

# 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

Unauthorizedfileaccessss,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

The screenshot shows the Elastic Cloud interface at <https://cloud.elastic.co/deployments>. On the left, there's a sidebar with navigation links: Hosted deployments, Serverless projects, Connected clusters, Access and security (Network security, Trust management, Extensions), Organization (Members, Contacts, API keys, Security), and Billing and subscription. The main area is titled "Hosted deployments" and shows a single entry: "SOC-Internship-Elastic". This entry includes a green checkmark icon, the ID "81daec33", and the version "v9.2.3". It also lists the region "Mumbai (ap-south-1)", two instance types ("aws.es.ml.c5d" and "aws.es.datashot.i3"), and RAM configurations. Below the entry are icons for Kibana, Logstash, Filebeat, and AWS Lambda, followed by the AWS logo.

### 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

The screenshot shows the Kibana interface at [https://soc-internship-elastic-81daec3.kb.ap-south-1.aws.elastic-cloud.com/app/home#/tutorial\\_directory/fileDataViz](https://soc-internship-elastic-81daec3.kb.ap-south-1.aws.elastic-cloud.com/app/home#/tutorial_directory/fileDataViz). The left sidebar has links for Security, Discover (selected), Dashboards, Rules, Alerts, Attack discovery, and More. The main area has tabs for "Sample data" and "Upload file" (which is selected). A progress bar shows the upload of "SOC\_Task2\_Sample\_Logs.txt" is at 100%. To the right of the progress bar, a blue icon with three vertical arrows indicates data flow. Below the progress bar, a list of steps shows the process: Creating index soc-task2-logs, Index searchable, Uploading files (with the file name listed), Creating data view, Upload complete, and All docs searchable. At the bottom are buttons for "Upload another file" and "Upload file to same index".

## 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:

- Logs were successfully ingested
- Time-based events are searchable
- Security incidents are visible in real-time

The screenshot shows the Kibana Discover interface. On the left, there's a sidebar with various navigation options like Security, Dashboards, Rules, Alerts, Attack discovery, and More. The main area is titled 'Untitled' and has a 'Data view' dropdown set to 'soc-task2-logs'. Below this is a search bar and a 'Filter your data using KQL syntax' input field. The central part of the screen displays a table with one row under 'Documents (1)'. The table has columns for '\_index' (with a value of 1), 'Field statistics' (with a value of 4), and a list of log entries. One entry is expanded, showing details about a connection attempt from user=charlie to ip=10.0.0.5 at 2025-07-03 06:13:14. Another entry shows a login success for user=bob at 2025-07-03 06:01:14. There are also entries for file access attempts from user=charlie and user=david.

_index	Field statistics	
attachment.content 2025-07-03 06:13:14   user=charlie   ip=10.0.0.5   action=connection attempt 2025-07-03 08:20:14   user=charlie   ip=192.168.1.101   action=connection attempt 2025-07-03 05:04:14   user=bob   ip=192.168.1.101   action=login success 2025-07-03 06:01:14   user=bob   ip=172.16.0.3   action=file accessed 2025-07-03 05:18:14   user=charlie   ip=172.16.0.3   action=login success 2025-07-03 04:27:14   user=david   ip=172.16.0.3	Summary	

## 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

The screenshot shows the Elasticsearch Discover interface. The left sidebar includes options for Security, Discover, Dashboards, Rules, Alerts, Attack discovery, and More. The main area has tabs for Data view (selected) and soc-task2-logs. A search bar at the top right contains the query "connection attempt". Below it, a table displays "Documents (1) Field statistics". One document is shown in detail:

attachment.content	2025-07-03 06:13:14   user=charlie   ip=10.0.0.5   action=connection attempt	2025-07-03 08:20:14   user=charlie   ip=192.168.1.01   action=login success
	01   action=connection attempt 2025-07-03 05:04:14   user=bob   ip=192.168.1.101   action=login success	2025-07-03 06:01:14   user=bob   ip=172.16.0.3   action=login success
	0.3   action=file accessed 2025-07-03 05:18:14   user=charlie   ip=172.16.0.3   action=login success	2025-07-03 04:27:14   user=david   ip=172.16.0.3   action=login success

