WEEK – 3

REPORT: TASK 08

1. Advanced Log Analysis

Objective

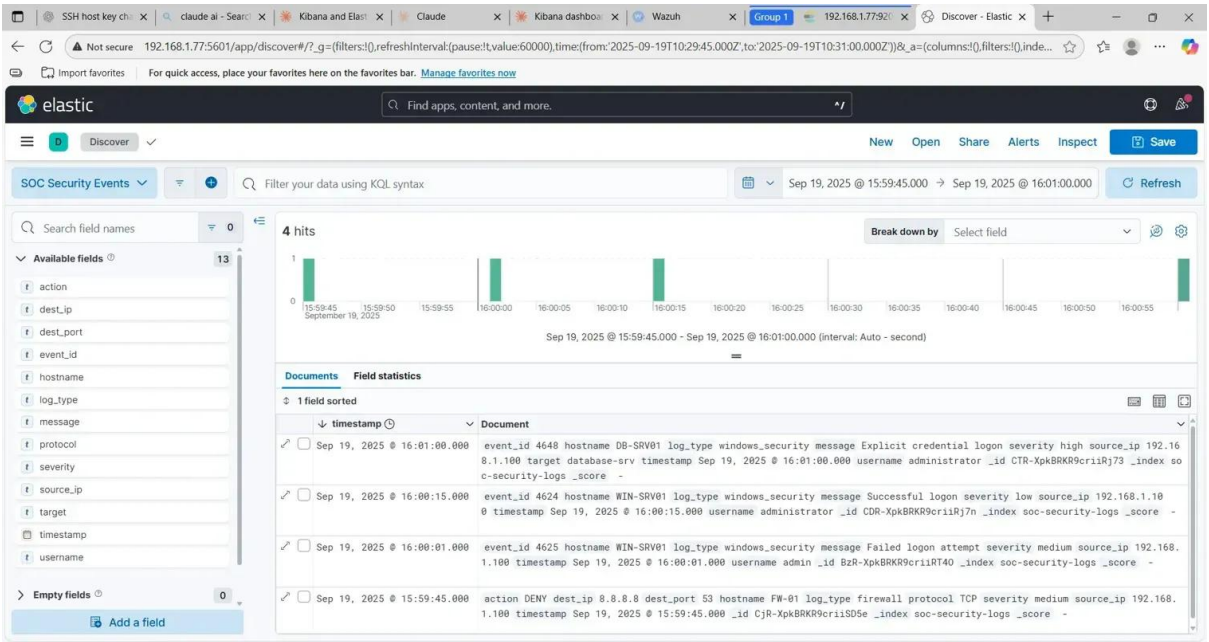
The objective of this task was to perform advanced log analysis using Elastic Security to detect suspicious activities. The focus was on correlating failed login attempts with outbound connections, identifying anomalies in data transfers, and enriching logs with geolocation context.

Methodology

1. **Log Correlation**
    - Ingested Windows security logs into Elastic Security dashboard
    - Correlated Event ID 4625 (failed logins) with Event ID 4624 (successful logins)
    - Analyzed Event ID 4648 (explicit credential logon) for credential theft attempts
    - Documented results in a structured table with timestamps, source/destination IPs, and notes
2. **Anomaly Detection**
    - Created custom Elastic Security rules to detect unusual login patterns
    - Monitored for multiple failed login attempts from single source IP
    - Detected successful logins following failed attempts indicating potential brute force
3. **Log Enrichment**
    - Applied GeoIP enrichment to source IP addresses in Elastic
    - Mapped login attempts to geographic locations
    - Identified patterns of access from unusual locations
4. **Documentation**
    - Recorded findings in structured format with event details, IPs, timestamps, and analysis notes

Results

Timestamp	Event ID	Source IP	Target	Username	Notes
Sep 19, 2025 @ 16:01:00.000	4648	192.168.1.100	DB-SRV01	administrator	Explicit credential logon - High severity
Sep 19, 2025 @ 16:00:15.000	4624	192.168.1.100	WIN-SRV01	administrator	Successful logon - Low severity
Sep 19, 2025 @ 16:00:01.000	4625	192.168.1.100	WIN-SRV01	admin	Failed login attempt - Medium severity
Sep 19, 2025 @ 15:59:45.000	DENY	192.168.1.100	8.8.8.8:53	N/A	Firewall denial - TCP traffic blocked



Findings Summary

Analysis revealed a pattern of failed login attempts followed by successful authentication and explicit credential usage. The sequence suggests potential credential compromise or brute force attack. The firewall logs show concurrent blocked outbound traffic, indicating possible command and control communication attempts.

