Comprehensive SOC Incident Response – Capstone Report

A comprehensive SOC simulation was conducted to evaluate detection, response, automation, analysis, and reporting capabilities across multiple security platforms. The exercise included attack simulation, adversary emulation, triage, containment, automation, root cause analysis, metrics calculation, and executive reporting.

Attack Simulation

A simulated exploitation was conducted against a vulnerable Metasploitable2 system using the Samba usermap script vulnerability via Metasploit. The exploit targeted improper input validation within the Samba service, representing a remote service exploitation scenario commonly observed in enterprise environments.

Adversary Emulation & Detection

MITRE Caldera was used to emulate adversary behavior aligned with **MITRE ATT&CK T1210 – Exploitation of Remote Services**. The emulated activity triggered monitoring alerts within the SIEM environment.

Timestamp	Source IP	Alert Description	MITRE Technique
2025-08-18 16:00:00	192.168.1.102	Samba exploit	T1210

Wazuh successfully detected abnormal service behavior and generated a High-priority alert.

Detection and Triage

The alert was triaged in TheHive and classified as High severity due to confirmed exploitation behavior. Log analysis validated abnormal process execution linked to the Samba service. The case was escalated for immediate containment.

Response and Containment

The affected virtual machine was isolated from the network to prevent lateral movement. The attacker IP (192.168.1.102) was blocked using CrowdSec enforcement. Connectivity tests confirmed containment effectiveness.

SOAR Automation

A playbook was triggered to automatically:

1. Extract malicious IP
2. Validate reputation
3. Block IP via CrowdSec
4. Create TheHive case

Automation successfully executed all containment steps and updated the case without manual intervention.

Post-Incident Analysis (RCA)

5 Whys Summary

- Why did exploitation occur? → Vulnerable Samba service exposed.

- Why was it exposed? → Patch not applied.
- Why was patch missing? → Incomplete asset management.
- Why incomplete? → No automated patch compliance monitoring.
- Why absent? → Lack of periodic security audits.

A Fishbone analysis categorized contributing factors under Technology, Process, Policy, and People.

Metrics Reporting

- **MTTD:** 2 Hours
- **MTTR:** 4 Hours
- **Dwell Time:** 2 Hours

Elastic Security dashboard visualized detection and response efficiency. Metrics indicate effective containment but highlight need for earlier vulnerability management.

Executive Report

Executive Summary

On 18 August 2025, a simulated exploitation targeting a vulnerable Samba service was detected and contained by the Security Operations Center. The activity was aligned with MITRE ATT&CK technique T1210 and represented remote service exploitation. Detection mechanisms functioned as expected, triggering alerts within 2 hours of compromise.

Timeline

16:00 – Exploit executed
16:05 – SIEM alert generated

16:30 – Triage initiated
17:00 – Containment executed
18:00 – Post-incident analysis completed

Root Cause Analysis

Investigation revealed that the affected system lacked recent security patches. Weak asset management processes contributed to delayed remediation. The vulnerability exposure allowed simulated adversary exploitation.

Recommendations

Implement automated patch management, continuous vulnerability scanning, enhanced monitoring rules for remote services, and routine adversary emulation exercises. Automation workflows should continue to be refined to further reduce response time and operational overhead.

Stakeholder Briefing

A simulated security incident involving exploitation of a vulnerable service was successfully detected and contained by the SOC team. The incident was identified within 2 hours and resolved within 4 hours, demonstrating effective monitoring and response procedures. The affected system was isolated immediately, and the malicious source was blocked to prevent further impact. Post-incident analysis revealed that delayed patching contributed to vulnerability exposure. Improvements are recommended in automated patch management, continuous monitoring, and proactive adversary testing. Overall, detection and containment controls functioned effectively, and no business systems or sensitive data were impacted. Continued investment in automation and proactive defense strategies will further strengthen the organization’s security posture.