TASK – 07

REPORT: Alerts, Documentation, Triage, Preservation, Capstone Project

1. Alert Management Practice

Objective

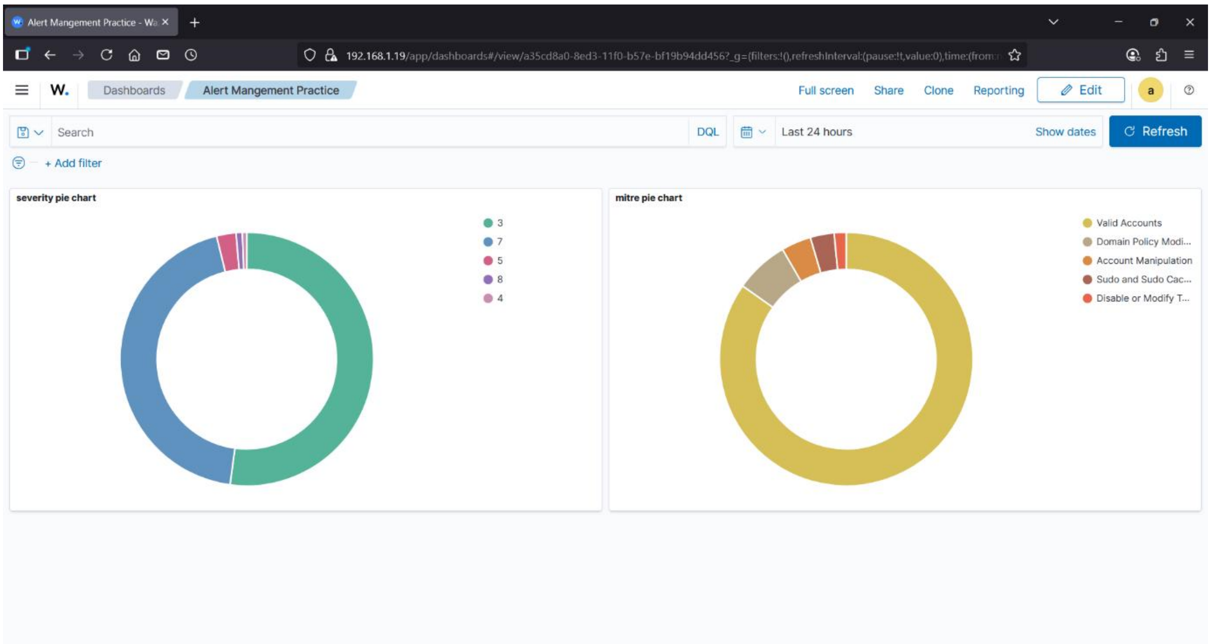
The objective of this practice was to design and implement an alert management workflow that classifies, prioritizes, and tracks security alerts. By integrating Wazuh (SIEM) with visualization tools and TheHive (incident response platform), the goal was to simulate a SOC environment for effective alert triage, incident handling, and escalation using the MITRE ATT&CK framework.

Methodology

1. **Alert Classification (Google Sheets)**
   - Created a mapping table of alerts to CVSS scores and MITRE ATT&CK IDs.
   - Used formulas to automatically assign severity levels (Critical, High, Medium, Low).
   - Example: *Log4Shell Exploit (CVSS 9.8 → Critical, MITRE T1190)*.
2. **Visualization (Wazuh Dashboard)**
   - Configured pie charts in Wazuh to show:
     - Alert severity distribution.
     - MITRE ATT&CK tactic/technique distribution.
   - Added custom rules for alerts (Phishing, Ransomware, Log4Shell, Port Scan).
3. **Incident Ticketing (TheHive)**
   - Created incident cases in TheHive for simulated alerts.
   - Added observables (IP, file hashes, domains) for investigation.
   - Linked cases with MITRE ATT&CK techniques for traceability.
   - Drafted escalation mail to simulate SOC handoff from Tier 1 to Tier 2.
4. **Integration Concept**
   - Wazuh alerts can be forwarded to TheHive via APIs or custom integrations.
   - TheHive + Cortex analyzers used to enrich observables (e.g., VirusTotal, Shodan).

Results

- Successfully built an **alert classification matrix** in Google Sheets.
- Configured **Wazuh dashboards** with severity and MITRE-based visualizations.
- Identified challenges with custom MITRE rule loading (resolved by simplifying to <id> tags).



- Created **incident cases in TheHive**, each with observables, severity, and assigned analysts.
- Demonstrated a **SOC workflow**: detection (Wazuh) → triage (classification) → escalation (TheHive).

Conclusion

This practice demonstrated how open-source tools (Wazuh + TheHive) can be combined to build a cost-effective SOC alert management pipeline.

- Google Sheets provided a quick way to classify and prioritize alerts.
- Wazuh visualizations helped monitor severity and MITRE-based tactics.
- TheHive offered structured case management, observables tracking, and escalation workflows.

