ALERT TRIAGE REPORT

1. Introduction

Alert triage is a critical Security Operations Centre (SOC) process that involves analyzing and prioritizing security alerts based on severity, impact, and risk level. The purpose of alert triage is to distinguish genuine security incidents from false positives and ensure efficient incident response.

This practical demonstrates the alert triage process using simulated security alerts modeled on industry-standard frameworks including Wazuh SIEM alert structures, MITRE ATT&CK attack techniques, and Common Vulnerability Scoring System severity scoring methodology. The triage workflow follows incident handling principles defined by National Institute of Standards and Technology SP 800-61 guidelines.

The objective is to evaluate alerts, identify real threats, classify severity, and determine appropriate response actions.

---

2. Objective

- To understand alert triage workflow.
- To analyze and validate security alerts.
- To differentiate true positives from false positives.
- To prioritize alerts based on severity.
- To recommend response actions.

---

3. Alert Triage Workflow

The alert triage process consists of the following steps:

3.1 Alert Collection

- Security alerts generated from log monitoring systems.
- Detection of suspicious activities and abnormal behavior.

3.2 Alert Validation

- Verify authenticity of alert.
- Check system logs and event details.
- Identify false positives.

3.3 Threat Classification

- Map alerts to attack techniques.
- Identify potential impact.
- Assign severity level.

3.4 Prioritization

- Rank alerts based on risk.
- Determine response urgency.

3.5 Escalation

- Forward critical alerts to incident response team.

---

4. Alert Data Analysis

Security alerts were analyzed based on event logs, authentication records, and system activity.

Sample Alert Records

Alert ID	Alert Type	Description	Initial Severity
AT-001	Failed Login Attempts	Multiple authentication failures detected	Medium
AT-002	Malware Alert	Suspicious file execution	High
AT-003	Unauthorized Access	Privilege escalation detected	High
AT-004	Network Anomaly	Unusual outbound traffic	Medium
AT-005	Suspicious Email	Possible phishing attempt	Low

---

5. Alert Validation Process

Each alert was validated using the following checks:

- Verification of log source.

- Analysis of timestamp and activity pattern.
- Comparison with baseline system behaviour.
- Cross-checking event frequency.

Validation Results

Alert ID	Validation Status	Result
AT-001	True Positive	Confirmed brute force activity
AT-002	True Positive	Malicious file detected
AT-003	True Positive	Unauthorized privilege escalation
AT-004	False Positive	Normal network backup traffic
AT-005	Suspicious	Requires monitoring

6. Threat Classification Using Attack Techniques

Alerts were mapped to standardized attack behaviors.

Alert ID	Technique ID	Attack Technique
AT-001	T1110	Brute Force Authentication
AT-002	T1059	Command Execution
AT-003	T1078	Valid Account Abuse
AT-005	T1566	Phishing

7. Alert Severity Reassessment

After validation, severity levels were reassessed based on impact and likelihood.

Alert ID	Initial Severity	Final Severity
AT-001	Medium	High
AT-002	High	Critical
AT-003	High	High
AT-004	Medium	Low
AT-005	Low	Medium

8. Alert Prioritization

Alerts were prioritized according to risk level and required response urgency.

Priority Levels

- **Critical** — Immediate response required.
- **High** — Urgent investigation required.

- **Medium** — Monitoring required.
- **Low** — Informational alert.

Final Priority Assignment

Alert ID	Priority Level	Action Required
AT-002	Critical	Immediate incident response
AT-001	High	Investigate authentication logs
AT-003	High	Verify user privileges
AT-005	Medium	Monitor email activity
AT-004	Low	No action required

---

9. Response Recommendations

Based on alert analysis, the following actions were recommended:

- Block suspicious IP addresses.
- Reset compromised credentials.
- Remove malicious files.
- Enable stronger authentication mechanisms.
- Monitor suspicious activities continuously.

---

10. Challenges in Alert Triage

- Large volume of alerts.
- Identification of false positives.
- Time constraints in analysis.
- Accurate threat classification.

Proper triage reduces alert fatigue and improves response efficiency.

---

11. Conclusion

The alert triage process enabled effective identification and prioritization of security threats. The practical demonstrated systematic evaluation of alerts through validation, classification, and severity assessment. The implementation followed industry-standard SOC procedures and improved understanding of threat analysis and response prioritization.