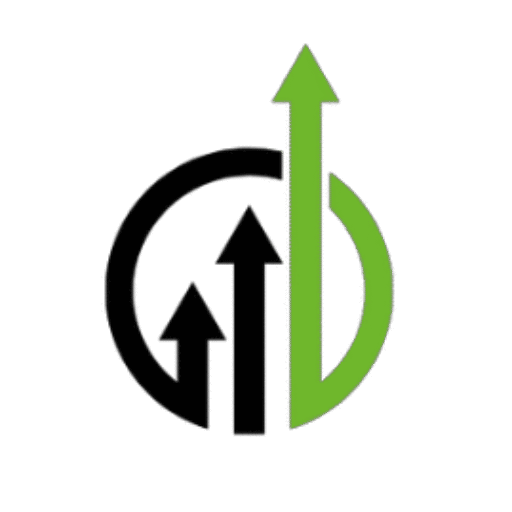
Security Alerts Monitoring and Incidence Reponse Report



**Program:** Future Interns Cyber Security Program

**Task 2:** Security Alert Monitoring & Incident Response

**Name:** Ilegbemi Damilola Olumide

**Date:** September 2025

**Tools Used:** Splunk Enterprise (Free Trial), SOC\_Task2 SampleLogs (Data Source)

## Introduction

As part of the Cybersecurity Internship Program at Future Interns, I undertook Task 2, which focused on Security Operations Center (SOC) monitoring and incident response. The objective