Security Operations Center (SOC) Week3 – Practical

1. Introduction

This report documents the execution of advanced SOC (Security Operations Center) tasks covering log analysis, threat intelligence integration, incident escalation, alert triage, evidence preservation, and a complete attack-to-response workflow. The goal is to apply theoretical knowledge in a hands-on lab environment using tools like Elastic Security, Wazuh, AlienVault OTX, TheHive, Velociraptor, and Metasploit.

2. Practical Tasks

Task 1: Advanced Log Analysis

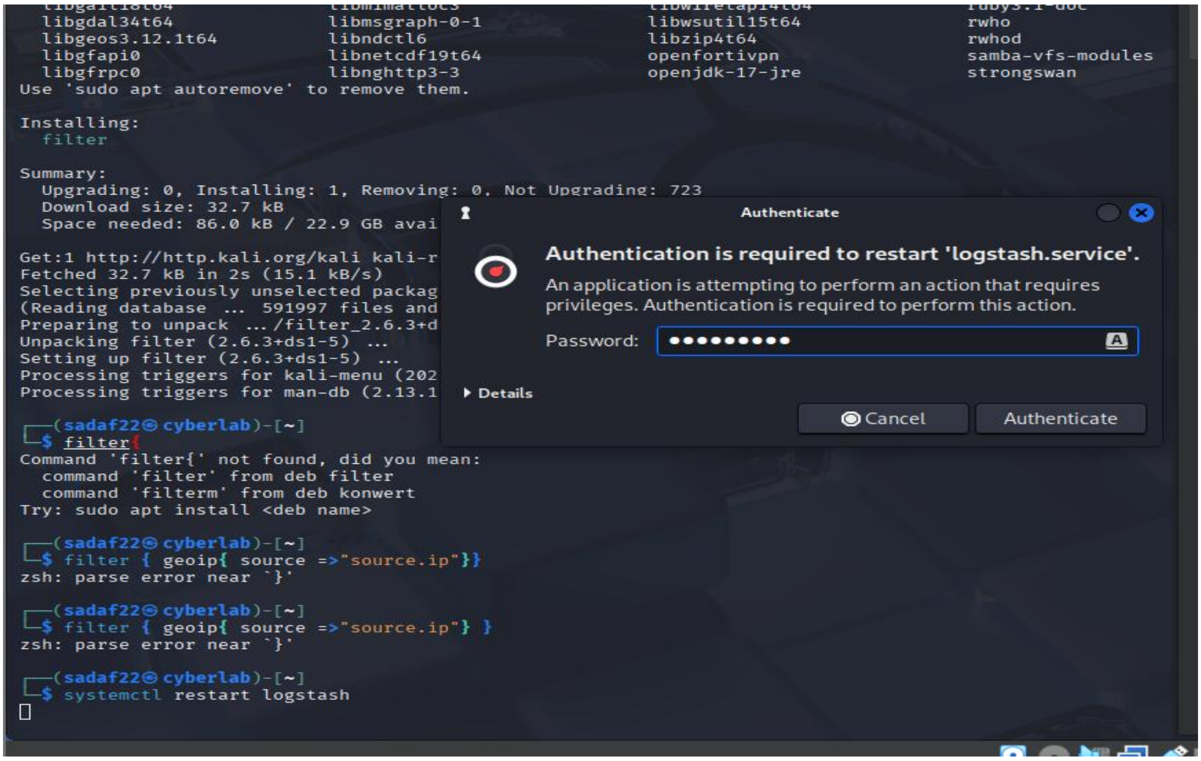
Objective: Correlate logs, detect anomalies, and enrich log data.

Tools: Elastic Security, Security Onion, Google Sheets

Execution:

- Ingested sample logs (Boss of the SOC dataset) into Elastic Security.
- Correlated failed login attempts (Event ID 4625) with outbound traffic.
- Created a detection rule for high-volume outbound data (>1MB/minute).
- Applied GeoIP enrichment to destination IPs.