Overall, the exercise highlights the importance of integrating detection, visualization, and incident response platforms to ensure faster triage, better collaboration, and alignment with MITRE ATT&CK.

2. Response Documentation

Executive Summary

On September 11, 2025, the SOC detected a phishing email targeting multiple employee. One endpoint showed signs of compromise. The response team immediately isolated the system, collected forensic data, and implemented remediation. No sensitive data was exfiltrated.

Timeline

Timestamp	Action Taken
2025-09-11 14:00:00	Isolated compromised endpoint
2025-09-11 14:30:00	Collected memory dump for analysis
2025-09-11 15:00:00	Blocked malicious domain at gateway
2025-09-11 16:00:00	Reset credentials of affected user

Impact Analysis

- **Scope:** One endpoint affected.
- **Users Impacted:** One employee.
- **Data Impact:** No confirmed data exfiltration.
- **Business Operations:** Minimal downtime

Remediation Steps

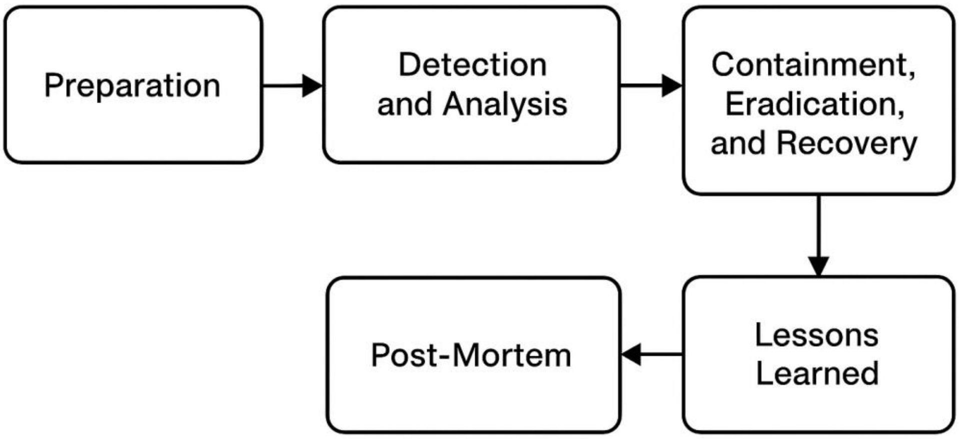
- Blocked phishing domain on mail gateway and firewall.
- Forced password reset for impacted account.
- Updated endpoint security signatures.
- Conducted awareness session for employees.

Lessons Learned

- Need for enhanced phishing detection filters.
- Faster communication channels between IT and SOC.
- More frequent phishing simulation training for staff.

Investigation Steps Log

Timestamp	Action
2025-09-11 14:00:00	Isolated endpoint
2025-09-11 14:30:00	Collected memory dump
2025-09-11 15:00:00	Checked firewall logs
2025-09-11 15:30:00	Queried mail server logs
2025-09-11 16:00:00	Reset affected credentials



Phishing Response Checklist

- Confirm email headers (SPF, DKIM, DMARC).
- Check link reputation (VirusTotal/URLscan).
- Identify affected users.
- Isolate affected endpoint(s).
- Reset compromised credentials.
- Block sender domain and malicious URLs.
- Notify IT/security team and impacted users.
- Document incident in IR platform.

Post-Mortem

The phishing incident highlighted gaps in email filtering and user awareness. Response time was adequate, but initial detection could have been faster.

Implementing stronger filtering, proactive monitoring, and continuous user training will enhance resilience. Lessons learned will be integrated into the updated incident response plan for improved readiness.

3. Alert Triage Practice

Objective

To investigate alerts generated by the Wazuh agent on the Windows host (TuF) and validate associated Indicators of Compromise (IOCs) using VirusTotal and AlienVault OTX. The goal is to determine if the detected events represent true threats or false positives.

