CYBERSECURUTY INTERNSHIP – TASK 2

FUTURE INTERNS

INCIDENT RESPONSE REPORT

Title: Security Alert Monitoring & Incident Response using Splunk

Intern Name: Anush N

Date: 15/07/2025

About the Task

As part of my cybersecurity internship with **Future Interns,** this task focused on stimulating real-world **Security Operations Center (soc)** operations. The aim was to monitor simulated security alerts using a **SIEM (Security Information and Event Management)** tool and respond to potential incidents like malware attacks, brute-force logins, and credential stuffing.

This task helped me to understand how SOC analysts operate detecting threats early, classifying them, and initiating appropriate incident response strategies.

Objective

The primary objectives of this task were to:

- Set up and explore a free SIEM tool (Splunk Cloud Trial)
- Ingest and analyze simulated system logs
- Identify suspicious activities (failed logins, unusual downloads, brute force attacks,
- malware detection)
- Classify incidents based on **severity (High, Medium, Low)**
- Draft a formal **Incident Response Report**
- Learn SOC procedures like alert triage, threat identification, and response planning

What I Did?

Here is a brief summary of my workflow:

1. Logged in to **Splunk Cloud** and uploaded a .csv log file named sample_security_logs_for_splunk.csv
2. Ran **search queries** to analyze login attempts, malware alerts, suspicious downloads
3. Took **screenshots** of the search results and events
4. Created a **severity classification table** with explanation
5. Drafted this professional **Incident Response Report**

Tools & Environment

Splunk Cloud (Free Trial) – SIEM tool for monitoring

Sample Log File – sample_security_logs_for_splunk.csv with simulated events

Edge Browser – For Splunk dashboards access

Snipping Tool – To capture screenshots

MS Word – Used to compile this report

Methodology

To complete the task effectively, the following step-by-step methodology was adopted:

1. **Log In & Setup**
   - Accessed https://www.splunk.com and logged in to Splunk Cloud
   - Navigated to "Add Data" and uploaded the .csv file

2. **Search & Filter Alerts**
   - Used Splunk's search functionality to identify suspicious entries
   - Key queries used:
     - index=main status=" failed"
     - index=main message="Brute force suspected" OR message="Possible credential stuffing"
     - index=main action="malware"
     - index=main action="download"

3. Alert Analysis

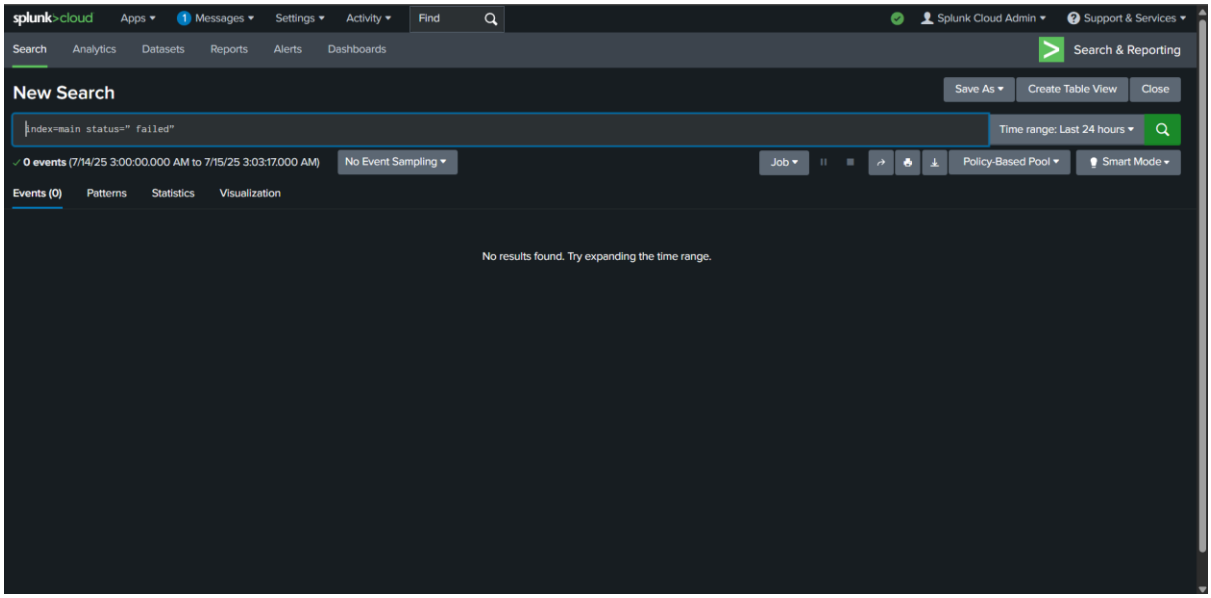
- Each suspicious entry was noted, and alerts were evaluated based on type, IP address, an message

