Security Operations Center (SOC) – Theory & Practical Lab Documentation

1. Introduction

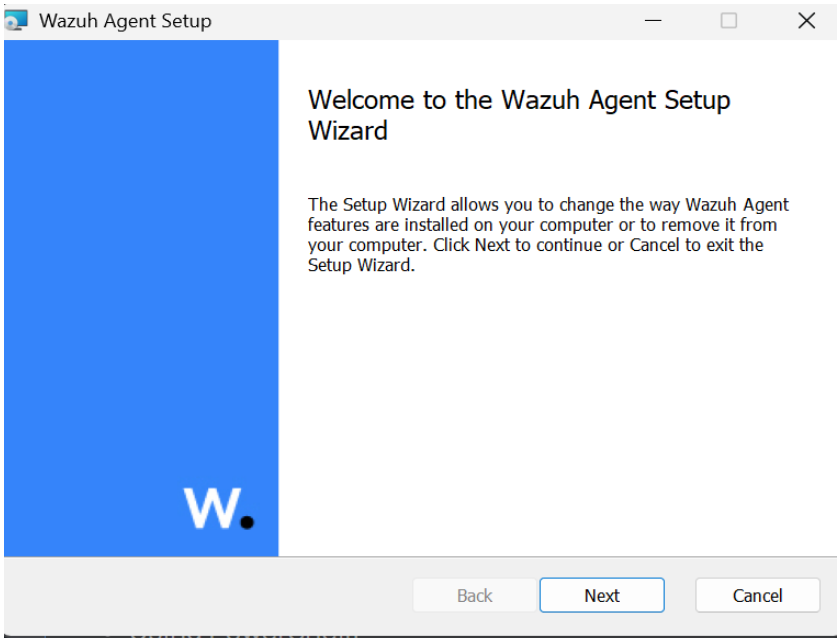
The Security Operations Center (SOC) is the centralized unit for monitoring, detecting, analyzing, and responding to cybersecurity incidents.
This document combines theoretical knowledge with hands-on practical activities to help develop both understanding and operational skills in SOC workflows.

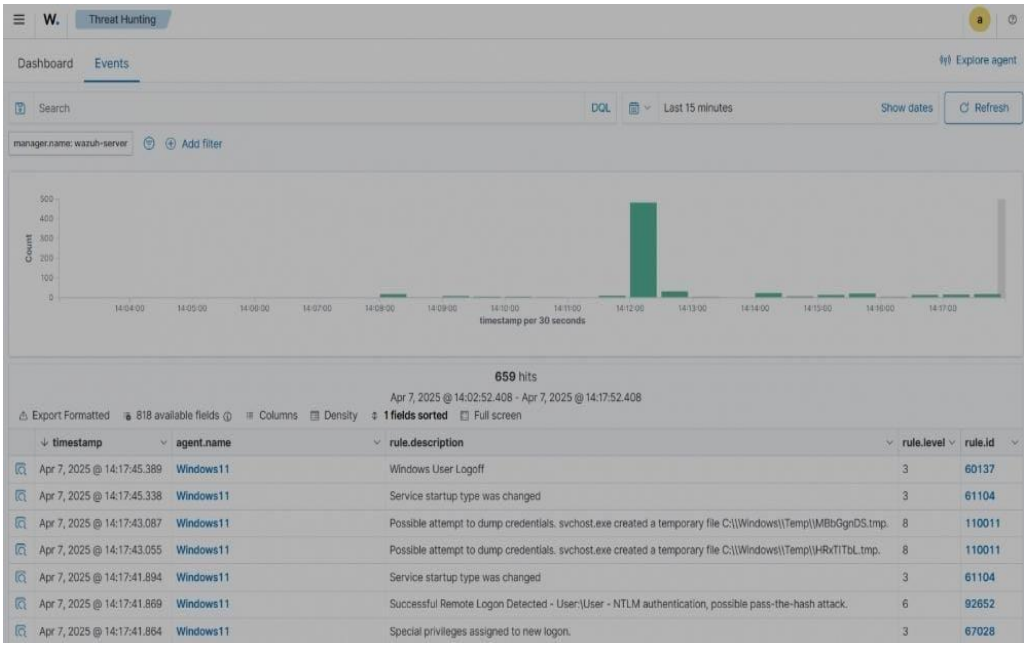
2. Theoretical Knowledge & Practical Applications

