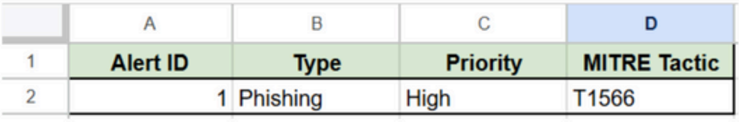
Alert Management Practice

Objective:

The objective of this task is to practice alert management by classifying security alerts, assigning priorities based on severity, mapping alerts to MITRE ATT&CK techniques, visualizing alert priorities using Wazuh dashboards, and documenting incident response and escalation.

Alert Classification System

An alert classification system was created using Google Sheets to categorize alerts based on type, priority, and associated MITRE ATT&CK techniques. This helps standardize alert handling and ensures consistent triage across SOC operations.

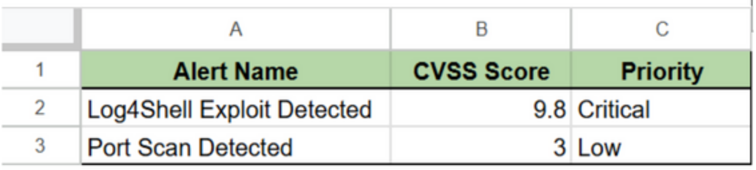


Alert ID	Type	Priority	MITRE Tactic
1	Phishing	High	T1566

Alert classification table mapping phishing alerts to MITRE ATT&CK.

Alert Prioritization Using CVSS

Alerts were prioritized using CVSS scores to assess severity and potential impact. High-risk vulnerabilities were assigned higher priority to ensure faster response.

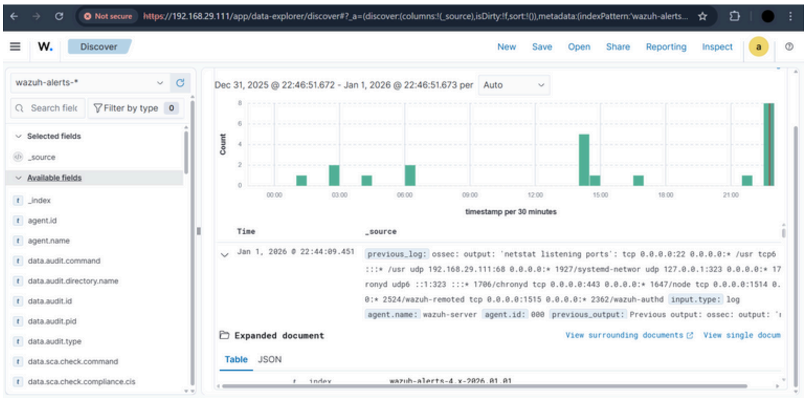


Alert Name	CVSS Score	Priority
Log4Shell Exploit Detected	9.8	Critical
Port Scan Detected	3	Low

CVSS-based alert prioritization.

Wazuh Alert Detection

Alerts were monitored and analyzed using the Wazuh SIEM platform. The alerts were observed through the Discover view, confirming successful ingestion and detection of security events.



```
https://192.168.29.111/app/data-explorer/discover#?_a=(discover:(columns:!(_source),isDirty:!f,sort:!()),metadata:(indexPattern:'wazuh-alerts...
```

Dec 31, 2025 @ 22:46:51.672 - Jan 1, 2026 @ 22:46:51.673 per Auto

```
Time                      _source
Jan 1, 2026 @ 22:44:09.451  previous_log: ossec: output: 'netstat listening ports': tcp 0.0.0.0:22 0.0.0.0:* /usr tcp6
                          :::* /usr udp 192.168.29.111:68 0.0.0.0:* 1927/systemd-networ udp 127.0.0.1:323 0.0.0.0:* 17
                          ronyd udp6 ::1:323 :::* 1706/chronyd tcp 0.0.0.0:443 0.0.0.0:* 1647/node tcp 0.0.0.0:1514 0.
                          0:* 2524/wazuh-remoted tcp 0.0.0.0:1515 0.0.0.0:* 2362/wazuh-authd input.type: log
                          agent.name: wazuh-server agent.id: 000 previous_output: Previous output: ossec: output: 'ı
```

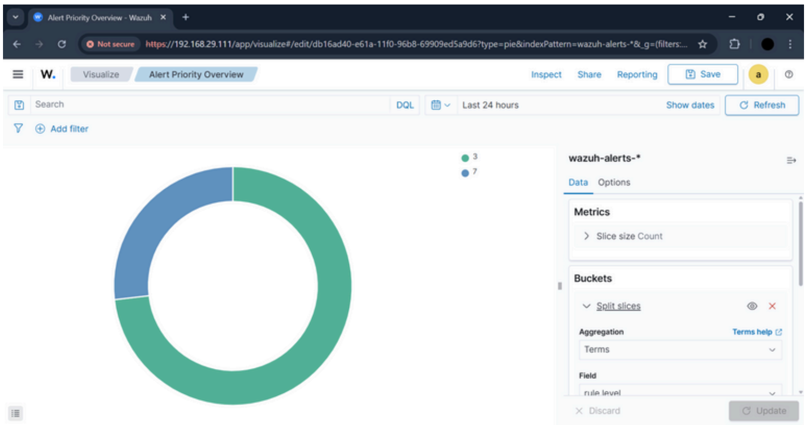
Expanded document

```
t  _index        wazuh-alerts-4.x-2026.01.01
```

Alerts detected and analyzed in Wazuh.

Wazuh Dashboard Creation

A dashboard was created in Wazuh to visualize alert priorities. A pie chart was used to display the distribution of alerts based on severity levels, providing quick situational awareness.



```
https://192.168.29.111/app/visualize#/edit/db16ad40-e61a-11f0-96b8-69909ed5a9d6?type=pie&indexPattern=wazuh-alerts-*&_g=(filters:...
```

Metrics: Slice size Count

Buckets: Split slices

Aggregation: Terms

Field: rule.level

Alert priority visualization dashboard in Wazuh.

Incident Ticket (TheHive)

An incident ticket was drafted in TheHive to document a critical security alert.

Incident Ticket Details:

- Title: [Critical] Ransomware Detected on Server-X
- Description: Indicators include suspicious executable file crypto_locker.exe and source IP 192.168.1.50.
- Priority: Critical
- Assignee: SOC Analyst

Escalation Email

Subject: Escalation – Critical Ransomware Alert Detected

A critical ransomware alert was detected on Server-X indicating the presence of a suspicious executable file, crypto_locker.exe, originating from IP address 192.168.1.50. Immediate containment actions have been initiated. Due to the severity of the incident and potential business impact, this alert is being escalated to Tier 2 for further investigation and response. Please review the incident details and advise on next steps.

Key Learning

This task improved understanding of alert classification, priority assignment using CVSS, dashboard-based monitoring, and escalation procedures in SOC operations.