



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.

The screenshot shows the VirusTotal analysis page for the IP address 192.168.1.101. The main summary card indicates 0 detections from 10+ files. The IP is listed as 'private'. Below the card, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY (29). The DETECTION tab displays a table of security vendor analysis results. The table includes columns for vendor (Abusix, ADMINUSLabs, AlienVault, Acronis, AllLabs (MONITORAPP), AlphaSOC) and status (all show 'Clean'). A green bar at the bottom of the table area encourages users to join the community and automate checks. The overall interface is dark-themed.



The screenshot shows the CYART web application interface. At the top, there is a navigation bar with links: LevelBlue/Labs, Dashboard, Browse, Scan Endpoints, Create Pulse, Submit Sample, API Integration, and a search bar set to 'All' and '192.168.1.101'. Below the navigation bar, a message says 'We've found 2 results for "192.168.1.101"'. A horizontal menu bar below the message includes 'Pulses (0)', 'Users (0)', 'Groups (0)', 'Indicators (2)', 'Malware Families (0)', 'Industries (0)', and 'Adversaries (0)'. The main content area is titled 'Indicators Search' and displays the results for 'ashenone.fun' (Type: Domain). It includes a URL entry field with the value 'http://aaqsarprma.com/imgs/krewa/nqxa.php?id=7k97o...'. On the left side, there is a sidebar with filter options: 'Filter by' dropdown set to 'All Time', a search input field containing '192.168.1.101', a 'Reset Filters' button, a checkbox for 'Show expired indicators', and a 'Indicator Type' dropdown with options 'All (2)', 'CIDR (0)', and 'CVE (0)'.

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.