

# Managing Cases in Google SecOps

Using Case Management in Security Operations

---

September 2024

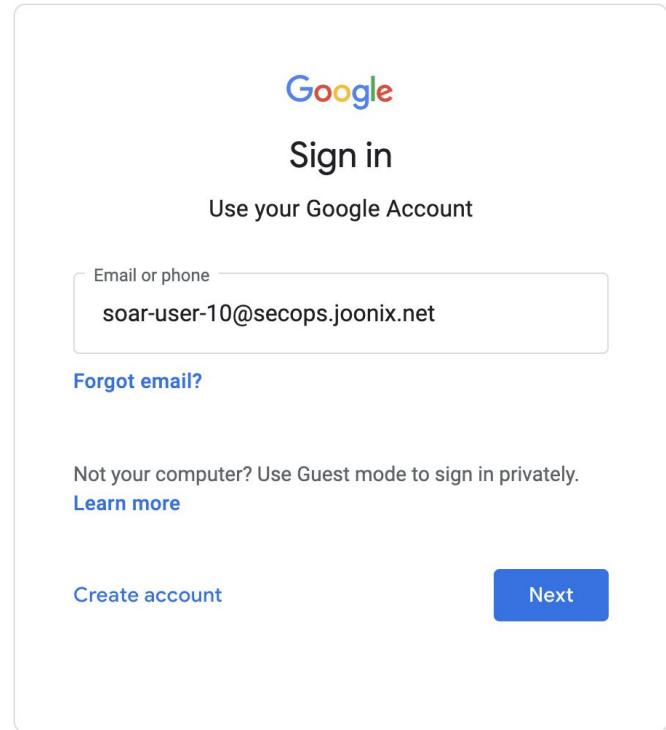


# Agenda

- SecOps Primer
- Case Management Familiarization
- Your Workdesk
- Manual Actions
- Exercise

# Login Instructions (1)

- 1) Open a new Incognito Window in your Chrome Browser
- 2) Navigate to the Google SecOps instance URL:  
**<https://goo.gle/secops-workshop>**
- 3) Use the account assigned to you by your instructor that uses Google Workspace as Identity Provider



The image shows a screenshot of the Google Sign-in page. At the top right, it says "Sign in" and "Use your Google Account". Below that is a text input field labeled "Email or phone" containing "soar-user-10@secops.joonix.net". To the left of the input field is a link "Forgot email?". Below the input field, there is a note "Not your computer? Use Guest mode to sign in privately." followed by a link "Learn more". At the bottom left is a link "Create account" and at the bottom right is a blue button labeled "Next".



## Login Instructions (2)

4) If you get “Verify It’s you” screen, click on “Confirm your recovery email” option

Google

### Verify it's you

To help keep your account safe, Google wants to make sure it's really you trying to sign in

[Learn more](#)

[soar-user-10@secops.joonix.net](#) ▾

Choose how you want to sign in:

- Get a verification code at [soa\\*\\*\\*\\*\\*@se\\*\\*\\*\\*\\*.net](#)
- Use another phone or computer to finish signing in
- Confirm your recovery email
- Get help

5) Type “[soarworkshop-instructor@secops.joonix.net](#)” as the recovery email and click Next

Google

### Verify it's you

To help keep your account safe, Google wants to make sure it's really you trying to sign in

[Learn more](#)

[soar-user-10@secops.joonix.net](#) ▾

Confirm the recovery email address you added to your account: [soa\\*\\*\\*\\*\\*@se\\*\\*\\*\\*\\*.net](#)

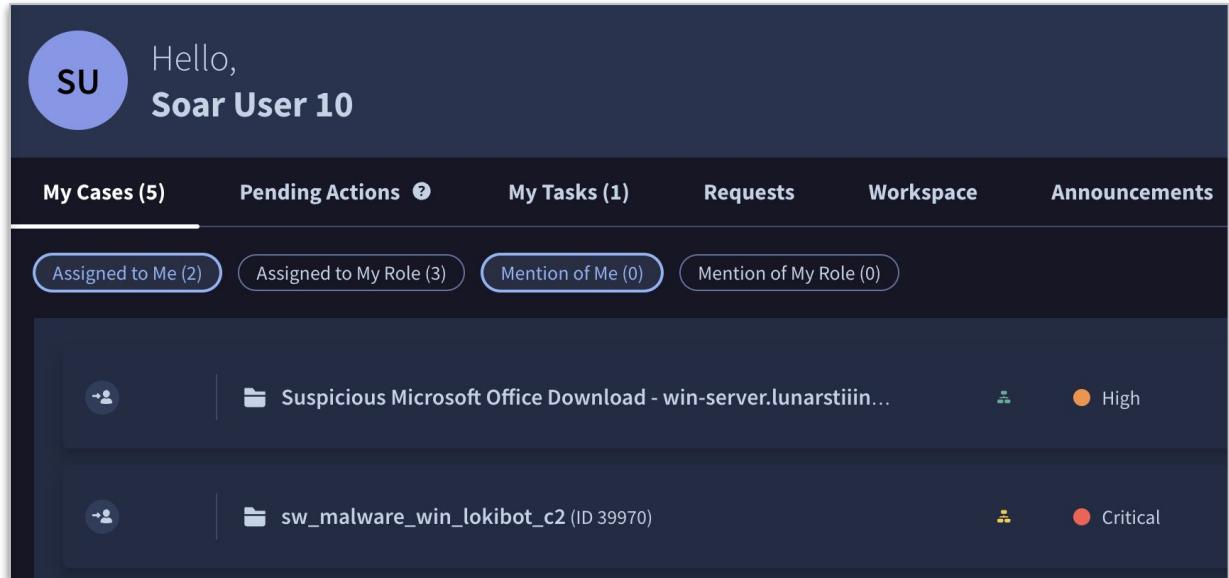
Enter recovery email address

[Try another way](#) [Next](#)

# Login Instructions (3)

6) We are now logged into Google SecOps with a view similar to this

7) Open a new tab in the same Incognito Window and navigate to <https://gmail.com/> which we will use during the workshop



The screenshot shows the Soar User 10 dashboard. At the top, it says "Hello, Soar User 10". Below that is a navigation bar with tabs: "My Cases (5)" (which is active), "Pending Actions 0", "My Tasks (1)", "Requests", "Workspace", and "Announcements". Under the "My Cases" tab, there are five cards representing different cases. The first card is titled "Suspicious Microsoft Office Download - win-server.lunarstiin..." and has a "High" priority indicator. The second card is titled "sw\_malware\_win\_lokibot\_c2 (ID 39970)" and has a "Critical" priority indicator.

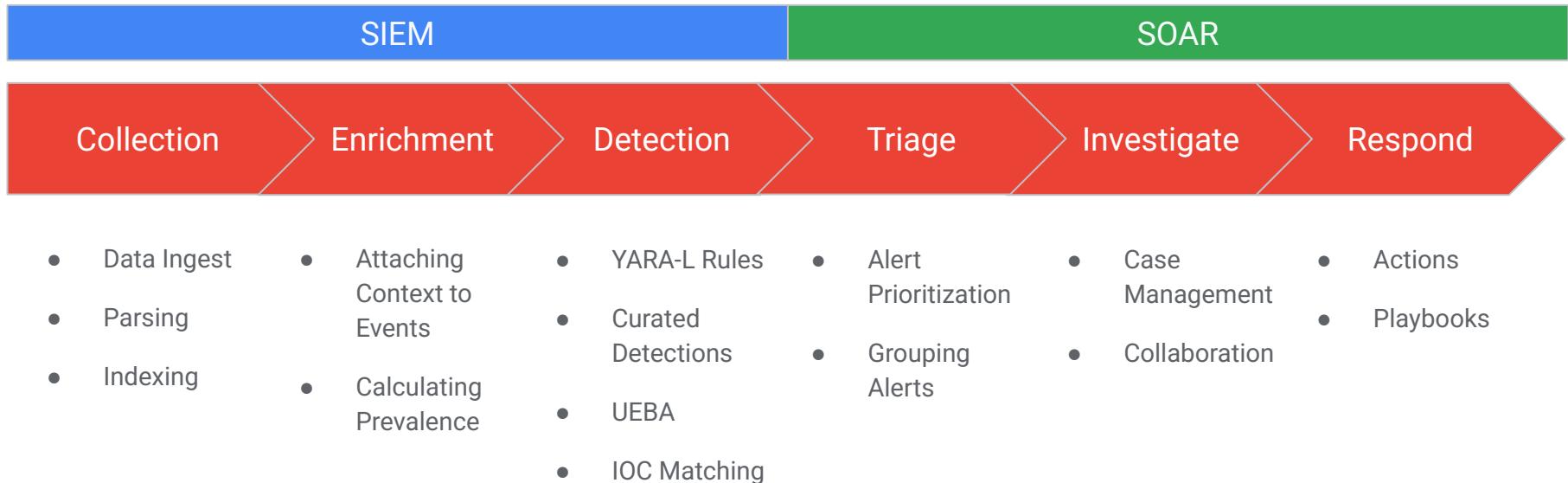


Google SecOps

# SecOps Primer



# Google Security Operations Platform





# Orchestration and Automation in SecOps

SecOps is not just using a SIEM, but bringing automation and orchestration to streamline response





