Saumyaa Prajapat
21BCI0265

# ASSIGNMENT 3

## Understanding SOC, SIEM, and QRadar

### 1. Introduction to SOC

A security operations center (SOC) – sometimes called an information security operations center or ISOC – is a team of in-house or outsourced IT security experts that oversees the entire infrastructure Company IT, real time, and fix them quickly and effectively.

The key benefit of operating or outsourcing a SOC is that it unifies and coordinates an organization's security tools, measures, and ability to respond to security incidents. This often leads to improved security policies and precautions, faster threat detection, and a quicker, more efficient, and more cost-effective response to security threats.

**Purpose:**

The main task of SOC is security monitoring and warning. This includes collecting and analysing data to identify suspicious activities and improve organizational security. Threat data is collected from firewalls, intrusion detection systems, intrusion prevention systems, security information and event management (SIEM) systems, and threat intelligence. Alerts are sent to SOC team members whenever deviations, unusual trends, or other signs of compromise are detected.

**Key Function and Roles:**

- Explore assets:

By gaining in-depth knowledge of all hardware, software, tools and technology used within the organization, SOCs ensure that assets are monitored for security incidents.

- Monitor behaviour:

SOC analyses technology infrastructure 24 hours a day, 7 days a week, 365 days a year to detect any abnormalities. The SOC uses both reactive and proactive measures to ensure that unusual activities are detected and resolved quickly. Behavioural monitoring of unwanted activities is used to reduce false positives.

- Maintain an activity log:

Every activity and communication that takes place within the company must be recorded by the SOC team. Activity logs allow the SOC to go back and identify past actions that may have caused a cybersecurity breach. Log management also helps establish a baseline for what is considered normal activity.

- Warning classification:

Not all security incidents are equal. Some incidents pose a higher risk to the organization than others. Assigning severity ratings helps SOC teams prioritize the most severe alerts.

- Incident response:

SOC teams perform incident response when a compromise is discovered.

- Investigate the root cause:

After an incident, the SOC may be tasked with investigating when, how and why the incident occurred. During investigations, SOC relies on log information to trace the root of the problem and prevent recurrence.

- Compliance management:

SOC team members must act in accordance with organizational policies, industry standards, and legal requirements.

Saumyaa Prajapat
21BCI0265

## 2. SIEM Systems

Security information and event management, or SIEM, is a security solution that helps organizations identify and resolve potential security threats and vulnerabilities. SIEM platforms started out as log management tools, combining security information management (SIM) and security event management (SEM) to enable real-time monitoring and analysis of the security of related events, as well as monitor and log security data for compliance or auditing purposes. purpose.

**Importance of SIEM:**

SIEM solutions benefit businesses in a variety of ways and have become an important part of streamlining security processes.

- Real-time threat identification:

SIEM solutions enable centralized compliance testing and reporting across a company's entire infrastructure. Advanced automation streamlines the collection and analysis of system logs and security events to reduce internal resource usage while meeting strict compliance reporting standards.

- Improved organizational efficiency:

Because of the improved visibility of IT environments that it provides, SIEM can be an essential driver of improving interdepartmental efficiencies. A central dashboard provides a unified view of system data, alerts and notifications, enabling teams to communicate and collaborate efficiently when responding to threats and security incidents.

- Detecting advanced and unknown threats:

Using integrated threat intelligence feeds and AI technology, SIEM solutions can help security teams respond more effectively to a wide range of cyberattacks

- Conduct forensic investigation:

SIEM solutions allow organizations to efficiently collect and analyze log data from all of their digital assets in one place. This gives them the ability to recreate past incidents or analyze new ones to investigate suspicious activity and implement more effective security processes.

- Assessing and reporting on compliance:

Compliance auditing and reporting is both a necessary and challenging task for many organizations. SIEM solutions dramatically reduce the resource expenditures required to manage this process by providing real-time audits and on-demand reporting of regulatory compliance whenever needed.

- Monitoring Users and Applications:

SIEM solutions monitor every network activity of all users, devices, and applications, dramatically improving transparency across the entire infrastructure and detecting threats, regardless of assets and services.

## 3. Overview of QRadar

IBM QRadar collects, processes, aggregates, and stores network data in real time. QRadar uses this data to manage cybersecurity by providing real-time monitoring and insights, alerts and breaches, and responding to cyber threats.

IBM QRadar SIEM (Security Information and Event Management) is a modular architecture that provides real-time visibility into your IT infrastructure that you can use to detect threats and priorities. You can scale QRadar to meet your stream and log collection and analysis needs. You can add integration modules to your QRadar platform, such as QRadar Risk Manager, QRadar Vulnerability Manager, and QRadar Incident Forensics. The operation of the QRadar Security Intelligence Platform consists of three layers and applies to any QRadar deployment architecture, regardless of its size and complexity.

**Key features**

- Task scanner:

the task scanner component scans specified properties, at scheduled intervals. This parsing mechanism executes actions when the attribute value matches a specified value.

- Script Engine:

This script engine is a plug-in module that provides trigger points and plug-ins for the identity management system. This can be achieved using the JavaScript and Groovy programming languages.

- Policy Service:

This component allows validations to be applied to objects or properties when they are updated or created.

- Audit Logging:

Audit Logging performs logging operations for all affected system users and also configures the log repository. This uses collated data as the basis for reports and activity logs to capture internal and external audience activities.

- Storage:

This component abstracts the pluggable storage layer. The IDM modular framework provides the ability to collate and synchronize data with a variety of external data stores such as relational databases (RDBMS), LDAP data servers, CSV and XML files.

**Deployment options**

- On premises:

Organizations can deploy QRadar on their own infrastructure, giving them full control over hardware and software configuration.

- Cloud:

IBM offers a cloud version of QRadar, allowing organizations to take advantage of cloud management and scalability.

## 4. Use Cases

- Log Management:

Databases, applications, users, and servers generate large amounts of log data. SIEM tools can standardize and centralize log data collection. This enables seamless security analysis and correlation, while also allowing the IT security team to search through the data for specific keywords or values.

- Phishing Detection:

Phishing is an attempt to obtain sensitive information used for fraud and identity theft. This includes attempts to obtain personal information, such as social security numbers, bank account numbers, or PIN codes and passwords. Phishing, especially spear phishing, is often used to gain initial access within a network. When they receive phishing emails, analysts can use SIEM to track who received them, clicked on links within them, or responded to them, allowing them to take immediate action to minimize damage.

- SIEM for automation:

SIEM automates threat detection activities and provides the basis for automated incident response. Moving security alerts and incidents to Logpoint SOAR enables increased incident response speed by automating manual tasks, helping to reduce security costs and increase SOC productivity.