Assignment-3

Date- 8/9/2023

Vidit Sharma
21BCY10055

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 experience with IBM QRadar, a popular SIEM tool.

Introduction to SOC:

A security operations center (SOC) – sometimes called an information security operations center, or ISOC – is an in-house or outsourced team of IT security professionals that monitors an organization’s entire IT infrastructure, 24/7, to detect cybersecurity events in real time and address them as quickly and effectively as possible.
An SOC also selects, operates, and maintains the organization’s cybersecurity technologies, and continually analyzes threat data to find ways to improve the organization's security posture.
The chief benefit of operating or outsourcing an SOC is that it unifies and coordinates an organization’s security tools, practices, and response to security incidents. This usually results in improved preventative measures and security policies, faster threat detection, and faster, more effective and more cost-effective response to security threats. An SOC can also improve customer confidence, and simplify and strengthen an organization's compliance with industry, national and global privacy regulations.

Purpose: The function of the security operations center (SOC) is to monitor, prevent, detect, investigate, and respond to cyber threats around the clock.

Key functions performed by the SOC:

1. Take Stock of Available Resources:

The SOC's primary responsibilities involve safeguarding assets, which includes devices, data, and defensive tools. To protect effectively, the SOC needs complete visibility across the network, covering all devices, servers, software, and third-party services. Additionally, the SOC must be well-versed in its cybersecurity toolset and workflows for optimal efficiency.

2. Preparation and Preventative Maintenance:

The SOC focuses on both preparation and preventative maintenance to enhance security:

- **Preparation:** SOC members stay updated on security trends, research emerging threats, create security roadmaps, and develop disaster recovery plans.

- **Preventative Maintenance:** This involves actions like regular system maintenance, updates, firewall policy updates, patching vulnerabilities, and securing applications to make attacks more difficult.

3. Continuous Proactive Monitoring:

The SOC employs continuous proactive monitoring using tools like SIEM, EDR, SOAR, or XDR to scan the network 24/7. This enables immediate detection of abnormalities and emerging threats, improving response times and reducing human analysis through behavioural analysis.

4. Alert Ranking and Management:

When monitoring tools issue alerts, it is the responsibility of the SOC to look closely at each one, discard any false positives, and determine how aggressive any actual threats are and what they could be targeting. This allows them to triage emerging threats appropriately, handling the most urgent issues first.

5. Threat Response:

These are the actions most people think of when they think of the SOC. As soon as an incident is confirmed, the SOC acts as first responder, performing actions like shutting down or isolating endpoints, terminating harmful processes (or preventing them from executing), deleting files, and more. The goal is to respond to the extent necessary while having as small an impact on business continuity as possible.

6. Recovery and Remediation:

In the aftermath of an incident, the SOC will work to restore systems and recover any lost or compromised data. This may include wiping and restarting endpoints, reconfiguring systems or, in the case of ransomware attacks, deploying viable backups in order to circumvent the ransomware. When successful, this step will return the network to the state it was in prior to the incident.

7. Log Management:

The SOC manages logs, collecting and reviewing network activity and communication logs organization-wide. This data establishes a baseline, detects threats, and aids in incident response and forensics, often with the help of SIEM for data aggregation and correlation.

8. Root Cause Investigation:

In the aftermath of an incident, the SOC is responsible for figuring out exactly what happened when, how and why. During this investigation, the SOC uses log data and other information to trace the problem to its source, which will help them prevent similar problems from occurring in the future.

9. Security Refinement and Improvement:

Cybercriminals are constantly refining their tools and tactics—and in order to stay ahead of them, the SOC needs to implement improvements on a continuous basis. During this step, the plans outlined in the Security Road Map come to life, but this refinement can also include hands-on practices such as red-teaming and purple-teaming.

10. Compliance Management:

The SOC ensures compliance with industry and regulatory standards (e.g., GDPR, HIPAA, PCI DSS) by conducting regular audits and adhering to best practices, safeguarding data and minimizing legal and reputational risks from breaches.

What are the roles and responsibilities of a Security Operations Center (SOC)?