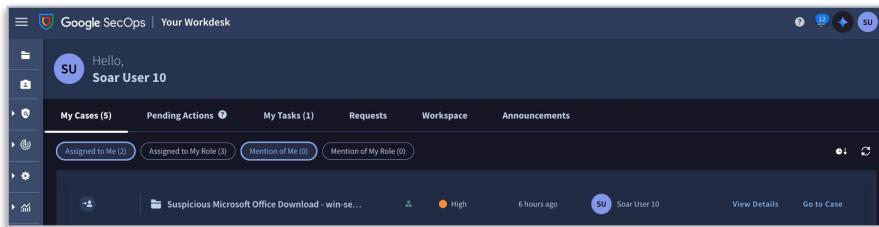
# Terminology

- **Alerts** : Detections generated by rules and made up of events
- **Case** : A collection of one or more alerts grouped by common values and time
- **Entity** : Objects of interest in an alert
  - Examples include hostname, username, filehash, domain, ip address, process name and more
- **Integration** : Third party solutions that Secops can send or receive API calls from
- **Action** : Part of integrations. Used for specific API calls with third parties
- **Connector** : Responsible for alert ingestion
- **Job** : Acts as a scheduler and allows for a health check sync
- **Playbook** : Workflow of action blocks executed following a trigger
  - **Trigger** : Mandatory block that starts a playbook

# Case Management Workflow

Different approaches

Workdesk



< not exclusive approaches >

Cases



Analysts are interacting with cases assigned to them, and pending actions :

- [+] well structured and organized SOC team
- [+] better priority management
- [-] requires higher maturity to structure the SOC Team
- [-] lack of visibility to other cases

Analysts are interacting within the global cases list :

- [+] broad view of all cases
- [+] doesn't require additional configuration to structure the processes
- [-] the analyst doesn't see immediately the actions that are pending



# Familiarization with Case Management



## Case List

Google SecOps | Cases

5 Cases

Click 1

Search Case Name

Click 2

Case ID	Case Description	Severity	Type
W1	Suspicious Microsoft Office Download - win-server.lunarstiiness.com	3	SU
W1	wmic_ntds_dit_T1003_003_cisa_report	4	T1
W1	recon_environment_enumeration_active_directory_cisa_report	1	T1
W1	recon_suspicious_commands_cisa_report	1	T1
W1	sw_malware_win_lokibot_c2	1	SU

# Case Overview

**sw\_malware\_win\_lokibot\_c2**

ID 4064    Workshop 10    Triage    2023-11-27 06:24:45

SU Soar User 10

[Manage Tags](#)

[Explore](#)

**1. SW\_MALWARE\_WIN\_L...** (1) •  
2023-11-27 05:48:40

**Overview** ?

**Case Description** ?

Click here to add description

**Pending actions (1)** ?

Failed Pending

**Endpoint investigation ?** Critical SU 9 hours ago The external entities (domain and URL) are suspicious. Request a full... [View Playbook](#) [Respond](#)

**Alerts (1)** ?

#	Alert Name	Time	Events	Priority	Playbook Attached	Alert SLA	Status
1	SW_MALWARE_WIN_L...	2023-11-27 05:48:40	1	Critical	Case Manageme...	N/A	Open

[View details](#)



Google

# Case Overview



# Google SecOps

**sw\_malware\_win\_lokibot\_c2**

ID 4064    Workshop 10    Triage    2023-11-27 06:24:45    SU Soar User 10

Manage Tags

**M Mandiant** Expand

 ALPHASTAND.WIN

**Score: 94**

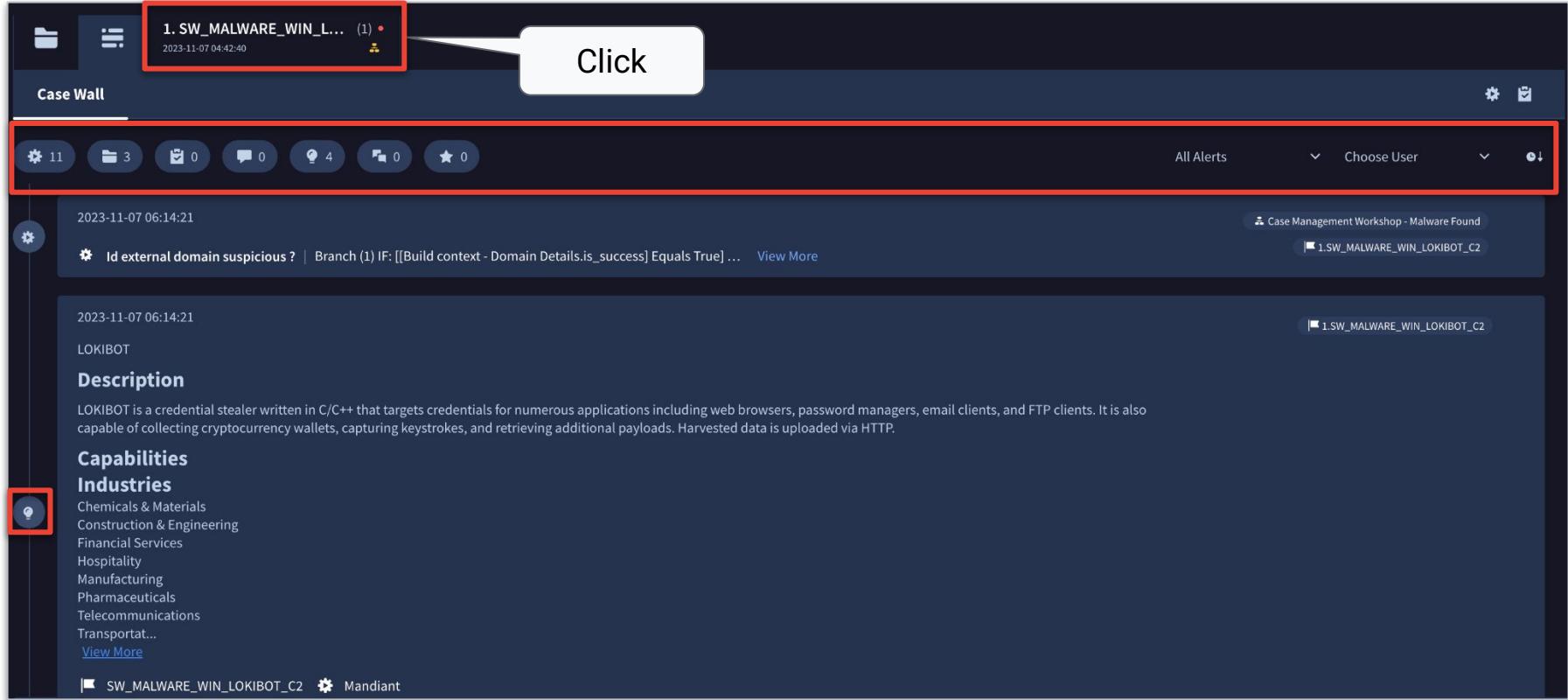
First Seen: 2013-05-04T10:00:45.000Z  
Last Seen: 2023-11-27T04:08:47.000Z  
Sources: sebsauvage,ookangzheng,imperium\_ra8,Mandiant  
For more details visit the following link:  
<https://advantage.mandiant.com/indicator/fqdn/alphastand.win>

**Entities Highlights (7)** ⓘ

 10.128.0.21	<a href="#">Explore</a>	<a href="#">View details</a>	<a href="#">⚙️</a>
Network Name    Network Address			
Lunars-Internal    10.128.0.0/24			
 WIN-ADFS.LUNARSTIIINESS.COM	<a href="#">Explore</a>	<a href="#">View details</a>	<a href="#">⚙️</a>
 185.189.112.157	<a href="#">Explore</a>	<a href="#">View details</a>	<a href="#">⚙️</a>
 HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1071/001/	<a href="#">View details</a>	<a href="#">⚙️</a>	
 HTTP://ALPHASTAND.WIN/ALIEN/FRE.PHP	<a href="#">View details</a>	<a href="#">⚙️</a>	
 ALPHASTAND.WIN	<a href="#">Explore</a>	<a href="#">View details</a>	<a href="#">⚙️</a>

Google

# Case Wall - Audit Trail



1. SW\_MALWARE\_WIN\_L... (1) •  
2023-11-07 04:42:40

Click

Case Wall

All Alerts Choose User

11 3 0 4 0 0

2023-11-07 06:14:21

\* Id external domain suspicious ? | Branch (1) IF: [[Build context - Domain Details.is\_success] Equals True] ... View More

Case Management Workshop - Malware Found  
1.SW\_MALWARE\_WIN\_LOKIBOT\_C2

2023-11-07 06:14:21

LOKIBOT

**Description**

LOKIBOT is a credential stealer written in C/C++ that targets credentials for numerous applications including web browsers, password managers, email clients, and FTP clients. It is also capable of collecting cryptocurrency wallets, capturing keystrokes, and retrieving additional payloads. Harvested data is uploaded via HTTP.

