

PROJECT REPORT: Log Analysis and Threat Classification using Splunk



Name: Pranit Kalambate

Date: November 18, 2025

Subject: Security Information and Event Management (SIEM) Implementation

TABLE OF CONTENT

SR.NO	NAME	PAGE
1.	OBJECTIVE	3
2.	METHODOLOGY	4
3.	RESULTS AND VISUALIZATION	10
4	CONCLUSION	12

1.OBJECTIVE

The objective of this project was to configure a Splunk Enterprise environment to ingest Linux authentication logs and implement a classification system for SSH brute-force attacks. The goal was to distinguish between high-severity threats (targeted attacks on valid accounts) and low-severity noise (automated bot scanning).

Environment & Tools

SIEM Platform: Splunk Enterprise (v10.0.1) installed on Windows.

Log Source: Kali Linux machine.

Data Transport: Splunk Universal Forwarder.

Target Log File: `/var/log/auth.log` (Linux Authentication Logs).

2.METHODOLOGY

2.1. Data Ingestion and Initial Analysis

The project began by forwarding the `/var/log/auth.log` file from the Linux machine to the Splunk indexer. An initial search was performed to identify all failed SSH login attempts using the keyword "Failed password".

Search Query:

`index=* "Failed password"

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** `index=* "Failed password"`. The results are filtered to show events from Nov 18, 2025, between 3:30:00.000 PM and 3:30:17:000 PM.
- Event Count:** 14 events.
- Event List:** The list displays 14 log entries, each containing a timestamp, host information, and the exact log message. Several messages are highlighted with red boxes:
 - Nov 18/25 2:21:48.422 PM host=kali source=/var/log/auth.log sourcetype=linux_secure: failed password for root from ::1 port 46668 ssh2
 - Nov 18/25 2:21:57.21 PM host=kali source=/var/log/auth.log sourcetype=linux_secure: failed password for invalid user admin from ::1 port 39484 ssh2
 - Nov 18/25 2:20:48.357 PM host=kali source=/var/log/auth.log sourcetype=linux_secure: failed password for invalid user testuser from ::1 port 57142 ssh2
 - Nov 18/25 2:19:53.572 PM host=kali source=/var/log/auth.log sourcetype=linux_secure: failed password for invalid user apacheuser from ::1 port 68362 ssh2

Figure 1: Raw search results showing failed login attempts.

2.2. Developing Threat Logic

Upon analyzing the raw logs, two distinct patterns emerged:

- 1) Pattern A: Attacks against specific, valid users (e.g., 'root'). This indicates a targeted attempt to breach a known account.
- 2) Pattern B: Attacks against non-existent users (e.g., 'admin', 'testuser', 'apacheuser'). This indicates generic "spray-and-pray" scanning.

2.3. Configuring "High Risk" Event Types

To prioritize targeted attacks, a specific search filter was applied to exclude invalid users. This isolates attempts on valid accounts (like root).

Search Query:

`index=* "Failed password" * NOT invalid`

The screenshot shows the Splunk 10.0.1 interface with a search bar containing the query `index=* "Failed password" * NOT invalid`. The search results table displays five events from November 17, 2025, between 3:30:00.000 PM and 3:39:42.000 PM. Each event log entry includes a timestamp, host (kali), source (varlog/auth.log), and sourcetype (linux_secure). The logs show multiple failed password attempts for root from various ports (e.g., 46668, 48357, 18498) on the host 'kali'. The entire search bar and the first few rows of the table are highlighted with a red box.

