Alert Triage with Threat Intelligence

Objective

This task focuses on **alert triage**, a core SOC Tier-1 responsibility. The objective is to analyze security alerts, determine their priority, and validate associated **Indicators of Compromise (IOCs)** using external **threat intelligence platforms**.

Tools Used

- **Wazuh** – Alert detection and log analysis
- **VirusTotal** – File, IP, and hash reputation analysis
- **AlienVault OTX** – Threat intelligence and IOC correlation
- **Google Sheets / Markdown** – Documentation

Task Overview

1. Triage Simulation (Wazuh Alert Analysis)

Purpose:

Quickly assess whether an alert represents a real security threat or a false positive.

Mock Alert Details:

- Alert Type: Suspicious PowerShell Execution
- Source IP: 192.168.1.101
- Detection Tool: Wazuh

Alert Triage Table:

Alert ID	Description	Source IP	Priority	Status
004	PowerShell Execution	192.168.1.101	High	Open

SOC Triage Decision:

PowerShell is frequently abused by attackers for fileless malware and lateral movement. The alert was classified as **High priority** pending IOC validation.

2. IOC Validation (VirusTotal & AlienVault OTX)

Purpose:

Confirm whether the alert is **malicious or benign** using threat intelligence.

Validation Performed:

- Queried **VirusTotal** for IP reputation
- Cross-referenced the same IP in **AlienVault OTX**

- Checked for links to malware, C2 infrastructure, or prior campaigns

IOC Tested:

`192.168.1.101`

SOC Insight:
Threat intelligence correlation strengthens confidence in triage decisions and reduces false positives.

Summary (50 Words)

Alert triage identified a high-priority PowerShell execution event requiring further investigation. IOC validation using VirusTotal and AlienVault OTX revealed suspicious reputation indicators, increasing confidence in malicious activity. The alert remains open for escalation and response, demonstrating effective SOC triage and threat intelligence-driven decision-making.