# **Introduction to SIEM**

**SOC Learning Report – Introduction to SIEM**

**Analyst:** Inam Qadeer  
**Tool(s) Used:** SIEM Platform (TryHackMe Lab), Splunk

**1. Executive Summary**

The *Introduction to SIEM* lab explains the fundamentals of Security Information and Event Management systems, covering how they collect, index, and search logs to detect security events.  
It also introduces the core features common to most SIEM platforms, such as search queries, filtering, timelines, and dashboards.  
The focus is on building basic and advanced queries to find relevant events in a dataset.

**2. Investigation / Learning Steps**

1. Learned the **purpose of SIEM** in centralizing log data from multiple sources for security monitoring.
2. Understood **log ingestion** — how data flows from endpoints/network devices into the SIEM.
3. Explored **search queries** to filter events based on conditions.
4. Practiced using **time filters** to narrow searches to specific periods.
5. Identified **anomalies** by spotting deviations in logs.
6. Learned how **dashboards** and **visualizations** can be used for faster triage.

**3. Findings**

* SIEMs are essential for correlating data from multiple sources to detect complex attacks.
* Search syntax allows analysts to pinpoint specific events such as failed logins or suspicious IP activity.
* Time-based filtering is critical when investigating incidents with a known timeframe.
* Dashboards provide a high-level overview but require query skills for deeper analysis.

