



Cyber Security Internship Report

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

Author: Waggari Misganu Ebsa

Internship Submitted to: Future Intern

Tools: Splunk Cloud Free Trial

Submission: September 2025

Table of Contents

Cyber Security Internship Report	1
Task 2: Security Operations Center (SOC) Internship Task: Security Alert Monitoring & Incident Response Simulation	1
Executive Summary.....	3
1. Introduction	3
Purpose	3
Scope.....	3
2. Environment Setup & Exploration	3
Exploration Activities:	3
3. Incident Classification by Priority.....	3
4. Remediation & Recommendations	4
5. Conclusion.....	4
6. Appendices.....	4
A. SPL Queries Executed:	4
B. Evidence (Screenshots):.....	4
7. References	6

Executive Summary

This report presents the analysis of simulated security logs using Splunk Cloud, a SIEM (Security Information and Event Management) tool. The objective was to detect suspicious activities such as repeated failed login attempts and sensitive file access, classify incidents by severity, and recommend effective remediation strategies.

The findings revealed multiple brute-force login attempts from suspicious IPs and a critical incident involving unauthorized access to the `/etc/passwd` file. These incidents underscore the importance of proactive monitoring, detection, and incident response in safeguarding organizational assets.

1. Introduction

Purpose

The purpose of this project was to simulate real-world incident detection and response by analyzing log data in Splunk Cloud. The task focused on identifying brute-force attacks, repeated login failures, and attempts to access sensitive system files.

Scope

- ✚ Log Source: `sample_logs.txt` (simulated logs)
- ✚ Platform: Splunk Cloud Free Trial
- ✚ Focus Areas: Failed login attempts, brute-force indicators, and sensitive file access events

2. Environment Setup & Exploration

Environment:

- ✚ Splunk Cloud Free Trial was used to ingest and analyze simulated logs.
- ✚ Log file included authentication attempts, usernames, IP addresses, and system access events.

Exploration Activities:

- ✚ Verified ingestion of logs into Splunk.
- ✚ Executed SPL queries to identify failed logins, repeated failed attempts by IP, and sensitive file access events.
- ✚ Reviewed suspicious IP activity and correlated events for context.

3. Incident Classification by Priority

Incident Type	IP Address	Priority	Notes
Sensitive file access attempt	192.168.1.10	High	Unauthorized access to /etc/passwd
Brute-force login attempts	192.168.1.11	High	3 failed login attempts
Brute-force login attempts	192.168.1.12	High	3 failed login attempts
Repeated login failures	192.168.1.10	Medium	2 failed logins before success

4. Remediation & Recommendations

Priority	Recommendations
High	Enable account lockouts after multiple failed login attempts
High	Monitor and block suspicious IPs (e.g., 192.168.1.11, 192.168.1.12)
High	Enable alerts for access to sensitive files like /etc/passwd
Medium	Enforce strong password policies and monitor repeated login failures
Medium	Implement Multi-Factor Authentication (MFA) to strengthen login security

5. Conclusion


The incident response exercise demonstrated how SIEM tools like Splunk enable early detection of malicious activities. The analysis uncovered high-priority threats such as brute-force login attempts and unauthorized sensitive file access. Implementing the recommended remediations—including account lockout, MFA, and sensitive file monitoring—will significantly improve security resilience. This task reinforced practical SOC skills for real-world security operations.

