📄 Incident Response Report

Security Alert Monitoring and Incident Response – Task 2

Objective

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

Tools Used

Splunk Enterprise (Free Trial) was used as the SIEM tool to monitor and analyze simulated SSH authentication logs. A sample SSH log file was uploaded into Splunk, and log searches were performed to identify suspicious login attempts. No real-time attack execution was performed during this task.

Log Analysis

While monitoring the SSH authentication logs in Splunk, multiple failed login attempts were observed from the same IP address within a short time interval. The login attempts targeted different usernames such as **admin** and **root**, indicating a possible automated brute force attack. The repetitive nature and frequency of these 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 indicated abnormal authentication behavior and suggested a potential unauthorized access attempt against the system.

Incident Classification

Based on the alert analysis, 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 detecting the suspicious activity, the source IP address was identified and blocked to prevent further login attempts. Authentication logs were reviewed to ensure that no unauthorized access had occurred. Continuous monitoring was enabled in Splunk 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
- Regularly monitor authentication logs using SIEM-based alerts

Screenshots Evidence

The following screenshots are included as evidence of the analysis process:

- Splunk Enterprise dashboard after successful installation
- Successful upload of SSH authentication log file
- Search results displaying multiple failed SSH login attempts

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 using Splunk 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.