Security Alert Monitoring & Incident Response - Task 2

Intern Name : Indala Lokesh Babu

Internship Domain : Cyber Security

Task Title : Security Alert Monitoring & Incident Response

Date : July 2025

Tools Used : Splunk Cloud Free Trial

Objective :

The Objective of this task was to analyze simulated security logs using a SIEM tool(Splunk), detect suspicious activities such as failed login attempts and sensitive file access, and prepare a professional incident response report based on the findings.

Log Source :

- **Log File Name :** sample_logs.txt
- **Description :** Simulated logs containing login attempts, usernames, IP addresses, system access events
- **Upload Platform :** Splunk Cloud Free Trial

Queries Executed :

- Query 1 – Show All Logs
  index="main"
  #Verified that logs were uploaded successfully and viewable in the Splunk console.
- Query 2 – Failed Login Attempts
  index="main" status="failed"
  #Displayed all events where login attempts failed.
- Query 3 – Count of Failed Logins by IP
  index="main" status="failed"
  | stats count by ip
  #Grouped failed login attempts per IP address.
- Query 4 – Repeated Failed Logins (Potential Brute Force)
  index="main" status="failed"
  | stats count by ip
  | where count > 2

#Highlighted Ips that had 3 or more failed login attempts :
192.168.1.11 ; 192.168.1.12

- Query 5 – Sensitive File Access Attempt
  index="main" path="/etc/passwd"
  #Detected that 192.168.1.10 accessed /etc/passwd ,indicating a possible privilege escalation attempt.

Incident Type	IP Address	Severity	Notes
Brute-force login attempts	192.168.1.11	High	3 failed login attempts
Brute-force login attempts	192.168.1.12	High	3 failed login attempts
Sensitive file access attempt	192.168.1.10	Critical	Accessed /etc/passwd file
Repeated login failures	192.168.1.10	Medium	2 failed logins before success

Recommendations :

- Enable account lockout after multiple failed login attempts
- Block or monitor IPs showing suspicious activity
- Enable alerts for sensitive file access(e.g.., **/etc/passwd**)
- Enforce strong password policies
- Implement Multi-Factor Authentication(MFA)

Screenshots Included :

- All logs view (all_events.png)
- Failed login attempts (failed_login.png)
- Grouped logins by IP (top_failed_by_ip.png)
- Suspicious IPs (suspicious_ip.png)
- Sensitive file access (file_access.png)

Summary :

This task provided practical experience in :

- Using a SIEM tool (Splunk)
- Writing basic SPL queries
- Detecting brute forces and suspicious activities.
- Documenting incidents in a structured report

This forms the foundation of what real-world Security Operations Center (SOC) teams do for live incident monitoring and response.