Cyber Security with IBM QRadar

Assignment – 3

Name: Karthik G

Reg No: 21BEC0642

Campus: Vellore

Introduction to Security Operation Centre (SOC):

A security operations centre, or SOC, is a team of IT security professionals that monitors, detects, analyses, and investigates cyber threats on behalf of the organization. For indications of a cyber security incident, networks, servers, computers, endpoint devices, operating systems, applications, and databases are continuously inspected. The SOC team evaluates feeds, creates rules, pinpoints exceptions, improves responses, and continuously scans for new vulnerabilities.

SOC's Key roles:

1. Monitoring and Detection: To detect suspicious or malicious activity, SOC teams continuously monitor network traffic, system logs, and security alerts. They employ a variety of tools and technologies to detect potential security incidents.
2. Security Incident Investigation: SOC analysts conduct in-depth investigations into security incidents to determine how they occurred, what data may have been compromised, and what remediation steps must be taken.
3. Security Information and Event Management (SIEM) Tools: SIEM tools are an essential part of SOC operations. They collect and correlate security event data from a variety of sources, allowing analysts to identify patterns and anomalies that indicate security threats.
4. Vulnerability Management: SOC personnel are responsible for identifying and correcting vulnerabilities in the organization's systems and software. They rank vulnerabilities according to their severity and potential impact.
5. Incident Response: When a security incident is detected, SOC analysts act quickly to contain the threat and minimize its impact. This includes investigating the incident, determining the root cause, and working with other teams to resolve it.
6. Threat Intelligence: To stay informed about emerging threats and vulnerabilities, SOC teams collect and analyse threat intelligence data.

This information enables them to defend against potential attacks in advance.

The SOC's role is to keep the organization's security posture strong by quickly detecting and responding to security threats, mitigating the impact of incidents, and constantly improving security measures.

Security Information and Event Management (SIEM):

SIEM is a solution that assists organizations in detecting, analysing, and responding to security threats before they disrupt business operations. SIEM, pronounced "sim," is a security management system that combines security information management (SIM) and security event management (SEM). SIEM technology collects event log data from a variety of sources, uses real-time analysis to identify activity that deviates from the norm, and takes appropriate action. In short, SIEM provides organizations with visibility into network activity, allowing them to respond quickly to potential cyberattacks and meet compliance requirements. SIEM technology has evolved over the last decade to make threat detection and incident response smarter and faster with artificial intelligence.

Security Information and Event Management (SIEM) systems are essential in modern cybersecurity for several reasons:

- Centralized Visibility: SIEM platforms collect and aggregate data from different sources across an organization's network and systems, such as logs, events, and alarms, to provide centralised visibility. This centralised visibility provides security professionals with a comprehensive perspective of their environment, making it easier to detect and investigate risks.
- Real-time Monitoring: Real-time Monitoring: SIEM products support real-time monitoring, allowing organisations to detect suspicious or unusual activity as it occurs. This quick awareness of potential risks is essential for timely response.
- Notification: Notification and alerting: SIEM systems create alerts and notifications based on established rules and event correlation. These notifications can be tailored to prioritise key risks, allowing security professionals to focus on the most pressing issues.
- Forensics and Investigation: Forensics and Investigation: SIEM tools can be used to store historical data, which is useful for forensic analysis and investigation. Security teams can track the phases of an attack, establish the root cause, and take preventative measures.

- Threat Detection and Analysis: SIEM platforms use advanced analytics and correlation techniques to find trends and abnormalities that may indicate security concerns. They can aid in the detection of advanced assaults, insider threats, and zero-day vulnerabilities.
- Incident Response Support: Support for Incident Response: SIEM tools help with incident response by giving extensive information about security issues, such as their extent, impact, and timeframe. This data is critical for promptly containing and reducing hazards.

To summarise, SIEM is critical in modern cybersecurity because it gives organisations the tools and skills, they need to monitor their digital environments, detect security risks, respond quickly to incidents, and maintain regulatory compliance. In an increasingly complex and moving threat landscape, it is a critical component of a strong cybersecurity posture.

IBM QRadar:

IBM QRadar popular Security Information and Event Management (SIEM) solution and is a network security management platform that provides situational awareness and compliance support. QRadar uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment.

Key features:

- Cloud Integration: The platform supports cloud environments and can collect and analyze security data from cloud services and applications, providing visibility into hybrid and multi-cloud environments.
- Integration: QRadar connects with a variety of security technologies, such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and endpoint security solutions.
- Vulnerability Management: QRadar can integrate with vulnerability assessment tools to prioritize security vulnerabilities based on their risk and potential impact.
- Real-time Monitoring: QRadar provides real-time monitoring and correlation of security events and records.
- Machine Learning and Artificial Intelligence (AI): IBM QRadar includes machine learning and artificial intelligence (AI) technologies to improve threat identification and reduce false positives.
- Scalability: QRadar is scalable and capable of handling the data volumes and processing needs of large companies and complicated networks.

- Customization: Users can construct customised dashboards and reports to visualise security data in ways that are tailored to their individual requirements.
- Automation and Orchestration: QRadar allows organizations to automate response actions to certain types of security incidents. It can also integrate with security orchestration platforms to streamline incident response workflows.
- Asset Discovery and Classification: QRadar can automatically discover and classify assets on the network, helping organizations understand their attack surface and better protect critical assets.

These features make IBM QRadar a comprehensive and powerful SIEM solution that helps organizations monitor, detect, respond to, and mitigate security threats effectively while also meeting compliance requirements.

Use cases:

1: Detect and respond to malicious data exfiltration.

QRadar can be used to monitor network traffic for suspicious activity that may indicate data exfiltration. For example, QRadar can be used to detect large volumes of data being transferred to unknown IP addresses, or to detect data being transferred in an encrypted format at unusual times of day. Once suspicious activity is detected, QRadar can alert the SOC analyst and provide them with the information they need to investigate and respond to the incident.

Example:

A SOC analyst receives an alert from QRadar that there is a large volume of data being transferred from a critical server to an unknown IP address. The analyst investigates the alert and determines that the data is being transferred in an encrypted format at an unusual time of day. The analyst then blocks the data transfer and takes steps to investigate the source of the malicious activity.

2. Detect and respond to malware infections.

QRadar can be used to monitor logs from a variety of sources, including endpoints, servers, and security devices, for signs of malware infection. For example, QRadar can be used to detect suspicious file activity, such as the creation of new files in unusual locations or the modification of existing files. Once suspicious activity is detected, QRadar can alert the SOC analyst and provide them with the information they need to investigate and respond to the incident.

Example:

A SOC analyst receives an alert from QRadar that a suspicious file has been created on a critical server. The analyst investigates the alert and determines that the file is a known malware sample. The analyst then quarantines the file and takes steps to clean up the infected server.

Thank YOU!