SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

VII SEMESTER

1923702 – CYBER THREAT INTELLIGENCE

Regulation – 2019

Academic Year 2025-2026 (Odd Semester)

Prepared by

Ms.T.Sathya, Assistant Professor (O.G)

SUBJECT: 1923702 – CYBER THREAT INTELLIGENCE
SEM/YEAR: VII / IV

UNIT I - DEFINING CYBER THREAT INTELLIGENCE
The Need for Cyber Threat Intelligence: The menace of targeted attacks, The monitor– and–respond strategy, Why the strategy is failing, Cyber Threat Intelligence Defined, Key Characteristics: Adversary based, Risk focused, Process oriented, Tailored for diverse consumers, The Benefits of Cyber Threat Intelligence

PART – A

Q.No	Question	Level	Competence
1	List the types of threat intelligence.	BTL3	Applying
2	Point out the need for Cyber Threat Intelligence.	BTL4	Analyzing
3	What is Cyber Threat Intelligence?	BTL1	Remembering
4	Discuss about the tools used for threat intelligence.	BTL2	Understanding
5	Outline the benefits of Cyber Threat Intelligence.	BTL2	Understanding
6	Explain the reasons why cyber threat intelligence is essential.	BTL1	Remembering
7	Define Monitor and Respond strategy.	BTL1	Remembering
8	Define Adversary based characteristics of CTI.	BTL1	Remembering
9	Explain the key components of Monitor and respond strategy.	BTL2	Understanding
10	Define the limitations of Monitor and Respond strategy.	BTL1	Remembering
11	Generalize your view about menace of targeted attacks.	BTL6	Creating
12	Infer how CTI addresses the menace of targeted attacks.	BTL4	Analyzing
13	Identify what are the indicators of Compromise.	BTL3	Applying
14	Define threat detection.	BTL2	Understanding
15	Examine the available malware disassembler tools.	BTL3	Applying
16	Assess the term Post-Incident Analysis.	BTL5	Evaluating
17	List the key characteristics of Cyber Threat Intelligence.	BTL1	Remembering
18	Point out the concept of operational threat intelligence.	BTL4	Analyzing
19	Discuss the reasons for the failure of Monitor and respond strategy.	BTL6	Creating
20	Assess the characteristics of Risk based CTI.	BTL5	Evaluating
21	Identify what is threat hunting.	BTL3	Applying
22	What is the threat intelligence lifecycle?	BTL2	Understanding
23	Differentiate between threat data and threat intelligence.	BTL4	Analyzing
24	Explain how we can avoid data breach.	BTL5	Evaluating

PART – B

Q.No	Question	Level	Competence
1	Explain the key characteristics of Cyber Threat Intelligence in detail. (13)	BTL1	Remembering
2	Write short notes on (i) Threat hunting. (7) (ii) Threat detection. (6)	BTL1	Remembering
3	Describe in detail about Monitor and respond strategy.(13)	BTL1	Remembering
4	(i) Describe about adversary based characteristics of CTI .(7) (ii) Describe process oriented characteristics of CTI (6)	BTL2	Understanding
5	Examine the following: (i) Threat data. (7) (ii) Cyber threat. (6)	BTL2	Understanding
6	(i) Describe the need for Cyber Threat Intelligence. (5) (ii) Explain the benefits of Cyber Threat Intelligence. (8)	BTL1	Remembering

