



## **Security Alert Monitoring & Incident Response Report**

**Name:** Olakunle Olasubomi Priscilla

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

**Program:** Future Interns Cybersecurity Internship

**Tools Used:**

- ❖ Splunk Enterprise (Free Trial)
- ❖ SOC\_Task2 SampleLogs (Data Source)

**Date:** August 2025

## Task Summary

This task focused on using Splunk as a Security Information and Event Management (SIEM) tool to monitor and analyze simulated security events. Key steps included:

- Configuring Splunk to process security logs.
- Generating dashboards to visualize detected alerts.
- Triggering automated alert actions for suspicious events.
- Preparing a communication email template for management reporting.

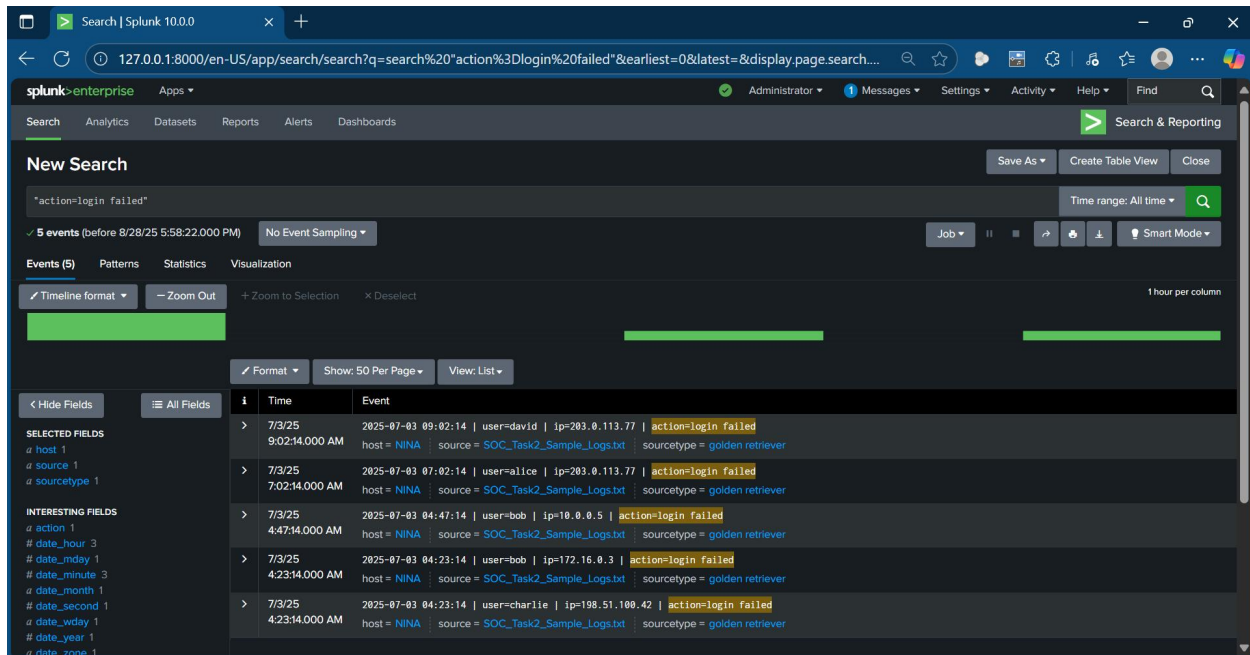
Through this process, I practiced fundamental SOC analyst responsibilities such as log monitoring, threat detection, incident classification, and structured escalation.

## Identified Alerts

### 1. Multiple Login Attempts (High Priority).

#### ❖ Observation:

Splunk logs revealed several failed login attempts originating from multiple external IP addresses. The repeated nature of these attempts suggests a potential brute-force attack targeting user accounts.



