Cover Page

Task 2 - Incident Response Report

Prepared by: **Dakshayani Sindiri**

Internship Program: **Future Interns - Cyber Security**

GitHub Repository:
https://github.com/dakshayanisindiri-98/FUTURE_CS_02

LinkedIn Profile:
https://www.linkedin.com/in/dakshayani-sindiri-a55037302

Date: **September 2025**

Dakshayani Sindiri
dakshayanisindiri@gmail.com

Table of Contents

1. Executive Summary
2. Introduction & Scope
3. Objectives
4. Tools & Environment
5. Methodology
6. SPL Queries and Explanations
7. Dashboards
8. Findings & Analysis
9. Recommendations
10. Conclusion
11. Appendix

1. Executive Summary

This report outlines the process and outcomes of analyzing cybersecurity logs using **Splunk** as part of the Future Interns Cyber Security Internship.

The task involved detecting malware activity, monitoring login events, identifying suspicious IP addresses, and generating visual dashboards to track security incidents.

Key Highlights:

- Total events analyzed: 50
- Malware detections: 11
- Most targeted IP: 203.0.113.77
- Most common threat type: Trojan Detected

The findings provide actionable insights to strengthen network defense mechanisms and enhance monitoring strategies.

2. Introduction & Scope

Introduction:

This task simulates real-world Security Operations Center (SOC) activities by using Splunk to analyze security logs.

The primary goal is to develop hands-on skills in threat detection, log analysis, and incident reporting.

Scope of Analysis:

- Only one log file was used: SOC_Task2_Sample_Logs.txt
- The analysis focused on:
  - Malware detection and classification
  - Login successes and failures
  - Identification of suspicious or repeated connection attempts
- Tool used exclusively: **Splunk Enterprise**

3. Objectives

The main objectives of this task were to:

- Detect and analyze malware events in the logs.
- Identify suspicious login activities, including successes and failures.
- Determine the most frequently attacked IP addresses.
- Visualize trends using Splunk dashboards.
- Generate actionable recommendations to mitigate future threats.

4. Tools & Environment

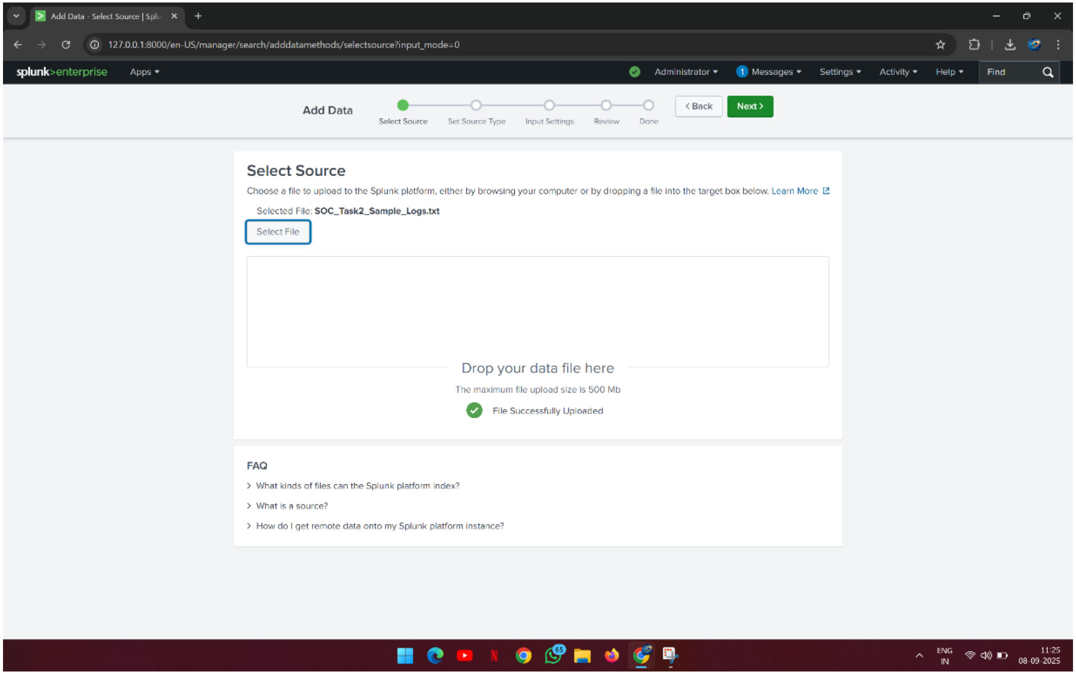
Tool / Resource	**Details**
Operating System	Windows 11 Home
Splunk Enterprise	Free Trial Version
Log File	SOC_Task2_Sample_Logs.txt
Index Used	main
Source Type	future-interns-01

5. Methodology

The analysis was performed in the following step-by-step process:

Step 1: Uploading Logs

- Uploaded SOC_Task2_Sample_Logs.txt into Splunk.
- Configured index as main and source type as future-interns-01.



Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

Selected File: **SOC_Task2_Sample_Logs.txt**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

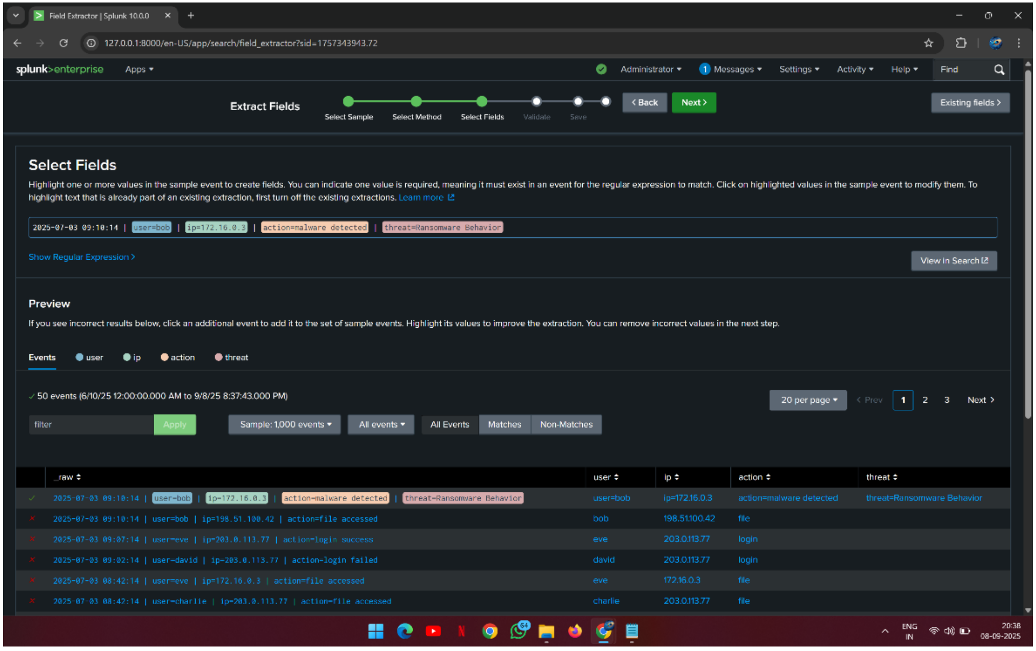
✓ File Successfully Uploaded

FAQ

- What kinds of files can the Splunk platform index?
- What is a source?
- How do I get remote data onto my Splunk platform instance?

Step 2: Field Extractions

- Created custom field extractions to parse key data:
    - **user**
    - **ip**
    - **action**
    - **threat**
- These extractions helped Splunk identify and organize data efficiently.



Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn more

```
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
```

Show Regular Expression ›

View in Search

Preview

If you see incorrect results below, click an additional event to add it to the set of sample events. Highlight its values to improve the extraction. You can remove incorrect values in the next step.

✓ 50 events (6/10/25 12:00:00.000 AM to 9/8/25 8:37:43.000 PM)

	_raw	user	ip	action	threat
✓	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior	user=bob	ip=172.16.0.3	action=malware detected	threat=Ransomware Behavior
✗	2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed	bob	198.51.100.42	file	
✗	2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success	eve	203.0.113.77	login	
✗	2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed	david	203.0.113.77	login	
✗	2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed	eve	172.16.0.3	file	
✗	2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed	charlie	203.0.113.77	file	

Step 3: Writing SPL Queries

- Developed SPL queries to analyze various events.
- Queries covered:
    - Counting events
    - Identifying malware activity
    - Login success and failure tracking
    - Threat categorization

Step 4: Creating Dashboards

- Built visual dashboards to interpret data patterns:
    1. **Top IPs with Malware Activity** (Column Chart)
    2. **Login Attempts Trend** (Line Chart)
    3. **Unique IP Count** (Single Value Panel)

Step 5: Reporting

- Compiled all findings, visualizations, and recommendations into this report.

