Security Operations Center (SOC) – Incident Response Report

Intern Details

Name: Tanish Jaiswal

Role: SOC Intern

SIEM Tool Used: Elastic Stack (ELK) – Elastic Cloud

Platform: Kibana Discover

Cloud Provider: AWS

Region: Mumbai (ap-south-1)

1. Objective

This project simulates real-world **Security Operations Center (SOC)** activities, where continuous monitoring, alert analysis, and incident response are critical to protecting organizational assets.

Using **Elastic SIEM**, simulated security logs were ingested, analyzed, and investigated to identify suspicious behavior such as:

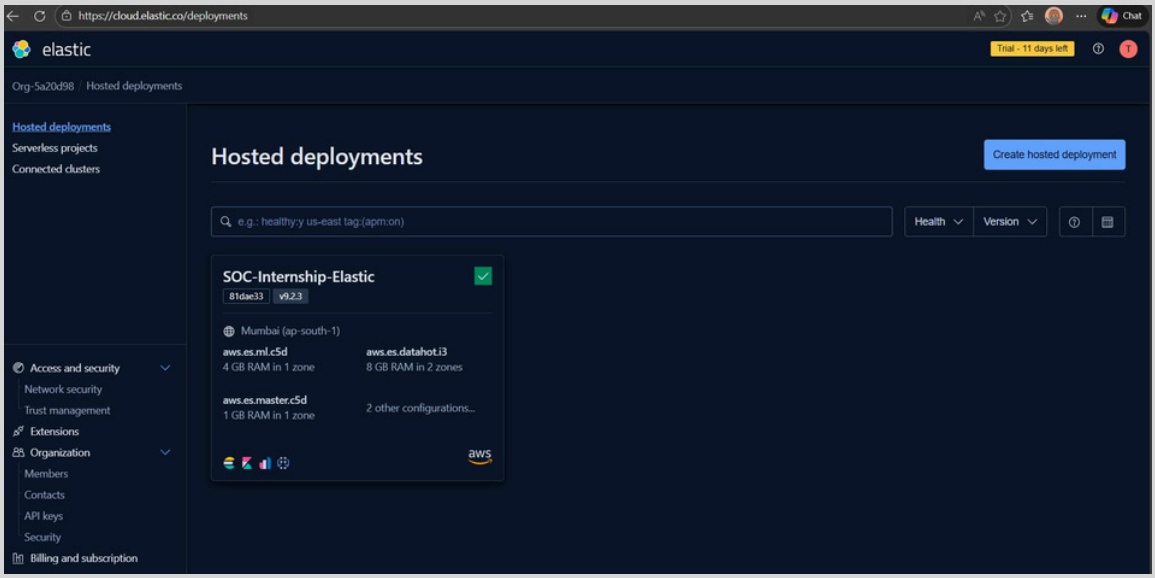
Failedloginattempts,Malwaredetections
Unauthorizedfileaccesss,UnusualIPactivity

2. Environment Setup

Elastic Cloud was deployed using AWS Mumbai (ap-south-1). Kibana Discover was used to analyze ingested logs.

Deployment Details:

Elastic Cloud Hosted Deployment
Elastic search & Kibana enabled
Index created for log ingestion