**Capabilities**

**Industries**

Chemicals & Materials  
Construction & Engineering  
Financial Services  
Hospitality  
Manufacturing  
Pharmaceuticals  
Telecommunications  
Transportat...  
[View More](#)

SW\_MALWARE\_WIN\_LOKIBOT\_C2    Mandiant



# Alert Overview

Click

Events (1)  

Alert Details (4)

Alert name	Product	Start Time	End Time
SW_MALWARE_WIN_LOKIBOT_C2	RULE	2023-11-27 05:48:40 UTC+00	2023-11-27 05:48:40 UTC+00

Pending Actions (1) ⓘ

Status	Action	Last Update	Details	View Playbook	Respond
Failed	Endpoint investigation ?	SU 10 hours ago	The external entities (domain and URL) are suspicious. Request a full investigation of the...	<a href="#">View Playbook</a>	<a href="#">Respond</a>

Events Table (1) ⓘ

metadata.event_type	metadata.vendor_name	ingested_timestamp	principal.ip	principal.userid
NETWORK_HTTP	Zscaler	2023-11-27T06:06:03.194677Z	IP 10.128.0.21	PHIL.ALDWIN



## Alert - Event View

sw\_malware\_win\_lokibot\_c2

ID 39362 Workshop 29 Triage September 06, 2024 06:25:33 Soar User 29

Manage Tags

1. SW\_MALWARE\_WIN\_LOKIBO... (1) • September 06, 2024 04:28:45

Overview Events (1) Playbooks (1) Graph

NAME	TYPE	SOURCE / PRODUCT	ARTIFACTS	PORT	OUTCOME	TIME
NETWORK_HTTP	NETWORK_HTTP	RULE	HTTP://ALPHASTAND.WIN/ALIE...			September 06, 2024 04:28:45

Click



# Alert - Event/Detection Details

The screenshot shows a security alert interface with the following details:

**Alert Summary:**  
1. SW\_MALWARE\_WIN\_LOKIBO... (1) •  
September 06, 2024 04:28:45

**Navigation:** Overview, Events (1), **Playbooks (1)**, Graph, Settings, More

**Event Details:**  
NAME: NETWORK\_HTTP  
TYPE: NETWORK\_HTTP  
SOURCE / PRODUCT: RULE  
ARTIFACTS: HTTP://ALPHA...  
OUTCOME: Pending  
TIME: September 06, 2024 04:28:45

A callout bubble with the text "Click" points to the "Playbooks (1)" tab.

**Playbook Configuration (Details View):**

**Playbook Name:** NETWORK\_HTTP

**Default Action:**

Field Name	Value
event_metadata_productId	2230936060833153955
event_metadata_eventTimestamp	2024-09-06T03:28:45Z
event_metadata_eventType	<b>NETWORK_HTTP</b>
event_metadata_vendorName	Zscaler
event_metadata_productName	NSS
event_metadata_ingestedTimestamp	2024-09-06T05:06:07.053482Z
event_metadata_id	AAAAABCLMjnc8eYfS9KC6C074oAAAAABQ...
event_metadata_logType	ZSCALER_WEBPROXY
event_metadata_baseLabels_logTypes_1	ZSCALER_WEBPROXY
event_metadata_baseLabels_allowScope...	True
event_metadata_enrichmentLabels_logT...	WINDOWS_AD

A red box highlights the "event\_metadata\_eventType" field value "NETWORK\_HTTP". A red arrow points from the highlighted field to the bottom right corner of the details panel.



# Alert Playbook Status

Chronicle | Cases

## sw\_malware\_win\_lokibot\_c2

ID 4064 Workshop 10 Triage 2023-11-27 06:24:45

Manage Tags

Click 2

1. Click on the Graph tab.

2. Click on the purple node in the graph.

Playbooks (1)

Graph

Playbooks (1)

Case Management Workshop...

Click

Graph

Write a comment...

Endpoint investigation ? 2023-11-08 15:48:50

Message to Assignee

The external entities (domain and URL) are suspicious. Request a full investigation of the endpoint ?

Target Entities

- WIN-ADFS.LUNARSTIINESS.COM
- IP 10.128.0.21
- PHIL.ALDWIN
- IP 185.189.112.157
- URL HTTP://ALPHASTAND.WIN/ALIEN/FRE.PHP
- URL HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1071/001/
- ALPHASTAND.WIN

Action Parameters

The external entities (domain and URL) are suspicious. Do you want to request a full investigation of the endpoint ?

Yes

No

No but inform the End User

Done

Close

# Alert - Graph

**Click**

**Overview**  Events (1) Playbooks (1) **Graph**   

**Graph Summary**

**SW\_MALWARE\_WIN\_LOKIBOT\_C2**

- Status: Open
- Severity: Critical
- Priority: Critical
- Risk Score: 90 **ALERT RISK - HIGH**
- Detected: 2023-11-07T05:42:40.000
- Created: 2023-11-07T07:00:29.761
- Last Updated: 2023-11-07T07:14:13.047
- Rule: [sw\\_malware\\_win\\_lokibot\\_c2](#)
- Description: Identify default Lokibot C2 Traffic

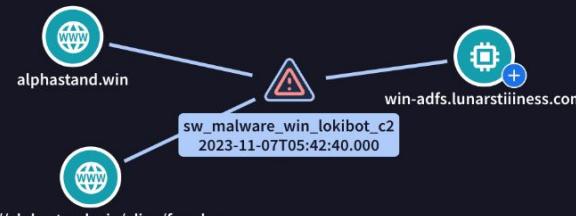
**HTTP://ALPHASTAND.WIN/ALIEN/FRE.PHP**

**ALPHASTAND.WIN**

- Domain name: alphastand.win
- First time seen: 2023-11-03T03:52:41.000
- Last time seen: 2023-11-07T05:42:40.000
- Creation time: 2023-01-10T16:52:21.000
- Expiration time: 2024-01-10T16:52:21.000

**GRAPH**

GRAPH OPTIONS | RESET LAYOUT | NOVEMBER 06, 05:42 PM - NOVEMBER 07, 05:42 PM



The graph visualization shows three entities connected to a central alert node. The entities are represented by icons: a globe for alphastand.win, a gear for win-adfs.lunarstiiness.com, and a warning triangle for the alert itself. The alert node contains the text "sw\_malware\_win\_lokibot\_c2" and the timestamp "2023-11-07T05:42:40.000". Below the graph, there is a table of events.

EVENTS	ENTITIES	ALERT CONTEXT		
<b>EVENTS</b>	 Search events...	 WRAP TEXT  COLUMNS 		
TIMESTAMP	EVENT	USER	HOSTNAME	PROCESS NAME
2023-11-07T05:42:40.000	<b>NETWORK_HTTP</b> phil.aldrin to alphastand.win	phil.aldrin	win-adfs.lunarstiiness.com	[Unknown]



Google SecOps

# Entity Highlights - Case and Alerts

sw\_malware\_win\_lokibot\_c2

ID 4064 Workshop 10 Triage 2023-11-27 06:24:45 Soar User 10

Manage Tags

Entities Highlights (7) ⓘ

IP 10.128.0.21 Network Name LunarS-Internal Network Address 10.128.0.0/24	Explore View details ⚙️	IP WIN-ADFS.LUNARSTIIINESS.COM	Explore View details ⚙️
PHIL.ALDRIN	Explore View details ⚙️	IP 185.189.112.157	Explore View details ⚙️
URL HTTP://ALPHASTAND.WIN/ALIEN/FRE.PHP	View details ⚙️	URL HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1071/001/	View details ⚙️
ALPHASTAND.WIN	Explore View details ⚙️		

Click



# User Overview, Events and Alerts

SEARCH i New Features Go to Legacy search ⋮ ^

Enter any question here, for example "Find externally shared documents with confidential in the title"

Generate Query

1 principal.user.userid = "phil.aldrin" OR target.user.userid = "phil.aldrin"

History UDM Lookup Lists Generated Query ! ! Rewrite Case Sensitivity Off AUGUST 30, 03:31 PM - SEPTEMBER 06, 03:31 PM Run Search ⋮

OVERVIEW EVENTS (7) ALERTS (7)

Trend over time Prevalence

ADD FILTER CLEAR APPLY TO SEARCH AND RUN

AGGREGATIONS

Search fields or values...

GROUPED FIELDS ?