2.1 SOC Fundamentals and Operations

Purpose: Proactive threat detection, incident response, and continuous monitoring.
Roles: Tier 1/2/3 Analysts, SOC Manager, Threat Hunters.
Key Functions: Log analysis, alert triage, threat intelligence integration.
Frameworks: NIST Cybersecurity Framework, MITRE ATT&CK.
Practical Task:

- **Tool:** Wazuh / Splunk Phantom.
- **Activity:** Create an automated playbook for a phishing incident.
- **Steps:**
    1. Configure email alert ingestion.
    2. Set automated triage actions (IP lookup, URL scan).
    3. Test with a simulated phishing email.
- **Evidence:** Screenshot of triggered playbook and actions taken.

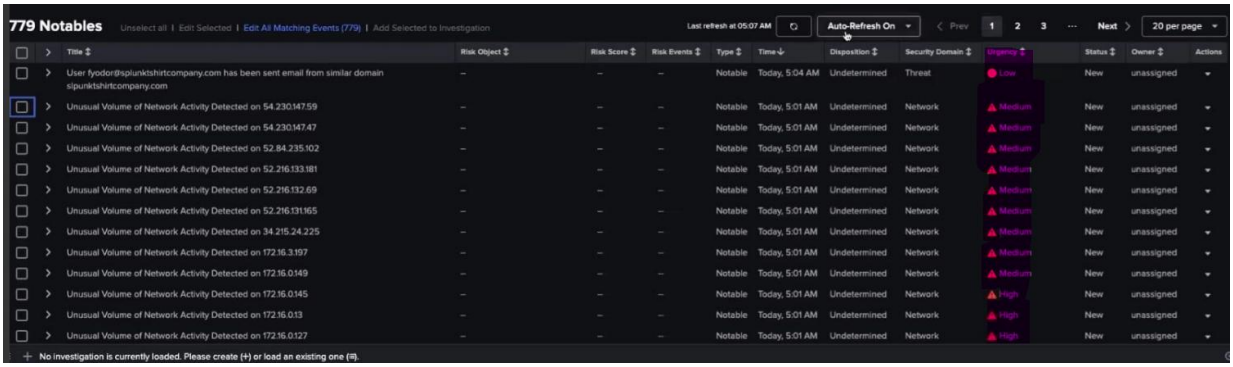




2.2 Security Monitoring Basics

Objective: Detect anomalies, unauthorized access, and policy violations.
Tools: SIEM (Splunk, Elastic SIEM).
Metrics: False positives/negatives, MTTD.
Practical Task:

- **Tool:** Elastic SIEM.
- **Activity:** Import and analyze “Boss of the SOC” dataset.
- **Evidence:** Annotated screenshot of flagged events.



Suspicious Patterns

1. **Multiple “Unusual Volume of Network Activity Detected” Alerts**
    - Repeated alerts from different IP addresses within the same minute (5:01 AM) — could indicate scanning, brute-force attempts, or data exfiltration attempts.
2. **Similar Time Stamps**