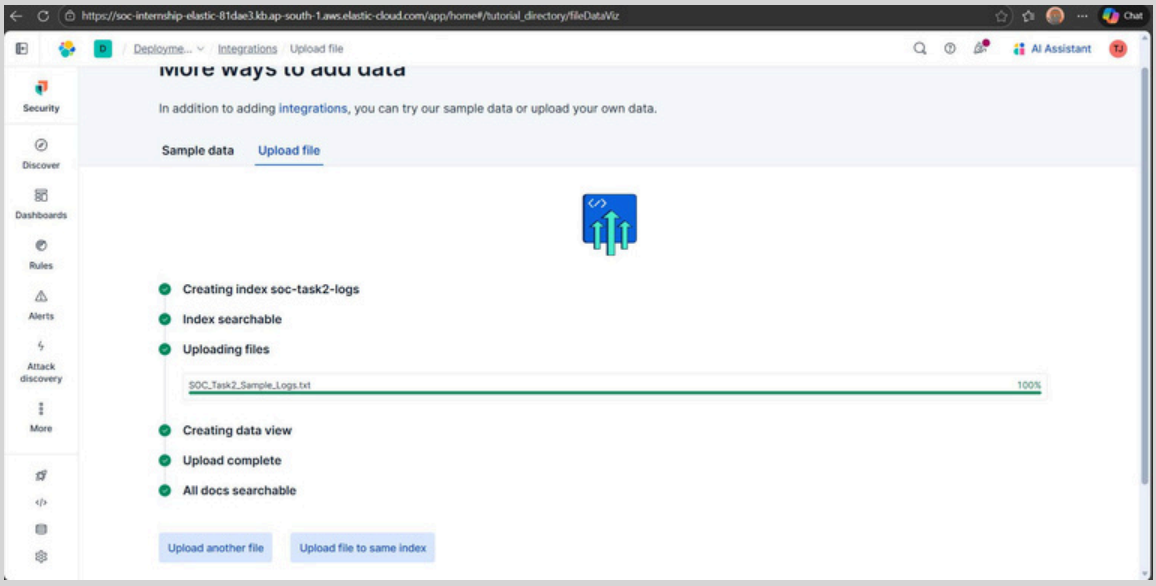
3. Log Ingestion

The provided sample log file (SOC_Task2_Sample_Logs) was uploaded using Kibana's Upload File feature, creating a new index named soc-task2-logs.

Actions Performed:

□ □ □ □

Uploaded log file
Created index: soc-task2-logs
Generated Data View
Verified log visibility in Discover

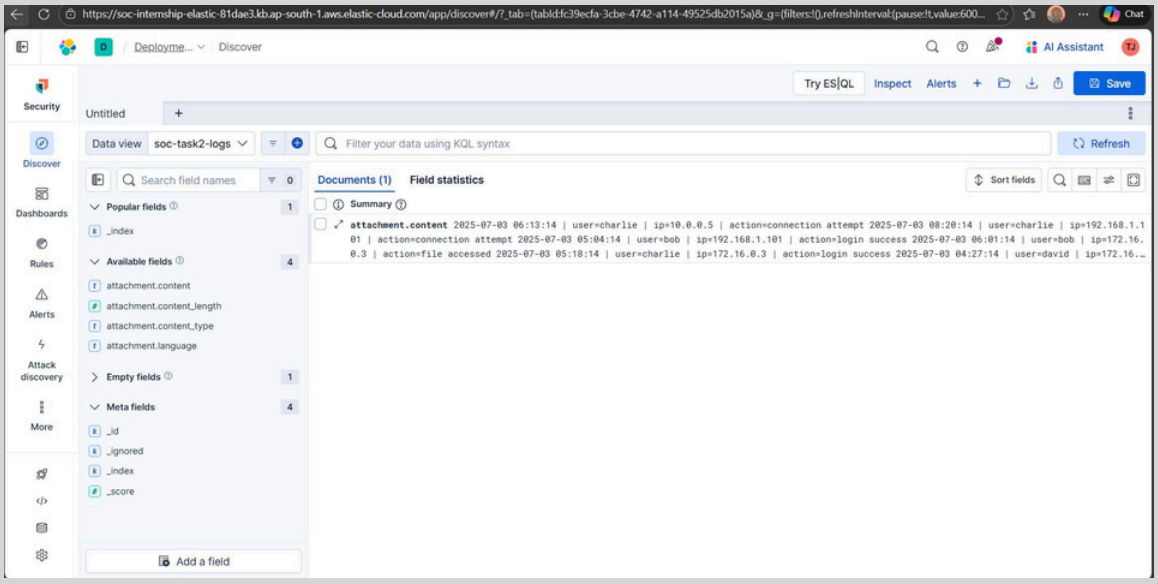


4. Log Analysis (Discover View)

Logs were analyzed in Kibana Discover using time-based filtering. Multiple security events such as login failures, malware detections, and file access were identified.

This view confirms that:

Logsweresuccessfullyingested
Time-basedeventsaresearchable
Securityincidentsarevisibleinrealtime



