Incident Classification and Categorization Report

1. Objective

The objective practical is to understand incident classification in a Security Operations Centre (SOC) environment by identifying different types of security incidents, categorizing them using standardized frameworks, and enriching incidents with contextual metadata. This process helps security analysts efficiently investigate threats, improve response accuracy, and maintain structured security monitoring.

---

2. Introduction

Incident classification is a fundamental activity in Security Operations Centre (SOC) operations. It involves identifying the nature of a security event, categorizing it into predefined incident types, and mapping it to recognized cybersecurity frameworks. Proper classification helps analysts understand attack patterns, determine response strategies, and maintain consistent documentation.

In real-world environments, organizations use standardized incident classification frameworks to ensure consistency in threat identification and reporting. These frameworks help analysts categorize incidents such as malware attacks, phishing attempts, denial-of-service attacks, insider threats, and data breaches.

This practical uses simulated incident datasets modeled using industry-standard frameworks including MITRE ATT&CK for attack technique mapping, ENISA incident taxonomy for structured classification, and VERIS for standardized incident recording. The simulation replicates real-world security incidents such as phishing attacks, unauthorized access, and malware infections to demonstrate incident classification procedures in a controlled SOC environment.

---

3. Importance of Incident Classification

Incident classification plays a critical role in security monitoring and incident response.

Key Benefits:

- Enables faster threat identification

- Improves incident response efficiency
- Standardizes reporting procedures
- Supports threat intelligence analysis
- Enhances forensic investigations
- Helps identify attack patterns and trends

Proper classification ensures consistent communication between SOC analysts and security teams.

---

4. Types of Security Incidents

Security incidents can be categorized into different types based on the nature of the attack or threat behaviour.

4.1 Malware Incidents

Malicious software designed to disrupt, damage, or gain unauthorized access to systems.

Examples:

- Ransomware
- Trojans
- Spyware
- Worms

4.2 Phishing Attacks

Fraudulent attempts to obtain sensitive information through deceptive emails or websites.

Indicators:

- Suspicious links
- Fake login pages
- Email spoofing

4.3 Distributed Denial of Service (DDoS)

Attempts to disrupt service availability by overwhelming systems with traffic.

Indicators:

- Sudden traffic spikes
- Service unavailability
- Network congestion

4.4 Insider Threats

Security risks originating from authorized users misusing privileges.

Examples:

- Unauthorized data access
- Data leakage
- Privilege abuse

4.5 Unauthorized Access

Attempts to gain system access without proper authentication.

Indicators:

- Multiple failed login attempts
- Privilege escalation
- Unusual login patterns

Incident Categories

Incident Type	Description	Risk Level
Malware	Malicious software execution	High
Phishing	Social engineering attack	Medium
DDoS	Service disruption attack	High
Insider Threat	Internal misuse of privileges	High
Unauthorized Access	Unauthorized login activity	Medium

5. Incident Classification Frameworks

Standardized frameworks provide structured methods for incident classification and investigation.

5.1 MITRE ATT&CK Framework

MITRE ATT&CK provides a knowledge base of adversarial tactics and techniques observed in real-world cyberattacks. It helps analysts map security incidents to specific attack behaviors.

Examples of Techniques:

Technique ID	Technique Name	Description
T1566	Phishing	Credential harvesting through email
T1110	Brute Force	Password guessing attacks
T1059	Command Execution	Execution of malicious commands
T1190	Exploit Public-Facing Application	External system exploitation
T1078	Valid Accounts	Misuse of legitimate credentials

5.2 ENISA Incident Taxonomy

ENISA provides a structured classification model for cybersecurity incidents based on attack type, impact, and affected assets. It supports consistent incident reporting across organizations.

Classification Areas:

- Malware incidents
- Network attacks
- Unauthorized access
- Data breaches
- Service disruption

5.3 VERIS Framework

VERIS provides a standardized format for describing security incidents by recording:

- Threat actor
- Attack method
- Impact
- Assets affected

This framework improves incident documentation and threat intelligence sharing.

6. Incident Metadata and Contextual Information

SOC analysts enrich incidents with contextual metadata to improve investigation accuracy.

6.1 Key Metadata Fields

- Timestamp of event
- Source IP address
- Destination system
- File hash
- User account involved
- Indicators of Compromise (IOCs)

Proper metadata collection helps correlate security events and identify attack sources.

---

7. Simulated Incident Dataset Analysis

A simulated incident dataset was analyzed to demonstrate classification procedures.

Sample Incident Records

Incident ID	Incident Type	Source IP	Affected System	MITRE Technique	Status
INC001	Phishing Email	192.168.1.10	User Workstation	T1566	Investigating
INC002	Brute-force Login	192.168.1.20	Authentication Server	T1110	Open
INC003	Malware Detection	192.168.1.30	File Server	T1059	Contained
INC004	Unauthorized Access	192.168.1.40	Database Server	T1078	Open
INC005	SQL Injection	192.168.1.50	Web Server	T1190	Investigating
INC006	Insider Data Transfer	Internal User	File System	T1078	Open
INC007	Ransomware Activity	192.168.1.60	Production Server	T1059	Critical
INC008	Suspicious Network Traffic	192.168.1.70	Firewall	T1046	Monitoring
INC009	Credential Harvesting	192.168.1.80	User Account	T1566	Investigating

8. Analysis and Findings

The analysis revealed:

- Phishing attacks targeting user credentials
- Unauthorized access attempts to sensitive systems
- Malware execution on critical servers
- Privilege escalation activities
- Suspicious network behavior indicating potential intrusion

Mapping incidents to standardized frameworks improved threat visibility and investigation accuracy.

---

9. Recommendations

- Implement strong authentication controls.
- Conduct security awareness training to prevent phishing.
- Monitor privileged account activities.
- Deploy endpoint detection solutions.
- Maintain incident classification standards.

---

10. Conclusion

This practical demonstrated incident classification techniques in a SOC environment using standardized frameworks and simulated security data. Proper incident classification improves threat detection accuracy, supports efficient incident response, and enhances organizational cybersecurity posture.