Basic Splunk Security Monitoring Project

Prepared by: Mythresh Sai Mahadev

Masters in Cybersecurity Operations

Webster University

Project Overview

This project sets up a security monitoring environment using Splunk to simulate real-time alerting on failed login attempts and system errors. Sample syslog and auth.log files are used to demonstrate security monitoring capabilities, including custom field extraction, dashboard creation, and alert configuration.

Table of Contents

1. Introduction
2. Objectives
3. Step 1: Setting Up the Splunk Environment
4. Step 2: Data Ingestion
5. Step 3: Field Extraction
6. Step 4: Dashboard Creation
7. Step 5: Alert Configuration
8. Step 6: Testing and Troubleshooting
9. Conclusion

Introduction

In the field of cybersecurity, continuous monitoring is essential to detect potential threats and respond to incidents. This project leverages Splunk as a Security Information and Event Management (SIEM) tool to monitor log files, extract meaningful data, visualize events, and trigger alerts. By analyzing system logs, Splunk enables real-time detection of security events.

Objectives

- Set up a Splunk instance to manage and analyze log data.
- Extract key fields from logs for focused analysis.
- Create dashboards to monitor failed login attempts and system errors.
- Configure alerts for real-time notification of specific events.
- Simulate and validate alert functionality using sample data.

Step 1: Setting Up Your Splunk Environment

1.1 Install Splunk

1. **Download Splunk:**
   - Visit **Splunk's official website** and create an account if you haven't already.
   - Download the latest version of **Splunk Enterprise** for your operating system. Splunk offers a free trial version that should be suitable for this project.
2. **Install Splunk:**
   - **Linux:** Open a terminal and navigate to the folder where you downloaded the .deb package.

```bash
sudo dpkg -i splunk-package-name.deb
```

   - **Windows:** Run the installer and follow the on-screen instructions.
3. **Start Splunk:**
   - **Linux:**

```bash
cd /opt/splunk/bin
sudo ./splunk start
```

   - **Windows:** Open Splunk from the Start menu.
4. **Set Admin Credentials:**
   - On the first launch, Splunk will ask you to create an admin account. Set a secure username and password, as you'll use these credentials to log in.
5. **Log In:**
   - Open a browser and go to http://localhost:8000.
   - Log in with the credentials you set up.

1.2 Verify the Installation

- After logging in, you'll see the Splunk dashboard. This confirms that the installation was successful.

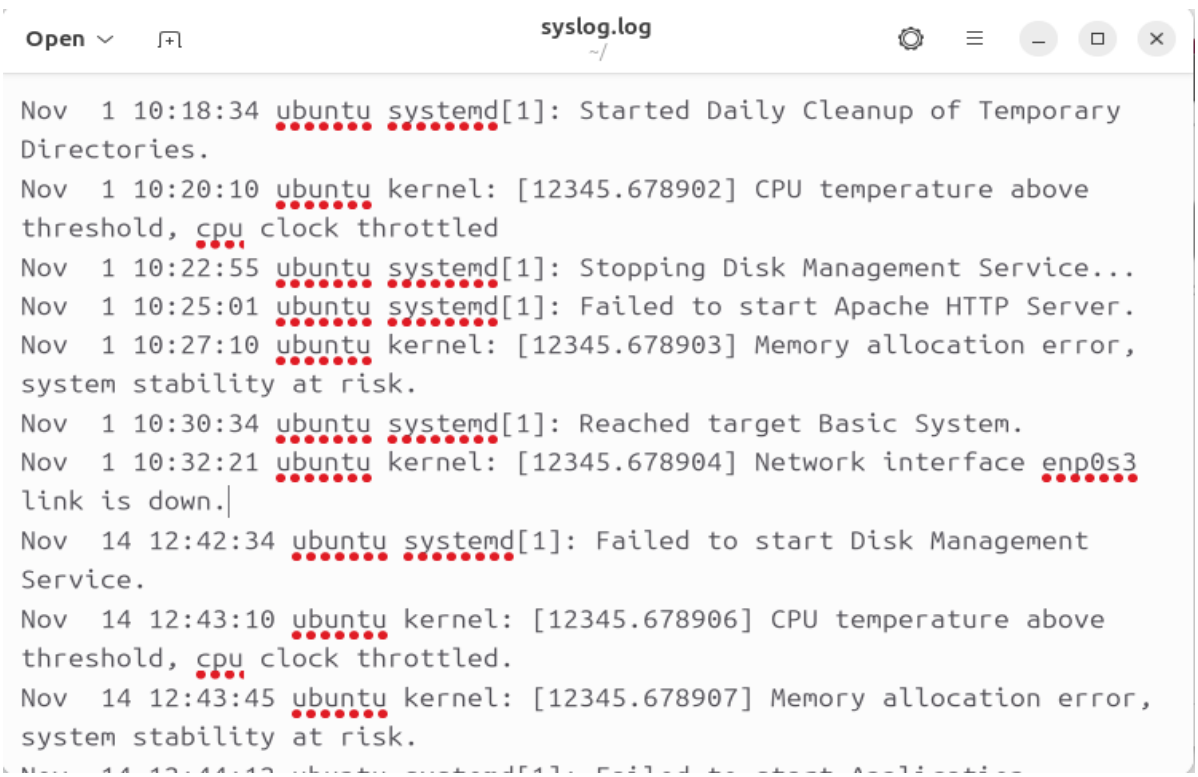
Step 2: Setting Up Data Inputs (Syslog and Auth.log Data)

For basic monitoring, we'll import sample logs to simulate login events and system errors.

