# Security Alert Monitoring Report – Splunk SIEM

(Internship Simulation Task)

## 📌 Project Title:

Security Incident Detection and Analysis Using Splunk SIEM

## 👨‍💻 Internship Program:

Future Interns – Cybersecurity Internship  
Conducted by Future Interns

## 🧑‍🎓 Intern Name:

Hari Rakesh Yengantiwar

## 🧰 Tools & Technologies Used:

• 🖥️ Splunk Enterprise (Local Setup – Windows)  
• 🧪 Log Sources: Authentication, System, Network & Application Logs  
• 📸 Screenshots captured from Splunk Search & Reporting  
• 📝 Report compiled using Microsoft Word

## 🌍 Test Environment:

• Host Machine: Windows 11  
• Splunk Index Source: Manually uploaded log files (Application, Syslog, Network, Auth)  
• Environment: Local (Standalone Analysis)

# 🧾 Executive Summary

This report summarizes a Security Operations Center (SOC) simulation exercise conducted using Splunk Enterprise.  
The purpose was to monitor and analyze security alerts generated from multiple log sources — including authentication,  
system, and network logs — to identify potential security threats. The project demonstrates hands-on SOC analyst activities  
such as log ingestion, searching, alert triage, and incident reporting.

# 🌐 Scope of Assessment

The objective of this project was to simulate a SOC environment and perform:  
• Log ingestion and parsing in Splunk  
• Searching for suspicious patterns (failed logins, firewall changes, USB drivers)  
• Classifying and prioritizing alerts  
• Preparing an incident response summary

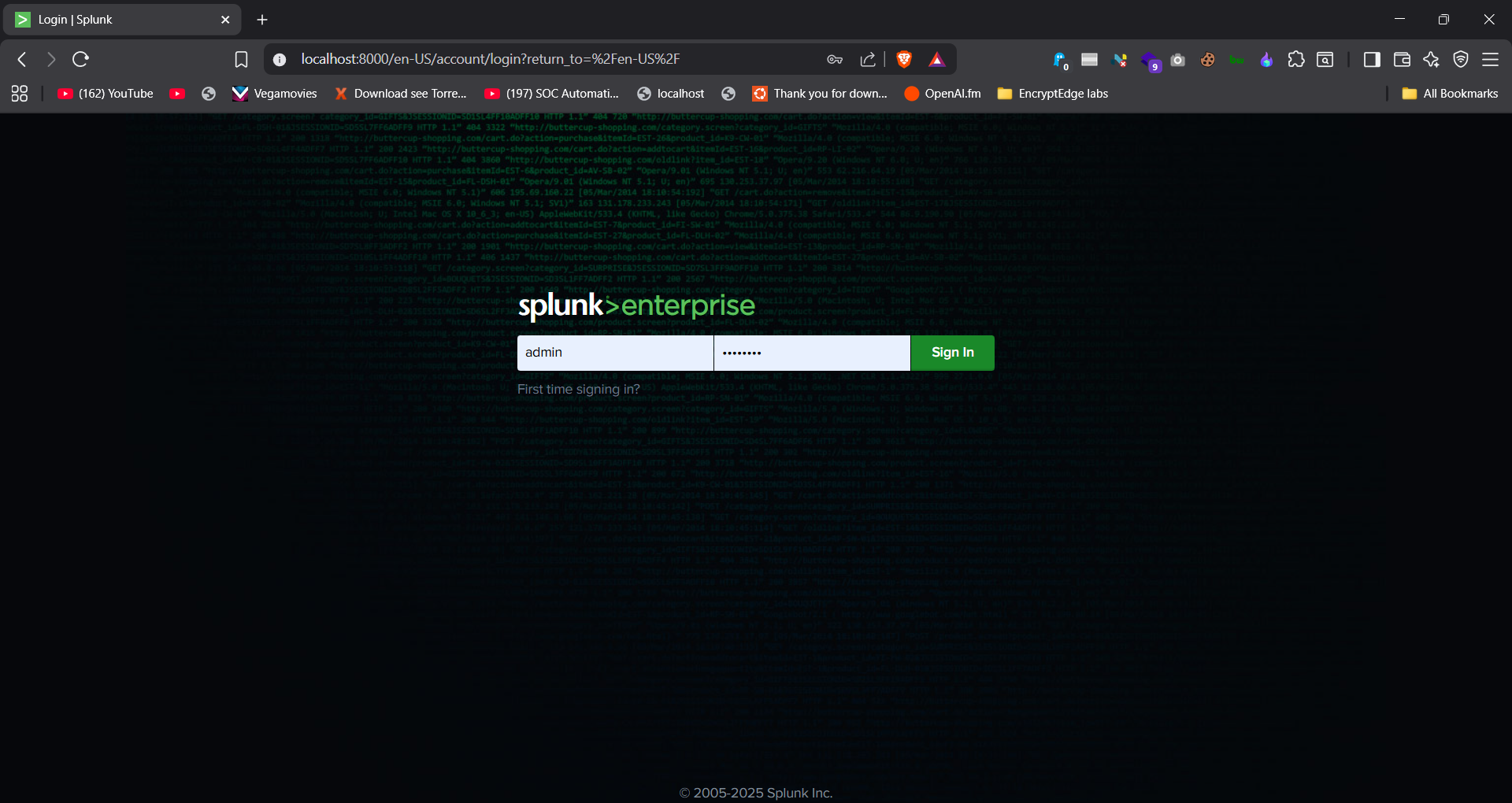
## 🔎 Logs Used:

• Application.txt – Application errors and runtime failures  
• syslog.txt – System-level events and driver installations  
• Network Logs.txt – Firewall changes and network activity  
• auth.log – Authentication attempts and failed logins

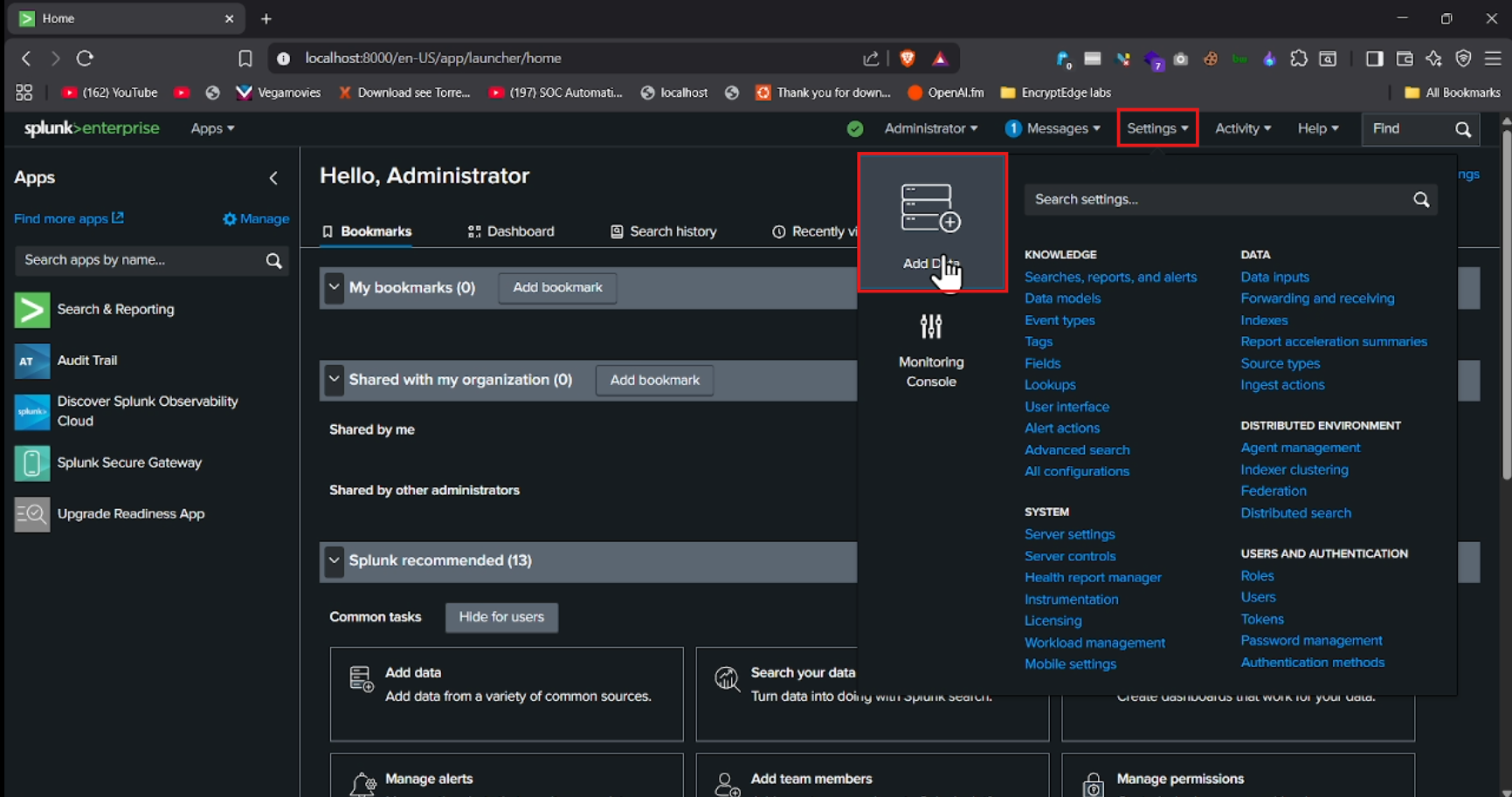
# 🚨 Incident Summary Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Incident # | Type of Alert | Severity | Description | Recommended Action |
| 1 | Firewall Rule Modified | High | Firewall rule added/deleted in logs | Verify if rule was authorized, reset to default |
| 2 | Failed Login Attempts | High | Multiple failed passwords in auth.log | Check source IP, enable account lockout |
| 3 | Unrecognized USB Driver | Medium | USBPcap driver detected | Remove unauthorized drivers, inspect device |
| 4 | Application Errors (.NET) | Low | Repeated runtime errors | Investigate for tampering or crashes |

