Security Alert Monitoring & Incident Response

Cyber Security Task 2 | Future Interns

Intern: Safik Rahman

1. Security Alert Monitoring & Analysis using Splunk SIEM

In today's dynamic cybersecurity environment, **Security Information and Event Management (SIEM)** tools are essential for detecting, analyzing, and responding to potential threats. This report presents a simulated security monitoring task conducted using **Splunk Enterprise**, a leading SIEM platform.

The task involved uploading and analyzing sample log files, identifying potential suspicious activities, classifying incidents, and documenting findings along with recommended mitigation steps.

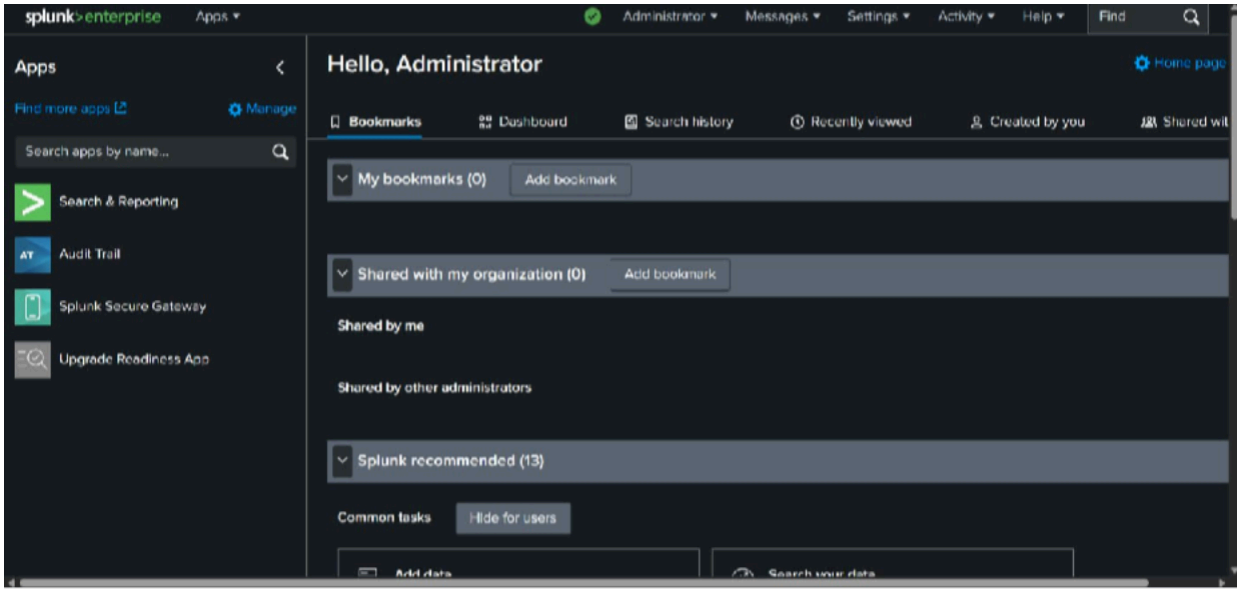
2. Tools & Environment Setup

System Configuration

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

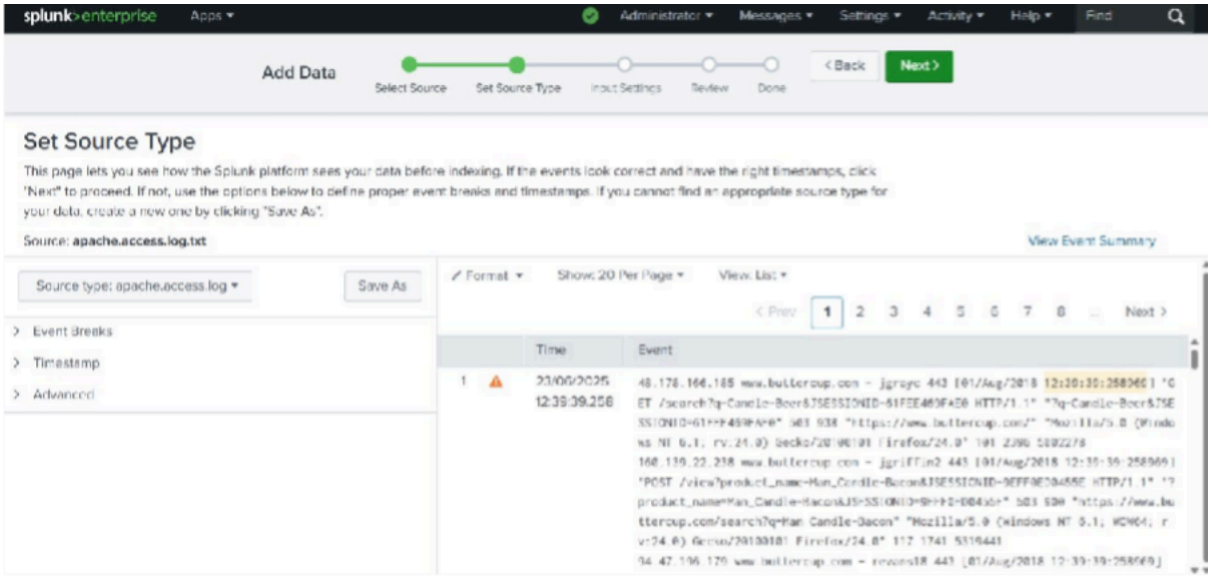
Installation Process

- Downloaded Splunk from the official website (splunk.com).
- Installed and launched via http://127.0.0.1:8000.
- Set up user credentials and accessed the main dashboard.