Time	Event
11/18/25 2:21:18.422 PM	2025-11-18T14:21:18.422919+05:30 kali sudo: prinit : TTYpts/0 ; PWD /home/prinit ; USER root ; COMMAND /usr/bin/grep 'Failed password' /var/log/auth.log host = kali source = varlog/auth.log sourcetype = linux_secure
11/18/25 2:21:05.721 PM	2025-11-18T14:21:05.721414+05:30 kali sshd[261]: Failed password for root from ::1 port 46668 ssh2 host = kali source = varlog/auth.log sourcetype = linux_secure
11/18/25 2:20:58.304 PM	2025-11-18T14:20:58.18498+05:30 kali sshd[261]: Failed password for root from ::1 port 46668 ssh2 host = kali source = varlog/auth.log sourcetype = linux_secure
11/18/25 2:20:48.357 PM	2025-11-18T14:20:48.357408+05:30 kali sshd[261]: Failed password for root from ::1 port 46668 ssh2 host = kali source = varlog/auth.log sourcetype = linux_secure
11/18/25 2:18:41.808 PM	2025-11-18T14:18:41.80865+05:30 kali sudo: prinit : TTYpts/0 ; PWD /home/prinit ; USER root ; COMMAND /usr/bin/grep 'Failed password' /var/log/auth.log host = kali source = varlog/auth.log sourcetype = linux_secure

Figure 2: Filtering logs to show only potential targeted attacks.

This search logic was saved as a new Event Type named "highrisky".

Priority: 3 (High)

Color: Red

Rationale: High priority is assigned because the attacker knows the username is valid, significantly increasing the risk of a breach.

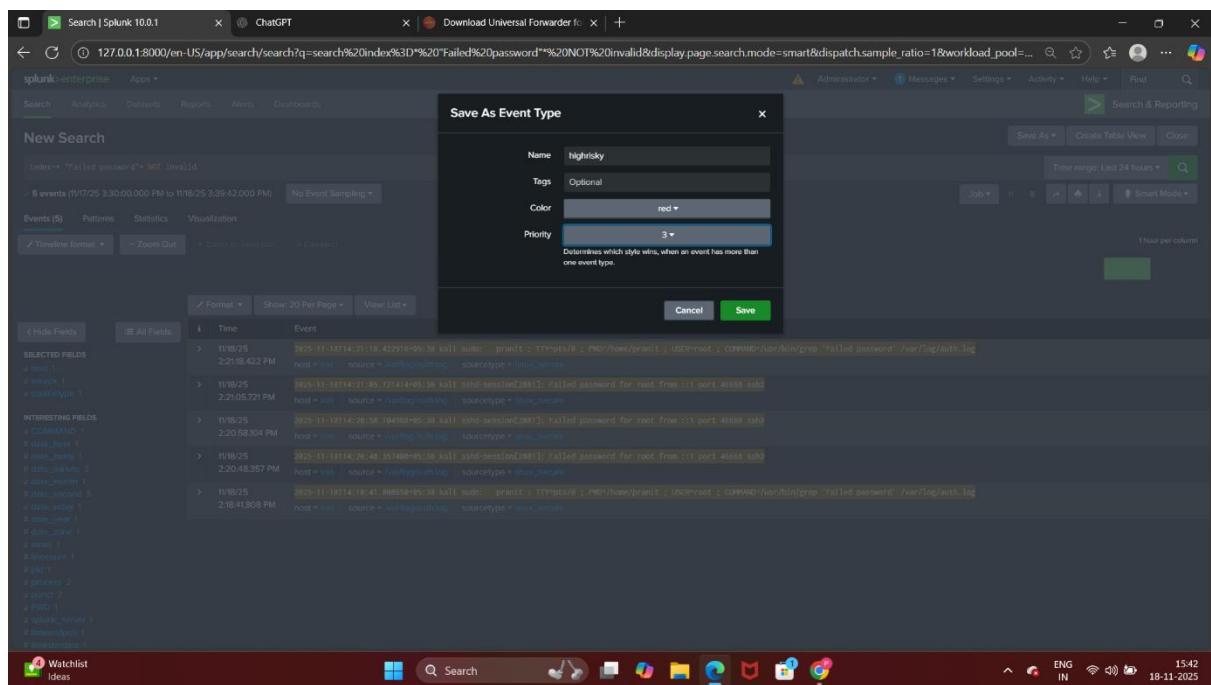


Figure 3: Configuring the High Risk Event Type.

2.4. Configuring "Less Risky" Event Types

Next, a filter was created to identify the noise generated by bots guessing random usernames.