2.1 Prepare Sample Data Files

1. Obtain Sample Logs:

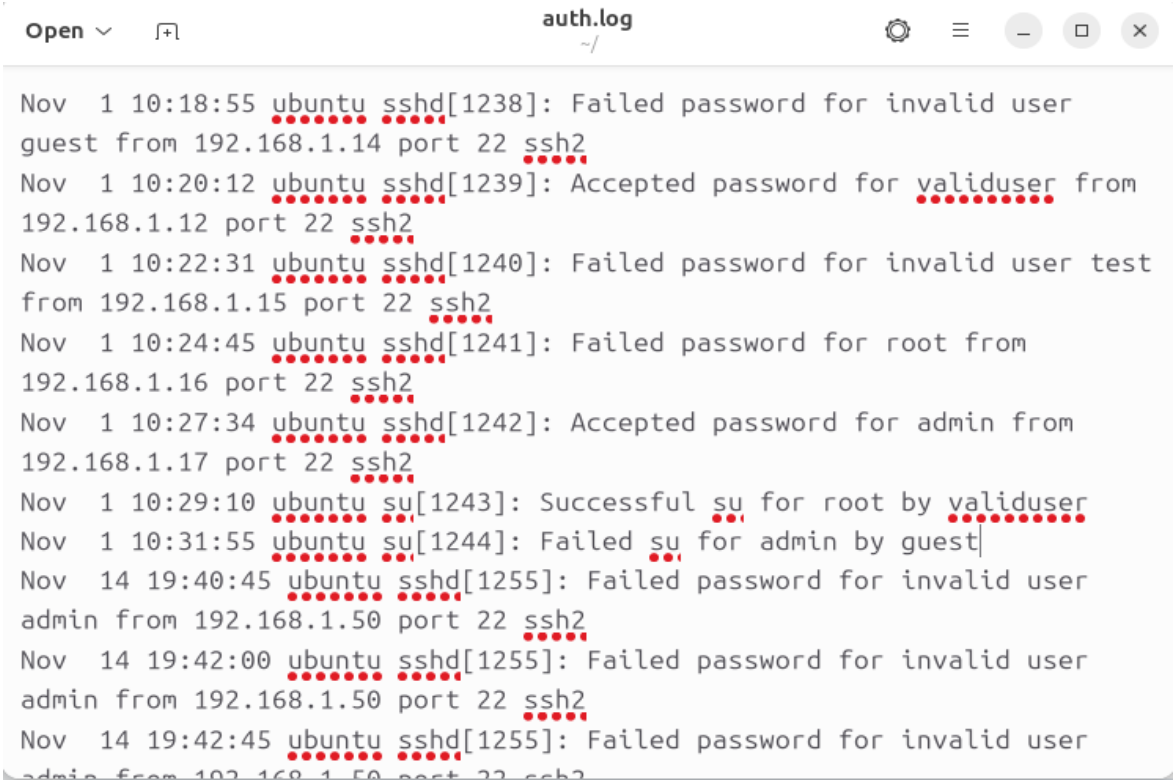
- For this project, we'll use two types of logs:
  - **Syslog:** To capture system events.
  - **Auth.log:** To track login attempts.
- You can either download sample syslog and auth.log files or generate them if you have access to logs on a Linux server or you can manually add the sample data as a text file.
- **Syslog file:** Sample log data



```
Open                    syslog.log
                        ~/

Nov  1 10:18:34 ubuntu systemd[1]: Started Daily Cleanup of Temporary
Directories.
Nov  1 10:20:10 ubuntu kernel: [12345.678902] CPU temperature above
threshold, cpu clock throttled
Nov  1 10:22:55 ubuntu systemd[1]: Stopping Disk Management Service...
Nov  1 10:25:01 ubuntu systemd[1]: Failed to start Apache HTTP Server.
Nov  1 10:27:10 ubuntu kernel: [12345.678903] Memory allocation error,
system stability at risk.
Nov  1 10:30:34 ubuntu systemd[1]: Reached target Basic System.
Nov  1 10:32:21 ubuntu kernel: [12345.678904] Network interface enp0s3
link is down.
Nov  14 12:42:34 ubuntu systemd[1]: Failed to start Disk Management
Service.
Nov  14 12:43:10 ubuntu kernel: [12345.678906] CPU temperature above
threshold, cpu clock throttled.
Nov  14 12:43:45 ubuntu kernel: [12345.678907] Memory allocation error,
system stability at risk.
```

- **Auth.log file:** Sample log data



2. Save and Organize Logs:

- Place these files in a location where Splunk can access them, for example, in a folder named **Sample_Logs**.

2.2 Importing Data into Splunk

1. **Go to Settings > Add Data** in Splunk.
2. Choose Upload and select the syslog and auth.log files you saved.

3. Set Source Type:

- Splunk might automatically detect the source type. If not:
  - Choose ‘syslog’ for the **syslog file**.
  - Choose ‘authlog’ for **auth.log file**.

4. Set Index:

- Create a new index named **security_monitoring** or use the default main index.

5. Click Next and Review your settings, then click **Submit**.

Step 3: Extracting Fields for Action and Severity

Field extraction is necessary to ensure that Splunk can recognize and categorize information like action (for login attempts) and severity (for system errors) within your data. Since Splunk doesn't automatically know these fields from your raw logs, you'll need to create custom field extractions.

