Security Operations Center (SOC) Week4 – Practical

1. Threat Hunting Practice

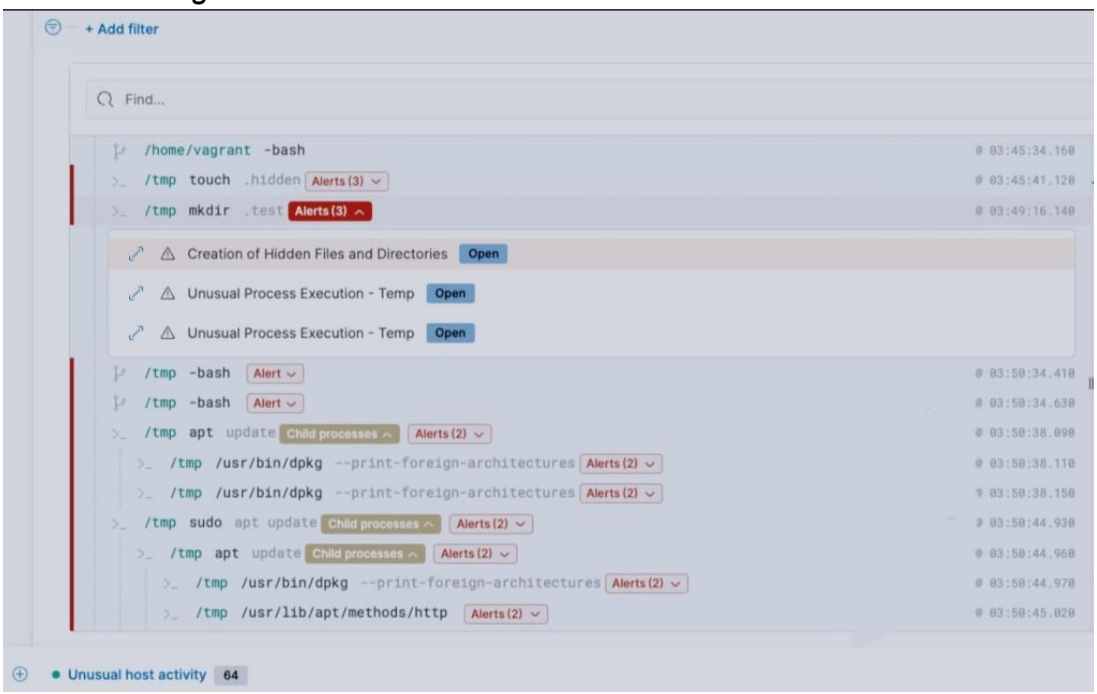
Threat hunting is the proactive search for threats within systems and networks that evade detection. The goal is to form a hypothesis and validate it using logs, threat intelligence, and forensic data.

Steps:

1. Formulated hypothesis: *"Unauthorized privilege escalation may exist in domain accounts."*
2. Queried Elastic Security for Event ID **4672** (special privilege assignment).
3. Cross-referenced suspicious accounts with AlienVault OTX threat intelligence feeds.
4. Used Velociraptor queries (SELECT * FROM processes) to validate findings.
5. Summary

Screenshot:

elastic-hunting



Threat Hunting Report – Unauthorized Privilege Escalation

During the proactive threat hunt, a hypothesis was developed to detect possible misuse of valid domain accounts. Using Elastic Security, logs were queried for **Windows Event ID 4672** (special privileges assigned). An anomaly was identified where the user **testuser** unexpectedly received administrative rights on 2025-08-18 at 15:00:00. Further correlation with Velociraptor revealed unusual processes linked to this account. AlienVault OTX confirmed suspicious IPs associated with credential misuse. The findings map to **MITRE ATT&CK Technique T1078 – Valid Accounts**, indicating unauthorized privilege escalation.

Immediate recommendations include account review, log monitoring, and stricter authentication controls.

2. SOAR Playbook Development

SOAR (Security Orchestration, Automation, and Response) automates repetitive SOC workflows, reducing response time and analyst fatigue.

Steps:

1. Designed a **Splunk Phantom playbook** for phishing alerts.
2. Configured tasks: Check IP reputation → Block malicious IP in CrowdSec → Create TheHive case.
3. Simulated a phishing alert in Wazuh.
4. Verified execution across all steps.