Search Query:

`index=* "Failed password" * * for invalid user`

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Contains the query: `index=* "Failed password" * * for invalid user`.
- Results Panel:** Shows 9 events from 11/17/25 3:30:00.000 PM to 11/18/25 3:34:43.000 PM. The events list includes:
 - 2025-11-18T14:38:37.849883+05:30 [kali] sshd-session[2865]: Failed password for invalid user admin from ::1 port 39484 ssh2 host = kali | source = /var/log/auth.log sourcetype = linux_secure
 - 2025-11-18T14:39:25.890798+05:30 [kali] sshd-session[2865]: Failed password for invalid user admin from ::1 port 39484 ssh2 host = kali | source = /var/log/auth.log sourcetype = linux_secure
 - 2025-11-18T14:39:25.890800+05:30 [kali] sshd-session[2865]: Failed password for invalid user admin from ::1 port 39484 ssh2 host = kali | source = /var/log/auth.log sourcetype = linux_secure
 - 2025-11-18T14:39:25.890801+05:30 [kali] sshd-session[2865]: Failed password for invalid user admin from ::1 port 39484 ssh2 host = kali | source = /var/log/auth.log sourcetype = linux_secure
 - 2025-11-18T14:39:25.890802+05:30 [kali] sshd-session[2865]: Failed password for invalid user admin from ::1 port 39484 ssh2 host = kali | source = /var/log/auth.log sourcetype = linux_secure
 - 2025-11-18T14:39:25.890803+05:30 [kali] sshd-session[2865]: Failed password for invalid user admin from ::1 port 39484 ssh2 host = kali | source = /var/log/auth.log sourcetype = linux_secure
 - 2025-11-18T14:39:25.890804+05:30 [kali] sshd-session[2865]: Failed password for invalid user admin from ::1 port 39484 ssh2 host = kali | source = /var/log/auth.log sourcetype = linux_secure
 - 2025-11-18T14:39:25.890805+05:30 [kali] sshd-session[2865]: Failed password for invalid user admin from ::1 port 39484 ssh2 host = kali | source = /var/log/auth.log sourcetype = linux_secure
 - 2025-11-18T14:39:25.890806+05:30 [kali] sshd-session[2865]: Failed password for invalid user admin from ::1 port 39484 ssh2 host = kali | source = /var/log/auth.log sourcetype = linux_secure
- Bottom Status Bar:** Shows system status including battery level (-0.8%), network (ENG IN), and date (15:36 18-11-2025).

Figure 4: Filtering logs to show generic bot activity.

This search logic was saved as an Event Type named "lessrisky".

Priority: 8 (Low)

Color: Blue

Rationale: While these events are malicious, they are usually automated and less likely to succeed compared to targeted attacks.