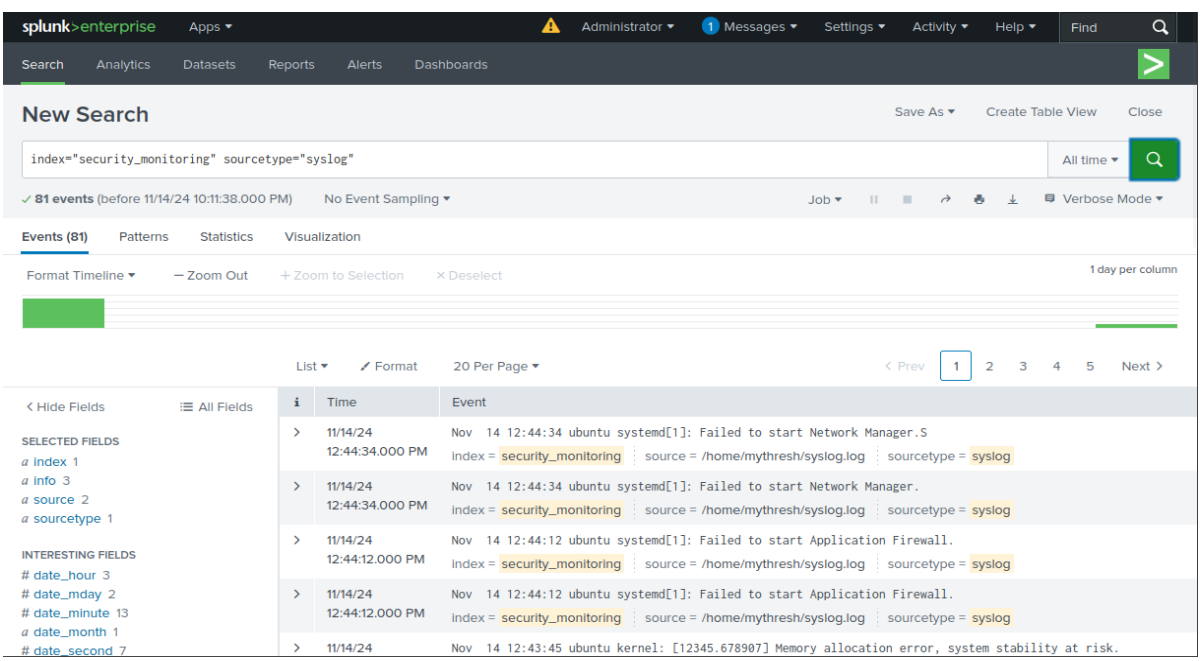
Here's how to extract fields like **action** and **severity**:

3.1 Field Extraction for action (Login Attempts)

1. **Navigate to Search:**
    - Go to Search in Splunk, and search within your authlog data to identify login attempts.
2. **Run a Query to View the Raw Data:**
    - Use the following query to view the raw authlog data:

```spl
index=security_monitoring sourcetype=authlog
```

- **Search** results using the above query:



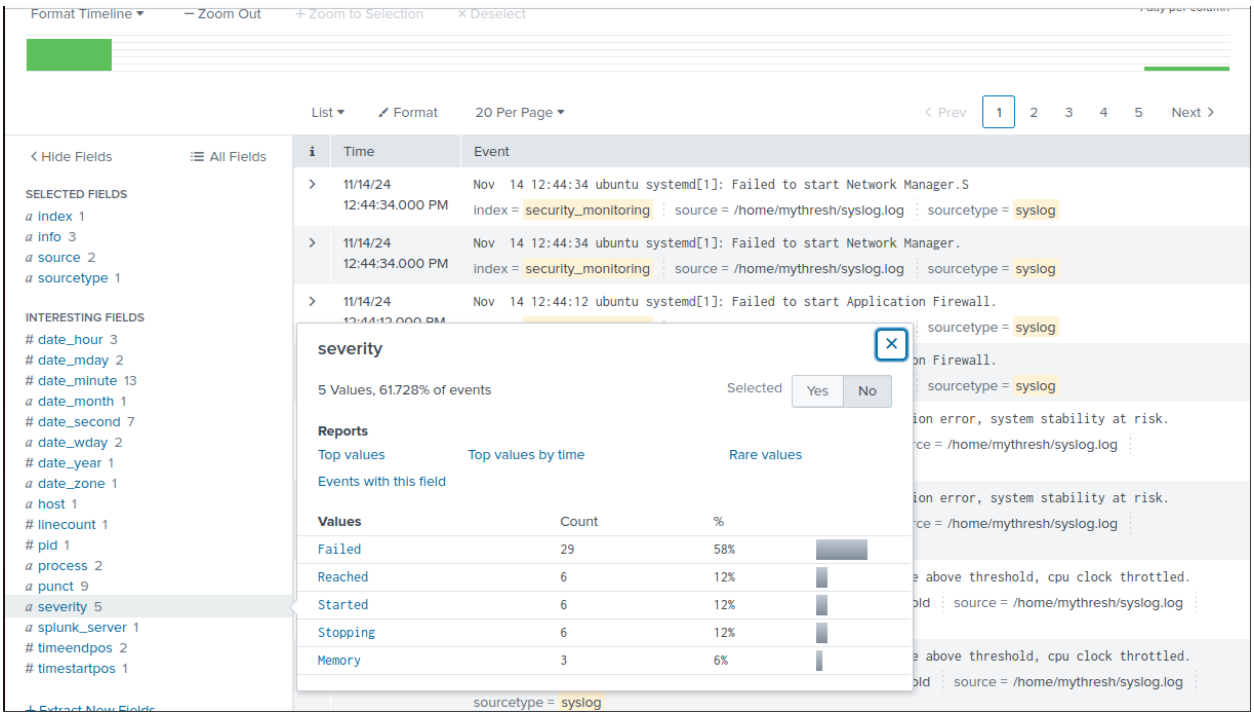
3. Extract the action Field:

- Identify patterns in the raw events, such as keywords like **“failed”** or **“success.”**
- Click on an event, and then on the **Event Actions** menu, select **Extract Fields**.
- Use **Interactive Field Extractor (IFX)**:
  - Highlight the part of the event that specifies the action (e.g., "failed" or "success").
  - Name this field **‘action’**.
  - Splunk will suggest a regular expression; test and refine it to ensure it accurately captures both success and failure.