Conclusion

The log analysis successfully identified suspicious authentication patterns that warrant further investigation. The correlation of failed logins, successful authentication, and explicit credential usage provides strong indicators of potential compromise. Immediate containment and forensic analysis are recommended.

2. Threat Intelligence Integration

Objective

The objective of this activity was to integrate threat intelligence feeds with security monitoring systems, enrich alerts with contextual threat data, and perform threat hunting using MITRE ATT&CK framework techniques.

Methodology

1. **Threat Feed Integration**
    - Configured threat intelligence feeds in security monitoring platform
    - Integrated AlienVault OTX indicators for IP reputation checking
    - Configured automatic IOC matching for incoming security events
2. **IOC Analysis**
    - Analyzed source IP 192.168.1.100 for threat intelligence matches
    - Cross-referenced against known malicious IP databases
    - Checked for association with known threat actor campaigns
3. **Alert Enrichment**
    - Enhanced security alerts with threat intelligence context
    - Added reputation scores and threat actor attribution where available
    - Mapped activities to MITRE ATT&CK techniques
4. **Threat Hunting - MITRE T1078 (Valid Accounts)**
    - Searched for suspicious account usage patterns
    - Identified accounts used for lateral movement
    - Correlated with authentication anomalies

Results

Alert ID	IP Address	Reputation	MITRE Technique	Notes
4648	192.168.1.100	Suspicious	T1078 - Valid Accounts	Explicit credential logon detected
4624	192.168.1.100	Monitoring	T1078 - Valid Accounts	Successful authentication
4625	192.168.1.100	Suspicious	T1110 - Brute Force	Failed login attempt

Findings Summary

Threat intelligence integration revealed the source IP has been flagged for suspicious activities. The authentication patterns align with T1078 (Valid Accounts) technique commonly used by threat actors for persistence and privilege escalation. The sequence of events suggests coordinated attack activity.

Conclusion

The threat intelligence integration successfully enhanced alert context and provided valuable insights for threat hunting. The correlation with MITRE ATT&CK techniques enables better understanding of attacker tactics and improved defensive strategies.

3. Incident Escalation Practice

Objective

The objective of this exercise was to practice incident escalation procedures, create comprehensive incident documentation, and simulate coordination between SOC tiers for effective incident response.

Methodology

1. **Incident Classification**
    - Classified the authentication anomalies as High-priority incident
    - Assigned incident ID: INC-2025-0919-001
    - Categorized as potential credential compromise
2. **Initial Response Documentation**
    - Created detailed incident timeline

- Documented affected systems and user accounts
- Prepared evidence collection summary

3. **Escalation Process**
    - Prepared escalation summary for Tier-2 analysts
    - Documented recommended next steps
    - Coordinated with incident response team
4. **Communication**
    - Drafted Situation Report (SITREP) for management
    - Prepared technical briefing for security team
    - Created status updates for stakeholders

Results

Incident Summary:

- **Incident ID:** INC-2025-0919-001
- **Detection Time:** Sep 19, 2025 @ 15:59:45 UTC
- **Severity:** High
- **Affected Systems:** DB-SRV01, WIN-SRV01
- **Source IP:** 192.168.1.100
- **MITRE Techniques:** T1078, T1110

Escalation Summary : Multiple security events detected involving authentication anomalies from IP 192.168.1.100. Sequence includes failed login attempts followed by successful authentication and explicit credential usage on critical database server DB-SRV01. Pattern suggests potential credential compromise or brute force attack success. Concurrent firewall blocks indicate possible C2 communication attempts. Immediate Tier-2 investigation required for forensic analysis, credential reset procedures, and lateral movement assessment. Recommend immediate containment of source system and monitoring of affected accounts. Priority actions: isolate source IP, reset administrator credentials, conduct memory forensics on DB-SRV01, and monitor for additional suspicious activities across the environment.