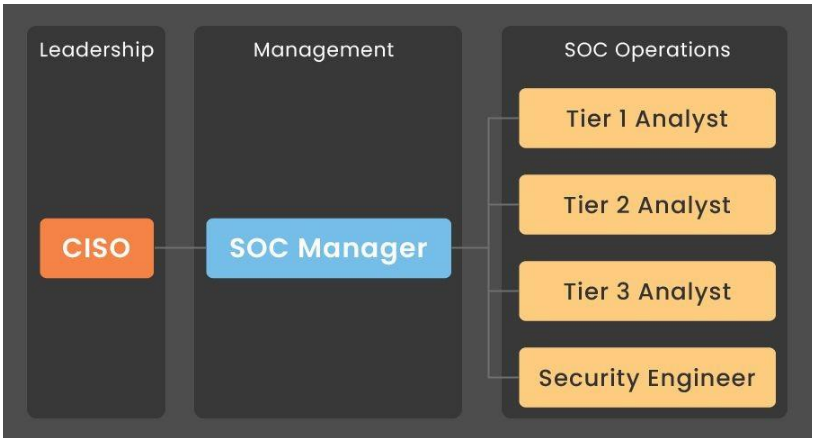
SOCs were created to facilitate collaboration among security personnel, with a primary focus on security monitoring and alerting, including the collection and analysis of data to identify suspicious activity and improve the organization's security.
A SOC can streamline the security incident handling process as well as help analysts triage and resolve security incidents more efficiently and effectively. In today’s digital world, a SOC can be located in-house, in the cloud (a virtual SOC), staffed internally, outsourced (e.g., to an MSSP or MDR) or a mix of these.
SOCs can provide continuous protection with uninterrupted monitoring and visibility into critical assets across the attack surface. They can provide a fast and effective response, decreasing the time elapsed between when the compromise first occurred and the mean time to detection.

Security Analyst: Security Analysts ensures that the proper training is in place and that staff follow procedures and policies. Security Analysts work together with the internal IT team and business administrators to communicate about security limitations and produce documentation or reports. The average salary of a Security Analyst is 6 lakh per year.

Security Engineer/ Architect: They maintain and suggest monitoring and analysis tools. They build a security architecture and work with developers to secure this architecture. They can be a software or hardware specialist who gives appropriate attention to security aspects when producing information systems. They produce tools and solutions that allow organizations to respond efficiently to attacks. A Security Engineer can earn an average 7.48 lakh per year.

SOC Manager: The SOC Manager manages the security operations team and reports to the CISO (Chief Information Security Officer). They control the security team, give technical guidance, and also maintain financial activities. The SOC Manager supervises the activities of the SOC team, including hiring, training, and assessing staff. A SOC Manager can earn 44 lakh per year.

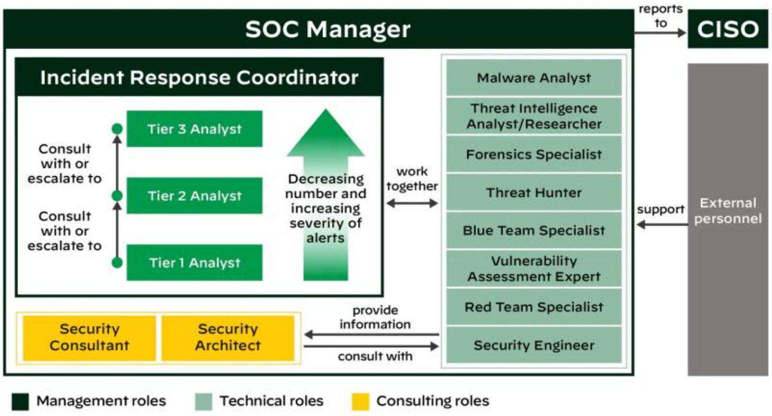
CISO: They define the security operations of the organization. They interact with management about security issues and compliance tasks. The CISO gives a final look at policies, strategies, and procedures relating to the organization’s cybersecurity. They also have a primary role in compliance, risk management, and implement policies to meet particular security demands. A CISO can earn 52 lakh per year.



Tier 1 SOC Analysts monitor user activity and security signals, identifying potential threats.

Tier 2 Analysts remediate attacks, collect data for analysis, and investigate security incidents, restoring system operations.

Tier 3 Analysts proactively assess vulnerabilities, conduct penetration tests, update security systems, and enhance overall security strategies.



