Rohit Patiballa
21BCI0278

Assignment 3

Understanding SOC, SIEM, and QRadar

1. Introduction to SOC

The Security Operations Center (SOC) serves as the hub for an organization's security operations. A SOC, also known as an information security operations center (ISOC), is a centralized location where information security professionals use technology to create and maintain a security architecture to monitor, detect, analyze, and respond to cyber security incidents, often 24 hours a day.

The security team, including security analysts and engineers, monitors all activity on servers, databases, networks, applications, endpoints, websites, and other systems to identify threats. potential security threats and stop them as quickly as possible. They also monitor relevant external sources (such as threat intelligence) that may affect the organization's security posture.

Purpose of SOC:

• Threat detection:
SOC teams continuously monitor network traffic, system logs, and security alerts to identify unusual or suspicious activity that may indicate a security breach.

• Response to the incident:
When a security incident is detected, the SOC initiates a structured incident response process. This includes containing the threat, investigating the incident, and minimizing its impact.

• Vulnerability management:
SOCs typically conduct vulnerability assessments to identify weaknesses in an organization's systems and applications, enabling proactive remediation.

• Safety information:
SOC analysts collect and analyze threat intelligence to understand evolving cyber threats and trends, helping organizations stay ahead of potential attacks.

• Compliance and reporting:
SOC teams ensure that the organization complies with regulatory requirements regarding data security and privacy. They also produce reports for regulators and regulators.

Main function:

• Monitor:
Continuously monitor network and system activity to detect signs of intrusion, unauthorized access, or malicious behavior.

• Alarm:
Create alerts and notifications when security incidents are detected. These warnings are usually classified by severity.

• Investigation:
SOC analysts investigate security incidents, analyze logs, perform forensics, and determine the scope and impact of incidents. Response to the incident:
Develop and implement incident response plans to prevent, mitigate, and recover from security incidents.

• Forensic:
Collect digital evidence to understand how incidents occurred and support legal action or further analysis.

• Threat information:
Use data sources and threat databases to identify emerging threats and vulnerabilities relevant to your organization.

• Report:
Provide regular reports on security incidents, trends and vulnerabilities to stakeholders, including senior management.

2. SIEM system

Security Information and Event Management, or SIEM, is a security solution that helps organizations identify and address potential security threats and vulnerabilities before they have a chance to disrupt operations. your business. SIEM systems help enterprise security teams detect anomalies in user behavior and use artificial intelligence (AI) to automate many of the manual processes involved in detecting threats and applications. incident response.

Meaning of SIEM:

• Summary and correlation:
SIEM systems aggregate data from multiple sources, including logs, network traffic, and security alerts. They connect this data and provide a comprehensive view of an organization's security posture.

• Real-time monitoring:
SIEM provides real-time monitoring, enabling organizations to detect and respond to security incidents as they occur, reducing the potential impact of a breach. Warnings and Cautions:
The SIEM generates alerts and notifications when suspicious or unusual activities are detected, enabling rapid response.

• Compliance Management:
SIEM systems help organizations meet regulatory compliance requirements by providing auditing processes, reporting capabilities, and security controls.

• Threat detection:
SIEM uses advanced analytics and machine learning to identify patterns and anomalies that indicate potential security threats.

• Response to the incident:
SIEM supports incident response by providing tools for investigation, incident tracking, and case management.

3. QRadar overview

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 statistics, 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 prioritize. You can scale QRadar to meet your stream and log collection and analysis needs. You can add integration modules such as QRadar Risk Manager, QRadar Vulnerability Manager and QRadar Incident Forensics to your QRadar platform.

Key Features and Abilities:

• Collect logs and events:
QRadar aggregates and normalizes data from multiple sources, including logs, network resources, and security devices, to provide a comprehensive view of an organization's security landscape.

• Real-time monitoring:
It provides real-time monitoring and correlation of security events, enabling rapid threat detection and alerts. Advanced analytics:
QRadar uses advanced analytics, including User Behavior Analysis (UBA) and threat intelligence sources, to identify suspicious activity and emerging threats.

• Accident investigation:
The platform provides tools for in-depth incident investigation, including packet capture and endpoint visualization.

• Panels and reports:
QRadar provides customizable dashboards and reporting capabilities to visualize security data and generate compliance reports.

• Integration:
It supports integration with a variety of security technologies, including firewalls, intrusion detection systems (IDS/IPS), and endpoint security solutions.

Deployment options:

• On the website:
Organizations can deploy QRadar on their own infrastructure, giving them full control over hardware and software configuration.

• Cloud:
IBM offers a cloud-based version of QRadar that allows organizations to take advantage of cloud-based management and scalability.

4. Use cases

• Search for threats:
The process of actively searching for cyber risks within an organization or network is called threat hunting. Threat scanning may be performed to resolve a security issue or to detect new and unknown attacks or intrusions. Searching for threats requires access to security data from anywhere in the enterprise, which a SIEM can provide.

• Detection of compromised user credentials:
Make sure you have a use case and workflow for detecting any attempts to compromise user credentials using brute force, Pass the Hash, Golden Ticket or other methods. In the event of a successful breach, it is important to identify affected users and organizations in order to investigate the impact and prevent further damage.

• Phishing detection:
Phishing is an attempt to obtain confidential information that is used for fraud and identity theft. This includes attempts to obtain personal information such as social security numbers, bank account numbers or PINs and passwords. It is important to ensure that this type of information is protected throughout the organization. Phishing, especially phishing, is often used to gain access within a network. When analysts receive phishing emails, SIEM allows them to track who received them, clicked on links or responded to them, allowing them to take immediate action to minimize damage.

• Secure cloud applications:
The cloud service brings with it many advantages, but also comes with challenges: meeting new compliance requirements, improving control and monitoring of user access or preparing for possible malware infections and data leaks. SIEMs must support cloud-based applications as log sources, such as Salesforce, Office365 or AWS, to extend threat detection and compliance monitoring capabilities to the cloud.