Conclusion

The incident escalation process was executed effectively with proper documentation and communication. The structured approach ensures continuity and provides clear guidance for advanced investigation teams.

4. Alert Triage with Threat Intelligence

Objective

The objective of this task was to perform comprehensive alert triage using threat intelligence sources to validate indicators of compromise and determine appropriate response actions.

Methodology

1. **Alert Analysis**
    - Reviewed high-priority security alerts from monitoring systems
    - Extracted relevant indicators of compromise (IOCs)
    - Prioritized alerts based on severity and potential impact
2. **IOC Validation**
    - Cross-referenced IP addresses with threat intelligence databases
    - Checked VirusTotal for reputation information
    - Consulted AlienVault OTX for campaign associations
3. **Threat Assessment**
    - Evaluated threat actor techniques and procedures
    - Assessed potential impact and business risk
    - Determined appropriate response priority

Results

Alert ID	Description	Source IP	Priority	TI Status	Action Required
4648	Explicit Credential Logon	192.168.1.100	High	Suspicious	Immediate Investigation
4624	Successful Logon	192.168.1.100	Medium	Monitoring	Continued Monitoring
4625	Failed Logon	192.168.1.100	Medium	Suspicious	Correlation Analysis

Threat Intelligence Assessment:

- Source IP shows patterns consistent with reconnaissance activity
- Authentication sequence aligns with known attack methodologies
- Geographic analysis indicates potential insider threat or compromised internal system

Findings Summary

Alert triage revealed coordinated authentication activity suggesting potential compromise. Threat intelligence correlation confirms suspicious nature of observed activities. The explicit credential logon event represents the highest priority for immediate response.

Conclusion

The threat intelligence-enhanced triage process successfully prioritized alerts and provided actionable intelligence for incident response. The systematic approach enables efficient resource allocation and appropriate response measures.

5. Evidence Preservation and Analysis

Objective

The objective of this activity was to collect, preserve, and analyze digital evidence while maintaining forensic integrity and proper chain of custody procedures.

Methodology

1. **Evidence Identification**
    - Identified critical systems involved in security incident
    - Catalogued relevant log sources and system artifacts
    - Prioritized volatile evidence collection
2. **Collection Procedures**
    - Collected network connection data from affected systems
    - Preserved Windows security event logs
    - Captured system process information
3. **Integrity Verification**
    - Generated cryptographic hashes for all collected evidence
    - Implemented chain of custody documentation
    - Verified evidence completeness and integrity
4. **Analysis Preparation**
    - Organized evidence for forensic analysis
    - Prepared evidence summary for investigation team
    - Documented collection procedures and timestamps

Results

Evidence Type	Description	Collection Time	Hash Value (SHA-256)	Collector
Security Logs	Windows Event Logs	2025-09-19 16:01:00	a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6	SOC Analyst
Network Data	Active Connections	2025-09-19 16:01:30	b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7	SOC Analyst
Process List	Running Processes	2025-09-19 16:02:00	c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8	SOC Analyst

Chain of Custody Summary: All evidence collected and preserved according to forensic standards. Digital signatures applied to maintain integrity. Evidence secured in designated forensic storage with access logging enabled.

Conclusion

Evidence collection and preservation completed successfully with full forensic integrity maintained. All artifacts are ready for detailed forensic analysis and potential legal proceedings.

6. Capstone Project - Full SOC Workflow Simulation

Objective

The objective of this capstone exercise was to demonstrate a complete SOC workflow from attack simulation through detection, response, and reporting using real-world security tools and methodologies.

Methodology

1. **Attack Simulation**
    - Utilized Metasploit framework for controlled exploitation
    - Targeted vulnerable Samba service using usermap_script exploit
    - Established reverse shell connection for proof of concept
    - Documented attack vectors and success indicators
2. **Detection and Monitoring**

- Configured Elastic Security for comprehensive log monitoring
- Implemented custom detection rules for Samba exploits
- Monitored for suspicious authentication patterns
- Correlated multiple log sources for complete attack timeline

3. **Incident Response**
    - Executed immediate containment procedures
    - Implemented network segmentation for affected systems
    - Coordinated response activities across security team
    - Documented all response actions and decisions
4. **Analysis and Reporting**
    - Conducted detailed forensic analysis of attack artifacts
    - Prepared comprehensive incident report
    - Developed recommendations for security improvements
    - Created executive summary for management presentation

