AI for Cyber Security with IBM Qradar

Assignment-3

Name: MAYANDI VARUN

Assignment Title: 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 experiencewith IBM QRadar, a popular SIEM tool.

Instructions:

1. Introduction to SOC: Begin by providing a comprehensive overview of what a Security Operations Center (SOC) is. Explain its purpose, key functions, and the role it plays in an organization's cybersecurity strategy.

2. SIEM Systems: Explore the concept of Security Information and Event Management (SIEM) systems. Discuss why SIEM is essential in modern cybersecurity and how it helps organizations monitor and respond to security threats effectively.

3. QRadar Overview: Research IBM QRadar and describe its key features, capabilities, and benefits as a SIEM solution. Include information on its deployment options (on-premises vs. cloud).

4. Use Cases: Provide real-world use cases and examples of how a SIEM system like IBM QRadar can be used in a SOC to detect and respond to security incidents

Overview of **Security Operations Center (SOC)**

Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

A SOC acts like the hub or central command post, taking in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside. The proliferation of advanced threats places a premium on collecting context from diverse sources. Essentially, the SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC must decide how they will be managed and acted upon.

Functions of SOC

The function of a security operations team and, frequently, of a security operations center (SOC), is to monitor, detect, investigate, and respond to cyberthreats around the clock. Security operations teams are charged with monitoring and protecting many assets, such as intellectual property, personnel data, business systems, and brand integrity. As the implementation component of an organization's overall cybersecurity framework, security operations teams act as the central point of collaboration in coordinated efforts to monitor, assess, and defend against cyberattacks.

Monitoring and Analysis:

- Continuous monitoring of network traffic and security events.
- Analyzing logs, alerts, and other data sources to identify patterns indicative of security threats.

Incident Detection and Response:

- Detecting security incidents in real-time and generating alerts.
- Investigating incidents to understand the nature and scope of the threat.
- Responding to incidents promptly, containing the threat, and eradicating it from the network.

Threat Intelligence:

- Leveraging threat intelligence sources to stay informed about the latest threats and vulnerabilities.
- Incorporating threat intelligence into security monitoring and incident response processes.

Vulnerability Management:

- Identifying and prioritizing vulnerabilities within the organization's systems.
- Coordinating with IT teams to patch or mitigate vulnerabilities before they can be exploited.

Compliance Monitoring:

- Ensuring that the organization complies with relevant cybersecurity regulations and standards.

Providing documentation and reports for audits and compliance purposes.

User Education and Awareness:

- Educating employees about cybersecurity best practices and potential threats.
- Conducting training programs to enhance the organization's overall security awareness.

Role of SOC in Organization’s Cybersecurity Strategy:

Proactive Threat Detection: SOC's continuous monitoring and analysis help in the proactive detection of security threats, allowing organizations to respond swiftly, minimizing potential damage.