**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.

The screenshot shows the Elasticsearch interface with the URL [https://soc-internship-elastic-81dae3.kb.ap-south-1.aws.elastic-cloud.com/app/discover/?\\_tab=\(tabledfc39efca-3cbe-4742-a114-49525db2015a\)&\\_g=\[filters:\[\],refreshInterval\[pause:lt,value:600,...\]](https://soc-internship-elastic-81dae3.kb.ap-south-1.aws.elastic-cloud.com/app/discover/?_tab=(tabledfc39efca-3cbe-4742-a114-49525db2015a)&_g=[filters:[],refreshInterval[pause:lt,value:600,...]). The left sidebar includes links for Security, Discover, Dashboards, Rules, Alerts, Attack discovery, and More. The main area displays a search bar with the query "login success" and a table of search results. The table has columns for "Documents (1)" and "Field statistics". One document is expanded, showing fields like \_index, attachment.content, and \_id.

Documents (1)	Field statistics
<input type="checkbox"/> <a href="#">attachment.content</a> 2025-07-03 06:13:14   user=charlie   ip=10.0.0.5   action=connection attempt 2025-07-03 08:20:14   user=charlie   ip=192.168.1.101 01   action=connection attempt 2025-07-03 05:04:14   user=bob   ip=192.168.1.101   action=login success 2025-07-03 06:01:14   user=bob   ip=172.16.0.3   action=file accessed 2025-07-03 05:18:14   user=charlie   ip=172.16.0.3   action=login success 2025-07-03 04:27:14   user=david   ip=172.16.0.3	<input type="checkbox"/> <a href="#">Summary</a>

**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

The screenshot shows the Elastic Cloud interface with the URL [https://soc-internship-elastic-81dae3kb.ap-south-1.aws.elastic-cloud.com/app/discover#/?\\_tab=\(tablefc39ecfa-3cbe-4742-a114-49525db2015a\)&\\_g=\(filters:\[\],refreshInterval:\[pause:lt,value:600...](https://soc-internship-elastic-81dae3kb.ap-south-1.aws.elastic-cloud.com/app/discover#/?_tab=(tablefc39ecfa-3cbe-4742-a114-49525db2015a)&_g=(filters:[],refreshInterval:[pause:lt,value:600...)

The left sidebar includes navigation links for Security, Discover, Dashboards, Rules, Alerts, Attack discovery, and More. The main area displays a search interface with a "Data view" dropdown set to "soc-task2-logs". A search bar contains the query "file accessed". The results are shown in a table with two tabs: "Documents (1)" and "Field statistics". The "Documents" tab lists one document with the following details:

attachment.content	2025-07-03 06:13:14	user	charlie	ip	10.0.0.5	action	connection attempt	2025-07-03 08:20:14	user	charlie	ip	192.168.1.1			
	01	action	connection attempt	2025-07-03 05:04:14	user	bob	ip	192.168.1.101	action	login success	2025-07-03 06:01:14	user	bob	ip	172.16.0.3
	0.3	action	"file accessed"	2025-07-03 05:18:14	user	charlie	ip	172.16.0.3	action	login success	2025-07-03 04:27:14	user	david	ip	172.16.0.1

The "Field statistics" tab shows the following counts for fields:

- attachment.content: 1
- \_index: 4
- attachment.content\_length: 4
- attachment.content\_type: 4
- attachment.language: 4
- Empty fields: 1
- Meta fields: 4
- \_id: 4
- \_ignored: 4
- \_index: 4
- \_score: 4

At the bottom, there is a button to "Add a field".

**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



```
attachment.content 2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt 2025-07-03 08:20:14 | user=bob | ip=192.168.1.101 | action=login success 2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed 2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success 2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt 2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat:Trojan Detected 2025-07-03 08:20:14 | user=eve | ip=172.1...
```



```
attachment.content 2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt 2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success 2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed 2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success 2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt 2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat:Trojan Detected 2025-07-03 08:30:14 | user=eve | ip=172.1...
```

**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:

- SIEM deployment and log ingestion
- Alert identification and prioritization
- Incident investigation using timelines
- Proper documentation and reporting

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

THANK  
YOU