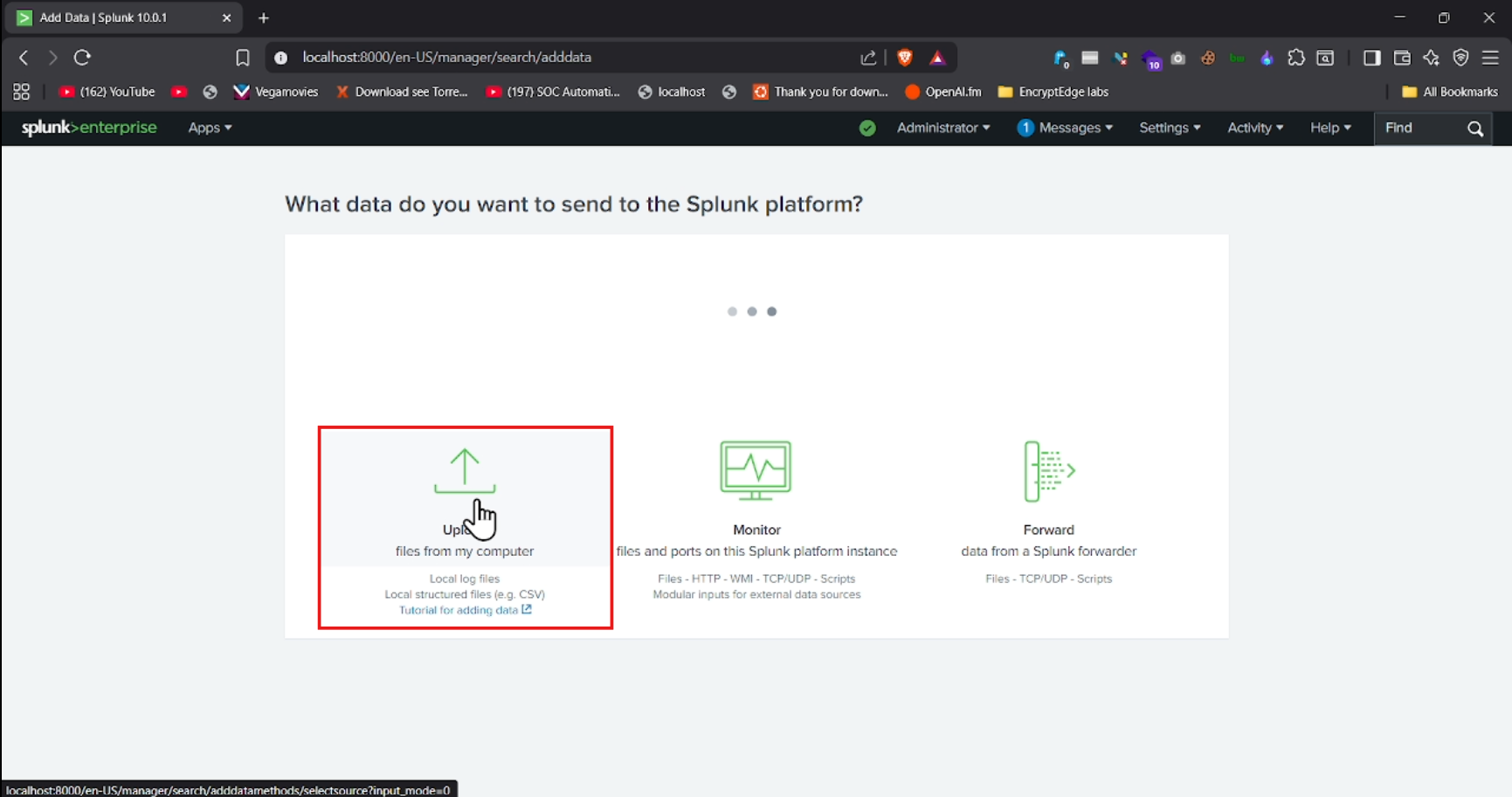
# 🔍 Detailed Findings



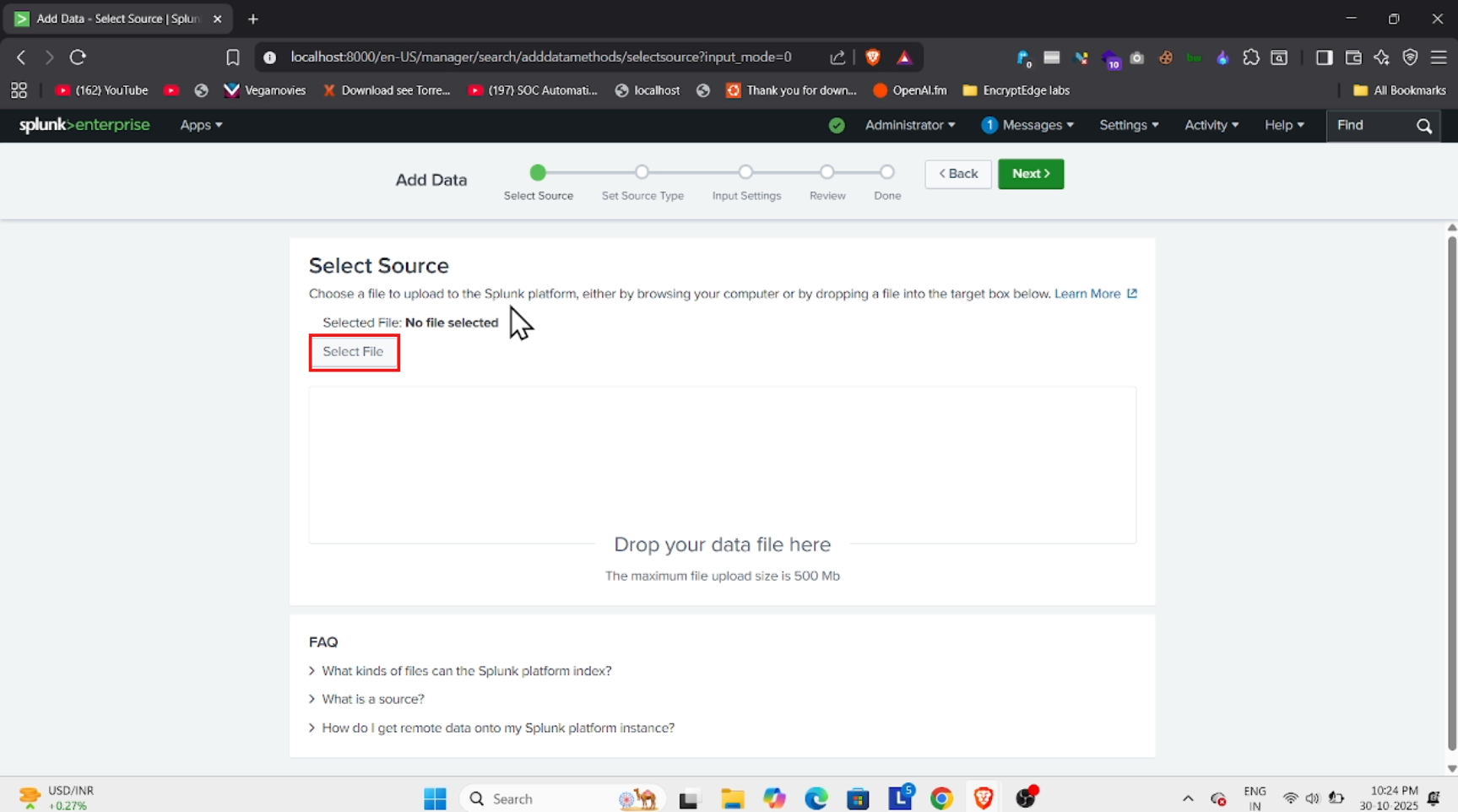
1.png – Splunk Login Page  
  
This is the Splunk Enterprise login screen where the user logs in using admin credentials. It is the first