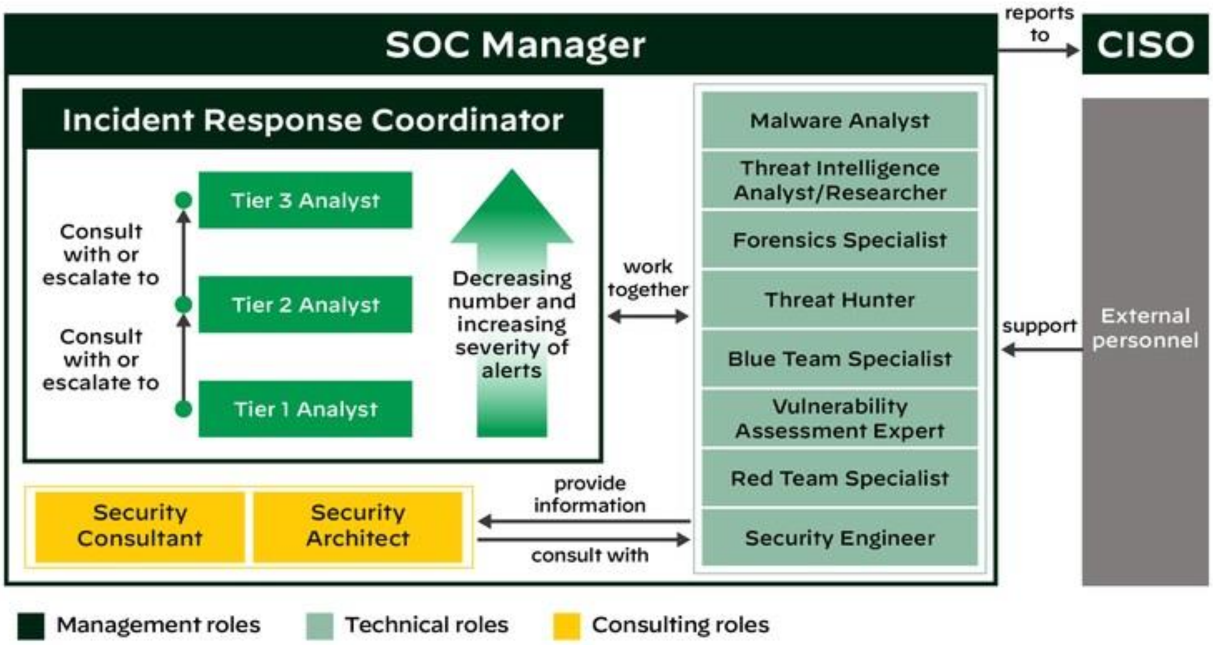
Rapid Incident Response: By quickly identifying and containing security incidents, SOCs mitigate the impact of cyberattacks, reducing downtime and data exposure.

Continuous Improvement: SOC activities provide valuable insights into an organization's security posture. Analysis of incidents and threats leads to continuous improvements in security measures and policies.

Compliance and Risk Management: SOCs ensure that the organization complies with relevant regulations. They also play a crucial role in managing cybersecurity risks effectively.

Resource Optimization: By centralizing cybersecurity efforts, SOCs optimize the use of resources. Skilled professionals and advanced technologies are efficiently utilized to handle a wide range of security challenges.

Enhancing Business Trust: A well-functioning SOC enhances customer and stakeholder trust by demonstrating a strong commitment to cybersecurity. This trust is vital for the reputation and credibility of the organization.

