Security Alert Monitoring & Incident Response Report

Name: Oyekale Olamide David

Task 2: Security Alert Monitoring & Incident Response Report

Program: Future Interns Cybersecurity Internship

Date: August 2025

Tools Used:

- Splunk Enterprise (Free Trial)
- SOC_Task2SampleLogs (Data Source)

Task Summary

The project involved simulating the responsibilities of a Security Operations Center (SOC) analyst through the use of Splunk. Log data was ingested and examined to uncover anomalous activities, assess and categorize threats according to severity, and replicate incident response procedures. This exercise served to strengthen practical skills and technical readiness for foundational SOC analyst positions.

Methodology

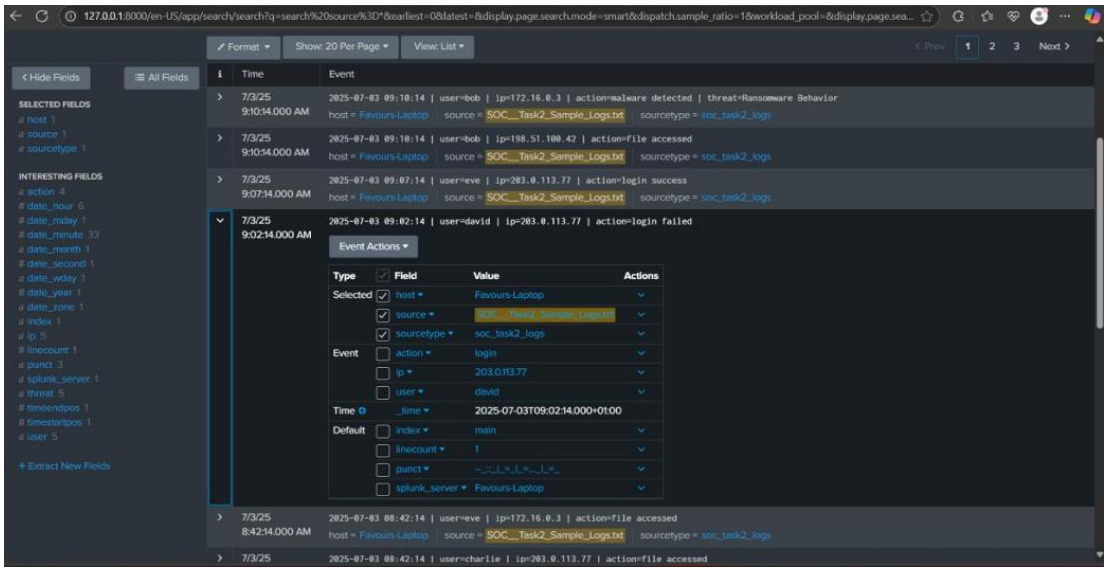
- Uploaded and indexed log data into Splunk.
- Executed Splunk queries to detect anomalies and suspicious activities.
- Conducted detailed investigations on individual alerts.
- Classified threats by severity (Low, Medium, High).
- Simulated incident response actions for medium- and high-severity alerts.

This process provided practical experience in core SOC analyst functions, including log monitoring, threat detection, incident classification, and structured escalation.