step to access Splunk to perform log analysis.



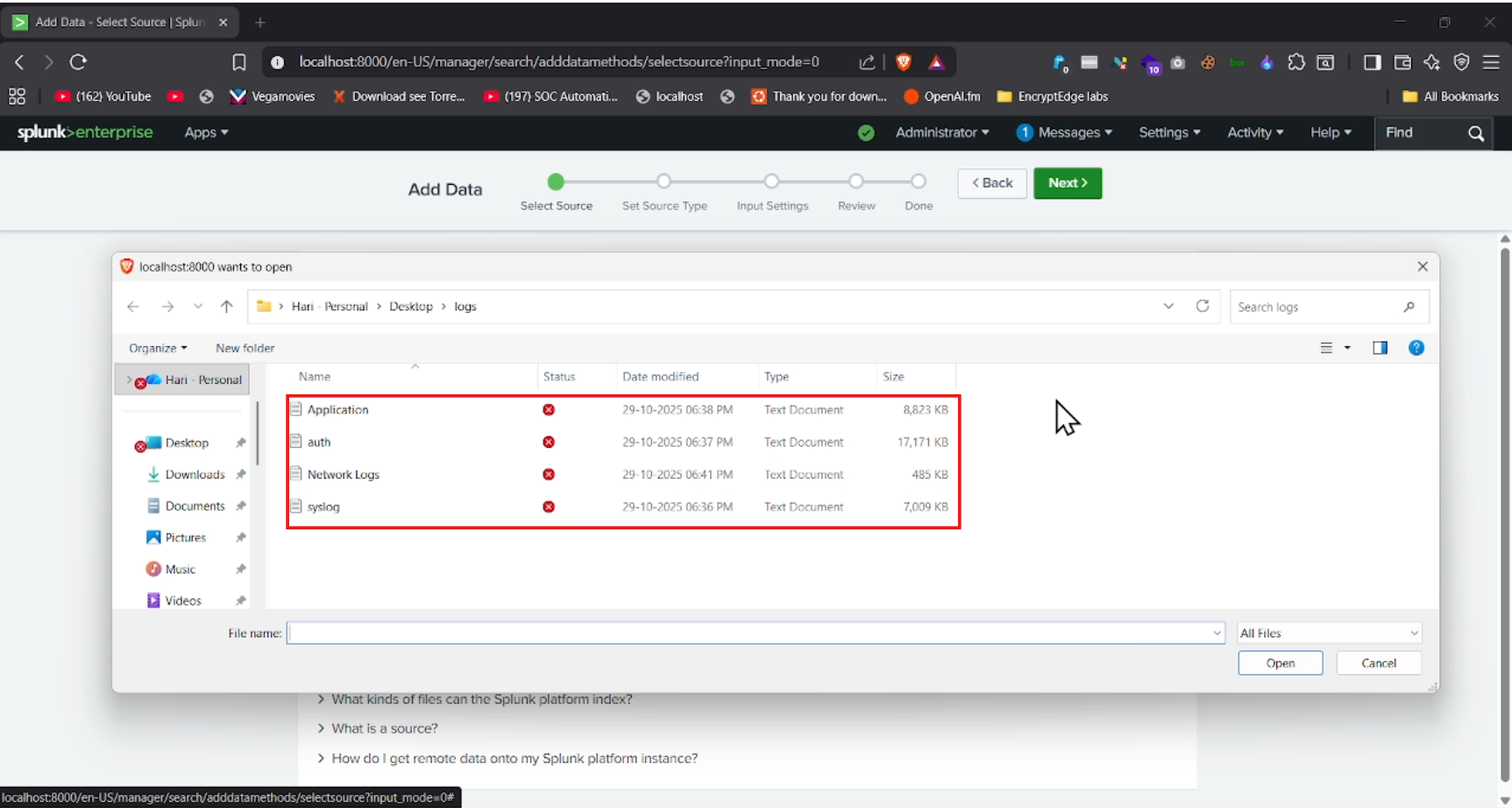
2.png – Splunk Home Dashboard  
  
After login, this is the main Splunk dashboard where you can manage apps, add data, search logs, and view dashboards.



