BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – B.Sc.(ANCS)-Hons-2022
Course Name – Security Operations Center (SOC)
Course Code - BNCSC501
(Semester V)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Identify the step that is NOT part of the risk management process.
   a) Risk Identification b) Risk Mitigation
   c) Risk Avoidance d) Risk Encryption

(ii) State the primary goal of incident response.
   a) Prevent all security incidents from occurring b) Detect and respond to security incidents in real-time
   c) Assign blame to the individuals responsible for the incident d) Recover lost data after an incident

(iii) Identify the maturity level that indicates a well-optimized SOC with continuous improvement practices.
   a) Level 1 - Initial b) Level 2 - Repeatable
   c) Level 3 - Defined d) Level 4 - Managed

(iv) Select the phase that involves defining the SOC's mission, objectives, and scope.
   a) Planning Phase b) Implementation Phase
   c) Operational Phase d) Integration Phase

(v) Identify the purpose of a SOC capabilities roadmap.
   a) To outline the physical layout of the SOC facility b) To define the roles and responsibilities of SOC team members
   c) To prioritize the development of cybersecurity capabilities over time d) To create incident response playbooks for various scenarios

(vi) Select the primary purpose of a Network Flow Monitoring tool.

a) Analyze and report on network traffic patterns. b) Block all incoming network traffic.
c) Monitor data collection for compliance. d) Enhance cloud security.

(vii) Identify the defination of a vulnerability in the context of cybersecurity.
a) A weakness that could be exploited to compromise security. b) A malicious software.
c) A security tool. d) An encrypted communication channel.

(viii) Identify one of the key challenges in designing a Security Operations Center (SOC) team.
a) Difficulty in hiring skilled personnel. b) Overestimating budget requirements.
c) Underestimating threat intelligence. d) Automating all processes.

(ix) Identify the primary purpose of vulnerability scanning within a Security Operations Center (SOC).
a) To simulate real-world attacks b) To identify known vulnerabilities
c) To educate employees about security d) To analyze security logs

(x) State the purpose of continuous monitoring in vulnerability management.
a) To stop vulnerability scanning once detected b) To detect changes and trigger new scans
c) To simulate real attacks d) To create incident reports

(xi) Identify the step that follows vulnerability identification in the vulnerability management process.
a) Risk prioritization b) Incident reporting
c) User awareness training d) Network segmentation

(xii) Identify the phase that involves validating that vulnerabilities have been effectively remediated.
a) Vulnerability identification b) Risk prioritization
c) Remediation planning d) Vulnerability validation

(xiii) Identify the aspect of an SOC's documentation to review for alignment with best practices.
a) Facilities management logs b) Financial audit reports
c) Incident response playbooks d) Employee payroll records

(xiv) Identify the capability that evaluates an SOC's proactive approach to threat detection.
a) Mean time between failures (MTBF) b) Mean time to restore service (MTRS)
c) Threat hunting d) Employee satisfaction surveys

(xv) Identify what should periodic assessments of SOC technology focus on.
a) Annual employee training programs b) Integration with cloud services
c) SIEM and endpoint protection tools d) Monthly budget allocations

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Define the primary objectives of a Security Operations Center (SOC). (3)
3. Explain the key steps involved in conducting a risk assessment for a SOC. (3)
4. Describe the role of endpoint data in SOC operations. (3)
5. Discuss the role of compliance audits in ensuring effective vulnerability management. (3)
6. Explain the role of the Cyber Kill Chain framework in a SOC. (3)

OR

Explain the main objectives of conducting red teaming exercises and how they contribute to improving SOC defenses. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Write the risk management process in cybersecurity. (5)
8. How does the MITRE ATT&CK framework assist in improving SOC capabilities? (5)
9. What are three key strategies for enhancing malware detection capabilities in a SOC? (5)
10. Analyze the process analysis phase of an SOC assessment. (5)
11. Evaluate the importance of collaboration and communication within an SOC. (5)
12. Explain the key challenges faced by organizations in the field of cybersecurity and discuss how these challenges can be mitigated. (5)

OR

Explain the concept of information assurance and its significance in ensuring the security of sensitive data and systems. (5)

****