The screenshot displays the Splunk Enterprise web interface. At the top, the search bar contains the query "action=login failed". Below the search bar, the results are shown in a table format. The table has columns for Time, Event, and various fields like host, user, ip, and source. The events listed are:

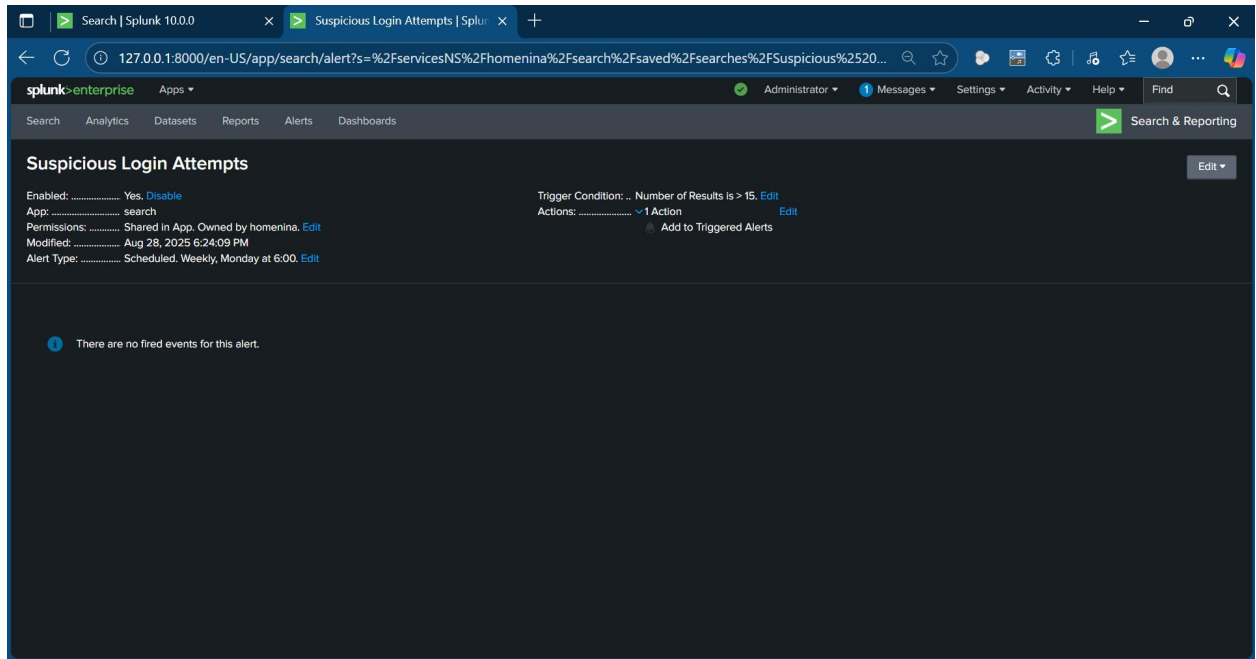
Time	Event
7/3/25 9:02:14.000 AM	2025-07-03 09:02:14   user=david   ip=203.0.113.77   action=login failed   host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever
7/3/25 7:02:14.000 AM	2025-07-03 07:02:14   user=alice   ip=203.0.113.77   action=login failed   host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever
7/3/25 4:47:14.000 AM	2025-07-03 04:47:14   user=bob   ip=10.0.0.5   action=login failed   host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever
7/3/25 4:23:14.000 AM	2025-07-03 04:23:14   user=bob   ip=172.16.0.3   action=login failed   host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever
7/3/25 4:23:14.000 AM	2025-07-03 04:23:14   user=charlie   ip=198.51.100.42   action=login failed   host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever

#### ❖ Impact:

If successful, this could lead to account compromise and unauthorized access to sensitive data.

### ❖ Response & Remediation:

- Classified it as High Priority due to potential account takeover.
- Triggered Splunk alert actions to notify security personnel.