3. Log File Ingestion

Using the **“Add Data”** feature in Splunk, a sample `.log` file was uploaded to simulate event ingestion from a fictional e-commerce website.



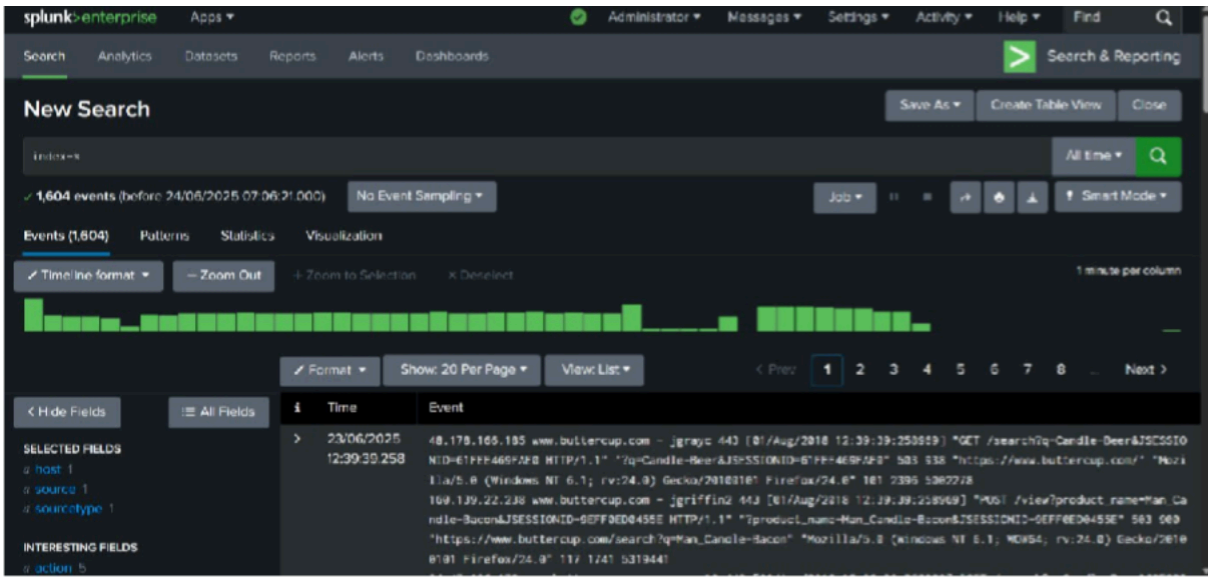
4. Log Analysis Workflow

1. Initial Search

To verify data ingestion, the query:

```
index=*
```

was executed, successfully retrieving over **1600 events**.

