SOC - Azure

Overview

Room URL: https://tryhackme.com/room/azuresentinel-aoc2025-a7d3h9k0p2

Difficulty: Medium

Category: SOC

Date Completed: 12/12/2025

Objectives

- Understand the importance of alert triage and prioritisation
- Explore Microsoft Sentinel to review and analyse alerts
- Correlate logs to identify real activities and determine alert verdicts

Table of Contents

Introduction

The dashboards are lighting up. Alerts are flooding in from the Azure tenant, and the Evil Bunnies' attack is unfolding in real time. McSkidy knows that jumping into every alert at once would be chaos—some are noise, others are false positives, and a few represent genuine threats that could compromise The Best Festival Company's entire infrastructure. This is where **alert triaging** becomes the difference between panic and precision. By systematically assessing severity, timing, attack context, and impact, McSkidy can cut through the noise and focus on what truly matters:

stopping the Evil Bunnies before they cripple the Christmas season. The challenge ahead requires not just identifying threats, but understanding the relationship between alerts, correlating evidence across logs, and building a timeline that reveals the full scope of the compromise.

Key Challenges

- **Eight open incidents** across the Azure tenant (four high-severity, four medium-severity)
- **Attack progression** visible through related alerts pointing to the same entities
- **Privilege escalation and persistence** tactics indicating advanced compromise
- **Time-sensitive response** required to prevent further damage.

Walk Through

Step 1: Accessing Microsoft Sentinel

1. Navigate to the **Azure Portal** and search for **Microsoft Sentinel**
2. Click on your dedicated Sentinel instance
3. Under the **Threat management** dropdown, select the **Incidents** tab to view triggered incidents
4. Press the `<<` button to expand the view for better visibility
5. If incidents don't appear, refresh your browser page
6. **Note:** If no incidents are visible, ensure you've set a custom date range to capture the current timeframe

Step 2: Understanding the Alert Landscape

From the incident overview, you should observe:

- **Four high-severity incidents** - prioritize these first as they represent potential compromise points or privilege-escalation activities
- **Four medium-severity incidents** - investigate after addressing critical threats
- **Total of eight open incidents** requiring triage and analysis

Step 3: Triaging High-Severity Alerts Using the Four Dimensions

Apply the **triage framework** to each alert:

Dimension	Question	Action
Severity	How bad is this?	Review alert rating (Informational → Critical)
Time	When did this occur?	Check timestamp and frequency of related activities
Context	Where in the attack lifecycle?	Identify stage (reconnaissance, persistence, exfiltration)
Impact	Who or what is affected?	Assess asset importance and potential business risk

Step 4: Examining the Linux PrivEsc—Kernel Module Insertion Alert

1. Click on the **Linux PrivEsc—Kernel Module Insertion** alert to open it
2. In the summary panel, observe:
   - **Three events** related to this alert
   - **Alert creation time** (note the timestamp)
   - **Three entities** involved in the compromise
   - **Tactic classification:** Privilege Escalation
3. Click **View full details** to access extended information including:
   - **Incident Timeline** - shows sequence of related activities
   - **Similar Incidents** - reveals other alerts connected to the same entities

Step 5: Understanding Alert Correlation

Examine which alerts share the same entities (machine, user, or IP address). When multiple detections link to a single entity, they typically represent **different stages of the same intrusion**, not isolated incidents.

Example attack progression pattern:

```
Root SSH Login from External IP
    ↓ (Initial Access)
SUID Discovery
    ↓ (Privilege Escalation Reconnaissance)
Kernel Module Insertion
    ↓ (Persistence & Privilege Escalation)
```

Step 6: Diving into Log Analysis - Querying Raw Events

1. From the alert's **full details view**, click **Events** in the **Evidence** section
2. Observe the actual kernel module names and installation timestamps
3. To perform deeper analysis, switch to **KQL mode**:
   - Click the **Simple mode** dropdown (upper-right corner)
   - Select **KQL mode**
4. Run the following KQL query to examine all events from a specific host (e.g., **app-02**):

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

5. Press **Run** and wait for results to render

Step 7: Analyzing the Log Results

After executing the query, you'll observe a sequence of suspicious events around the kernel module installation:

1. `cp` **command execution** - creates a shadow file backup (credential theft preparation)
2. **User Alice added to sudoers group** - grants elevated privileges
3. **backupuser account modification** - performed by root (privilege escalation confirmation)
4. **malicious_mod.ko insertion** - the malicious kernel module installation
5. **Root SSH authentication** - successful remote access with elevated privileges

Step 8: Contextualizing the Attack Sequence

The surrounding events tell a comprehensive story:

- **Shadow file backup** indicates attacker preparation for credential harvesting
- **Sudoers group modification** reveals persistence planning
- **User account modifications** show privilege escalation tactics
- **Kernel module installation** confirms advanced persistence mechanism
- **Root SSH access** demonstrates successful system compromise

This pattern is **highly unusual** for normal system operations and clearly indicates **privilege escalation and persistence behavior**.

Step 9: Decision and Escalation

Based on the evidence:

1. **Confirm this is not a false positive** - the attack sequence is coherent and intentional
2. **Escalate to the incident response team** immediately - this represents active compromise
3. **Document the findings** including:
   - Affected hosts (app-02 and others with kernel module alerts)
   - Timeline of events
   - Attack progression (initial access → privilege escalation → persistence)
   - Indicators of compromise (IOCs)
   - Recommended remediation steps

Step 10: Correlating Remaining Alerts

Repeat the triage and investigation process for:

- The remaining three high-severity incidents
- All four medium-severity incidents
- Document any additional entities or attack patterns discovered

---

Lessons Learned

- **Alert triage efficiency depends on a structured framework** – applying the four dimensions (severity, time, context, impact) allows analysts to prioritize threats systematically and avoid alert fatigue, ensuring focus remains on genuine threats like the Evil Bunnies' kernel module persistence mechanisms.
- **Correlation reveals attack progression** – by linking related alerts through common entities (hosts, users, IPs) and examining raw logs in Microsoft Sentinel, analysts can reconstruct the full attack timeline, from initial access through privilege escalation to persistence, transforming isolated detections into a coherent incident narrative that informs escalation and remediation decisions.

Resources

TryHackMe

Revision #1

Created 2025-12-14 19:40:17 UTC by David Rizzo

Updated 2025-12-14 19:41:03 UTC by David Rizzo