3.png – Add Data Options  
  
The user selects 'Upload files from my computer' to ingest the log files (Application.txt, syslog.txt, Network Logs.txt, auth.log) for analysis.



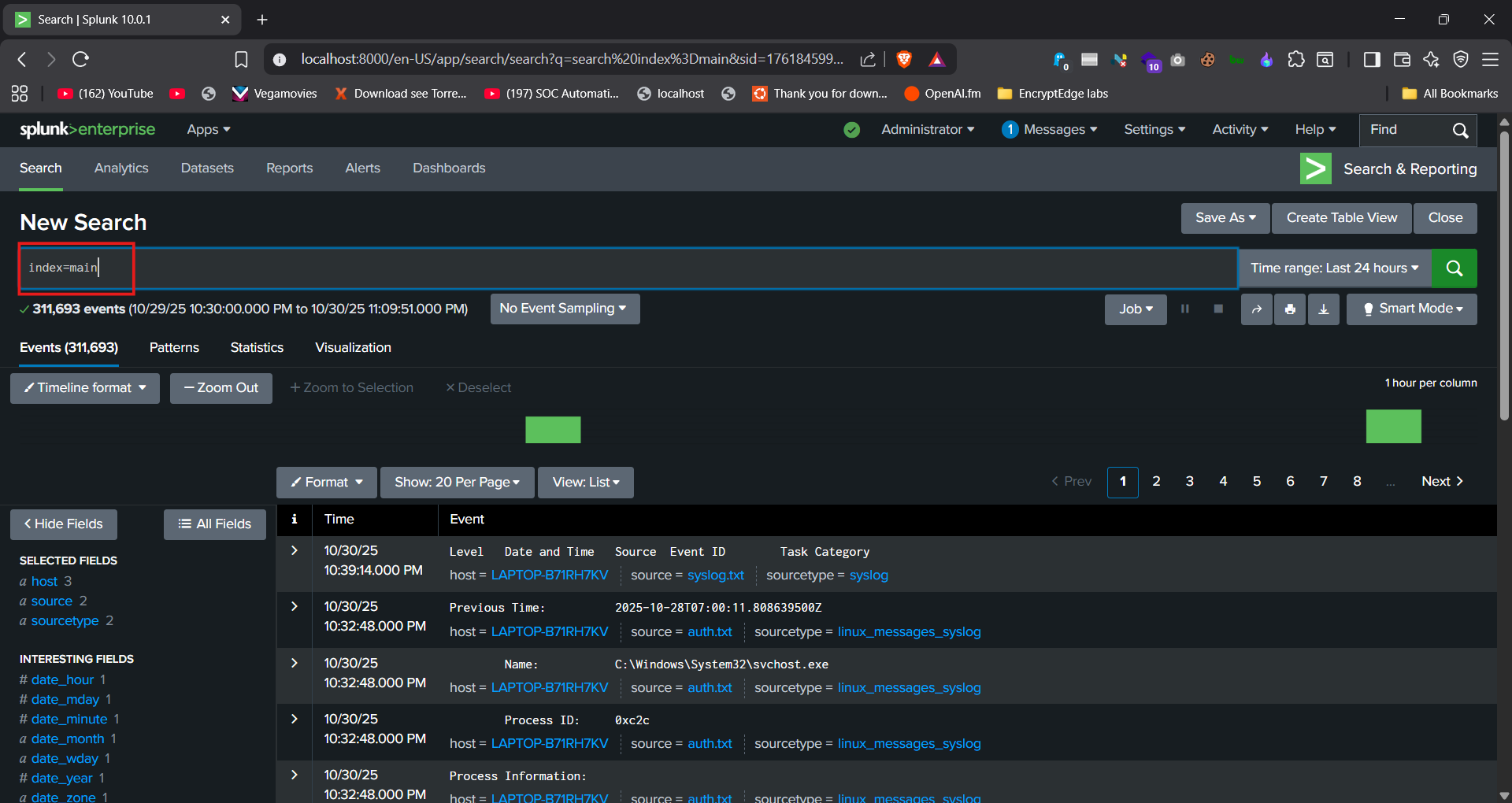
4.png – Upload Log Files  
  
This step shows uploading local log files into Splunk, preparing them for indexing and searching.



