Security Alert Monitoring & Incident Response

Internship Project - Cybersecurity | Future Interns

Intern: Yatin Annam

1. Introduction

In the evolving landscape of cybersecurity, Security Information and Event Management (SIEM) tools are indispensable in identifying, monitoring, and responding to security threats. This report details the monitoring of simulated security alerts using **Splunk Enterprise**, one of the industry-standard SIEM solutions.

The task involved uploading and analysing sample log files, identifying potential suspicious activities, classifying incidents, and documenting the findings along with remediation steps.

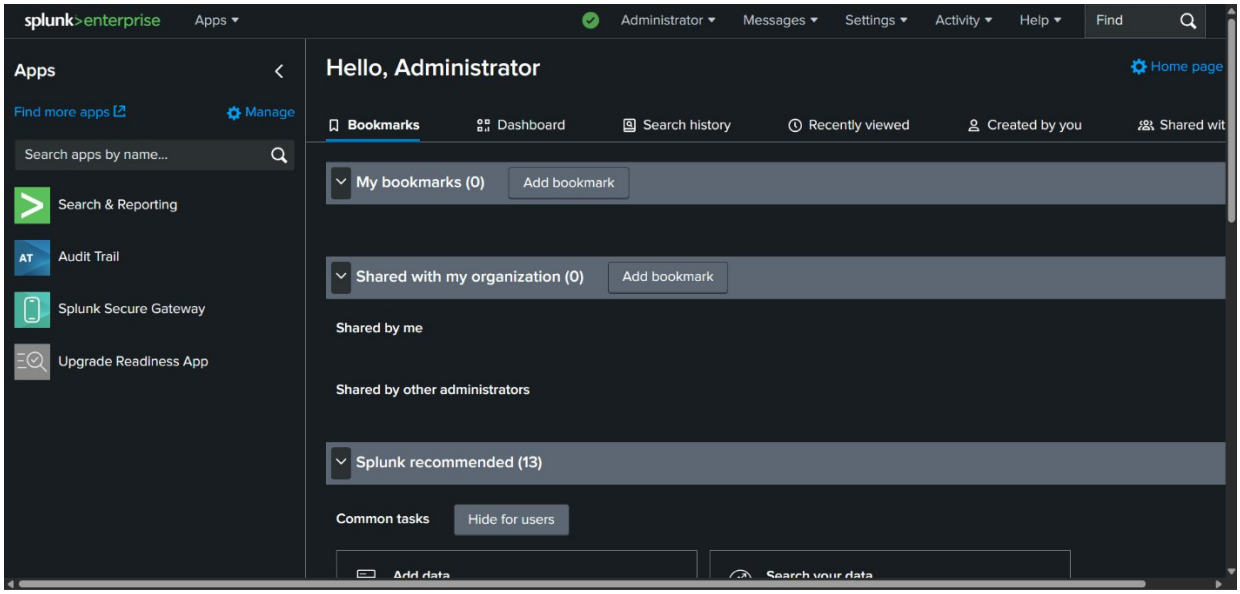
2. Tools & Environment Setup

2.1 System Details

- **Operating System:** Windows 10
- **Tool Used:** Splunk Enterprise (Free Trial)
- **Browser:** Google Chrome
- **Log Type:** Simulated Web Access Logs (Buttercup Games sample logs)

