SHIVANSHU TIWARI 21BDS0191 ASSIGNMENT-3

Assignment Title: Understanding SOC, SIEM, and Q Radar

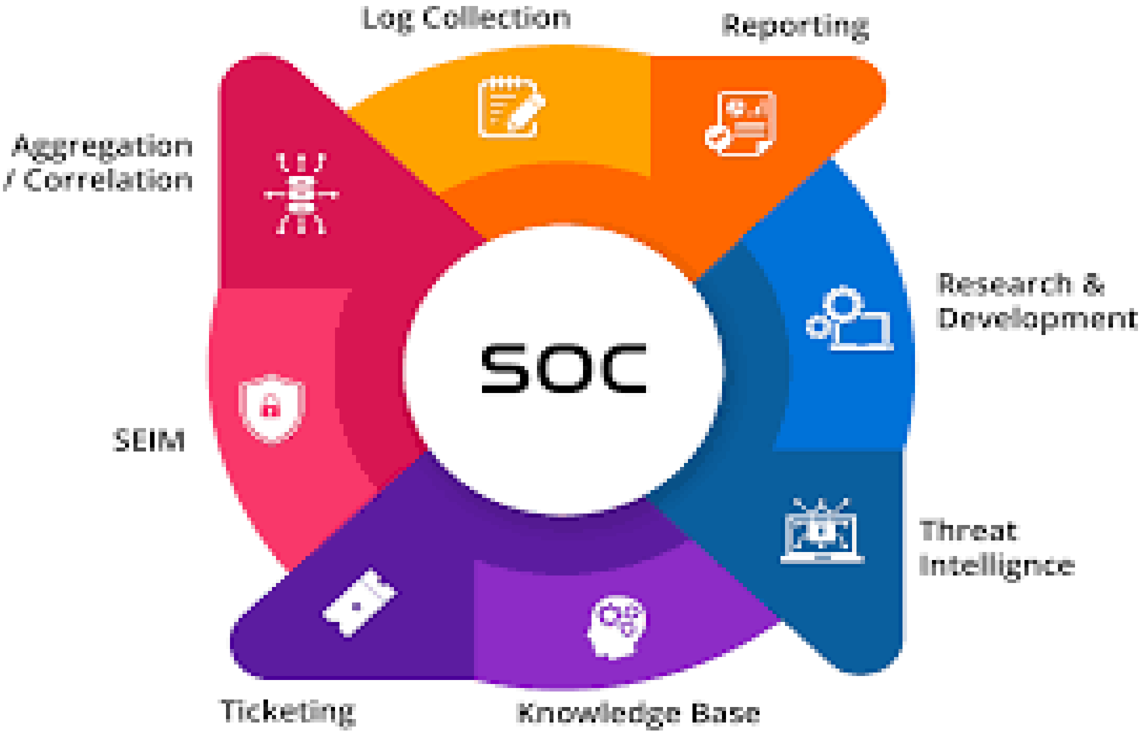
Objective: The objective of this assignment is to explore the concepts of Security Operations Centers

(SOCs), Security Information and Event Management (SIEM) systems, and gain hands-on experience

with IBM QRadar, a popular SIEM tool.

Introduction to SOC- Security Operations Center (SOC)

A security operations center improves an organization's threat detection, response and prevention capabilities by unifying and coordinating all cybersecurity technologies and operations.



SOC headquarters at IBM-

What is a Security Operations Center (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 analyses threat data to find ways to improve the organization's security posture.

Purpose of a SOC: The primary purpose of a SOC is to enhance an organization's cybersecurity posture by proactively identifying and mitigating security threats and incidents. This includes protecting against cyberattacks, data breaches, malware infections, insider threats, and other malicious activities.

What an Security Operations Center (SOC) does-

SOC activities and responsibilities fall into three general categories.

1-Monitoring and Detection:

Continuous Monitoring: The SOC continuously monitors an organization's IT infrastructure, including networks, systems, applications, and data, to identify abnormal or suspicious activities. Security Alerts: It analyzes security alerts generated by various security tools, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, and antivirus software.

Anomaly Detection: SOC analysts use baseline behavior and anomaly detection techniques to identify deviations from normal system or user activity, which could indicate a security threat.

2-Incident Response and Management:

Incident Detection: When a security incident is detected, the SOC initiates the incident response process to investigate . Incident Triage: Analysts assess the severity and scope of the incident, determining if it's a false positive or a genuine threat. Containment and Mitigation: If an incident is confirmed, the SOC takes actions to contain the threat, minimize damage, and prevent further compromise. Forensics and Investigation: Detailed investigations are conducted to understand how the incident occurred, what data or systems were affected, and who may be responsible.

