Alert Triage with Automation

Activities

- Alert triage and enrichment
- Automated threat intelligence validation

Tools Used

- Wazuh – Alert generation and monitoring
- TheHive – Incident management and automation
- VirusTotal – File hash reputation check

Task 1: Triage Simulation (Mock Alert Analysis)

A simulated alert was analyzed in Wazuh for a suspicious file download detected on an internal system.

Alert Documentation

Alert ID	Description	Source IP	Priority	Status
005	Suspicious File Download	192.168.1.102	High	Open

Triage Actions

- Verified alert source and affected host
- Identified unusual outbound file download behavior
- Classified alert as High Priority due to potential malware risk
- Escalated for threat intelligence validation

Task 2: Automated Validation with Threat Intelligence

Automation Workflow

1. Alert forwarded from Wazuh to TheHive
2. File hash extracted from alert artifact
3. TheHive automatically queries VirusTotal
4. Reputation results attached to incident
5. Analyst reviews verdict for response decision

Threat Intelligence Summary (50 Words)

The suspicious file hash was automatically analyzed using VirusTotal via TheHive integration. VirusTotal reported multiple detections from reputable antivirus engines, classifying the file as malicious. Based on enriched threat intelligence, the alert was confirmed as a true positive, requiring immediate containment and host isolation.