IBM-CYBERSECURITY & QRADAR STAGE-3

Anil Kumar Madduri anilkumarmadduri@mictech.edu.in

Understanding SOC / SEIM and QRadar

SOC: (Security Operations Centre): A SOC is a centralized team or facility responsible for monitoring, detecting, responding to, and mitigating security incidents within an organization.

SOC-Cycle: This cycle typically includes the following stages

1. Monitoring and Detection:

In the initial stage, the SOC uses the SIEM system to continuously monitor and collect data from various sources, such as logs, network traffic, and security events.

2.Analysis and Alerting:

The collected data is analysed by the SIEM system to identify anomalies, patterns, and potential security threats. When the SIEM detects a security incident or suspicious activity, it generates alerts and sends them to the SOC.

3. Investigation and Response:

SOC analysts receive these alerts and conduct investigations to determine the nature and severity of the security incident. They may gather additional context and evidence to understand the incident fully. Once the incident is understood, the SOC initiates a response plan to mitigate the threat and minimize potential damage.

4. Resolution and Remediation:

After the incident is contained, the SOC works on resolving the issue and remediating any vulnerabilities that may have been exploited. This may involve patching systems, updating security policies, or making configuration changes to prevent a similar incident from happening in the future.

5. Documentation and Reporting:

The SOC documents the details of the incident, including its timeline, impact, and the actions taken for future reference and compliance purposes.

SIEM (Security Information and Event Management):

SIEM solutions are software platforms that collect and analyse data from various sources, including logs, events, and security-related data, to provide a holistic view of an organization's security posture.

SIEM Cycle:

The SIEM cycle is a continuous process that allows organizations to maintain a proactive and adaptive approach to cybersecurity. It empowers the SOC by providing valuable data and automated analysis, which helps in identifying and responding to security threats more efficiently.

1. Data Collection:

The SIEM cycle begins with the collection of data from various sources within the organization, including logs, events, network traffic, and security-related data. Data is gathered from diverse systems, devices, and applications, both on-premises and in the cloud.

2. Normalization and Parsing:

The collected data is normalized and parsed to ensure that it is in a consistent format that the SIEM system can analyse. This stage helps in standardizing data and making it more understandable for analysis.

3. Data Analysis and Correlation:

The SIEM system analyses the normalized data to identify patterns, anomalies, and potential security threats. Correlation rules are applied to correlate various events and identify potential security incidents.

4. Alerting and Notification:

When the SIEM system detects an event or a set of events that match predefined rules or indicate a potential security incident, it generates alerts. These alerts are sent to the SOC for further investigation.

MISP:

MISP (Malware Information Sharing Platform & Threat Sharing) is an open-source threat intelligence platform designed to improve the sharing of structured threat information. MISP can significantly enhance the capabilities of a Security Operations Centre (SOC) and a Security Information and Event Management (SIEM) system by providing valuable threat intelligence data and facilitating collaboration among security professionals. Incorporating MISP into the SOC and SIEM ecosystem enables organizations to harness the power of threat intelligence, improve their ability to detect and respond to cyber threats, and strengthen their overall cybersecurity posture.

Deploying soc in college/Institute:

Deploying a Security Operations Centre (SOC) in a college or educational institution is a vital step in ensuring the security of sensitive data, intellectual property, and the privacy of students, faculty, and staff.

1. Assessment and Planning:

Identify Objectives: Clearly define the goals and objectives of the SOC. Determine what you want to protect, what threats you want to address, and what resources are available.

Risk Assessment: Conduct a risk assessment to identify vulnerabilities and threats specific to the college environment. This assessment will help prioritize security measures. Budget and

Resources: Determine the budget and resources available for setting up and operating the SOC. This includes staffing, technology, and ongoing operational costs.

2. Design and Infrastructure:

Select Location: Choose a suitable physical location for the SOC. It should be secure, accessible, and equipped with the necessary infrastructure. Hardware and Software: Acquire the hardware and software necessary for the SOC. This includes servers, network monitoring tools, SIEM systems, and incident response platforms. Connectivity: Ensure that the SOC has robust connectivity to monitor network traffic and security logs effectively.

3. Staffing and Training:

Hire and Train Staff: Recruit and train SOC analysts and incident responders who will staff the centre. They should be well-versed in cybersecurity, incident detection, and response. Continuous Training: Provide ongoing training to keep SOC staff updated on the latest threats and technologies.

Threat intelligence:

1.Threat Intelligence Feeds:

Subscribe to threat intelligence feeds, such as those from commercial providers, open-source platforms, government agencies, and information sharing and analysis centres (ISACs). These feeds provide real-time information about known threats and vulnerabilities.