4. Save the Extraction:

- Test the extraction with various events to confirm accuracy, then save it.

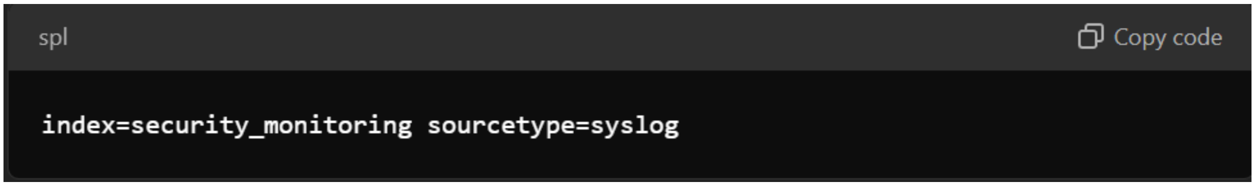
5. After the Extraction:



3.2 Field Extraction for severity (System Errors)

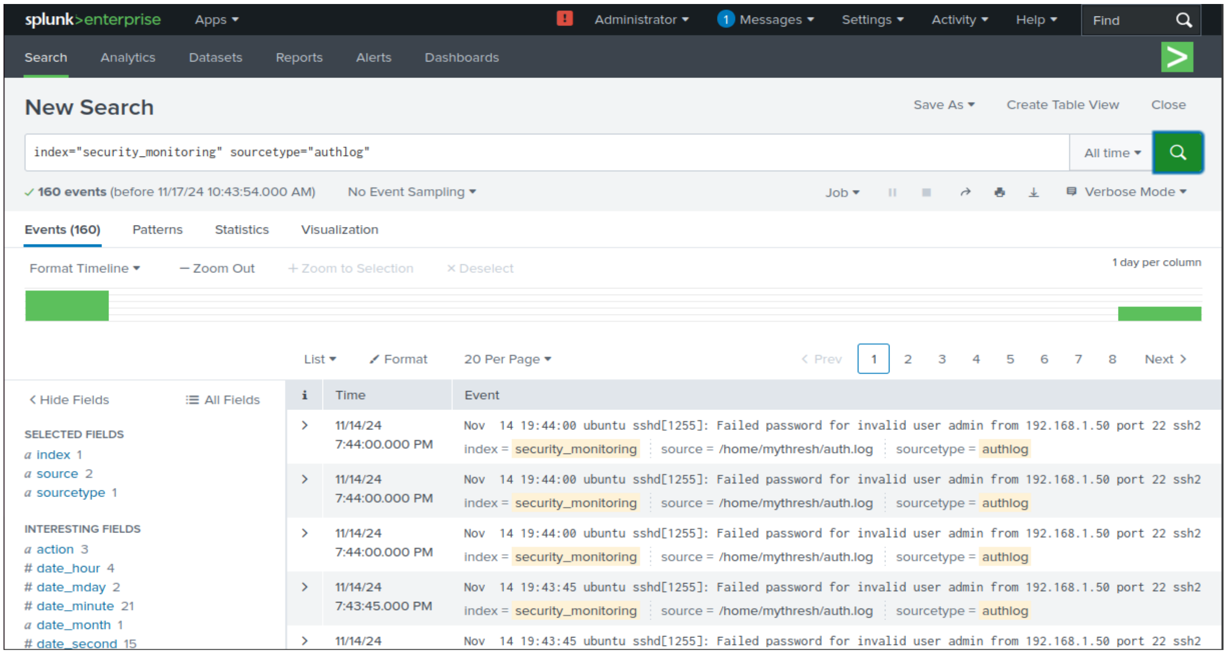
1. Search within Syslog Data:

- Use this query to search your syslog data



```spl
index=security_monitoring sourcetype=syslog
```

- **Search** results using the above query:



```
index="security_monitoring" sourcetype="authlog"
```

✓ 160 events (before 11/17/24 10:43:54.000 AM)