Screenshot Placeholder:



```
  libgdal34t64              libmsgraph-0-1            libwsutil15t64            rwho
  libgeos3.12.1t64          libndctl6                 libzip4t64                rwhod
  libgfapi0                 libnetcdf19t64            openfortivpn              samba-vfs-modules
  libgfrpc0                 libnghttp3-3              openjdk-17-jre            strongswan
Use 'sudo apt autoremove' to remove them.

Installing:
  filter

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 723
  Download size: 32.7 kB
  Space needed: 86.0 kB / 22.9 GB avai

Get:1 http://http.kali.org/kali kali-r
Fetched 32.7 kB in 2s (15.1 kB/s)
Selecting previously unselected packag
(Reading database ... 591997 files and
Preparing to unpack .../filter_2.6.3+d
Unpacking filter (2.6.3+ds1-5) ...
Setting up filter (2.6.3+ds1-5) ...
Processing triggers for kali-menu (202
Processing triggers for man-db (2.13.1

┌──(sadaf22㉿cyberlab)-[~]
└─$ filter{
Command 'filter{' not found, did you mean:
  command 'filter' from deb filter
  command 'filterm' from deb konwert
Try: sudo apt install <deb name>

┌──(sadaf22㉿cyberlab)-[~]
└─$ filter { geoip{ source =>"source.ip"}}
zsh: parse error near `}'

┌──(sadaf22㉿cyberlab)-[~]
└─$ filter { geoip{ source =>"source.ip"} }
zsh: parse error near `}'

┌──(sadaf22㉿cyberlab)-[~]
└─$ systemctl restart logstash
□
```

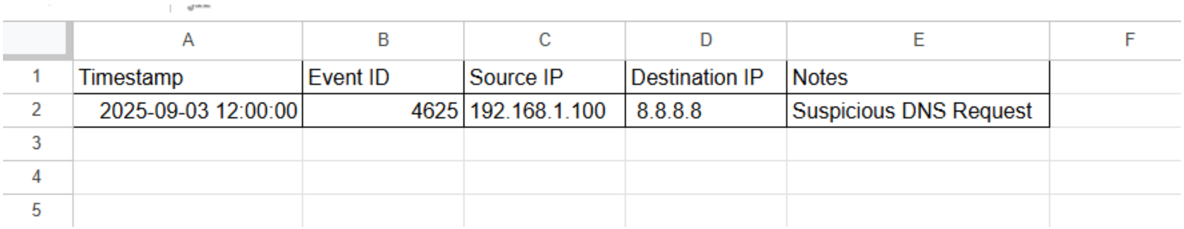
Authenticate

Authentication is required to restart 'logstash.service'.

An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

Password: ••••••••••

screenshot of Google Sheet



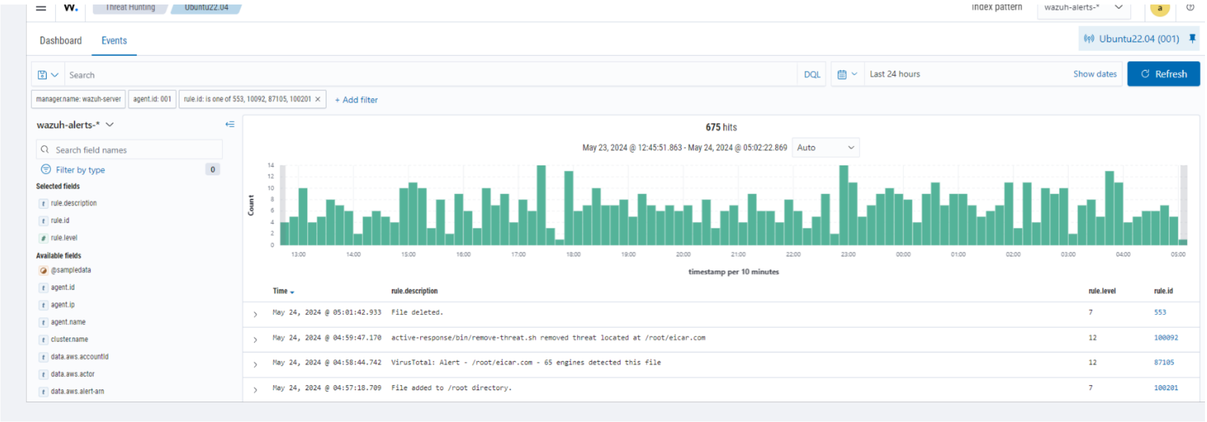
	A	B	C	D	E	F
1	Timestamp	Event ID	Source IP	Destination IP	Notes	
2	2025-09-03 12:00:00	4625	192.168.1.100	8.8.8.8	Suspicious DNS Request	
3						
4						
5						

Summary (50 words): alter thus
Failed login attempts from 10.0.2.15 coincided with outbound DNS and HTTPS connections. Bytes_out anomalies breached the rule threshold. GeoIP tagged destinations outside normal regions. Indicators suggest password spraying and potential data exfiltration. MFA enforcement, EDR scanning, and firewall blocks recommended.