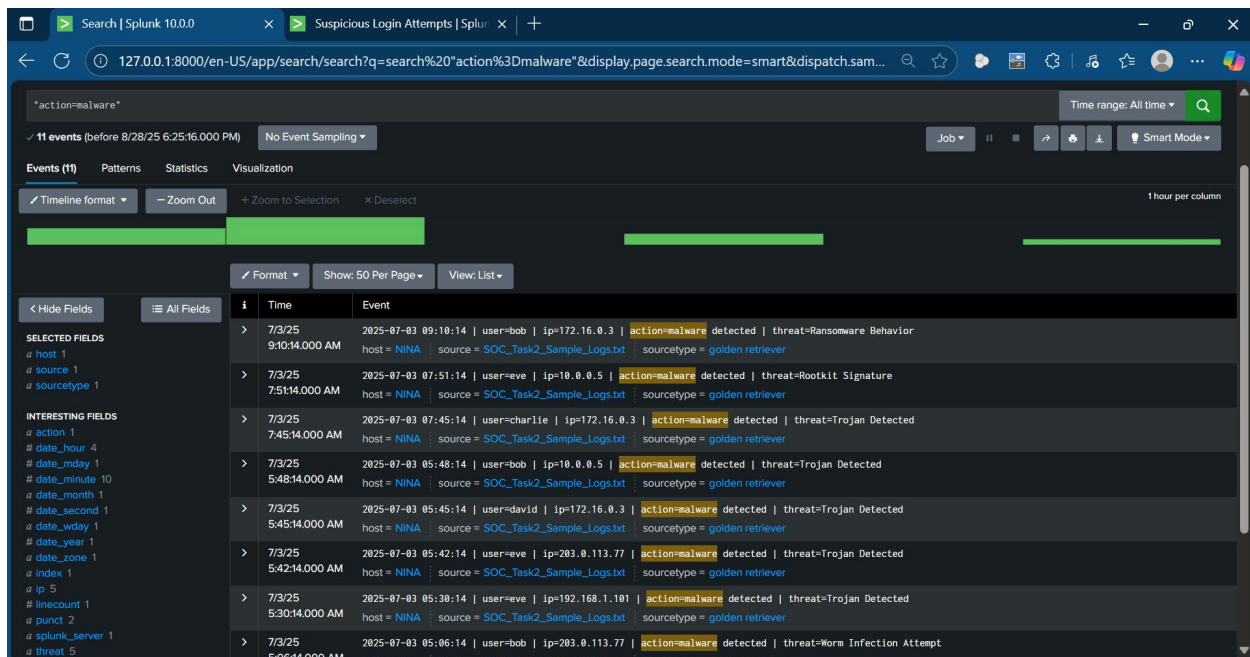
### ❖ Recommended Actions:

- Implement account lockout policies after repeated failures.
- Enforce Multi-Factor Authentication (MFA).

