Security Alert Monitoring and Incident Response – Task 2

Objective

The objective of this task is to monitor simulated security alerts, identify suspicious activities, classify potential security incidents, and document appropriate incident response actions using basic SIEM concepts.

Tools Used

Simulated security log files were analyzed using concepts related to Security Information and Event Management (SIEM). No real-time attacks were executed during this task. The analysis was performed on sample SSH authentication logs similar to those monitored by SIEM tools such as Splunk or the ELK Stack.

Log Analysis

During the monitoring of simulated SSH authentication logs, multiple failed login attempts were observed from the same IP address within a short time period. The attempts targeted different usernames such as **admin** and **root**, which indicates a possible automated brute force attack. The high frequency and repetitive nature of these login failures triggered a security alert.

Alert Identification

A security alert was generated due to repeated failed SSH login attempts originating from a single IP address. The alert highlighted abnormal authentication behavior, suggesting a potential unauthorized access attempt against the system.

Incident Classification

Based on the analysis of the alert, the incident was classified as follows:

- **Incident Type:** Brute Force Attack
- **Category:** Unauthorized Access Attempt
- **Severity Level:** Medium
- **Incident Status:** No successful breach detected

Incident Response Actions

After identifying the suspicious activity, the source IP address was blocked to prevent further login attempts. Authentication logs were carefully reviewed to confirm that no unauthorized access had occurred. Additional monitoring was enabled to detect similar suspicious activities in the future.

Recommendations

- Implement account lockout policies after multiple failed login attempts
- Enable multi-factor authentication (MFA) for remote system access
- Restrict SSH access using IP whitelisting or firewall rules
- Continuously monitor authentication logs using SIEM-based alerts

Conclusion

This task demonstrated the process of monitoring simulated security alerts, identifying suspicious activities, and responding to a potential security incident. By analyzing SSH authentication logs and applying SIEM concepts, the incident was successfully identified and classified. Appropriate response actions and preventive recommendations were documented to enhance the overall security posture of the system.