Incident Response Report – SOC Internship Project

NAME: Oderinde Toluwanimi

TASK 2: Security Operations Center (SOC) Internship Task: Security Alert Monitoring & Incident Response Simulation

PROGRAM: Future Interns Cybersecurity Internship

Date: September 2025

System Monitored: Splunk Enterprise 10.0.0

Data Source: SOC_Task2_Sample_Logs (Simulated)

Environment: Kali Linux (Lab)

1. Executive Summary

Between **June 3rd 2025 00:00:00** and **June 3rd 2025 23:59:59**, simulated security events were ingested and analyzed using Splunk SIEM. The purpose of this exercise was to emulate the activities of a Security Operations Center (SOC) analyst, including log analysis, alert creation, incident classification, and reporting.

Key findings during the monitoring window included:

- **Multiple malware detections** (including ransomware and trojans) indicating potential endpoint compromise.
- **Repeated failed login attempts** suggesting brute-force or credential-stuffing activity.
- **Suspicious successful logins from multiple IPs** pointing to possible account misuse.
- **Post-malware file access activity** that could indicate lateral movement or data exfiltration attempts.

The incidents were prioritized into **High, Medium, and Low severity levels** based on their potential impact and likelihood, and recommendations were prepared for containment, eradication, and recovery.

This report provides a comprehensive breakdown of findings, supporting evidence, and suggested remediation actions to strengthen the security posture of the environment.

2. Environment Overview

Tools and Configuration:

- **Splunk Enterprise 10.0.0**: Installed on Kali Linux, configured to ingest simulated SOC logs.
- **Data Source:** SOC_Task2_Sample_Logs.txt -- includes system, authentication, network, and malware events.
- **Index:** main
- **Sourcetype:** soc_lab

- **Extracted Fields:** user, ip, action, threat

Dashboard Panels Implemented:

1. Malware detections over time (timechart).
2. Top users with malware alerts (bar chart).
3. Failed login attempts by user and IP (table/bar).
4. Threat type distribution (bar chart).
5. Timeline of all actions (stacked area chart).

Alerts Configured:

- High severity: Ransomware detection, Trojan/Worm/Rootkit detection, Post-malware file access.
- Medium severity: Multiple failed logins, Multi-IP logins per user.

---

3. Findings

3.1 Malware Detections

- **Description:** Splunk identified multiple malware-related alerts across different user sessions, including ransomware, trojan, worm, and rootkit signatures.
- **Impact: High** -- malware presence can lead to data loss, encryption of files (ransomware), or system compromise.
- **Evidence:**

Splunk Query:

```
 index=main sourcetype=soc_lab action="malware detected"
| stats count by user, threat
```

  -
  - **Dashboard Screenshot:** Malware timechart panel showing spikes.

    - **Triggered Alerts:** “High - Ransomware Detected”.

3.2 Failed Login Attempts

- **Description:** Certain accounts (notably alice) showed excessive failed login attempts, often from the same external IP address. This pattern indicates brute-force attempts or stolen credential testing.

- **Impact: Medium** -- repeated failures degrade security posture and suggest targeted attacks.

- **Evidence:**

Splunk Query:

```
index=main sourcetype=soc_lab action="login failed"
| stats count by user, ip
| where count > 5
```

    -
    - **Dashboard Screenshot:** Failed logins by user/IP.
    - **Triggered Alerts:** “Medium - Multiple Failed Logins”.

3.3 Multi-IP Logins

- **Description:** Some users (e.g., carol) logged in successfully from multiple distinct IP addresses within a short timeframe. This behavior may suggest account compromise or credential sharing.

- **Impact: Medium** -- legitimate in rare cases, but often a red flag.

- **Evidence:**

Splunk Query:

```
 index=main sourcetype=soc_lab action="login success"
| stats dc(ip) as distinct_ips by user
| where distinct_ips > 1
```

    -
    - **Dashboard Screenshot:** Multi-IP login detection.
    - **Triggered Alerts:** “Medium - User Logged in from Multiple IPs”.

