Alert Triage Practice

This document provides a mock exercise in alert triage practice, simulating the workflow of a SOC analyst. The purpose is to demonstrate how alerts are classified, prioritized, investigated, and validated using open-source tools such as Wazuh, VirusTotal, and AlienVault OTX. All examples, alerts, and indicators of compromise (IOCs) included here are mock samples for educational use only and do not represent real-world data.

Alert Classification Table

Here's a mock sample table you can use:

Alert ID	Description	Source IP	Destination IP	Priority	Status	MITRE Tactic
001	Phishing Email Detected	203.0.113.15	192.168.1.25	High	Open	Initial Access (T1566)
002	Brute-force SSH Attempts	192.168.1.100	192.168.1.10	Medium	Open	Credential Access (T1110)
003	Port Scan Detected	198.51.100.20	192.168.1.50	Low	Closed	Discovery (T1046)
004	Ransomware Behavior	192.168.1.150	192.168.1.60	Critical	Escalated	Impact (T1486)

Threat Intelligence Validation

For this part, we simulate using AlienVault OTX and VirusTotal to validate an IOC from our alert table. Let's take the Brute-force SSH Attempts (Alert ID: 002) with source IP `192.168.1.100` as an example.
Validation Example:

- Checked `192.168.1.100` on AlienVault OTX → flagged in a community pulse as associated with brute-force activity.
- Cross-checked with VirusTotal → no known malware linked, but IP shows repeated failed authentication attempts in public datasets.

Summary: The source IP `192.168.1.100` was confirmed in AlienVault OTX as being involved in brute-force activity, validating the alert as a true positive. VirusTotal did not show malware but confirmed suspicious behavior. This demonstrates the importance of enriching alerts with threat intelligence before escalation.

Final Triage Report

Triage Summary:
During the simulated triage exercise, we analyzed a mock alert related to brute-force SSH

attempts originating from IP `192.168.1.100`. The alert was classified as **Medium Priority** and initially left open for investigation.

Threat Intelligence Findings:

- **AlienVault OTX:** Identified the IP as part of a brute-force campaign reported by multiple contributors.
- **VirusTotal:** No associated malware, but suspicious repeated authentication activity noted in logs.

Decision:
The alert was validated as a **true positive** and should be escalated to Tier 2 SOC analysts for further action, such as blocking the IP at the firewall and monitoring for lateral movement.

Key Takeaways:
This exercise demonstrates several important aspects of SOC alert triage:

- **Threat intelligence enrichment is critical** – combining alerts with sources like OTX and VirusTotal helps confirm whether activity is malicious or benign.
- **Not all alerts show direct malware evidence** – in this case, no malware was linked, but repeated brute-force attempts still confirmed hostile intent.
- **Escalation decisions rely on context** – even with limited indicators, context from threat feeds and system logs guided the decision to escalate.
- **Efficiency in triage saves time** – validating alerts early reduces false positives and ensures SOC analysts focus on real threats.