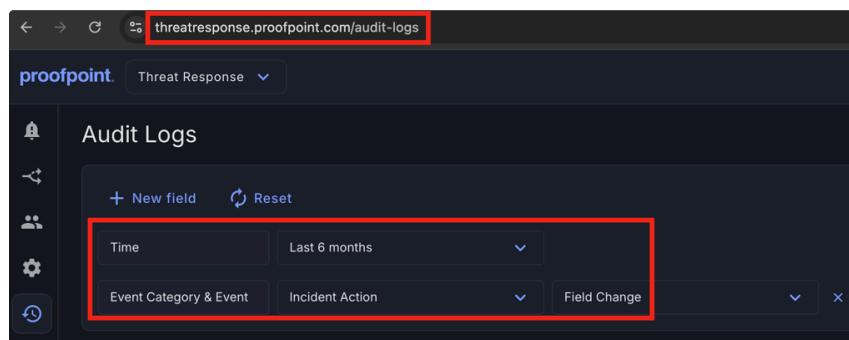


incidents_*.csv

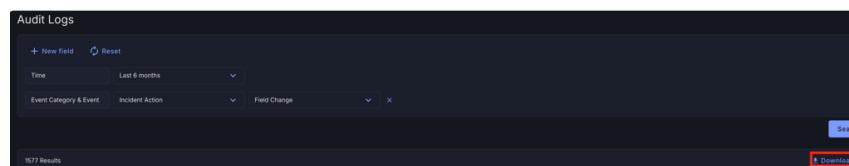
Go to Audit logs



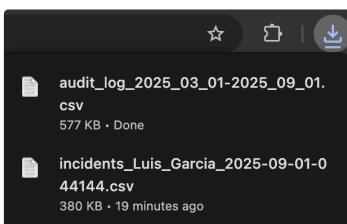
Filter



Export the csv file

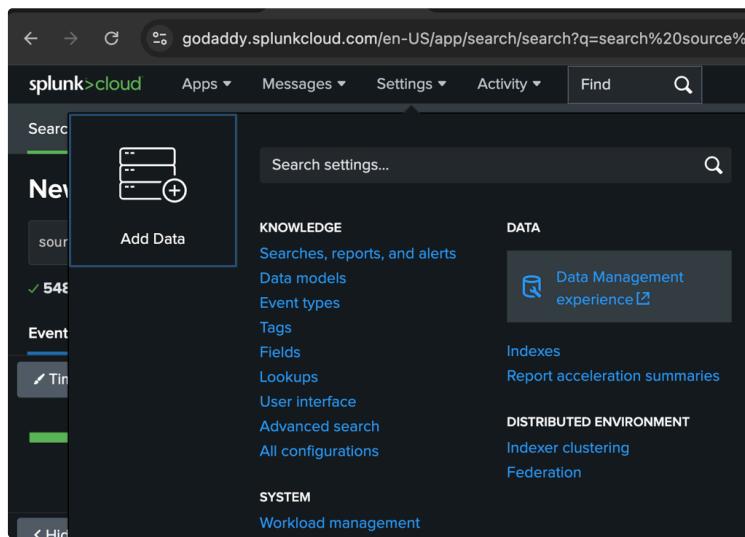


audit_*.csv



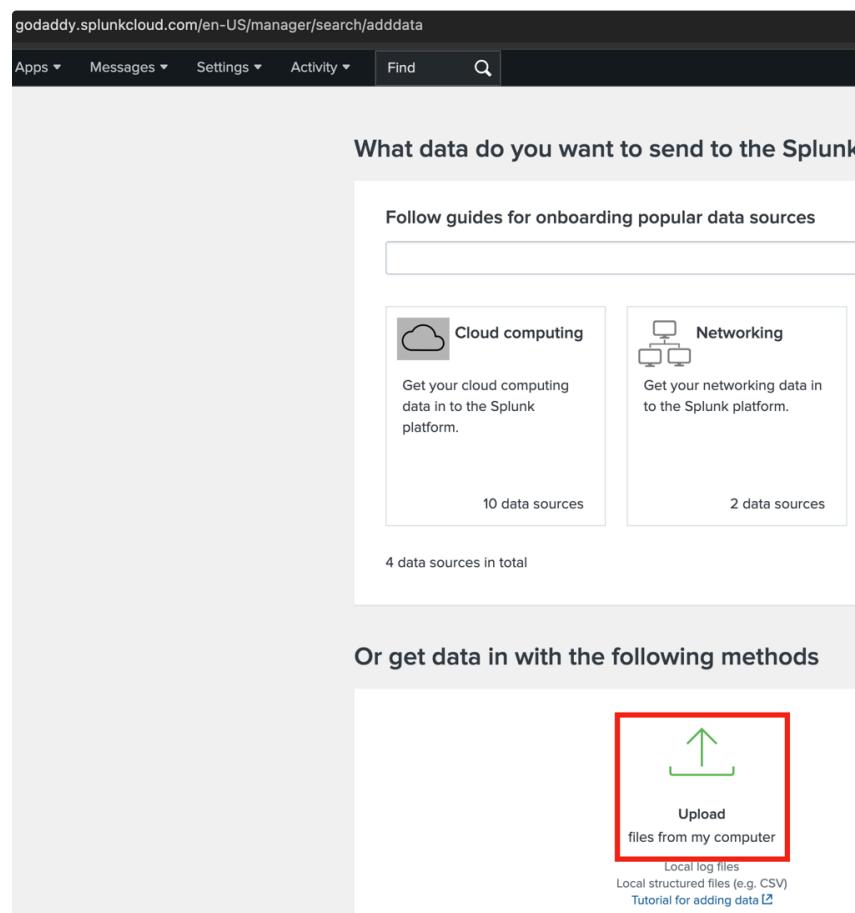
Upload logs into Splunk

Upload the logs to Splunk index="proofpoint_trap" or index="proofpoint_trap_dev" to practice the process.



