SECURITY ALERT MONITORING & INCIDENT RESPONSE

Comprehensive SOC Analysis Using Elastic Stack and Kali Linux

Prepared For: Future Interns

Prepared By: Doddy Shivani

Email: d.shiv1922@gmial.com

Phone: +91-9703561119

Date: 16 October 2025

Version: 1.0

CONFIDENTIAL – This report contains sensitive cybersecurity assessment information intended only for authorized recipients.

Project Overview

This repository showcases a **hands-on SOC (Security Operations Center) analysis** conducted during a **cybersecurity internship**, leveraging the **Elastic Stack (Kibana, Elasticsearch, Logstash)** and **Kali Linux**.
The project focuses on **threat detection**, **incident response**, and **remediation strategies**, with each security event mapped to the **OWASP Top 10 vulnerabilities**.

Through this project, real-world attack simulations were analyzed to strengthen proactive defense mechanisms and enhance log visibility in enterprise environments.

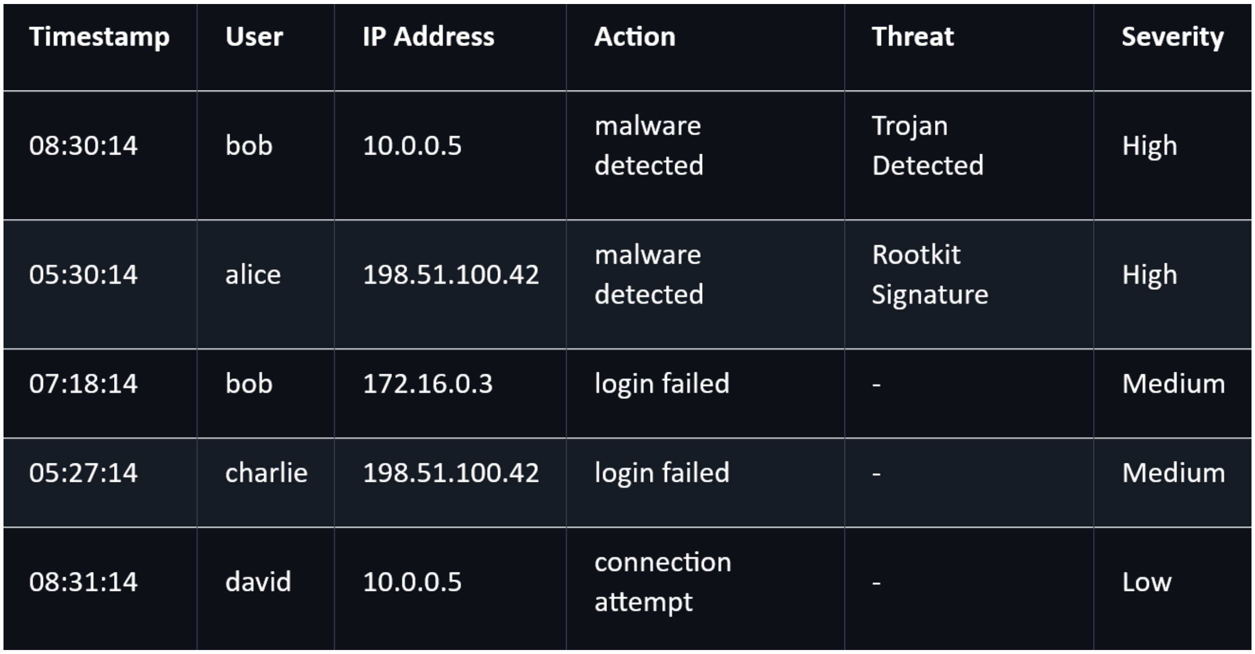
Tools & Technologies

- **Elastic Stack (Elasticsearch, Logstash, Kibana)** – For centralized logging, visualization, and analytics
- **Kali Linux** – For security testing and generating simulated attacks
- **Sample Log Files** – For threat investigation and pattern analysis
- **MS Word** – For professional reporting and documentation

Key Highlights

- **Real-Time Log Analysis:** Investigated network and system logs through **Kibana Discover** dashboards
- **Threat Detection:** Identified **malware infections (Trojan, Rootkit)** through abnormal log behaviors
- **Brute-Force & Login Failure Analysis:** Tracked unauthorized login attempts to detect **brute-force attacks**
- **Connection Attempt Monitoring:** Analyzed suspicious IP connections and potential lateral movement
- **Alert Severity Classification:** Categorized alerts based on **impact and threat level** for effective incident prioritization

Incident Timeline



Timestamp	User	IP Address	Action	Threat	Severity
08:30:14	bob	10.0.0.5	malware detected	Trojan Detected	High
05:30:14	alice	198.51.100.42	malware detected	Rootkit Signature	High
07:18:14	bob	172.16.0.3	login failed	-	Medium
05:27:14	charlie	198.51.100.42	login failed	-	Medium
08:31:14	david	10.0.0.5	connection attempt	-	Low

Recommendations

To ensure effective containment and recovery, the following **security countermeasures** were implemented:

- **Isolate Infected Hosts:** Immediately disconnect compromised systems from the network to prevent lateral spread.
- **Initiate Endpoint Malware Scans:** Perform deep scans using updated antivirus and EDR tools to eliminate malicious files.
- **Audit User Credentials:** Review authentication logs and enforce password resets for affected or suspicious accounts.
- **Monitor Flagged IP Ranges:** Continuously track and block malicious IPs to prevent recurring intrusion attempts.