6. SPL Queries and Explanations

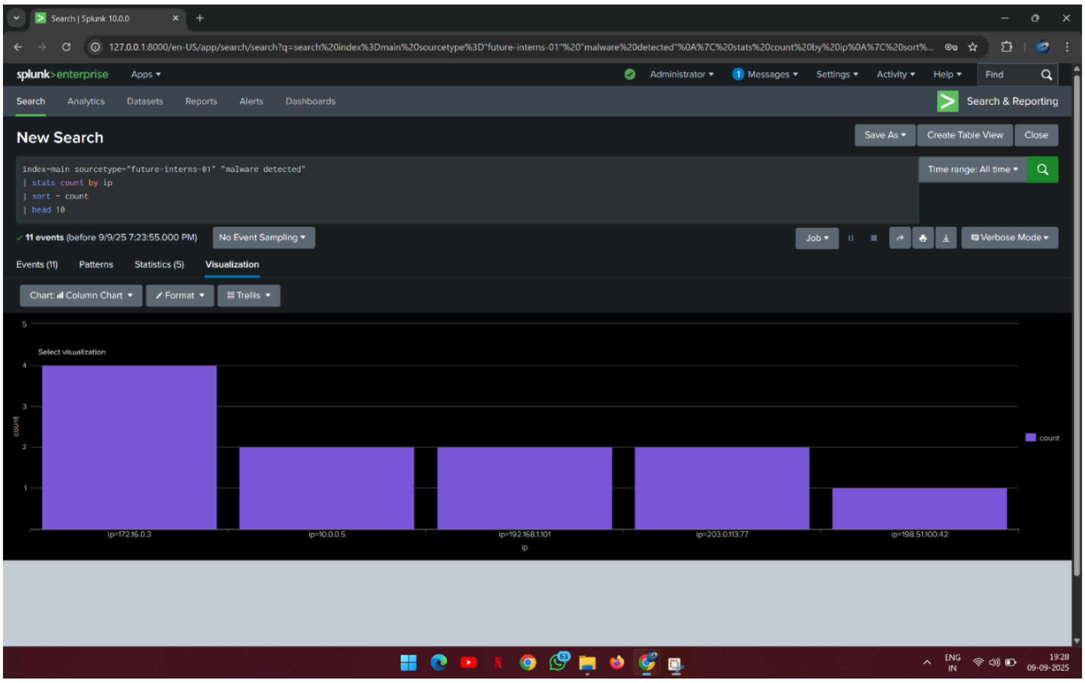
SPL Query	Purpose	Expected Output
index=main sourcetype="future-interns-01" | stats count as Total_Events	Count all events in the dataset	Total number of logs
index=main sourcetype="future-interns-01" ("login success" OR "login failed")	Identify all login successes and failures	List of all login-related events
index=main sourcetype="future-interns-01" "malware detected" | stats count by ip	Find top IPs with malware activity	Table of IPs sorted by count
index=main sourcetype="future-interns-01" | stats dc(ip) as Unique_IPs	Count distinct IP addresses	Displays the total number of unique IPs
index=main sourcetype="future-interns-01" "malware detected" | stats count by threat	Identify different malware types	Table of threats by count

7. Dashboards

Dashboard 1: Top IPs with Malware

- **Purpose:** Identify IP addresses with repeated malware detections.
- **Visualization:** Column Chart
- **SPL Query:**

```
index=main sourcetype="future-interns-01" "malware detected"
| stats count by ip
| sort - count
| head 10
```

