Alert Triage with Threat Intelligence (Mock Simulation)

Objective

The objective of this task was to simulate alert triage in a SOC environment and demonstrate the analyst workflow for prioritization and IOC validation using threat intelligence platforms.
Alert Triage

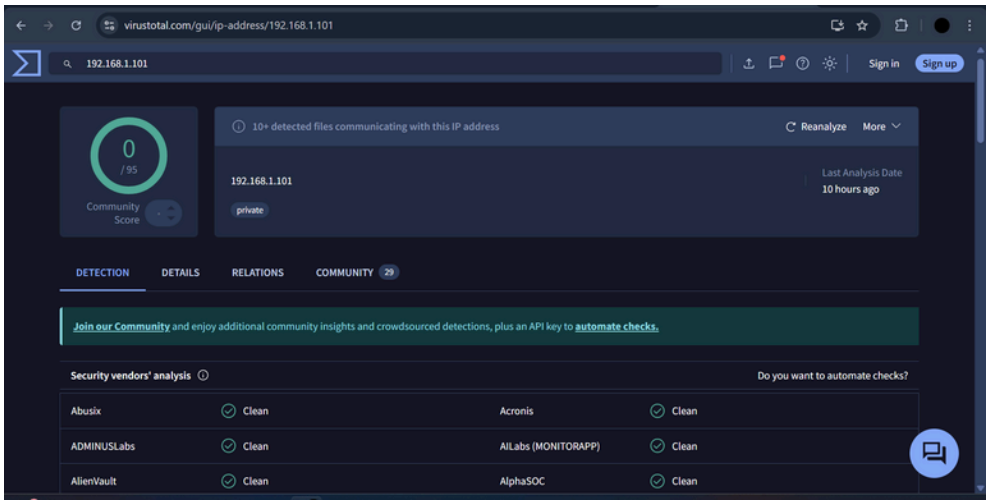
A mock Wazuh alert representing suspicious PowerShell execution was analyzed as part of this exercise.

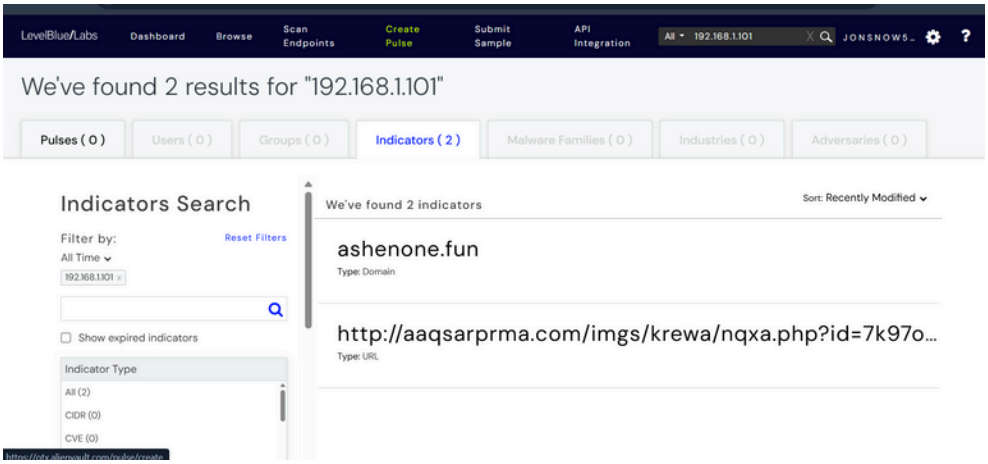
Alert ID	Description	Source IP	Priority	Status
4	PowerShell Execution	192.168.1.101	High	Open

The alert was intentionally simulated to practice triage decision-making and alert documentation.

IOC Validation

The source IP address (192.168.1.101) was analyzed using threat intelligence platforms:
VirusTotal: The IP address is a private IP with no detections reported by security vendors.
AlienVault OTX: No active pulses or confirmed malicious reputation were associated with the IP.





Analysis Summary

This mock alert was analyzed as High priority due to suspicious PowerShell execution behavior. IOC validation was performed using VirusTotal and AlienVault OTX. The source IP is a private address and did not show confirmed malicious reputation. The alert remains open for monitoring as part of the simulated SOC workflow. This mock exercise demonstrates standard SOC alert triage and IOC validation workflow.Given the absence of confirmed malicious indicators, the alert was kept open for monitoring rather than escalation.