of this task was to simulate real-world SOC analyst duties, including log ingestion, suspicious activity detection, incident classification, dashboard creation, alert configuration, and documentation of findings.

## Environment Setup

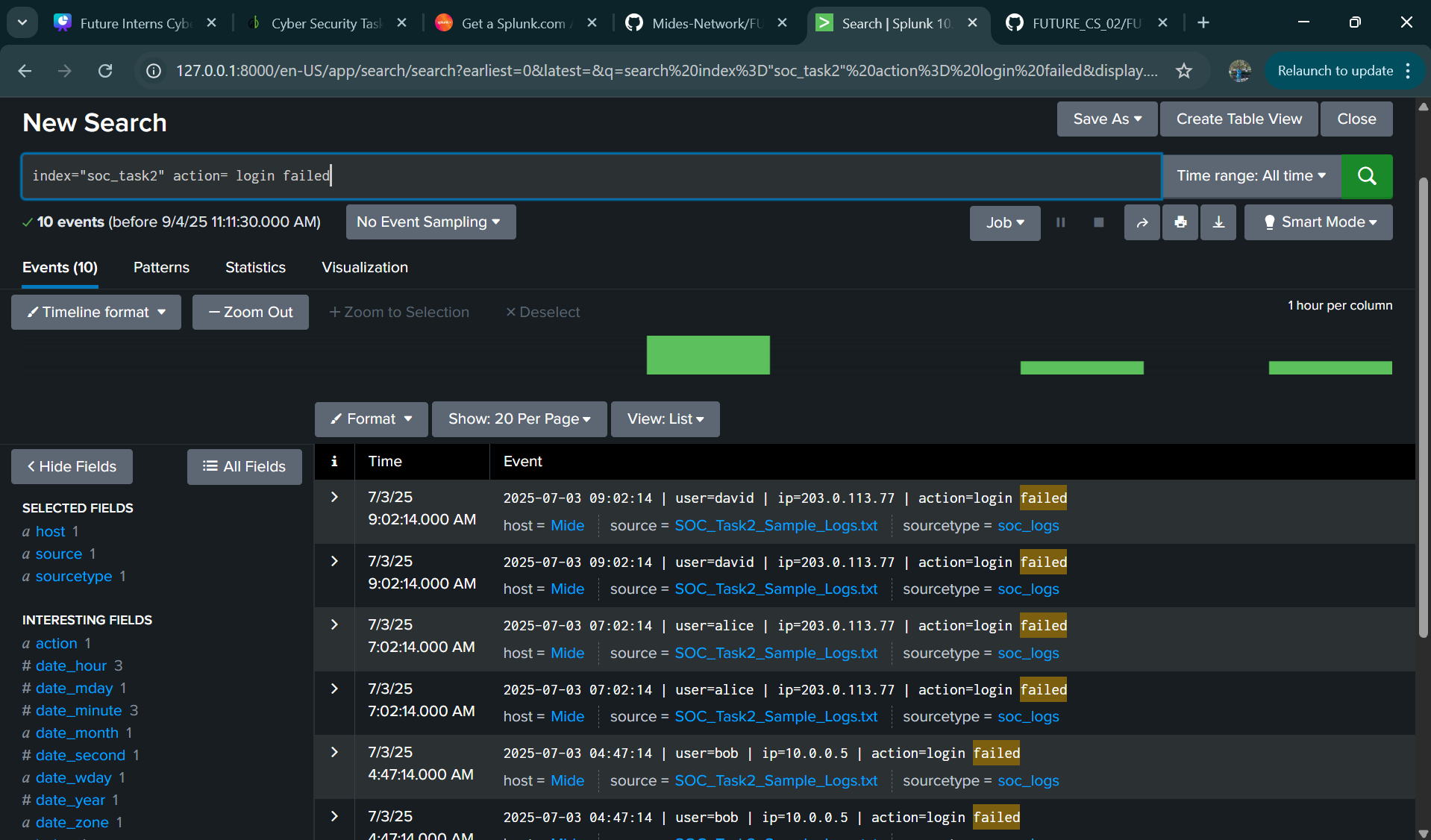
- Tool Used: Splunk Enterprise (Free Trial)  
- Dataset: SOC\_Task2\_Sample\_Logs.txt (Data source)  
- Index Created: soc\_task2  
- Sourcetype: soc\_logs  
The dataset contained simulated security events such as logins, file access logs, malware detection alerts, and IP addresses.