7	Examine about various Cyber Threat Intelligence tools in detail. (13)	BTL3	Applying
8	Explain the following: i) Cyber threat Intelligence tools. (7) ii) Common Indicators of Compromise. (6)	BTL4	Analyzing
9	Explain in detail about Threat Intelligence life cycle (13)	BTL4	Analyzing
10	Explain the concept of risk based characteristics of Cyber Threat Intelligence. (13)	BTL2	Understanding
11	Compare and contrast various types of Cyber Threat Intelligence.(13)	BTL3	Applying
12	Explain the various types of cyber threat attacks in detail. (13)	BTL6	Creating
13	Explain the following in detail: (i) Features of Cyber Threat Intelligence tools. (8) (ii) Components of Cyber Threat Intelligence. (5)	BTL 5	Evaluating
14	Analyze and Explain the tailored for diverse consumer characteristics of CTI (13)	BTL4	Analyzing
15	Briefly explain the key aspects of menace of targeted attacks (13)	BTL2	Understanding
16	(i)Examine Cyber Threat Intelligence with suitable examples.(8) (ii)Explain the threat indicators. (5)	BTL3	Applying
17	Define Monitor and Respond strategy and explain the reasons for the failure of Monitor and Respond strategy in detail.(13)	BTL 5	Evaluating

PART - C			
Q.No	**Question**	**Level**	**Competence**
1	Explain the Cyber Threat Intelligence Lifecycle in detail. (15)	BTL5	Evaluating
2	Discuss the reasons for the failure of Monitor and Respond strategy in detail. (15)	BTL6	Creating
3	Discuss about various Cyber Threat Intelligence tools and their features in Detail. (15)	BTL6	Creating
4	Explain the key characteristics of Cyber Threat Intelligence with suitable examples for each. (15)	BTL5	Evaluating
5	Write brief notes on (i) Data breach. (5) (ii) Vulnerability and cyber-attacks. (5) (iii) Post- Incident Analysis. (5)	BTL5	Evaluating

UNIT –II DEVELOPING CYBER THREAT INTELLIGENCEREQUIREMENTS

Assets That Must Be Prioritized: Personal information, Intellectual property, Confidential business information, Credentials and IT systems information, Operational systems. Adversaries: Cybercriminals, Competitors and cyber espionage agents, Hack activists. Intelligence Consumers: Tactical users, Operational users, Strategic users

UNIT –II [PART-A]

Q.No	Question	Competence	Level
1	Define Assets with example.	Remembering	BTL1
2	Define the term Confidential business information.	Remembering	BTL1
3	What are threat intelligence requirements.	Remembering	BTL1
4	Explain why threat intelligence requirements are important.	Evaluating	BTL5
5	Examine various assets.	Applying	BTL3
6	Write about threat intelligence.	Remembering	BTL1
7	Explain the term threat actor.	Analyzing	BTL4
8	Differentiate between threat and threat intelligence.	Understanding	BTL2
9	Summarize the common types of cyber threats.	Understanding	BTL2
10	Differentiate cybercriminals and cyber espionage agents.	Understanding	BTL2
11	Justify insider threats.	Creating	BTL6
12	What is the role of competitors in developing cyber threat intelligence requirements?	Remembering	BTL1
13	Discuss how the assets can be prioritized.	Understanding	BTL2
14	What are the top three ransomware threats to the organization?	Remembering	BTL1
15	Discover some considerations for prioritizing intellectual property assets.	Applying	BTL3
16	Examine the considerations for prioritizing confidential business information assets.	Applying	BTL3
17	Analyze how the cyber criminals exploit the vulnerability.	Analyzing	BTL4
18	Explain who are the nation and state actors.	Evaluating	BTL5
19	Classify the intelligence consumers.	analyzing	BTL4
20	Prepare a note on script kiddies.	Creating	BTL6
21	List out the cons of Lizard Squad.	Understanding	BTL2
22	Discuss WikiLeaks. Give example.	Evaluating	BTL5
23	Examine the role of hack activist.	Applying	BTL3
24	Explain how can we identify threat landscape.	Analysing	BTL4

UNIT –II [PART-B]

Q.No		Question	Marks	Competence	Level
1	-	Describe in detail about Assets with examples.	13	Remembering	BTL1
2	A	Summarize the threat intelligence requirements.	07	Evaluating	BTL5
	B	Explain why are the threat intelligence requirements important?	06		
3	-	Discuss the various intelligence consumers in detail.	13	Understanding	BTL2
4	-	Discuss the role of various adversaries in detail.	13	Understanding	BTL2
5	-	Illustrate how a single threat intelligence requirement can be operationalized.	13	Applying	BTL3
6	A	Write short notes on the following assets: (i) Confidential business information	07	Analysing	BTL4
	B	(ii) Operational systems	06		
7	A	List out the features of various threat intelligence tools.	13	Remembering	BTL1
8	-	Analyze the considerations for prioritizing confidential business information assets in detail.	13	Analysing	BTL4
9	-	List the considerations for prioritizing personal information assets in detail.	13	Remembering	BTL1