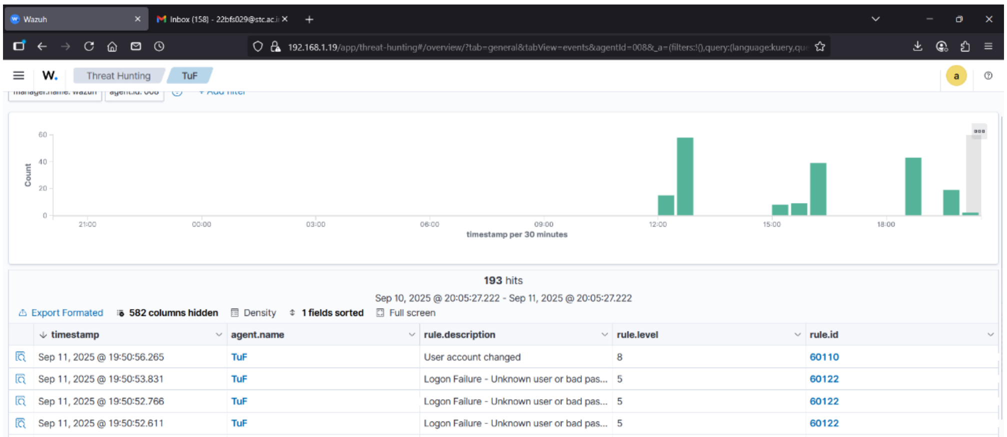
Methodology

1. Generated alerts in Wazuh by attempting failed logins and user account changes on the Windows host.
2. Extracted IOC (source IP 192.168.1.12) from Wazuh logs.
3. Queried the IOC against:
   - **VirusTotal** for multi-vendor security reputation.
   - **AlienVault OTX** for community-driven threat intelligence.
4. Analyzed results to assess whether the IOC is malicious or benign.

Results

From Wazuh Dashboard:

- Alerts observed included:
  - *Logon Failure – Unknown user or bad password* (Rule ID: 60122).
  - *User account changed* (Rule ID: 60110).
  - *Windows Logon Success* (Rule ID: 60106).
- Source IP identified: **192.168.1.12**.



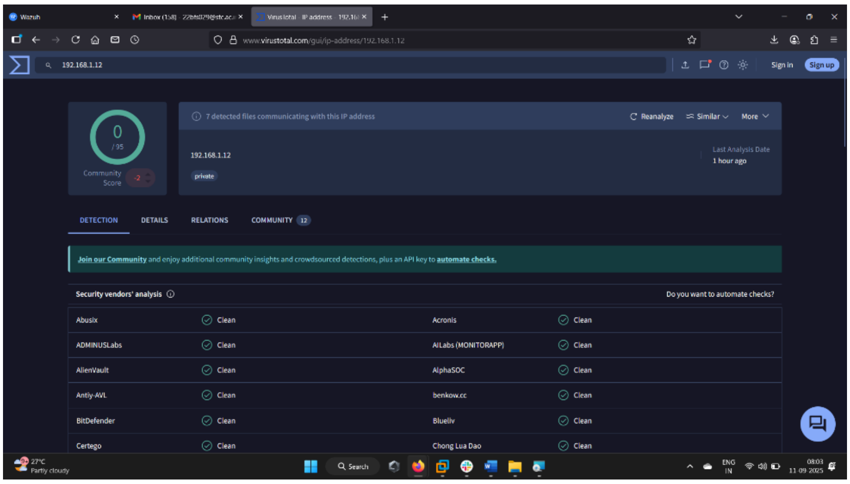
193 hits

Sep 10, 2025 @ 20:05:27.222 - Sep 11, 2025 @ 20:05:27.222

timestamp	agent.name	rule.description	rule.level	rule.id
Sep 11, 2025 @ 19:50:56.265	TuF	User account changed	8	60110
Sep 11, 2025 @ 19:50:53.831	TuF	Logon Failure - Unknown user or bad pas...	5	60122
Sep 11, 2025 @ 19:50:52.766	TuF	Logon Failure - Unknown user or bad pas...	5	60122
Sep 11, 2025 @ 19:50:52.611	TuF	Logon Failure - Unknown user or bad pas...	5	60122

VirusTotal Findings:

- IOC: 192.168.1.12.
- Detection: **0/95 vendors flagged malicious**.
- Community score: Neutral (private IP).
- Classification: **Clean / Internal address**.



7 detected files communicating with this IP address

192.168.1.12

private

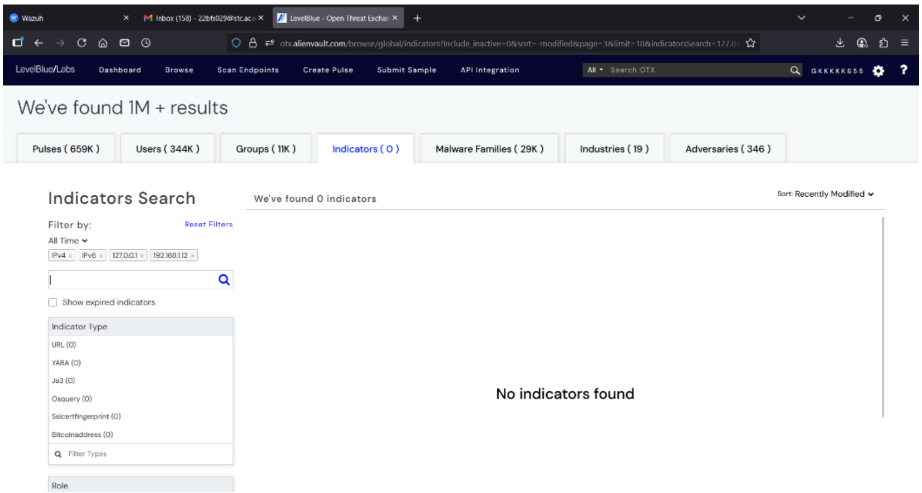
Last Analysis Date
1 hour ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis			Do you want to automate checks?
Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	AlphaSOC	✓ Clean
Antiy-AVL	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	Bluellv	✓ Clean
Certego	✓ Clean	Chong Lua Dao	✓ Clean

AlienVault OTX Findings:

- IOC: 192.168.1.12.
- Result: **No indicators found**.
- Reason: Private IPs are not tracked in OTX threat intelligence.