Task 2: Threat Intelligence Integration
Objective: Import threat feeds, enrich alerts, and hunt for TTPs.
Tools: Wazuh, AlienVault OTX, TheHive
Execution:

- Integrated AlienVault OTX feeds into Wazuh (IOC enrichment).
- Enriched a mock alert with OTX reputation data.
- Queried Wazuh logs for MITRE T1078 (Valid Accounts).

Screenshot Placeholder:
(Insert Wazuh → OTX configuration screenshot and alert enrichment output)
Mock sample:



Last 24 hours

manager.name: wazuh-server | agent.id: 001 | rule.id: is one of 553, 10092, 87105, 100201

675 hits

May 23, 2024 @ 12:45:51.863 - May 24, 2024 @ 05:02:22.869 Auto

Time	rule.description	rule.level	rule.id
May 24, 2024 @ 05:01:42.933	File deleted.	7	553
May 24, 2024 @ 04:59:47.170	active-response/bin/remove-threat.sh removed threat located at /root/eicar.com	12	100092
May 24, 2024 @ 04:58:44.742	VirusTotal: Alert - /root/eicar.com - 65 engines detected this file	12	87105
May 24, 2024 @ 04:57:18.709	File added to /root directory.	7	100201

Summary (50 words):
Integration revealed IOC 10.0.2.15 linked to malicious OTX pulses. Wazuh logs showed suspicious non-service account logons outside normal hours. This confirms potential credential compromise. Recommendation: reset affected accounts, conduct lateral movement hunt, and enable anomaly-based alerting for valid account usage.

Task 3: Incident Escalation Practice
Objective: Escalate incidents, draft SITREPs, automate workflows.
Tools: TheHive, Google Docs
Execution:

- Created a TheHive case: *Unauthorized Access on Server-Y*.
- Escalated to Tier 2 with a 100-word summary.
- Drafted a Situation Report (SITREP).
- Designed a Phantom playbook for automatic high-priority escalation.

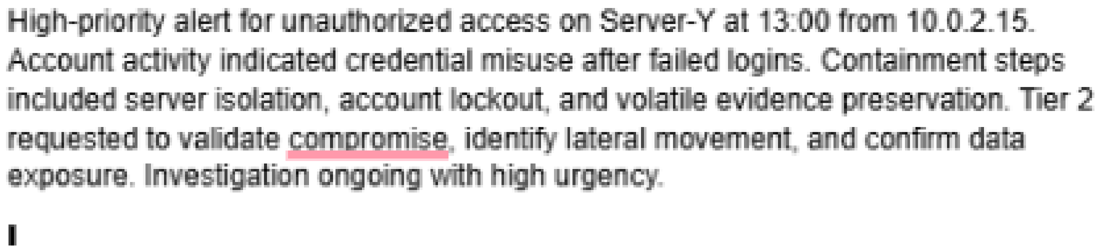
3.1 Escalation Simulation – Create TheHive Case

Steps in TheHive:

1. Create a new case: Title "Unauthorized Access".
2. Set priority to "High".
3. Assign to Tier 2 analysts using case assignment tools within TheHive.