## 2. Malware Detection Alerts (High Priority)

### ❖ Observation:

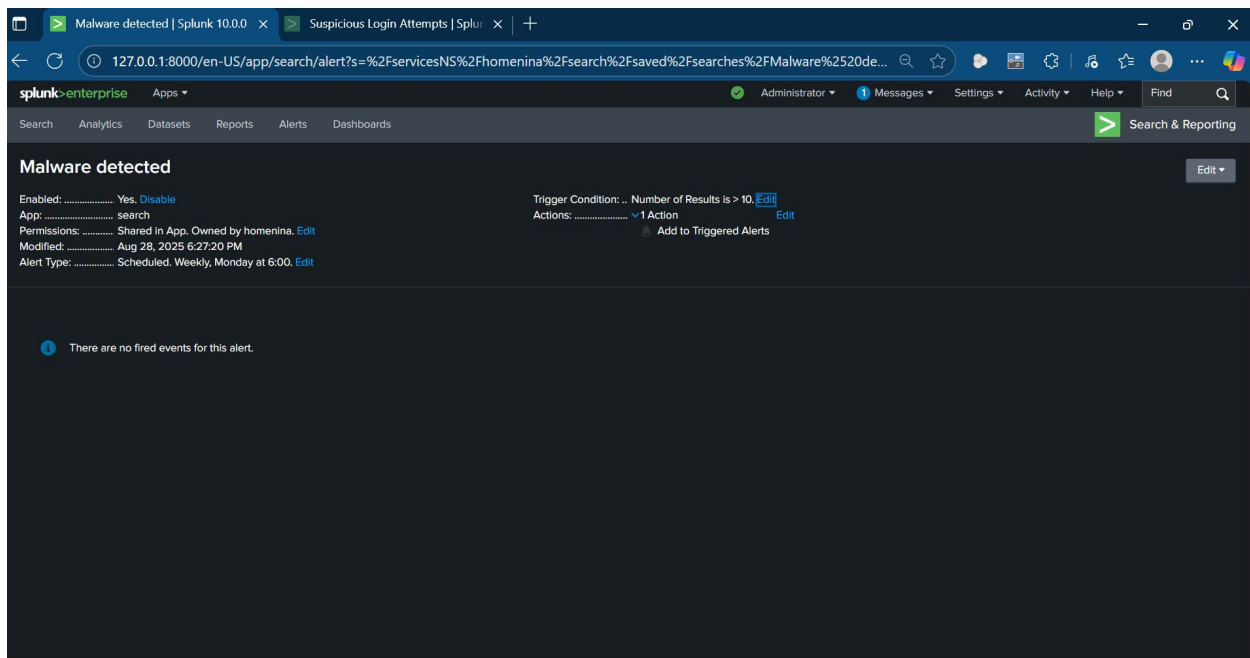
Using Splunk SPL queries, multiple malware-related alerts were identified. These included signs of ransomware, rootkits, Trojans, worms, and spyware. The events originated from different IP addresses, indicating widespread attempts at compromise.



- **Impact:**  
These malware activities pose a severe risk of data theft, system compromise, and operational disruption.

## ❖ Response & Remediation:

- Classified as High Priority due to potential large-scale infection.
- Configured Splunk to trigger immediate security team notifications.



### ❖ Recommended Actions:

- Isolate affected hosts.
- Conduct full malware scans with updated signatures.

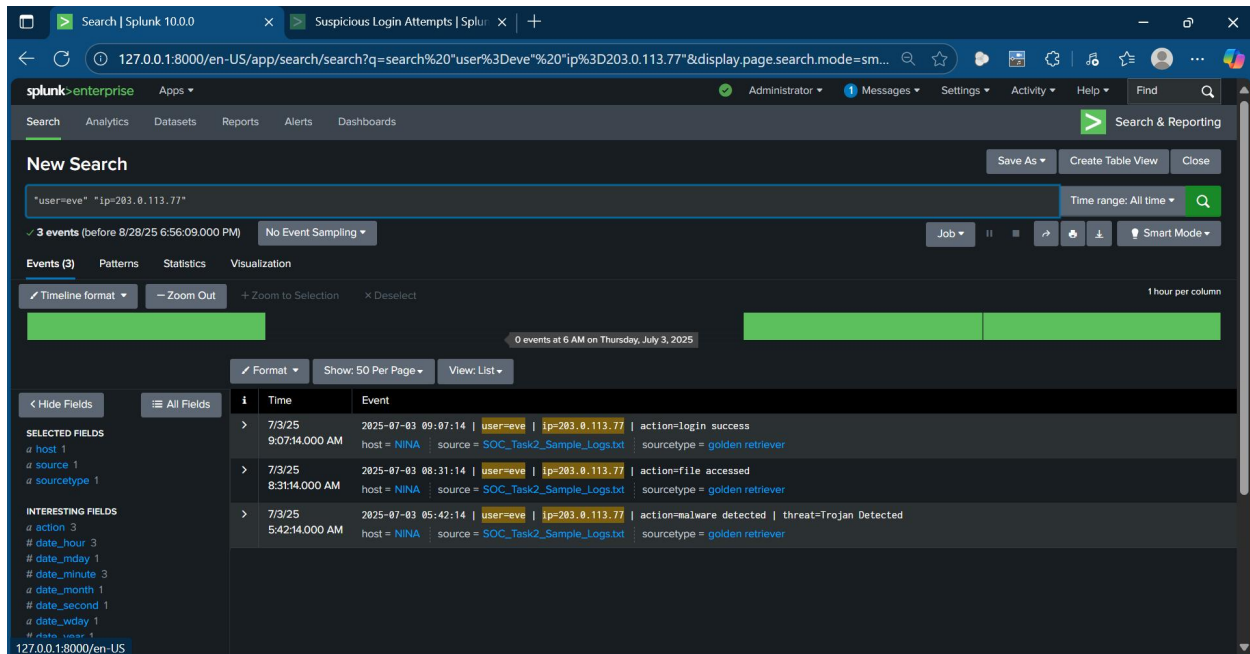
## 3. Suspicious Host Activity – Potential Compromise (High Priority)

