CAPSTONE REPORT (Alert-to-Response Cycle)

1. Introduction

This capstone project demonstrates a complete Security Operations Center (SOC) workflow from attack simulation to detection, triage, response, containment, and reporting. The exercise was conducted in a controlled lab environment using industry-recognized cybersecurity tools and frameworks.

The simulation follows structured methodologies based on:

- MITRE ATT&CK for attack technique mapping
- National Institute of Standards and Technology Incident Handling Guidelines (SP 800-61)
- Wazuh for detection and alert monitoring
- CrowdSec for automated blocking and response
- Metasploit for controlled attack simulation

The objective of this project is to simulate a real-world attack and execute a structured incident response lifecycle.

2. Objective

- Simulate a cyber attack in a lab environment
- Detect malicious activity using SIEM
- Perform alert triage and classification
- Contain and remediate the attack
- Document the full incident lifecycle
- Provide technical and non-technical reporting

3. Attack Simulation

Target Environment

- Metasploitable2 Virtual Machine

- Monitoring enabled via Wazuh Agent

Attack Performed

Exploitation of the VSFTPD 2.3.4 backdoor vulnerability.

Metasploit Module Used

```
exploit/unix/ftp/vsftpd_234_backdoor
```

This vulnerability allows remote command execution.

MITRE ATT&CK Mapping

Timestamp	Source IP	Alert Description	MITRE Technique
2026-02-13 11:00:00	192.168.1.100	VSFTPD Exploit Attempt	T1190

Technique Explanation:

T1190 – Exploit Public-Facing Application
Attackers exploit vulnerable services exposed to the internet.

4. Detection Phase

The attack was detected through log monitoring in Wazuh.

Wazuh Alert Sample

Alert ID	Severity	Rule ID	Description
1012	High	5710	Suspicious FTP exploit attempt detected

The alert was classified as **High Priority** due to:

- Public-facing service exploitation
- Remote command execution capability
- Risk of system compromise

5. Alert Triage

Triage Process

1. Verified source IP reputation
2. Checked system logs
3. Correlated FTP service logs
4. Validated exploit behavior
5. Confirmed unauthorized shell access

IOC Identified

- Source IP: 192.168.1.100
- Service: FTP
- Exploit Signature: VSFTPD Backdoor

The alert was confirmed as **True Positive**.

6. Containment Phase

Immediate actions taken:

- Isolated affected VM
- Disabled FTP service
- Blocked attacker IP using CrowdSec
- Terminated malicious shell session

Verification

Ping test from attacker machine failed after IP blocking.

Containment was successful.

7. Eradication and Recovery

- Removed vulnerable VSFTPD version
- Updated system packages
- Applied latest security patches

- Restarted services
- Re-enabled monitored access

System restored to operational state.

8. Timeline of Events

Time	Event
11:00	Exploit launched
11:01	Wazuh alert generated
11:03	Alert triage started
11:07	VM isolated
11:10	IP blocked
11:20	Vulnerability patched
11:40	System restored

9. Executive Summary (Technical)

A controlled exploit targeting the VSFTPD 2.3.4 vulnerability was executed against a monitored virtual machine. The attack was successfully detected by Wazuh SIEM and mapped to MITRE ATT&CK technique T1190. Alert triage confirmed remote command execution capability. The affected system was isolated, and the attacker IP was blocked using CrowdSec. The vulnerable service was patched, and the system was restored. The incident demonstrated effective SOC alert detection, triage, containment, eradication, and documentation procedures aligned with NIST incident response guidelines.

10. Stakeholder Briefing (Non-Technical)

A simulated cyber attack targeted one of our test servers using a known software vulnerability. The monitoring system detected the attack immediately. Our security team quickly investigated the alert, isolated the affected system, and blocked the attacker’s access. The vulnerable software was updated to prevent further exploitation. No production systems were impacted. This exercise confirmed that our monitoring and response processes are working effectively. It also helped us identify improvement areas in patch management and system hardening to reduce future risks.

11. Lessons Learned

- Patch management must be continuous
- Public-facing services require strict monitoring
- Real-time alerting reduces response time
- Automated blocking improves containment efficiency
- Regular vulnerability scanning is necessary

12. Recommendations

1. Implement automated vulnerability scanning
2. Enable stricter firewall policies
3. Deploy intrusion prevention systems
4. Schedule regular patch audits
5. Conduct quarterly SOC simulation drills

13. Conclusion

The capstone exercise successfully demonstrated a complete SOC workflow from attack simulation to recovery. The detection and response were aligned with MITRE ATT&CK mapping and NIST guidelines. The structured approach ensured effective containment and system restoration. This project validates practical SOC readiness and operational understanding of real-world cybersecurity incident management.