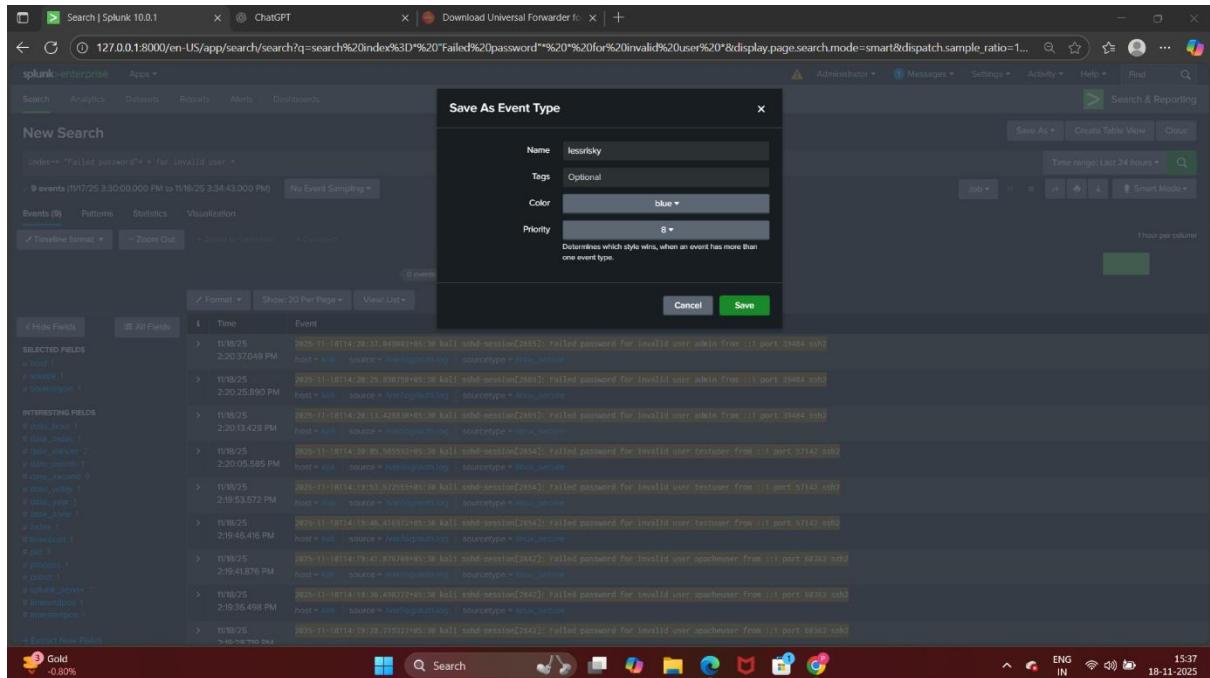


Figure 5: Configuring the Less Risky Event Type.

3.RESULTS AND VISUALIZATION

3.1. Enhanced Log Visibility

After applying the Event Types, the Splunk search interface now automatically tags and color-codes the incoming logs. This allows a security analyst to immediately spot critical alerts (Red) amidst the background noise (Blue).

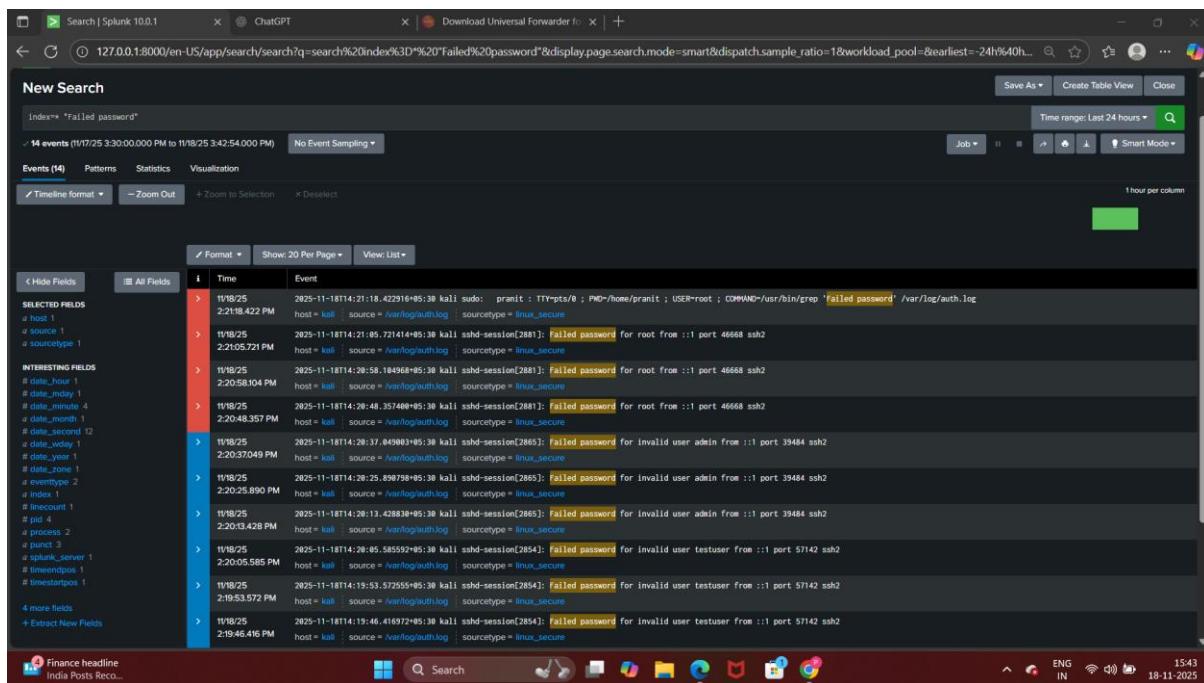


Figure 6: The final output showing color-coded events based on risk priority.

