# Cyber Threat Analysis Dashboard using Splunk

A Cybersecurity Log Visualization Project

**Author:** Urvashi Sharma

**Tool:** Splunk Enterprise (Cloud)

**Date:** October 2025

## 1. Project Overview

This project focuses on analyzing Windows Event Logs and IoT-based network data using Splunk to identify event types, trends, and geolocation patterns. The goal is to demonstrate practical cybersecurity log analysis skills through dashboard creation and visualization.

**Key Objectives:**

- To visualize system event logs using Splunk Dashboards.
- To identify error and warning trends in real-time.
- To analyze event origin using geographic mapping.
- To correlate system and IoT activity logs for anomaly detection.

## 2. Dataset Description

- **Dataset 1:** RT_IOT2022.csv
  - Contains IoT-related connection data such as:
  - Protocols (TCP, UDP, ICMP)
  - Source and destination ports
  - Services (DNS, HTTP, MQTT, DHCP, etc.)
- **Dataset 2:** eventlog.csv
  - Contains Windows event log data including: MachineName, Category, EntryType (Error, Warning, Information), Source, Message, TimeGenerated
  - Geo fields: country, regionName, city, timezone, isp

## 3. Methodology

1. **Data Import: I**mported sample Windows Event logs into Splunk using the "Add Data" feature.
2. **Log Parsing:** Ensured timestamps, hostnames, and event codes were properly indexed.
3. **Query Development (SPL):** Developed SPL queries for each metric like attack frequency, severity levels, port analysis, etc. (Sample commands shown below).
4. **Dashboard Creation:** Added visual panels such as bar charts, line charts, and maps to visualize attack trends and network insights.
5. **Insight Extraction:** Interpreted each visualization to identify threat patterns and anomalies.
6. **Layout Design:** Exported and neatly aligned the dashboard visuals for presentation.

## Sample SPL Commands (for reference):

- To visualize different type of attack frequency

```
index=main source="RT_IOT2022.csv"
| stats count by Attack_type
| where Attack_type!=""
| sort - count
```

Time range: All time

- To identify and visualize the Top destination ports for attacking a system

```
index=main source="RT_IOT2022.csv"
| stats count by id_resp_p
| sort -count
| head 10
```

Time range: All time

- To identify the most popular time period of attacks

```
index=main source="RT_IOT2022.csv"
| eval event_time=_indextime
| timechart span=45h count by Attack_type
```

Time range: All time

- To identify the different types of activities carried out

```
index=main source="eventlog.csv"
| stats count by Category
| sort -count
```

Time range: All time

## 4. Visualization Description

| Visualization | Description |
|---|---|
| **1. Attack Frequency Analysis** | Displays the distribution of different attack types captured from IoT logs to identify the most recurring threats. |
| **2. Attack Frequency Trend** | Shows how attack occurrences vary over time, highlighting peak periods of potential intrusion attempts. |
| **3. Windows Log Severity Distribution** | Pie chart representing proportions of *Information*, *Warning*, and *Error* events in the system logs. |
| **4. Windows Event Frequency Over Time** | Time-based visualization showing fluctuations in log generation to detect unusual activity spikes. |
| **5. Global Distribution of Log Events** | Geolocation map highlighting where events were generated, indicating possible regions of concern. |
| **6. Top Network Services Observed** | Visualizes the frequency of protocols/services (e.g., DNS, MQTT, HTTP) to understand active communication channels. |
| **7. Top 10 Destination Ports** | Bar chart showing the most commonly targeted destination ports, useful for identifying suspicious traffic patterns. |
| **8. Top Windows Log Categories** | Highlights which system components or categories produce the most log activity, aiding in source-based analysis. |

## 5. Insights & Observations

- **IoT Threats:** Analysis revealed that TCP was the dominant protocol, indicating its central role in data exchange among IoT devices. Most attacks targeted MQTT and DNS services — a sign of protocol exploitation or device misconfiguration.
- **Attack Frequency Trend:** The time-series chart showed periodic spikes in attack frequency, possibly aligning with scheduled network scans or automated bot activity. This insight could support incident response planning and threat hunting strategies.

- **Windows Event Severity:** A majority of system events were Information-level**,** but notable clusters of Warning and Error logs indicated system instability and potential configuration issues.
- **Event Frequency Pattern:** The event frequency timechart highlighted bursts of log generation at irregular intervals — which could correspond to patch installations, failed logons, or service restarts.
- **Geolocation Data:** Event origins were traced primarily to two cities, suggesting limited test environments or controlled deployment setups. These findings are valuable for geo-based access validation and location-based security monitoring**.**
- **Network Service and Port Activity:** The Top Services and Ports charts revealed active MQTT communication over standard and non-standard ports. Frequent targeting of specific destination ports indicates the need for tighter firewall rule auditing**.**
- **Overall Threat Insight:** The combined dashboard provides both macro (IoT) and micro (Windows system) visibility into network and device-level events. This demonstrates how Splunk can be leveraged as a SIEM tool to correlate and monitor diverse security data sources effectively.

## 6. Skills Demonstrated

- Log Data Analysis
- Splunk SPL Querying
- Cybersecurity Monitoring
- Dashboard Design & Visualization
- Incident Trend Identification

## 7. Tools & Technologies

| Category | Tools |
|---|---|
| Log Analysis | Splunk Enterprise |
| Data Format | CSV (IoT and Event Logs) |
| Visualization | Pie Chart, Bar Chart, Timechart, Cluster Map |
| Data Fields | EntryType, Source, city, proto, service |

## 8. Conclusion

This project successfully showcases the use of Splunk for practical cybersecurity analytics. Through visualization and log correlation, it provides insights into event types, source activities, and geolocation of system events.

The dashboard serves as a foundational model for **SIEM-based threat monitoring** and **log anomaly detection** in enterprise environments.

## 9. References


- Splunk Docs: https://docs.splunk.com/Documentation/Splunk
- Dataset: *RT_IOT2022.csv* and *eventlog.csv* (Publicly available cybersecurity log data from Kaggle)