Introduction

Clear and concise documentation is essential for efficient security operations, particularly in the high-stakes environment of incident response. This guide provides a foundational reference for **Security Operations Center (SOC) Analysts** on standardizing alert prioritization, incident classification, and executing the response lifecycle, The ultimate purpose is to ensure consistent, timely, and effective handling of all security events.

1. Alert Priority Levels

Alert prioritization determines the order in which security events are addressed, based on **impact** and **urgency.**

- **Priority Definitions:** Severity is typically categorized as **Critical, High, Medium,** or **Low,** often mapped to the potential consequences of an event, such as a data breach or service disruption. For instance, **Critical** denotes events like active *ransomware encryption,* while **High** might cover *unauthorized admin access.*
- **Assignment Criteria:** Prioritization relies on factors like **asset criticality** (e.g., production server vs. test VM), **exploit likelihood** (e.g., a known CVE with a public exploit), and **business impact** (e.g., financial loss).
- **Scoring Systems:** The **Common Vulnerability Scoring System (CVSS)** is mastered for risk quantification, where a score, such a 9.8 for *Log4shell (CVE-2021-44228),* is mapped to a **Critical** priority SOC tools like *Spluck's risk scoring* are also explored for automated prioritization.

1.2. Incident Classification

Classification involves categorizing and enriching security events to streamline the investigation process.

- **Incident Categories:** Events are classified by **type,** such as **malware, phishing, DDoS,** *insider threats* (e.g., unauthorized data export), or **data exfiltration.**
- **Taxonomy:** Frameworks like **MITRE ATT&CK** (e.g., *T1566-Phishng),* **ENISA Incident Taxonomy,** and **VERIS** (Vocabulary for Event Recording and Incident Sharing) framework provide standardized labeling for security events.

- **Contextual Metadata:** Incidents must be enriched with details, or **metadata,** including affected systems, timestamps, source IPs, and **Indicators of Compromise (IOC)** (e.g., a *malicious hash).*

1.3. Basic Incident Response

The response process follows a structured **Incident Lifecycle** to ensure a comprehensive and recoverable resolution.

- **Incident Lifecycle:** The six phases are: **Preparation** (e.g., playbooks), **Identification** (e.g., alert triage), **Containment** (e.g., isolate systems), **Eradication** (e.g., remove malware), **Recovery** (e.g., restore services), and **Lessons Learned** (e.g., post-mortem).
- **Procedures:** Key procedures include **system isolation, evidence preservation** (e.g., memory dumps), *communication protocols,* and leveraging **SOAR** (Security Orchestration, Automation, and response) tools like *Splunk Phantom* for workflow orchestration.

2. Alert Triage and Management Practice

Alerts are mapped to MITRE ATT&CK techniques in a system like Google Sheets:

Alert ID	**Type**	**Priority**	**MITRE Tactic**
001	Phishing	**HIGH**	T1566
003	Malware	**Critical**	T1567

2.1.2 Incident Ticket Draft

A ticket is drafted in **TheHive** to initiate the formal response process:

- **Title: [Critical]** Ransomware Detected on Server-X
- **Description:** Indicators: **[File: *crypto_locker.exe*], [IP:** 192.168.1.50**]**
- **Priority: Critical**
- **Assignee:** SOC Analyst

2.2 Response Documentation and Evidence

Documentation is critical for tracking actions, maintaining the **chain of custody,** and conducting post-incident analysis.

2.2.1 Investigation Steps Log

All actions taken during **Containment** and **Eradication** are logged with timestamps:

Timestamp	**Action**
2025-11-22 14.00.00	**Isolated endpoint**
2025-11-22 14.00.30	**Collected memory dump**

2.2.2. Evidence Preservation Record

Documentation of preserved evidence (e.g., using **Velociraptor** or **FTK Imager**) is vital for forensic analysis:

Item	**Description**	**Collected By**	**Date**	**Hash Value**
Memory Dump	Server-X Dump	SOC Analyst	2025-08-18	SHA256

2.3 Capstone Project

This scenario simulates a complete incident from attack to reporting, utilizing tools like **Metasploit, Wazuh,** and **CrowdSec.**

2.3.1 Detection and Triage Log

A log of the initial detection and classification of the simulated attack (e.g., exploiting a *vsftpd backdoor* ***):***

Timestamp	**Source IP**	**Alert Description**	**MITRE Technique**
2025-11-22 11:00:00	192.168..XX.XX	**VSFTPD exploit**	T1190

2.3.2 Stakeholder Briefing

A draft briefing for a non-technical manager summarizes the incident clearly, ensuring direct and clear communication:

"At 11:00 AM, our systems detected a **critical** exploit on Server-X, specifically an attempted takeover using a known *VSFTPD vulnerability*. The incident was immediately contained. We successfully isolated the affected server and utilized **CrowdSec** to permanently block the attacker's IP from our network perimeter. A full forensic investigation and system rebuild is underway to ensure the threat is fully eradicated and that business services can be fully recovered as quickly as possible. The *Containment* phase is complete."

Summary

The successful management of security events relies on the consistent application of **standardized criteria** for alert prioritisation (**CVSS**), proper **classification** (using frameworks like **MITRE ATT&CK**), and strict adherence to the **Incident Response Lifecycle.** Through continuous practice with tools like **Wazuh, TheHive,** and **Velociraptor,** SOC Analysts develop the essential skills to efficiently detect, contain, and revolver from sophisticated threats, ensuring minimal business impact.