Notification & Escalation Plan

A structured **incident communication workflow** was followed to maintain clarity and speed in response:

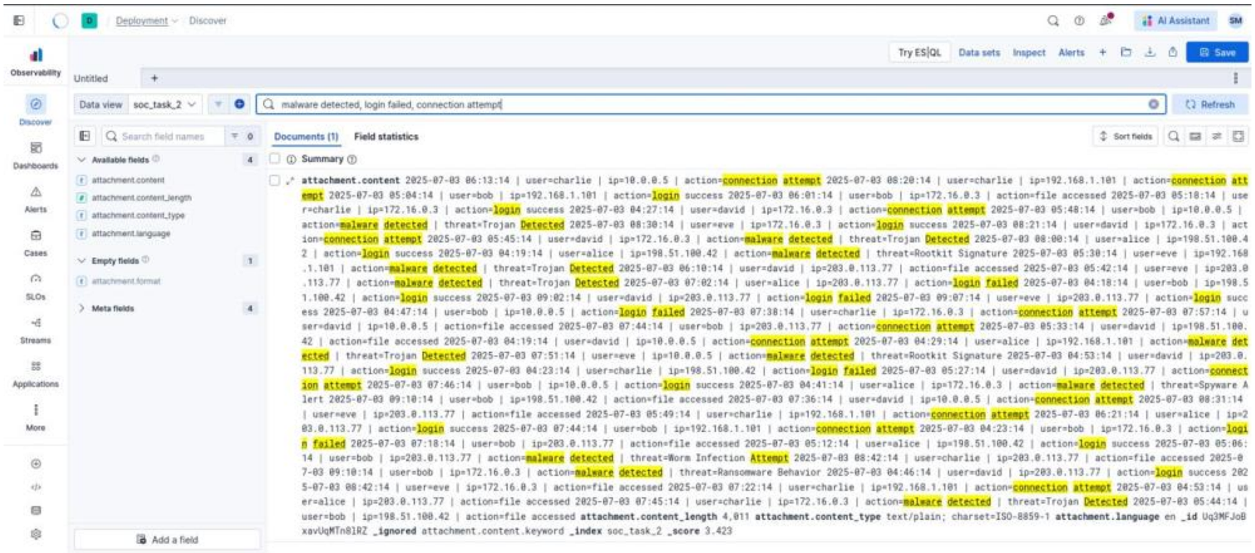
- **Alert SOC Lead:** Automated alerts triggered to notify the SOC Lead in real-time.
- **Report to IT Security Manager:** Comprehensive incident summary shared with analysis findings and next-step recommendations.

- **Prepare Containment Instructions:** Action plan distributed to system admins for immediate remediation and future prevention.

Dashboard Insights & Visualizations

Key **Kibana dashboards** were created to enhance situational awareness and visualize threat patterns:

- **Filtered Threats & Actions:** Interactive view of detected anomalies and response actions taken.
- **Alert Visualizations:** Graphical representation of incident trends, login failures, and malware detections.
- **Severity Breakdown:** Categorization of alerts into **Low**, **Medium**, **High**, and **Critical** impact levels for better prioritization.



malware detected, login failed, connection attempt

```
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 att
empt 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 | use
r=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=172.16.0.3 | action=login success 2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | act
ion=connection attempt 2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected 2025-07-03 08:00:14 | user=alice | ip=198.51.100.4
2 | action=login success 2025-07-03 04:19:14 | user=alice | ip=198.51.100.42 | action=malware detected | threat=Rootkit Signature 2025-07-03 05:30:14 | user=eve | ip=192.168
.1.101 | action=malware detected | threat=Trojan Detected 2025-07-03 06:10:14 | user=david | ip=203.0.113.77 | action=file accessed 2025-07-03 05:42:14 | user=eve | ip=203.0
.113.77 | action=malware detected | threat=Trojan Detected 2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed 2025-07-03 04:18:14 | user=bob | ip=198.5
1.100.42 | action=login success 2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed 2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login succ
ess 2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed 2025-07-03 07:38:14 | user=charlie | ip=172.16.0.3 | action=connection attempt 2025-07-03 07:57:14 | u
ser=david | ip=10.0.0.5 | action=file accessed 2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt 2025-07-03 05:33:14 | user=david | ip=198.51.100.
42 | action=file accessed 2025-07-03 04:19:14 | user=david | ip=10.0.0.5 | action=connection attempt 2025-07-03 04:29:14 | user=alice | ip=192.168.1.101 | action=malware det
ected | threat=Trojan Detected 2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature 2025-07-03 04:53:14 | user=david | ip=203.0.
113.77 | action=login success 2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed 2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connect
ion attempt 2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success 2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware A
lert 2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed 2025-07-03 07:36:14 | user=david | ip=10.0.0.5 | action=connection attempt 2025-07-03 08:31:14
| user=eve | ip=203.0.113.77 | action=file accessed 2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection attempt 2025-07-03 06:21:14 | user=alice | ip=2
03.0.113.77 | action=login success 2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt 2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=logi
n failed 2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed 2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login success 2025-07-03 05:06:
14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt 2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed 2025-0
7-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior 2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login success 202
5-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed 2025-07-03 07:22:14 | user=charlie | ip=192.168.1.101 | action=connection attempt 2025-07-03 04:53:14 | us
er=alice | ip=203.0.113.77 | action=file accessed 2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected 2025-07-03 05:44:14 |
user=bob | ip=198.51.100.42 | action=file accessed attachment.content_length 4,011 attachment.content_type text/plain; charset=ISO-8859-1 attachment.language en _id Uq3MFJoB
xavUqMTn81RZ _ignored attachment.content.keyword _index soc_task_2 _score 3.423
```