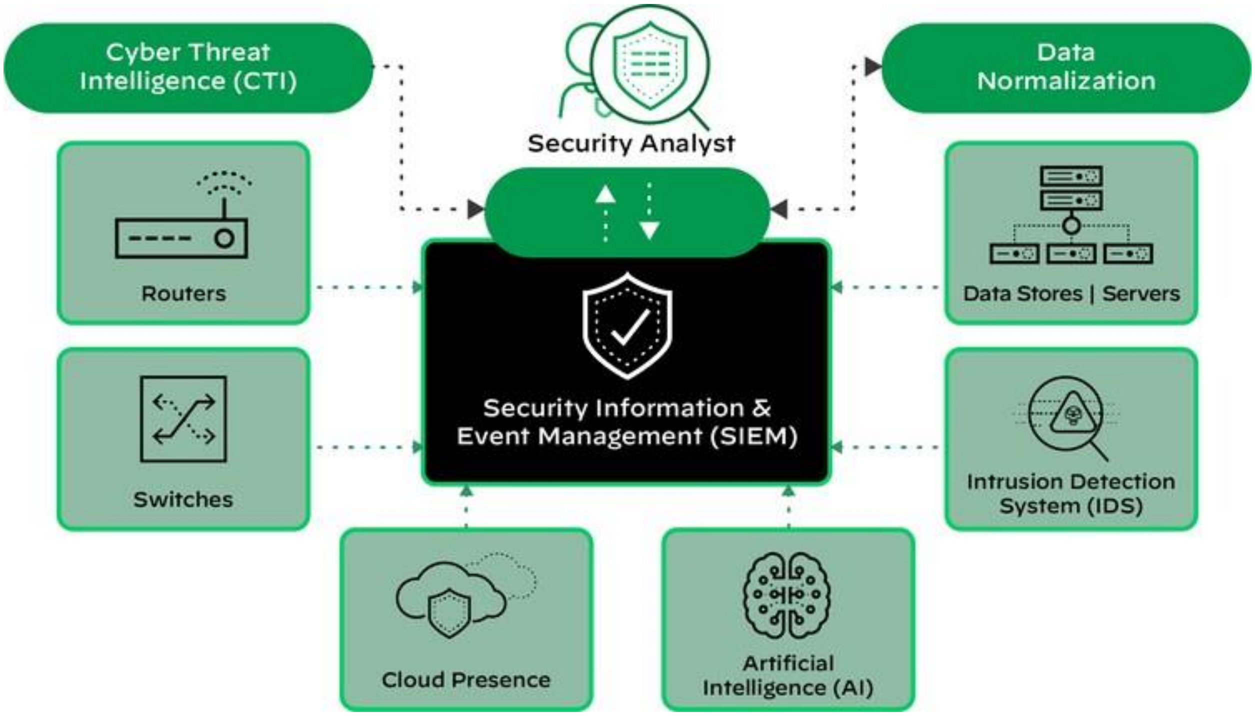


Source: Security Operations Center: A Systematic Study and Open Challenges

Security Information and Event Management (SIEM):

Security information and event management (SIEM) is an approach to security management that combines security information management (SIM) and security event management (SEM) functions into one security management system. It's a comprehensive solution in the realm of cybersecurity that provides real-time analysis of security alerts generated by various hardware and software infrastructures within an organization.

SIEM systems work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers and network equipment, as well as specialized security equipment, such as firewalls, antivirus programs or intrusion prevention systems (IPSes). The collectors forward events to a centralized management console, where security analysts sift through the noise, connecting the dots and prioritizing security incidents.


Cyber Threat Intelligence (CTI)
Security Analyst
Data Normalization
Routers
Data Stores | Servers
Security Information & Event Management (SIEM)
Switches
Intrusion Detection System (IDS)
Cloud Presence
Artificial Intelligence (AI)

Benefits of SIEM Systems:

Threat Detection: SIEM tools can identify patterns of potentially malicious activities in real-time, helping in the early detection of security threats.

Incident Response: They enable organizations to respond quickly and effectively to security incidents by providing detailed information about the nature and scope of the threat.

Compliance Management: SIEM systems assist organizations in meeting regulatory compliance requirements by generating reports and alerts for specific security events.

Log Management: SIEM systems collect and store log data from various sources, providing a centralized platform for log management and analysis.

Forensic Analysis: In case of security breaches, SIEM tools can provide historical data and logs for forensic analysis, helping in understanding the nature and extent of the attack.

Centralized Visibility: SIEM offers a centralized view of an organization's security posture, making it easier to monitor and manage security events and incidents.

Why is SIEM important?

SIEM makes it easier for enterprises to manage security by filtering massive amounts of security data and prioritizing the security alerts the software generates.

SIEM software enables organizations to detect incidents that may otherwise go undetected. The software analyzes the log entries to identify signs of malicious activity. In addition, since the system gathers events from different sources across the network, it can re-create the timeline of an attack, enabling an organization to determine the nature of the attack and its effect on the business.

A SIEM system can also help an organization meet compliance requirements by automatically generating reports that include all the logged security events among these sources. Without SIEM software, the company would have to gather log data and compile the reports manually.

A SIEM system also enhances incident management by helping the company's security team to uncover the route an attack takes across the network, identify the sources that were compromised and provide the automated tools to prevent the attacks in progress.

How does SIEM work?

SIEM tools gather event and log data created by host systems throughout a company's infrastructure and bring that data together on a centralized platform. Host systems include applications, security devices, antivirus filters and firewalls. SIEM tools identify and sort the data into categories such as successful and failed logins, malware activity and other likely malicious activity.

