Operational Workflow Report

1. Overview

This document describes the complete operational workflow followed during the Capstone.The workflow followed a structured sequence:

Reconnaissance → Exploitation → Detection → Triage → Containment → Documentation → Metrics → Root Cause Analysis → Reporting

2. Phase 1 – Infrastructure Preparation

Before initiating any attack, the SOC monitoring stack was prepared.

2.1 Log Ingestion Setup

- Filebeat was configured to monitor:
  /var/log/auth.log
- Filebeat forwarded logs to Elasticsearch.
- Elasticsearch indexed logs in near real time.
- Kibana was used to visualize and query log data.

This ensured that any authentication attempts or suspicious activity would be captured.

2.2 Response Layer Setup

CrowdSec was deployed to:

- Monitor authentication logs
- Detect malicious behavior patterns
- Apply IP ban decisions

This provided automated containment capability.

2.3 Case Management Setup

TheHive was deployed via Docker to simulate a SOC case management system.

This allowed:

- Case creation
- Observable tracking
- MITRE ATT&CK tagging
- Task assignment and documentation

3. Phase 2 – Attack (SSH Brute Force)

Date: 27 February 2026

3.1 Attack Execution

Multiple failed SSH login attempts were generated against the Ubuntu SOC VM to simulate a brute-force attempt.

The objective was to trigger:

- Log generation
- Detection via SIEM
- Automated response

4. Phase 3 – Detection in SIEM

4.1 Log Analysis

Authentication failures appeared in Kibana Discover.

Key indicators observed:

- Repeated failed login attempts
- Same source IP
- Short time interval between attempts

A Lens visualization was created to demonstrate the spike in failed authentication attempts.

4.2 Detection Timestamp

First malicious authentication event observed:

Feb 27, 2026 – 11:45:45 UTC

This timestamp marked the beginning of the incident lifecycle.

5. Phase 4 – Containment and Response

After confirming malicious behavior:

5.1 IP Identification

The source IP was extracted from logs.

5.2 Ban Execution

Decision verified using: sudo cscli decisions list

Containment Timestamp: Feb 27, 2026 – 11:51:15 UTC

This marked the response completion time.

6. Phase 5 – Exploitation (Samba Attack)

Date: 28 February 2026

A second controlled attack was performed against Metasploitable2.

6.1 Reconnaissance

Nmap scan executed:

nmap -sV -T3 192.168.64.6

Results revealed:

- Samba service running on ports 139 and 445
- Multiple vulnerable services exposed

6.2 Exploitation

Metasploit module used:

exploit/multi/samba/usermap_script

Configuration:

- RHOSTS set to Metasploitable2 IP
- Payload: cmd/unix/reverse

Result:

- Command shell session opened
- whoami returned root
- id confirmed root privileges

This demonstrated impact severity and successful compromise.

7. Phase 6 – Incident Triage & Case Documentation

TheHive was used to complete SOC documentation.

7.1 Case Creation

- Title: SSH Brute Force & Samba Exploitation Simulation
- Severity: High
- Status: Open → Resolved

7.2 Observables Added

- Source IP address
- Target IP address
- MITRE ATT&CK Mapping:
    - T1110 – Brute Force
    - T1210 – Exploitation of Remote Services

7.3 Task Workflow

Tasks created:

- Validate detection
- Confirm exploitation impact
- Apply containment
- Document metrics
- Perform RCA

8. Phase 7 – Metrics Calculation

Using recorded timestamps:

Initial Detection: 11:45:45
Containment: 11:51:15

Dwell Time:

5 minutes 30 seconds

MTTD:

~1 minute (log ingestion near real time)

MTTR:

~5 minutes

These metrics were calculated to give performance measurement in SOC operations.

9. Phase 8 – Root Cause Analysis

Using 5 Whys:

1. Why was the system compromised?
   Because vulnerable services were exposed.
2. Why were they exposed?
   No hardening baseline was applied.
3. Why was the hardening missing?
   No configuration enforcement policy.
4. Why no enforcement?
   Lack of predefined secure deployment standard.
5. Why no standard?
   Absence of governance in lab configuration.

Fishbone categories identified:

- Configuration
- Monitoring
- Network Exposure
- Process

10. Phase 9 – Adversary Emulation (Caldera)

Caldera server was successfully deployed and UI accessed.

However, full agent execution was limited due to:

- ARM64 architecture
- Sandcat binary compatibility
- Dependency constraints

Despite this, adversary behavior was simulated via Metasploit exploitation.

11. Overall SOC Workflow Representation

The complete operational lifecycle achieved:

Attack Simulation
↓
SIEM Detection
↓
Investigation & Log Correlation
↓
Case Creation in SOAR
↓
Containment via IP Ban
↓
Metrics Calculation
↓
Root Cause Analysis
↓
Executive Reporting

12. Conclusion

This project demonstrates a realistic SOC operational workflow under controlled lab conditions. The environment simulated both unsuccessful (brute-force) and successful (Samba exploitation) attack scenarios.

Despite resource and architecture limitations, detection, response, containment, documentation, and reporting objectives were fully achieved.