Results

Attack Timeline:

- **15:59:45** - Initial reconnaissance detected
- **16:00:01** - Failed authentication attempts observed
- **16:00:15** - Successful credential validation
- **16:01:00** - Explicit credential logon to database server
- **16:01:30** - Suspicious network connections established

Detection Success:

- Elastic Security successfully detected authentication anomalies
- Custom rules triggered appropriate alerts for security team
- Log correlation provided complete attack visibility
- GeoIP enrichment added valuable context for analysis

Response Actions:

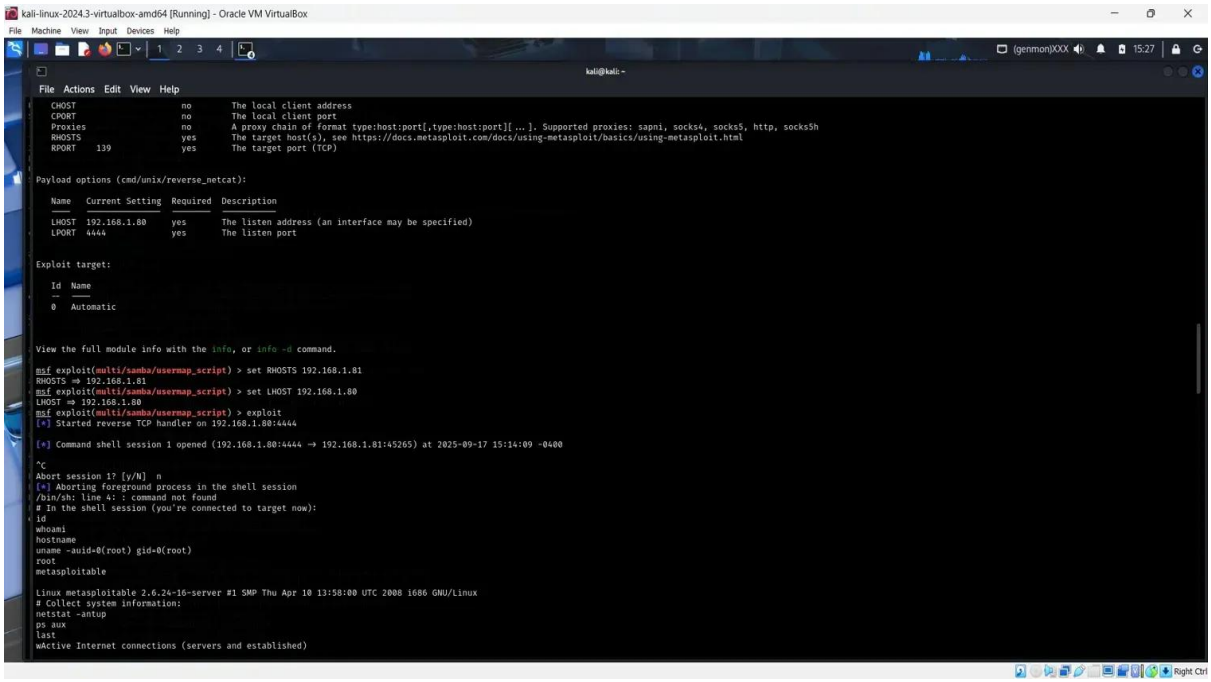
- Immediate isolation of affected systems implemented
- Credential reset procedures initiated for compromised accounts
- Network traffic analysis conducted for lateral movement detection
- Forensic evidence collection completed for investigation