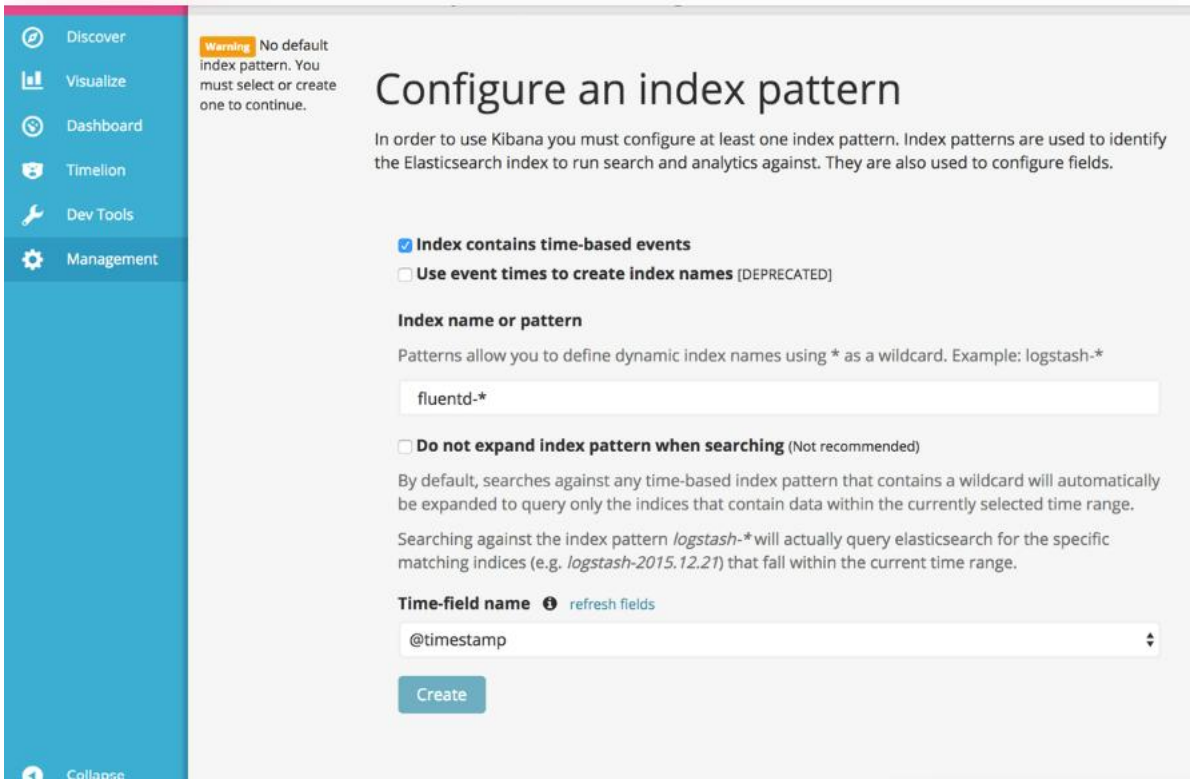
   - All events are clustered in a very short time window (5:01 AM to 5:04 AM), which is unusual for normal traffic patterns and points toward a coordinated or automated activity.
3. **Multiple Alerts from Same IP Addresses**
   - IP **172.16.9.105** triggered three alerts in quick succession.
   - IP **172.16.9.106** also triggered multiple alerts.
   - Suggests persistent or repeated probing/connection attempts.
4. **High Urgency Alerts Present**
   - Two alerts marked as **High** urgency from the 172.16.x.x subnet — likely internal network hosts showing abnormal activity, which might indicate an insider threat or compromised machine.