10	**A**	Classify the various threat intelligence requirements in detail.	07	Remembering	BTL1
	B	Explain about threat intelligence in detail.	06		
11	-	Summarize the various roles of (i) Syrian Electronic Army (7) (ii) AntiSec (6)	13	Understanding	BTL2
12	-	Illustrate the role of Competitors and cyber espionage agents in developing cyber threat intelligence requirements	13	Applying	BTL3
13	-	Write short notes on (i) Liquid squad (7) (ii) Wikileaks (6)	13	Applying	BTL3
14	-	Formulate how the hacktivists impact on cyber threat intelligence requirements.	13	Creating	BTL6
15	-	Discuss about various roles of threat actors in detail.	13	Understanding	BTL2
16	-	Classify the role of hacktivists in detail.	13	Analysing	BTL4
17	-	Evaluate how the intelligence property information and Credentials and IT systems information assets can be prioritized.	13	Evaluating	BTL5
UNIT -II[PART-C]					
1	Evaluate how a single threat intelligence requirement can be operationalized.		15	Evaluating	BTL5
2	Explain the following: (i) Tactical Users (5) (ii) Operational Users (5) (iii) Strategic Users (5)		15	Creating	BTL6
3	Explain the following: (i) Personal Information (5) (ii) Intellectual Property (5) (iii) Confidential business information (5)		15	Evaluating	BTL5
4	Generalize in detail about the steps for developing cyber threat intelligence requirements.		15	Creating	BTL6
5	Compare the following: (i) Cybercriminals (5) (ii) Competitors and Cyber Espionage agents (5) (iii) Hack activists (5)		15	Creating	BTL6

UNIT–III COLLECTING CYBER THREAT INFORMATION

Threat Indicators, File hashes and reputation data, Technical sources: honey pots and scanners, Industry sources: malware and reputation feeds. Level 2: Threat Data Feeds, Cyber threat statistics, reports, and surveys, Malware analysis. Level 3: Strategic Cyber Threat Intelligence, Monitoring the underground, Motivation and intentions, Tactics, techniques, and procedures

UNIT–III [PART-A]

Q.No	Question	Competence	Level
1	Define threat indicator with an example.	Remembering	BTL1
2	What are the different categories of threat indicators?	Remembering	BTL1
3	Explain how to manage file hashes.	Evaluating	BTL5
4	Define threat data feeds.	Remembering	BTL1
5	How to formulate cyber threat statistics.	Analysing	BTL4
6	Define file hashes and reputation data.	Remembering	BTL1
7	Explain the strategic cyber threat intelligence.	Applying	BTL3
8	Discuss about industry sources for collecting the threat information.	Understanding	BTL2
9	Summarize the technical sources for collecting the cyber threat information.	Understanding	BTL2
10	Write about the potential threat indicators.	Understanding	BTL2
11	Which tool is used to detect honey pot? Justify your answer.	Creating	BTL6
12	What is survey in cyber security threat data?	Remembering	BTL1
13	How can we identify and detect insider threat?	Applying	BTL3
14	What is an insider threat?	Remembering	BTL1
15	Discover the motivation of strategic cyber threat intelligence.	Applying	BTL3
16	Discuss the tools for malware analysis.	Understanding	BTL2
17	Analyse how do you check if a token is a honey pot.	Analysing	BTL4
18	Explain the steps of malware analysis.	Evaluating	BTL5
19	Analyze threat hunting with threat intelligence.	Analysing	BTL4
20	Develop reports and surveys of cyber threat statistics based on threat data feeds.	Creating	BTL6
21	List out the examples of strategic threat intelligence.	Understanding	BTL2
22	What is TTP in threat hunting?	Evaluating	BTL5
23	Examine why malware analysis is needed.	Applying	BTL3
24	What are the new tactics techniques and procedures used by threat actors?	Analysing	BTL4