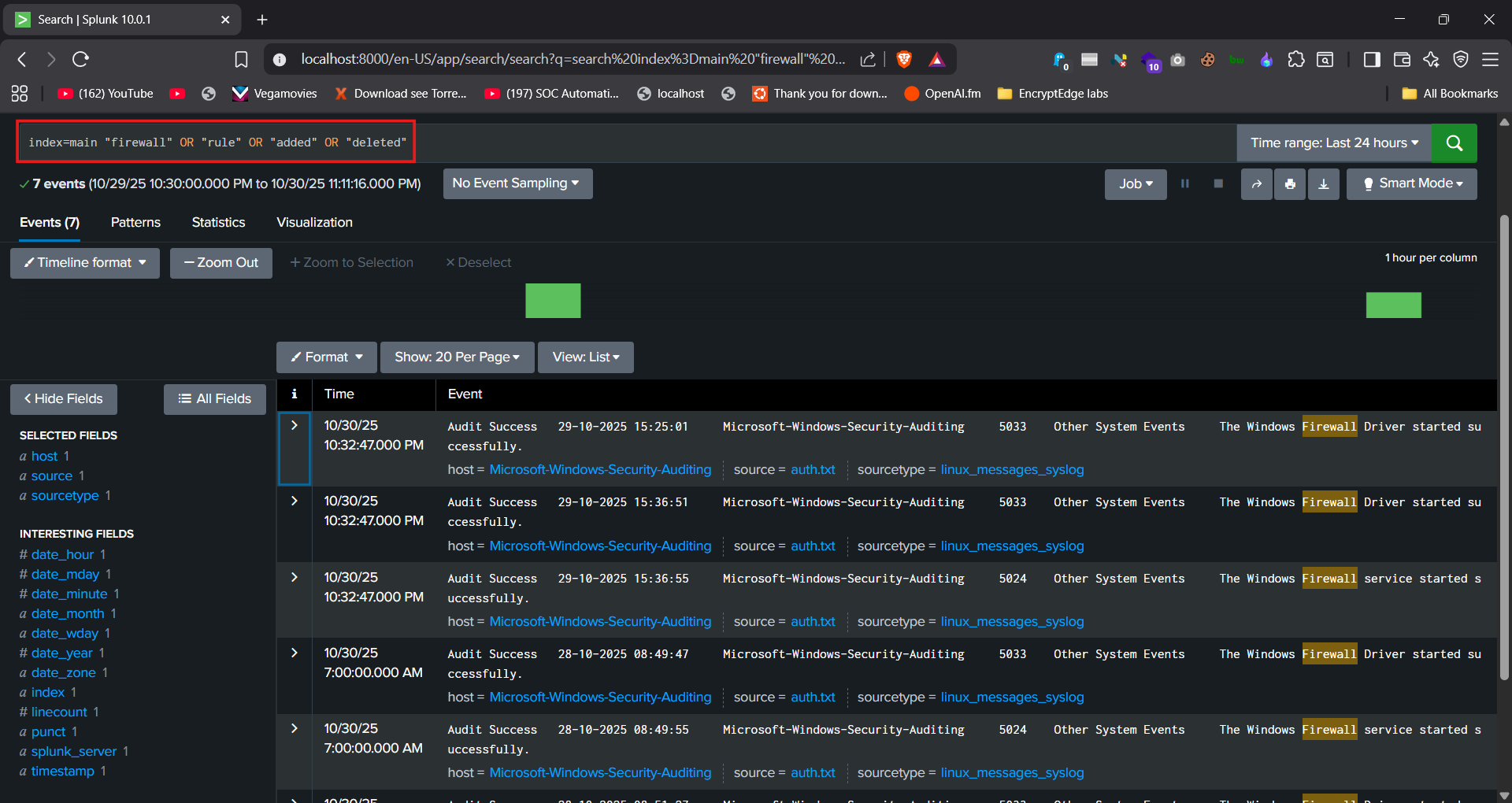
5.png – Selecting Log Files  
  
This screenshot displays the file selection window for the log sources used in this SOC task.