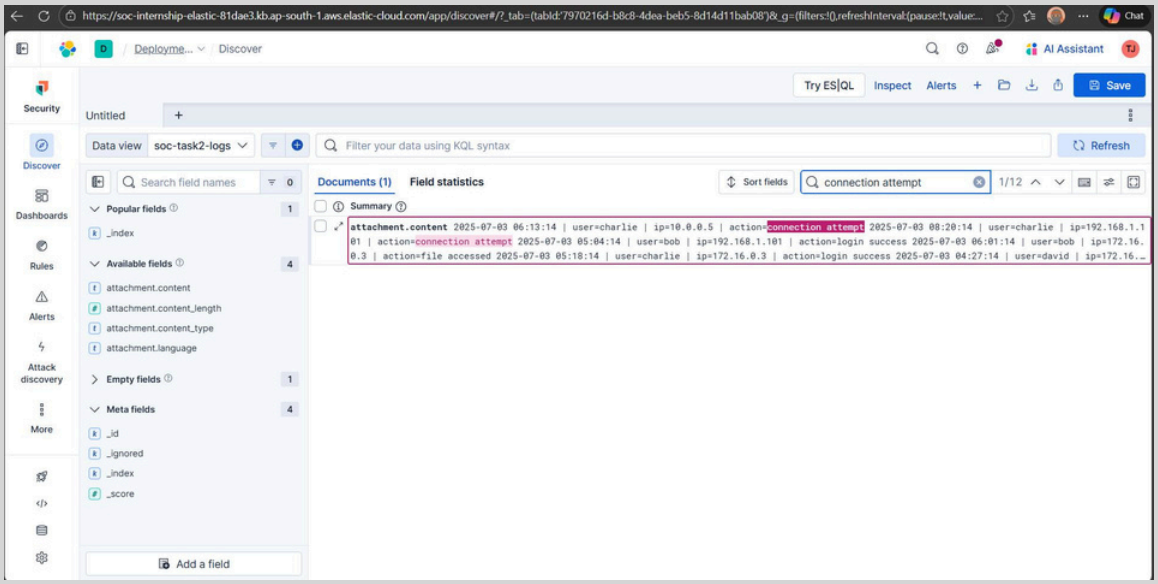
5. Identified Incidents & Severity

Incident 1: Multiple **connection attempt** events were detected, indicating reconnaissance or brute-force behavior.

Severity: Medium

Examples from logs:

- user=charlie | ip=10.0.0.5
- user=david | ip=172.16.0.3
- user=bob | ip=203.0.113.77



Impact: Risk of unauthorized account compromise. **Response:**

Monitor account activity
Enforce account lockout policies
Enable multi-factor authentication (MFA)

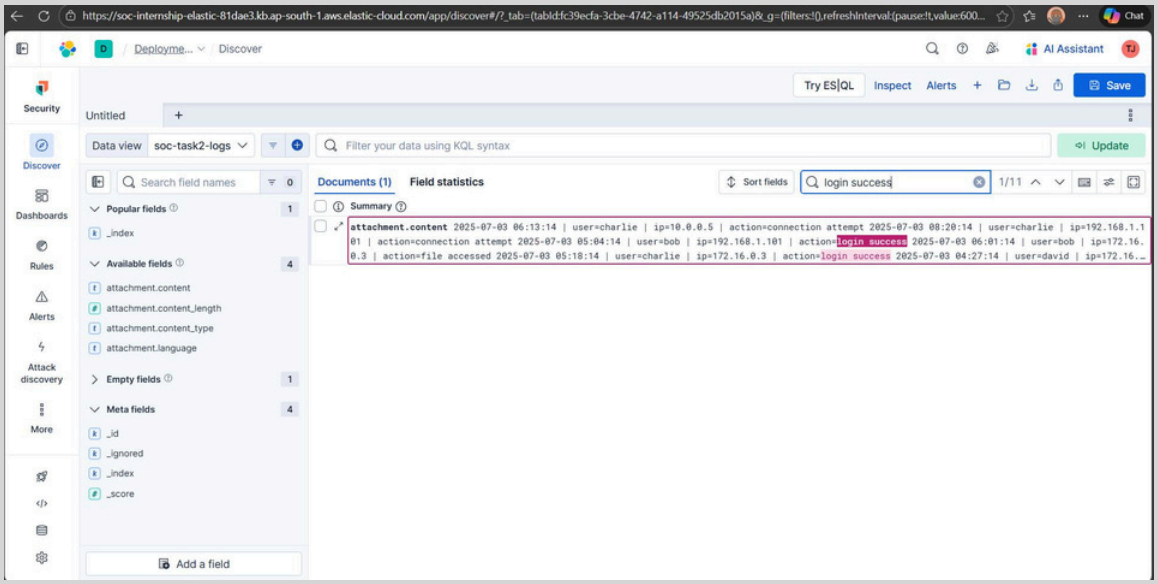
Incident 2: Both successful and failed login attempts were observed.

Severity: Medium

Successful logins: alice, bob, david, eve

Failed logins: alice, bob, david, charlie

This indicates possible credential testing or compromised accounts.