3.4 Suspicious File Access After Malware Detection

- **Description:** Logs show file access events occurring shortly after malware detection on the same host. This suggests lateral movement or an attacker attempting persistence.
- **Impact: High** -- potential compromise extending beyond initial infection.
- **Evidence:**

Splunk Query:

```
index=main sourcetype=soc_lab
| transaction user ip maxspan=1h
| search action="malware detected" action="file accessed"
```

    -
    - **Dashboard Screenshot:** Post-malware activity detection.
    - **Triggered Alerts:** “High - File Access After Malware Detection”.

---

4. Incident Classification

Timestamp	User	IP	Action	Threat	Severity	Notes
2025-07-03 09:10	bob	172.16.0.3	malware detected	Ransomware Behavior	High	Host should be isolated immediately
2025-07-03 07:02	alice	203.0.113.77	login failed	-	Medium	Possible brute-force attempt
2025-07-03 10:20	carol	10.0.0.8	login success	-	Medium	Logged in from 2 IPs in 15 minutes

---

5. Recommendations

Containment:

- Isolate affected hosts (e.g., Bob's machine) from the network.
- Block external IPs showing repeated login failures.

Eradication & Recovery:

- Perform full malware scans and wipe/rebuild infected hosts if necessary.
- Reset and enforce strong credentials for impacted accounts.
- Apply patches and updates across systems.

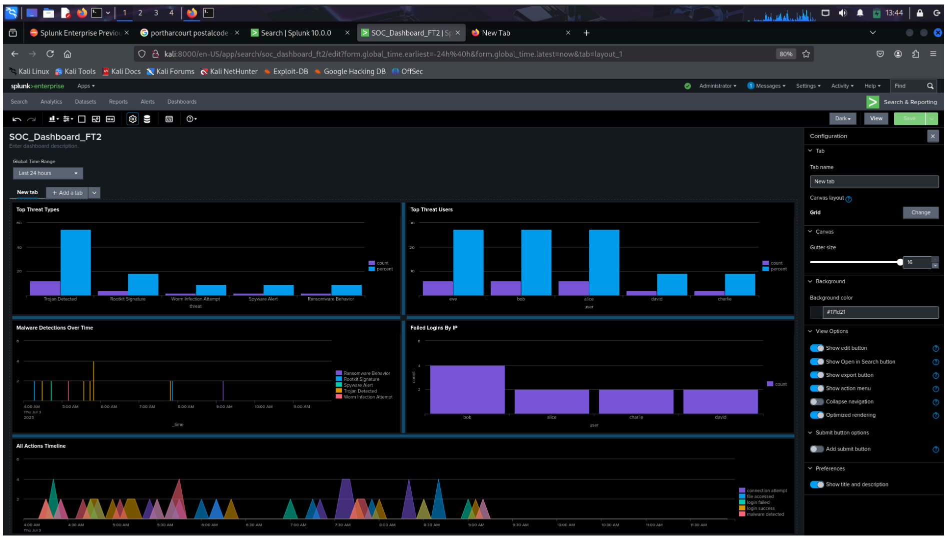
Monitoring & Prevention:

- Tune Splunk alerts to cover emerging threats.
- Enforce account lockout policies after X failed login attempts.
- Deploy endpoint detection & response (EDR) tools for deeper visibility.
- Develop SOC playbooks for common scenarios (ransomware, brute force, etc.).

---

6. Appendices

- **Appendix A:** SOC Monitoring Dashboard screenshots.



kali:8000/en-US/app/search/soc_dashboard_ft2/edit?form.global_time.earliest=-24h%40h&form.global_time.latest=now&tab=layout_1

SOC_Dashboard_FT2

Enter dashboard description.

Global Time Range: Last 24 hours

Configuration

Tab name: New tab

Canvas layout: Grid

Gutter size: 16

Background color: #171d21

View Options

- ● Show edit button
- ● Show Open in Search button
- ● Show export button
- ● Show action menu
- ○ Collapse navigation
- ● Optimized rendering