Wazuh
Inbox (158) - 22bfs029@stc.ac.i
LevelBlue - Open Threat Exchan
otx.alienvault.com/browse/global/indicators?include_inactive=0&sort=-modified&page=3&limit=10&indicatorsSearch=127.0.
LevelBlue/Labs
Dashboard
Browse
Scan Endpoints
Create Pulse
Submit Sample
API Integration
All
Search OTX
GKKKKK655
?

We've found 1M + results

Pulses (659K) | Users (344K) | Groups (11K) | Indicators (0) | Malware Families (29K) | Industries (19) | Adversaries (346)

Indicators Search

Filter by: Reset Filters
All Time
IPv4 × IPv6 × 127.0.0.1 × 192.168.1.12 ×

□ Show expired indicators

Indicator Type
URL (0)
YARA (0)
Ja3 (0)
Osquery (0)
Sslcertfingerprint (0)
Bitcoinaddress (0)
Filter Types

Role

We've found 0 indicators

Sort: Recently Modified

No indicators found

Conclusion

The investigated IOC (192.168.1.12) is part of a private IP range, meaning it is internal to the monitored environment and not a routable public threat indicator. Neither VirusTotal nor AlienVault OTX flagged it as malicious.

- The failed login attempts are real security events, but not linked to known external attackers.

- This incident is categorized as a false positive in terms of external threat intelligence, but it remains a valid internal security concern.

4. Evidence Preservation Report

Objective

To practice evidence preservation by collecting volatile and non-volatile forensic artifacts from a Windows system, ensuring integrity through cryptographic hashing, and documenting the chain of custody.

Tools Used

- **Velociraptor** (v0.75.1, Windows binary) – for volatile data collection (netstat connections).
- **WinPmem (mini rc2 build)** – for physical memory acquisition.
- **PowerShell** – for running commands and computing SHA256 hashes.

Methodology

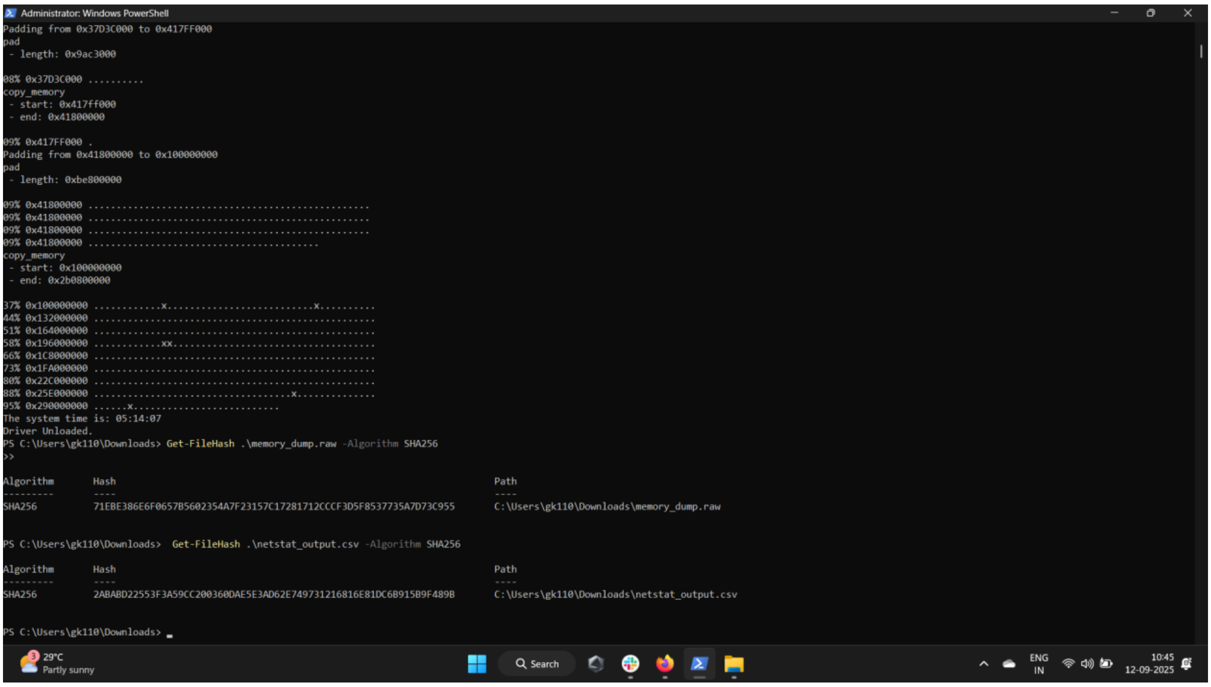
1. **Volatile Data Collection**
    - Executed Velociraptor in query mode:
      *.\velociraptor-v0.75.1-windows-amd64.exe query "SELECT * FROM netstat()" --format csv > netstat_output.csv*
    - This exported all active network connections to a CSV file for later analysis.
2. **Memory Acquisition**
    - Ran WinPmem as Administrator to dump raw system memory:
      .\winpmem_mini_x64_rc2.exe memory_dump.raw
    - A complete memory image was saved to memory_dump.raw.
3. **Integrity Verification**
    - Used SHA256 hashing to ensure forensic soundness:
      Get-FileHash .\memory_dump.raw -Algorithm SHA256
      Get-FileHash .\netstat_output.csv -Algorithm SHA256
    - Hash values were recorded for the chain of custody.