Alerts identified

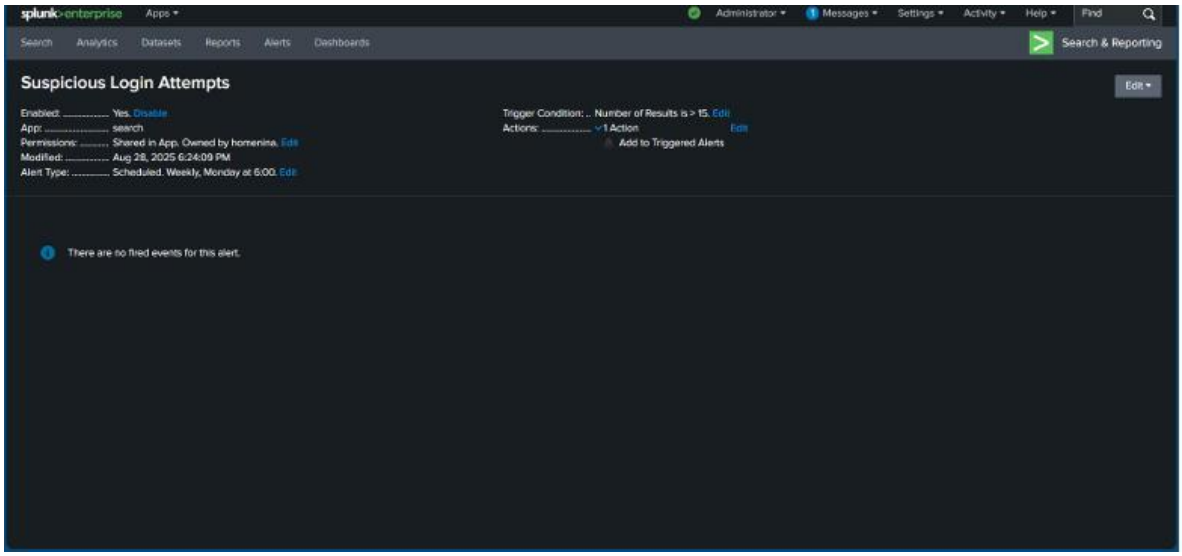
1. Multiple Failed Login Attempts (Medium severity)

I identified a high volume of failed login attempts originating from a single IP address within a short period. This activity is indicative of a potential brute-force attack aimed at compromising user credentials.



Impact: If successful, this attack could result in unauthorized access to user accounts, potential privilege escalation, and further compromise of sensitive resources.

Remediation and Response (Simulated): An **internal alert** was raised, and the source IP was placed under **continued monitoring** for potential escalation.

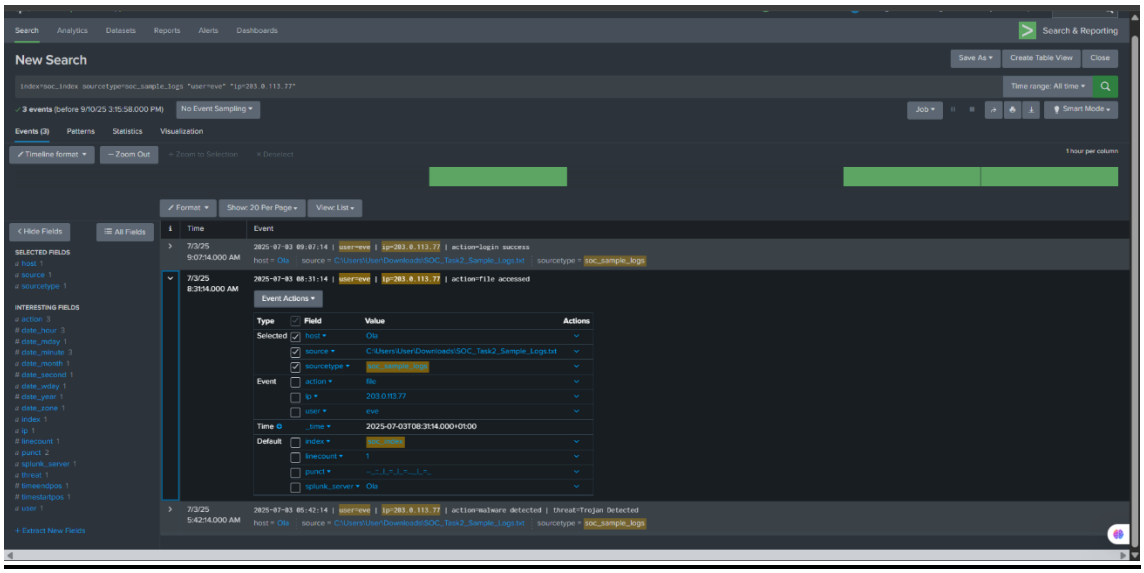


Recommended Response Actions:

- Block or blacklist the source IP address.
- Monitor for additional failed login attempts across the network.
- Review authentication logs for targeted accounts.
- Enforce account lockout policies after a defined number of failed attempts.
- Escalate if privileged accounts or multiple accounts are being targeted.

