Capstone SOC Project Report

Executive Summary

On September 29, 2025, a comprehensive Security Operations Center (SOC) capstone exercise was conducted to demonstrate end-to-end incident response capabilities. The exercise simulated a real-world Samba exploitation attack using Metasploit against a Metasploitable2 training system, followed by complete detection, analysis, containment, and reporting workflows. The attack was successfully detected within one second through network-based monitoring (PCAP capture and Wazuh Agent 007). A TheHive case was created for incident tracking, and automated response was implemented via CrowdSec IP blocking. The entire incident lifecycle from initial compromise to full containment was completed in 72.75 minutes, demonstrating response capabilities significantly exceeding industry benchmarks. This exercise successfully integrated multiple SOC tools and methodologies including SIEM analysis, case management, SOAR automation, root cause analysis, and executive reporting. All phases were documented with proper chain-of-custody procedures, resulting in a comprehensive evidence package suitable for forensic review.

Attack Simulation (Phase 1)

Objective: Execute a controlled exploitation to generate authentic incident data Execution: - Attack vector: Metasploit Framework multi/samba/usermap_script exploit - MITRE ATT&CK; Technique: T1210 (Exploitation of Remote Services) - Attacker system: Kali Linux (192.168.1.79) - Target system: Metasploitable2 (192.168.1.77) - Attack timestamp: 13:30:54 Results: - Successful exploitation achieved root shell access (uid=0, gid=0) - Reverse shell established via netcat on port 4444 - Malicious processes spawned: PIDs 4878 (netcat), 4879 (shell) - Reconnaissance commands executed: id, whoami, uname, ifconfig, ps aux, netstat Evidence Collected: - Complete Metasploit console output - Process listing showing malicious activity - Network connection data

Detection & Response

- Detection: Real-time PCAP + Wazuh Agent 007 - Case Management: TheHive Case #3 - Containment: CrowdSec IP blocking (Decision ID 173986) - Completion: 14:43:39

Key Metrics

Root Cause Analysis

Primary Issue: Lack of network segmentation between training and production environments Contributing Factors: - Vulnerable Samba 3.0.20 service - No host-based firewalls - Missing patch management for training systems

Recommendations

Immediate: Implement network segmentation for training labs Short-term: Deploy host-based firewalls on training systems Long-term: Establish formal network zoning policy and regular vulnerability scanning

Conclusion

Successfully demonstrated complete SOC workflow from attack simulation through detection, containment, analysis, and reporting. All phases documented with professional-grade evidence and proper chain of custody. Performance metrics significantly exceeded industry standards. Identified critical network segmentation gap with prioritized remediation plan. Status: Complete Date: September 29, 2025

Metric	Value	Industry Avg	Performance
MTTD	<1 second	280 seconds	99.6% faster
MTTR	72.75 minutes	73.5 days	99.9% faster
Detection Rate	100%	Variable	Complete
False Positives	0	Variable	Perfect