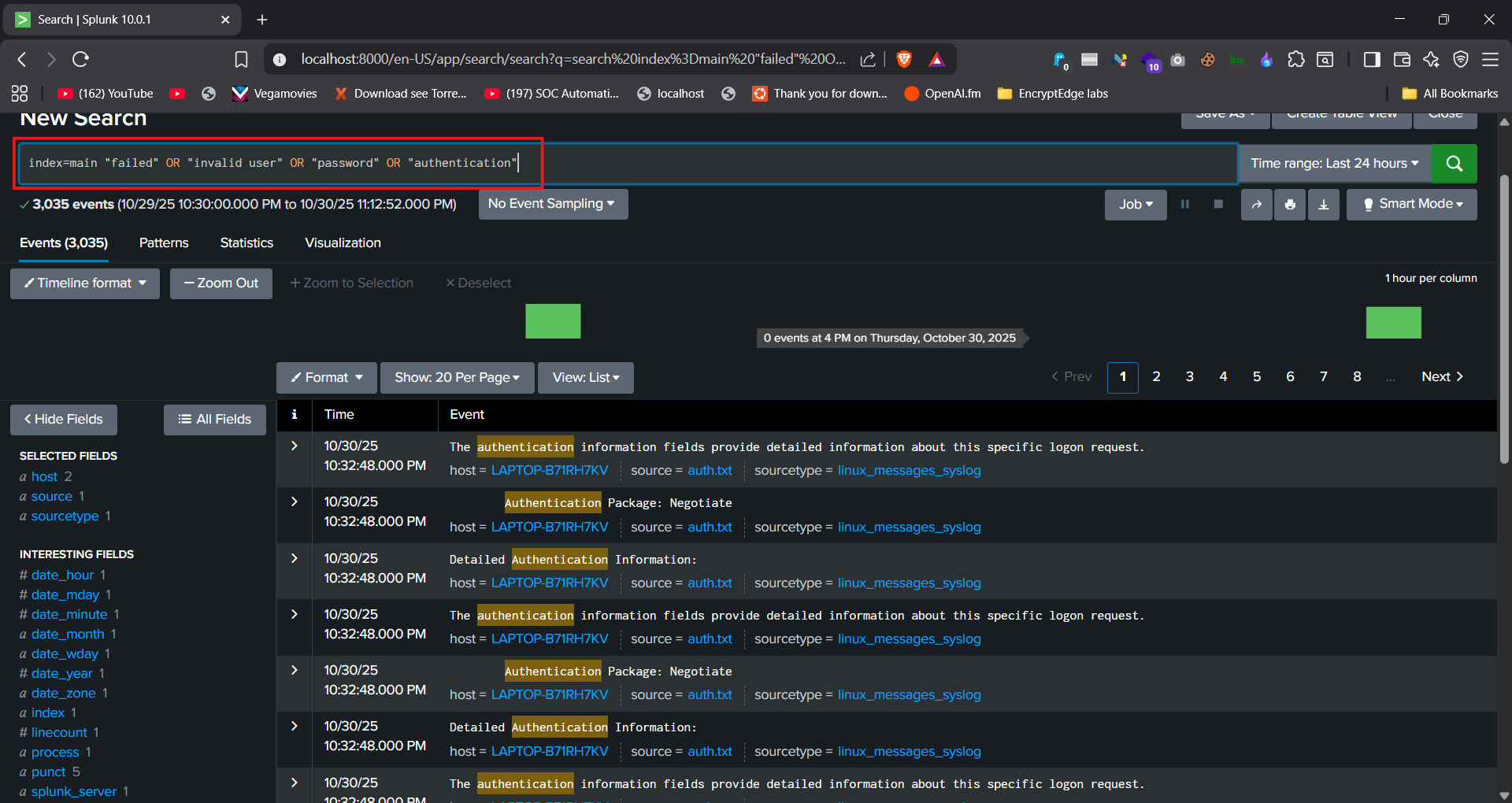
6.png – Set Source Type  
  
Here, the source type (plain text) is assigned to help Splunk interpret and index the logs correctly.



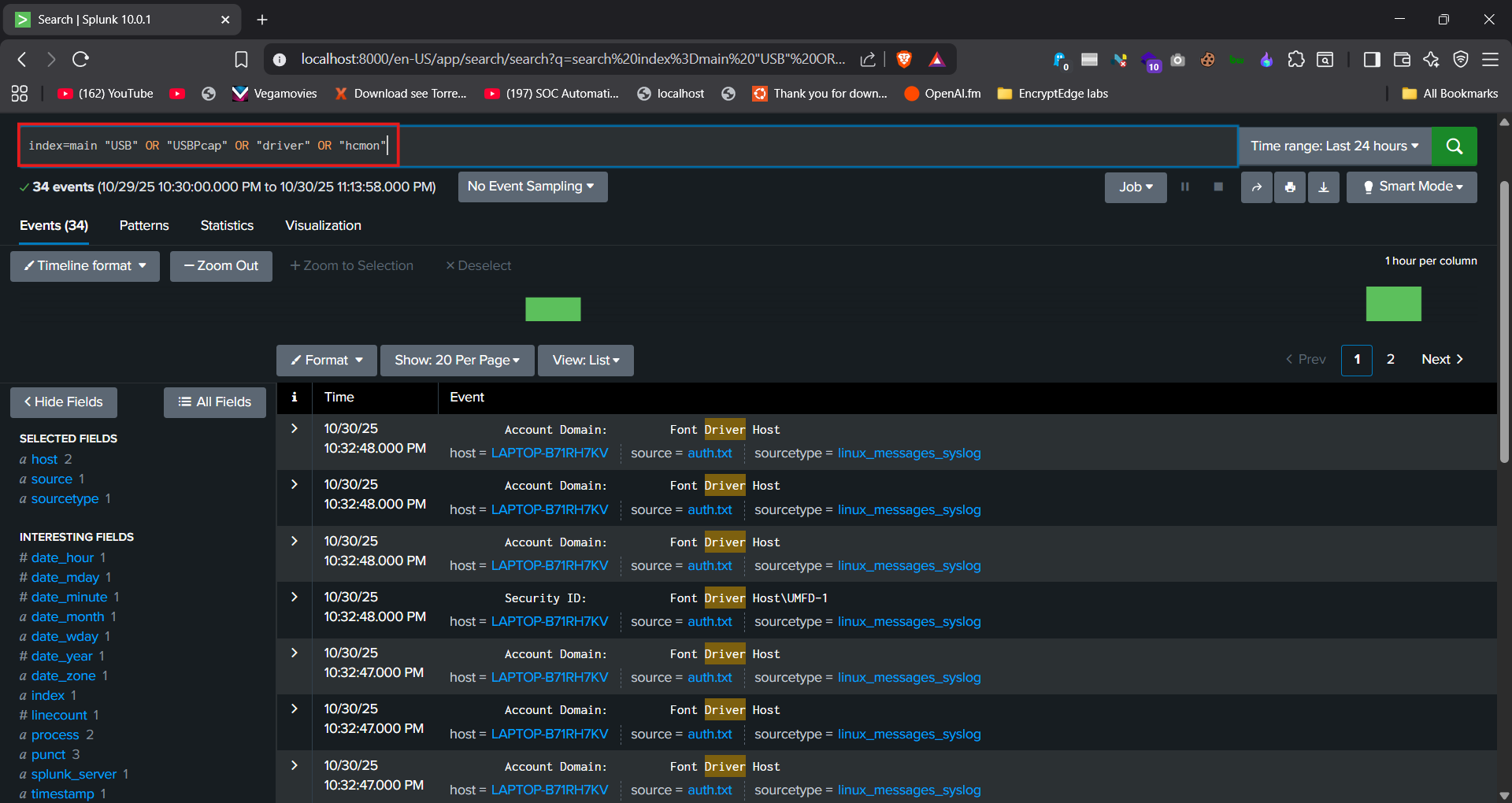
7.png – Viewing Indexed Logs  
  
After indexing, 'index=main' displays all ingested events, which can then be filtered for suspicious activity.