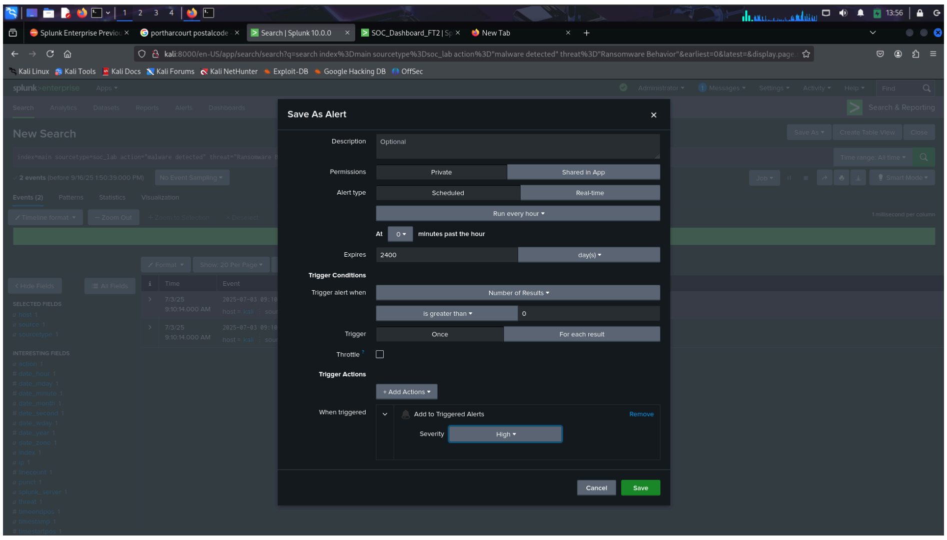
Submit button options

- ○ Add submit button

Preferences

- ● Show title and description

- **Appendix B:** Triggered Alert screenshots.

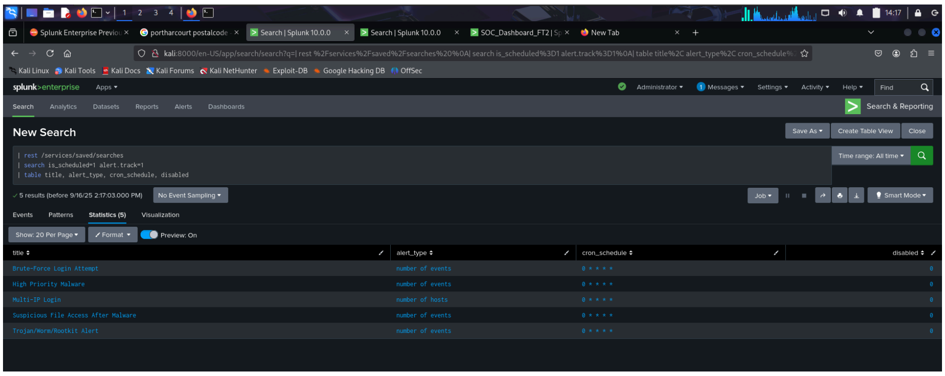


kali:8000/en-US/app/search/search?q=search index%3Dmain sourcetype%3Dsoc_lab action%3D"malware detected" threat%3D"Ransomware Behavior"&earliest=0&latest=&display.page

Save As Alert

Description	Optional
Permissions	Private / Shared in App
Alert type	Scheduled / Real-time
	Run every hour ▾
At 0 ▾	minutes past the hour
Expires	2400 day(s) ▾
Trigger Conditions	
Trigger alert when	Number of Results ▾
	is greater than ▾ 0
Trigger	Once / For each result
Throttle	□
Trigger Actions	
	+ Add Actions ▾
When triggered	Add to Triggered Alerts (Remove)
	Severity: High ▾

Cancel Save



kali:8000/en-US/app/search/search?q=| rest %2Fservices%2Fsaved%2Fsearches%20%0A| search is_scheduled%3D1 alert.track%3D1%0A| table title%2C alert_type%2C cron_schedule%