Evidence Preservation: The SOC ensures that digital evidence is preserved for potential legal or law enforcement purposes.

3-*Vulnerability Management and Threat Hunting:*

Vulnerability Assessment: SOC teams assess and prioritize vulnerabilities in the organization's infrastructure and applications. They work to ensure that critical vulnerabilities are remediated promptly.

Patch Management: Updates and patches are applied to systems and software to address known vulnerabilities.

Threat Hunting: SOC personnel proactively search for hidden threats within the organization's environment that may have evaded automated detection systems. They use advanced analytics, threat intelligence, and manual investigations to identify potential threats.

Key Security Operations Center (SOC) team members-

In general, the chief roles on an SOC team include:

The SOC manager-who runs the team, oversees all security operations, and reports to the organization's CISO (chief information security officer).

Security engineers,- who build out and manage the organization's security architecture. Much of this work involves evaluating, testing, recommending, implementing and maintaining security tools and technologies. Security engineers also work with development or DevOps teams to make sure the organization's security architecture is included application development cycles.

- **Security analysts** – also called security investigators or incident responders – who are essentially the first responders to cybersecurity threats or incidents. Analysts detect, investigate, and triage (prioritize) threats; then they identify the impacted hosts, endpoints and users, and take the appropriate actions to mitigate and contain the impact or the threat or incident. (In some organizations, investigators and incident responders are separate roles classified as Tier 1 and Tier 2 analysts, respectively.)

Threat hunters (also called expert security analysts)- specialize in detecting and containing advanced threats – new threats or threat variants that manage to slip past automated defences.

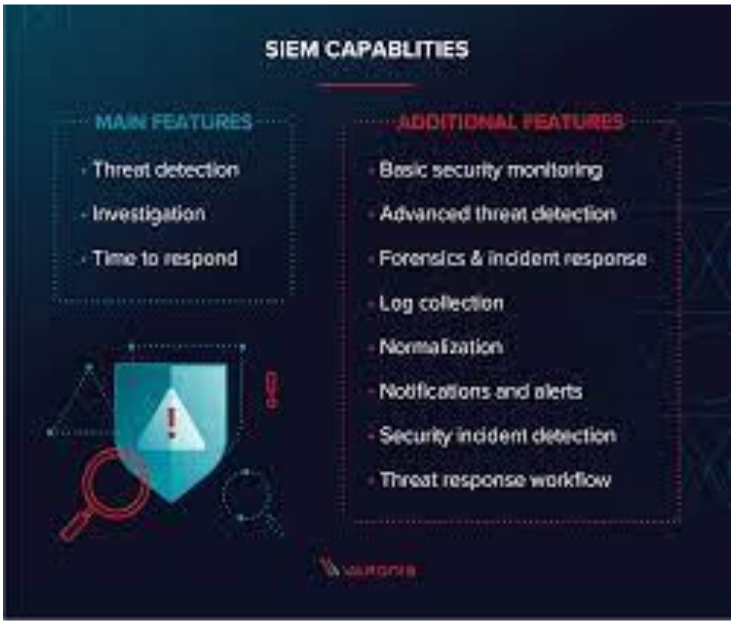
Role in an Organization's Cybersecurity Strategy: The SOC is a critical component of an organization's overall cybersecurity strategy for several reasons:

1. Early Threat Detection: By monitoring systems and networks around the clock, a SOC can detect security threats early, allowing for timely response and mitigation.
2. Reduced Downtime and Damage: Rapid incident response helps minimize downtime and reduces the potential damage caused by cyberattacks.
3. Compliance and Reporting: The SOC ensures that the organization complies with cybersecurity regulations and provides valuable data and reports for audits and regulatory purposes.
4. Continuous Improvement: The SOC's analysis of security incidents and vulnerabilities informs the organization's cybersecurity strategy, helping it adapt to evolving threats.
5. Risk Management: The SOC assists in identifying and prioritizing security risks, allowing the organization to allocate resources effectively to address the most critical threats.

Security information and event management (SIEM)-

What is SIEM-Security Information and Event Management (SIEM) systems are a crucial component of modern cybersecurity strategies. SIEM solutions provide organizations with the capability to monitor, collect, correlate, analyse, and respond to security-related data and events from various sources within their IT infrastructure.