## Identified Alerts

### Multiple Login Attempts

Using Splunk, I identified repeated failed login attempts originating from external IP addresses, particularly **203.0.113.77**. This pattern suggests a brute-force attack targeting user accounts.

This activity was classified as a **High Priority Alert** due to the risk of unauthorized account compromise.

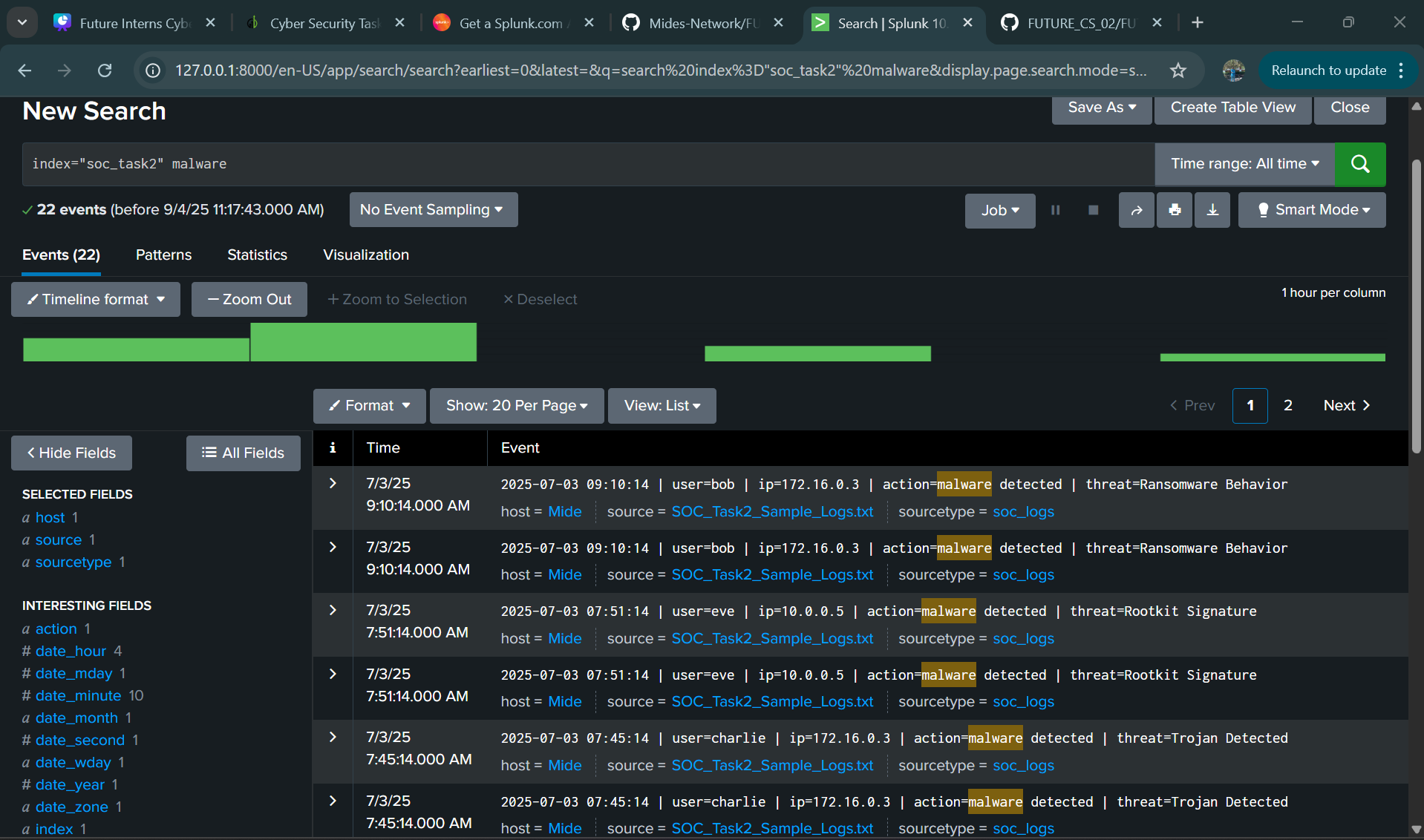


**Remediation Suggestions:**  
i. Implement account lockout policies after repeated failed attempts.  
ii. Enforce Multi-Factor Authentication (MFA) for all user accounts.

### 2. Malware Detection Alerts

Through SPL queries, I filtered suspicious events related to malware activity. Logs revealed detections of **Trojans, ransomware behavior, and rootkit signatures** across multiple IPs. These highlight potential compromise attempts within the environment.

This activity was classified as a **High Priority Alert** because of the severe risk associated with malware infections.

