NAME – **MILAN RATH**

UNDERSTANDING SOC, SIEM, and QRadar.

Let's First talk about QRadar….

QRadar is a tool that provides security information and how we manage that information. It collects security vulnerabilities, operating system applications, network data, and all sorts of activities the host machine does. It generally performs organization or MNC companies. It uses this data to provide a piece of factual information and alert them to respond to network threats.

THERE ARE SOME KEY FEATURES OF QRADAR.

1) **IT HELP USER TO ANALYZE THREAT FASTER AND ALERT ORGANISATION TO CATCH THE THREATS.**
2) **IT HAS REAL-TIME THREAT DETECTION.**
3) **QRADAR USES A POSTGRESQL DATABASE AS A DATA STORE.**
4) **QRADAR IS SCALABLE AND EASY TO USE.**
5) **IT HAS MANY DASHBOARDS TO WRITE CODES OR WRITE DIFFERENT SCRIPTS TO GET THE INFORMATION YOU NEED.**

BENEFITS OF SIEM SOLUTION…

- **Increased efficiency.**
- **Fewer potential security breaches.**
- **We have reduced security event impact.**
- **Lower costs.**
- **Better reporting, log collection, analysis, and retention.**
- **Enhanced compliance.**

Information On Its Deployment Options On-Premises vs. Cloud

An on-premises data center is a group of servers you privately own and control. Traditional cloud computing (as opposed to hybrid or private cloud computing models) involves leasing data center resources from a third-party service provider.

On-premise deployment is when data is stored on your own servers, and you install and manage the software. An on-premise software infrastructure means that all the software is stored on your hardware on your company's premises. This requires your company's IT department to maintain the infrastructure independently.

Types of Cloud Computing Deployment Models

- **Public Cloud.**
- **Private Cloud.**
- **Hybrid Cloud.**
- **Community Cloud.**
- **Multi-Cloud.**

INTRODUCTION TO SOC…….

A security operations center (SOC) is a centralized unit that monitors and protects an organization from cyber attacks. SOCs also work to restore systemsand recover any lost or compromised data.

KEY FUNCTIONS…

- **taking stock of available resources**
- **Preparation and preventative maintenance**
- **Continuous proactive monitoring**
- **Alert ranking and management**

- **Threat response**
- **Recovery and remediation**
- **Log management**
- **Root cause investigation**

ROLE PLAY IN CYBERSECURITY…

- **Monitoring and protecting an organization's assets, including intellectual property, personnel data, business systems, and brand integrity.**
- **Preventing, detecting, analyzing, and responding to cybersecurity incidents.**
- **Collecting and analyzing data to identify suspicious activity and improve the organization's security.**
- **Investigating potential incidents.**

SIEM SYSTEM….

CONCEPT OF SECURITY INFORMATION AND EVENT MANAGEMENT.

Security information and event management (SIEM) is a security management system that combines security information management (SIM) and security event management (SEM). SIEM systems collect event log data from multiple sources, analyze it in real-time, and take appropriate action.
SIEM systems provide a holistic view of an organization's information security.

SIEM systems help organizations recognize potential security threats and vulnerabilities before they have a chance to disrupt. They can also help organizations:

- **Streamline compliance reporting**
- **Detect incidents that would otherwise not be detected**

- **Improve the efficiency of incident handling**

The primary component of a SIEM tool is the Log Collection component. This component collects all the logs from the end devices using different sets of protocols. The log collection protocol will differ based on the device type.

WHY SIEM IS IMPORTANT FOR MODERN

Security Information and Event Management (SIEM) software helps organizations manage security by filtering and prioritizing security alerts. SIEM software collects and analyzes log data from digital assets in one place. This allowsorganizations to:

- **Recreate past incidents**
- **Investigate suspicious activity**
- **Identify unusual activity**
- **Respond quickly to incidents**

KEY ROLE OF SIEM FOR CYBERSECURITY

SIEM tools collect data from a variety of sources, including:

- **Host systems**
- **Networks**
- **Firewalls**
- **Antivirus security devices**

SIEM tools can help organizations strengthen their security posture as they scale. However, SOC analysts may spend a significant amount of time configuring and integrating an SIEM solution with their existing security architecture.

#) some real-world use cases of how the IBM Security Information and Event Management (SIEM) system can be used in a Security Operations Center (SOC) to detect and respond to security incidents.

- **Detecting unauthorized access SIEM can be used to detect unauthorized access to systems and data by monitoring for anomalous activity, such as failed login attempts, suspicious file access, and unusual network traffic. For example, SIEM can be configured to alert SOC analysts if a user attempts to log in to a system from an unusual location or if a user accesses a file that they are not authorized to access.**
- **Detecting malware infections SIEM can be used to detect malware infections by monitoring for suspicious activity on systems and networks. For example, SIEM can be configured to alert SOC analysts if a system is sending out a large number of spam emails or if a network connection is being made to a known malicious IP address.**
- **Detecting data breaches SIEM can be used to detect data breaches by monitoring for unusual patterns of data access and transfer. For example, SIEM can be configured to alert SOC analysts if a large amount of data is being transferred from a system to an external location or if a user is accessing a large number of sensitive files.**
- **Detecting insider threats SIEM can be used to detect insider threats by monitoring for suspicious activity by users who have access to systems and data. For example, SIEM can be configured to alert SOC analysts if a user downloads a large amount of data from a system or if a user attempts to access a system that they have not accessed before.**

In addition to these specific use cases, SIEM can also be used to:

- **Improve visibility into security events SIEM provides a centralized view of security events from across an organization's systems and networks. This can help SOC analysts to identify and respond to security incidents more quickly and effectively.**
- **Automate security incident response SIEM can be used to automate certain aspects of security incident response, such as isolating infected systems and blocking malicious traffic. This can help SOC analysts to respond to security incidents more quickly and efficiently.**
- **Generate security reports SIEM can be used to generate security reports that can be used to identify trends and patterns in security events. This information can be used to improve the organization's security posture and to identify areas where additional security controls are needed.**

IBM Security SIEM is a popular choice for SOCs because it offers a wide range of features and capabilities that can help organizations to detect and respond to security incidents more effectively. IBM Security SIEM also integrates with a wide range of other security solutions, which can help organizations to build a comprehensive security infrastructure.