SOC Log Monitoring and Threat Detection Dashboard Report

1. Introduction

Effective Security Operations Center (SOC) monitoring depends on continuous visibility into authentication behavior, web activity, and request patterns. Centralized log analysis enables early detection of brute-force attacks, reconnaissance attempts, and abnormal traffic sources.

This project implements a **SOC-focused threat detection dashboard using Splunk Enterprise**, built on sample security logs to simulate real-world attack scenarios. The dashboard is designed for **analyst-driven investigation**, emphasizing detection and situational awareness rather than automated response.

This report documents the dashboard's **design, SPL logic, and security relevance**, demonstrating practical SIEM and SOC monitoring skills.

2. Objective

The objectives of this project were:

- To ingest and analyze security-relevant logs in Splunk
- To detect authentication abuse and brute-force behavior
- To identify web directory enumeration and reconnaissance activity
- To analyze request volume patterns by source IP
- To build SOC-style dashboards using SPL and Splunk visualizations

3. Data Sources

Index Used:
`soc_logs`

Log Types Analyzed:

- Linux authentication logs (SSH failed password events)
- Web server access logs (HTTP status codes and URI paths)
- Source IP–based request activity

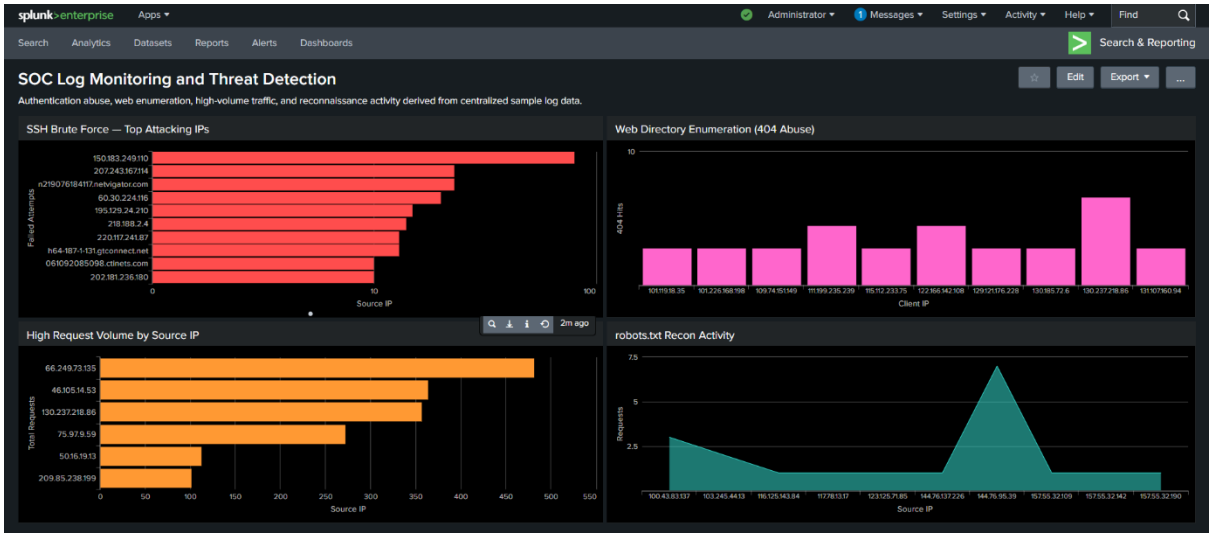
Data Characteristics:
Logs represent simulated enterprise traffic and attacker behavior commonly observed in SOC environments.

4. Tools and Technologies Used

- Splunk Enterprise (Local Installation)
- SPL (Search Processing Language)
- Classic Splunk Dashboards
- Visualizations:
  - Bar charts
  - Line charts
  - Tables
  - Area charts

5. Dashboard Design and Implementation

A centralized dashboard titled **"SOC Log Monitoring and Threat Detection"** was created. Each panel corresponds to a common SOC detection use case.