Click

EVENTS	PIVOT	Search events...	WRAP TEXT	COLUMNS	⋮
TIMESTAMP	EVENT	USER	HOSTNAME	PROCESS NAME	⋮
2024-09-06T03:28:45.000	<span>! ALERT</span> NETWORK_HTTP phil.aldrin to alphastand.win	phil.aldrin	win-adfs.lunarstiiness.com	[Unknown]	⋮



# Entity Highlights - Case and Alerts

sw\_malware\_win\_lokibot\_c2

ID 4064 Workshop 10 Triage 2023-11-27 06:24:45 Soar User 10

Manage Tags

Entities Highlights (7) ⓘ

IP 10.128.0.21	Explore ⓘ	View details	⚙️
Network Name LunarS-Internal Network Address 10.128.0.0/24			
PHIL.ALDRIN	Explore ⓘ	View details	⚙️
URL HTTP://ALPHASTAND.WIN/ALIEN/FRE.PHP	Explore ⓘ	View details	⚙️
ALPHASTAND.WIN	Explore ⓘ	View details	⚙️
WIN-ADFS.LUNARSTIIINESS.COM	Explore ⓘ	View details	⚙️
IP 185.189.112.157	Explore ⓘ	View details	⚙️
URL HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1071/001/	View details	⚙️	



# Entity Explorer

Chronicle | Entity Explorer - PHIL.ALDRIN

PHIL.ALDRIN This entity was involved in **27** cases during the last 3 months **1** Malicious Cases

Entity Details

Field Name	Value
Type	USERUNIQNAME
Environment	Workshop 10
OriginalIdentifier	phil.aldrin
IsInternalAsset	False
IsSuspicious	False
IsEnriched	False
IsVulnerable	False
IsArtifact	False

Last Cases (27)

sw_malware_win_lokibot_c2	2023-11-08 17:01:22 ID 1609	Closed - External attack, MALICIOUS
sw_malware_win_lokibot_c2	2023-11-27 06:24:44 ID 4064	
sw_malware_win_lokibot_c2	2023-11-26 06:26:48 ID 3983	Closed - Other, NOT_MALICIOUS
sw_malware_win_lokibot_c2	2023-11-25 06:20:18 ID 3870	Closed - Other, NOT_MALICIOUS

Entity Log

Linked Entities (5)

- WIN-ADFS
- 10.128.0.21
- ::1
- HTTP://ALPHASTAND.WIN/ALIEN/FRE.PHP
- HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1071/001/

Case Distribution

Product	Count
RULE	51

Add Comment



# Exercise: Exploring Our Case Further

With a better understanding of how cases and alerts are displayed in Google SecOps, let's further explore this case to answer the following questions

Based on the VirusTotal Insights in the Case Overview tab:

- What does Sophos classify the URL as?
- When was the domain alphastand.win created?

Within the alert, what is the http user agent for the event that triggered the alert?

Pivoting to an IP specific view, is the external IP address in the Entities Highlights section communicating with other systems in our environment?

Are there any specific entities in the highlights that jumped out and make you want to look into them further?

# What does Sophos Classify the URL as?

**sw\_malware\_win\_lokibot\_c2**

ID 4064    Workshop 10    Triage    2023-11-27 06:24:45

[Manage Tags](#)

[Insights](#)

**M Mandiant** [Expand](#)

**LOKIBOT**

**Description**  
LOKIBOT is a credential stealer written in C/C++ that targets credentials for numerous applications including web browsers, password managers, email clients, and FTP clients. It is also capable of collecting cryptocurrency wallets, capturing keystrokes, and retrieving additional payloads. Harvested data is uploaded via HTTP.

**Capabilities**

**Industries**  
Chemicals & Materials  
Construction & Engineering  
Financial Services  
Hospitality  
Manufacturing  
Pharmaceuticals  
Telecommunications  
Transportation

**Details**  
Aliases: Mosaicloader (Bitdefender), Purecrypter (ZScaler)  
Last Activity Time: 2023-11-08T20:00:27.820Z  
For more details visit the following link:  
<https://advantage.mandiant.com/malware/malware--bcdca978-5419-5d22-a424-786367cf6e3c>

**VirusTotalV3** [Expand](#)

**URL** <HTTP://ALPHASTAND.WIN/ALIEN/FRE.PHP>

**Detected: 18Threshold: 4**

Title:	404 - File or directory not found.
Status Code:	200
Content Length:	1245
Dr.Web:	known infection source
Forcepoint ThreatSeeker:	bot networks. compromised websites
Sophos:	command and control
Xcitium Verdict Cloud:	unknown

**More Info:**  
<https://www.virustotal.com/gui/url/aHR0cDovL2FscGhhc3RhbmQu2luL2FsaWVuL2ZyZS5waHA/detection>

**VirusTotalV3** [Expand](#)

**URL** <HTTP://ALPHASTAND.WIN/ALIEN/FRE.PHP>

**Detected: 18Threshold: 4**

Title:	404 - File or directory not found.
Status Code:	200
Content Length:	1245
Dr.Web:	known infection source
Forcepoint ThreatSeeker:	bot networks. compromised websites
Sophos:	command and control
Xcitium Verdict Cloud:	professional networking
Webroot:	Bot Nets
Reputation:	-81
Voted as malicious:	8 times

**More Info:**  
<https://www.virustotal.com/gui/url/aHR0cDovL2FscGhhc3RhbmQu2luL2FsaWVuL2ZyZS5waHA/detection>

NS 300 ns4.alphastand.win

Whois

Google

# When was the domain alphastand.win created?



Google SecOps

Insights ⓘ

**M Mandiant**

**LOKIBOT**

**Description**  
LOKIBOT is a credential stealer that targets numerous applications, including email clients, and File Transfer Protocol (FTP) cryptocurrency wallets. Harvested credentials are used to compromise other systems.

**Capabilities**

**Industries**  
Chemicals & Materials  
Construction & Engineering  
Financial Services  
Hospitality  
Manufacturing  
Pharmaceuticals  
Telecommunications  
Transportation

**Details**  
**Aliases:** Mosaicloader  
**Last Activity Time:** 2023-01-10 00:00:00  
For more details visit <https://advantage.mandiant.com/5d22-a424-786367cf8>

**VirusTotalV3** Expand

**ALPHASTAND.WIN**  
Detected: 19 Threshold: 1

**Reputation:** -1  
**Voted as malicious:** 1 times

**DNS Records:**

Type	Value	TTL
NS	ns6.alphastand.win	300
NS	ns8.alphastand.win	300
NS	ns2.alphastand.win	300
NS	ns7.alphastand.win	300
A	35.204.181.10	300
TXT	v=spf1 include:_incspfcheck.mailspike.net ?all	300
SOA	ns8.alphastand.win	2560
MX	mx1.alphastand.win	300
NS	ns3.alphastand.win	300
NS	ns1.alphastand.win	300
NS	ns4.alphastand.win	300
MX	mx2.alphastand.win	300
NS	ns5.alphastand.win	300

**Whois**

Administrative city: REDACTED FOR PRIVACY  
Administrative country: REDACTED FOR PRIVACY  
Administrative state: REDACTED FOR PRIVACY  
Create date: 2023-01-10 00:00:00  
Domain name: alphastand.win  
Domain registrar id: 81

Expand

**VirusTotalV3** Expand

**ALPHASTAND.WIN**  
Detected: 19 Threshold: 1

**Reputation:** -1  
**Voted as malicious:** 1 times

**DNS Records:**

Type	Value	TTL
NS	ns6.alphastand.win	300
NS	ns8.alphastand.win	300
NS	ns2.alphastand.win	300
NS	ns7.alphastand.win	300
A	35.204.181.10	300
TXT	v=spf1 include:_incspfcheck.mailspike.net ?all	300
SOA	ns8.alphastand.win	2560
MX	mx1.alphastand.win	300
NS	ns3.alphastand.win	300
NS	ns1.alphastand.win	300
NS	ns4.alphastand.win	300
MX	mx2.alphastand.win	300
NS	ns5.alphastand.win	300

**Whois**

Administrative city: REDACTED FOR PRIVACY  
Administrative country: REDACTED FOR PRIVACY  
Administrative state: REDACTED FOR PRIVACY  
Create date: 2023-01-10 00:00:00  
Domain name: alphastand.win  
Domain registrar id: 81

Google



Within the alert, what is the http user agent for the event that triggered the alert? (1/2)

The screenshot shows an alert summary for 'sw\_malware\_win\_lokibot\_c2' with ID 39362, created by 'Workshop 29' on September 06, 2024 at 06:25:33. The alert is currently in 'Triage' status. A callout bubble labeled 'Click' points to the alert title. Another callout bubble labeled 'Click' points to the 'Events (1)' button, which is highlighted with a red border. The event details table below also has a red border around its first row.

NAME	TYPE	SOURCE / PRODUCT	ARTIFACTS	PORT	OUTCOME	TIME
NETWORK_HTTP	NETWORK_HTTP	RULE	HTTP://ALPHASTAND.WIN/AIE...			September 06, 2024 04:28:45

The screenshot shows the details of the single event from the previous table. The event is identified as 'Events Table (1)'. A callout bubble labeled 'Click' points to the 'View More' button, which is highlighted with a red border. The event details table includes columns for METADATA.EVENT\_TYPE, METADATA.VENDOR\_NAME, INGESTED\_TIMESTAMP, PRINCIPAL.IP, and PRINCIPAL.USERNAME.