### ❖ Observation:

Logs for host 203.0.113.77 revealed a concerning sequence of events:

- Successful login recorded.
- File access immediately followed.
- Malware detection (Trojan) later triggered.

This progression strongly indicates that the host was compromised after login.

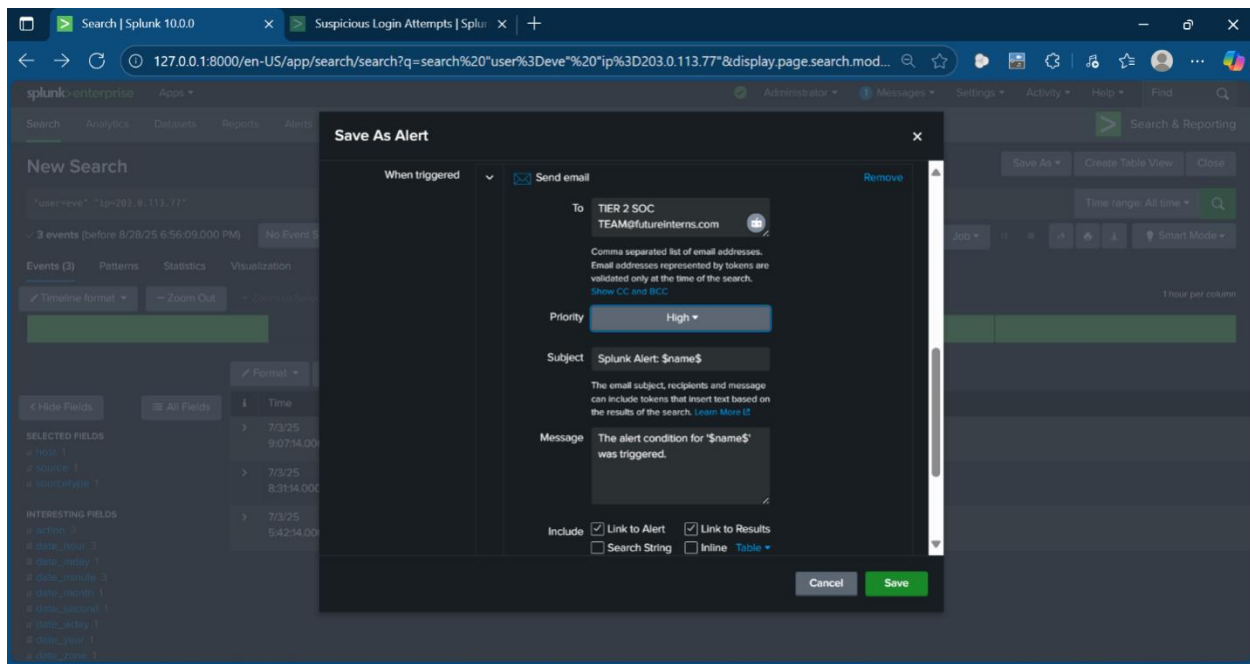


### ❖ Impact:

Such activity shows both unauthorized access and malware execution, increasing the likelihood of data exfiltration and spread to other systems.

### ❖ Response & Remediation:

- Classified as High Priority.
- Configured Splunk email alert to escalate directly to Tier 2 SOC analysts.