The SIEM software generates security alerts when it identifies potential security issues. Using a set of predefined rules, organizations can set these alerts as a low or high priority.

IBM Security QRadar SIEM is a comprehensive security intelligence platform designed to help organizations manage all the complexities of their security operations processes from one unified platform.

Features

Threat investigation

Threat Investigator works with Case Management to find cases that warrant an investigation and automatically starts investigating. The investigation fetches artifacts attached to the case and starts data mining. After Threat Investigator completes several rounds of data mining, it generates a timeline of the incident that consists of MITRE ATT&CK tactics and techniques plus a chain graph of the incident.

Delivered as SaaS on AWS

The SaaS on AWS delivery method allows you to get up and running quickly, without the need for ongoing updates or management. It enables you to focus on patching important vulnerabilities and reviewing anomalous conditions.

Federated search

Federated search allows you to search data in the cloud or on premises in a single, unified way. You can break down data silos and unlock cross-functional insights with an intuitive search experience that requires no data movement, freeing up IT resources.

Data collection

Data collector makes it possible to get telemetry data set up and ingest with just a few clicks. It supports many protocols, including passive and active. Passive protocols listen for events on specific ports while active protocols use APIs or other communication methods to connect to external telemetry that poll for events.

Detection and response center

The center streamlines the adoption of new use cases by centralizing management of detection and response use cases, reducing complexity and improving efficiency. You can use rules management across cloud or on premises to view, create and adjust with the easy-to-use rule editor.