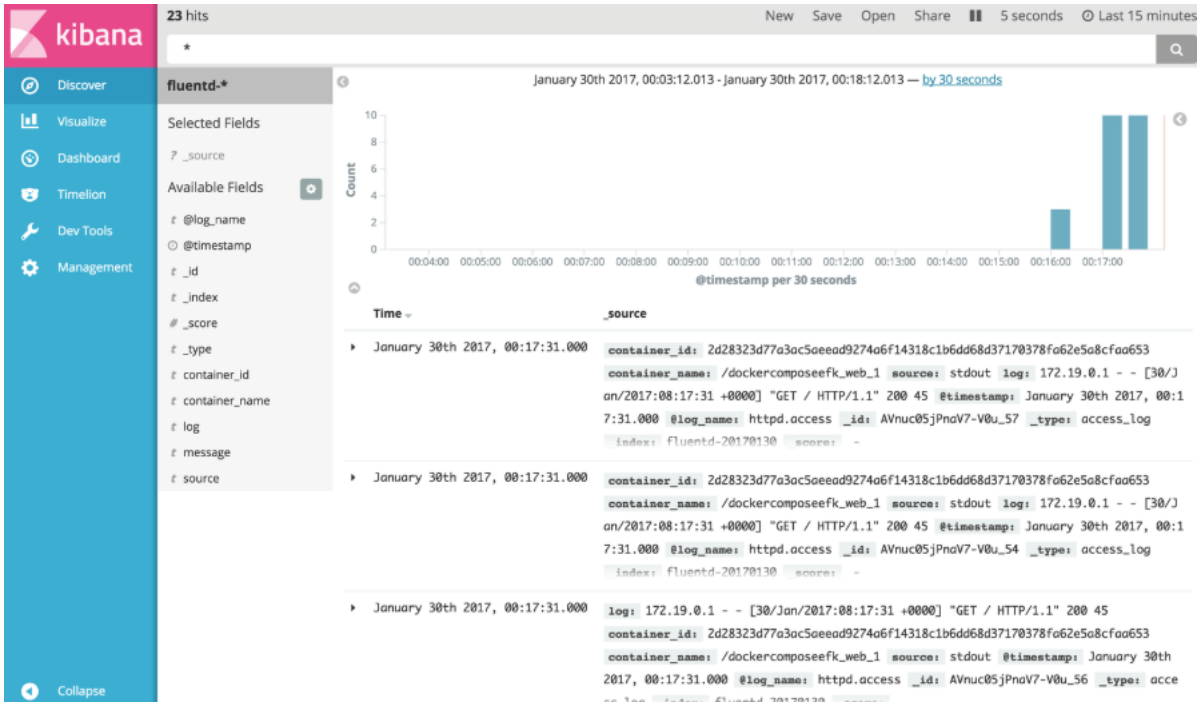
Documented Anomalies

- **Internal IP Anomalies**: Multiple internal IPs (172.16.x.x) generating high and medium urgency alerts at the same time.
- **Burst of Activity**: Events occurred in a very short timeframe, suggesting a spike rather than normal usage.
- **Different Geolocations Possible**: Presence of multiple public IPs (54.x.x.x, 52.x.x.x, 34.x.x.x) in the same time range may suggest external connections or scanning attempts from multiple sources.
- **Mixed Urgency Levels in the Same Burst**: Indicates possibly related events but with varying detected severities.

2.3 Log Management Fundamentals
Lifecycle: Collection → Normalization → Storage → Retention → Analysis.
Log Types: Windows Event Logs, Syslog, Apache logs.
Normalization Format: JSON, CEF.
Practical Task:

- **Tool:** Fluentd + Elastic SIEM.
- **Activity:** Forward Syslog messages to SIEM.
- **Steps:**
  1. Install Fluentd on Ubuntu.
  2. Run logger "Test message".
  3. Verify log in SIEM.
- **Evidence:** Screenshot of received log.