UNIT–II[PART-B]

Q.No		Question	Marks	Competence	Level
1	**-**	Describe in detail about threat indicators.	13	Remembering	BTL1
2	-	Summarize about file hashes and reputation data in detail	13	Evaluating	BTL5
3	-	Discuss the technical sources for collecting the threat information.	13	Understanding	BTL2
4	-	Discuss the industrial sources for collecting the threat information.	13	Understanding	BTL2
5	-	Illustrate threat data feeds with examples.	13	Applying	BTL3
6	**A**	Explain about cyber threat statistics.	07	Analysing	BTL4
	B	Explain in detail about reports and surveys on threat data feeds.	06		
7	**A**	Explain about threat intelligence feed in detail.	07	Remembering	BTL1
	B	Differentiate between threat hunting and threat intelligence.	06		
8	-	Analyze the steps for malware analysis with suitable examples.	13	Analysing	BTL4
9	-	Describe about strategic cyber threat intelligence in detail.	13	Remembering	BTL1
10	**A**	Explain about threat data feed in detail.	07		

	B	Discuss in detail about cyber threat statistics, reports and surveys.	06	Remembering	BTL1
11	-	Summarize about malware and reputation data feeds in detail	13	Understanding	BTL2
12	-	Illustrate about level 2 and level 3 collection of cyber threat information.	13	Applying	BTL3
13	-	Classify the industry sources and technical sources of cyber threat information.	13	Applying	BTL3
14	-	Develop reports and surveys of cyber threat statistics based on threat data feeds. Explain it with examples.	13	Creating	BTL6
15	-	Write short notes on (i) Threat data feed (7) (ii) Threat hunting (6)	13	Understanding	BTL2
16	-	Analyse the concepts of malware analysis and also write about the tools for analyzing the malware.	13	Analysing	BTL4
17	-	Evaluate Tactics, techniques, and procedures in detail with suitable examples.	13	Evaluating	BTL5
UNIT-II[PART-C]					
1	Analyze the tools for malware and explain the tools in detail.		15	Creating	BTL6
2	Evaluate strategic cyber threat intelligence in detail.		15	Evaluating	BTL5
3	Analyze the difference between level 2 and level 3 cyber threat information		15	Analysing	BTL4
4	Generalize in detail about industry sources and technical sources of collecting the threat information.		15	Creating	BTL6
5	Analyze about Tactics, techniques, and procedures in detail with suitable examples.		15	Analysing	BTL4

UNIT – IV : ANALYZING AND DISSEMINATING CYBER THREAT INTELLIGENCE

Information versus Intelligence, Validation and Prioritization: Risk scores, Tags for context, Human assessment. Interpretation and Analysis: Reports, Analyst skills, Intelligence platform, Customization. Dissemination: Automated feeds and APIs, Searchable knowledge base, Tailored reports.

PART – A

Q.No	Question	Level	Competence
1	Differentiate between threat information and threat intelligence.	BTL3	Applying
2	Point out the importance of validation and prioritization.	BTL4	Analyzing
3	List out the steps for validating the threat information.	BTL1	Remembering
4	Discuss about automated feeds with examples.	BTL2	Understanding
5	Define risk score.	BTL2	Understanding
6	List the role of tags in prioritize the security issues.	BTL1	Remembering
7	Define threat intelligence dissemination.	BTL1	Remembering
8	List the steps for interpreting the threat information.	BTL1	Remembering
9	What is the role of human in risk assessment?	BTL2	Understanding
10	Define threat identification in risk assessment?	BTL1	Remembering
11	Generalize your view about analyzing the cyber threat intelligence.	BTL6	Creating
12	Analyze the role of risk scoring.	BTL4	Analyzing
13	Distinguish between interpretation and customization.	BTL3	Applying
14	What is intelligence platform?	BTL2	Understanding
15	Show the advantages of human assessment in validation.	BTL3	Applying
16	Assess how do you validate a risk assessment.	BTL5	Evaluating
17	List the techniques for threat dissemination.	BTL1	Remembering
18	Compare: customization and Dissemination.	BTL4	Analyzing
19	How do you analyze cyber threats?	BTL6	Creating
20	Assess the characteristics of analyst skills in interpretation of threat intelligence.	BTL5	Evaluating
21	List the role of intelligence platform.	BTL3	Applying
22	What are tailored reports?	BTL2	Understanding
23	Analyze the steps for interpreting the threat information.	BTL4	Analyzing
24	Explain the concept of searchable knowledge base.	BTL5	Evaluating

