SOC LOG MONITORING & INCIDENT RESPONSE SIMULATION USING SPLUNK

Project Description:

This project simulates the core responsibilities of a Security Operations Centre (SOC) analyst by analysing log data using Splunk. The goal is to detect, categorize, and respond to potential security incidents, simulating real-world SOC workflows including alert triage, threat detection, and stakeholder communication.

Project Tasks & Deliverables

Task 1: Log Ingestion

- The sample log file SOC_Task2_Sample_Logs.txt was ingested into Splunk using a custom sourcetype soc_logs.
- Host field was set to SOC-simulated.
- Field extractions were configured using Splunk's rex function to parse user, ip, action, and threat values.
- Smart Mode helped extract key fields for search-time analysis.

Task 2: Log Analysis

- SPL queries were used to search for:
    - malware detected events
    - login failed attempts
    - Unusual file accessed entries
- Patterns like repeated login failures and malware infections were flagged as suspicious.

Task 3: Alert Categorization

- Each event was classified as:
  - High: Advanced malware threats (e.g., Rootkit, Ransomware, Worm)
  - Medium: Failed logins or file access from public IPs
  - Low: Normal user behaviour from internal IPs
- Severity was computed using eval severity=case(...) in Splunk with proper field trimming.

Task 4: Incident Reporting

- **Two detailed incident reports** were created:
  - **Incident 1**: Malware threat from user bob (Worm from public IP) — High severity
  - **Incident 2**: Failed login from public IP for user bob — Medium severity
- Reports included evidence, impact assessment, and recommended actions.

Task 5: Stakeholder Communication

- Two forms of simulated communication were created:
  - Formal email briefing to SOC manager
  - Informal SOC Slack/Teams message
- Both formats outlined the incident, impact, and next steps.

Task 6: Dashboard Creation

A custom Splunk dashboard SOC Threat Monitoring was built with the following panels:

1. Events by Severity (Pie/Bar Chart)
2. Top Threat Types (Bar Chart)
3. Top Source IPs (Bar or Table)
4. Recent Events Table

This dashboard enables quick triage and threat visibility for SOC teams.