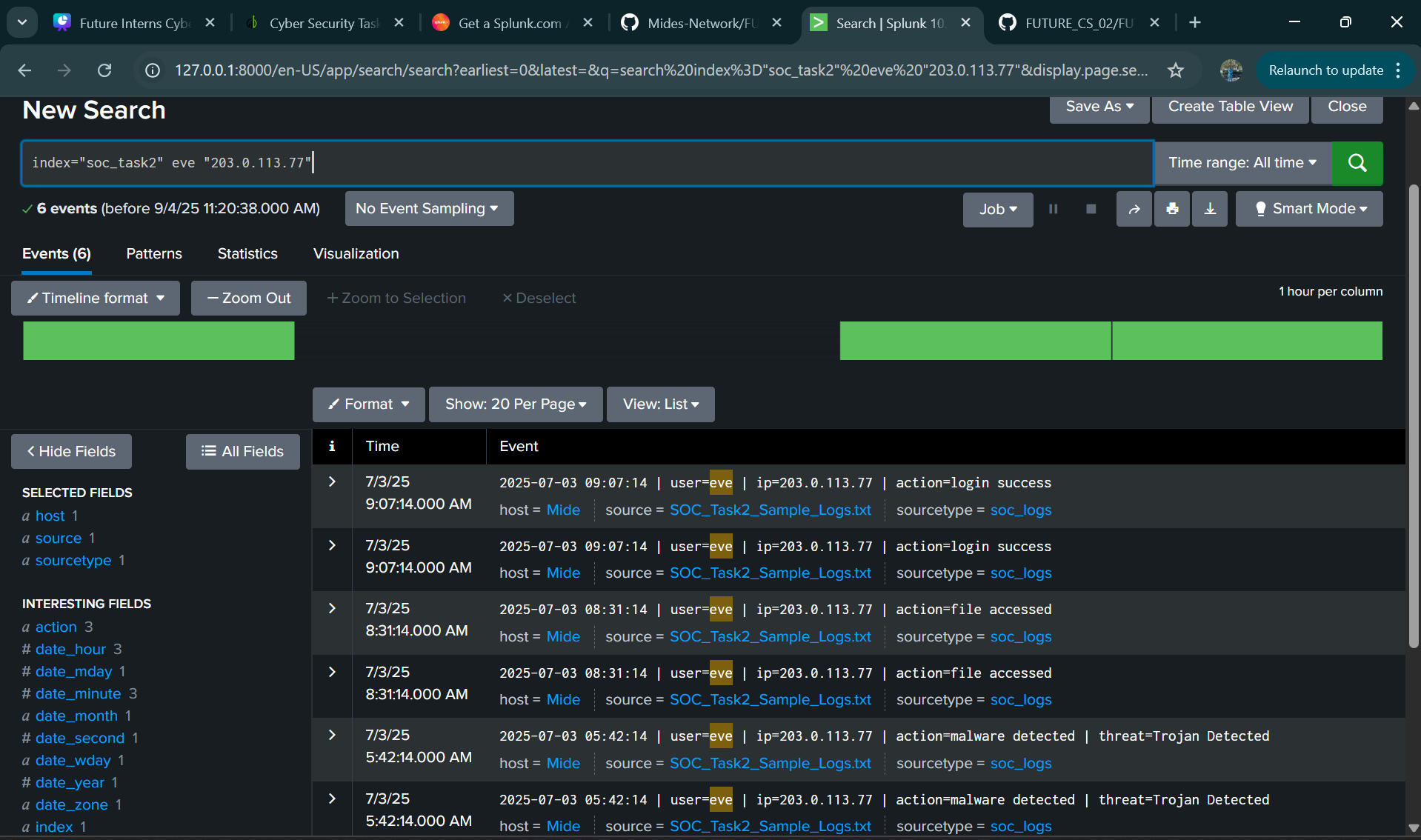


**Remediation Suggestions:**  
i. Immediately isolate affected hosts to prevent malware propagation.  
ii. Run updated malware scans and remove infections.

### Suspicious Host Activity (IP: 203.0.113.77)

Further investigation of events linked to **203.0.113.77** showed a sequence of suspicious actions: multiple failed logins, a successful login, file access, and subsequent malware detection.

This chain of events strongly suggests the host was compromised. The incident was escalated as a **High Priority Alert** because it combines both successful access and malware execution.