The screenshot shows the Splunk Cloud search interface. The top navigation bar includes links for 'splunk>cloud', 'Apps', 'Messages', 'Settings', 'Activity', 'Find', and a search bar. On the left, there's a sidebar with sections for 'Search', 'New', 'Event', and 'System'. Under 'Event', there are several sub-options like 'Sources', 'Logs', 'Metrics', and 'Audit'. A prominent blue button labeled 'Add Data' is located in the center of the interface. The main content area has sections for 'KNOWLEDGE', 'DATA', 'DISTRIBUTED ENVIRONMENT', and 'SYSTEM', each with various sub-links.

Click on upload



The screenshot shows the 'godaddy.splunkcloud.com/en-US/manager/search/adddata' page. The top navigation bar is identical to the previous screenshot. The main content area is titled 'What data do you want to send to the Splunk?' and features a section titled 'Follow guides for onboarding popular data sources'. Below this are two cards: 'Cloud computing' (10 data sources) and 'Networking' (2 data sources). A note at the bottom states '4 data sources in total'. Further down, a section titled 'Or get data in with the following methods' includes a card for 'Upload files from my computer', which is highlighted with a red box. Other options listed include 'Local log files', 'Local structured files (e.g. CSV)', and a 'Tutorial for adding data' link.

Select the audit or incidents file

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn more](#)

Selected File: **audit_log_2025_09_01.csv**

Select File

Set Source Type

This page lets you see how the Splunk platform saves your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **audit_log_2025_09_01.csv**

| | time | Customer Id # | Date # | Email Address # | Entity Name # | Event # | Event Category # | Event Details # | Event Guid # |
|---|---------------------|-------------------------------------|---------------------------------|----------------------|---------------|-----------------------|------------------|--|-------------------------------------|
| 1 | 9/25 4:52:00:63 PM | a#0554b-4606-3a9b-9829-44290ae03f9e | 2025-09-01T16:52:00.633668-0000 | hharidas@godaddy.com | incident | incident_field_change | incident | ID: INC-34865, changed fields: [] | 7384-e02-9b31-4f5-1b92-20c4d474c2d8 |
| 2 | 9/25 4:51:47:819 PM | a#0554b-4606-3a9b-9829-44290ae03f9e | 2025-09-01T16:51:47:819761-0000 | hharidas@godaddy.com | incident | incident_field_change | incident | ID: INC-34865, changed fields: [(updatedate)(2025-09-01 12:42:20.005686, 2025-09-01 16:51:47:79877), date_index, record] | Q1956ea-e02c-43b0-9fc-9003ax32ff830 |

Select the index to upload the data

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Constant value

Regular expression on path

Segment in path

Host field value: **sh-l-0c00a2cc7098f45b0.godaddy.sp**

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index: **proofpoint_trap**

Review the upload details

Add Data

Review

Input Type Uploaded File
 File Name audit_log_2025_03_01-2025_09_01.csv
 Source Type csv
 Host sh-i-0c00a2cc7098f45b0.godaddy.splunkcloud.com
 Index proofpoint_trap

Splunk Query

```

1 index=proofpoint_trap source="incidents_*.csv"
2 | eval incident_id='Incident Id'
3 | eval created_time=strptime(Created, "%Y-%m-%d %H:%M:%S.%f")
4 | eval closed_time=strptime(Closed, "%Y-%m-%d %H:%M:%S.%f")
5 | fields incident_id created_time closed_time
6 | where isnotnull(created_time)
7 | append [
8     search index=proofpoint_trap source="audit_log_*.csv"
9     | eval incident_id=replace('Event Details', ".*ID\\\$*:\\\$*INC-
(\$\d+).*", "\$1")
10    | where NOT match('Event Details', "State=\$\$(open, closed\$\$)")
11    | where NOT match('Event Details', "changed fields: \$\{\\\$\\}")
12    | eval updated_start=_time
13    | fields incident_id updated_start
14 ]
15 | stats min(created_time) as created_time, min(updated_start) as
updated_start, min(closed_time) as closed_time by incident_id
16 | where isnotnull(created_time) AND isnotnull(updated_start) AND
isnotnull(closed_time)
17 | eval time_to_response_min = round((updated_start - created_time) /
60, 2)
18 | eval time_to_close_min = round((closed_time - created_time) / 60, 2)
19 | table incident_id created_time updated_start closed_time
time_to_response_min time_to_close_min
20 | stats avg(time_to_response_min),avg(time_to_close_min)

```