.

Printed Page:-4 **Subject Code:- BCSCY0511**

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute Affiliated to AKTU, Lucknow)
B.Tech
SEM: V - 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-a. The main goal of Cyber Threat Intelligence is to reduce what? (CO1, K2) 1

(a) Financial investment
(b) Security risk
(c) Hardware usage
(d) Data storage size

1-b. CTI differs from raw data because it provides what?(CO1,K1) 1

(a) Actionable insights
(b) Unprocessed logs
(c) Encrypted backups
(d) Firewall settings

1-c. Abbreviation TTPs in MITRE ATT&CK refers to (CO2,K1) 1

(a) Tracking, Timing, and Planning
(b) Tools, Targets, and Processes
(c) Testing, Training, and Policies
(d) Tactics, Techniques, and Procedures

1-d. In ATT&CK framework, tactics represent(CO2,K1) 1

(a) Adversary goals
(b) Software versions
(c) Employee shifts
(d) Hardware purchases

1-e. Identify the source of intelligence that relies on freely available information such as 1

blogs and news articles.(CO3,K2)

(a) Open-Source Intelligence
(b) Human Intelligence
(c) Closed Intelligence
(d) Technical Intelligence

1-f. Classify the type of intelligence often purchased through vendors and subscription services.(CO3,K2) 1

(a) Technical Intelligence
(b) Closed/Private Intelligence
(c) Human Intelligence
(d) Open-Source Intelligence

1-g. Indicators of Compromise (IOCs) are best described as.(CO4,K2) 1

(a) Artifacts of past malicious activity
(b) Preventive security measures
(c) User credentials
(d) Mitigation strategies

1-h. File hashes, IP addresses, and domain names are examples of.(CO4,K1) 1

(a) Encryption keys
(b) Behavioral patterns
(c) Indicators of Compromise
(d) Incident reports

1-i. The primary role of CTI in incident response is to.(CO5,K1) 1

(a) Encrypt traffic
(b) Provide context for attacks
(c) Generate spam emails
(d) Reduce hardware costs

1-j. CTI integration into SOC workflows primarily improves.(CO5,K1) 1

(a) Firewall speed
(b) Log file storage
(c) Email filtering
(d) Alert triage accuracy

2. Attempt all parts:-

2.a. Differentiate between tactical and operational intelligence by providing one practical example each.(CO1.K2) 2

2.b. List the four elements of the Diamond Model of Intrusion Analysis(CO2,K2) 2

2.c. Describe one advantage of Closed/Private Threat Intelligence.(CO3,K1) 2

2.d. Explain the difference between IOC and IOA.(CO4,K2) 2

2.e. List two common sources of threat intelligence data.(CO5,K2) 2

SECTION-B 30

3. Attempt all parts:-

3.a. Answer any one of the following:-

3.a.(i)	Examine the influence of organizational culture on the success of CTI implementation in globally distributed corporations.(CO1,K2)	6
3.a.(ii)	Evaluate the role of AI and ML in enhancing the timeliness and accuracy of CTI outputs across different lifecycle stages.(CO1,K2)	6

3.b. Answer any one of the following:-

3.b.(i)	Evaluate the Diamond Model of Intrusion Analysis by examining adversary, infrastructure, capability, and victim, and analyze how these elements interact to reveal attack patterns. (CO2,K3)	6
3.b.(ii)	Develop an integrated threat analysis method that combines ATT&CK, Diamond Model, and Kill Chain, demonstrating their joint value through a case study.(CO2,K2)	6

3.c. Answer any one of the following:-

3.c.(i)	Analyze the differences among Open-Source, Closed, Technical, and Human Intelligence with examples.(CO3,K3)	6
3.c.(ii)	Discuss the challenges faced while relying on OSINT for cyber defense.(CO3,K3)	6

3.d. Answer any one of the following:-

3.d.(i)	Describe the process of analyzing IOCs and IOAs during a cyber incident.(CO4,K2)	6
3.d.(ii)	Compare and contrast APT groups and hacktivist groups in terms of tactics and motivations.(CO4,K2)	6

3.e. Answer any one of the following:-

3.e.(i)	Analyze the challenges faced while embedding CTI into incident response processes.(CO5,K2)	6
3.e.(ii)	Evaluate the benefits of vendor platforms for integrating threat intelligence into SOC operations.(CO5,K3)	6

SECTION-C 50

4. Answer any one of the following:-

4-a.	Examine the role of organizational culture and leadership in determining the success or failure of CTI initiatives.(CO1,K2)	10
4-b.	Design a CTI architecture tailored for a critical infrastructure sector such as the power grid, addressing unique threat and regulatory requirements.(CO1,K3)	10

5. Answer any one of the following:-

5-a.	Explain the objectives of the MIT*2.* Question Text and Hints RE ATT&CK framework and discuss how it helps organizations in understanding attacker behavior beyond traditional signature-based methods.(CO2,K2)	10
5-b.	Discuss how ATT&CK adoption varies between industries such as finance, healthcare, and government, highlighting sector-specific drivers and barriers.(CO2,K2)	10

6. Answer any one of the following:-

6-a.	Critically evaluate the role of OSINT in building cyber defense strategies.(CO3,K2)	10
6-b.	Discuss the reliability issues of Human Intelligence with real-world examples.(CO3,K2)	10

.

7. Answer any one of the following:-

7-a.	Analyze the SolarWinds attack, describing the techniques, tactics, and indicators used by the threat actors.(CO4,K2)	10
7-b.	Evaluate the WannaCry ransomware incident, focusing on its propagation methods and organizational impact.	10

8. Answer any one of the following:-

8-a.	Analyze recent case studies where CTI-driven threat hunting prevented critical security incidents, and explain the methodologies used.(CO5,K2)	10
8-b.	Investigate how AI-driven analytics in CTI have transformed predictive threat modeling in cybersecurity operations.(CO5,K2)	10