METADATA.EVENT_TYPE	METADATA.VENDOR_NAME	INGESTED_TIMESTAMP	PRINCIPAL.IP	PRINCIPAL.USERNAME
NETWORK_HTTP	Zscaler	2024-09-06T05:06:07.053482Z	IP 10.128.0.21	PHIL.ALDRIN



Within the alert, what is the http user agent for the event that triggered the alert? (2/2)

**NETWORK\_HTTP** X

agent

You could scroll through the fields or type in a portion of the field name like this

Default	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 YaBrowser/23.9.0.2325 Yowser/2.5 Safari/537.36
Field Name	value
event_network_http_userAgent	Mozilla/5.0 (Windows NT 10.0; WOW64) Ap... <span>⋮</span>

Time ▼



Google SecOps

# Is the external IP address in the Entities Highlights widget communicating with other systems? (1/2)

The screenshot shows the Soar platform interface with the following details:

- Header:** sw\_malware\_win\_lokibot\_c2, ID 4064, Workshop 10, Triage, 2023-11-27 06:24:45, Soar User 10.
- Manage Tags:** Manage Tags button.
- Entities Highlights (7):**
  - IP:** 10.128.0.21 (Network Name: LunarS-Internal, Network Address: 10.128.0.0/24). Buttons: Explore, View details, Settings.
  - IP:** WIN-ADFS.LUNARSTIIINESS.COM. Buttons: Explore, View details, Settings.
  - IP:** 185.189.112.157. Buttons: Explore (highlighted with a red box), View details, Settings.
  - PHIL.ALDRIN**. Buttons: Explore, View details, Settings.
  - URL:** HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1071/001/. Buttons: View details, Settings.
  - URL:** HTTP://ALPHASTAND.WIN/ALIEN/FRE.PHP. Buttons: View details, Settings.
  - ALPHASTAND.WIN**. Buttons: Explore, View details, Settings.

A large white arrow points from a button labeled "Click" to the "Explore" button for the IP address 185.189.112.157.



# Is the external IP address in the Entities Highlights widget communicating with other systems?(2/2)

SEARCH i New Features Go to Legacy search ⋮ ^

Enter any question here, for example "Find externally shared documents with confidential in the title"

1 target.ip = "185.189.112.157"

Generated Query Like Rewrite Case Sensitivity Off SEPTEMBER 05, 03:42 PM - SEPTEMBER 06, 03:42 PM Run Search ⋮

History UDM Lookup Lists

OVERVIEW EVENTS (1) ALERTS (1) Click

Trend over time Prevalence

ADD FILTER CLEAR APPLY TO SEARCH AND RUN

EVENTS PIVOT Search events... WRAP TEXT COLUMNS ⋮ ▼

TIMESTAMP	EVENT	USER	HOSTNAME	PROCESS NAME
2024-09-06T03:28:45.000	1 ALERT NETWORK_HTTP phil.aldrin to alphastand.win	phil.aldrin	win-adfs.lunarstiiness.com	[Unknown]



Google SecOps

# Your Workdesk



# My Cases

The screenshot shows the 'My Cases' section of the Google SecOps platform. A user profile for 'Soar User 10' is at the top left, with a 'Hello.' greeting and a 'Click' annotation pointing to the profile picture.

The main navigation bar includes 'My Cases (5)', 'Pending Actions', 'My Tasks (1)', 'Requests', 'Workspace', and 'Announcements'. Below this, filters show 'Assigned to Me (2)', 'Assigned to My Role (3)', 'Mention of Me (0)', and 'Mention of My Role (0)'. A 'Click' annotation points to the 'View Details' button for the first case listed.

The first case, 'Suspicious Microsoft Office Download - win-se...', is highlighted with a red box around its 'View Details' button. It shows a yellow icon, a 'High' priority level, and was created '6 hours ago' by 'Soar User 10'. A 'Click' annotation points to the 'View Details' button for this case.

The second case, 'sw\_malware\_win\_lokibot\_c2 (ID 39970)', also has a red box around its 'View Details' button. It shows a red icon, a 'Critical' priority level, and was created '11 hours ago' by 'Soar User 10'.

Annotations at the bottom explain the icons: a yellow square is labeled 'Playbook status', a red circle is labeled 'Priority', and a blue rectangle is labeled 'Creation time'.

Case ID	Status	Priority	Created By	Action
Suspicious Microsoft Office Download - win-se...	Yellow icon	High	6 hours ago	Soar User 10
sw_malware_win_lokibot_c2 (ID 39970)	Red icon	Critical	11 hours ago	Soar User 10

Playbook  
status

Creation  
time



# Case Summary Status

Google SecOps | Your Workdesk

Hello,  
Soar User 10

Numbers of alerts for the case

Current stage

1 Alerts

Triage

My Cases (5) Pending Actions ? My Tasks (1) Requests Workspace Announcements

Assigned to Me (2) Assigned to My Role (3) Mention of Me (0) Mention of My Role (0)

Suspicious Microsoft Office Download - win-se... High 6 hours ago

sw\_malware\_win\_lokibot\_c2 (ID 39970) Critical 11 hours ago

Case Management Workshop - Malware Found (Pending for user)  
Case assigned to Soar User 10  
12 hours ago

1 Click

Click

Cancel Go To Case



Google SecOps

# Pending Actions

The screenshot shows the Chronicle Workdesk interface. At the top, there's a navigation bar with 'Chronicle' and 'Your Workdesk' on the left, and user status icons on the right. Below the navigation bar, a message says 'Hello, Soar User 10'. The main area has tabs for 'My Cases (3)', 'Pending Actions (1) ?' (which is active), 'My Tasks', 'Requests', 'Workspace', and 'Announcements'. Under the 'Pending Actions' tab, there's a list of one item: 'SW\_MALWARE\_WIN\_LOKIBOT\_C2'. The details for this item include: 'The external entities (domain and URL) are suspicious. Request a full investigation of...', an icon for 'Endpoint investigation?', a red box around it, a red arrow pointing down to the text 'Name of the stage/step in the playbook', a red box around the 'Respond' button, and a callout bubble with the text 'Click' pointing to the 'Respond' button.

My Cases (3) Pending Actions (1) ? My Tasks Requests Workspace Announcements

Critical (1) High (0) Medium (0) Low (0) Informative (0)

Search... ▾

SW\_MALWARE\_WIN\_LOKIBOT\_C2

The external entities (domain and URL) are suspicious. Request a full investigation of...

Endpoint investigation?

Critical 11 hours ago View Case ID 4064 Respond

Click

Name of the stage/step in the playbook



Google SecOps

# Pending Action Details

Chronicle | Your Workdesk

Hello,  
**Soar User 10**

My Cases (3) Pending Actions (1) My Tasks Requests Workspace Announcements

Critical (1) High (0) Medium (0) Low (0) Informative (0)

SW\_MALWARE\_WIN\_LOKIBOT\_C2 SU

The external entities (domain and URL) are suspicious. Request a full investigation o... Endpoint investigation ?

**1** Click Yes

**2** Click Done

**Endpoint investigation ?**

**Message to Assignee**  
The external entities (domain and URL) are suspicious. Request a full investigation of the endpoint ?

**Target Entities**

WIN-ADFS.LUNARSTIINESS.COM	IP 10.128.0.21
PHIL.ALDRIN	IP 185.189.112.157
HTTP://ALPHASTAND.WIN/ALIEN/FRE.PHP	URL HTTPS://ATTACK.MITRE.ORG/TECHNIQU...
ALPHASTAND.WIN	

**Instance**

**Action Parameters**  
The external entities (domain and URL) are suspicious. Do you want to request a full investigation of the endpoint ?

Yes  
 No  
 No but inform the End User

**View Case**

**Additional information:**  
It is an external threat

**Target Entities:**  
Malicious Domain  
Malicious URL  
External IP Address  
Username  
Hostname  
Internal IP Address  
MITRE ATT&CK Technique

**Pending Playbook Action:**  
Analyst response requested

Google



# Responding and Taking Action

SOAR - Malware Identified - Investigate this Endpoint Inbox x Print Edit

No Reply <no-reply@secops.joonix.net>  
to me ▾

11:40 AM (0 minutes ago) Star Reply More

Case Name: sw\_malware\_win\_lokibot\_c2  
Case ID: 826  
Case Creation Time: 2023-11-07 06:13:48 UTC+00

Alert Name: SW\_MALWARE\_WIN\_LOKIBOT\_C2  
Alert Creation Time: 2023-11-07 04:42:40 UTC+00

**Case details**

Associated Entities: [WIN-ADFS.LUNARSTIIINESS.COM](#), 10.128.0.21, PHIL.ALDRIN, 185.189.112.157, [HTTP://ALPHASTAND.WIN](#), [WIN/ALIEN/FRE.PHP](#), [HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1071/001/ALPHASTAND.WIN](#)

**Entities**

**sw\_malware\_win\_lokibot\_c2 Status CLOSED** Case has status of closed

ID 826 Default Environment Triage 2023-11-07 16:40:25

Manage Tags T3 @Tier3 Explore

**Case owner is T3 (Tier 3)**

1. SW\_MALWA... (1) • Closed Closed ✓

2023-11-07 04:42:40

**Alert has status of closed**

Overview Events (1) Playbooks (1) Graph

Alert Details (4)

Google



Google SecOps

# Manual Actions



# Manual Actions

Can be triggered on a per entity basis

Provides additional context around entities in an alert or case

Dependent upon the integrations installed on your instance

Will highlight Google SecOps, Mandiant and VirusTotal today but additional integrations can be downloaded from the Marketplace

The screenshot shows the Google SecOps Marketplace interface. At the top, there are three tabs: 'Use Cases', 'Integrations' (which is highlighted with a red box), and 'Power Ups'. Below the tabs, there are filters for 'Type' (All Integrations) and 'Status' (All). There are also category buttons for 'Security', 'Threat Intelligence', 'IT & Infrastructure', 'Access Management', and 'IAM'. A search bar at the top right says 'Search for integrations...'. The main area is titled 'Latest Releases' and features two cards: 'EclecticIQ' (Community, v 1.0, NEW) and 'Mandiant Managed Defense' (Certified, v 1.0, MDR, NEW). Each card has 'Details' and 'Install' buttons. Below these cards, there is a section titled 'Other Integrations that might interest you'.



