Understanding SOC, SIEM, and QRadar

Objective:

The objective of this assignment is to explore the concepts of Security Operations Centers (SOCs), Security Information and Event Management (SIEM) systems, and gain hands-on experience with IBM QRadar, a popular SIEM tool.

What is SOC(Security Operations Center)

An organization's entire IT infrastructure is monitored round-the-clock by a team of IT security experts known as a security operations centre (SOC), also known as an information security operations centre (ISOC), in order to identify cybersecurity events in real time and respond to them as quickly and effectively as possible.

Purpose &Key Features

An SOC chooses, manages, and maintains the cybersecurity tools used by the company. It also continuously assesses threat information to identify methods to strengthen the security posture of the company.

An organization's security practices, procedures, and reaction to security events are unified and coordinated by a SOC, which is the main advantage of running one in-house or outsourcing it. This generally leads to better security policies and preventative measures, quicker threat detection, and quicker, more effective, and more affordable responses to security problems. Additionally, a SOC may increase consumer confidence and streamline and reinforce an organization's adherence to local, national, and international privacy requirements.

ROLE

SOC activities and responsibilities fall into three general categories:

Preparation, planning and prevention

A Security Operations Center (SOC) is an IT security team that monitors an organization's IT infrastructure 24/7 to detect and address cybersecurity events. They select, operate, and maintain cybersecurity technologies and analyze threat data to improve security posture. The main benefit of operating or outsourcing an SOC is unifying and coordinating security tools, practices, and response to incidents, leading to improved preventative measures, faster threat detection, and cost-effective responses. SOC activities include preparation, planning, and prevention, including asset inventory, routine maintenance, incident response planning, regular testing, and staying current on the latest security solutions and technologies. This helps organizations improve customer confidence and comply with industry, national, and global privacy regulations. SOCs also perform vulnerability assessments and penetration tests to fine-tune applications, security policies, best practices, and incident response plans.

Monitoring, detection and response

Security Operations Centers (SOCs) continuously monitor IT infrastructure 24/7/365 for known exploits and suspicious activity. The core monitoring technology is security information and event management (SIEM), which aggregates alerts and telemetry from software and hardware on the network. Some SOCs have adopted extended detection and response (XDR) technology, providing more detailed telemetry and monitoring. Log management is crucial for establishing normal activity and revealing anomalies. Threat detection involves sorting signals from noise and triaging threats by severity. Modern SIEM solutions include artificial intelligence (AI) to automate these processes. In response to a threat or incident, SOCs take actions such as root cause investigation, shutting down compromised endpoints, isolating network traffic, paused applications, deleting files, running antivirus software, and decommissioning passwords.

Recovery, refinement and compliance

The Security Operations Center (SOC) is responsible for recovery and remediation after an incident, restoring impacted assets to their pre-incident state. Post-mortem and refinement

involve using new intelligence to address vulnerabilities, update processes, and revise response plans. The SOC ensures compliance with data privacy regulations like GDPR, CCPA, PCI DSS, and HIPAA, ensuring users, regulators, and law enforcement are notified and incident data is retained for evidence and auditing.

What is SIEM?

SIEM is a security management system that combines security information and event management. It helps organizations detect, analyze, and respond to security threats before they harm business operations. SIEM technology collects event log data, analyzes deviant activity, and takes appropriate action.

PURPOSE &Key Features

SIEM is a security management system that combines security information and event management. It helps organizations detect, analyze, and respond to security threats before they harm business operations. SIEM technology collects event log data, analyzes deviant activity, and takes appropriate action.

Why is it Essential

SIEM tools have a number of advantages that can improve a company's overall security posture, including:

- An overview of the main dangers
- Threat detection and reaction in real time
- Monitoring and reporting of regulatory compliance Advanced threat intelligence
- monitoring users, apps, and devices with more transparency

ROLE

The cybersecurity ecosystem of an organisation should include SIEM. In order to streamline security operations, SIEM provides security teams with a central location to gather, combine, and analyse large amounts of data from throughout a business. Additionally, it offers operational features including dashboards that rank threat activity and compliance reporting and incident management.

Qradar

IBM Security® QRadar® SIEM applies machine learning and user behavior analytics to network traffic alongside traditional logs, providing analysts with more accurate, contextualized and prioritized alerts. QRadar SIEM makes threat detection smarter so you can remediate faster while maintaining your bottom line.

Benfits

Use near real-time analytics to intelligently investigate and prioritize high-fidelity alerts based on the credibility, relevance and severity of the risk.
Machine-learning based analytics identify anomalies as potential threat actors against a baseline determined by both individual activity and that of a learned peer group.
QRadar SIEM augments traditional log data by monitoring key network flow data so you increase the scope of protection provided.

Features

Network behavior collection devices
Get a deeper view into your network with supported external flow protocols.
Event log sources
Access more than 450 device support modules (DSM) and more than 370 applications to capture activity across your environment.
AWS integrations
Utilize deep integration with 10 AWS native services to ingest a broad spectrum of AWS logs and network flows into QRadar SIEM.

USE CASES:

Accelerate threat detection
In today's hyperconnected world, cyber criminals act with increasing agility and speed. So too must security teams. IBM Security QRadar SIEM helps teams meet the quick response challenge with automated, near-real-time threat detection.

QRadar SIEM can analyze millions of events in near real time by using thousands of prebuilt use cases, User Behavior Analytics, Network Behavior Analytics, application vulnerability data, and X-Force® Threat Intelligence to deliver high-fidelity alerts.

Detect and respond to ransomware
Ransomware has become one of cybercrime's strongest business models, costing organizations billions of dollars every year. In a ransomware attack, cybercriminals steal or encrypt valuable data and then demand payment for its safe return. These attacks have evolved from a consumer-level nuisance into sophisticated malware with advanced encryption abilities, and no single industry, geography or size of business is immune.

Protecting your organization from ransomware and other types of malware requires a quick response, because with every passing second, more files are encrypted and more devices are infected—driving up both the damage and the cost. IBM Security QRadar SIEM helps you detect these threats rapidly, so you can take immediate, informed action to prevent or minimize the effects of the attack.

Identify and detect cyber threats
Whether researching the latest threat intelligence or expanding on the details of a high priority alert, security analysts often need to search and pinpoint indicators of compromise. They need tools that are easy to use, powerful, fast, and accurate to find. QRadar SIEM normalized event data provides a structure of event properties that allows simple queries to find related attack activity across disparate data sources.

Automate compliance
As cyber attacks become more widespread, proof of cybersecurity compliance becomes increasingly important to clients and governing bodies. However, ensuring compliance often requires cybersecurity teams to act across complex sets of standards and regulations that differ by industry and country. Automation can help.

IBM recognizes the critical importance of compliance and up-to-date certifications for clients relying on its products. IBM Security QRadar SIEM compliance solutions reduce risk and help to manage complex compliance requirements by running your SIEM log data through compliance extension for most regulatory standards free of charge. It also delivers automatic compliance reporting against standards your organization needs to meet.