📘 HTTP Log Analysis & Web Traffic Monitoring Using Splunk SIEM

📌 Project Overview

This project demonstrates how a Security Operations Center (SOC) analyzes HTTP web server logs using Splunk SIEM to monitor web traffic, detect anomalies, and identify potential security threats such as brute-force attempts, suspicious file access, abnormal traffic spikes, and malicious user behavior.

The project follows a structured SOC workflow:
Log Ingestion → Field Extraction → Traffic Analysis → Anomaly Detection → User Behavior Monitoring

This lab simulates real-world SOC alert investigation and threat detection techniques.

🎯 Project Objectives

- Search and analyze HTTP events in Splunk
- Extract meaningful fields from raw HTTP logs
- Understand normal vs abnormal web traffic patterns
- Detect suspicious or anomalous activities
- Monitor user behavior for potential attacks
- Simulate real-world SOC alert investigation

🛠️ Tools & Technologies Used

- Splunk Enterprise / Splunk Free
- HTTP / Web Server Access Logs
- Search Processing Language (SPL)
- SOC Analysis Methodology

Fields Analyzed:

- Timestamp
- HTTP Method
- URI
- Status Code
- Source IP
- User-Agent
- User / Session ID

🔍 Step 1: Search for HTTP Events

Confirm that HTTP logs are successfully ingested into Splunk.

🔎 SPL Query

```
index=main sourcetype=http
```

✅ Outcome

- Verified successful ingestion of HTTP events
- Raw HTTP logs visible in Splunk
- Baseline visibility established

🧩 Step 2: Extract Relevant Fields

HTTP logs are often unstructured. Field extraction enables meaningful analysis.

```
index=main sourcetype=http
```

📌 Fields Extracted

- method (GET, POST, PUT, DELETE)
- uri (requested endpoint)
- status (HTTP response code)
- src_ip (client IP)
- user_agent
- user
- session_id

✅ Outcome

- Improved log readability
- Enabled statistical analysis
- Prepared data for detection use cases

📊 Step 3: Web Traffic Analysis

3.1 HTTP Request Method Distribution

```
index=main sourcetype=http
| stats count by method
```

SOC Insight:

- Excessive POST requests may indicate brute-force or data exfiltration

3.2 Top Accessed URLs

index=main sourcetype=http
| top limit=10 uri

SOC Insight:

- Repeated access to admin or hidden endpoints may indicate scanning or exploitation

---

3.3 HTTP Response Code Analysis

index=main sourcetype=http
| stats count by status

SOC Insight:

- High 404 / 403 → Directory brute-forcing
- Repeated 500 → Exploitation attempts

🚨 Step 4: Anomaly Detection

4.1 Traffic Volume Over Time

index=main sourcetype=http
| timechart span=1h count

SOC Insight:

- Sudden spikes may indicate DDoS or automated attacks

4.2 High Error Response Detection

index=main sourcetype=http
| stats count by status
| where status >= 400

SOC Insight:

- Indicates scanning, brute-force, or authentication abuse

4.3 Suspicious IP Investigation

```
index=main sourcetype=http
| search src_ip="suspicious_ip"
```

SOC Insight:

- Useful for threat intelligence correlation and IP blocking

👤 Step 5: User Behavior Monitoring

5.1 Failed Login Attempts

```
index=main sourcetype=http
| search action="login" status="failed"
| stats count by user
```

SOC Insight:

- Multiple failures suggest brute-force or credential stuffing

---

5.2 Session Duration Analysis

```
index=main sourcetype=http
| stats range(_time) as session_duration by session_id
| stats avg(session_duration) as avg_session_duration by user
```

SOC Insight:

- Extremely long or short sessions may indicate bots or session hijacking

---

🧠 **Security Findings**

- Identified abnormal HTTP error trends
- Detected suspicious access to sensitive endpoints
- Observed potential brute-force login behavior
- Established baseline web traffic behavior
- Improved visibility into user activity and sessions

MITRE ATT&CK Mapping

Technique ID	Description
T1071.001	Web-based Command and Control
T1110	Brute Force
T1046	Network Service Discovery
T1190	Exploit Public-Facing Application