2. Suspicious Host Activity– Potential Compromise (High severity)

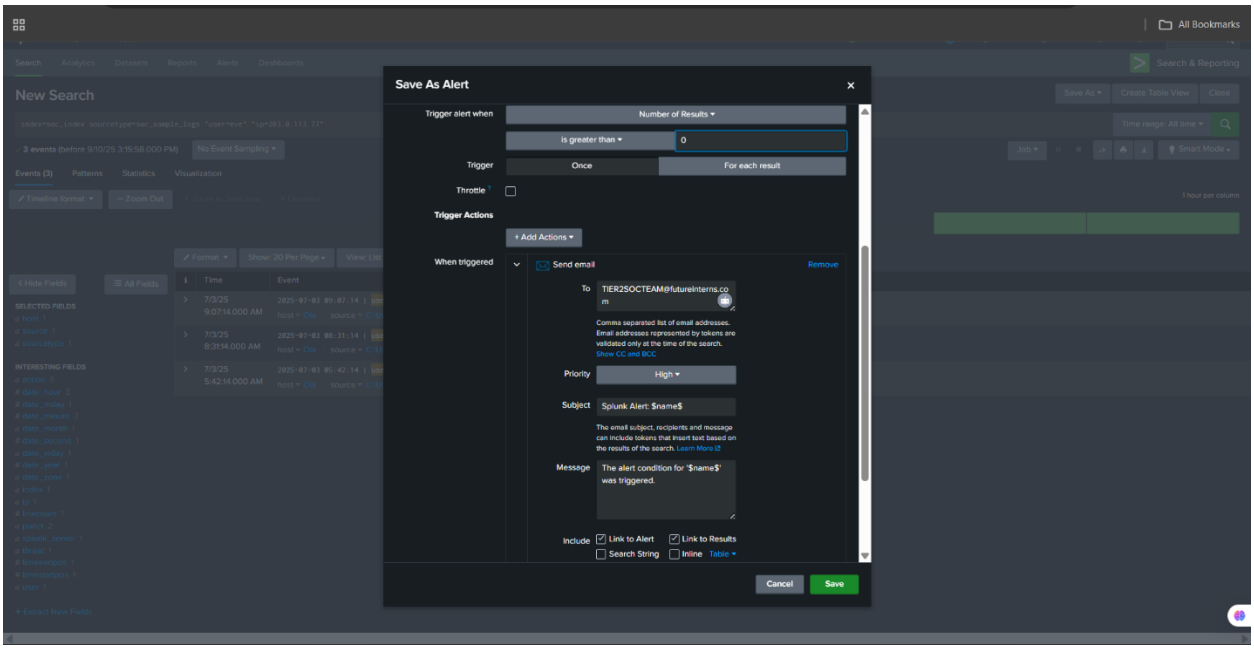
A high-severity security incident was identified on host **203.0.113.77**. Logs showed a successful login followed by immediate file access, and later a malware detection alert for a Trojan. This sequence strongly indicates that the host was compromised.



Impact: The compromise could allow unauthorized access to sensitive files, malware installation, and potential spread to other systems.

Remediation and Response (simulated):

- Classified the incident as **High Priority**.
- Configured a **Splunk email alert** to automatically escalate the case to Tier 2 SOC analysts.