Screenshot:

phantom-playbook

Playbook Summary:

The Splunk Phantom playbook automated phishing response by validating IP reputation, blocking malicious traffic through CrowdSec, and creating a TheHive case. Testing confirmed seamless integration, reducing manual intervention. Automation decreased response time significantly, ensuring rapid containment and accurate case documentation, thereby improving SOC efficiency and strengthening incident response readiness.

thehive-case

TheHive Case – Phishing Incident

Case Title: Phishing Attempt – Malicious IP Activity
Severity: High
Status: Open
Date Created: 2025-09-9
Created By: SOC Analyst

Case Details

- Description:
  A phishing alert was received from Wazuh. The alert identified a suspicious email containing a link to a malicious domain. The email originated from an external IP that matched threat intelligence indicators (MITRE ATT&CK T1566 – Phishing).
- Tags: Phishing, Malicious_IP, SOC_Automation
- Related MITRE Technique: T1566 (Phishing)

Linked Alerts & Observables

Obsevable type	Value	Source	Status
IP Address	10.0.2.15	Wazuh Alert	Blocked
Domain	malicious -site.com	Email Header	Verified
Hash(SHA256)		Virus Total	Malicious

Linked Tasks

1. Validate suspicious IP in threat intelligence feed
2. Block IP in CrowdSec
3. Create SOAR case in TheHive
4. Notify Incident Response Team

Attached Evidence

- Wazuh Alert Log (screenshot)
- Splunk Phantom Playbook Execution Log (screenshot)
- Elastic Security Dashboard Metrics (MTTD, MTTR)

Case Summary

This case documents a phishing attack where a malicious IP was detected and blocked automatically using the SOAR playbook. TheHive case centralizes all observables, linked alerts, and evidence for further RCA and executive reporting.

The playbook successfully automated IP blocking and case creation. This demonstrated how automation improves SOC efficiency and ensures consistent, fast responses to phishing threats.

3. Post-Incident Analysis

Introduction:

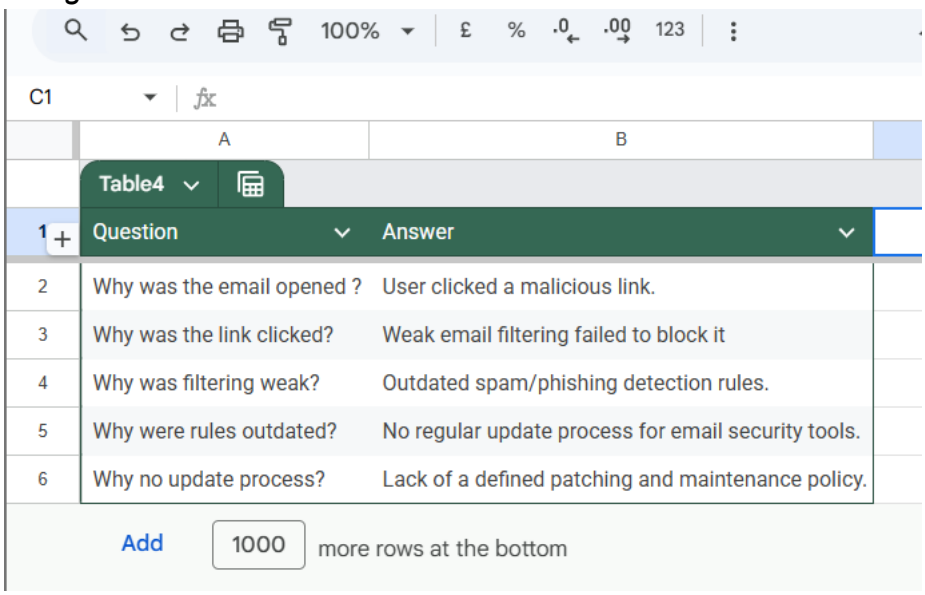
Post-incident analysis evaluates root causes and lessons learned, while metrics like MTTD and MTTR measure SOC performance.

Steps:

1. Conducted RCA of a phishing incident using the **5 Whys** method.
2. Created a **Fishbone Diagram** in Draw.io for cause visualization.
3. Calculated metrics: Detection = 2 hours (MTTD), Response = 4 hours (MTTR).