4. Severity Classification

- Each alert was categorized into High, Medium, or Low severity

5. Documentation

- Screenshots were taken and compiled into a structured report with impact and mitigation suggestions



Summary of Detected Alerts

Timestamp	Source IP	Username	Event Description	Severity
2025-07-01 10:30:00	198.51.100.99	admin	Malware detected in file upload	**High**
2025-07-01 10:25:00	203.0.113.90	root	Possible credential stuffing	**High**
2025-07-01 10:18:00	203.0.113.45	admin	Brute force suspected	**High**
2025-07-01 10:22:00	192.168.1.15	bob	Login from restricted location	Medium
2025-07-01 10:20:00	198.51.100.23	alice	Confidential report downloaded	Medium
2025-07-01 10:17:00	192.168.1.12	unknown	Multiple failed login attempts	Low
2025-07-01 10:15:00	192.168.1.10	admin	Single failed login	Low

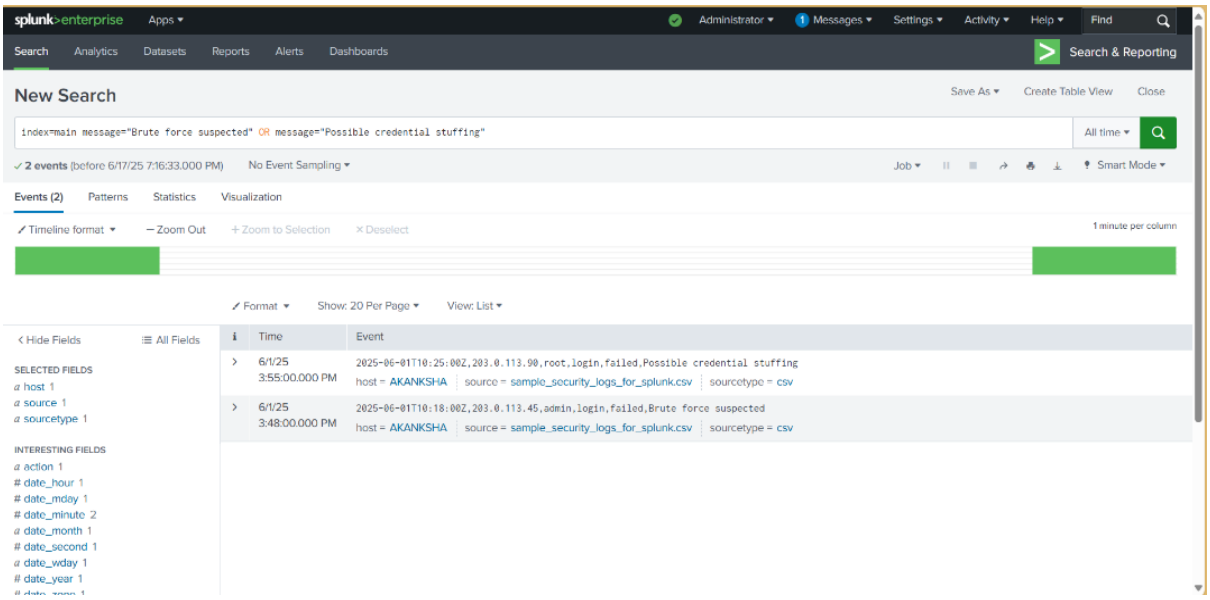


Figure: Brute force login attempts detected for the admin account from suspicious Ips

Also observed repeated failed login attempts for the ‘root’ user account, possibly indicating a credential stuffing attempt.