SELECTED FIELDS
a index 1
a source 2
a sourcetype 1

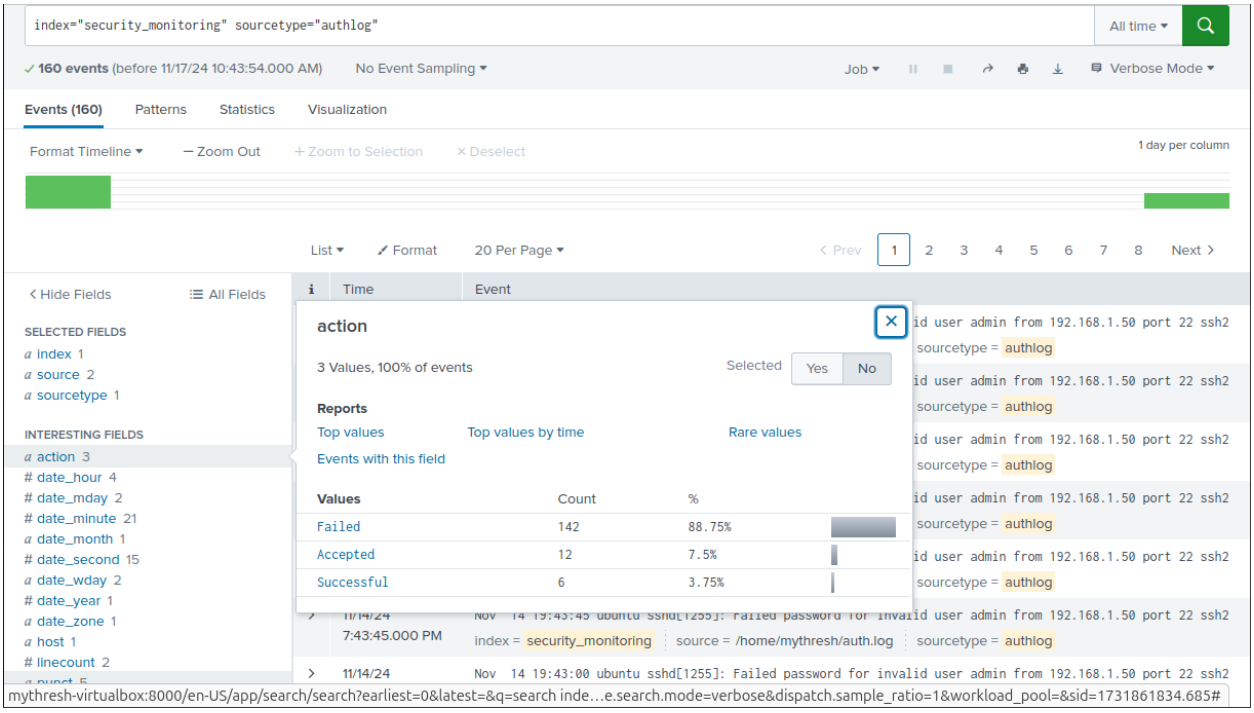
INTERESTING FIELDS
a action 3
date_hour 4
date_mday 2
date_minute 21
a date_month 1
date_second 15

i	Time	Event
>	11/14/24 7:44:00.000 PM	`Nov  14 19:44:00 ubuntu sshd[1255]: Failed password for invalid user admin from 192.168.1.50 port 22 ssh2` index = security_monitoring source = /home/mythresh/auth.log sourcetype = authlog
>	11/14/24 7:44:00.000 PM	`Nov  14 19:44:00 ubuntu sshd[1255]: Failed password for invalid user admin from 192.168.1.50 port 22 ssh2` index = security_monitoring source = /home/mythresh/auth.log sourcetype = authlog
>	11/14/24 7:44:00.000 PM	`Nov  14 19:44:00 ubuntu sshd[1255]: Failed password for invalid user admin from 192.168.1.50 port 22 ssh2` index = security_monitoring source = /home/mythresh/auth.log sourcetype = authlog
>	11/14/24 7:43:45.000 PM	`Nov  14 19:43:45 ubuntu sshd[1255]: Failed password for invalid user admin from 192.168.1.50 port 22 ssh2` index = security_monitoring source = /home/mythresh/auth.log sourcetype = authlog
>	11/14/24	`Nov  14 19:43:45 ubuntu sshd[1255]: Failed password for invalid user admin from 192.168.1.50 port 22 ssh2`

2. Extract the severity Field:

- Look for keywords that indicate severity levels, such as **“error,” “warning,” or “info.”**
- Use the same **Extract Fields** tool to isolate the severity information.
- Name this field severity and ensure the regular expression captures all relevant severity levels.

3. **After the Extraction:**



4. **Test and Save**:
   - Test the extraction with various events to confirm accuracy, then save it.

Step 4: Creating Basic Dashboards for Monitoring

We'll set up a simple dashboard to visualize login events and system errors. This will help in identifying patterns or issues immediately.

4.1 Create a New Dashboard

1. **Navigate to Dashboards**:
   - In Splunk's main menu, go to **Dashboards** and click **Create New Dashboard**.
2. **Name Your Dashboard**:
   - Set a name, such as "Security Monitoring Dashboard."
   - Choose a suitable app (e.g., Search & Reporting) and the **Shared in App** permission for now.
3. **Select Dashboard Studio**:
   - For more flexibility, select **Classic Dashboard Studio**..

4.2 Add Panels to Display Key Metrics

Let's add panels to show:

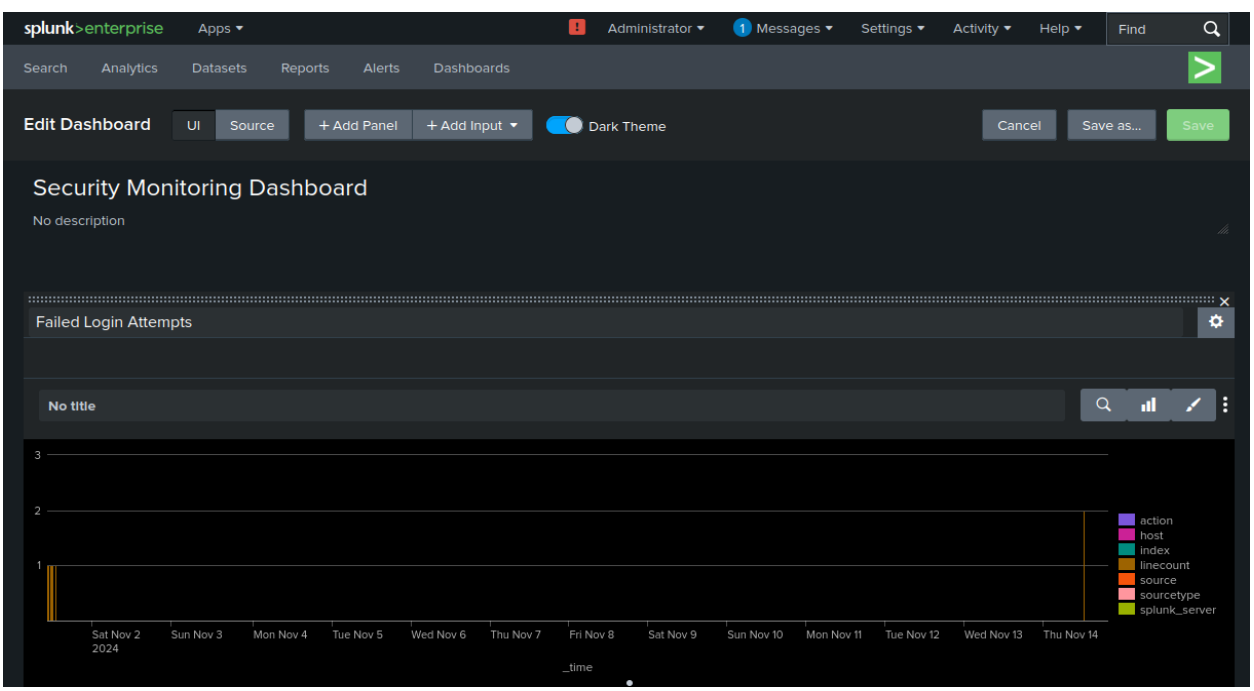
- **Failed Login Attempts**
- **Successful Login Attempts**
- **System Errors**