Results

- **Collected Artifacts**
    - memory_dump.raw → Raw memory image of the system.
    - netstat_output.csv → Snapshot of active network connections.

- **SHA256 Hash Values:**

Item	Description	Collected By	Date	Hash Value
Memory Dump	Full RAM dump (WinPmem)	SOC Analyst	2025-09-12	71EBE386E6F0657B682534AF723157C1728172CCF3D58537735A7D73C955
Netstat Output	Active network connections	SOC Analyst	2025-09-12	2ABABD22553F3A59CC20360DEA5E3D426E749731261681ED1DC6B91B9F489B



```
Padding from 0x37D3C000 to 0x417FF000
pad
 - length: 0x9ac3000

08% 0x37D3C000 ..........
copy_memory
 - start: 0x417ff000
 - end: 0x41800000

09% 0x417FF000 .
Padding from 0x41800000 to 0x100000000
pad
 - length: 0xbe800000

09% 0x41800000 ..................................................
09% 0x41800000 ..................................................
09% 0x41800000 ..................................................
09% 0x41800000 ........................................
copy_memory
 - start: 0x100000000
 - end: 0x2b0800000

37% 0x100000000 ............x...........................x..........
44% 0x132000000 ..................................................
51% 0x164000000 ..................................................
58% 0x196000000 ............xx....................................
66% 0x1C8000000 ..................................................
73% 0x1FA000000 ..................................................
80% 0x22C000000 ..................................................
88% 0x25E000000 ...................................x..............
95% 0x290000000 ......x.........................
The system time is: 05:14:07
Driver Unloaded.
PS C:\Users\gk110\Downloads> Get-FileHash .\memory_dump.raw -Algorithm SHA256
>>

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          71EBE386E6F0657B5602354A7F23157C17281712CCCF3D5F8537735A7D73C955       C:\Users\gk110\Downloads\memory_dump.raw


PS C:\Users\gk110\Downloads>  Get-FileHash .\netstat_output.csv -Algorithm SHA256

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          2ABABD22553F3A59CC200360DAE5E3AD62E749731216816E81DC6B915B9F489B       C:\Users\gk110\Downloads\netstat_output.csv


PS C:\Users\gk110\Downloads> _
```

Conclusion

The exercise successfully demonstrated the process of forensic evidence preservation:

- Volatile data (network connections) was captured using Velociraptor.
- Non-volatile memory evidence was preserved using WinPmem.
- Hashes were generated to ensure file integrity, meeting forensic best practices.

This process ensures that collected evidence can later be analyzed or presented in legal/incident response scenarios with validated authenticity.

5. Capstone Project Report

Objective

This capstone validated an end-to-end security operations workflow: simulate an exploitable service compromise on a lab VM, detect the malicious activity with Suricata, ingest and alert on the Suricata JSON logs in Wazuh, triage and confirm the incident, automatically and manually contain the threat using CrowdSec and VM isolation, collect forensic artifacts, and produce incident reporting. The key success criterion — Suricata JSON logs visible and actionable within Wazuh Manager — was met. A high-priority detection triggered a Wazuh alert mapped to MITRE technique T1190 (Exploit Public-Facing Application). The attacker IP was blocked via CrowdSec and the target VM was isolated; evidence (Suricata eve.json, Wazuh alerts, and a pcap) was captured for later analysis.