How SIEM WORKS-SIEM works by combining two technologies: a) Security information management (SIM), which collects data from log files for analysis and reports on security threats and events, and b) security event management (SEM), which conducts real-time system monitoring, notifies network admins about important issues and establishes correlations between security events.



SIEM CAPABLITIES

MAIN FEATURES

- Threat detection
- Investigation
- Time to respond

ADDITIONAL FEATURES

- Basic security monitoring
- Advanced threat detection
- Forensics & incident response
- Log collection
- Normalization
- Notifications and alerts
- Security incident detection
- Threat response workflow

The security information and event management process can be broken down as follows:

1. **Data collection** – All sources of network security information, e.g., servers, operating systems, firewalls, antivirus software and intrusion prevention systems are configured to feed event data into a SIEM tool .Most modern SIEM tools use agents to collect event logs from enterprise systems, which are then processed, filtered and sent them to the SIEM. Some SIEMs allow agentless data collection. For example, Splunk offers agentless data collection in Windows using WMI.
2. **Policies –** profile is created by the SIEM administrator, which defines the behaviour of enterprise systems, both under normal conditions and during pre-defined security incidents. SIEMs provide default rules, alerts, reports, and dashboards that can be tuned and customized to fit specific security needs.

3. **Data consolidation and correlation** – SIEM solutions consolidate, parse and analyse log files. Events are then categorized based on the raw data and apply correlation rules that combine individual data events into meaningful security issues.
4. **Notifications –** If an event or set of events triggers a SIEM rule, the system notifies security personnel.

Why SIEM is Essential in Modern Cybersecurity:

Complex Threat Landscape: The cybersecurity threat landscape is constantly evolving, with attackers using increasingly sophisticated techniques. SIEM systems provide the agility and adaptability needed to detect and respond to these evolving threats.

Data Volume and Complexity: Organizations generate vast amounts of security data, making it challenging to manually monitor and analyse. SIEMs automate this process and provide insights from diverse data sources.

Regulatory Requirements: Many industries are subject to strict data protection and privacy regulations. SIEM systems help organizations meet compliance requirements by ensuring proper data handling and reporting.

Rapid Incident Response: SIEMs enable organizations to respond swiftly to security incidents, reducing the potential impact and minimizing downtime.

Threat Intelligence Integration: The integration of threat intelligence data helps organizations proactively identify and mitigate threats based on the latest threat intelligence feeds and known attack patterns.

The Future of SIEM-

Companies usually will express two primary concerns regarding the ability of their existing technologies to handle cybersecurity threats now and in the future. First, SIEM solutions don’t usually support very large workloads (i.e., big data) and struggle to handle the large numbers of alerts and contextual data required. Second, most tools that detect, investigate, and respond to threats are unintuitive.

These concerns are driving new solutions to address the needs of hybrid models, ever-growing data, digital transformations, and cloud-based environments. Modern practices often expose organizations to new threats, with attack surfaces growing alongside expanding systems. There is demand for new disruptive technology.

UEBA revolutionized the SIEM market back in 2013, reducing the risks resulting from the reliance of end-users on correlation rules. Later, innovations such as data lakes helped respond to cloud adoption trends by collecting logs from multiple cloud services. Next, SOAR capabilities and cloud-based SIEM accompanied further changes in market demand.

What is IBM QRADAR-

IBM® Q Radar is a network security management platform that provides situational awareness and compliance support.

Q Radar uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment.

Exploring Q Radar-

Log activity

In IBM Q Radar, you can monitor and display network events in real time or perform advanced searches.

Network activity

In IBM Q Radar you can investigate the communication sessions between two hosts.

Assets

IBM Q Radar automatically creates asset profiles by using passive flow data and vulnerability data to discover your network servers and hosts.

Offenses

In IBM Q Radar you can investigate offenses to determine the root cause of a network issue.

Reports

In IBM Q Radar you can create custom reports or use default reports.

Data collection

IBM Q Radar accepts information in various formats and from a wide range of devices, including security events, network traffic, and scan results.

Q Radar rules

Rule perform tests on events, flows, or offenses. If all the conditions of a test are met, the rule generates a response.

Supported web browsers

For the features in IBM Q Radar products to work properly, you must use a supported web browser.

Apps overview

IBM Q Radar apps are created by developers. After a developer creates an app, IBM certifies and publishes it in the IBM Security App Exchange. Q Radar administrators can then browse and download the apps and then install the apps into Q Radar to address specific security requirements.

Apps that are installed by default with Q Radar

To improve workflow, some apps that were previously only available on the IBM Security App Exchange are now installed by default.

