**Stage 3 Report**

Title: Exploring the Capabilities of SOC/SEIM

**SOC**

Security Operations Center (SOC) is a centralized unit within an organization that monitors and manages security concerns and incidents. It serves as the hub for detecting, analyzing, and responding to security threats in real-time. SOC teams employ various tools and technologies to ensure the safety and security of the organization's digital assets. The SOC plays a crucial role in safeguarding against cyberattacks and minimizing the potential impact of security incidents.

**SOC Cycle**

The SOC operates in a continuous cycle that includes monitoring, detection, analysis, response, and improvement. This cyclical approach allows the SOC to adapt to evolving threats and improve security over time.

**SIEM**

Security Information and Event Management (SIEM) is a comprehensive solution that provides real-time analysis of security alerts generated by various hardware and software systems. SIEM systems collect and aggregate log data generated throughout the organization's technology infrastructure, analyze it, and provide actionable insights. SIEM tools are instrumental in monitoring security events, managing security incidents, and ensuring compliance with security policies.

**SIEM Cycle**

The SIEM cycle encompasses data collection, normalization, analysis, and reporting. It helps organizations identify anomalies and potential security incidents.

**MISP**

Malware Information Sharing Platform & Threat Sharing (MISP) is an open-source threat intelligence platform that facilitates the sharing of structured threat information. MISP is designed to improve the sharing of structured threat information and indicators of compromise (IOCs), enhancing the overall security posture of organizations.

Our College Network Information

Understanding the structure and layout of our college network is crucial for deploying a SOC. It involves identifying critical assets, network topology, access points, and potential vulnerabilities. This knowledge forms the foundation for an effective security strategy.

How to Deploy SOC in our College

Deploying a SOC in our college entails a comprehensive plan that includes defining roles and responsibilities, selecting the right tools, creating incident response procedures, and establishing key performance indicators (KPIs). This step will require collaboration with stakeholders and a clear understanding of the college's security objectives.

**Threat Intelligence**

Threat intelligence involves collecting, analyzing, and disseminating information about potential threats and vulnerabilities. It empowers organizations to proactively defend against cyberattacks by understanding the tactics, techniques, and procedures used by threat actors.

**Incident Response**

Incident response is the process of managing and mitigating the impact of security incidents. It involves preparation, identification, containment, eradication, recovery, and lessons learned to ensure the organization is better prepared for future incidents.

**Qradar & Understanding About the Tool**

IBM QRadar is a leading SIEM solution that assists organizations in detecting and responding to security threats. Understanding its capabilities, features, and the process of configuring and managing QRadar is essential for effective security monitoring.

**Conclusion**

Stage 1: In the previous stages, we gained insights into web application testing, learning to identify vulnerabilities and risks within web applications.

Stage 2: We explored Nessus, a valuable vulnerability assessment tool, and analyzed its capabilities in identifying vulnerabilities within our network.

Stage 3: In this stage, we delved into the world of SOC, SIEM, and QRadar Dashboards. We gained an understanding of the critical role these elements play in securing our organization's digital assets.

Future Scope

Stage 1: The future scope of web application testing includes further enhancing our skills, staying updated with emerging threats, and exploring advanced testing techniques.

Stage 2: Our understanding of the testing process will continue to evolve as we delve deeper into vulnerability assessment tools and their applications.

Stage 3: For SOC/SEIM, the future scope involves implementation within our college, continuous improvement of our security strategy, and ongoing training for SOC teams.

Topics Explored

**SOC**: Explored the concept and significance of a Security Operations Center.

**SOC Cycle**: Learned about the continuous cycle of SOC operations.

**SIEM**: Explored the critical role of Security Information and Event Management.

**SIEM Cycle**: Discussed the phases involved in a SIEM cycle.

**MISP**: Discovered the value of the Malware Information Sharing Platform.

**Our College Network Information**: Gained insights into understanding the structure of our college network.

**How to Deploy SOC in our College**: Explored the steps to deploy a SOC within the college environment.

**Threat Intelligence**: Learned about collecting and using threat intelligence for proactive security.

**Incident Response**: Explored the incident response process.

Qradar & Understanding About the Tool: Gained understanding of IBM QRadar and its significance in security operations.