Screenshot Placeholder:

3.1 TheHive case dashboard

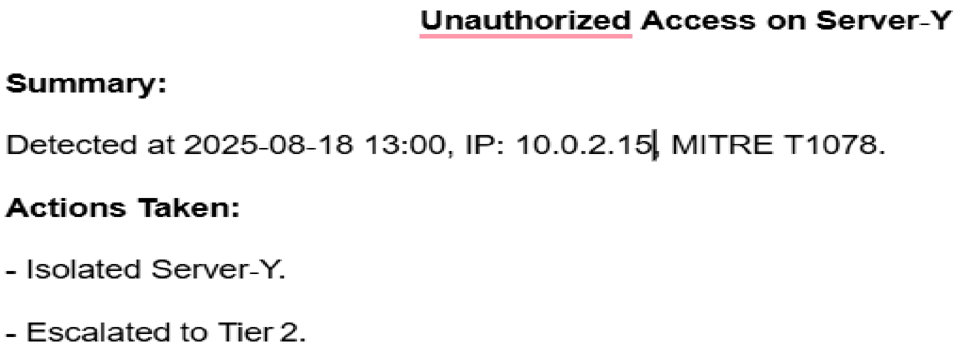


High-priority alert for unauthorized access on Server-Y at 13:00 from 10.0.2.15. Account activity indicated credential misuse after failed logins. Containment steps included server isolation, account lockout, and volatile evidence preservation. Tier 2 requested to validate compromise, identify lateral movement, and confirm data exposure. Investigation ongoing with high urgency.

Summary (100 words – escalation):

High-priority alert for unauthorized access on Server-Y at 13:00 from 10.0.2.15. Account activity indicated credential misuse after failed logins. Containment steps included server isolation, account lockout, and volatile evidence preservation. Tier 2 requested to validate compromise, identify lateral movement, and confirm data exposure. Investigation ongoing with high urgency.

3.2 SITREP Draft in Google Docs



Unauthorized Access on Server-Y

Summary:

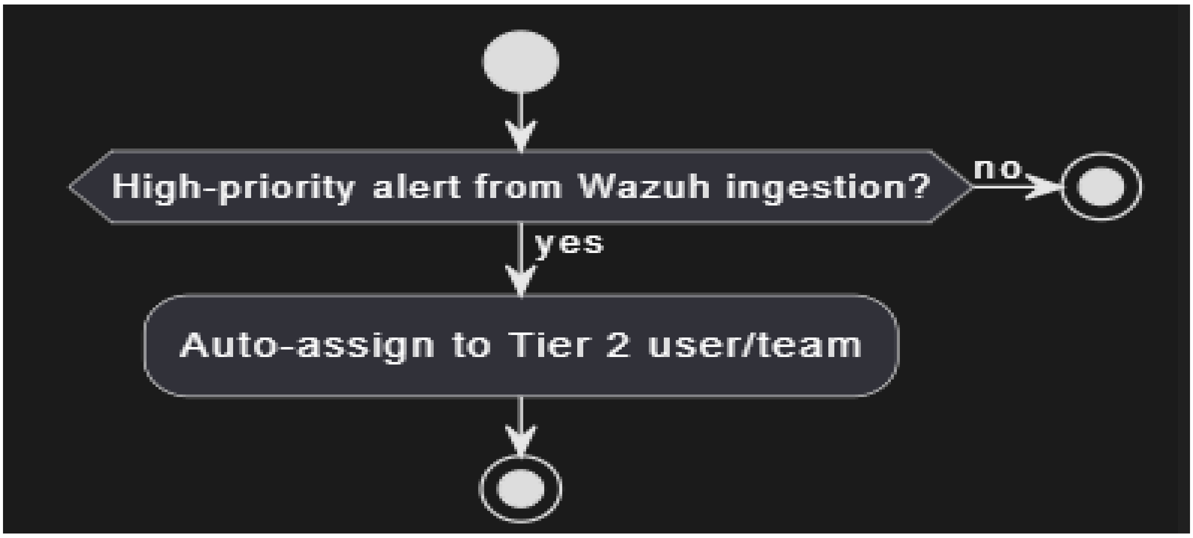
Detected at 2025-08-18 13:00, IP: 10.0.2.15, MITRE T1078.

Actions Taken:

- Isolated Server-Y.

- Escalated to Tier 2.