2.4 Security Tools Overview

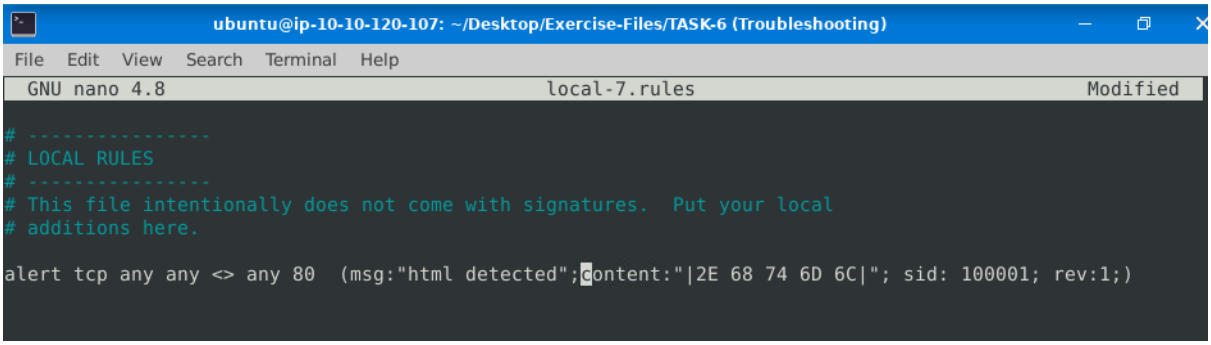
Categories:

- SIEM: Splunk, QRadar.

- EDR: CrowdStrike.
- IDS/IPS: Snort.
- Vulnerability Scanners: Nessus.

Practical Task:

- **Tool:** Snort.
- **Activity:** Create detection rule for malicious domain.
- **Steps:**
    1. Install Snort.
    2. Add rule:
    3. tcp any any -> any 80 (msg:"Malicious Domain"; content:"malicious.com"; http_uri; sid:1000001;)
    4. Test with curl http://malicious.com.
- **Evidence:** Screenshot of Snort alert.



2.5 Basic Security Concepts

CIA Triad: Confidentiality, Integrity, Availability.

Key Differences: Threat vs Vulnerability vs Risk.

Principles: Defense-in-depth, Zero Trust.

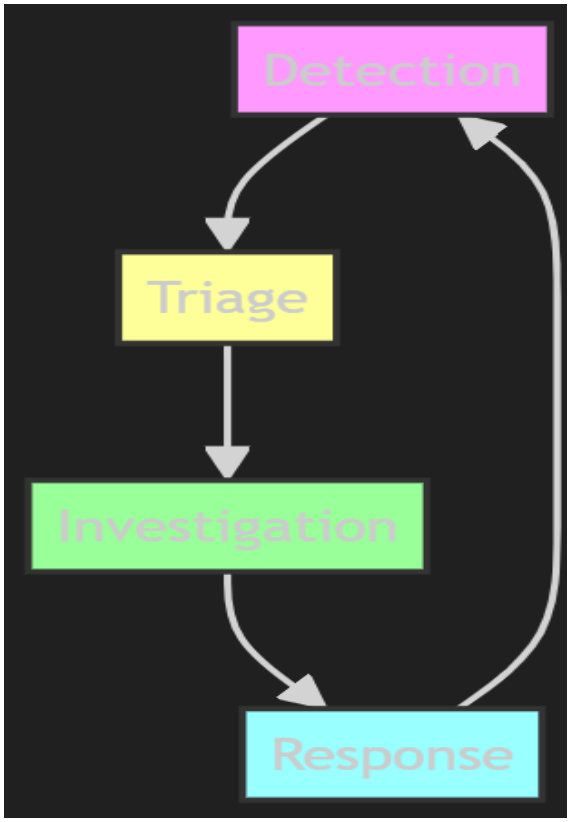
Practical Task:

- **Tool:** Case study review.
- **Activity:** Analyze Equifax breach and identify failed security controls.
- **Evidence:** Summary:
- The 2017 Equifax data breach compromised the personal information of approximately 147 million individuals, including Social Security numbers, birth dates, addresses, and in some cases, driver's license numbers. The breach was primarily caused by Equifax's failure to patch a known vulnerability (Apache Struts CVE-2017-5638) despite public disclosure and available security updates. This unpatched flaw allowed attackers to exploit the web application and gain unauthorized access to sensitive data.
- Key failed security controls included:
- **Patch Management Deficiency** – The organization failed to promptly apply critical security patches.