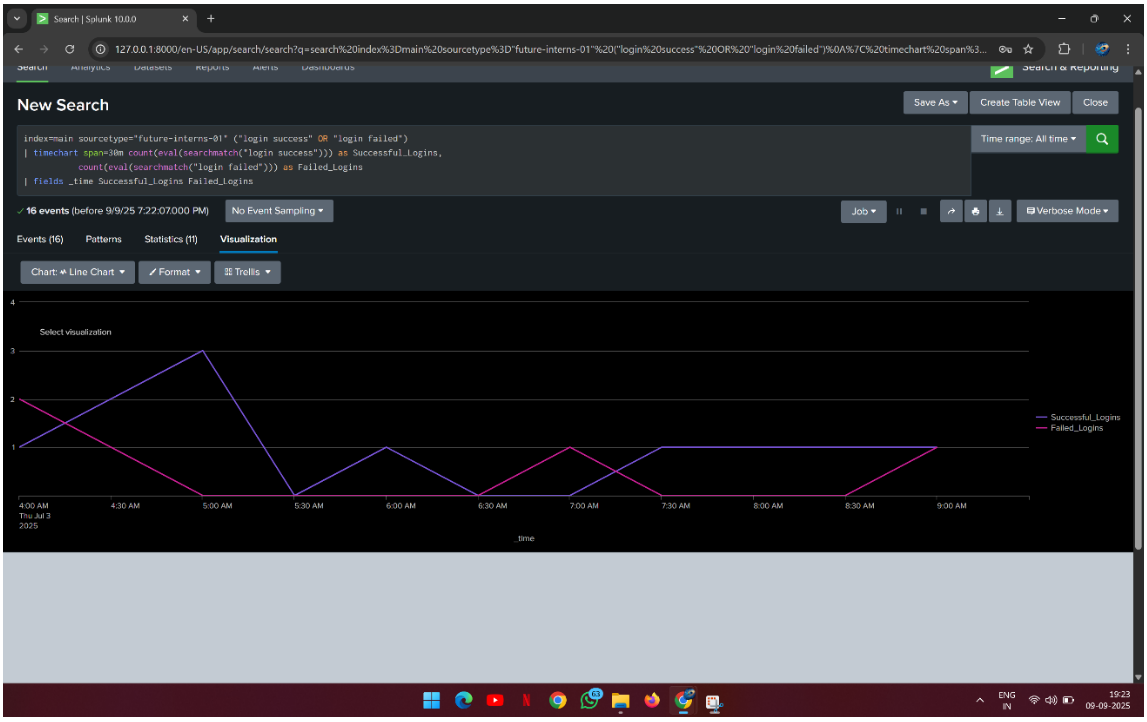


```
index=main sourcetype="future-interns-01" "malware detected"
| stats count by ip
| sort - count
| head 10
```

✓ 11 events (before 9/9/25 7:23:55.000 PM)

Dashboard 2: Login Attempts Trend

- **Purpose:** Display login successes and failures over time to detect unusual activity.
- **Visualization:** Line Chart
- **SPL Query:**
  index=main sourcetype="future-interns-01" ("login success" OR "login failed")
  | timechart span=30m count(eval(searchmatch("login success"))) as Successful_Logins,
    count(eval(searchmatch("login failed"))) as Failed_Logins



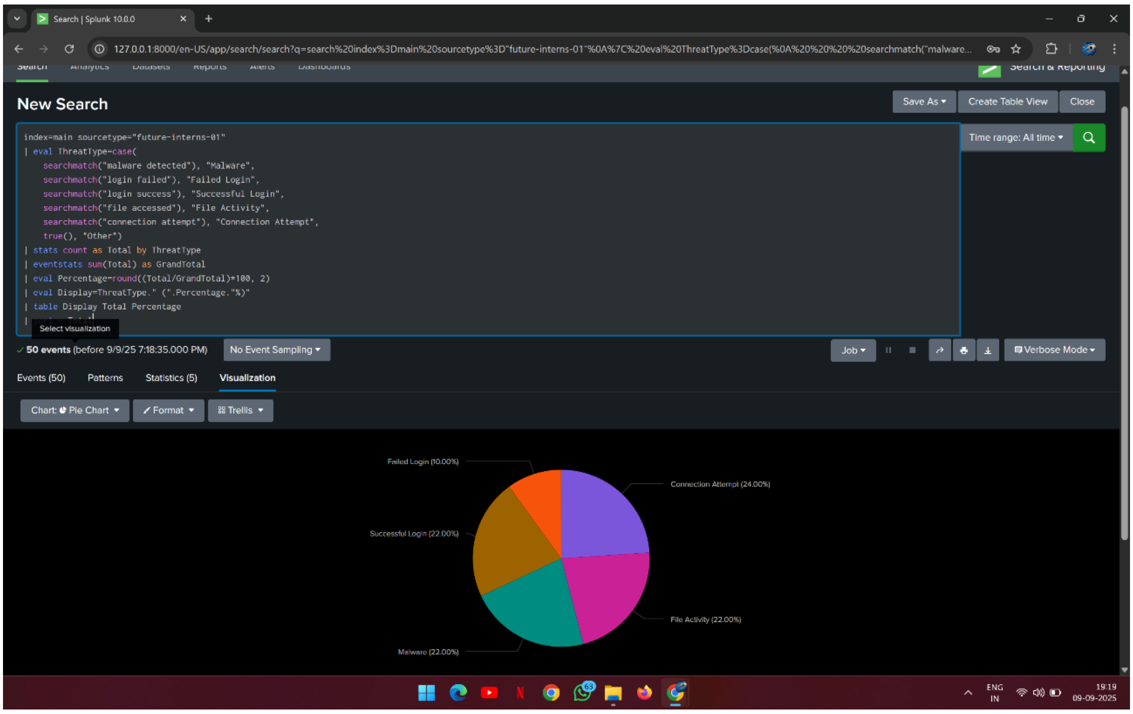
```
index=main sourcetype="future-interns-01" ("login success" OR "login failed")
| timechart span=30m count(eval(searchmatch("login success"))) as Successful_Logins,
         count(eval(searchmatch("login failed"))) as Failed_Logins
| fields _time Successful_Logins Failed_Logins
```