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

SIEM Systems:

Security information and event management, SIEM for short, is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations.
SIEM, pronounced “sim,” combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action.
In short, SIEM gives organizations visibility into activity within their network so they can respond swiftly to potential cyberattacks and meet compliance requirements.
In the past decade, SIEM technology has evolved to make threat detection and incident response smarter and faster with artificial intelligence.

How does SIEM work?

At the most basic level, all SIEM solutions perform some level of data aggregation, consolidation and sorting functions in order to identify threats and adhere to data compliance requirements. While some solutions vary in capability, most offer the same core set of functionality:

1. **Log Management:**

SIEM collects and analyzes event data from various sources, both on-premises and in the cloud, including users, endpoints, applications, networks, and security tools. It can also integrate with threat intelligence feeds to identify and respond to known threats.

2. **Event Correlation and Analytics:**

Event correlation in SIEM uses advanced analytics to identify and mitigate potential threats, improving mean time to detect (MTTD) and mean time to respond (MTTR) for IT security teams by automating complex analysis.

3. **Incident Monitoring and Security Alerts:**

SIEM provides a centralized dashboard for monitoring, alert triaging, threat identification, and rapid response. It includes real-time visualizations to highlight unusual activity and uses predefined rules to trigger immediate alerts and threat mitigation.

4. **Compliance Management and Reporting:**

SIEM assists organizations with compliance by automating data collection and generating real-time reports for standards like PCI-DSS, GDPR, HIPAA, and SOX, streamlining security management and early violation detection. It often includes pre-built add-ons for compliance reporting.

SIEM is essential in modern cybersecurity

Proactive IT security risk monitoring is crucial for all organizations, regardless of size. SIEM solutions streamline security workflows and offer significant benefits by centralizing data, detecting threats, and facilitating rapid response.

1. Real-time threat recognition-

SIEM solutions provide real-time threat recognition and streamline compliance auditing and reporting for an organization's entire infrastructure. They employ advanced automation to efficiently collect and analyze system logs and security events, reducing the strain on internal resources and ensuring compliance with reporting standards.

2. AI-driven automation-

Modern SIEM solutions integrate with AI-driven automation, such as SOAR systems, to save time and resources. These systems use machine learning to swiftly identify and respond to threats, outpacing traditional methods and improving business security.

3. Improved organizational efficiency-

SIEM enhances interdepartmental efficiencies by offering improved visibility of IT environments. Its central dashboard consolidates data, alerts, and notifications, facilitating seamless communication and collaboration among teams when addressing security threats and incidents.

4. Detecting advanced and unknown threats-

SIEM solutions, with integrated threat intelligence and AI technology, enhance an organization's ability to respond effectively to various cyber threats, including:

- Insider Threats: These originate from authorized individuals within the organization who pose security risks.
- Phishing: Deceptive messages targeting users to steal sensitive information.
- Ransomware: Malware that locks data or devices, demanding a ransom.
- DDoS Attacks: Overwhelming network or system traffic to disrupt services.
- Data Exfiltration: Unauthorized data theft, conducted manually or through malware.

SIEM helps organizations adapt to the evolving cybersecurity landscape by detecting and responding to both known and unknown threats.

5. Conducting forensic investigations-

SIEM simplifies computer forensic investigations of post-security incidents. It centralizes log data from all digital assets, enabling efficient analysis to recreate past incidents and investigate suspicious activity, leading to improved security processes.

6. 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.

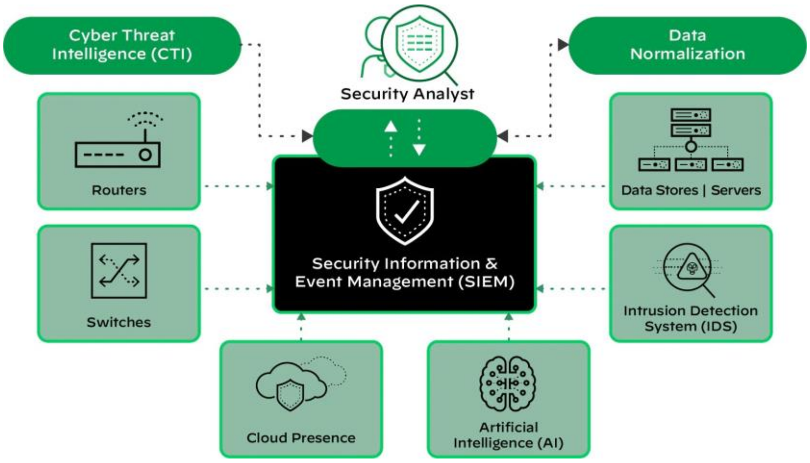
7. Monitoring Users and Applications-

SIEM provides essential visibility for monitoring users and applications, vital in today's remote work and BYOD environment. It tracks network activity across users, devices, and applications, enhancing transparency and detecting threats beyond the traditional network perimeter.