- **Inadequate Vulnerability Management** – Insufficient scanning and monitoring processes allowed the vulnerability to remain undetected for months.
- **Weak Network Segmentation** – Sensitive personal data was stored in systems accessible from the compromised environment without adequate isolation.
- **Lack of Strong Data Encryption** – Some sensitive data was not encrypted at rest, increasing exposure.
- **Poor Incident Detection and Response** – The breach went undetected for over two months, indicating gaps in intrusion detection and response capabilities.
- This case highlights the importance of timely patching, continuous vulnerability assessment, strong network segmentation, data encryption, and proactive monitoring to prevent and mitigate large-scale data breaches.

2.6 Security Operations Workflow
Stages: Detection → Triage → Investigation → Response.
Practical Task:

- **Tool:** TheHive.
- **Activity:** Simulate phishing incident escalation workflow.
- **Evidence:** Screenshot of workflow diagram.



2.7 Incident Response Basics

IR Lifecycle: Preparation → Identification → Containment → Eradication → Recovery → Lessons Learned.

Practical Task:

- **Tool:** NIST IR Playbook.
- **Activity:** Simulate ransomware tabletop exercise.
- **Evidence:** Completed IR checklist.

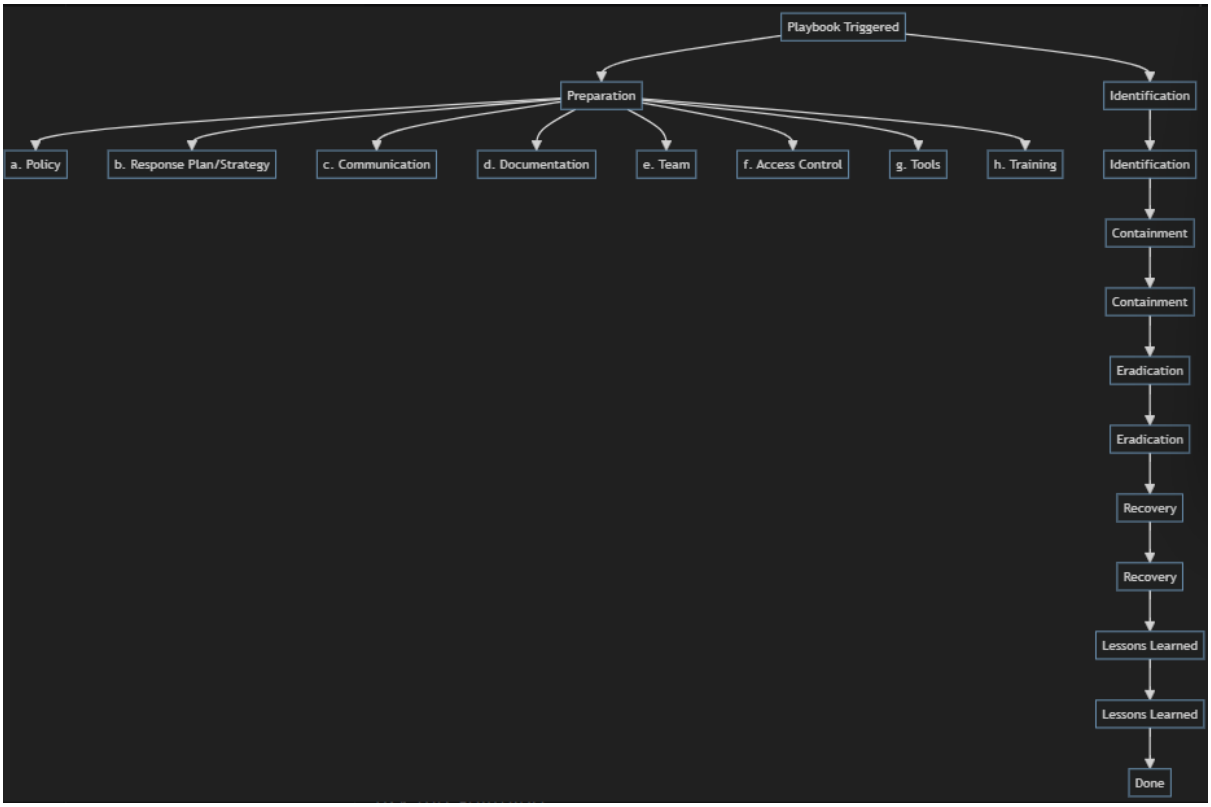
Responsible Team	Detect & Analyse	Response (Containment)	Response (Eradicate)	Recover (Systems/Services)
IT Team	- Monitor and analyze alerts from antivirus, EDR, and SIEM tools for ransomware indicators. - Identify affected devices and isolate them from the network immediately.	- Disconnect infected devices from the network (wired/wireless). - Instruct remote employees to shut down and ship devices to IT for inspection. - Disable compromised accounts.	- Remove malicious files and processes using security tools. - Patch exploited vulnerabilities. - Reset all compromised credentials.	- Restore clean backups for affecte systems. - Re-image compromised devices. - Verify system integrity before reconnecting to the network.
Communications – Internal	- Gather information from staff regarding suspicious activity (e.g., phishing emails).	- Provide updates to staff about containment actions. - Clarify which data and services are impacted.	- Keep employees informed of progress during eradication. - Share guidance on safe system usage after cleanup.	- Notify staff once systems are restored. - Provide instructions for passworc resets and MFA setup.
Communications – External	- Monitor public chatter and news for mentions of the incident. - Track potential customer complaints or questions.	- Coordinate with PR to prepare an official holding statement. - Maintain consistent messaging to the public.	- Issue factual updates as approved by Legal. - Counter misinformation.	- Publish recovery updates for customers and partners. - Confirm service restoration timelines.
Legal	- Assess breach in relation to laws/regulations (e.g., GDPR, HIPAA).	- Approve public communications and customer notifications. - Ensure compliance with breach disclosure laws.	- Oversee removal of unlawful data access. - Review contracts for liability clauses.	- Ensure recovery steps meet legal standards. - Work with compliance auditors.
Crisis Coordinator	- Evaluate the scope and severity of the attack. - Determine urgency of executive-level escalation.	- Coordinate with all teams to ensure containment steps are followed. - Keep leadership informed of progress.	- Oversee eradication steps to ensure they meet the incident plan.	- Confirm restoration progress and business continuity readiness. - Organize final service validation.