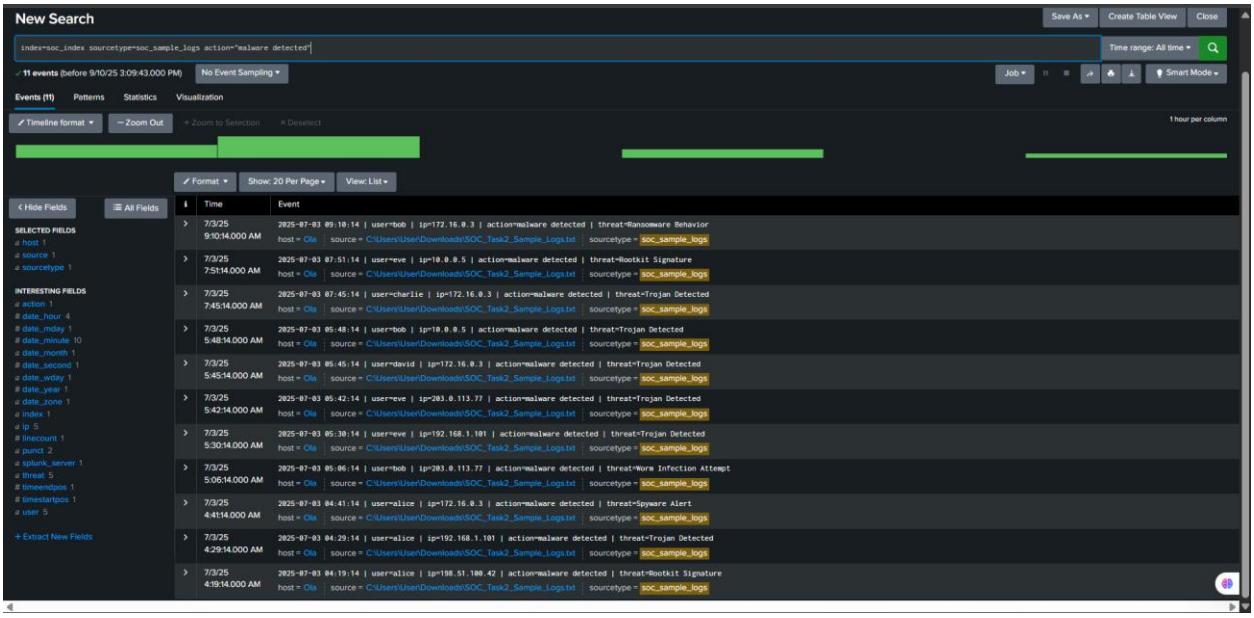


Recommended Response Actions:

- Isolate the affected host.
- Reset associated credentials.
- Conduct forensic and malware analysis.
- Monitor for further suspicious activity across the network.

3. Malware Detection Alerts (High severity)

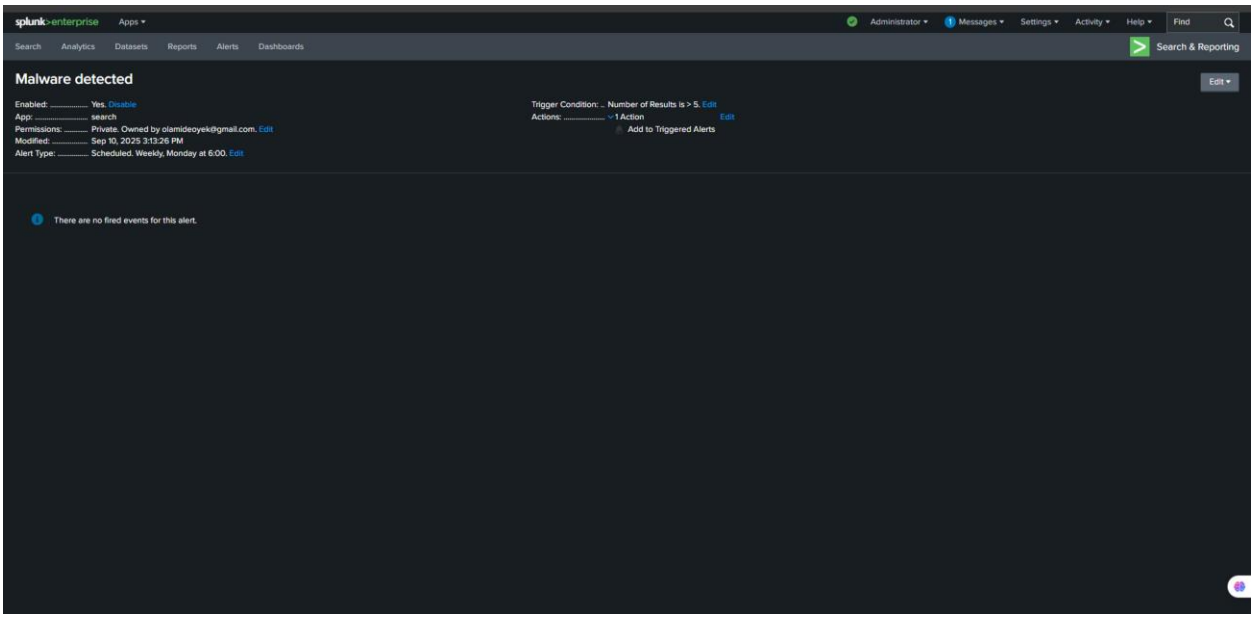
The use of Splunk SPL queries revealed numerous malware-related alerts, including indicators of ransomware, rootkits, Trojans, worms, and spyware. The activity originated from multiple IP addresses, suggesting broad and coordinated compromise attempts.