Google SecOps

# Navigate to a Case from Your Workdesk

The screenshot shows the Soar Workdesk interface. A red box highlights the 'My Cases' icon in the sidebar. A callout bubble labeled 'Click' points to the 'My Cases (4)' tab. A red circle with the number '1' is positioned above the 'My Cases' tab. Another red box highlights the 'Go to Case' button next to a case card. A callout bubble labeled 'Click' points to this button. A red circle with the number '2' is positioned below the 'Go to Case' button.

Click 1

Hello,  
Soar User 10

My Cases (4) Pending Actions 0 My Tasks Requests Workspace Announcements

Assigned to Me (1) Assigned to My Role (3) Mention of Me (0) Mention of My Role (0)

Suspicious Microsoft Office Download - win-ser... High 8 hours ago Soar User 10 View Details Go to Case

2 Click

# Cases & Alerts Review



Suspicious Microsoft Office Download - win-server.lunarstiiiness.com

ID 4065 Workshop 10 Investigation 2023-11-27 18:29:45

SU Soar User 10

Manage Tags

1. RECON\_ENVIRONMEN... (9) • 2023-11-27 04:33:00

2. RECON\_SUSPICIOUS\_... (6) • 2023-11-27 04:39:00

3. SW\_SUSPICIOUS\_DO... (2) • 2023-11-27 05:43:00

4. RECON\_CREDENTIAL... (10) • 2023-11-27 04:36:00

5. PORT\_PROXY\_FORWA... (4) • 2023-11-27 04:55:30

5 Alerts

Overview

How many alerts are a part of this case?

How many events are part of each alert?

Have playbooks been run on any alerts yet? If so, which ones and what are their current state?

# Cases & Alerts Review

Suspicious Microsoft Office Download - win-server.lunarstiiiness.com

ID 4065 Workshop 10 Investigation 2023-11-27 18:29:45 SU Soar User 10

Manage Tags

1. RECON\_ENVIRONMENT\_ENUMERATION\_ACTIVE\_DIRECT... (9) • 2. RECON\_SUSPICIOUS\_COMMANDS\_CISA\_REPORT (6) • 3. SW\_SUSPICIOUS\_DOWNLOAD\_OFFICE (2) • 4. RECON\_CREDENTIAL\_THEFT\_CISA\_REPORT (10) • 5. PORT\_PROXY\_FORWARDING\_T1090\_CISA\_REPORT (4) •

5 Alerts

Overview

Alerts (5)

#	Alert Name	Time	Events	Priority	Playbook Attached	Alert SLA	Status	Action
1	RECON_ENVIRONMENT_ENUMERATION_ACTIVE_DIRECT...	2023-11-27 04:33:00	9	Low	N/A	N/A	Open	<a href="#">View details</a>
2	RECON_SUSPICIOUS_COMMANDS_CISA_REPORT	2023-11-27 04:39:00	6	Low	N/A	N/A	Open	<a href="#">View details</a>
3	SW_SUSPICIOUS_DOWNLOAD_OFFICE	2023-11-27 05:43:00	2	Critical	Case Management ...	N/A	Open	<a href="#">View details</a>
4	RECON_CREDENTIAL_THEFT_CISA_REPORT	2023-11-27 04:36:00	10	Low	N/A	N/A	Open	<a href="#">View details</a>
5	PORT_PROXY_FORWARDING_T1090_CISA_REPORT	2023-11-27 04:55:30	4	Low	N/A	N/A	Open	<a href="#">View details</a>



# Manual Actions - Case View

## Suspicious Microsoft Office Download - win-server.lunarstiiiness.com

[Explore](#)

ID

4065



Workshop 10



Investigation



2023-11-27 18:29:45



Soar User 10

[Manage Tags](#)

1. RECON\_ENVIRONMEN... (9) •

2023-11-27 04:33:00

2. RECON\_SUSPICIOUS\_... (6) •

2023-11-27 04:39:00

3. SW\_SUSPICIOUS\_DO... (2) •

2023-11-27 05:43:00

4. RECON\_CREDENTIAL... (10) •

2023-11-27 04:36:00

5. PORT\_PROXY\_FORWA... (4) •

2023-11-27 04:55:30

5 Alerts

[Overview](#)[Entities Highlights \(63\)](#)

Click

Or

Click



LEGIT

Explore

View details



C:\WINDOWS\SYSTEM32\NET1.EXE

Explore

View details



WIN\_REGISTRY

Explore

View details



4268

Explore

View details



MYANMARFREEDOMNETWORK.ORG

Explore

View details



34D5EA586A61B0ABA512C0CB1D3D8B15

Explore

View details



E92A2FA67AD2F7367ABA1ABF237D245B5E36291C5A4A9F0...

Explore

View details



WIN\_TOKEN

Explore

View details



5716

Explore

View details



24.103.111.114

Explore

View details



HTTPS://MYANMARFREEDOMNETWORK.ORG/JQUERY.MIN.JS

View details



HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1204/001/

View details





# Manual Action - Mandiant Enrich Entities

1 Click on the **MandiantThreatIntelligence** section in the sidebar.

2 Select the alert **SW\_SUSPICIOUS\_DOWNLOAD\_OFFICE**.

3 Select **24.103.111.114** and **myanmarfreedomnetwork.org** from the entity list.

4 Set Score Threshold to 50.

5 Click the **Execute** button.

# Insights

?

 Insights ⓘ

## M MandiantThreatIntelligence

Expand



MYANMARFREEDOMNETWORK.ORG

**Score: 100**

**First Seen:** 2023-06-06T10:36:54.000Z

**Last Seen:** 2024-08-29T09:05:27.000Z

**Sources:** Mandiant

For more details visit the following link:

<https://advantage.mandiant.com/indicator/fqdn/myanmarfreedomnetwork.org>

## M MandiantThreatIntelligence

Expand



24.103.111.114

**Score: 51**

**First Seen:** 2021-08-17T23:40:34.000Z

**Last Seen:** 2024-02-08T14:18:44.000Z

**Sources:** blocklist\_de,Mandiant

For more details visit the following link:

<https://advantage.mandiant.com/indicator/ipv4/24.103.111.114>

# Mandiant Threat Intel Detail

**MANDIANT ADVANTAGE** ▾ Attack Surface Management Security Validation Threat Intelligence What's New Breach Analytics for Chronicle

THREAT INTELLIGENCE Free Trial: 120 Days Remaining Google Adoption Eng ▾ Reports & Analysis Explore Digital Threat Monitoring File Analysis Settings  Search

 myanmarfreedomnetwork.org

### Indicator Details

**Analyst Verdict - Malicious** LAST UPDATED 2023-09-21

100 

**Note:** A Mandiant Analyst provided a direct score for this Indicator

Our Analysts directly reviewed this Indicator and provided an overriding verdict. Our regular machine learning analysis & processing of intelligence sources still occurred, but the Analyst's verdict is the one that is displayed.

**SHOW MORE**

Source	Mandiant
First Seen	Jun 6, 2023
Last Seen	Jul 6, 2023

**Actor Attribution**  TEMP.Hex

**Campaign Associations**  CAMP.22.033

### Actor Attribution

 **TEMP.Hex** SEPTEMBER 5, 2023

TEMP.Hex is a China-nexus cyber espionage actor that uses POISONIVY malware and a distinct mutex structure to primarily target political, defense and commercial interests in the nations bordering China and the US. TEMP.Hex campaigns are likely carried out to collect information in support of national security and economic interests that align with Chinese sponsors. Further, TEMP.Hex operations demonstrate a threat...

**Related Malware** BADFLICK, BEACON, BLACKSHEEP, BLASTPAD, BOPEEP, BOTCHDATE, CANDYSHELL,...

**Source Regions** China

**Targeted Regions** Australia, Austria, Belgium, Cambodia, China, Czech Republic, Egypt, France, Hong Kong, Hungary, India,...

**Targeted Industries** Agriculture, Chemicals & Materials, Civil Society & Non-Profits, Construction & Engineering, Education, Energy & Utilities, Financial Services, Governments, Healthcare, Hospitality, Insurance, Legal & Profession...