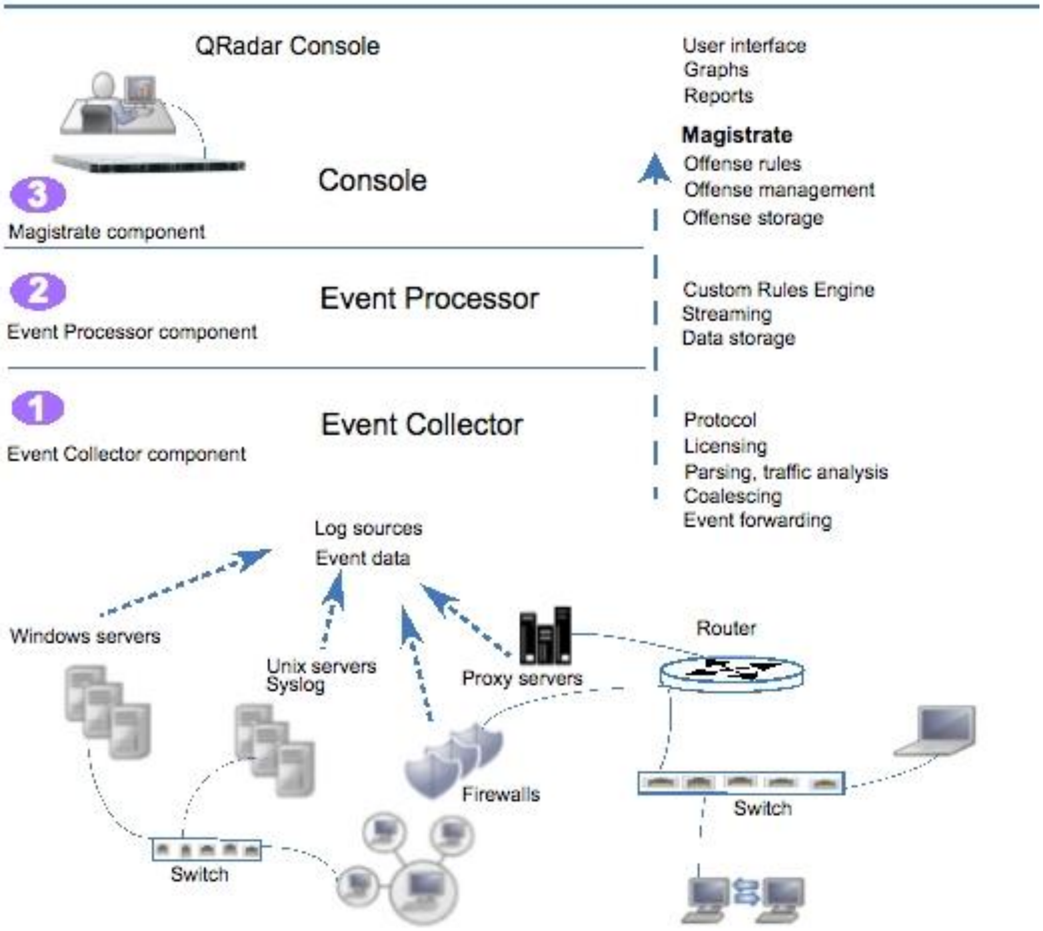
Unified user experience

Integrating across EDR and XDR, Log Insights, SIEM and SOAR products helps you make faster and more accurate decisions. Insights and actions are automatically provided across investigation and response workflows, including the ability to automatically enrich artifacts with threat intelligence, create cases and recommended responses.

Benefits

Accelerate threat response by focusing on alerts that matter

- Use near real-time analytics to intelligently investigate and prioritize high-fidelity alerts based on the credibility, relevance and severity of the risk.
- Identify insider threats and risky user behavior
- 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.
- Get the most out of your network activity with NDR built in QRadar SIEM augments traditional log data by monitoring key network flow data so you increase the scope of protection provided.



Deployment Options:

Available as an on-premises, cloud or SaaS solution, QRadar offers flexible deployment options for today's evolving businesses to deploy security where it is needed most. Featuring advanced analytics, AI-driven investigations, real-time threat detection, and comprehensive IT compliance management, QRadar has all the capabilities your business needs to detect, investigate, prioritize, and respond threats across your entire organizaiton while ensuring your business continuity.

1. On-Premises Deployment:

In an on-premises deployment model, IBM QRadar software and associated components are installed and run on hardware infrastructure within an organization's own data center. This option offers several advantages:

Control: Organizations have full control over their infrastructure, allowing them to customize hardware configurations and network settings according to their specific requirements and security policies.

Security: Some organizations, especially those dealing with sensitive data or operating in highly regulated industries, prefer on-premises deployments because they can maintain end-to-end control over their security measures.

Compliance: On-premises deployment allows organizations to adhere to specific compliance requirements that might mandate keeping certain data within the organization's physical boundaries.

Integration: On-premises deployments can be more easily integrated with existing on-site systems and applications.

However, on-premises deployments also come with challenges such as higher initial costs, ongoing maintenance responsibilities, and the need for a skilled IT team to manage the infrastructure.

2. Cloud Deployment:

Cloud-based deployment options for IBM QRadar involve hosting the software and related services on cloud infrastructure provided by IBM or other cloud service providers. Here are the key points related to cloud deployments:

Scalability: Cloud deployments offer scalability, allowing organizations to scale resources up or down based on demand. This flexibility is particularly useful for handling fluctuating workloads and managing large volumes of data.

Managed Services: Cloud deployments often come with managed services, where the cloud provider handles maintenance, updates, and security patches. This can offload the burden of day-to-day management from the organization's IT staff.

Cost-Efficiency: Cloud deployments can reduce upfront capital expenditures as organizations typically pay for the services on a subscription or pay-as-you-go basis. This can make it more cost-effective, especially for smaller organizations.

Accessibility: Cloud-based QRadar can be accessed from anywhere with an internet connection, allowing security teams to monitor and respond to security incidents remotely.

Integration with Cloud Services: Cloud deployments facilitate integration with other cloud-based services and tools, creating a seamless and integrated security ecosystem.

Disaster Recovery: Cloud providers often have robust disaster recovery mechanisms in place, ensuring data backup and availability even in the case of unexpected events.