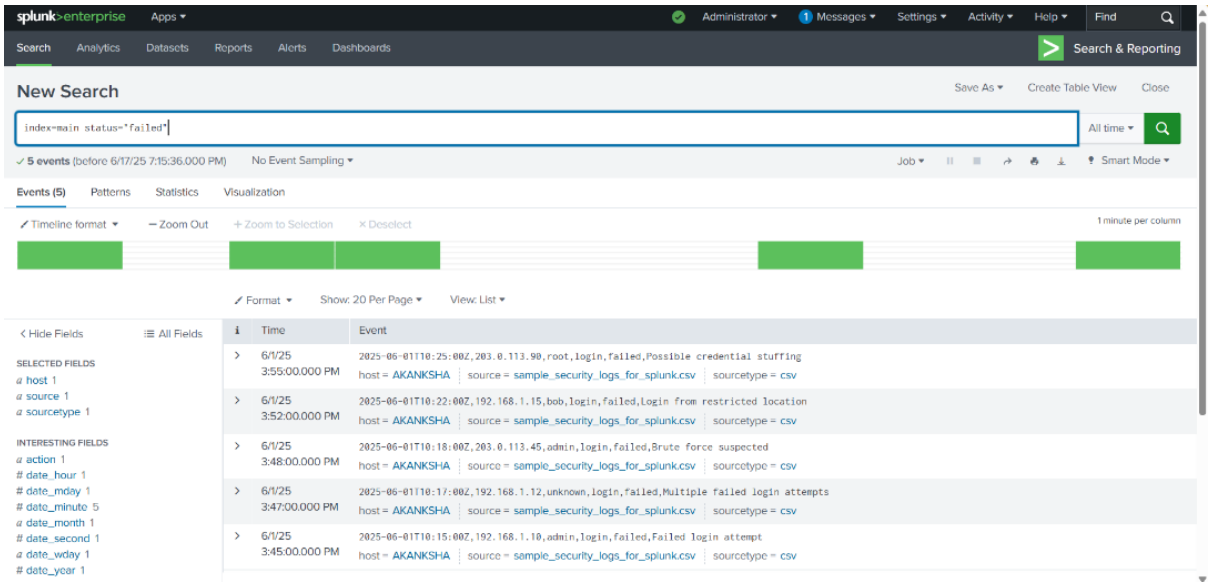
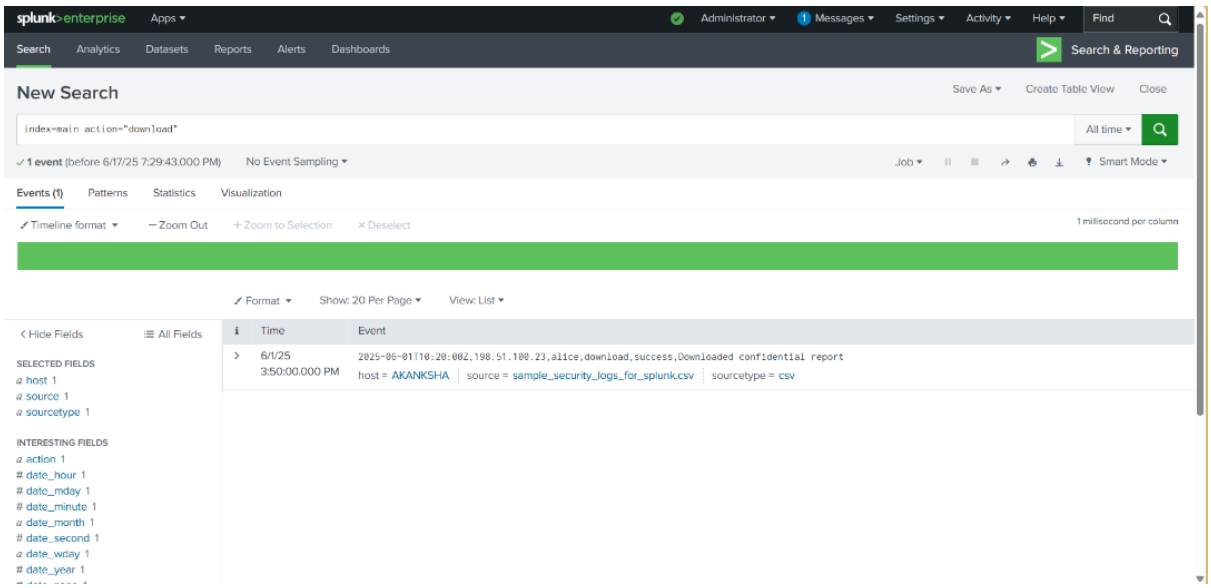