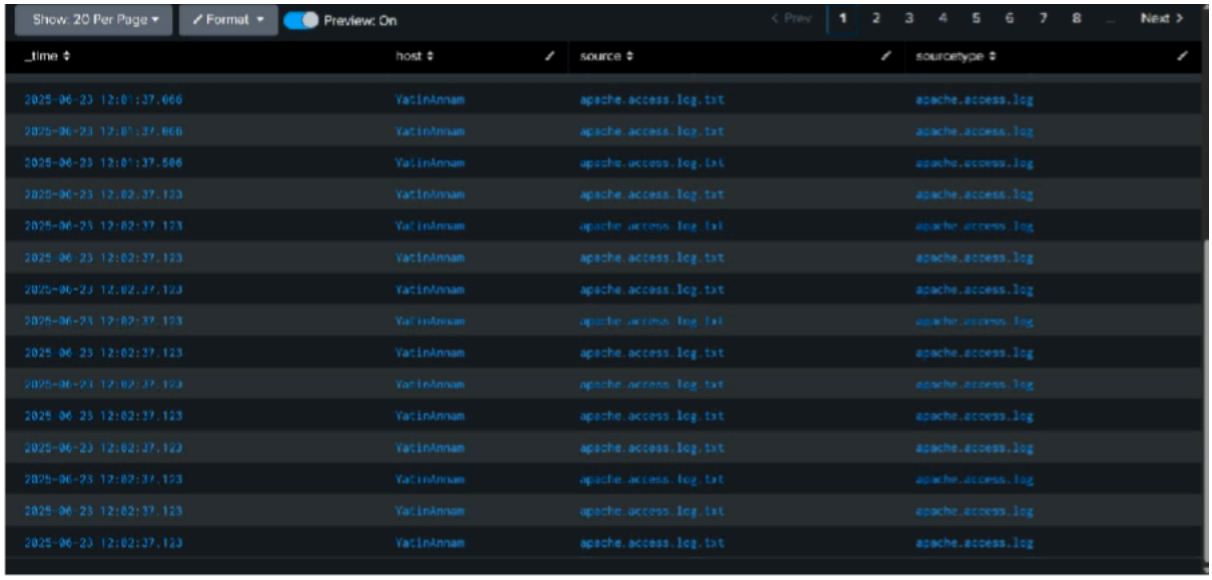


2. Table View of Log Fields

Structured view was generated using:

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

This helped visualize request patterns and anomalies.

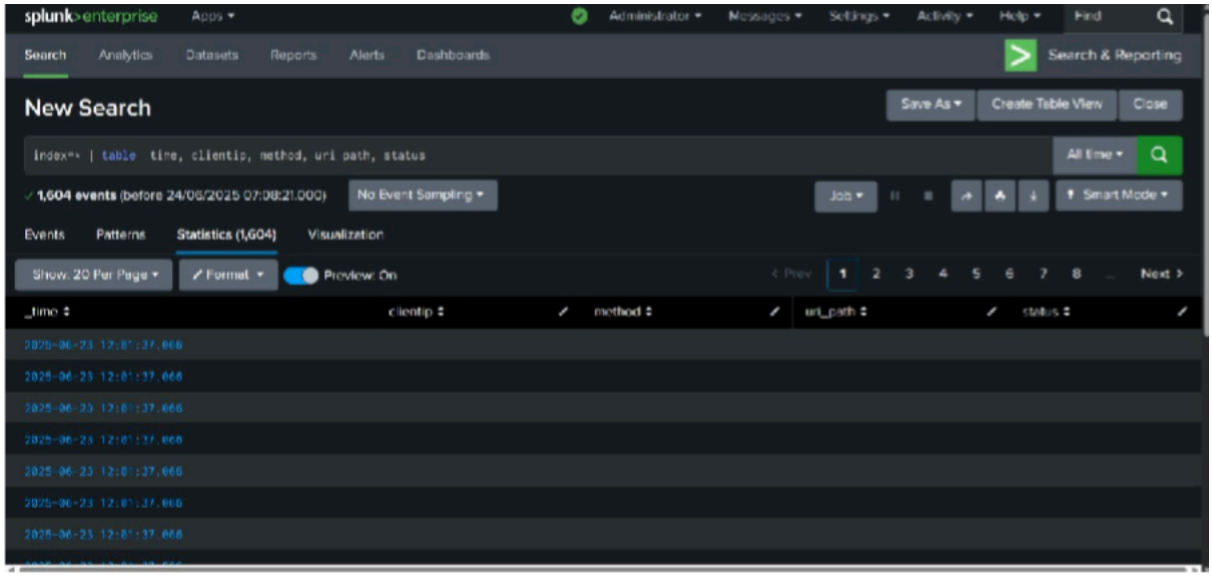


5. Simulated Incident Detection & Classification

While the logs were clean, sample scenarios were constructed to replicate real-world threat detection.

Incident 1: Repetitive Access Indicating Scanning Behavior

- **Timestamp:** 2025-06-23 12:01:37
- **Observation:** Multiple hits on product pages within the same second, suggesting automated scanning.
- **Log Evidence:** Identical timestamps, repetitive URIs, missing or malformed fields.
- **Classification: Medium Severity – Reconnaissance Activity**
- **Recommendation:** Implement request throttling and anomaly-based detection alerts.



Incident 2: Suspicious Access to Sensitive URLs

- **Indicators:** Access to URIs such as /admin, /search, along with HTTP 403/503 status codes.
- **Interpretation:** Potential unauthorized access or failed login attempts.
- **Classification: Low to Medium Severity**
- **Recommendation:** Enforce access controls, review access policies, and monitor high-risk endpoints.

Recommendations for Enhanced Monitoring

- **Automated Alerting:** Configure Splunk alerts for repeated requests, specific keywords, or HTTP errors (≥ 400).
- **Custom Field Extraction:** Define extractions for clientip, uri_path, and status to improve visibility.
- **Rate Limiting:** Limit requests from a single IP to prevent denial-of-service-type behavior.
- **Regular Review:** Perform manual reviews for logs not covered by automated rules.

Conclusion

This simulated exercise successfully showcased the functionality of **Splunk SIEM** in collecting, visualizing, and analyzing log data. Although the logs were simulated, the task reflected typical workflows in a Security Operations Center (SOC) environment. It reinforced core skills in log analysis, incident classification, and response planning—critical components of any effective cybersecurity strategy.

Report Prepared by: Safik Rahman