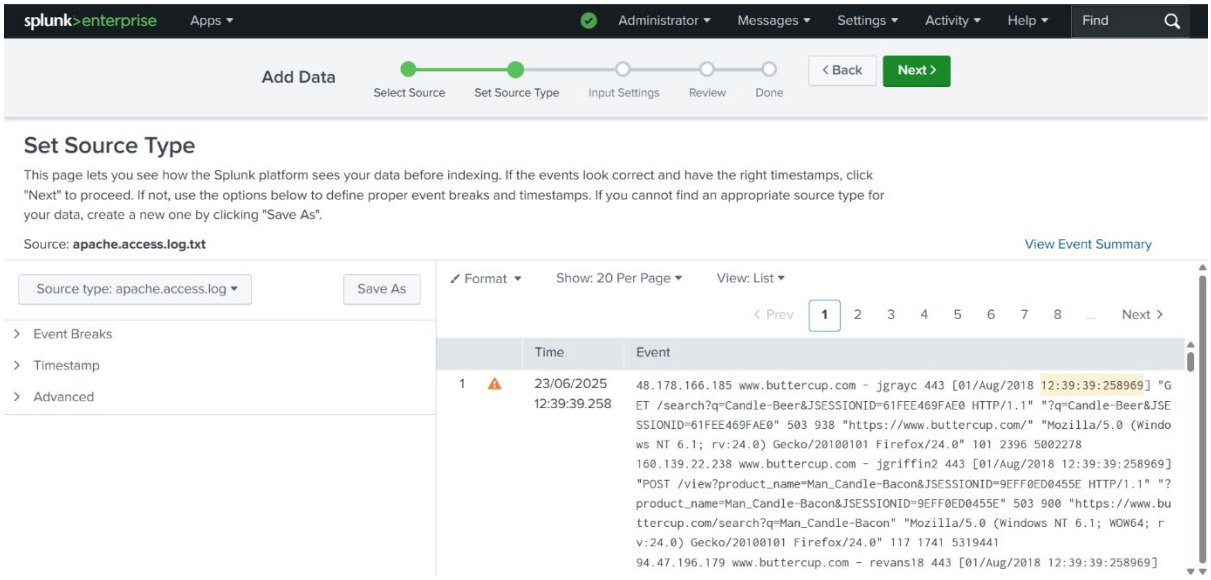
2.2 Installation Steps

1. Downloaded Splunk from splunk.com.
2. Installed and accessed Splunk via http://127.0.0.1:8000.
3. Set up login credentials and accessed the main dashboard.



3. Uploading Log Files

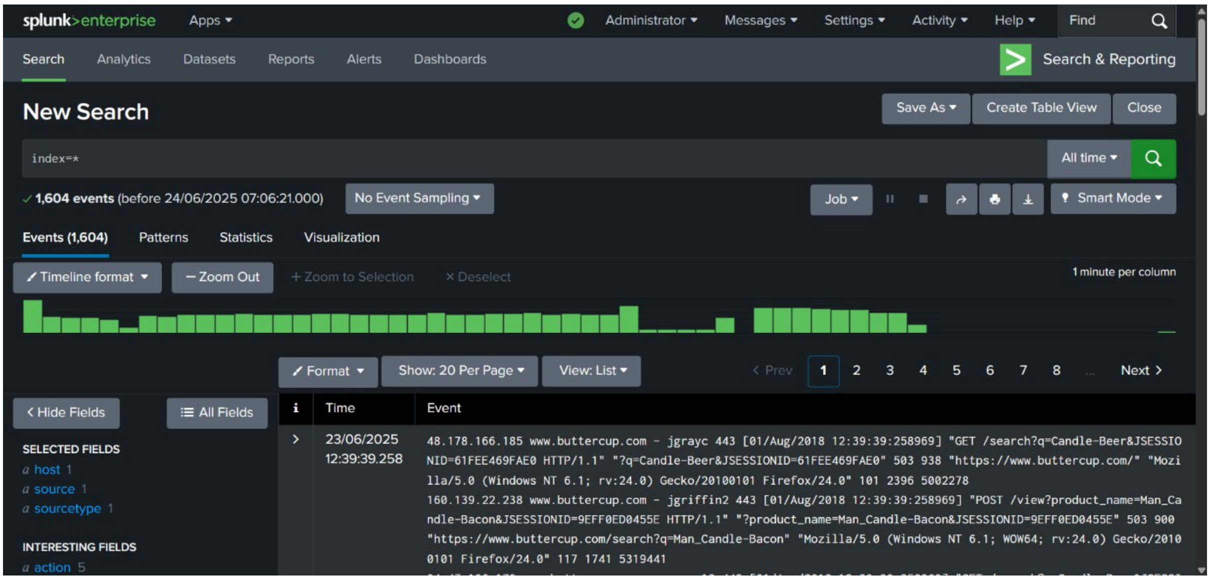
Using the “Add Data” feature in Splunk, a sample .log file was uploaded to simulate real-time event monitoring. This file contained web access events from a fictional e-commerce website.



