SOC Week 2 – Notes

Prepared by: Kartheek

Introduction

This document provides the details about theoretical and practical knowledge acquired during Week 2 task. It covers essential cybersecurity principles including alert management practice, response documentation, alert triage practice, evidence preservation, and capstone project.

1. Theoretical Knowledge

1.1 Alert Priority Levels

Alert prioritization ensures that analysts address the most critical threats first. Priorities are defined based on the severity and potential business impact.

Alert priority level types are:

• Critical – Active exploitation or severe business disruption (e.g., ransomware encryption)
• High – Unauthorized access or lateral movement within critical systems
• Medium – Suspicious but non-active threats requiring monitoring
• Low – Informational alerts or minimal risk activities

Factors such as asset criticality, exploit likelihood, and business impact determine the alert level. The CVSS (Common Vulnerability Scoring System) helps standardize risk quantification. For example, a CVSS 9.8 vulnerability (like Log4Shell) is classified as Critical.

1.2 Incident Classification

Incident classification provides a framework to categorize and handle different security incidents effectively.

Common Categories:

• Malware – System infection or backdoor activity
• Phishing – Social engineering attacks through deceptive emails
• DDoS – Denial of service attacks disrupting availability
• Insider Threat – Unauthorized access or data theft by employees
• Data Exfiltration – Sensitive data exfiltrated to external sources

Frameworks such as MITRE ATT&CK, ENISA, and VERIS are used to standardize classification. Example: MITRE ATT&CK T1566 corresponds to Phishing.

1.3 Basic Incident Response

Incident response is a structured approach to manage and mitigate security breaches.

Incident Response Phases:

1. Preparation – Develop playbooks, tools, and communication protocols.
2. Identification – Detect and confirm incidents through alert triage.

3. Containment – Isolate affected systems to prevent lateral spread.
4. Eradication – Remove root cause or malware.
5. Recovery – Restore systems and validate their functionality.
6. Lessons Learned – Conduct post-incident reviews for improvement.

2. Practical Application

2.1 Alert Management Practice

This alert management practice focuses on creating and prioritizing alerts using tools such as Wazuh, TheHive, and Google Sheets.

Steps:

• Creating an alert classification table mapping alerts to MITRE ATT&CK techniques.
• Assigning priorities using CVSS scores.
• Creating tickets in TheHive for each alert.
• Draft escalation emails summarizing incident details and indicators of compromise.

Example Table:

Alert ID	Type	Priority	MITRE Tactic
001	Phishing	High	T1566

2 Response Documentation

Response documentation ensures every step of an investigation is recorded for transparency and auditing.

Tasks:

• Creating a response template with Executive Summary, Timeline, Impact Analysis, and Lessons Learned.
• Maintaining investigation logs including timestamps and analyst actions.
• Developing a phishing response checklist (verifying headers, analyzing URLs, identifying affected users).

Example Log:

Timestamp	Action
2025-08-18 14:00	Isolated endpoint
2025-08-18 14:30	Collected memory dump

3 Alert Triage Practice

In triage, validation of alerts and identification of false positives will be done.

Threat intelligence platforms such as VirusTotal and AlienVault OTX assist in IOC validation.

Example Table:

Alert ID	Description	Source IP	Priority	Status
002	Brute-force SSH	192.168.1.100	Medium	Open

4 Evidence Preservation

Proper evidence preservation maintains data integrity and legal admissibility during investigations.

Key Steps:

• Use Velociraptor to collect volatile data (netstat, processes, memory).
• Acquire memory dumps and hash them using SHA256.
• Record collection metadata including collector name, date, and description.

Example Evidence Log:

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

5 Capstone Project

The capstone integrates all previous modules to simulate a real-world SOC workflow.

Tasks:

• Simulate an attack using Metasploit (e.g., vsftpd backdoor exploit).
• Detect attack via Wazuh and document alerts.
• Respond using CrowdSec to isolate compromised VMs and block IPs.
• Prepare a comprehensive incident report with executive summary and recommendations.

Example Table:

Timestamp	Source IP	Description	MITRE Technique
2025-08-18 11:00	192.168.1.100	VSFTPD exploit	T1190