Panel 1: Failed Login Attempts

1. Click on **Add New Panel** in the dashboard editor.
2. **Search Query**:
    - Use this query to capture failed login attempts

```spl
index=security_monitoring sourcetype=authlog action="failed"
```

3. **Visualization**:
    - Choose a **Column Chart** or **Table** visualization to show recent failed login attempts.
4. **Configure Panel Settings**:
    - Title: "Failed Login Attempts"
    - Adjust any visualization settings as desired.

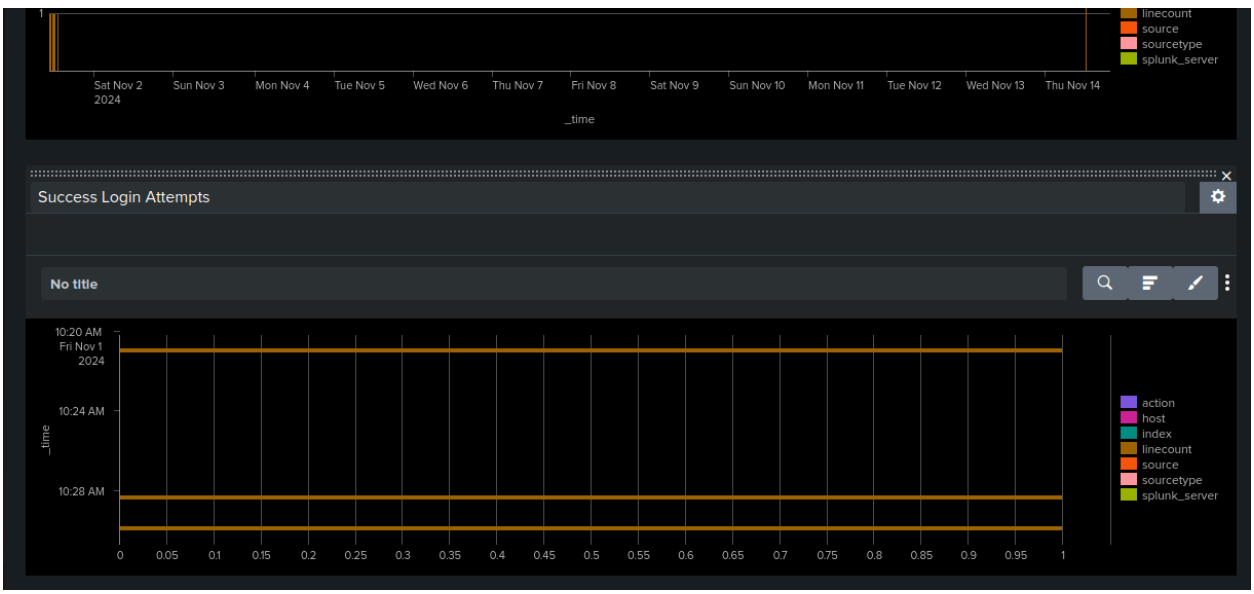


Panel 2: Successful Login Attempts

1. Add another panel and enter the following query to capture successful logins:

```spl
index=security_monitoring sourcetype=authlog action="Accepted"
```

2. **Visualization**:
   - Choose a **Bar Chart** or **Table** visualization to show recent failed login attempts.
3. **Configure Panel Settings**:
   - Title: "Failed Login Attempts"
   - Adjust any visualization settings as desired.