SIEM (Security Information and Event Management) helps organizations monitor and respond to security threats effectively through several key mechanisms:

- Centralized Data Collection: SIEM collects security data from various sources, including servers, endpoints, applications, and network devices, and consolidates it into a single dashboard. This centralized view provides a comprehensive understanding of the organization's digital environment.

- Real-time Analysis: SIEM solutions analyze incoming data in real-time using predefined rules and correlation algorithms. This enables the rapid detection of security incidents and threats as they occur, reducing the mean time to detect (MTTD).
- Alerting and Notifications: SIEM generates alerts and notifications when suspicious activity is detected, enabling security teams to respond promptly to potential threats. This reduces the mean time to respond (MTTR) and minimizes the impact of security incidents.
- Threat Intelligence Integration: Many SIEM solutions integrate with external threat intelligence feeds, allowing organizations to correlate internal security data with known threat signatures and profiles. This enhances the ability to detect emerging threats and vulnerabilities.
- Incident Investigation: SIEM stores extensive log data, which is invaluable for forensic analysis. Security teams can investigate security incidents, identify their root causes, and understand their scope to implement effective remediation strategies.
- Compliance Management: SIEM assists organizations in meeting regulatory compliance requirements by generating real-time compliance reports for standards such as GDPR, HIPAA, and PCI DSS. This simplifies compliance efforts and reduces the risk of non-compliance-related penalties.
- Automation and Orchestration: Modern SIEM solutions often integrate with security orchestration, automation, and response (SOAR) systems, allowing for automated responses to certain threats. This saves time and resources for IT teams.
- Improved Interdepartmental Communication: SIEM's centralized dashboard fosters communication and collaboration among different departments when responding to security threats. It provides a unified view of data, alerts, and notifications.


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)

IBM QRadar:

IBM QRadar is a sophisticated security information and event management (SIEM) solution that helps organizations protect against cybersecurity threats. It centralizes and analyzes data from various sources to detect real-time security incidents, automates responses, and generates compliance reports. QRadar employs advanced analytics, machine learning, and threat intelligence integration to enhance an organization's security posture and incident response capabilities.
It gathers and analyzes data from diverse sources to detect security incidents in real-time, automates responses, and generates compliance reports.
It is a robust tool for proactive cybersecurity management and threat mitigation.

Benefits of IBM QRader-

1. **Unified analyst experience**

An intuitive user interface empowers analysts to work more quickly and efficiently throughout their investigation and response processes, with shared insights and automated actions across products. By using unique, enterprise-grade AI capabilities, analysts can automatically contextualize and prioritize threats.

2. **Cloud delivery, speed and scale**

IBM Security QRadar Suite is offered as a cloud service on AWS, making deployment in cloud environments straightforward. It seamlessly integrates with public cloud and SaaS log data. The suite introduces cloud-native security observability and log management tailored for handling large-scale data, providing lightning-fast searches and swift analytics. This enhances security capabilities in the cloud with ease and speed.

3. **Open platform and pre-built integrations**

The suite brings together core technologies needed in today’s security operation centers, built on an open platform and wide partner ecosystem with more than 900 pre-built integrations for flexibility and choice across IBM and third-party products. It includes native, pre-integrated capabilities for Threat Intelligence, Log Management, EDR, SIEM and SOAR.

Key features of IBM QRader-

1.Threat investigation-

Threat Investigator collaborates with Case Management to identify cases for investigation and initiates the process automatically. It gathers attached artifacts and conducts data analysis. Following multiple rounds of data mining, it produces an incident timeline with MITRE ATT&CK tactics and techniques, along with a visual representation of the incident in a chain graph. This simplifies the process of identifying and addressing potential threats.