Name :- M Om Nivas Reg no :- 21BCE9706

E-Mail :- omnivas.21bce9706@vitapstudent.ac.in

Understanding SOC, SIEM, and QRadar

Weekly

Assignment – 3

Security Operations Centers (SOCs) :-

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 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.

What an Security Operations Center (SOC) does

Preparation, planning and prevention

Asset inventory. An SOC needs to maintain an exhaustive inventory of everything that needs to be protected, inside or outside the data center (e.g. applications, databases, servers, cloud services, endpoints, etc.) and all the tools used to protect them (firewalls, antivirus/anti-malware/anti-ransomware tools, monitoring software, etc). Many SOCs will use an asset discovery solution for this task.

Routine maintenance and preparation. To maximize the effectiveness of security tools and measures in place, the SOC performs preventative maintenance such as applying software patches and upgrades, and continually updating firewalls, whitelists and blacklists, and security policies and procedures. The SOC may also create system back-ups – or assist in creating back-up policy or procedures – to ensure business continuity in the event of a data breach, ransomware attack or other cybersecurity incident.

Incident response planning. The SOC is responsible for developing the organization's incident response plan, which defines activities, roles, responsibilities in the event of a threat or incident – and the metrics by which the success of any incident response will be measured.

Regular testing. The SOC team performs vulnerability assessments – comprehensive assessments that identify each resource's vulnerability to potential threats, and the associate costs. It also conducts penetration tests that simulate specific attacks on one more systems. The team remediates or fine-tunes applications, security policies, best practices and incident response plans based on the results of these tests.

Staying current. The SOC stays up to date on the latest security solutions and technologies, and on the latest threat intelligence – news and information about cyberattacks and the hackers of perpetrate them, gathered from social media, industry sources, and the dark web.

Monitoring, detection and response

Log management – the collection and analysis of log data generated by every network event – is a subset of monitoring that's important enough to get its own paragraph. While most IT departments collect log data, it's the analysis that establishes normal or baseline activity, and reveals anomalies that indicate suspicious activity. In fact, many hackers count on the fact that companies don't always analyze log data, which can allow their viruses and malware to run undetected for weeks or even months on the victim's systems. Most SIEM solutions include log management capability.

Incident response. In response to a threat or actual incident, the SOC moves to limit the damage. Actions can include:

• Root cause investigation, to determine the technical vulnerabilities that gave hackers access to the system, as well as other factors (such as bad password hygiene or poor enforcement of policies) that contributed to the incident

• Shutting down compromised endpoints or disconnecting them from the network

• Isolating compromised areas of the network or rerouting network traffic

• Pausing or stopping compromised applications or processes

• Deleting damaged or infected files

• Running antivirus or anti-malware software

• Decommissioning passwords for internal and external users.

Many XDR solutions enable SOCs to automate and accelerate these and other incident responses.

Security Information and Event Management (SIEM) systems :-

SIEM Defined

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 do SIEM tools work?

SIEM tools collect, aggregate, and analyze volumes of data from an organization’s applications, devices, servers, and users in real-time so security teams can detect and block attacks. SIEM tools use predetermined rules to help security teams define threats and generate alerts

SIEM capabilities and use cases

SIEM systems vary in their capabilities but generally offer these core functions:

- Log management: SIEM systems gather vast amounts of data in one place, organize it, and then determine if it shows signs of a threat, attack, or breach.
- Event correlation: The data is then sorted to identify relationships and patterns to quickly detect and respond to potential threats.
- Incident monitoring and response: SIEM technology monitors security incidents across an organization's network and provides alerts and audits of all activity related to an incident.

SIEM systems can mitigate cyber risk with a range of use cases such as detecting suspicious user activity, monitoring user behavior, limiting access attempts and generating compliance reports.

Benefit of using a SIEM

SIEM tools offer many benefits that can help strengthen an organization's overall security posture, including:

- A central view of potential threats
- Real-time threat identification and response
- Advanced threat intelligence
- Regulatory compliance auditing and reporting
- Greater transparency monitoring users, applications, and devices