Impact:
If successful, these attacks could result in large-scale compromise, including data encryption and loss (ransomware), privilege escalation (rootkits, Trojans), unauthorized data exfiltration (spyware), and lateral spread across the network (worms).

Remediation and Response (simulated):

- Classified as a High-Priority incident due to the risk of large-scale infection.
- Configured Splunk to automatically trigger immediate notifications to the security team.

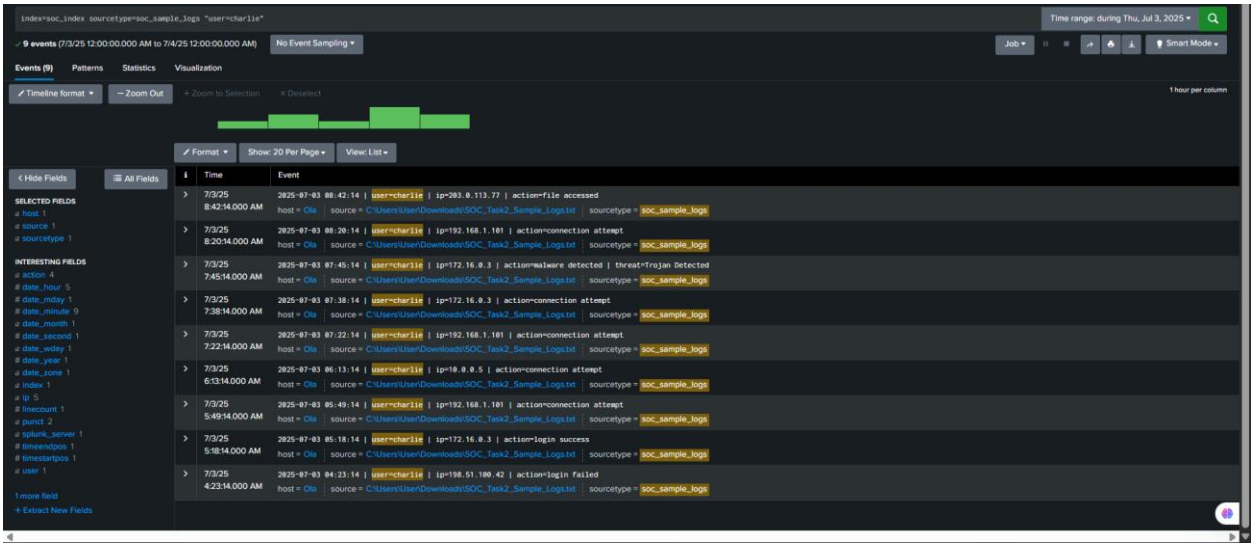


Recommended Response Actions:

- Immediately block and blacklist identified malicious IP addresses.
- Conduct malware scans across affected hosts to identify infections.
- Isolate and remediate compromised endpoints.
- Apply security patches and ensure updated anti-malware defenses.
- Increase monitoring of inbound and outbound traffic for related activity.