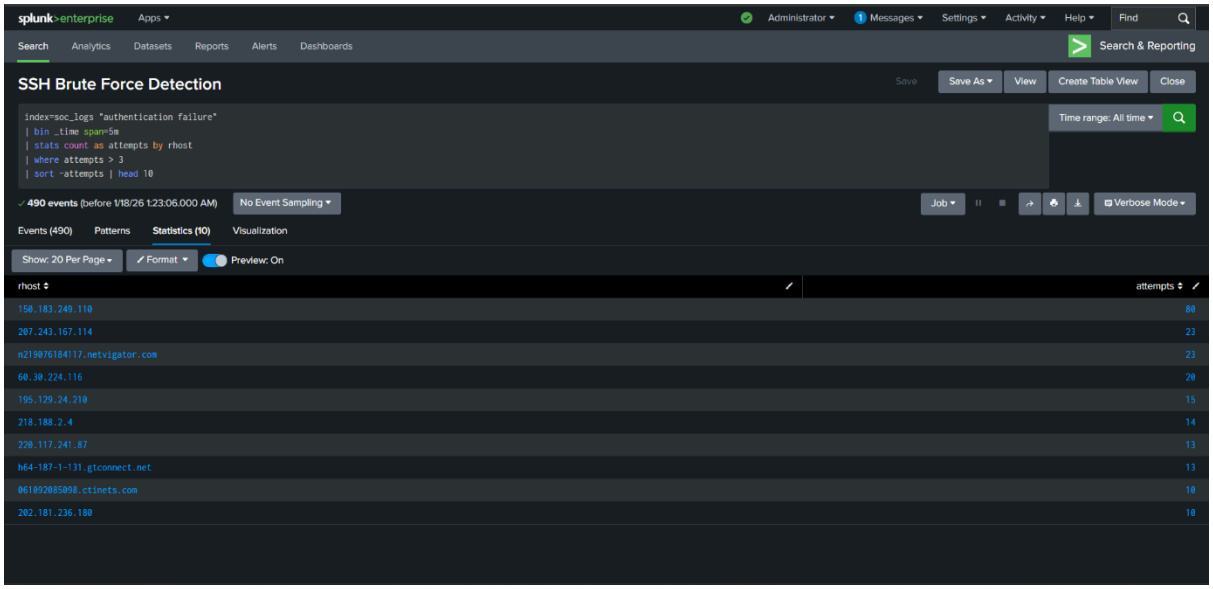
5.1 SSH Brute Force – Top Attacking IPs

Search Logic:

```
index=soc_logs "authentication failure"
| stats count as attempts by host
| where attempts > 3
| sort -attempts
| head 10
```

Visualization: Horizontal Bar Chart

Purpose:
Identifies hosts generating repeated SSH authentication failures, indicating brute-force or credential-stuffing attempts.



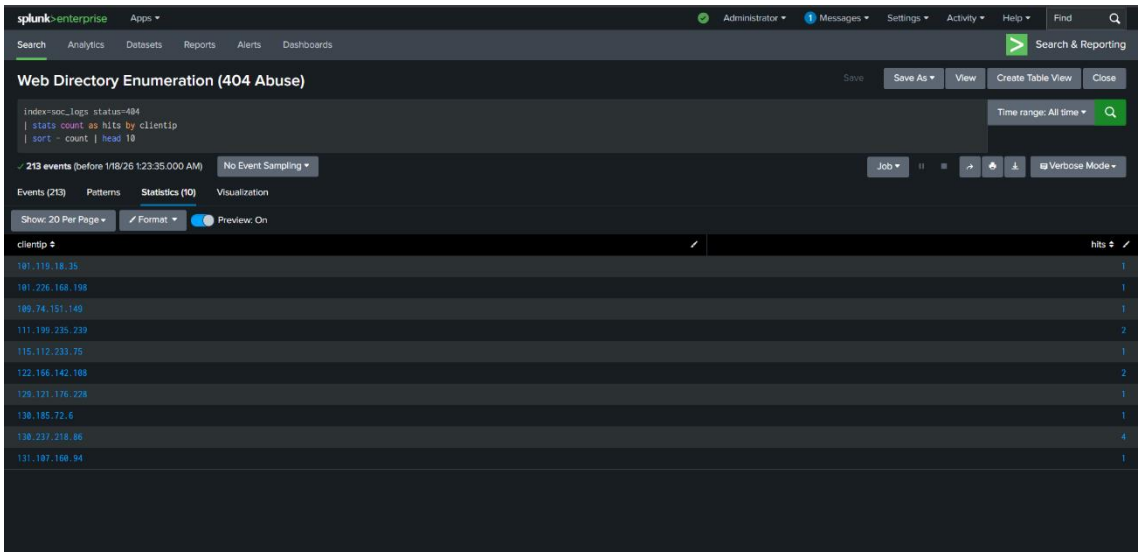
5.2 Web Directory Enumeration (404 Abuse)

Search Logic:

```
index=soc_logs status=404
| stats count as hits by clientip
| sort -hits
| head 10
```

Visualization: Bar Chart

Purpose:
Detects directory and file enumeration by tracking repeated 404 errors from the same client IPs, a common reconnaissance technique.