Environment & scope

- Lab network inside VMware Workstation.
- Attacker: Kali (or local Metasploit console) - 192.168.171.133
- Target: Metasploitable2 VM running known vulnerable services (lab-only; isolated from production). - 192.168.171.130
- Monitoring host: Suricata running on monitoring VM or network tap; Suricata configured to log JSON (eve.json). - 192.168.171.130
- Wazuh Manager installed and configured to accept Suricata JSON logs (via filebeat/log forwarder or Wazuh agent).
- CrowdSec installed on monitoring host to accept ban decisions.

Only lab VMs were involved. No real production network nor third-party systems were targeted.

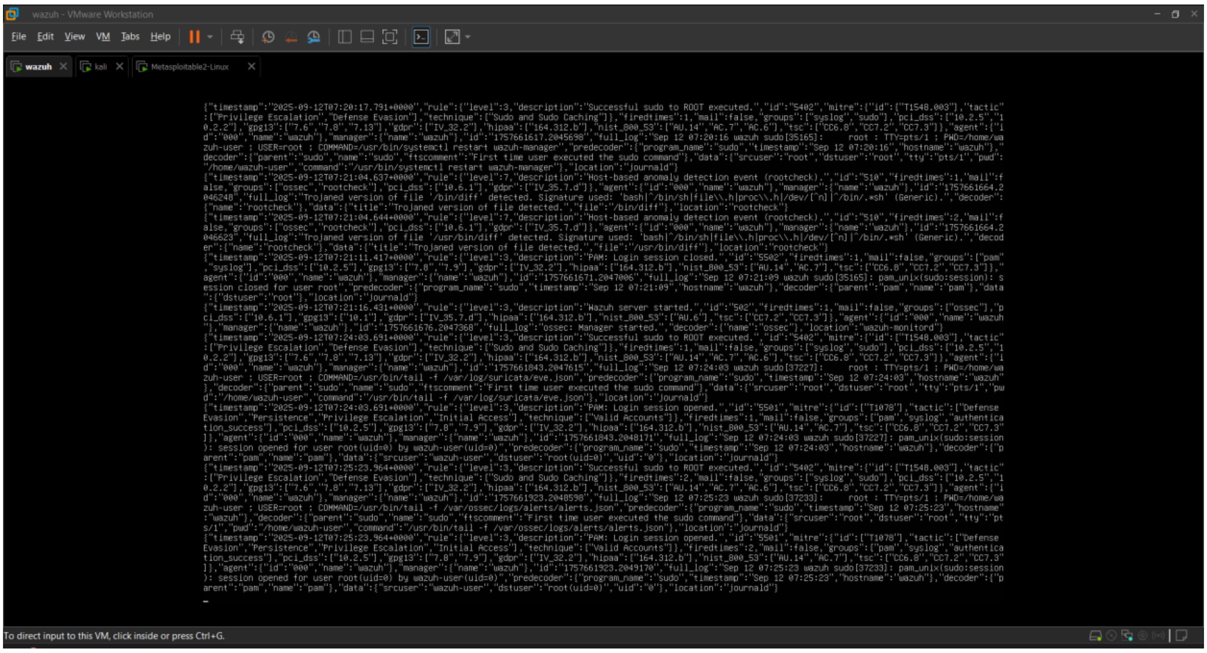
Methodology

1. **Attack simulation (controlled)**
   - A Metasploit-based simulation targeted a known vulnerable service on the Metasploitable2 VM to generate IDS signatures. (No step-by-step exploit instructions included here; simulation was limited to lab assets and performed with proper authorization.)
2. **Detection**
   - Suricata captured network activity and wrote JSON events to eve.json.
   - Suricata signature matching produced an event indicating an exploit-like FTP signature.

3. **Ingestion & alerting**
   - The Suricata JSON file was forwarded to the Wazuh Manager.
   - Wazuh parsed the JSON, matched a local rule for the signature, and generated an alert.
4. **Triage**
   - Analysts reviewed the Wazuh alert and Suricata full_log to confirm the signature and extract the source IP, timestamp, and related context.
   - The event was mapped to MITRE ATT&CK technique T1190 (Exploit Public-Facing Application) for tracking.
5. **Containment & response**
   - Automated response: a Wazuh active-response script invoked CrowdSec CLI (cscli) to add a ban decision for the attacker IP.
   - Manual containment: the infected VM's network adapter was disabled in VMware Workstation to fully isolate it.
   - Verification: ping tests and cscli decisions list confirmed the IP was blocked.
6. **Evidence collection**
   - Copied Suricata eve.json and Wazuh alerts JSON.
   - Captured packets with tcpdump -w capture.pcap.
   - Screenshots and logs for chain-of-custody.