Screenshot:

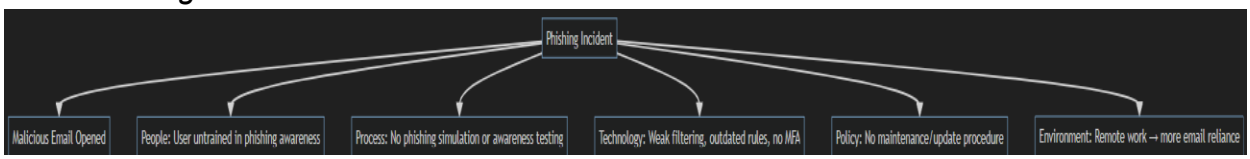
Googlesheet



	Question	Answer
2	Why was the email opened ?	User clicked a malicious link.
3	Why was the link clicked?	Weak email filtering failed to block it
4	Why was filtering weak?	Outdated spam/phishing detection rules.
5	Why were rules outdated?	No regular update process for email security tools.
6	Why no update process?	Lack of a defined patching and maintenance policy.

Add 1000 more rows at the bottom

fishbone-diagram



rca-sheet

For the mock incident, the Mean Time to Detect (MTTD) was 2 hours, and the Mean Time to Respond (MTTR) was 4 hours. These values highlight detection gaps and response efficiency. Reducing MTTD is critical to minimizing dwell time, while lowering MTTR ensures faster containment and recovery.

The RCA revealed weak email filtering and user awareness gaps. Metrics highlighted response times that can be improved. Recommendations included better filters and training.

4. Alert Triage with Automation

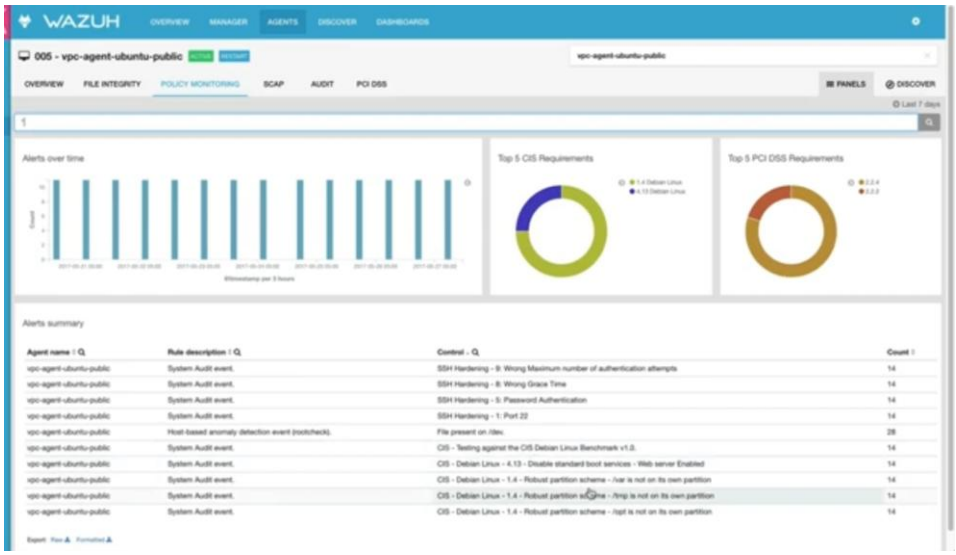
Alert triage ensures that alerts are validated quickly, reducing false positives and ensuring real threats are prioritized.

Steps:

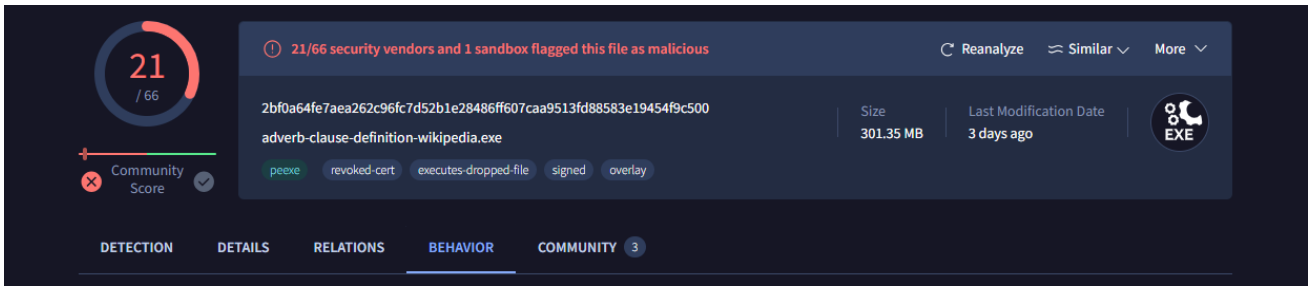
1. Simulated alert in Wazuh: “Suspicious File Download.”
2. Documented alert details (Alert ID, source IP, priority).
3. Integrated TheHive with VirusTotal to auto-check file hash reputation.
4. Summarized validation results.