✓ 16 events (before 9/9/25 7:22:07.000 PM)

Dashboard 3:Threats with Percentage (Pie Chart)

- **Purpose**: Show the distribution of different threat categories with their respective percentages to easily identify the most common threats in the logs.
- **Visualization:** Pie Chart Panel
- **SPL Query:**

```
index=main sourcetype="future-interns-01"
| eval ThreatType=case(
    action="malware detected","Malware",
    action="login failed","Failed Login",
    action="login success","Successful Login",
    action="file accessed","File Activity",
    action="connection attempt","Connection Attempt",
    true(),"Other")
| stats count by ThreatType
| eventstats sum(count) as Total
| eval Percentage=round((count/Total)*100,2)
| eval Display=ThreatType." (".Percentage."%)"
| fields Display count
```



127.0.0.1:8000/en-US/app/search/search?q=search%20index%3Dmain%20sourcetype%3D"future-interns-01"%0A%7C%20eval%20ThreatType%3Dcase(%0A%20%20%20%20searchmatch("malware...

New Search

```
index=main sourcetype="future-interns-01"
| eval ThreatType=case(
    searchmatch("malware detected"), "Malware",
    searchmatch("login failed"), "Failed Login",
    searchmatch("login success"), "Successful Login",
    searchmatch("file accessed"), "File Activity",
    searchmatch("connection attempt"), "Connection Attempt",
    true(), "Other")
| stats count as Total by ThreatType
| eventstats sum(Total) as GrandTotal
| eval Percentage=round((Total/GrandTotal)*100, 2)
| eval Display=ThreatType." (".Percentage."%)"
| table Display Total Percentage
| sort - Total
```

✓ 50 events (before 9/9/25 7:18:35.000 PM)

Time range: All time

8. Findings & Analysis

Metric	Value
Total Events Analyzed	50
Total Malware Detections	11
Failed Login Attempts	5
Successful Logins	11
Most Targeted IP	203.0.113.77

Metric	**Value**
Most Common Threat	Trojan Detected

Analysis:

- IP **203.0.113.77** was the most frequently associated with malware and suspicious activity.
- Multiple failed login attempts indicate potential **brute-force attacks**.
- **Trojan malware** was the most common threat type observed.
- Malware activity was concentrated on a few IPs, suggesting targeted attacks.

9. Recommendations

Based on the findings:

- Isolate infected machines immediately and perform full malware scans.
- Enable **multi-factor authentication (MFA)** for all sensitive accounts.
- Implement account lockout policies after 3–5 failed login attempts.
- Configure Splunk alerts for real-time detection of malware and suspicious logins.
- Review dashboards daily to identify early warning signs.

10. Conclusion

The analysis successfully identified patterns of malicious activity and login behaviors using Splunk.

By implementing the recommended actions, the organization can significantly reduce the risk of future incidents and maintain a robust cybersecurity posture.

11. Appendix

- Complete list of SPL queries.
  1. **Display first 5 logs**
  2. **Display first 10 logs in a table**
  3. **Total number of logs**
  4. **Show all logins(success and failure events)**
  5. **Total logins, success, and failure in one table**
  6. **Count events by IP address**
  7. **Top 20 most active IPs**
  8. **Count events by username**
  9. **Display only malware detection logs**
  10. **Count malware events by IP**
  11. **Malware vs Login Failures by IP**
  12. **Threats grouped by type**
  13. **Top 5 malware-affected IPs**
  14. **Timeline of all events**
  15. **Unique IP Count**
  16. **Threats with percentage (Pie Chart)**
  17. **Top IPs with Malware Events (Column Chart)**
  18. **Login Attempts Trend Over Time (Line Chart)**
- GitHub link to screenshots folder: https://github.com/dakshayanisindiri-98/FUTURE_CS_02