-> Exploring about SOC,SIEM and QRADAR :-

- 1.) Security Operation 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.

The function of a security operations teams and, that 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.

- The 10 key functions performed by the SOC :

- 1. Take Stock of Available Resources :

The SOC is responsible for two types of assets—the various devices, processes and applications they're charged with safeguarding, and the defensive tools at their disposal to help ensure this protection.

- 2. Preparation and Preventative Maintenance :

Even the most well-equipped and agile response processes are no match for preventing problems from occurring in the first place. To help keep attackers at bay, the SOC implements preventative measures, which can be divided into two main categories.

- 3. Continuous Proactive Monitoring :

Tools used by the SOC scan the network 24/7 to flag any abnormalities or suspicious activities. Monitoring the network around the clock allows the SOC to be notified immediately of emerging threats, giving them the best chance to prevent or mitigate harm. Monitoring tools can include a SIEM or an EDR, better even a SOAR or an XDR, the most advanced of which can use behavioral analysis to “teach” systems the difference between regular day-to-day operations and actual threat behavior, minimizing the amount of triage and analysis that must be done by humans.

- 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 ransomeware 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 is responsible for collecting, maintaining, and regularly reviewing the log of all network activity and communications for the entire organization. This data helps define a baseline for “normal” network activity, can reveal the existence of threats, and can be used for remediation and forensics in the aftermath of an incident. Many SOCs use a SIEM to aggregate and correlate the data feeds from applications, firewalls, operating systems and endpoints, all of which produce their own internal logs.

- 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 :

Many of the SOC's processes are guided by established best practices, but some are governed by compliance requirements. The SOC is responsible for regularly auditing their systems to ensure compliance with such regulations, which may be issued by their organization, by their industry, or by governing bodies. Examples of these regulations include GDPR, HIPAA, and PCI DSS. Acting in accordance with these regulations not only helps safeguard the sensitive data that the company has been entrusted with—it can also shield the organization from reputational damage and legal challenges resulting from a breach.

- ## 2.) Security Information and Event Management :-

SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. SIEM systems help enterprise security teams detect user behavior anomalies and use artificial intelligence to automate many of the manual processes associated with threat detection and incident response.

The original SIEM platforms were log management tools, combining security information management and security event management to enable real-time monitoring and analysis of security-related events, as well as tracking and logging of security data for compliance or auditing purposes.

Over the years, SIEM software has evolved to incorporate user and entity behavior analytics(UEBA), as well as other advanced security analytics, AI and machine learning capabilities for identifying anomalous behaviors and indicators of advanced threats. Today SIEM has become a staple in modern-day security operation centers(SOC’s) for security monitoring and compliance management use cases.

- ## The Benefits of SIEM :

- 1.) Real-time threat recognition :

SIEM solutions enable centralized compliance auditing and reporting across an entire business infrastructure. Advanced automation streamlines the collection and analysis of system logs and security events to reduce internal resource utilization while meeting strict compliance reporting standards.

- 2.) AI-driven automation :

Today's next-gen SIEM solutions integrate with powerful security orchestration, automaton and response (SOAR) systems, saving time and resources for IT teams as they manage business security. Using deep machine learning that automatically learns from network behavior, these solutions can handle complex threat identification and incident response protocols in significantly less time than physical teams.

- 3.) Improved organizational efficiency :

Because of the improved visibility of IT environments that it provides, SIEM can be an essential driver of improving interdepartmental efficiencies. A central dashboard provides a unified view of system data, alerts and notifications, enabling teams to communicate and collaborate efficiently when responding to threats and security incidents.

- 4.) Detecting advanced and unknown threats :

Considering how quickly the cybersecurity landscape changes, organizations need to be able to rely on solutions that can detect and respond to both known and unknown security threats. Using integrated threat intelligence feeds and AI technology, SIEM solutions can help security teams respond more effectively to a wide range of cyberattacks including:

- i.) Insider threats - security vulnerabilities or attacks that originate from individuals with authorized access to company networks and digital assets.

- ii.) Phishing - messages that appear to be sent by a trusted sender, often used to steal user data, login credentials, financial information, or other sensitive business information.

- iii.) Ransomeware - malwarethat locks a victim’s data or device and threatens to keep it locked or worse unless the victim pays a ransom to the attacker.

- iv.) Distributed denial of service(DDOS) - attacks that bombard networks and systems with unmanageable levels of traffic from a distributed network of hijacked devices (botnet), degrading performance of websites and servers until they are unusable.

- v.) Data Exfiltration – theft of data from a computer or other device, conducted manually, or automatically using malware.

- 5.) Conducting forensic investigations :

SIEM solutions are ideal for conducting computer forensic investigations once a security incident occurs. SIEM solutions allow organizations to efficiently collect and analyze log data from all of their digital assets in one place. This gives them the ability to recreate past incidents or analyze new ones to investigate suspicious activity and implement more effective 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.
Monitoring Users and Applications.With the rise in popularity of remote workforces, SaaS applications and bring your own device (BYOD) policies, organizations need the level of visibility necessary to mitigate network risks from outside the traditional network perimeter. SIEM solutions track all network activity across all users, devices, and applications, significantly improving transparency across the entire infrastructure and detecting threats regardless of where digital assets and services are being accessed.

- ## 3.) QRADAR :-

IBM QRadar is an enterprise security information and event management (SIEM) product. It collects log data from an enterprise, its network devices, host assets and operating systems, applications, vulnerabilities, and user activities and behaviors.

IBM QRadar is a network security management platform that provides situational awareness and compliance support. QRadar uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment.

QRadar uses a PostgreSQL database as a data store. Automatic vacuuming and reindexing are routine database maintenance activities that help QRadar function optimally, but it is sometimes necessary to run these processes manually.

- The QRadar architecture functions the same way regardless of the size or number of components in a deployment. The following three layers that are represented in the diagram represent the core functionality of any QRadar system.

- 1.) 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 denies, 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.

- 2.) 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.

- 3.) 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.

- i.) QRadar Components :
  Use IBM QRadar components to scale a QRadar deployment, and to manage data collection and processing in distributed networks.
- ii.)Qradar maximum EPS certification methodology :
  IBM QRadar appliances are certified to support a certain maximum events per second (EPS) rate. Maximum EPS depends on the type of data that is processed, system configuration, and system load.
- iii.)QRadar events and flows :
  The core functions of IBM QRadar SIEM are managing network security by monitoring flows and events.