#### ❖ Recommended Actions:

- Quarantine the affected host.
- Conduct forensic analysis of login activity and accessed files.

#### 4. Unauthorized Internal Connection Attempt (Medium Priority)

##### ❖ Observation:

Additional log review revealed a suspicious internal connection attempt from user *charlie* to IP 10.0.0.5, an internal/private network host. This attempt was logged shortly after repeated failed external logins and malware detection alerts, suggesting possible lateral movement attempts.

Time	Event
7/3/25 8:42:14.000 AM	2025-07-03 08:42:14   user=charlie   ip=203.0.113.77   action=file accessed host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever
7/3/25 8:20:14.000 AM	2025-07-03 08:20:14   user=charlie   ip=192.168.1.101   action=connection attempt host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever
7/3/25 7:45:14.000 AM	2025-07-03 07:45:14   user=charlie   ip=172.16.0.3   action=malware detected   threat=Trojan Detected host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever
7/3/25 7:38:14.000 AM	2025-07-03 07:38:14   user=charlie   ip=172.16.0.3   action=connection attempt host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever
7/3/25 7:22:14.000 AM	2025-07-03 07:22:14   user=charlie   ip=192.168.1.101   action=connection attempt host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever
7/3/25 6:13:14.000 AM	2025-07-03 06:13:14   user=charlie   ip=10.0.0.5   action=connection attempt host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever
7/3/25 5:49:14.000 AM	2025-07-03 05:49:14   user=charlie   ip=192.168.1.101   action=connection attempt host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever
7/3/25 5:18:14.000 AM	2025-07-03 05:18:14   user=charlie   ip=172.16.0.3   action=login success host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever
7/3/25 4:23:14.000 AM	2025-07-03 04:23:14   user=charlie   ip=198.51.100.42   action=login failed host = NINA   source = SOC_Task2_Sample_Logs.txt   sourcetype = golden retriever

### ❖ Impact:

This raises concern that the attacker may have already obtained some level of access and was probing the internal environment to expand control.

### ❖ Response & Remediation:

Classified as High Priority because it shows signs that an attacker may already be inside the system and trying to spread to other parts of the network.

**Save As Alert**

When triggered: ☒ Send email

To: TIER 2 SOC  
TEAM@futureinterns.com

Priority: High

Subject: Splunk Alert: \$name\$

Message: The alert condition for '\$name\$' was triggered.

Include: ☒ Link to Alert ☒ Link to Results  
☐ Search String ☐ Inline ☐ Table

Cancel Save

❖ **Recommended actions:**

- Review network segmentation to prevent unauthorized east-west traffic.
- Audit internal access logs for other unusual connection attempts.
- Monitor user *charlie* for abnormal activities across other systems.