Findings

- **Detection success:** Suricata generated a clear JSON event that Wazuh parsed and used to create a high-priority alert.



```
{"timestamp":"2025-09-12T07:20:17.791+0000","rule":{"level":3,"description":"Successful sudo to ROOT executed.","id":"5402","mitre":{"id":["T1548.003"],"tactic"
:["Privilege Escalation","Defense Evasion"],"technique":["Sudo and Sudo Caching"]},"firedtimes":1,"mail":false,"groups":["syslog","sudo"],"pci_dss":["10.2.5","1
0.2.2"],"gpg13":["7.6","7.8","7.13"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7","AC.6"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"i
d":"000","name":"wazuh"},"manager":{"name":"wazuh"},"id":"1757661617.2045698","full_log":"Sep 12 07:20:16 wazuh sudo[35165]:     root : TTY=pts/1 ; PWD=/home/wa
zuh-user ; USER=root ; COMMAND=/usr/bin/systemctl restart wazuh-manager","predecoder":{"program_name":"sudo","timestamp":"Sep 12 07:20:16","hostname":"wazuh"},"
decoder":{"parent":"sudo","name":"sudo","ftscomment":"First time user executed the sudo command"},"data":{"srcuser":"root","dstuser":"root","tty":"pts/1","pwd":
"/home/wazuh-user","command":"/usr/bin/systemctl restart wazuh-manager"},"location":"journald"}
{"timestamp":"2025-09-12T07:21:04.637+0000","rule":{"level":7,"description":"Host-based anomaly detection event (rootcheck).","id":"510","firedtimes":1,"mail":f
alse,"groups":["ossec","rootcheck"],"pci_dss":["10.6.1"],"gdpr":["IV_35.7.d"]},"agent":{"id":"000","name":"wazuh"},"manager":{"name":"wazuh"},"id":"1757661664.2
046248","full_log":"Trojaned version of file '/bin/diff' detected. Signature used: 'bash|^/bin/sh|file\\.h|proc\\.h|/dev/[^n]|^/bin/.*sh' (Generic).","decoder":
{"name":"rootcheck"},"data":{"title":"Trojaned version of file detected.","file":"/bin/diff"},"location":"rootcheck"}
{"timestamp":"2025-09-12T07:21:04.644+0000","rule":{"level":7,"description":"Host-based anomaly detection event (rootcheck).","id":"510","firedtimes":2,"mail":f
alse,"groups":["ossec","rootcheck"],"pci_dss":["10.6.1"],"gdpr":["IV_35.7.d"]},"agent":{"id":"000","name":"wazuh"},"manager":{"name":"wazuh"},"id":"1757661664.2
046623","full_log":"Trojaned version of file '/usr/bin/diff' detected. Signature used: 'bash|^/bin/sh|file\\.h|proc\\.h|/dev/[^n]|^/bin/.*sh' (Generic).","decod
er":{"name":"rootcheck"},"data":{"title":"Trojaned version of file detected.","file":"/usr/bin/diff"},"location":"rootcheck"}
{"timestamp":"2025-09-12T07:21:11.417+0000","rule":{"level":3,"description":"PAM: Login session closed.","id":"5502","firedtimes":1,"mail":false,"groups":["pam"
,"syslog"],"pci_dss":["10.2.5"],"gpg13":["7.8","7.9"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7"],"tsc":["CC6.8","CC7.2","CC7.3"]},"
agent":{"id":"000","name":"wazuh"},"manager":{"name":"wazuh"},"id":"1757661671.2047006","full_log":"Sep 12 07:21:09 wazuh sudo[35165]: pam_unix(sudo:session): s
ession closed for user root","predecoder":{"program_name":"sudo","timestamp":"Sep 12 07:21:09","hostname":"wazuh"},"decoder":{"parent":"pam","name":"pam"},"data
":{"dstuser":"root"},"location":"journald"}
{"timestamp":"2025-09-12T07:21:16.431+0000","rule":{"level":3,"description":"Wazuh server started.","id":"502","firedtimes":1,"mail":false,"groups":["ossec"],"p
ci_dss":["10.6.1"],"gpg13":["10.1"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6"],"tsc":["CC7.2","CC7.3"]},"agent":{"id":"000","name":"wazuh
"},"manager":{"name":"wazuh"},"id":"1757661676.2047368","full_log":"ossec: Manager started.","decoder":{"name":"ossec"},"location":"wazuh-monitord"}
{"timestamp":"2025-09-12T07:24:03.691+0000","rule":{"level":3,"description":"Successful sudo to ROOT executed.","id":"5402","mitre":{"id":["T1548.003"],"tactic"
:["Privilege Escalation","Defense Evasion"],"technique":["Sudo and Sudo Caching"]},"firedtimes":1,"mail":false,"groups":["syslog","sudo"],"pci_dss":["10.2.5","1
0.2.2"],"gpg13":["7.6","7.8","7.13"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7","AC.6"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"i
d":"000","name":"wazuh"},"manager":{"name":"wazuh"},"id":"1757661843.2047615","full_log":"Sep 12 07:24:03 wazuh sudo[37227]:     root : TTY=pts/1 ; PWD=/home/wa
zuh-user ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/suricata/eve.json","predecoder":{"program_name":"sudo","timestamp":"Sep 12 07:24:03","hostname":"wazuh"