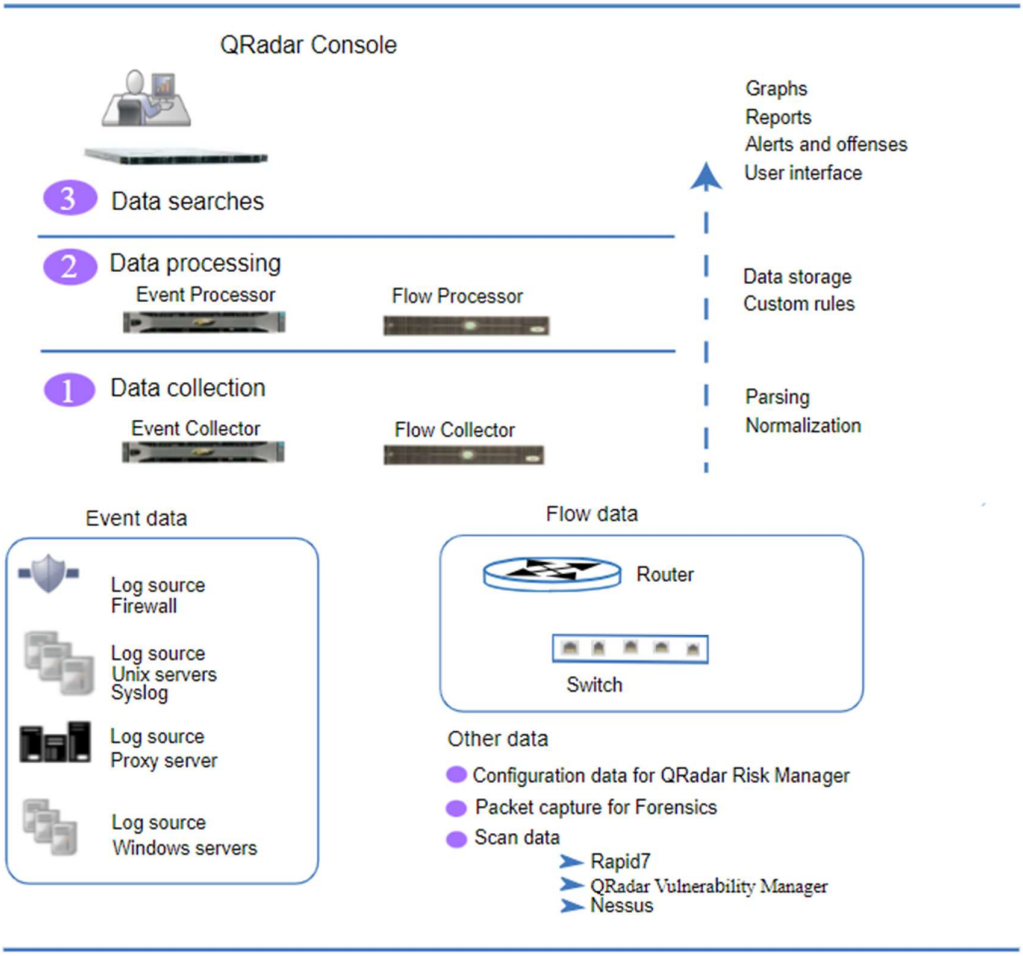
gain hands-on experience with IBM QRadar :-

QRadar architecture overview

When you plan or create your IBM® QRadar® deployment, it's helpful to have a good awareness of QRadar architecture to assess how QRadar components might function in your network, and then to plan and create your QRadar deployment.

IBM QRadar collects, processes, aggregates, and stores network data in real time. QRadar uses that data to manage network security by providing real-time information and monitoring, alerts and offenses, and responses to network threats.

IBM QRadar SIEM (Security Information and Event Management) is a modular architecture that provides real-time visibility of your IT infrastructure, which you can use for threat detection and prioritization. You can scale QRadar to meet your log and flow collection, and analysis needs. You can add integrated modules to your QRadar platform, such as QRadar Risk Manager, QRadar Vulnerability Manager,and QRadar Incident Forensics.



Data collection

Data collection is the first layer, where data such as events or flows is collected from your network. The All-in-One appliance can be used to collect the data directly from your network or you can use collectors such as QRadar Event Collectors or QRadar QFlow Collectors to collect event or flow data. The data is parsed and normalized before it passed to the processing layer. When the raw data is parsed, it is normalized to present it in a structured and usable format.

The core functionality of QRadar SIEM is focused on event data collection, and flow collection.

Event data represents events that occur at a point in time in the user's environment such as user logins, email, VPN connections, firewall denys, proxy connections, and any other events that you might want to log in your device logs.

Flow data is network activity information or session information between two hosts on a network, which QRadar translates in to flow records. QRadar translates or normalizes raw data in to IP addresses, ports, byte and packet counts, and other information into flow records, which effectively represents a session between two hosts. In addition to collecting flow information with a Flow Collector, full packet capture is available with the QRadar Incident Forensics component.

Data processing

After data collection, the second layer or data processing layer is where event data and flow data are run through the Custom Rules Engine (CRE), which generates offenses and alerts, and then the data is written to storage.

Event data, and flow data can be processed by an All-in-One appliance without the need for adding Event Processors or Flow Processors. If the processing capacity of the All-in-One appliance is exceeded, then you might need to add Event Processors, Flow Processors or any other processing appliance to handle the additional requirements. You might also need more storage capacity, which can be handled by adding Data Nodes.

Other features such as QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM), or QRadar Incident Forensics collect different types of data and provide more functions.

QRadar Risk Manager collects network infrastructure configuration, and provides a map of your network topology. You can use the data to manage risk by simulating various network scenarios through altering configurations and implementing rules in your network.

Use QRadar Vulnerability Manager to scan your network and process the vulnerability data or manage the vulnerability data that is collected from other scanners such as Nessus, and Rapid7. The vulnerability data that is collected is used to identify various security risks in your network.

Use QRadar Incident Forensics to perform in-depth forensic investigations, and replay full network sessions.

Data searches

In the third or top layer, data that is collected and processed by QRadar is available to users for searches, analysis, reporting, and alerts or offense investigation. Users can search, and manage the security admin tasks for their network from the user interface on the QRadar Console.

In an All-in-One system, all data is collected, processed, and stored on the All-in-One appliance.

In distributed environments, the QRadar Console does not perform event and flow processing, or storage. Instead, the QRadar Console is used primarily as the user interface where users can use it for searches, reports, alerts, and investigations.

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.

As enterprises pursue digital transformation, they face increasing danger from cybersecurity threats. COVID-19 has caused a massive increase in the number of vulnerable endpoints for remote workers.

END