2.8 Documentation Standards

Examples: Incident reports, SOPs, post-mortems.

Practical Task:

- **Tool:** SANS Incident Handler template.
- **Activity:** Document a mock DDoS incident.
- **Evidence:** Completed incident report.



3. Observations

I found it difficult to complete some of the tasks due to the unavailability of certain tools. This required me to troubleshoot issues by researching solutions across the internet, which helped me work around the limitations and proceed with the activity.

4. Conclusion

Theory–Practice Connection:

This SOC lab helped bridge theoretical knowledge with hands-on application by allowing me to analyze real-world security incidents and explore how security controls work in practice. I strengthened key skills such as incident analysis, troubleshooting, and applying investigative techniques to identify vulnerabilities and failures in security measures.

Key Skills Gained:

- Understanding of how security controls operate in a real-world SOC context.
- Analytical thinking for identifying weaknesses in systems.
- Troubleshooting and problem-solving when facing tool access issues.
- Research skills for finding alternative methods and solutions.

Suggestions for Improvement:

- Ensure that all required SOC tools are accessible and pre-tested before the lab.
- Provide clear, step-by-step alternative methods for cases where the main tools cannot be used.
- Include more simulated breach scenarios to strengthen investigative skills.

6. References

- NIST SP 800-61
- MITRE ATT&CK
- Elastic SIEM Docs
- SANS Incident Handler’s Handbook