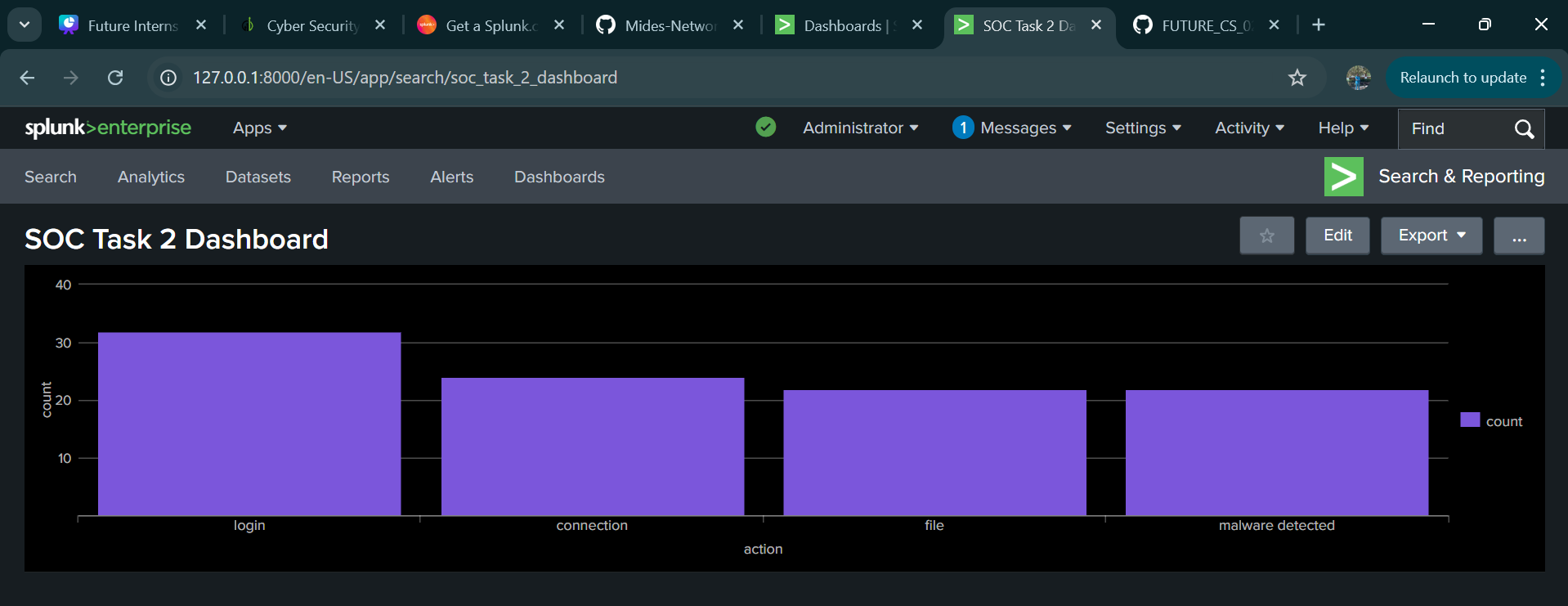


**Remediation Suggestions:**  
i. Quarantine or isolate the affected host from the network.  
ii. Conduct forensic analysis of login activity, accessed files, and possible data exfiltration.

## Dashboard Summary

A column chart dashboard was created in Splunk showing counts of suspicious activities such as failed logins, malware detections, and file access attempts.

This visualization provides insights into the frequency and distribution of alerts across users and IPs, supporting prioritization of incident response.