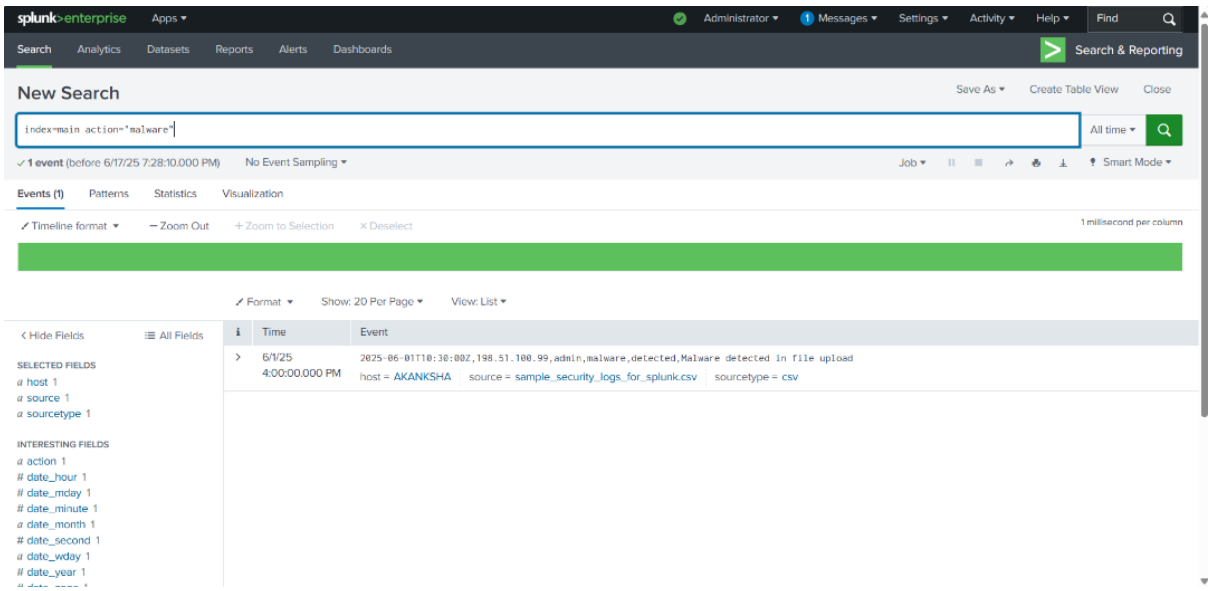
Figure: Credential stuffing based on repeated failed logins from multiple sources

Another notable event involved user ‘alice’ downloading a confidential report, flagged due to sensitive content access.



Incident Classification Table

Alert Type	Description	Severity	Reason for Classification
Malware Alert	Detected in admin upload	High	Indicated confirmed malicious content
Credential Stuffing Attempt	Login flood from multiple Ips	High	Matches known credential abuse pattern
Brute Force Login Attempt	Repeated failed attempts on admin account	High	Excessive failed login in short time
Suspicious Download	Confidential report downloads by alice	Medium	Possibly unauthorized access
Login from Unknown Location	Attempted by bob	Medium	Unusual source IP detected
Failed Login (Single)	One failed attempt by admin	Low	May be human error
Multiple Failed Logins	By unknown user	Low	No success, but notable attempt



Mitigation Recommendations

Threat	Recommended Action
Malware Upload	Implement antivirus scanning & restrict file types
Brute Force / Credential Abuse	Enforce lookouts, use CAPTCHA, apply rate limiting
Suspicious Logins	Add geofencing alerts, enforce MFA
Confidential Downloads	Enable download logging, limit user access
Multiple Failed	Logins Add alerting on 3+ failures per user/IP

Conclusion

This task gave me a real-world glimpse into the day-to-day work of SOC analysts. Using **Splunk,** I was able to:

- Ingest & analyze logs
- Detect actual suspicious patterns (malware, brute-force, IP anomalies)
- Understand how to classify & prioritize alerts
- Draft a formal response report based on cybersecurity industry practices

This exercise greatly strengthened my incident detection, alert triage, and log analysis skills, needed in a cybersecurity analyst's toolkit.