Assignment 3 **10.9.2023**

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. Instructions:

1. Introduction to SOC: Begin by providing a comprehensive overview of what a Security Operations Center (SOC) is. Explain its purpose, key functions, and the role it plays in an organization's cybersecurity strategy.

In-housed or out-sourced team of IT security professionals that monitors organization's entire IT infrastructure, 24/7 detect cybersecurity events in real time and address them as quickly and effectively as possible. A n 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. 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.

Preparation, planning and prevention
Monitoring, detection and response
Recovery, refinement and compliance

2. SIEM Systems: Explore the concept of Security Information and Event Management (SIEM) systems. Discuss why SIEM is essential in modern cybersecurity and how it helps organizations monitor and respond to security threats effectively.

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 (AI) to automate many of the manual processes associated with threat detection and incident response.
Log management tool, security information management and analysis of security-related events and tacking and logging security data
Used in SOC for security management and compliance management use cases. It performs data aggregation, consolidation and soring functions to find threats.
Log managemnet
Event Correlation and Analytics
Incident moniteriing and security alerts
Compliance management and reporting

Real time threat recognition
Improved organizational efficiency
Detecting advanced and unknown threats
Conducting forensic investigations
Assessing and reporting in compliance
Monitoring users and applications

3. QRadar Overview: Research IBM QRadar and describe its key features, capabilities, and benefits as a SIEM solution. Include information on its deployment options (on-premises vs. cloud).

IBM Qradar

The IBM QRadar is a security information and event management or SIEM product that is designed for enterprises. The tool collects data from the organization and the network devices. It also connects to the operating systems, host assets, applications, vulnerabilities, user activities, and behaviors. IBM QRadar is used to perform analysis of the log data and the network flows in real-time so that malicious activities can be identified and stopped as soon as possible. Thus, the main aim of the IBM QRadar is to prevent or minimize the damage to its host organization.

The IBM QRadar SIEM uses a real-time integrated Cybersecurity AI, machine learning, and behavior analytics to prevent the attacks in the blink of an eye and with a very less cost compared to what human supervision can ensure. QRadar can address the bulk security issues that the companies face and save a lot of money. The security teams that struggle with patching endpoints properly and updating them can get their problems solved with IBM BigFix that has QRadar SIEM integrated into it. Most of the common issues are solved with this.

Deployment of the IBM QRadar SIEM is possible in the form of software, hardware, or a product meant for virtual application. Event processors for the collection, storage, and analysis of event collectors and event data make up the architecture of the product. They help to capture and forward the data.

Management of SIEM can be performed by the SOC or Security Operations Center through centralized consoles. The flow processors are similar to the event processors, however, these are meant for network flows. The consoles offer a lot of help to the people who are managing or using the SIEM.

Comprehensive visibility - The product helps to gain a centralized insight into the data flows, events, and logs on the SaaS (software-as-a-service) and IaaS (infrastructure-as-a-service) environments and on-premises.

Elimination of manual tasks - All the events in a certain threat can be centrally seen in one place and the expensive manual tracking can be eliminated. Analysts can focus on investigating the matter (security threat), followed by a proper response.

Easily cater to the compliance protocols - It becomes easier to comply with the international policies and the external regulations that are achieved by leveraging the pre-built reports and templates.

Real-time threat detection - Out-of-the-box analysis is leveraged that analyzes the network flows and logs automatically and generates proper alerts and the attacks are then directed via the proper kill chain.

Deployment on cloud vs premises

Majority of on-premises QRadar clients achieved full operational status in less than three months. Those that took longer either had larger deployments, fewer dedicated resources or some skills gaps. QRadar on Cloud is up in weeks — and in many cases days — depending upon the scale.
On cloud can avoid hardware obsolescence.
In few cases, our existing on-premises clients said that QRadar on Cloud is their preferred method for expanding managed device coverage beyond network firewalls, switches, routers, intrusion prevention systems (IPS) and intrusion detection systems (IDS).

4. Use Cases: Provide 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.

Real world example, Mohawk College
Cyberattacks breach even strongest security system, quick detection is critical to managing and recovering from intrusion. So Mohawk worked to implement IBM security Qradar SIEM solution to quickly detect breaches and prioritize incident response. It decided to implement Qradar for SIEM solution against threats that might attack its complex IT environment.
On implementing Qradar as SIEM, the college got visibility into threats across on-premises and cloud environments. It also accelerates threat detection with prioritization to address most critical ones. It also integrates seamlessly with many system across the campus.

Another such example is Netox Oy, one of Finland's great technology success stories. An IBM Business Partner delivering IT services and solutions with a specialty in cybersecurity, Netox grew 70% in 2021 and is poised to achieve 30% annual sales growth through 2026. Such growth stems from strong demand for the company's cybersecurity services, along with good management and the right vendor partnerships.
"As customers' digital environments become more and more complex, they find it hard to understand all the different interactions and connections," says Marita Harju, Senior Manager, Cyber Security at Netox. "Our Netox Trust cybersecurity services provide visibility into their unknowns, and our playbooks help them respond when an attack happens. We enable business continuity so our customers can focus on their core business." Qradar had broad scalability and multilatency, that is a single platform can serve any class and number of customers, scalability to support customers as they grew and as Netox extended its reach, support for data protection and compliance regulations.