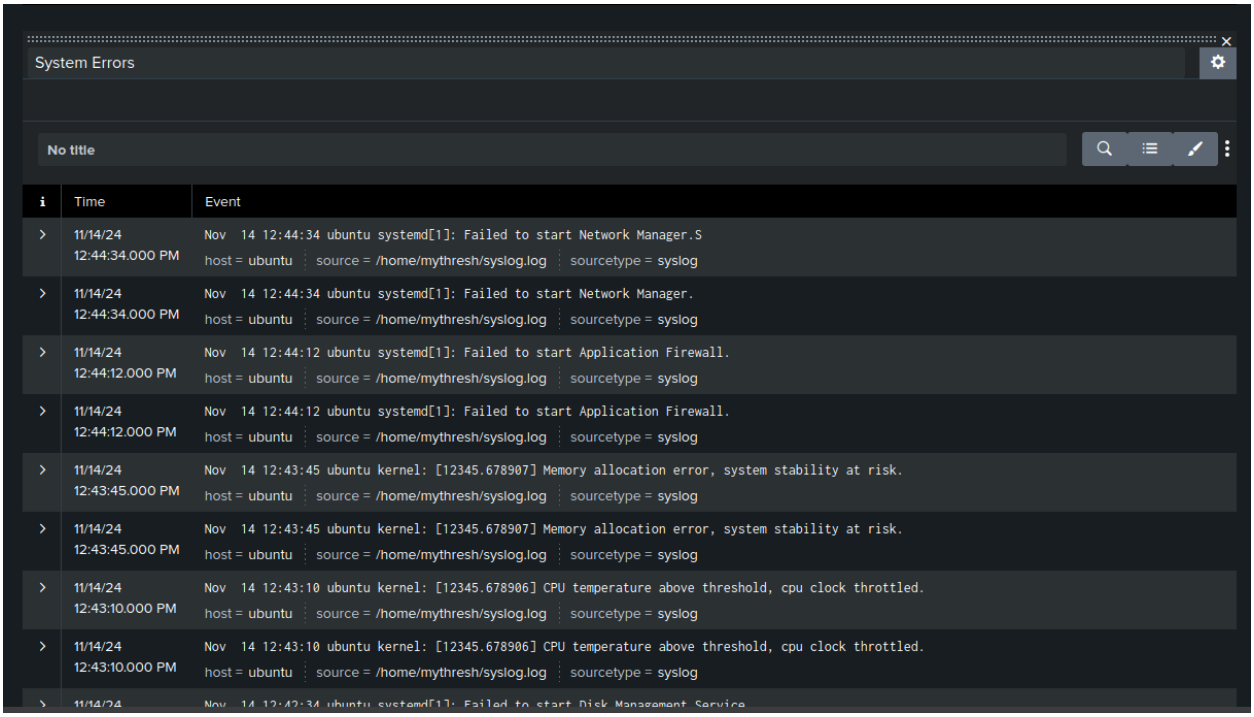


Panel 3: System Errors

1. For system errors, add a new panel and use this query:

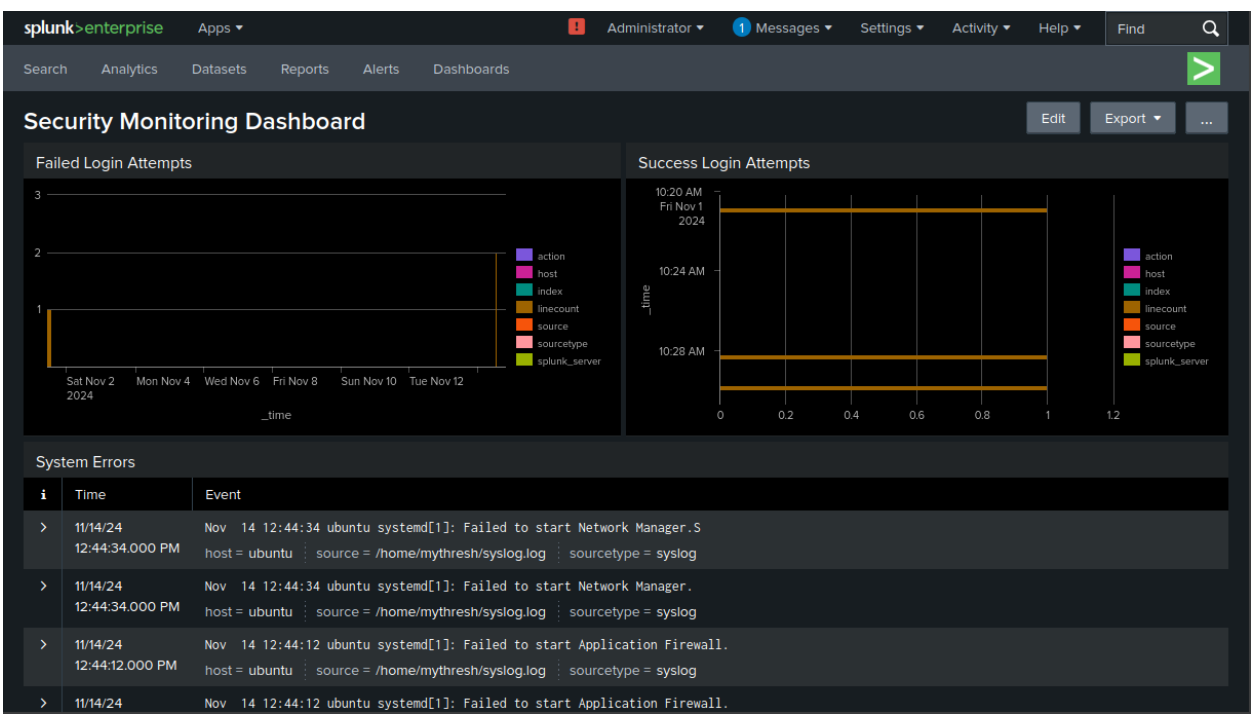
```spl
index=security_monitoring sourcetype=syslog (severity="*" OR info="*")
```

2. **Visualization**:
   - You can use a **Line Chart** or **Table** to see error trends over time.
3. **Title**: Set this panel's title to "System Errors."



4. **Save the Dashboard**:

- Once you've added all panels, click **Save**.



Step 5: Setting Up Alerts for Security Monitoring

Alerts will notify you of significant events, such as multiple failed login attempts and system errors. We'll configure basic alerts for common security monitoring scenarios.

5.1 Create a New Index for Alerts

1. **Navigate to Settings > Indexes**:
    - Go to the main Splunk dashboard, then **Settings** > **Indexes**.
2. **Create a New Index**:
    - Click on **New Index** and name it something like alert_logs.
    - Set any necessary retention policies (optional) based on how long you want to keep the alert data.
3. **Save the Index**:
    - Click **Save** to finalize your new index.

