Threat Intelligence Integration

Objective

This task focuses on integrating threat intelligence into SOC operations. The objective is to import threat feeds, enrich security alerts with intelligence context, and perform threat hunting using SIEM and case management tools.

Tools Used

- Wazuh – SIEM for alert generation and log analysis
- AlienVault OTX – Threat intelligence platform (IOC feeds)
- TheHive – Incident and case management
- Google Sheets / Markdown – Documentation

Task Overview

1. Threat Feed Import (AlienVault OTX → Wazuh)

Purpose:

Automatically detect known malicious indicators by matching logs against threat intelligence feeds.

Activity Performed:

- Integrated **AlienVault OTX threat feed** with Wazuh
- Enabled IOC matching for malicious IP addresses
- Tested detection using a **mock IP address**

Test IOC:

192.168.1.100

SOC Insight:

Threat feeds allow SOC teams to quickly identify known malicious infrastructure such as C2 servers, botnets, and scanners.

2. Alert Enrichment with Threat Intelligence

Purpose:

Add **reputation and context** to raw security alerts.

Enrichment Performed:

- Queried AlienVault OTX for IP reputation
- Enriched Wazuh alert with threat intelligence details

- Linked alert to known malicious activity

Enriched Alert Documentation:

Alert ID	IP	Reputation	Notes
003	192.168.1.100	Malicious (OTX)	Linked to C2 server

SOC Value:
Enrichment reduces investigation time by providing immediate context about the threat's severity and known behavior.

3. Threat Hunting (MITRE ATT&CK – T1078: Valid Accounts)

Purpose:
Proactively search for signs of **account misuse** rather than waiting for alerts.

MITRE Technique:

- **T1078 – Valid Accounts**

Hunting Query (Example):
user.name != "system"

Hunting Logic:

- Identify login activity from non-system accounts
- Review unusual login times or sources
- Detect potential compromised or abused credential

SOC Insight:
Threat hunting helps uncover stealthy attacks that bypass automated alerts, especially credential-based compromises.

Summary (50 Words)

Threat intelligence integration enhanced detection by matching Wazuh alerts with AlienVault OTX indicators. A malicious IP was identified and enriched with reputation data, confirming C2 activity. Threat hunting for MITRE T1078 revealed suspicious account usage, demonstrating proactive detection beyond signature-based alerts.