BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – B.Sc.(ANCS)-Hons-2023
Course Name – Security Operations Center Management
Course Code - BNC60120
(Semester VI)

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) Select the main objective of a Security Operations Center (SOC).
a) Software development
b) Continuous security monitoring and incident response
c) Network installation
d) User training only

(ii) Choose the best explanation of risk management in cybersecurity.
a) Removing all risks
b) Identifying, analyzing, and mitigating risks
c) Installing security tools
d) Monitoring users only

(iii) Identify the correct approach to manage SOC challenges and obstacles.
a) Avoid process documentation
b) Implement skilled staffing and defined procedures
c) Disable automation
d) Reduce collaboration

(iv) Identify the primary purpose of assessment methodology in a SOC.
a) Install security tools
b) Measure SOC effectiveness
c) Train employees
d) Develop applications

(v) Select how understanding threat landscape benefits SOC planning.
a) Increases false positives
b) Improves prioritization of defenses
c) Delays response
d) Reduces visibility

(vi) Select the most effective way to improve SOC infrastructure scalability.
a) Increase manual processes
b) Limit data sources
c) Reduce monitoring
d) Adopt modular and scalable design

(vii) Select the main role of IDS in network security.
a) Manage users
b) Detect malicious activity
c) Block all traffic
d) Encrypt data

(viii) Choose the best description of vulnerability management.

a) Install firewalls
b) Identify, assess, and remediate vulnerabilities
c) Encrypt traffic
d) Monitor users

(ix) Identify the correct step to improve SOC performance.

a) Regular reviews and assessments
b) Ignore metrics
c) Reduce staff
d) Disable tools

(x) Choose the final step of SOC case management.

a) Event intake
b) Monitoring
c) Enrichment
d) Closing and reporting

(xi) Choose the best description of a virtual SOC.

a) Tool-less SOC
b) Temporary SOC
c) On-site SOC only
d) Remotely delivered SOC services

(xii) Determine the most effective way to manage SOC transition.

a) Tool removal
b) Immediate shutdown
c) Staff reduction
d) Phased and planned implementation

(xiii) Determine why MITRE ATT&CK is valuable for threat hunting.

a) Provides structured attack knowledge
b) Replaces tools
c) Ensures compliance
d) Eliminates attacks

(xiv) Choose the best action when IoC is detected.

a) Reduce logging
b) Initiate investigation and response
c) Ignore alert
d) Disable monitoring

(xv) Select the best practice for malware detection improvement.

a) Disable updates
b) Use signatures only
c) Manual inspection only
d) Combine signatures and behavior analysis

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Differentiate between threat hunting and incident triage in a SOC. (3)
3. Describe the role of automated scanning in vulnerability management. (3)
4. Describe the benefits of collaboration with external partners in SOC operations. (3)
5. Explain the purpose of security data lakes. (3)
6. Analyze the impact of burnout on SOC operations. (3)

OR

Analyze why false positives are a major operational challenge in SIEM systems. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Define Threat and Vulnerability. (5)
8. Describe the key challenges faced by organizations in cybersecurity and how these challenges can be mitigated. (5)
9. Evaluate how insider threats affect an organization's cybersecurity posture. (5)
10. Explain how a SOC ensures compliance with regulations and standards. (5)
11. Explain how SOC review processes improve operational maturity. (5)
12. Compare and contrast Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). (5)

OR

Compare the use of sandboxes and honeypots as breach detection techniques. (5)

****