PART – B

Q.No	Question	Level	Competence
1	Describe in detail about (i) Threat information (7) (ii) Threat intelligence (6)	BTL1	Remembering
2	(i) List the advantages of risk scoring. (6) (ii) List the importance of Human assessment in validation and prioritization. (7)	BTL1	Remembering
3	Describe about the various steps in validation and prioritization of cyber information (13)	BTL1	Remembering
4	(i) Describe about risk scoring. (6) (ii) What are the steps in prioritizing the cyber threat information? (7)	BTL2	Understanding
5	Briefly explain about interpretation and analysis of cyber threat information. (13)	BTL2	Understanding
6	Describe about the intelligence platform in detail. (13)	BTL1	Remembering

7	Examine about (i) Analyst skills. (6) (ii) Intelligence platform. (7)	BTL3	Applying
8	Explain the following: (i) Reports (6) (ii) customization (7)	BTL4	Analyzing
9	(i) Explain how can we enhance the overall security posture and minimize the risk of security incidents. (6) (ii) How do you handle potential security incidents? (7)	BTL4	Analyzing
10	Describe in detail about Searchable knowledge base. (13)	BTL2	Understanding
11	Examine about (i) Interpretation and analysis (6) (ii) dissemination (7)	BTL3	Applying
12	(i) Discuss about the role of analysts. (8) (ii) How do the analysts assess the security needs of the organization? (5)	BTL6	Creating
13	Explain in detail about the reports of interpretation and analysis. (13)	BTL 5	Evaluating
14	Analyze and Explain about Automated feeds and APIs in detail.	BTL4	Analyzing
15	Briefly explain about steps involved in customization of threat data. (13)	BTL2	Understanding
16	Examine about (i) Searchable knowledge base (7) (ii) Tailored reports (6)	BTL3	Applying
17	Explain in detail about the steps in disseminating the cyber threat information. (13)	BTL 5	Evaluating

PART - C

Q.No	Question	Level	Competence
1	Explain in detail about the intelligence platform with suitable examples. (15)	BTL5	Evaluating
2	Describe the role of searchable knowledge base in disseminating the cyber threat data. (15)	BTL6	Creating
3	Describe about the various steps in validation and prioritization of cyber threat information. (15)	BTL6	Creating
4	Explain in detail about the steps in disseminating the cyber threat information. (15)	BTL5	Evaluating
5	Explain in detail about the interpretation and analysis of cyber threat information. (15)	BTL5	Evaluating

UNIT – V : OPEN SOURCE SOFTWARE DEVELOPMENT

Types of Partners: Providers of threat indicators, Providers of threat data feeds, Providers of comprehensive cyber threat intelligence. Important Selection Criteria: Global and cultural reach, Historical data and knowledge, Range of intelligence deliverables, APIs and integrations, Intelligence platform, knowledge base, and portal, Client services, Access to experts. Intelligence–driven Security.