4. Suspicious Internal Connection Attempt – Possible Lateral Movement (High severity)

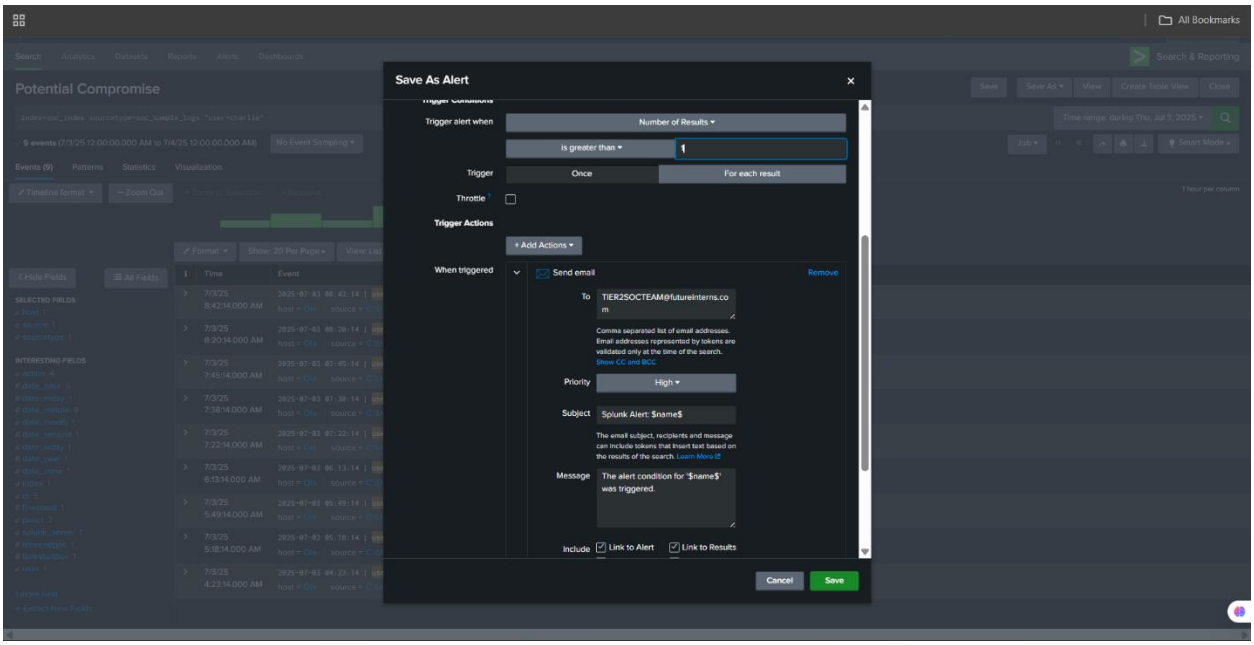
Additional log review revealed a suspicious internal connection attempt initiated by user **Charlie** to host **10.0.0.5** (internal/private network). This activity occurred shortly after repeated failed external login attempts and multiple malware detection alerts, suggesting a potential attempt at lateral movement within the environment.



Impact:
If confirmed, this activity may indicate that an attacker has gained access to internal credentials and is attempting to move laterally to expand their foothold within the network. This could lead to further system compromise and broader organizational impact.

Remediation and Response (simulated):

Classified as High Priority due to indications that an attacker may already have gained access to the system and is attempting lateral movement across the network.



Recommended Response Actions:

- Temporarily disable and investigate user account **Charlie**.
- Isolate host **10.0.0.5** for forensic analysis.
- Review authentication logs for signs of credential theft.
- Correlate activity with existing malware alerts to confirm scope of compromise.
- Escalate findings to Tier 2/Incident Response team for containment.