4. Search & Analysis of Logs

4.1 Initial Broad Search

The command index=* was used to fetch all available events. Over **1600 events** were indexed, indicating successful data ingestion.



4.2 Field-Based Table View

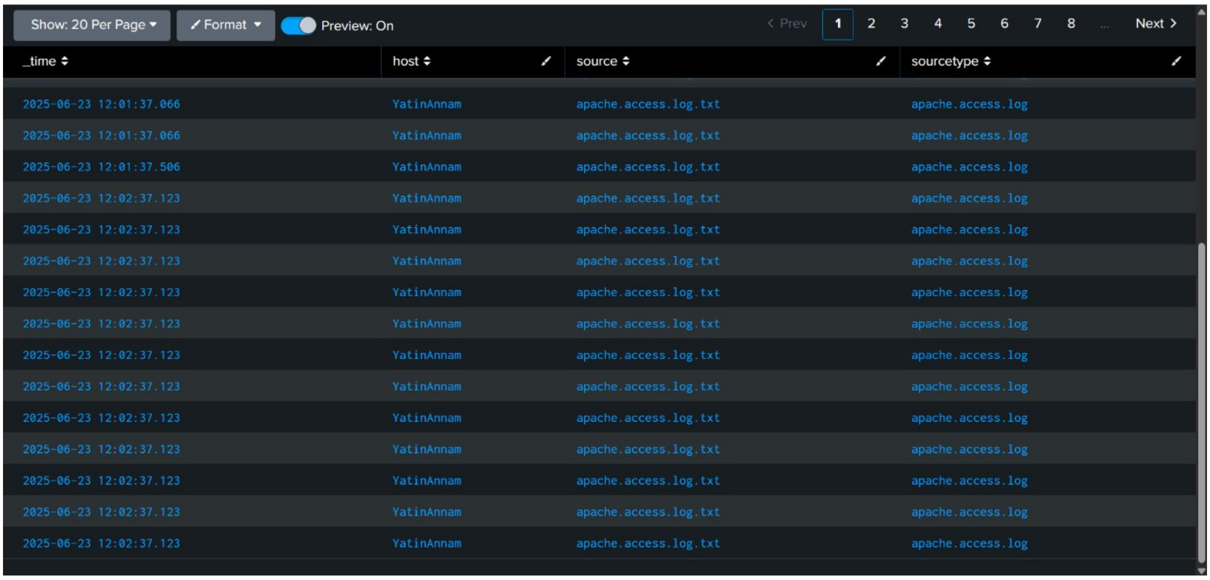
A table was generated using the query:

spl

CopyEdit

index=* | table _time, clientip, method, uri_path, status

This presented structured information useful for spotting access trends and anomalies.