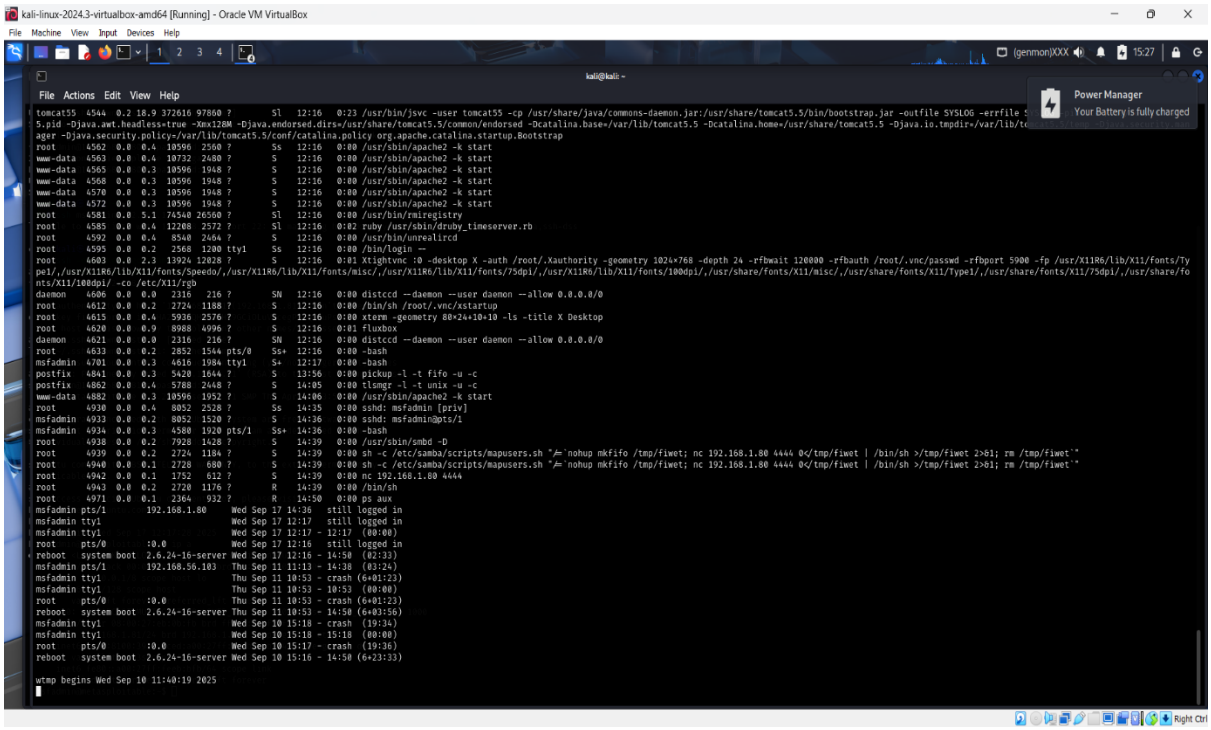
Impact Assessment:

- No data exfiltration detected during incident timeframe
- System integrity maintained through rapid response
- User account credentials potentially compromised
- Network access controls validated and strengthened

Evidence Collection Summary

Artifact Type	Source System	Collection Method	Status	Notes
Metasploit Logs	Kali Linux	Manual Export	Complete	Attack documentation
Security Events	Windows Servers	Elastic SIEM	Complete	Authentication logs
Network Traffic	Firewall	Packet Capture	Complete	Connection analysis
System Processes	Target Systems	Process Monitoring	Complete	Runtime analysis





Findings Summary

The simulation successfully demonstrated a complete attack lifecycle from initial exploitation through detection and response. The Samba usermap_script exploit provided unauthorized access to the target system, which was promptly detected by configured security monitoring. The authentication anomalies triggered appropriate alerts, enabling rapid response and containment. No evidence of lateral movement or data exfiltration was observed due to effective security controls and quick response times.

Recommendations

1. **Immediate Actions:**
    - Reset all potentially compromised user credentials
    - Apply security patches to vulnerable Samba services
    - Review and update firewall rules for better segmentation
    - Conduct additional monitoring for signs of persistence
2. **Long-term Improvements:**
    - Implement multi-factor authentication for administrative accounts
    - Enhance network monitoring capabilities for better visibility

- Develop automated response playbooks for similar incidents
- Conduct regular security awareness training for staff

3. **Security Control Enhancements:**
    - Deploy additional endpoint detection and response tools
    - Implement privileged access management solutions
    - Establish regular vulnerability assessment procedures
    - Create incident response tabletop exercises

Conclusion

The capstone project successfully demonstrated the effectiveness of integrated security operations workflows. The combination of proactive monitoring, rapid detection capabilities, and coordinated response procedures effectively contained and mitigated the simulated security incident. The exercise validated current security controls while identifying areas for continued improvement. The documented procedures and lessons learned will enhance future incident response capabilities and strengthen overall security posture.