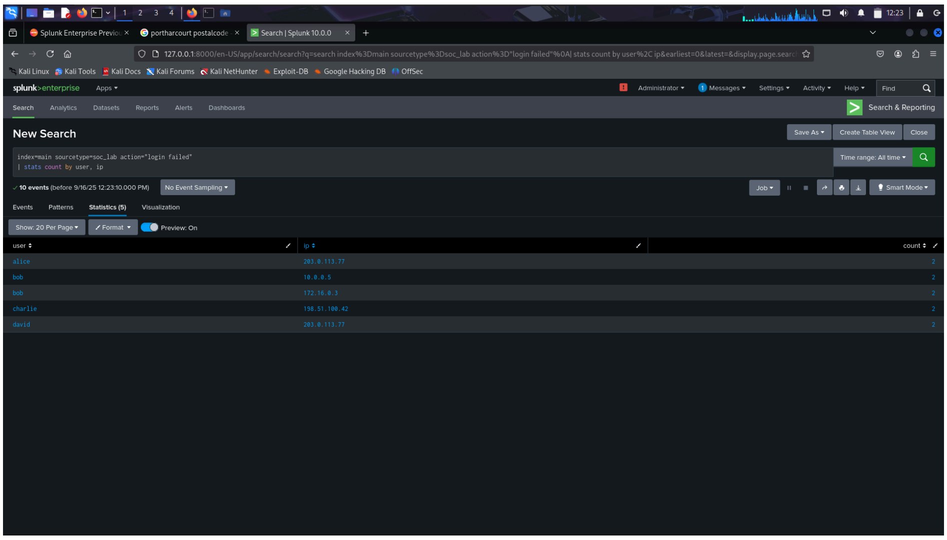
New Search

```
| rest /services/saved/searches
| search is_scheduled=1 alert.track=1
| table title, alert_type, cron_schedule, disabled
```

✓ 5 results (before 9/16/25 2:17:03.000 PM)

title	alert_type	cron_schedule	disabled
Brute-Force Login Attempt	number of events	0 * * * *	0
High Priority Malware	number of events	0 * * * *	0
Multi-IP Login	number of hosts	0 * * * *	0
Suspicious File Access After Malware	number of events	0 * * * *	0
Trojan/Worm/Rootkit Alert	number of events	0 * * * *	0

- **Appendix C:** More Images



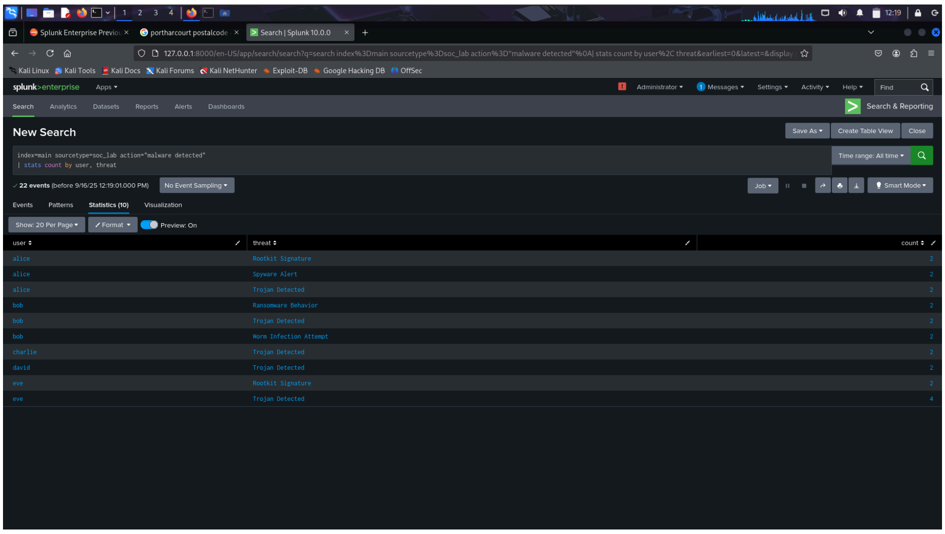
127.0.0.1:8000/en-US/app/search/search?q=search index%3Dmain sourcetype%3Dsoc_lab action%3D"login failed"%0A| stats count by user%2C ip&earliest=0&latest=&display.page.search

New Search

```
index=main sourcetype=soc_lab action="login failed"
| stats count by user, ip
```

✓ 10 events (before 9/16/25 12:23:10.000 PM)

user	ip	count
alice	203.0.113.77	2
bob	10.0.0.5	2
bob	172.16.0.3	2
charlie	198.51.100.42	2
david	203.0.113.77	2



New Search

```
index=main sourcetype=soc_lab action="malware detected"
| stats count by user, threat
```

✓ 22 events (before 9/16/25 12:19:01.000 PM)

user	threat	count
alice	Rootkit Signature	2
alice	Spyware Alert	2
alice	Trojan Detected	2
bob	Ransomware Behavior	2
bob	Trojan Detected	2
bob	Worm Infection Attempt	2
charlie	Trojan Detected	2
david	Trojan Detected	2
eve	Rootkit Signature	2
eve	Trojan Detected	4