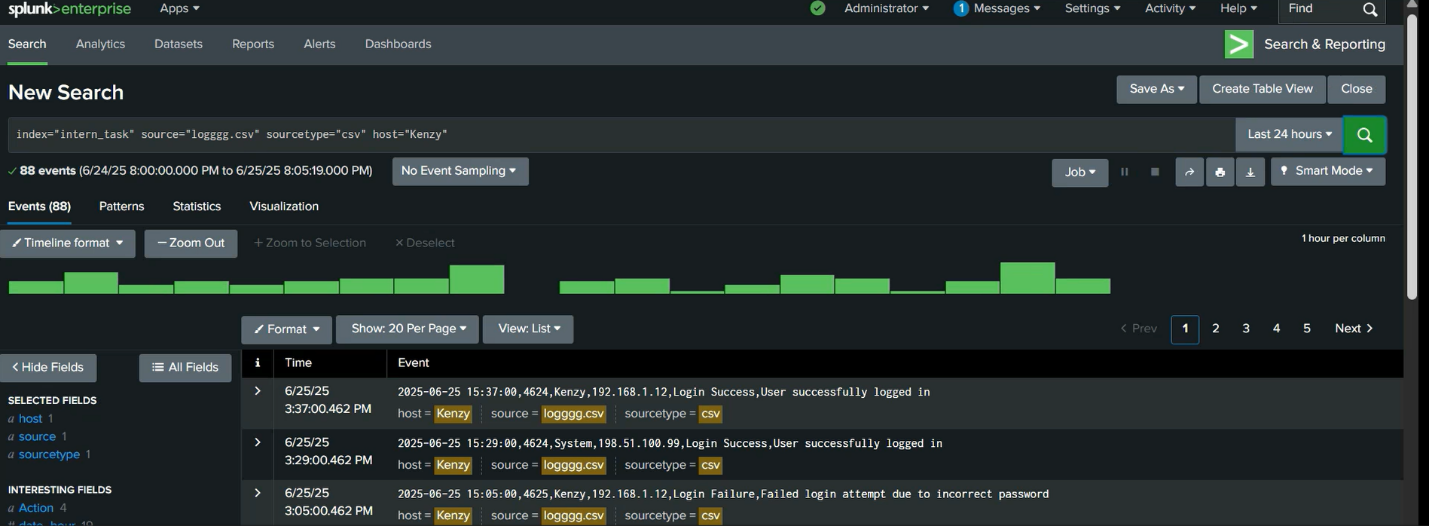
**SIEM Configuration Report**

**Preformed by Kenzy Hesham Ahmed**

**Tool used Splunk**

****

**Objective**:  
To configure a Security Information and Event Management (SIEM) system using **Splunk** for real-time monitoring, log analysis, and alerting.

**Installation & Setup**

* Downloaded and installed Splunk Enterprise.
* Created an admin account and logged in to the Splunk dashboard.
* Selected **“Add Data”** and uploaded system log files (loggg.csv).

**Log Analysis**

* Used **Search Processing Language (SPL)** to query logs.
  + Example: index=”intern\_task” sourcetype=”csv” EventCode=4625 | stats count by IP
* Performed searches to identify patterns such as:
  + **Failed logins by IP**

(index=”intern\_task” sourcetype=”csv” EventCode=4625 | stats count by IP)

* + **Failed logins by Usernames**

(index=”intern\_task” sourcetype=”csv” EventCode=4625 | stats count by Username)

* + **Log clear Events**

(index=”intern\_task” sourcetype=”csv” EventCode= 1102)

* + **Creation of new users**

(index=”intern\_task” sourcetype=”csv” EventCode=4720)

**Dashboard Creation**

* Created a custom dashboard titled **“intern\_task”**.
* Added panels with visualizations:
  + Bar Chart of failed logins.
  + Table of Log clear Events.
  + Table of Creation of new users

**Alert Configuration**

* Created a real-time alert to detect brute-force login attemps by monitoring EventCode 4625.

**Use Cases Addressed**

The SIEM setup in this project focused on detecting and monitoring several key security threats:

**Brute-force attacks:** Identified through multiple failed login attempts (EventCode 4625) from the same IP address.

**Suspicious IP activity:** Monitored connections and failures from unfamiliar or potentially malicious IPs.

**Log tampering:** Detected security log clearing attempts (EventCode 1102), which may indicate an attacker trying to hide evidence.

**Unauthorized account creation:** Tracked unexpected user creation events (EventCode 4720), which may signal privilege abuse.