5.2 Configure an Alert for Multiple Failed Login Attempts

1. **Create a Search for Failed Logins**:
    - Go to **Search & Reporting** and use the following query to find failed login attempts.

```spl
index=security_monitoring sourcetype=authlog action="failed"
```

    - This query isolates all failed login attempts in your authlog data.
2. **Set Conditions for the Alert**:
    - Click on **Save As** in the upper right corner and choose **Alert**.
    - **Alert Title**: Name it "Multiple Failed Login Attempts."
    - **Alert Type**: Select **Scheduled** if you want it to check periodically, or **Real-time** for instant detection.
    - **Trigger Conditions**:
        - Set the condition to trigger when there are, for example, **3 or more failed login attempts within 5 minutes**.

3. **Configure Alert Actions**:
   - In the **Alert Actions** section, choose **Log Event**.
   - **Event box: "`Alert triggered for multiple login attempts in 5 minutes`".**
   - **Destination Index**: Specify the `alert_logs` index. This index is where all triggered alert events will be stored.

4. **Save the Alert**.

5.3 Configure an Alert for System Errors

1. **Create a Search for System Errors**:

   - Use this search to capture error-level system logs:

```spl
index=security_monitoring sourcetype=syslog (severity="*" OR info="*")
```

   - This will isolate any events labeled as errors in the syslog data.

2. **Set Conditions for the Alert**:

   - Click on **Save As** in the upper right corner and choose **Alert**.
   - **Alert Title**: Name it "Multiple Failed Login Attempts."
   - **Alert Type**: Select **Scheduled** if you want it to check periodically, or **Real-time** for instant detection.
   - **Trigger Conditions**:
     - Set the condition to trigger when there are, for example, **3 or more failed login attempts within 5 minutes**.

3. **Configure Alert Actions**:
   - In the **Alert Actions** section, choose **Log Event**.
   - **Event box: "`Alert triggered for System errors`"**
   - **Destination Index**: Specify the `alert_logs` index. This index is where all triggered alert events will be stored.

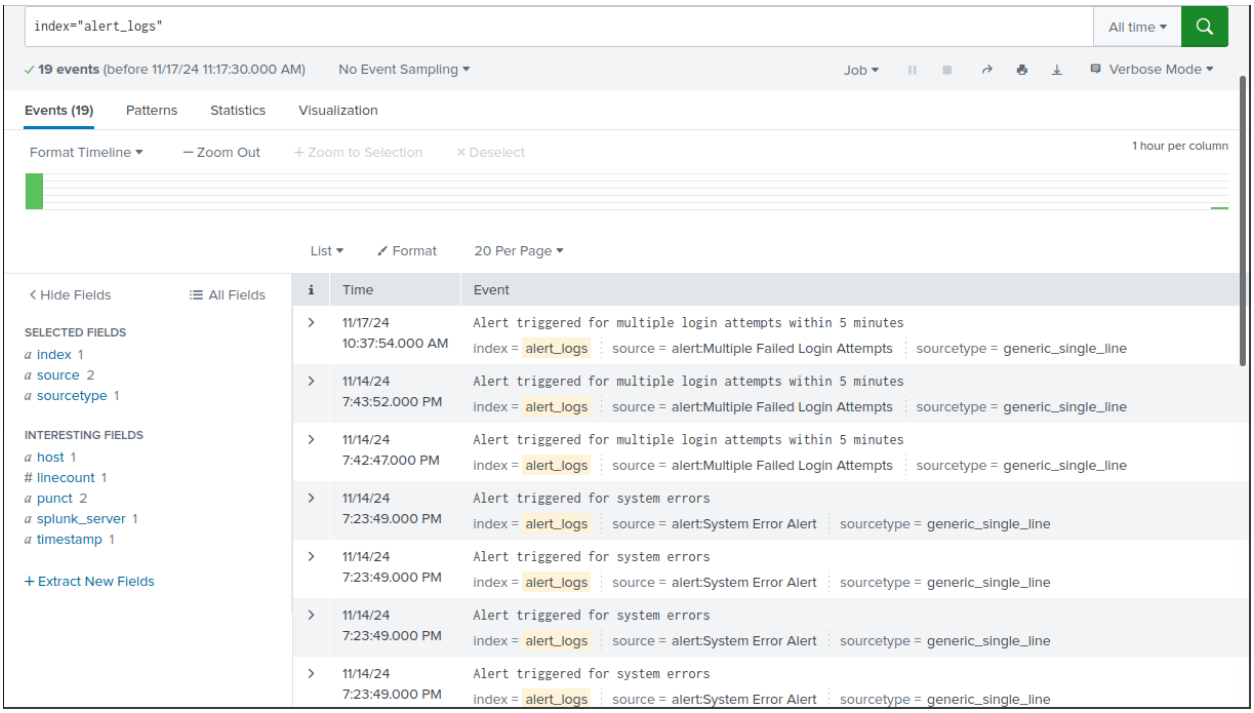
4. **Save the Alert**.

Step 6: Reviewing Alerts

Once saved, these configurations allow you to view your alert events in the **`alert_logs`** index using:

```spl
index=alert_logs
```

Here the **Search** results using the above query:



Conclusion

This project successfully demonstrates the setup of a basic security monitoring environment using Splunk, showcasing its capabilities as a powerful Security Information and Event Management (SIEM) tool. By leveraging sample syslog and auth.log files, we implemented critical SIEM features, including data ingestion, field extraction, dashboard creation, and alert configuration.

Through the simulation of real-world security scenarios such as failed login attempts and system errors, this project highlights the importance of continuous monitoring and rapid detection in maintaining a secure IT infrastructure. The ability to extract actionable insights from raw log data is critical for identifying potential threats, mitigating risks, and enhancing the overall security posture of an organization.