SUPPORTED WEB BROWSERS-For the features in IBM® Q Radar® products to work properly, you must use a supported web browser.

Web browser	Supported versions
64-bit Mozilla Firefox	-60 Extended Support -- Release and later
64-bit Microsoft Edge	38.14393 and later
64-bit Google Chrome	Latest

Key Features and Capabilities:

1. **Log and Event Data Collection**: Q Radar can collect and normalize log and event data from various sources, including network devices, servers, applications, cloud services, and security appliances.
2. **Real-time Event Correlation:** It employs advanced event correlation techniques to identify security incidents by correlating data from multiple sources. This helps in detecting complex attack patterns and threats.
3. **Threat Detection and Alerts**: Q Radar uses rule-based detection, anomaly detection, and behavioral analytics to identify potential security threats. When a threat is detected, it generates alerts and notifications for immediate action.
4. **Vulnerability Management:** It integrates vulnerability data to help organizations prioritize and remediate vulnerabilities that could be exploited by attackers.
5. **Incident Response:** Q Radar offers incident investigation and workflow capabilities, allowing security teams to investigate and respond to incidents more efficiently. Automated response actions can also be configured.

6. **User and Entity Behaviour Analytics (UEBA):** Q Radar can analyse user and entity behaviour to detect insider threats and compromised accounts by identifying unusual or suspicious activities.

Benefits of IBM Q Radar:

1. **Comprehensive Threat Detection**: Q Radar's advanced analytics and correlation capabilities enable organizations to detect both known and unknown threats effectively.
2. **Rapid Incident Response:** It helps security teams respond quickly to security incidents, minimizing potential damage.
3. **Scalability:** Q Radar is highly scalable and suitable for organizations of all sizes, from small businesses to large enterprises.
4. **Integration**: It integrates seamlessly with other IBM security products and third-party security solutions, creating a unified security ecosystem.
5. **Reduced False Positives:** Advanced analytics and machine learning help reduce false positives, allowing security teams to focus on real threats.
6. **Flexibility in Deployment**: Q Radar offers both on-premises and cloud deployment options, providing flexibility based on an organization's preferences and requirements.

Deployment Options:

IBM Q Radar offers two primary deployment options:

1. **On-Premises:** Organizations can deploy Q Radar on their own hardware infrastructure within their data centers. This option provides complete control over the hardware and security policies.
2. **Cloud:** IBM also offers Q Radar on Cloud, a fully managed cloud-based SIEM solution hosted on IBM Cloud infrastructure. This option is attractive for organizations looking to offload infrastructure management and benefit from cloud scalability.

Now we will see Real-world use cases and examples of how a SIEM system like IBM Q Radar can be used in a SOC to detect and respond to security incidents-

User and Entity Behaviour Analytics (UEBA):

Use Case: Q Radar can analyse user and entity behaviour to detect insider threats or compromised accounts.

Example: Q Radar can identify unusual access patterns by an employee who is accessing sensitive files outside their typical working hours.

Vulnerability Assessment Integration:

Use Case: Q Radar can integrate with vulnerability assessment tools to prioritize security patches based on the real-world risk.

Example: Q Radar can correlate detected vulnerabilities with active threats, allowing the SOC to focus on patching critical systems first.

Forensic Analysis:

Use Case: Q Radar can provide detailed historical logs and data for forensic investigations.

Example: In the event of a data breach, Q Radar can help trace the attacker's steps and identify the entry point and affected systems.

Compliance Monitoring and Reporting:

Use Case: Q Radar can assist in meeting regulatory compliance requirements by monitoring and reporting on security events.

Example: Q Radar can generate reports to demonstrate compliance with regulations like GDPR, HIPAA, or PCI DSS.

Insider Threat Detection:

Use Case: Q Radar can monitor user activities to identify potentially malicious actions by employees or contractors.

Example: If an employee starts copying sensitive files to a USB drive, Q Radar can generate an alert and initiate an investigation.

DDoS Attack Detection and Mitigation:

Use Case: Q Radar can identify and respond to Distributed Denial of Service (DDoS) attacks by analysing traffic patterns.

Example: Upon detecting a sudden surge in traffic from multiple sources, Q Radar can activate DDoS mitigation measures.

Conclusion of my assignment-

1-We studied about Security organization center (SOC), its features, uses, details of it.

2-We studied about Security Information and Event Management (SIEM)systems. and why SIEM is essential in modern cybersecurity

3- We studied about IBM Q Radar and described its key features, capabilities, and benefits as a SIEM solution. Include information on its deployment options (on-premises vs. cloud)