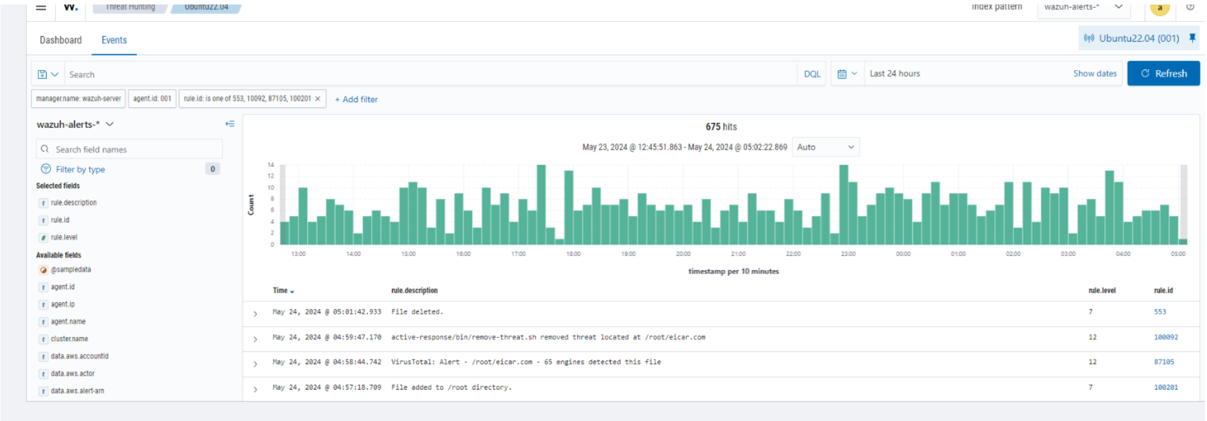
3.3 Workflow Automation – Splunk Phantom Playbook


High-priority alert from Wazuh ingestion?
no
yes
Auto-assign to Tier 2 user/team

Task 4: Alert Triage with Threat Intelligence
Objective: Triage alerts and validate IOCs.
Tools: Wazuh, VirusTotal, OTX
Execution:

- Analyzed a mock alert for suspicious PowerShell execution.
- Cross-referenced alert indicators with VirusTotal and OTX.

Mock sample:



manager.name: wazuh-server | agent.id: 001 | rule.id: is one of 553, 10092, 87105, 100201

675 hits

May 23, 2024 @ 12:45:51.863 - May 24, 2024 @ 05:02:22.869 Auto

Time	rule.description	rule.level	rule.id
May 24, 2024 @ 05:01:42.933	File deleted.	7	553
May 24, 2024 @ 04:59:47.170	active-response/bin/remove-threat.sh removed threat located at /root/eicar.com	12	100092
May 24, 2024 @ 04:58:44.742	VirusTotal: Alert - /root/eicar.com - 65 engines detected this file	12	87105
May 24, 2024 @ 04:57:18.709	File added to /root directory.	7	100201

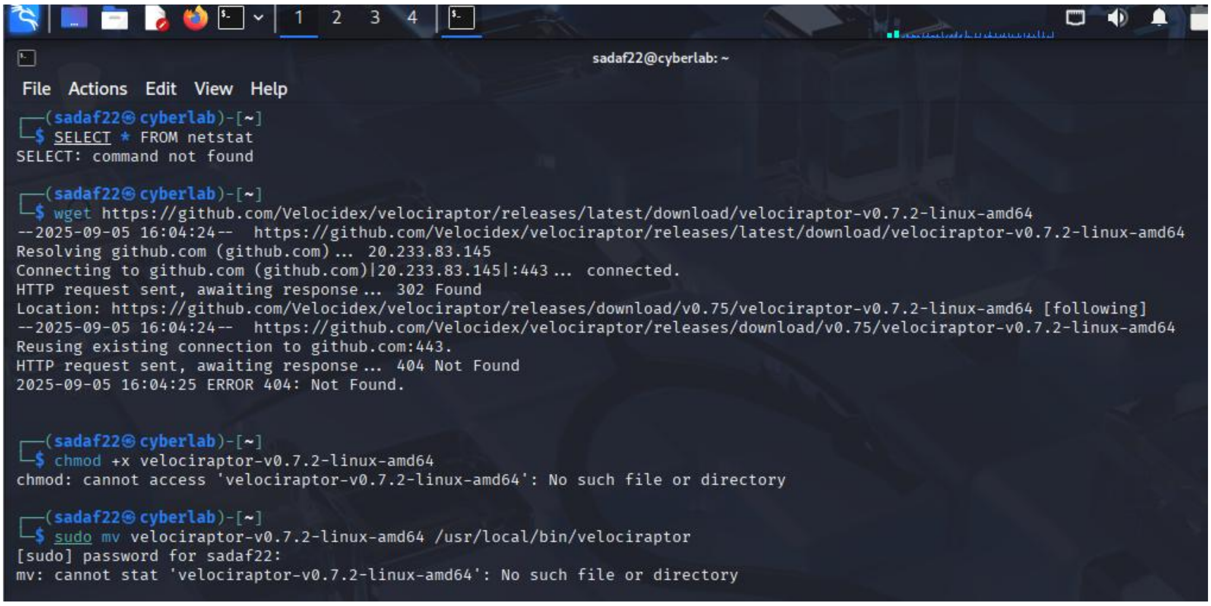
Summary (50 words):
Hash analysis showed detection by multiple AV engines. OTX linked the IP to recent credential theft campaigns. Evidence aligns with malicious PowerShell execution used for downloading payloads. Block indicators, reimage endpoint, and monitor outbound traffic for persistence attempts.