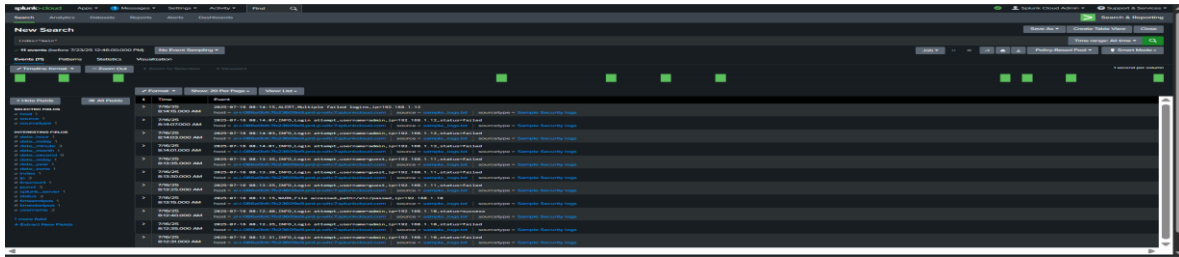
6. Appendices

A. SPL Queries Executed:

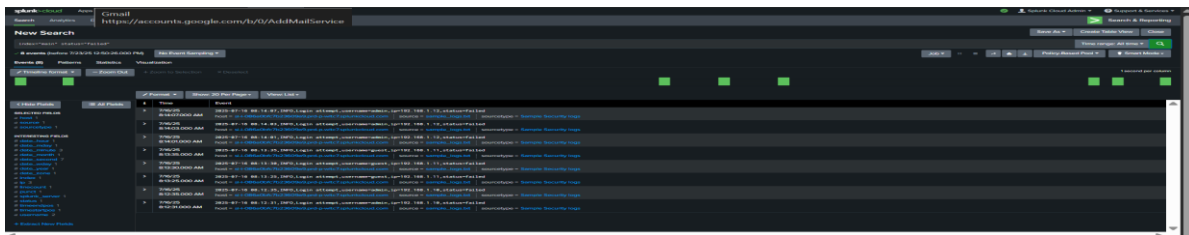
- Show All Logs: `index="main"`
- Failed Login Attempts: `index="main" status="failed"`
- Failed Logins by IP: `index="main" status="failed" | stats count by ip`
- Brute Force Detection: `index="main" status="failed" | stats count by ip | where count > 2`
- Sensitive File Access: `index="main" path="/etc/passwd"`

B. Evidence (Screenshots):

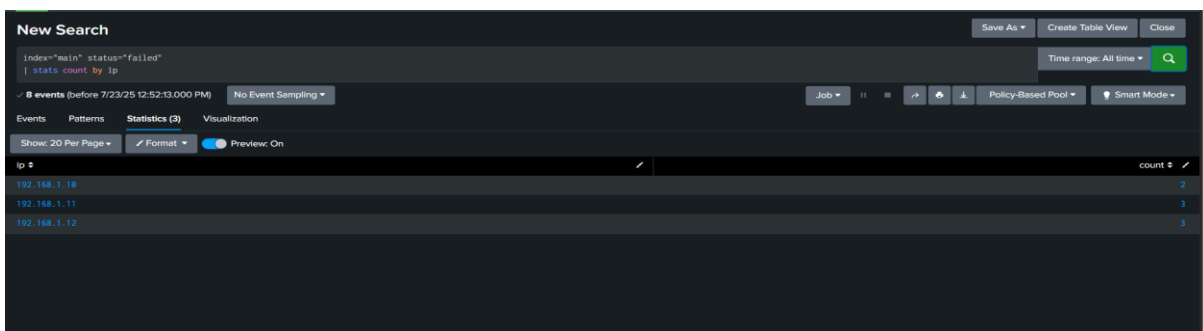
 All logs view (`all_events.png`)



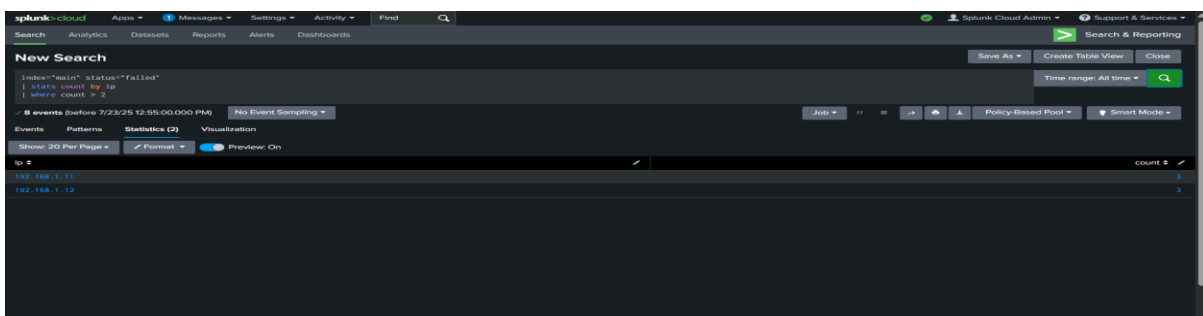
Failed login attempts (failed_login.png)



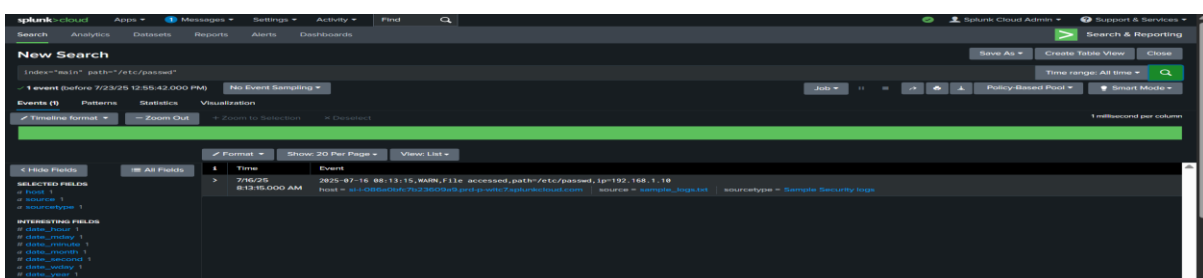
Grouped logins by IP (top_failed_by_ip.png)



Suspicious IPs (suspicious_ip.png)



Sensitive file access (file_access.png)



7. References

1. Splunk Documentation: <https://docs.splunk.com/>
2. OWASP Logging Cheat Sheet: <https://owasp.org/www-project-heat-sheets/>
3. NIST Cybersecurity Framework: <https://www.nist.gov/cyberframework>