### Campaign Associations

 **Espionage Actor with China Nexus Conducts Email...** CAMP.22.033 MAY 12, 2023

Since June 2022, Mandiant detected phishing emails sent to multiple government organizations by TEMP.Hex. The emails contained links to Google Drive-hosted RAR files. These archives generally contained at least one lure document and a legitimate Adobe program sharing the same theme as the email, the latter of which acts as a launcher for other files in the archive. These ultimately led to the execution of...

**Associated Actors** TEMP.Hex

**Associated Malware** BROWNSPARK, LIGHTPIPE, TWOPPIPE

**Targeted Regions** Australia, Austria, Belgium, Cambodia, China, Indonesia, Italy, Japan, Luxembourg, Mauritius, Montenegro, Myanmar, Poland, Saudi Arabia, Singapore, South Korea, Sri Lanka, Taiwan, United Kingdom, United States...



# Entities Highlights - Suspicious Entities

Entities Highlights (63) ⓘ

TRUSTED	<a href="#">Explore ↗</a>	<a href="#">View details</a>	<a href="#">⚙️</a>
IDLE	<a href="#">Explore ↗</a>	<a href="#">View details</a>	<a href="#">⚙️</a>
MYANMARFREEDOMNETWORK.ORG	<a href="#">Explore ↗</a>	<a href="#">View details</a>	<a href="#">⚙️</a>
UNKNOWN		<a href="#">View details</a>	<a href="#">⚙️</a>
WIN-SERVER.LUNARSTIIINESS.COM	<a href="#">Explore ↗</a>	<a href="#">View details</a>	<a href="#">⚙️</a>
1920	<a href="#">Explore ↗</a>	<a href="#">View details</a>	<a href="#">⚙️</a>
DETECT-DEBUG-ENVIRONMENT			
# 34D5EA586A61B0ABA512C0CB1D3D8B15	<a href="#">Explore ↗</a>	<a href="#">View details</a>	<a href="#">⚙️</a>
24.103.111.114	<a href="#">Explore ↗</a>	<a href="#">View details</a>	<a href="#">⚙️</a>
2212	<a href="#">Explore ↗</a>	<a href="#">View details</a>	<a href="#">⚙️</a>
# 91A427BEA3BE91328D5AE6FD04C48D74862D77D3685EA56...	<a href="#">Explore ↗</a>	<a href="#">View details</a>	<a href="#">⚙️</a>
HTTPS://ATTACK.MITRE.ORG/VERSIONS/V13/TECHNIQUES/T1555/		<a href="#">View details</a>	<a href="#">⚙️</a>



Google SecOps

# Case Options

Click

Suspicious Microsoft Office Download - win-server.lunarstiiness.com

ID 1677 Workshop 10 Investigation 2023-11-08 21:30:40

Manage Tags

Overview

1. SW\_SUSPICIOUS\_DO... (2) • 2023-11-08 04:37:00

2. RECON\_ENVIRONMEN... (6) • 2023-11-08 04:18:00

3. RECON\_ENVIRONME... (10) • 2023-11-08 04:24:00

4. RECON\_CREDENTIAL... (10) • 2023-11-08 04:30:00

5. PORT\_PROXY\_FORWA... (4) • 2023-11-08 04:49:30

Explore

Soar User 10

Action Context Menu:

- Mark as important
- Incident
- Stage
- Priority
- Report



# Alert Options

Click 1

Click 2

The screenshot shows the Google SecOps interface. At the top, there's a list of alerts with the first one highlighted by a red box and a callout 'Click 1'. Below the alerts is a navigation bar with 'Overview', 'Events (2)', 'Playbooks (1)', and 'Graph' buttons. To the right of the alerts is a settings icon and a three-dot menu. A callout 'Click 2' points to the three-dot menu. A red box highlights the menu, which contains the following options:

- Ingest alert as test case
- Move Alert
- Change Priority
- Add Entity
- View Other Alerts From The Rule
- Manage Alert Detection Rule
- Close Alert

Alert Details (5)

Alert name	Device Product	Start Time	End Time
SW_SUSPICIOUS_DOWNLOAD_OFFICE	RULE	2023-11-08 04:37:00 UTC+00	2023-11-08 04:42:00 UTC+00
Creation Time			
2023-11-08T21:25:12.170244Z			

Events (2) ⓘ



Google SecOps

# Case Tasks

The screenshot shows a dashboard titled "Case Tasks" with five cards representing different tasks:

- 1. SW\_SUSPICIOUS\_DO... (2) • 2023-11-08 04:37:00
- 2. RECON\_ENVIRONMEN... (6) • 2023-11-08 04:18:00
- 3. RECON\_ENVIRONME... (10) • 2023-11-08 04:24:00
- 4. RECON\_CREDENTIAL... (10) • 2023-11-08 04:30:00
- 5. PORT\_PROXY\_FO... (10) • 2023-11-08 04:49:30

A "Case Task" button is located in the top right corner of the dashboard.

The screenshot shows an "Add Task" modal with the following fields:

- Title: Review Before Closing
- Assign To: Secops Joonix
- Task Content: Please review and provide any additional commentary before we close this case out.
- Due Date: 2023-11-10 17:00

At the bottom are "Cancel" and "Save" buttons. A red arrow points to the "Save" button.

The screenshot shows the "Chronicle | Your Workdesk" interface with the following elements:

- User profile: Hello, Secops Joonix
- Navigation tabs: My Cases (1), Pending Actions, My Tasks (1) (highlighted with a red box), Requests, Workspace
- Task details:
  - Review Before Closing
  - Please review and provide any additional commentary before we close this case out.
  - Deadline: Nov 10, 2023
  - Edited by: Soar User 10 at Nov 8, 2023
  - Created by: Soar User 10 at Nov 8, 2023
  - Case Name: Suspicious Microsoft Office Download - win-server.lunarstiiness.com (ID 1677)
- Bottom buttons: View Task, Mark as done



# Adding Files or Commentary to a Case

Google SecOps | Cases

Suspicious Microsoft Office Download - win-server.lunarstiiiness.com

ID 40054 Workshop 10 Investigation September 11, 2024 18:36:09

Explore

Manage Tags

Alerts (3)

#	ALERT NAME	TIME	EVENTS	PRIORITY	PLAYBOOK ATTACHED	ALERT SLA	STATUS	View details
1	PORT_PROXY_FOR...	September 11, 2024...	2	Low	N/A	N/A	Open	<a href="#">View details</a>
2	RECON_CREDENTIALI...	September 11, 2024...	10	Low	N/A	N/A	Open	<a href="#">View details</a>
3	SW_SUSPICIOUS_D...	September 11, 2024...	2	Critical	Case Manage...	N/A	Open	<a href="#">View details</a>

Insights

MandiantThreatIntelligence Expand

MYANMARFREEDOMNETWORK.ORG

MandiantThreatIntelligence Expand

IP 24.103.111.114

Write a comment...

> T U

# Exercise - Working in a Case

Use the manual action to get related entities with a minimum score of 50 for the URL from the **Mandiant Threat Intelligence** integration for the URL: <https://myanmarfreedomnetwork.org/Js/jQuery.min.js>

- Find the results on the Case Wall and export the json output (if allowed)
- How many additional IOCs are there?
  - IP addresses? Domains? Email Addresses? File Hashes? URLs?
- Add the json attachment and a comment to the case - Validate that it was uploaded by reviewing the Case Wall

Use the manual action to get related IP addresses from VirusTotal for the domain **myanmarfreedomnetwork.org**

- What are those IP addresses?

Use the Case Tasks/Options and Alert Options to further tweak the case and alerts

- Go ahead and explore and let us know what else you find
- Note the changes on the case wall when different options are used

# Exercise - Working in a Case

Use the manual action to get related entities with a minimum score of 50 for the URL from the **Mandiant Threat Intelligence** integration for the URL: <https://myanmarfreedomnetwork.org/Js/jQuery.min.js>

- Find the results on the Case Wall and export the json output (if allowed)
- How many additional IOCs are there?
  - IP addresses? Domains? Email Addresses? File Hashes? URLs?
- Add the json attachment and a comment to the case - Validate that it was uploaded by reviewing the Case Wall

Use the manual action to get related IP addresses from VirusTotal for the domain **myanmarfreedomnetwork.org**

- What are those IP addresses?

In the Entities Highlights, there should be an entity with the name **c:\program files\7-zip\7z.exe**. Our organization does not use 7-zip. Pivot and execute a search to determine which user, on what system and what processes are associated with 7-zip.

Use the Case Tasks/Options and Alert Options to further tweak the case and alerts

- Go ahead and explore and let us know what else you find
- Note the changes on the case wall when different options are used



# Manual Action - Related Entities - URL

Manual Action ?

Search...

- EmailV2
- Functions
- GoogleChronicle
- MitreAttck
- Mandiant
- MandiantThreatIntelligence

Enrich Entities

Enrich IOCs

Get Malware Details

Get Related Entities

Ping

**M Get Related Entities**

Get information about ioc related to entities using information from Mandiant. Supported entities: Hostname, Domain, IP Address, URL, File Hash, Threat Actor.