Task 5: Evidence Preservation and Analysis
Objective: Preserve forensic evidence with integrity.
Tools: Velociraptor, FTK Imager

Execution:

- Collected netstat output and saved as CSV.
- Acquired a memory dump and calculated SHA256 hash.

Screenshot Placeholder:



```
┌──(sadaf22㉿cyberlab)-[~]
└─$ SELECT * FROM netstat
SELECT: command not found

┌──(sadaf22㉿cyberlab)-[~]
└─$ wget https://github.com/Velocidex/velociraptor/releases/latest/download/velociraptor-v0.7.2-linux-amd64
--2025-09-05 16:04:24--  https://github.com/Velocidex/velociraptor/releases/latest/download/velociraptor-v0.7.2-linux-amd64
Resolving github.com (github.com)... 20.233.83.145
Connecting to github.com (github.com)|20.233.83.145|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/Velocidex/velociraptor/releases/download/v0.75/velociraptor-v0.7.2-linux-amd64 [following]
--2025-09-05 16:04:24--  https://github.com/Velocidex/velociraptor/releases/download/v0.75/velociraptor-v0.7.2-linux-amd64
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 404 Not Found
2025-09-05 16:04:25 ERROR 404: Not Found.


┌──(sadaf22㉿cyberlab)-[~]
└─$ chmod +x velociraptor-v0.7.2-linux-amd64
chmod: cannot access 'velociraptor-v0.7.2-linux-amd64': No such file or directory

┌──(sadaf22㉿cyberlab)-[~]
└─$ sudo mv velociraptor-v0.7.2-linux-amd64 /usr/local/bin/velociraptor
[sudo] password for sadaf22:
mv: cannot stat 'velociraptor-v0.7.2-linux-amd64': No such file or directory
```

3. Conclusion

This lab provided hands-on experience across the SOC lifecycle log analysis, threat intelligence integration, escalation, triage, evidence handling, and end-to-end incident response. Through simulation, we demonstrated how to detect, investigate, contain, and report real-world threats. The capstone tied all components together in a practical SOC workflow.

References

1. Elastic Security. *Elastic SIEM and Security Analytics Documentation*. Elastic, 2025. Available at: https://www.elastic.co/guide/en/security/current/index.html
2. Security Onion Solutions. *Security Onion Documentation*. Security Onion, 2025. Available at: https://docs.securityonion.net
3. MITRE ATT&CK®. *Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) Framework*. MITRE Corporation, 2025. Available at: https://attack.mitre.org
4. AlienVault. *Open Threat Exchange (OTX) Platform Documentation*. AT&T Cybersecurity, 2025. Available at: https://otx.alienvault.com
5. Wazuh. *Wazuh Documentation – Security Monitoring and Threat Detection*. Wazuh, Inc., 2025. Available at: https://documentation.wazuh.com
6. TheHive Project. *TheHive Documentation – Incident Response Platform*. TheHive Project, 2025. Available at: https://docs.thehive-project.org

7. VirusTotal. *VirusTotal Documentation*. Google, 2025. Available at: https://docs.virustotal.com