Alert Priority Levels and Severity Assessment Report

1. Objective

The objective of this practical is to understand alert prioritization in a Security Operations Center (SOC) environment by analyzing security alerts, evaluating risk severity, and assigning appropriate priority levels based on standardized cybersecurity frameworks. The practical demonstrates how security analysts classify alerts using vulnerability scoring, asset criticality, and threat impact to ensure efficient incident response.

---

2. Introduction

A Security Operations Center (SOC) continuously monitors organizational systems to detect, analyze, and respond to cybersecurity threats. Modern security monitoring tools generate large volumes of alerts, making it necessary to prioritize incidents based on severity and business impact. Alert prioritization helps analysts identify critical threats, reduce response time, and prevent potential security breaches.

Alert prioritization involves evaluating threat impact, exploit likelihood, asset importance, and vulnerability severity. Standardized frameworks provide structured methods to assess risk and classify incidents consistently.

This practical uses simulated security alert datasets generated for SOC training purposes. The data is modeled based on industry-standard cybersecurity frameworks including Wazuh SIEM alert structures, Common Vulnerability Scoring System severity scoring methodology, and incident handling guidance from National Institute of Standards and Technology SP 800-61. The simulation replicates real-world security incidents such as brute-force attacks, malware detection, and unauthorized access attempts to demonstrate alert prioritization processes in a controlled environment.

---

3. Alert Prioritization in SOC

Alert prioritization is the process of ranking detected security events based on their potential impact and urgency. Proper prioritization ensures that critical incidents are addressed immediately while lower-risk alerts are monitored or reviewed later.

3.1 Importance of Alert Prioritization

- Reduces incident response time
- Prevents security breaches
- Improves resource allocation
- Minimizes false positives
- Enhances organizational security posture

---

4. Priority Level Classification

Security alerts are categorized into different priority levels based on risk severity and impact.

4.1 Critical Priority

- Immediate response required
- Active exploitation detected
- Severe system or data compromise possible
- Examples: ransomware attack, remote code execution

4.2 High Priority

- Unauthorized access attempts
- Privilege escalation activity
- Significant security risk

4.3 Medium Priority

- Suspicious behavior
- Potential indicators of compromise
- Requires monitoring and investigation

4.4 Low Priority

- Informational alerts
- Minimal security impact
- Logged for auditing purposes

Alert Priority Levels

Priority Level	Description	Response Requirement
Critical	Severe threat with major impact	Immediate action
High	High-risk activity	Urgent investigation
Medium	Suspicious behaviour	Scheduled analysis
Low	Informational event	Monitoring only

---

5. Alert Assignment Criteria

SOC analysts determine alert priority using multiple factors.

5.1 Asset Criticality

- Production servers → higher priority
- Test environments → lower priority

5.2 Exploit Likelihood

- Public exploit availability increases severity
- Known vulnerabilities increase risk

5.3 Business Impact

- Financial loss risk
- Data breach impact
- Service disruption

5.4 Threat Intelligence Correlation

- Known malicious IP addresses
- Malware signatures
- Attack indicators

---

6. Vulnerability Severity Assessment Using CVSS

The Common Vulnerability Scoring System (CVSS) provides a standardized method to assess vulnerability severity using numerical scores ranging from 0 to 10. The scoring system evaluates exploitability, impact, and environmental factors.

6.1 CVSS Severity Ratings

Score Range	Severity Level
9.0 – 10.0	Critical
7.0 – 8.9	High
4.0 – 6.9	Medium
0 – 3.9	Low

6.2 Example Vulnerability Analysis

CVE ID	Description	CVSS Score	Severity
CVE-2021-44228	Apache Log4j Remote Code Execution	9.8	Critical
CVE-2017-0144	SMB Vulnerability	8.1	High
CVE-2020-0601	Windows CryptoAPI Spoofing	6.5	Medium

CVSS scoring enables consistent risk evaluation and helps prioritize vulnerability remediation.

---

7. SIEM Alert Dataset Analysis

Security alerts were analyzed to simulate monitoring activity in a SOC environment.

Sample Security Alert Records

Alert ID	Event Description	Source IP	Severity	Assigned Priority
WZ001	SSH brute-force attack detected	192.168.1.10	Medium	Medium
WZ002	Malware signature detected	192.168.1.22	Critical	Critical
WZ003	Multiple failed login attempts	192.168.1.33	Medium	Medium
WZ004	Suspicious file hash detected	192.168.1.44	High	High
WZ005	Port scanning activity	192.168.1.55	Low	Low
WZ006	Privilege escalation attempt	192.168.1.66	High	High
WZ007	Ransomware behaviour detected	192.168.1.77	Critical	Critical
WZ008	SQL injection attempt	192.168.1.88	High	High
WZ009	Unusual outbound traffic	192.168.1.99	Medium	Medium
WZ010	Unauthorized administrator login	192.168.1.20	Critical	Critical

Observations

- Repeated login failures indicate brute-force attempts.
- Malware and ransomware alerts represent critical threats.
- Privilege escalation indicates potential system compromise.
- Network anomalies suggest possible data exfiltration.

---

8. Risk Assessment and Findings

The analysis identified multiple security risks:

- Unauthorized system access
- Malware execution
- Credential compromise
- Network intrusion attempts
- Data exfiltration risk

Critical and high-priority alerts require immediate investigation to prevent system compromise.

---

9. Recommendations

- Implement multi-factor authentication.
- Perform regular vulnerability patching.
- Monitor network traffic continuously.
- Deploy intrusion detection systems.
- Improve access control mechanisms.

---

10. Conclusion

This practical demonstrated the process of alert prioritization and severity assessment in a SOC environment using standardized frameworks and simulated security alerts. Proper prioritization improves incident response efficiency, reduces organizational risk, and enhances overall cybersecurity posture.