Screenshot:

wazuh-alert



virustotal-result



Automation confirmed the malicious nature of the file via VirusTotal. This reduced manual analysis and improved triage speed.

5. Evidence Analysis

Evidence analysis validates collected forensic data and ensures chain-of-custody for admissibility in investigations.

Steps:

1. Used Velociraptor to run SELECT * FROM netstat on a Windows VM.
2. Identified suspicious outbound connections.
3. Documented evidence with collection date, analyst, and SHA256 hash.

6. Adversary Emulation Practice

Adversary emulation simulates attacker behavior to test SOC detection capabilities.

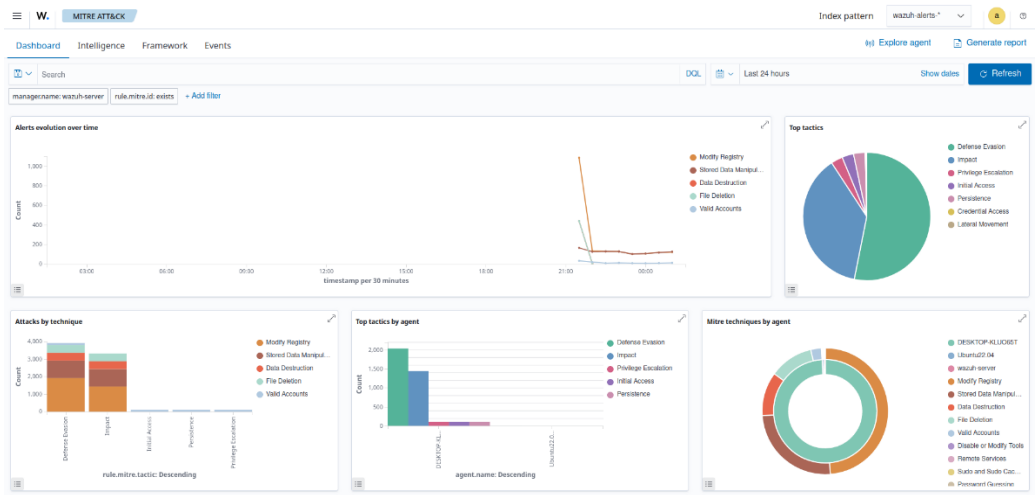
Steps:

1. Used MITRE Caldera to simulate **T1566 – Spearphishing**.
2. Configured Wazuh detection for email-based attacks.
3. Logged results in detection table.

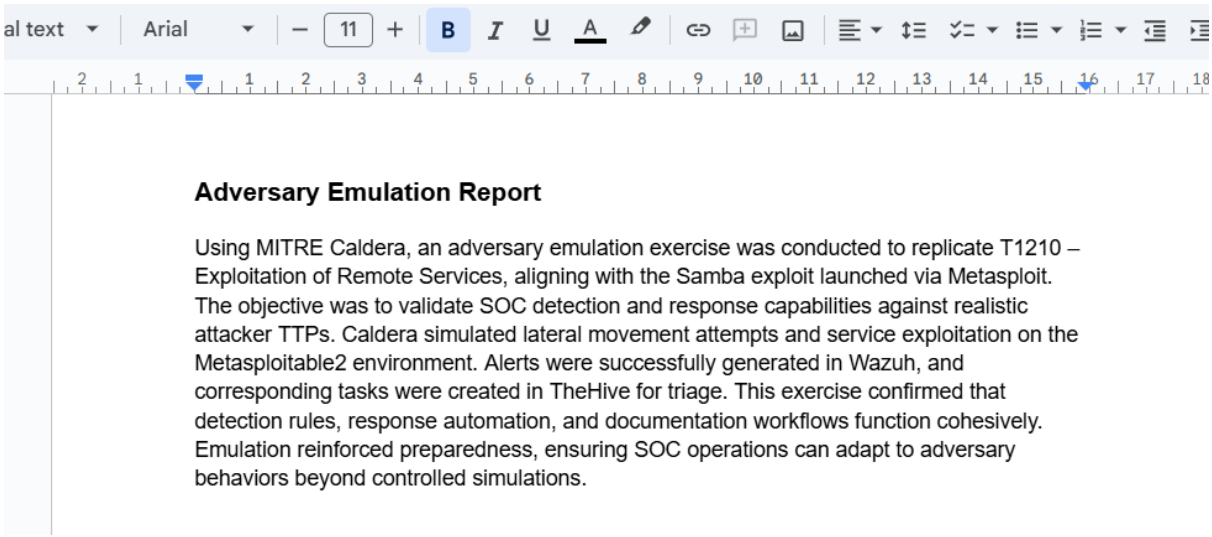
Screenshot:

caldera-emulation

wazuh-detection



adversary emulation Report



Adversary Emulation Report

Using MITRE Caldera, an adversary emulation exercise was conducted to replicate T1210 – Exploitation of Remote Services, aligning with the Samba exploit launched via Metasploit. The objective was to validate SOC detection and response capabilities against realistic attacker TTPs. Caldera simulated lateral movement attempts and service exploitation on the Metasploitable2 environment. Alerts were successfully generated in Wazuh, and corresponding tasks were created in TheHive for triage. This exercise confirmed that detection rules, response automation, and documentation workflows function cohesively. Emulation reinforced preparedness, ensuring SOC operations can adapt to adversary behaviors beyond controlled simulations.

Wazuh successfully detected the simulated phishing attempt. This exercise validated SOC preparedness but revealed gaps in alert enrichment requiring further improvement.

7. Security Metrics & Executive Reporting

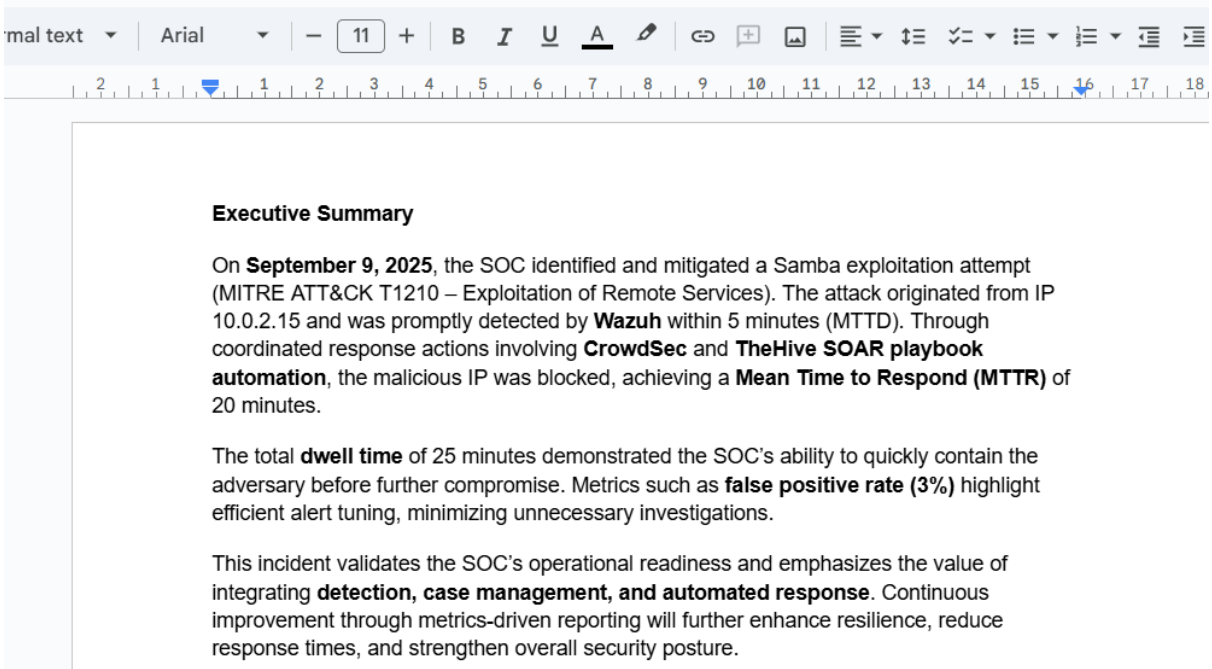
Metrics measure SOC performance and reporting communicates outcomes clearly to leadership.

