SIEM Case Study: Multi-Vector Attack Detection Using Splunk

Project Title:

Detecting and Analyzing Brute Force and DDoS Attacks Using Splunk SIEM

Objective:

Simulate and investigate a coordinated brute-force login and web-based DDoS attack using Splunk, applying detection logic and alerting based on Apache and Windows log data.

Tools & Technologies:

- Splunk SIEM
- Windows Event Logs
- Apache Web Server Logs
- Splunk Add-on for Apache
- Common Information Model (CIM)
- CyberChef, VirusTotal

Project Workflow:

1. Scenario Setup:

- Acted as SOC Analysts for "Virtual Space Industries (VSI)," facing simulated attacks by a competitor (JobeCorp).
- Logs included authentication attempts, server activity, and network behavior.

2. Data Ingestion & Normalization:

- Used the Splunk Add-on for Apache Web Server to ingest and parse logs (GET/POST requests, referrers, IPs).

- Ingested Windows server logs for user authentication activities and account status changes.

3. Detection & Alerting:

Created detection rules and alert thresholds:

- Brute-force login alerts (failed logons > 15/hour, successful logons > 25/hour)
- Account deletion alerts
- Suspicious POST request alerts (>10)
- Spike in non-US IPs (>200)

4. Attack Findings:

- Spikes in account lockouts and password resets.
- Over 800 POST requests in <1 second from Ukrainian IPs (DDoS).
- URI and user agent count dropped sharply.
- 404 errors rose from 2.1% to 15%.

5. Visualization:

- Dashboards for auth activity, HTTP methods, IP geolocation, and traffic trends.

Recommendations:

- Enforce MFA and lockout policies.
- Geo-restrict login access.
- Deploy IDS/IPS systems for traffic anomaly detection.