3.2. Statistical Analysis

A statistical chart was generated to compare the volume of high-risk events versus low-risk events. This visualization helps in understanding the nature of traffic hitting the server.

SPL for Visualization:

```
'index=*"Failed password" | stats count by eventtype'
```

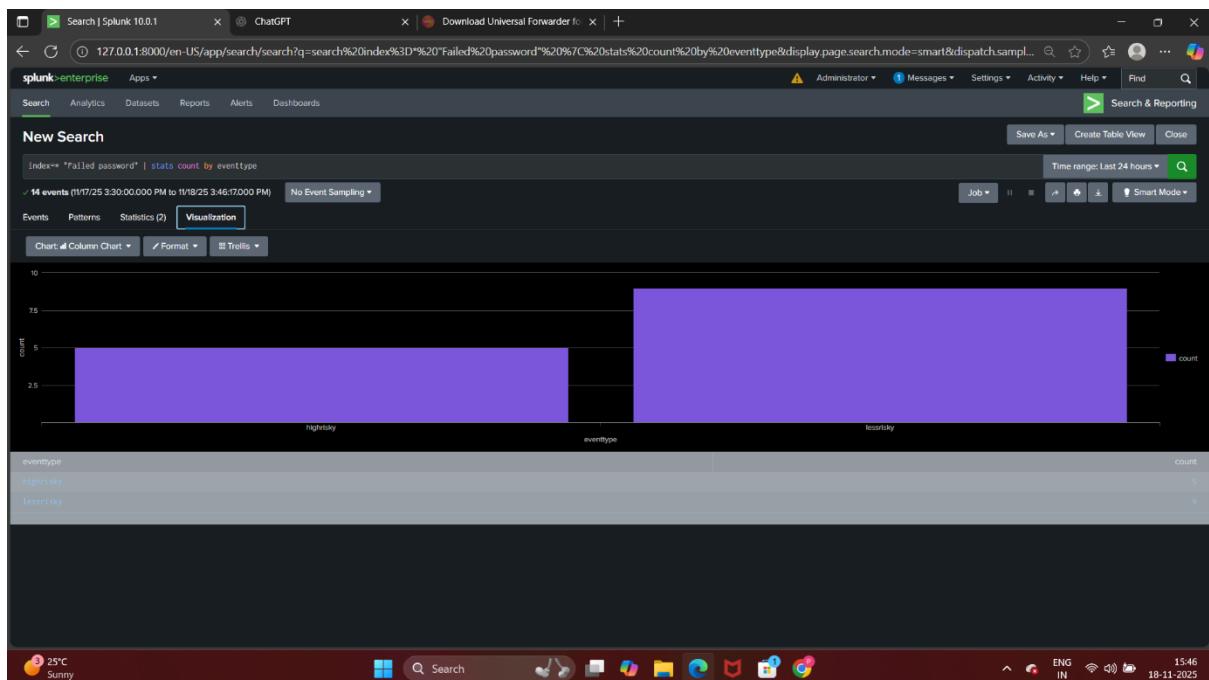


Figure 7: Bar chart comparing the count of High Risk vs. Less Risky events.

4.CONCLUSION

In this project, I successfully transformed raw text logs into actionable intelligence. By using Splunk's Event Types, I created a system that automatically prioritizes security incidents. This implementation demonstrates the critical role of a SIEM in reducing "alert fatigue" by visually distinguishing between generic automated scanning and targeted, high-severity intrusion attempts.