CYART SOC Team - Capstone Project: SOC Incident Response

What This Project Was About

We ran a full SOC incident response simulation. Basically, we acted like a real security team detecting and handling a cyberattack from start to finish. The goal was to practice spotting an attack, investigating it, stopping it, and writing up what happened.

Project Details:

- We simulated attacks on a vulnerable test system called Metasploitable2.
- Used a bunch of tools like Metasploit to attack, and Wazuh, CrowdSec, and Elastic Security to detect and analyze.
- We also used TheHive for managing incidents and MITRE Caldera to mimic attacker behaviors.
- The whole team worked together to learn how to handle real incidents.

What We Wanted to Achieve

- Simulate a real attack using a known vulnerability in Samba on Metasploitable2.
- Detect suspicious activity with our detection tools (Wazuh and CrowdSec).
- Emulate attacker tactics using MITRE Caldera to see how well we can detect them.
- Investigate and respond to the incident with TheHive and Elastic Security.
- Document everything clearly so others can understand what happened and how to fix it.

How We Did It

We followed the normal incident response steps:

Step	What We Did
Attack Simulation	Used Metasploit to exploit Samba vulnerability
Detection	Collected logs and alerts via Wazuh and CrowdSec
Triage	Validated alerts and prioritized incidents
Response	Took action to contain and stop the attack with TheHive
Analysis	Dug into logs and behavior using Elastic Security
Emulation	Used MITRE Caldera to simulate attacker moves (like exploiting remote services)
Reporting	Wrote detailed reports explaining what happened and how to fix it

Tools We Used

- **Metasploit** to launch attacks on the test machine.
- **Wazuh** and **CrowdSec** to spot weird or suspicious activity on hosts and networks.

- **TheHive** to track and manage the incident response process.
- **MITRE Caldera** to mimic attacker tactics and test our detection.
- **Elastic Security** to gather, correlate, and analyze logs for deep insight.
- **Google Docs** for working together on reports.

What We Found

- We successfully used Metasploit to exploit the Samba vulnerability on Metasploitable2.
- Wazuh spotted the remote exploit attempts and triggered alerts quickly.
- CrowdSec detected unusual behaviors that matched the attack timeline.
- TheHive helped us respond fast by organizing and assigning tasks.
- Caldera simulated attacker moves like lateral movement and privilege escalation, which we caught.
- Elastic Security gave us a detailed look at how the attack unfolded.
- We documented everything from start to finish, including causes and fixes.

Incident Timeline (Roughly)

When	What Happened	Tool Used	What We Did	Result
Start	Scanned Samba vulnerability	Metasploit	Launched exploit	Got initial access
+5 minutes	Detected remote exploit activity	Wazuh	Alert triggered	Incident flagged
+10 minutes	Noticed unusual behavior	CrowdSec	Correlated alerts	Confirmed attack pattern
+15 minutes	Created incident case	TheHive	Assigned response tasks	Response team activated
+20 minutes	Started emulating attacker tactics	MITRE Caldera	Simulated exploitation	Extended attack analysis
+30 minutes	Analyzed attack data	Elastic Security	Forensic investigation	Clarified attack scope
+45 minutes	Contained threat	TheHive	Ran containment playbook	Attack stopped
+60 minutes	Wrote report	Google Docs	Documented everything	Report ready

What Attack Steps We Saw

- Attacker used a Samba exploit to get into the system.
- Our detection tools caught the attack pretty fast by watching system logs and network traffic.
- TheHive made it easier to track the incident and coordinate actions.

- Caldera helped us mimic the attacker's next moves to test if we could detect them too.
- Elastic Security gave us powerful tools to analyze what happened at every stage.

What We Practiced in the Labs

- Using Metasploit to attack a vulnerable server.
- Setting up and tuning Wazuh and CrowdSec to detect attacks.
- Managing incidents with TheHive, from alert to containment.
- Running MITRE Caldera simulations of attacker behaviors.
- Using Elastic Security to hunt through logs and alerts.
- Writing clear reports and sharing findings with the team.

Skills We Built

Tech Skills

- How to launch exploits and test vulnerabilities.
- How to set up detection and alerting tools.
- How to organize and manage incidents.
- How to simulate attacker behaviors to improve detection.
- How to analyze logs and do threat hunting.

Soft Skills

- Working as a SOC team responding to incidents.
- Writing reports that both techies and non-techies can understand.
- Prioritizing and responding quickly to threats.
- Coordinating different tools and team members effectively.

What We Fixed and Improved

- Recommended patching Samba and other vulnerable services right away.
- Created better detection rules for Wazuh and CrowdSec to catch similar attacks.
- Improved playbooks in TheHive for quicker responses.
- Planned regular adversary simulations with Caldera to keep skills sharp.
- Set up Elastic Security to retain and analyze logs better for future hunts.

What's Included in Our Docs

- Detailed incident response report with timeline and analysis.
- Executive summary for management with the big picture.
- Playbooks and procedures for SOC incident handling.
- Detection rules and signatures we built.
- Scripts and configs for Caldera emulations.
- Elastic Security dashboards and forensic data exports.

What We Learned

- How real attackers behave and how to spot them fast.

- How to make different SOC tools work together smoothly.
- How to document incidents so everyone understands.
- How to simulate attacks to test defenses regularly.
- How to improve teamwork and communication during incidents.

Last Updated: January 30, 2026
Version: 1.0
Report Reference: SOC-Capstone-IR-2026