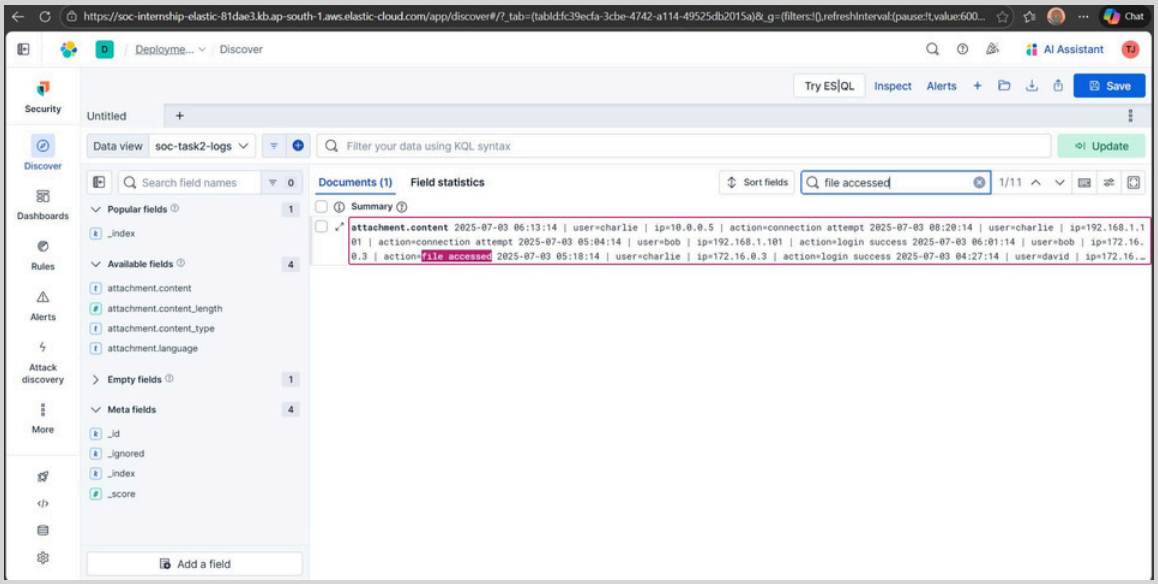
Incident 3: Several **file accessed** events occurred after login and malware detection.

Severity: Medium

Notable users: bob ,david ,eve ,charlie

Evidence:

- File access following malware alerts
- Possible data exfiltration attempt



Impact: Risk of data leakage. **Response:**
□ □

Audit accessed files
Apply least-privilege access control

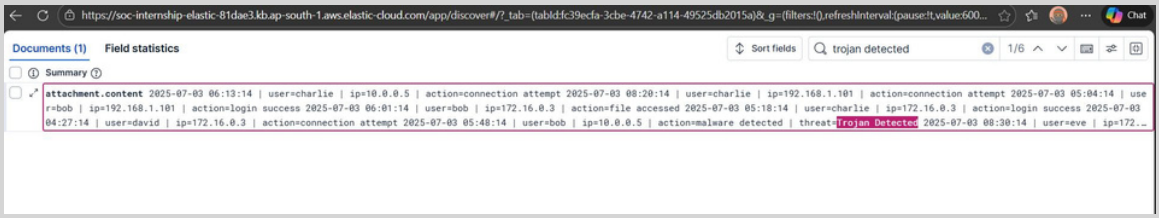
Incident 4: Multiple malware detections were identified across users and IPs.

Severity: High

Detected Threats:

Trojan Detected ,Rootkit Signature , Spyware Alert

Worm Infection Attempt , Ransomware Behavior



Impact: Potential system compromise and lateral movement. **Response:**
□ □ □

Isolate affected systems
Run antivirus scans
Patch vulnerabilities

6.Impact Assessment

Malware infections and unauthorized access attempts indicate potential system compromise, data exposure, and ransomware risk.

7. Remediation Recommendations

- Isolate infected systems
- Reset compromised credentials
- Block malicious IP addresses
- Deploy updated endpoint protection
- Enable continuous SIEM monitoring

8. Incident Communication (Email)

Subject: Security Incident Alert – Malware & Suspicious Activity Detected

Dear Management,

During routine SOC monitoring, multiple security alerts were detected including malware infections, failed login attempts, and suspicious file access.
Immediate containment steps have been initiated, and affected systems are under investigation.
Further updates will be shared as remediation progresses.

Regards,
SOC Team

9. Conclusion

This SOC simulation successfully demonstrated:

SIEMdeploymentandlogingestion
Alertidentificationandprioritization
Incidentinvestigationusingtimelines
Properdocumentationandreporting

Elastic SIEM proved effective in detecting and correlating multiple attack stages, mirroring real-world SOC operations.