Choose Instance \* Shared\_MandiantThreatIntelligence

Run on Alerts \* SW\_SUSPICIOUS\_DOWNLOAD\_OFFICE

**Entities**

Group Choose

Specific HTTPS://MYANMARFREEDOMNETWORK.ORG/JQUERY.MIN.JS

Lowest Severity Score \* 50

Max IOCs To Return 100

Cancel Execute



# Validating Actions

Case Wall

2023-11-08 04:37:00    2. RECON\_ENVIRONMEN... (6) •    3. RECON\_ENVIRONME... (10) •    4. RECON\_CREDENTIAL... (10) •    5. PORT\_PROXY\_FORWA... (4) •    5 Alerts

9 15 1 2 0 0

All Alerts Choose User

2023-11-08 23:48:25  
Manual action "Mandiant\_Get Related Entities" has finished running. by Soar User 10

2023-11-08 23:48:25  
**M Mandiant\_Get Related Entities** Successfully returned related indicators for the following entities using i... [View More](#)

2.SW\_SUSPICIOUS\_DOWNLOAD\_OFFICE



# Get Related Entity Details

M Mandiant\_Get Related Entities | Successfully returned related indicators for the following entities using information from Mandiant: http... [View Less](#)

Shared\_Mandiant

**Output message**

Successfully returned related indicators for the following entities using information from Mandiant: https://myanmarfreedomnetwork.org/Js/jQuery.min.js

**Scope**

**Parameters**

NAME	VALUE
Lowest Severity Score	50
Max IOCs To Return	100

**Return Values**

**Script Result**

```
is_success      true
```

**JSON Result**

```
0 [2]
Entity https://myanmarfreedomnetwork.org/Js/jQuery.min.js
EntityResult [5]
email [0]
> fqdn [68]
> hash [32]
ip [0]
url [0]
```



# Adding Commentary to a Case

`<> Shared_Mandiant_JSON_Result.json`

Here is a listing of associated domains and file hashes to the suspicious URL....

## Case Wall



9



15



1



2



2



0



0

2023-11-08 23:54:23



**Soar User 10** left a comment



`<> Shared_Mandiant_JSON_Result.json`

Here is a listing of associated domains and file hashes to the suspicious URL....



# Action - Related IPs from VirusTotal - Domain

### Manual Action

- Download File
- Enrich Hash
- Enrich IOC
- Enrich IP
- Enrich URL
- Get Domain Details
- Get Graph Details
- Get Related Domains
- Get Related Hashes
- Get Related IPs**
- Get Related URLs
- Ping
- Search Entity Graphs
- Search Graphs

**Get Related IPs**  
Get related IPs to the provided entities from VirusTotal. Note: this action requires a VT Enterprise token. Supported entities: URL, Filehash, Hostname. Note: only MD5, SHA-1 and SHA-256 are supported.

Choose Instance \*

Run on Alerts \*

**Entities**

Group

Specific

Results

Max IPs To Return

**Close** **Execute**



# Get Related IPs

2023-11-08 23:56:01

VirusTotalV3\_Get Related IPs | Successfully returned related IPs to the provided entities from VirusTotal. [View Less](#)

Shared\_VirusTotal

**Output message**

Successfully returned related IPs to the provided entities from VirusTotal.

**Scope**

---

**Parameters**

NAME	VALUE
Results	Combined
Max IPs To Return	40

---

**Return Values**

**Script Result**

is_success	true
------------	------

**JSON Result**

ips [3]

- 0 192.64.119.161
- 1 103.22.183.158
- 2 185.62.56.93

# Search on a Specific Entity

Suspicious Microsoft Office Download - win-server.lunarstiiness.com

ID 1677 Workshop 10 Investigation 2023-11-08 23:54:23 SU Soar User 10

Manage Tags

Entities Highlights (77) ⓘ

Entity Type	Value	Actions
#	9E28034CE3AEEA6951F790F8997DF44CFBF80BEFF9FB174...	Explore View details ⚙️
#	6679EA8FBEB539B5852CE8838420471FED0600F5050F337...	Explore View details ⚙️
#	935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C...	Explore View details ⚙️
C:	PROGRAM FILES\7-ZIP\	Explore (button highlighted with red box) View details ⚙️
#	E5888E649C881E4BBBCE472F6808F93B2B5564D3094995A...	Explore View details ⚙️
URL	HTTPS://ATTACK.MITRE.ORG/VERSIONS/V13/TECHNIQUES/T1090/	View details ⚙️
NETWORK_DNS	HTTPS://ATTACK.MITRE.ORG/VERSIONS/V13/TECHNIQUES/T1555/	Explore View details ⚙️
	C:\WINDOWS\SYSTEM32\NETSH.EXE	Explore View details ⚙️
#	935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C...	Explore View details ⚙️

# Searching for Values from Entities Highlights

**UDM SEARCH**

Enter any question here, for example "Find externally shared documents with confidential in the title"

```
1 principal.file.full_path = /*.*c:\\Program\\ Files\\7\\zip\\*/ OR src.file.full_path = /*.*c:\\Program\\ Files\\7\\zip\\*/ OR target.file.full_path = /*.*c:\\Program\\ Files\\7\\zip\\*/
```

History UDM Lookup Lists Generated Query Rewrite NOVEMBER 27, 05:08 PM - NOVEMBER 28, 05:08 PM Search :

OVERVIEW (0) EVENTS (8) ALERTS (1)

**8 EVENTS**

**ADD FILTER** CLEAR APPLY TO SEARCH AND RUN

EVENT	PIVOT	Search events...	WRAP TEXT	COLUMNS	⋮
TIMESTAMP	EVENT				⋮
2023-11-28T05:10:12.442	<span style="border: 1px solid red; padding: 2px;">1 ALERT</span> [PROCESS_LAUNCH] netsh.exe launched by cmd.exe				
2023-11-28T05:10:12.418	<span style="border: 1px solid red; padding: 2px;">1 ALERT</span> [PROCESS_LAUNCH] cmd.exe launched by DiskUtil-win-x64-installer.exe				
2023-11-28T05:09:56.434	<span style="border: 1px solid red; padding: 2px;">1 ALERT</span> [PROCESS_LAUNCH] netsh.exe launched by cmd.exe				
2023-11-28T05:09:56.410	<span style="border: 1px solid red; padding: 2px;">1 ALERT</span> [PROCESS_LAUNCH] cmd.exe launched by DiskUtil-win-x64-installer.exe				
2023-11-28T05:09:25.136	[PROCESS_LAUNCH] 7z.exe launched by cmd.exe				
2023-11-28T05:09:25.111	[PROCESS_LAUNCH] cmd.exe launched by DiskUtil-win-x64-installer.exe				
2023-11-28T05:09:09.449	[PROCESS_LAUNCH] 7z.exe launched by cmd.exe				
2023-11-28T05:09:09.425	[PROCESS_LAUNCH] cmd.exe launched by DiskUtil-win-x64-installer.exe				

**USER HOSTNAME PROCESS NAME**

tim.smith_admin	win-server.lunarstiiness.com	cmd.exe
tim.smith_admin	win-server.lunarstiiness.com	DiskUtil-win-x64-installer.exe
tim.smith_admin	win-server.lunarstiiness.com	cmd.exe
tim.smith_admin	win-server.lunarstiiness.com	DiskUtil-win-x64-installer.exe
tim.smith_admin	win-server.lunarstiiness.com	cmd.exe
tim.smith_admin	win-server.lunarstiiness.com	DiskUtil-win-x64-installer.exe
tim.smith_admin	win-server.lunarstiiness.com	cmd.exe
tim.smith_admin	win-server.lunarstiiness.com	DiskUtil-win-x64-installer.exe

# What Did We Learn About This Case?

Uncovered a suspicious domain, IP and URL

- These in turn helped uncover related IPs, domains and file hashes

Did you find it easy to gather this information using actions?

Does anyone want to share other actions they performed or anything they identified?

Would you prefer to have some of this gathered automatically for you before you start diving into a case?



# What Did We Learn About This Case?

Uncovered a suspicious domain, IP and URL

- These in turn helped uncover related IPs, domains and file hashes

7-zip appears to be running on one system in our environment and is being used by an admin

- Is there more we can learn about diskutil-win-x64-installer.exe?

Did you find it easy to gather this information using actions?

Does anyone want to share other actions they performed or anything they identified?

Would you prefer to have some of this gathered automatically for you before you start diving into a case?



# Summary

Events are used to generate detections via the rules engine

Alerts are organized into Cases

Cases provide a top level view with one or more alerts in each one

Playbooks are run on alerts

Manual actions can be run on entities at a case or alert level

The workdesk provides a user specific interface for cases, alerts and tasks assigned to them

A common case queue is available as well

# Handy Links

Case Overview:

<https://cloud.google.com/chronicle/docs/soar/investigate/working-with-cases/cases-overview>

Alert Overview:

<https://cloud.google.com/chronicle/docs/soar/investigate/working-with-alerts/whats-on-the-alert-overview-tab>

Marketplace Integrations: <https://cloud.google.com/chronicle/docs/soar/marketplace-integrations>

SecOps Community: <https://secopscommunity.com>

# Thank You