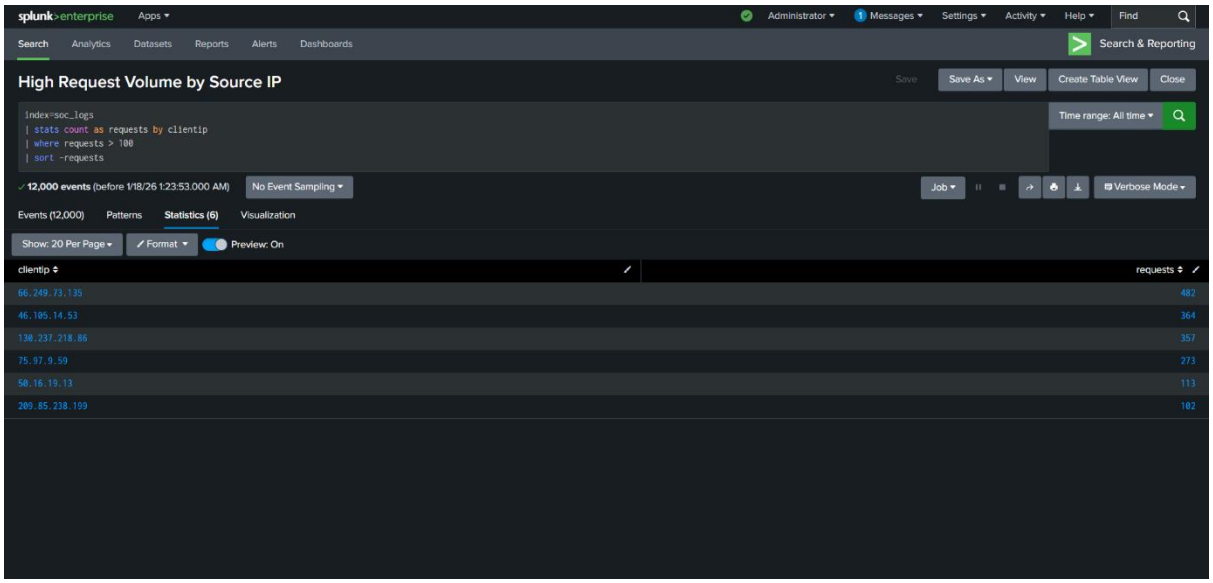
5.3 High Request Volume by Source IP

Search Logic:

```
index=soc_logs
| stats count as requests by clientip
| sort -requests
| head 10
```

Visualization: Bar Chart

Purpose:
Identifies IP addresses generating unusually high request volumes, which may indicate scanning, scraping, or denial-of-service style behavior.



5.4 robots.txt Reconnaissance Activity

Search Logic:

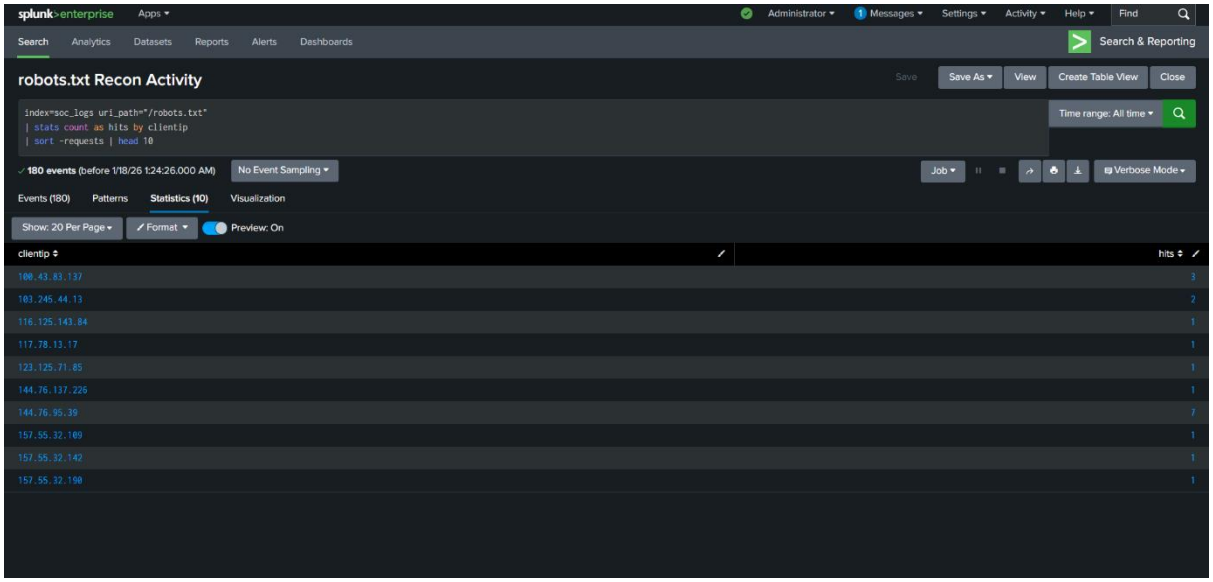
```
index=soc_logs uri_path="/robots.txt"
| stats count as hits by clientip
| sort -hits
| head 10
```

Visualization: Area Chart / Table

Purpose:
Monitors access to `robots.txt`, a file commonly requested by automated scanners and reconnaissance tools to identify restricted or sensitive paths.

This activity often precedes:

- Web enumeration
- Automated scanning
- Exploit discovery attempts



6. Cybersecurity Relevance

The dashboard directly reflects real SOC detection scenarios:

- SSH brute-force identification
- Web reconnaissance and enumeration detection
- Traffic anomaly analysis by source IP
- Early-stage attacker behavior visibility

The focus remains on **manual investigation and analyst context**, mirroring Tier-1 SOC workflows.

7. Conclusion

This project demonstrates hands-on capability in building a **SOC-style threat detection dashboard using Splunk Enterprise**. The dashboard translates raw authentication and web logs into actionable security insights using SPL and structured visualizations.

The work reflects readiness for **entry-level SOC and cybersecurity analyst roles**, with emphasis on detection logic, investigation-driven dashboards, and understanding of attacker behavior.

THANK YOU.