2.Integrate with SIEM:

Integrate threat intelligence feeds with the Security Information and Event Management (SIEM) system to automatically enrich security event data with relevant threat indicators. This helps the SIEM in identifying potential threats more accurately.

3.Customized Threat Intelligence:

Tailor threat intelligence to the college's specific needs and environment. Focus on collecting information relevant to the educational sector and the institution's infrastructure.

QRadar

Overview:

1.Data Collection and Normalization:

QRadar is used to collect and normalize data from various sources, including logs, network traffic, and security events across the college's IT infrastructure. This data provides the foundation for monitoring and analysis.

2.Real-time Event Correlation:

QRadar's advanced correlation engine helps identify patterns, anomalies, and potential security threats in real time. It can correlate events to detect complex, multi-stage attacks that might go unnoticed by simpler tools.

3.Alerting and Notification:

When QRadar detects suspicious or potentially malicious activities based on predefined rules and threat intelligence, it generates alerts and notifications. These alerts are sent to the SOC team for investigation.

4.Threat Intelligence Integration:

QRadar allows the integration of threat intelligence feeds, helping the SOC to keep up with the latest threat information. These feeds can provide context and relevance to detected security events.

Conclusion:

The generated detailed vulnerability report categorizes findings by severity levels, offering a nuanced understanding of their implications to enable effective prioritization and mitigation. Unlike conventional scanning methods, this project adopts a meticulous and systematic examination of the target website, exploring both well-known vulnerabilities and obscure entry points. This systematic approach directly contributes to the overall security of online platforms in an era where cyber threats pose significant risks to businesses, individuals, and governments. The proposed revenue model offers subscription packages to businesses and organizations in need of regular web vulnerability assessments, allowing them to select tiers based on scan frequency, depth of analysis, and support levels. The solution's scalability is achieved through cloud-based infrastructure, parallel processing, automated scaling, distributed computing, optimized algorithms, and API integrations, making it adaptable to various environments and capable of efficiently handling increasing workloads and data volumes. Overall, this project offers a holistic approach to web security, combining innovation, social impact, a sustainable business model, and scalability to address the growing challenges of cybersecurity in the digital age.

Our solution is designed to address this need, leveraging the formidable Nikto tool to perform a meticulous and thorough examination of web servers, systematically identifying and mitigating vulnerabilities. The scanning process meticulously examines server configurations, identifies outdated software, explores potential entry points, and uncovers various security vulnerabilities. By leveraging Nikto's extensive database and advanced scanning capabilities, it explores both well-known and obscure entry points, providing a holistic view of the website's security posture. The generated vulnerability report goes beyond merely listing potential security loopholes; it also offers a nuanced understanding of their implications, enabling website administrators to prioritize and address them effectively. The proposed subscription-based business model ensures a steady income stream, while scalability is achieved through advanced technology and infrastructure, making it a robust and sustainable solution for safeguarding sensitive data and user privacy in an era of increasing cyber threats. Business Impact: Using TLS version 1.0 can expose a system to various security risks, such as vulnerabilities to attacks like POODLE and BEAST, which can lead to data leakage and unauthorized access.

It employs an extensive database of known vulnerabilities, continuously updated to stay current with emerging threats, making it an indispensable tool for maintaining the integrity of an organization's digital assets. By identifying and prioritizing vulnerabilities, supporting compliance efforts, and offering a proactive approach to security, Nessus helps organizations stay ahead of the ever-evolving threat landscape. The future scope of web application testing in the project of deploying a SOC and SIEM in a college involves staying ahead of emerging technologies, security threats, and compliance requirements. The testing process will continually evolve to address new challenges, emphasizing proactive and adaptive security measures to protect the educational institution's web applications and data. The future scope of SOC and SIEM in a college or educational institution is characterized by continuous adaptation, automation, advanced threat detection, and a proactive approach to security.

Future Scope:

The future scope of this report extends far beyond its current findings, encompassing a wide range of potential directions for further research and development in the field of cybersecurity. To ensure the ongoing effectiveness of cybersecurity practices, several key areas warrant exploration.

First and foremost, there is a pressing need for the development and implementation of advanced vulnerability assessment techniques. As the threat landscape evolves, researchers and practitioners should delve into cutting-edge methods and tools that can provide a more nuanced and accurate understanding of vulnerabilities. Embracing emerging technologies, particularly artificial intelligence and machine learning, has the potential to revolutionize vulnerability identification and mitigation, enabling organizations to adopt a proactive defense strategy against constantly evolving threats.