Timeline of Events

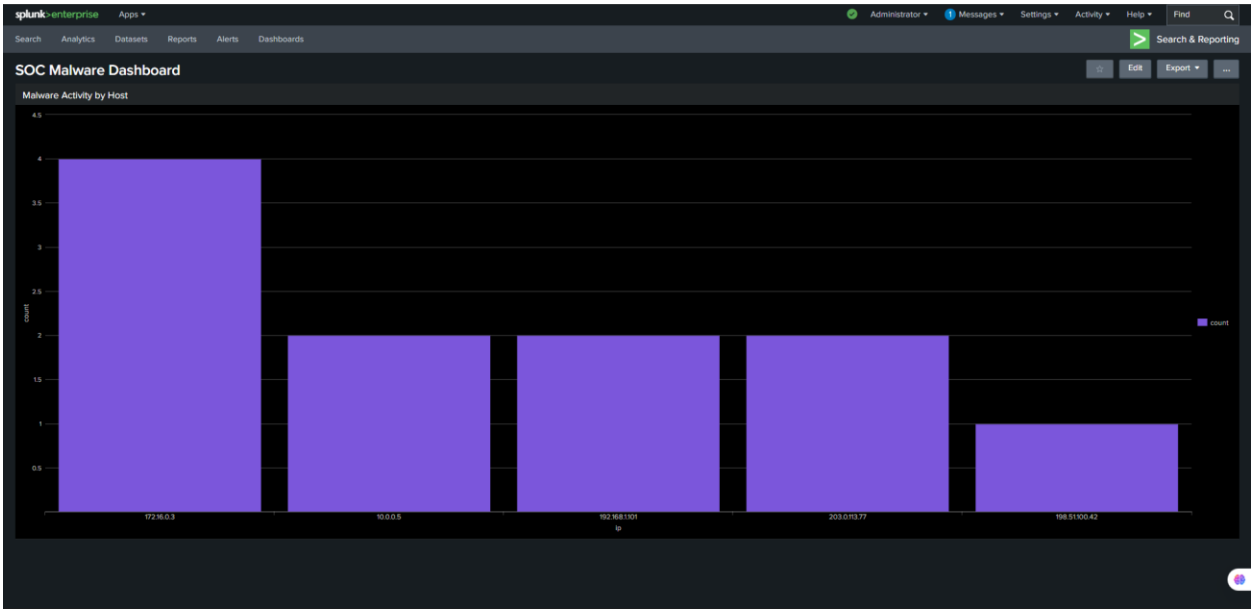
- **04:23 AM** – Failed login attempt from IP **"`198.51.100.42`."**
- **05:18 AM** – Successful login from IP **"`172.16.0.3`."**
- **05:49 AM – 07:22 AM** – Multiple suspicious connection attempts from IPs **"`192.168.1.101`", "`10.0.0.5`",** and "**`172.16.0.3`".**
- **07:45 AM** – Malware alert: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

Alert Classification Log

Alert	Severity	Source / Host Involved	Mitigation Steps
Multiple Failed Login Attempts	Medium	198.51.100.42, others	Apply MFA, enforce account lockout rules
Suspicious Host Activity (203.0.113.77)	High	203.0.113.77	Quarantine device, conduct forensic investigation

Malware Detection (Trojan)	High	172.16.0.3	Isolate affected system, perform malware analysis
Unauthorized Internal Connection Attempt	High	10.0.0.5 (Target), user=charlie	Validate network segmentation, review access logs

Dashboard Summary



In Splunk, I built a column chart dashboard with an SPL query to display malware activity across different hosts. The visualization shows how often malicious events occur and where they are concentrated, enabling quicker identification of the most impacted systems and more effective prioritization of response actions.

Conclusion

This project provided hands-on experience with Splunk in identifying and managing security incidents such as brute-force logins, malware infections, compromised hosts, and lateral movement. Working with log data and recording response actions allowed me to build practical SOC skills in threat detection, analysis, and reporting. The exercise ultimately underscored how SIEM solutions improve visibility across systems and support faster, more effective incident response.

(Optional) Communication Email Template

Subject: Executive Summary – High-Severity Security Incidents

Dear Security Lead,

During recent monitoring using Splunk, several **high-severity security incidents** were detected that pose potential risks to the organization's systems and data.

Summary of Key Findings:

- Multiple failed login attempts suggesting possible credential attacks.
- Indicators of compromise on one internal host.
- Malware activity detected on another host.
- An unauthorized internal connection attempt pointing to possible lateral movement.

Business Impact:
If left uncontained, these activities could result in unauthorized access to sensitive accounts, system compromise, malware spread, and disruption of business operations.

Mitigation Actions Taken:

- Immediate containment measures (isolation of affected hosts, account protections).
- Ongoing forensic investigations to determine scope and prevent recurrence.
- Strengthened monitoring to detect further suspicious activity.

A detailed incident report and recommendations will follow once the investigations are complete.

Kindly advise if further escalation or formal reporting is necessary.

Best regards,
Oyekale Olamide
SOC Analyst
Future Interns.