.

Printed Page:-4 **Subject Code:- BCSCY0412**

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute Affiliated to AKTU, Lucknow)
B.Tech
SEM: IV - THEORY EXAMINATION (2025 - 2026)
Subject: Cyber Threat Intelligence

Time: 3 Hours **Max. Marks: 100**

General Instructions:

IMP: *Verify that you have received the question paper with the correct course, code, branch etc.*
1. *This Question paper comprises of* ***three Sections -A, B, & C.*** *It consists of Multiple Choice Questions (MCQ's) & Subjective type questions.*
2. *Maximum marks for each question are indicated on right -hand side of each question.*
3. *Illustrate your answers with neat sketches wherever necessary.*
4. *Assume suitable data if necessary.*
5. *Preferably, write the answers in sequential order.*
6. *No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.*

SECTION-A 20

1. Attempt all parts:-

(1.1) The importance of CTI lies in enabling organizations to take the following kind of actions. (CO1, K2) 1

(a) User onboarding
(b) Routine maintenance
(c) Software installation
(d) Proactive security actions

(1.2) Strategic intelligence is designed to support the following level of decision-making. (CO1, K2) 1

(a) Executive decision-making
(b) Daily operations
(c) System monitoring
(d) Password resets

(1.3) Environments covered in ATT&CK knowledge base include. (CO2, K1) 1

(a) Enterprise, Mobile, ICS
(b) Only Cloud
(c) Only Hardware
(d) Only Social Media

(1.4) Victim element in the Diamond Model refers to (CO2, K2) 1

(a) Vendor partner
(b) Security analyst
(c) Target of intrusion
(d) CEO only

.

(1.5) Identify the method of data collection that actively monitors underground forums and marketplaces. (CO3, K2) 1

(a) Logs
(b) Honeypots
(c) Dark Web Monitoring
(d) Threat Feeds

(1.6) Recognize the open-source platform that supports STIX/TAXII standards for threat sharing. (CO3, K2) 1

(a) MISP
(b) ThreatConnect
(c) Recorded Future
(d) VirusTotal

(1.7) Attribution in threat actor profiling refers to. (CO4, K2) 1

(a) Linking attacks to responsible actors
(b) Encrypting sensitive files
(c) Collecting IOCs
(d) Changing system logs

(1.8) Hacktivist operations often include. (CO4, K1) 1

(a) Website defacement
(b) Banking trojans
(c) Zero-day exploits
(d) Phishing kits

(1.9) A key barrier to intelligence sharing is. (CO5, K2) 1

(a) Legal and trust issues
(b) Hardware cost
(c) Internet speed
(d) File compression

(1.10) Effective CTI sharing improves. (CO5, K2) 1

(a) Collective defense
(b) Employee productivity
(c) Power consumption
(d) Email marketing

2. Attempt all parts:-

(2.1) List the six phases of the intelligence lifecycle in their correct sequential order. (CO1, K1) 2

(2.2) Explain the purpose of TTPs in the MITRE ATT&CK framework. (CO2, K2) 2

(2.3) Describe Open-Source Intelligence with an example. (CO3, K1) 2

(2.4) Illustrate cybercriminal group in the context of threat intelligence. (CO4, K1) 2

(2.5) Define the concept of ROI in threat intelligence programs. (CO5, K2) 2

SECTION-B 30

Answer any one of the following:-

(3.1) Compare the effects of culture, regulations, and technology levels on implementation in different countries and industries. (CO1, K2) 6

(3.2) Explain the MITRE ATT&CK framework by describing its tactics, techniques, and procedures, and discuss its use in red teaming, threat hunting, and defensive planning. (CO1, K2) 6

Answer any one of the following:-

(3.3) Identify the limitations of current threat modeling frameworks, outline emerging alternatives, and summarize possible directions for improvement. (CO2, K2) 6

(3.4) Explain the working of red teams, blue teams, and security architects using threat modeling frameworks, and describe whether the framework design meets their needs. (CO2, K2) 6

Answer any one of the following:-

(3.5) Compare Honeypots and Logs as data collection methods. (CO3, K2) 6

(3.6) Summarize the role of Threat Feeds in reducing incident response time. (CO3, K2) 6

Answer any one of the following:-

(3.7) Explain how malware behavioral analysis assists in developing detection rules. (CO4, K3) 6

(3.8) Describe methods to collect and validate threat intelligence from multiple sources. (CO4, K3) 6

Answer any one of the following:-

(3.9) Discuss the role of deception technologies in proactive threat hunting. (CO5, K2) 6

(3.10) Explain how deception-based approaches can mislead attackers in SOC environments. (CO5, K2) 6

SECTION-C 50

4. Answer any one of the following:-

(4.1) Evaluate communication and feedback mechanisms that enable alignment of CTI outputs with stakeholder requirements. (CO1, K4). 10

(4.2) Analyze the organizational and technical barriers that hinder effective CTI integration with other cybersecurity disciplines. (CO1, K4). 10

5. Answer any one of the following:-

(5.1) Analyze the limitations of ATT&CK in detecting or mapping emerging techniques such as supply chain attacks and cloud-native threats. Suggest ways to overcome these challenges. (CO2, K4). 10

(5.2) Examine the technical, organizational, and cultural challenges that arise when 10

organizations attempt to integrate multiple CTI frameworks.
(CO2, K4).

6. Answer any one of the following:-

(6.1) Discuss the reliability issues of Human Intelligence with real-world examples. 10
(CO3, K3)

(6.2) Ellaborate the process of converting raw data into enriched and correlated intelligence. 10
(CO3, K3)

7. Answer any one of the following:-

(7.1) Analyze the SolarWinds attack, describing the techniques, tactics, and indicators used by the threat actors. 10
(CO4, K4)

(7.2) Analyze how threat actor motivation influences observed attack patterns. 10
(CO4, K4)

8. Answer any one of the following:-

(8.1) Identify, how deception technologies have been used to detect and trap advanced persistent threats in corporate networks. 10
(CO5, K4)

(8.2) Relate and analyse the best practices for measuring CTI ROI and present a framework for quantifying program effectiveness. 10
(CO5, K4)