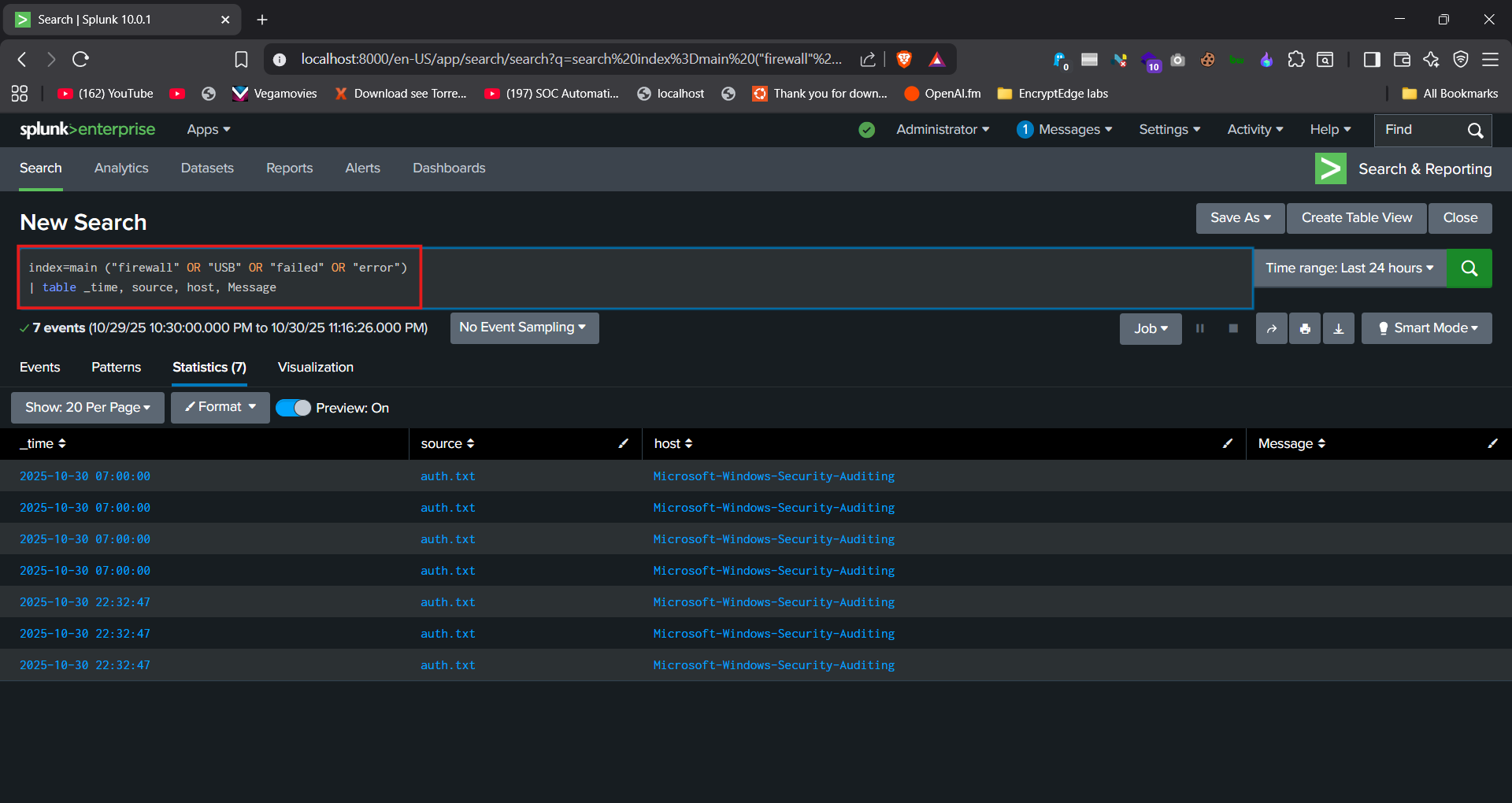
8.png – Firewall Log Search  
  
The search query filters firewall-related logs to detect any unauthorized rule changes.



9.png – Authentication Failure Search  
  
A search query to identify failed or invalid login attempts indicating brute-force or unauthorized access attempts.



10.png – USB and Driver Events  
  
Detects logs mentioning USBPcap or unrecognized drivers, which could mean data exfiltration or local packet capture.



11.png – Combined Query Results  
  
Shows a combined search of multiple log sources for suspicious indicators, giving a complete threat overview.

# ✅ Conclusion

This SOC simulation project successfully demonstrated real-world SIEM operations using Splunk.  
The intern effectively monitored logs, detected incidents, and prepared a structured response report —  
developing practical SOC skills in alert analysis, triage, and reporting.