Week 3 - Assignment

Dev Mehta - 21BCE2888

Understanding SOC, SIEM and QRadar

`1. Introduction to SOC`

An organization's centralized unit in charge of keeping an eye on, evaluating, and protecting its information systems and assets is known as a Security Operations Centre (SOC). Keeping the organization's networks, data, and IT infrastructure secure against online attacks is its main goal. A SOC's primary duties consist of:

- `Monitoring`
  Constantly keeping an eye on user behaviour, system activity, and network traffic for any odd trends that could point to a security concern.
- `Incident Detection`
  Identifying and categorizing security occurrences via monitored data analysis is known as incident detection. To identify abnormalities, it's necessary to understand what typical behaviour looks like.
- `Incident Response`
  Creating and putting into practice plans to prevent and quickly address security problems. This can entail deploying fixes, deleting malware, and isolating the afflicted systems.
- `Forensics`
  Investigating security incidents to determine the type and scale of an attack, assisting in strengthening security protocols, and averting further occurrences are referred to as forensics.

By offering continuous monitoring and quick reaction, SOCs play a critical role in an organization's cybersecurity strategy by reducing the effect of security breaches and preserving the confidentiality, integrity, and availability of data and systems.

2. SIEM Systems

Modern cybersecurity relies heavily on Security Information and Event Management (SIEM) systems because they allow businesses to gather, analyze, and correlate security data from diverse sources in real-time. Effective security threat monitoring and response are made possible for organizations by SIEM through:

- `Log Collection`
  The process of collecting log data from host systems, apps, and other elements of the organization's IT infrastructure.
- `Correlation`
  It is the process of comparing recorded security events to find trends, possible dangers, or vulnerabilities. Correlation makes it easier to spot complex assaults that individual event analysis could miss.
- `Alerting`
  Instantaneous notification of security administrators when a predetermined security incident takes place. These warnings allow for an immediate reaction to possible security problems.
- `Compliance Reporting`
  Creating reports to demonstrate that the organization's security procedures are in place and operating as intended, in accordance with internal rules and industry laws.

3. QRadar Overview

IBM QRadar is a leading SIEM solution that provides advanced security intelligence and analytics. Key features and benefits of IBM QRadar include:

- `Advanced Analytics`
  To identify advanced threats and atypical activity in real-time, QRadar uses behavioral analytics and machine learning.
- `Comprehensive Log Management`
  Gathers and examines log data from a range of sources, such as network devices, security appliances, operating systems, and applications.
- `Incident Forensics`
  Provides in-depth insight into security occurrences, assisting in thorough forensic examination.

- `User Behaviour Analytics`
  Analyzing user behaviour helps to spot compromised accounts and insider threats by tracking user actions and behaviours.
- `Cloud and On-Premises Deployment`
  QRadar offers flexibility by supporting both on-premises and cloud-based deployments, allowing businesses to select the one that best meets their needs and infrastructure.

4. Use Cases

Here are some actual use scenarios and illustrations of how a SOC may utilise a SIEM system like IBM QRadar to identify and react to security incidents:

- `Detecting Malware`
  QRadar can be used to detect malware infections by analyzing security logs for suspicious activity, such as unusual file access or network traffic patterns.
- `Detecting data breaches`
  QRadar can be used to detect data breaches by analyzing security logs for suspicious activity, such as unauthorized access to sensitive data or large-volume data transfers.
- `Detecting insider threats`
  QRadar can be used to detect insider threats by analyzing security logs for suspicious activity by users with privileged access or users who are accessing unusual data or systems.
- `Investigating security incidents`
  QRadar can be used to investigate security incidents by providing analysts with a centralized view of all relevant security data. This helps analysts to quickly understand the scope of the incident and identify the root cause.
- `Responding to security incidents`
  QRadar can be used to respond to security incidents by providing analysts with tools to quarantine infected systems, block malicious traffic, and notify appropriate personnel.

Overall, SIEM systems like IBM QRadar are essential tools for SOCs to *detect, investigate, and respond to security incidents effectively.*