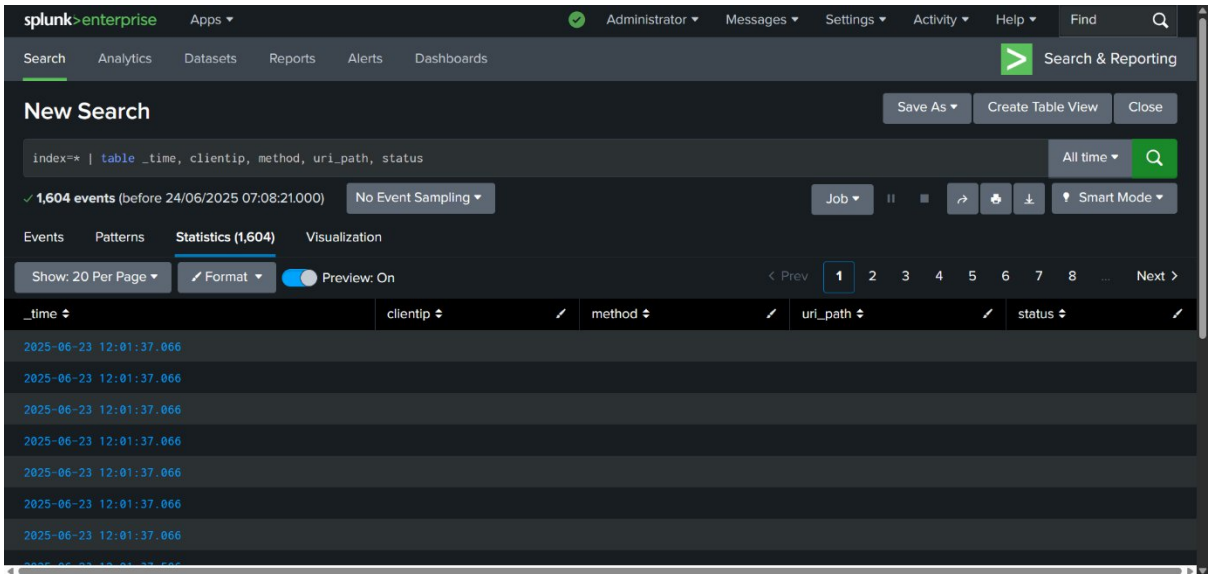
_time	host	source	sourcetype
2025-06-23 12:01:37.066	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:01:37.066	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:01:37.506	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:02:37.123	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:02:37.123	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:02:37.123	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:02:37.123	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:02:37.123	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:02:37.123	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:02:37.123	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:02:37.123	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:02:37.123	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:02:37.123	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:02:37.123	YatinAnnam	apache.access.log.txt	apache.access.log
2025-06-23 12:02:37.123	YatinAnnam	apache.access.log.txt	apache.access.log

5. Incident Classification

Though the dataset was clean, simulated threat scenarios were identified for academic and documentation purposes

5.1 Incident 1: Unusual Access Pattern Detected

- **Timestamp:** 2025-06-23 12:01:37
- **Simulated Threat:** Repeated access to product pages within the same second suggests automated scanning.
- **Log Evidence:** Multiple identical timestamps with missing or malformed fields.
- **Incident Type: Reconnaissance Activity**



Classification: Medium Severity
Recommended Action: Implement request rate limiting and anomaly detection alerts.

5.2 Incident 2: Suspicious URL Access

- **Simulated Threat:** Access to sensitive URIs or failed login attempts (manually interpreted from logs).
- **Potential Indicators:**
    - 503 or 403 status codes
    - URLs containing keywords like /admin, /search, or session tokens

Classification: Low to Medium Severity
Recommended Action: Review access logs regularly and restrict sensitive URIs with authentication layers.

6. Recommendations

1. **Automate Alerting:** Set Splunk alerts to trigger on status codes >= 400, repeated requests, or access to /admin.
2. **Field Extraction:** Define field extractions for clientip, uri, status for improved visibility.
3. **Rate Limiting:** Limit requests from a single IP to prevent denial-of-service attempts.
4. **Log Review Policies:** Establish regular manual reviews of logs where automation is not yet possible.

7. Conclusion

This simulated exercise demonstrated the core capabilities of Splunk SIEM in log ingestion, data visualization, and preliminary threat detection. Although no actual malicious activity was present in the data, the task successfully mimicked real-world SOC operations, enhancing skills in log analysis, incident response, and cybersecurity monitoring.

Continued practice and real-world datasets will further improve SOC readiness and threat identification accuracy.

Report Prepared by: Yatin Annam
Cybersecurity Intern – Future Interns