**Timeline of Events**

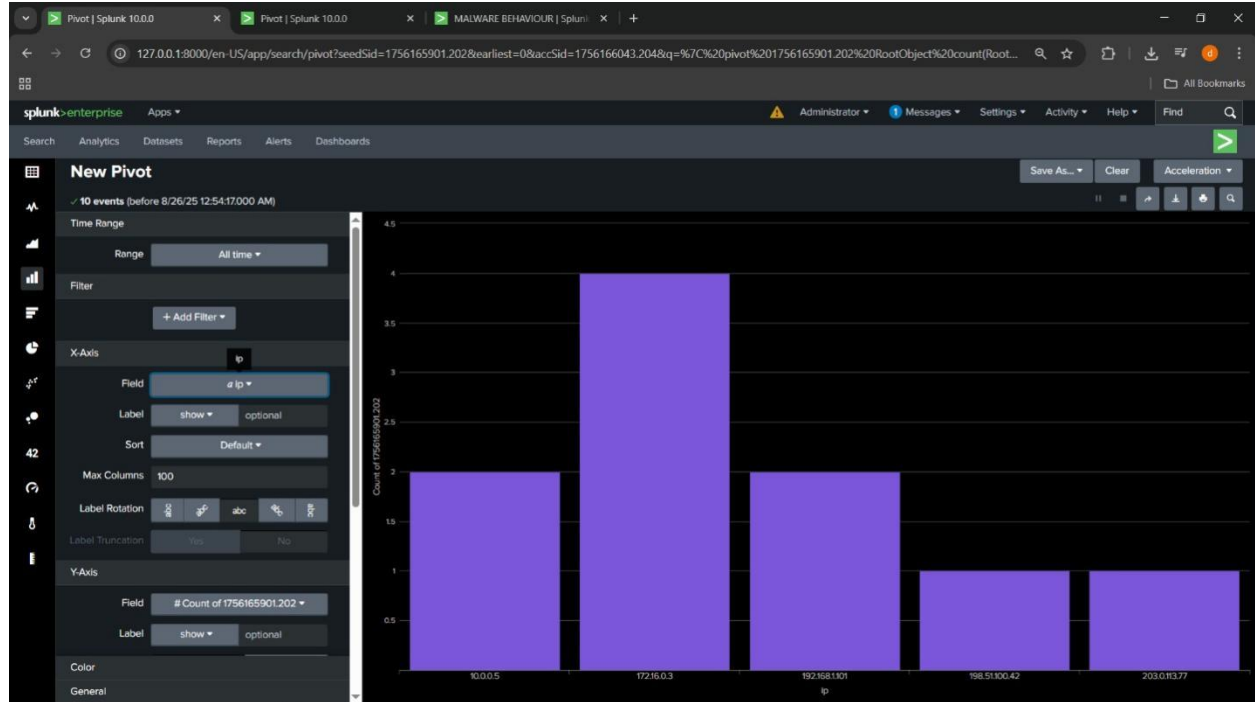
- **04:23 AM** – Failed login attempt from IP 198.51.100.42.
- **05:18 AM** – Successful login from IP 172.16.0.3.
- **05:49 AM – 07:22 AM** – Multiple suspicious connection attempts (192.168.1.101, 10.0.0.5, 172.16.0.3).
- **07:45 AM** – Malware alert: Trojan detected on IP 172.16.0.3.
- **08:20 AM** – Connection attempt from 192.168.1.101.
- **08:42 AM** – File accessed from compromised host 203.0.113.77.

**Alert Classification Log**

Alert	Severity	Source IP / Host	Recommended Action
Multiple Failed Login Attempts	High	198.51.100.42, others	Enforce MFA, lockout policy
Malware Detection (Trojan)	High	172.16.0.3	Isolate host, run malware scans
Suspicious Host Activity (203.0.113.77)	High	203.0.113.77	Quarantine host, forensic investigation
Unauthorized Internal Connection Attempt	High	10.0.0.5 (Target), user=charlie	Review segmentation, audit access logs



## Dashboard Summary



Using an SPL query in Splunk, I created a column chart dashboard that visualizes malware activity across multiple hosts. This chart highlights the frequency and distribution of malicious events, making it easier to see which systems are most affected and to prioritize incident response.

## **Optional Management Email Template**

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

Dear Security Lead,

During security log analysis using Splunk, I identified the following critical alerts:

- Multiple failed login attempts from external IPs (possible brute-force attack).
- Malware detections including ransomware, spyware, and Trojans.
- Suspicious host activity on **203.0.113.77** involving login, file access, and malware detection.
- Unauthorized internal connection attempt to IP **10.0.0.5** suggesting possible lateral movement.

Each incident was classified according to severity, with high-priority alerts escalated to the Tier 2 SOC team. Recommended actions include host isolation, enhanced authentication controls, malware scans, and forensic analysis.

Please advise on whether further escalation or reporting is required.

Best regards,  
Olakunle Olasubomi.

## **Conclusion**

This project showed how Splunk can detect and classify security incidents such as brute-force attempts, malware activity, host compromise, and lateral movement. By analyzing logs and documenting responses, I gained practical SOC skills in monitoring, incident classification, and reporting. Overall, the exercise highlighted the importance of SIEM tools in improving security visibility and response.