## Incident Classification Table

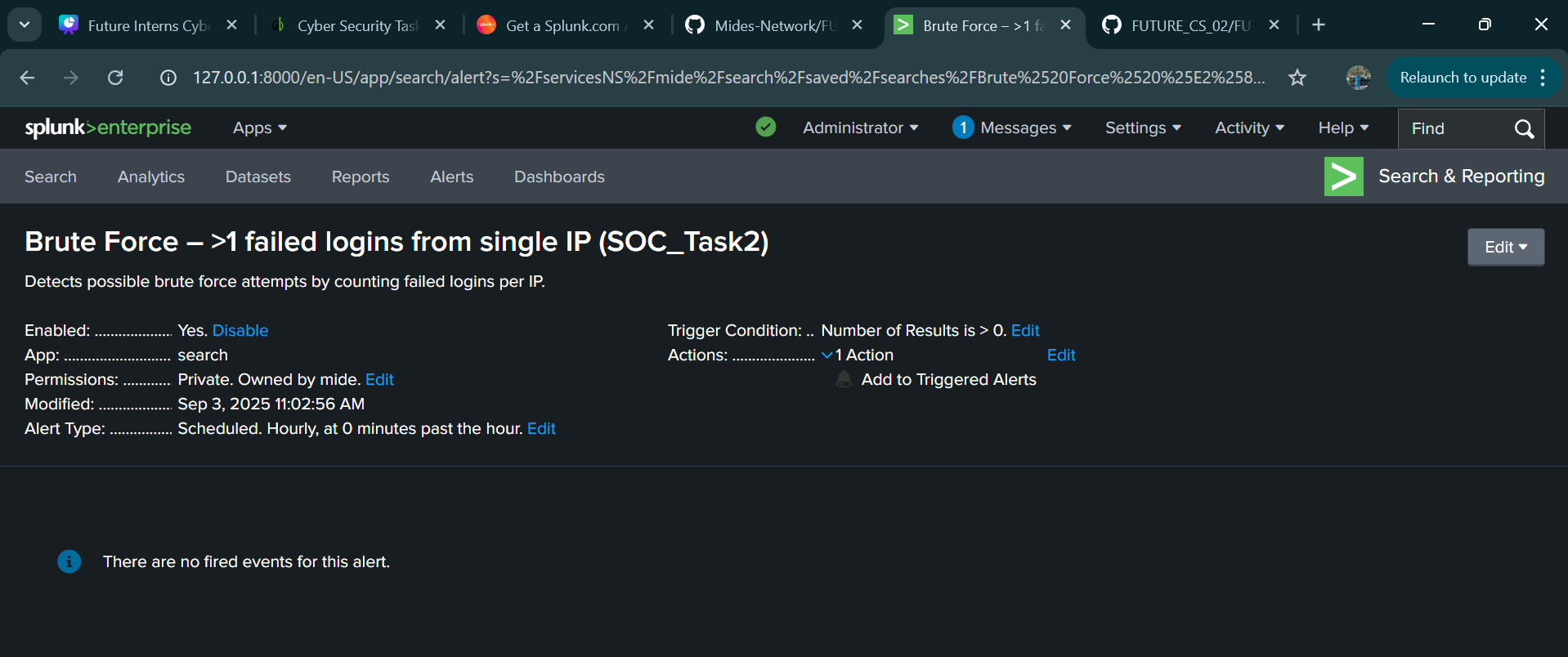
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Incident ID | Time (first seen) | IP | User(s) | Summary | Severity |
| INC-001 | 2025-07-03 04:53 | 203.0.113.77 | alice, bob | Multiple failed logins (brute force) | High |
| INC-002 | 2025-07-03 05:45 | 203.0.113.77 | david, eve | Malware detections (Trojan, Rootkit) | High |
| INC-003 | 2025-07-03 06:10 | 198.51.100.2 | charlie | File accessed from external IP | Medium |
| INC-004 | 2025-07-03 06:15 | 192.168.1.5 | internal\_user | Normal login success | Low |

## Incident Narrative

On July 3, 2025, Splunk analysis revealed brute force attempts from IP 203.0.113.77, which later triggered malware detections. Another IP (198.51.100.2) accessed files externally, classified as Medium severity. These findings demonstrate real-world attack patterns where adversaries attempt to gain access via brute force, then deploy malware once access is achieved. Immediate response actions include blocking malicious IPs, isolating hosts, resetting credentials, and conducting forensic investigation.

## Additional Evidence

Automated Alerting : To simulate SOC automation, I configured a Splunk alert for brute force attempts.



## Optional Email to Management

**Subject:** Summary of Security Alert Monitoring & Response

Dear Security Lead,

During the SOC simulation exercise in Splunk, I identified several critical alerts:

* Multiple failed login attempts from external IPs (possible brute-force attempts)
* Malware detections, including trojans, rootkits, and ransomware activity
* Suspicious host activity (IP 203.0.113.77) showing successful login, file access, and malware detection

These incidents were classified as High-Priority Alerts. Immediate recommendations include account lockout/MFA enforcement, isolating compromised hosts, running malware scans, and escalating incidents for forensic review.

Please advise if additional actions or escalation are required.

Best regards,  
**Ilegbemi Damilola Olumide**

## Skills Gained

- Practical use of Splunk for SOC analysis  
- Log analysis (failed logins, malware, external access)  
- Dashboard creation and visualization  
- Automated alert configuration  
- Professional incident reporting and classification