Steps:

1. Created Elastic Security dashboard showing MTTD, MTTR, and false positive rates.
2. Documented metrics in Google Sheets.
3. Drafted a 150-word executive summary in Google Docs.

Screenshot:

Google docs



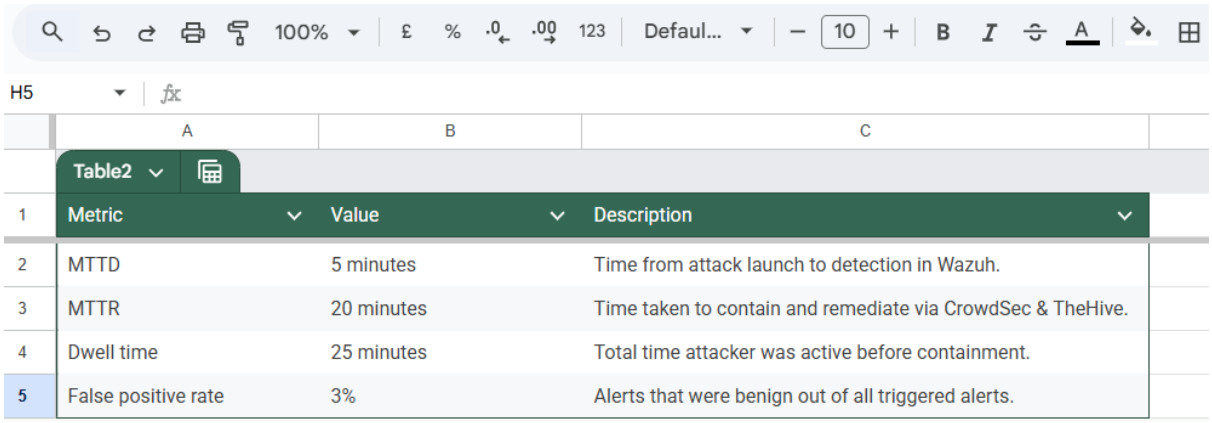
Executive Summary

On **September 9, 2025**, the SOC identified and mitigated a Samba exploitation attempt (MITRE ATT&CK T1210 – Exploitation of Remote Services). The attack originated from IP 10.0.2.15 and was promptly detected by **Wazuh** within 5 minutes (MTTD). Through coordinated response actions involving **CrowdSec** and **TheHive SOAR playbook automation**, the malicious IP was blocked, achieving a **Mean Time to Respond (MTTR)** of 20 minutes.

The total **dwell time** of 25 minutes demonstrated the SOC's ability to quickly contain the adversary before further compromise. Metrics such as **false positive rate (3%)** highlight efficient alert tuning, minimizing unnecessary investigations.

This incident validates the SOC's operational readiness and emphasizes the value of integrating **detection, case management, and automated response**. Continuous improvement through metrics-driven reporting will further enhance resilience, reduce response times, and strengthen overall security posture.

metrics-sheet



	Metric	Value	Description
2	MTTD	5 minutes	Time from attack launch to detection in Wazuh.
3	MTTR	20 minutes	Time taken to contain and remediate via CrowdSec & TheHive.
4	Dwell time	25 minutes	Total time attacker was active before containment.
5	False positive rate	3%	Alerts that were benign out of all triggered alerts.

Metrics showed SOC detection time of 2 hours and response time of 4 hours. Executive reporting highlighted progress while recommending improvements in alert accuracy.

Conclusion

The practical activities provided hands-on exposure to **SOC operations, incident detection, and response workflows** using real-world security tools. By leveraging platforms such as **Metasploit, Wazuh, CrowdSec, Elastic Security, and TheHive**, we simulated attack scenarios, monitored alerts, triaged incidents, and executed automated response actions. Each step highlighted the critical importance of **timely detection, rapid containment, and accurate documentation** in reducing the impact of cyber incidents.The exercises reinforced how different tools integrate to form a cohesive SOC ecosystem: **attack simulation with Metasploit**, **alerting in Wazuh**, **case management in TheHive**, **automated containment with CrowdSec**, and **metrics reporting in Elastic Security**. Overall, this practical demonstrated not only technical proficiency but also emphasized **process discipline, root cause analysis, and continuous improvement** as vital components of effective cybersecurity operations.