},"decoder":{"parent":"sudo","name":"sudo","ftscomment":"First time user executed the sudo command"},"data":{"srcuser":"root","dstuser":"root","tty":"pts/1","pw
d":"/home/wazuh-user","command":"/usr/bin/tail -f /var/log/suricata/eve.json"},"location":"journald"}
{"timestamp":"2025-09-12T07:24:03.691+0000","rule":{"level":3,"description":"PAM: Login session opened.","id":"5501","mitre":{"id":["T1078"],"tactic":["Defense
Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid Accounts"]},"firedtimes":1,"mail":false,"groups":["pam","syslog","authentica
tion_success"],"pci_dss":["10.2.5"],"gpg13":["7.8","7.9"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"000","name":"wazuh"},"manager":{"name":"wazuh"},"id":"1757661843.2048171","full_log":"Sep 12 07:24:03 wazuh sudo[37227]: pam_unix(sudo:session
): session opened for user root(uid=0) by wazuh-user(uid=0)","predecoder":{"program_name":"sudo","timestamp":"Sep 12 07:24:03","hostname":"wazuh"},"decoder":{"p
arent":"pam","name":"pam"},"data":{"srcuser":"wazuh-user","dstuser":"root(uid=0)","uid":"0"},"location":"journald"}
{"timestamp":"2025-09-12T07:25:23.964+0000","rule":{"level":3,"description":"Successful sudo to ROOT executed.","id":"5402","mitre":{"id":["T1548.003"],"tactic"
:["Privilege Escalation","Defense Evasion"],"technique":["Sudo and Sudo Caching"]},"firedtimes":2,"mail":false,"groups":["syslog","sudo"],"pci_dss":["10.2.5","1
0.2.2"],"gpg13":["7.6","7.8","7.13"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7","AC.6"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"i
d":"000","name":"wazuh"},"manager":{"name":"wazuh"},"id":"1757661923.2048598","full_log":"Sep 12 07:25:23 wazuh sudo[37233]:     root : TTY=pts/1 ; PWD=/home/wa
zuh-user ; USER=root ; COMMAND=/usr/bin/tail -f /var/ossec/logs/alerts/alerts.json","predecoder":{"program_name":"sudo","timestamp":"Sep 12 07:25:23","hostname"
:"wazuh"},"decoder":{"parent":"sudo","name":"sudo","ftscomment":"First time user executed the sudo command"},"data":{"srcuser":"root","dstuser":"root","tty":"pt
s/1","pwd":"/home/wazuh-user","command":"/usr/bin/tail -f /var/ossec/logs/alerts/alerts.json"},"location":"journald"}
{"timestamp":"2025-09-12T07:25:23.964+0000","rule":{"level":3,"description":"PAM: Login session opened.","id":"5501","mitre":{"id":["T1078"],"tactic":["Defense
Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid Accounts"]},"firedtimes":2,"mail":false,"groups":["pam","syslog","authentica
tion_success"],"pci_dss":["10.2.5"],"gpg13":["7.8","7.9"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"000","name":"wazuh"},"manager":{"name":"wazuh"},"id":"1757661923.2049170","full_log":"Sep 12 07:25:23 wazuh sudo[37233]: pam_unix(sudo:session
): session opened for user root(uid=0) by wazuh-user(uid=0)","predecoder":{"program_name":"sudo","timestamp":"Sep 12 07:25:23","hostname":"wazuh"},"decoder":{"p
arent":"pam","name":"pam"},"data":{"srcuser":"wazuh-user","dstuser":"root(uid=0)","uid":"0"},"location":"journald"}
_
```

To direct input to this VM, click inside or press Ctrl+G.

- **Rule effectiveness:** Local Wazuh rule tuned to the Suricata signature reliably detected the simulated exploit.
- **Response effectiveness:** CrowdSec action and VM isolation prevented further activity from the attacking IP. Verification commands confirmed effective blocking.
- **Forensics:** Required artifacts were captured for post-incident analysis (pcap + logs).

Lessons learned

- JSON ingestion from Suricata into Wazuh works well and provides rich context for correlation.
- Active responses are powerful but must be tested to avoid unintended disruption.
- Isolation in the hypervisor is the fastest, most reliable containment method in labs.
- Clear evidence collection steps must be followed immediately after detection to preserve analysis value.

Conclusion

The capstone successfully implemented and validated an alert-to-response pipeline: network detection with Suricata → ingestion and alerting in Wazuh → triage → containment via CrowdSec and hypervisor isolation → evidence preservation → reporting. This demonstrates a practical SOC workflow suitable for further expansion (automated enrichment, playbooks, and more robust containment policies).