CYBER SECURITY ASSIGNMENT QUESTION

DAY 9

1.Cyber Security Event Management

Question: Discuss the importance of event management in cyber security. Explain the difference between security events and incidents, and outline the key steps involved in managing security events effectively within an organization's security operations center (SOC).

2.Cyber Security Incident Management Process

Question: Explore the process of cyber security incident management. Describe the stages of incident response, roles and responsibilities of incident response team members, and the importance of communication and coordination during incident handling.

3.Threat Management Strategies

Question: Analyze the concept of threat management in cyber security. Identify common types of cyber threats, such as malware, phishing, and insider threats, and discuss strategies for managing and mitigating these threats effectively.

4. Vulnerability Management Best Practices

Question: Discuss the importance of vulnerability management in cyber security. Explain the difference between vulnerabilities and exploits, and outline best practices for identifying, assessing, and remediation of vulnerabilities in an organization's IT environment.

5.Case Study: Cyber Security Incident Response

Question: Analyze a real-world cyber security incident and evaluate the effectiveness of the incident response process. Identify strengths and weaknesses in the response efforts, and propose recommendations for improving incident response capabilities to mitigate similar incidents in the future.