PART – A

Q.No	Question	Level	Competence
1	Differentiate between threat indicator and threat data feeds	BTL3	Applying
2	Point out the importance of Intelligence platform.	BTL4	Analyzing
3	List the advantages of open source software development.	BTL1	Remembering
4	What are the Key characteristics of open source software development.	BTL2	Understanding
5	Define the role of CERTs and SOCs.	BTL2	Understanding
6	List the types of partners.	BTL1	Remembering
7	List who are the providers of threat data feeds.	BTL1	Remembering
8	List who are the providers of threat indicators.	BTL1	Remembering
9	Discuss the features of FireEye.	BTL2	Understanding
10	Define Intelligence–driven Security.	BTL1	Remembering
11	Generalize the key criteria for selecting the global and cultural reach in CTI.	BTL6	Creating
12	Analyze Cyber Threat Alliance.	BTL4	Analyzing
13	List the examples of Open-Source Threat Intelligence Platforms.	BTL3	Applying
14	Define the selection criteria related to historical data and knowledge in cyber threat intelligence.	BTL2	Understanding
15	Show the advantages of Threat actor profiles.	BTL3	Applying
16	Assess the role of threat hunting playbook.	BTL5	Evaluating
17	List the importance of Data Breach Repository.	BTL1	Remembering
18	Point out the uses of portal in CTI.	BTL4	Analyzing
19	Investigate Which platform provides highly actionable threat data.	BTL6	Creating
20	Assess the key aspects of APIs and integrations in cyber threat intelligence.	BTL5	Evaluating
21	List the role of Information sharing and analysis centers (ISACs).	BTL3	Applying
22	What are the client services provided for the security teams by the organization?	BTL2	Understanding
23	Point out the features of intelligence platform.	BTL4	Analyzing
24	Judge the role of threat intelligence experts.	BTL5	Evaluating

PART – B

Q.No	Question	Level	Competence
1	Describe the role of providers of threat indicators. (13)	BTL1	Remembering
2	(i) List the key elements of Intelligence driven security. (6) (ii) List the benefits of Intelligence driven security. (7)	BTL1	Remembering
3	Describe in detail about the key aspects of APIs and integration in CTI.(13)	BTL1	Remembering
4	Describe about providers of threat data feeds. (13)	BTL2	Understanding
5	Discuss the key selection criteria for CTI. (13)	BTL2	Understanding
6	Describe about the Range of intelligence deliverables in cyber threat intelligence. (13)	BTL1	Remembering
7	Examine about (i) Intelligence platform. (6)	BTL3	Applying

	(ii)Knowledge base and portal.(7)		
8	Explain the following: iii) Intelligence driven security. (7) iv) Threat intelligence Experts. (6)	BTL4	Analyzing
9	(i) Explain about the Providers of comprehensive cyber threat intelligence. (6) ii) Compare threat indicator and threat data feeds (7)	BTL4	Analyzing
10	Discuss the common types of partners in cyber threat intelligence model.(13)	BTL2	Understanding
11	Examine the following (i) FireEye (6) (ii) Symantec Threat Intelligence (7)	BTL3	Applying
12	i) Discuss the main characteristics of threat indicators. (6) ii) Explain about CrowdStrike Falcon Intelligence (7)	BTL6	Creating
13	Demonstrate Key characteristics and advantages of open source software development with examples. (13)	BTL 5	Evaluating
14	Briefly explain about Government cyber security Agencies. (13)	BTL4	Analyzing
15	Explain the Providers of comprehensive cyber threat intelligence. (13)	BTL2	Understanding
16	Examine the important selection criteria for cyber threat provider with global and cultural reach. (13)	BTL3	Applying
17	Explain the following: i) Cyber Threat Alliance (CTA) (6) ii) Cybersecurity Tech Accord. (7)	BTL 5	Evaluating

PART - C			
Q.No	**Question**	**Level**	**Competence**
1	Explain the following: i) Intelligence Platform. (5) ii) Range of Intelligence deliverables. (5) iii) Cyber Threat Alliance. (5)	BTL5	Evaluating
2	Examine the following: i) Providers of Comprehensive cyber threat intelligence. (8) ii) Experts of threat intelligence.(7)	BTL6	Creating
3	Discuss about the various types of partners in Cyber Threat Intelligence. (15)	BTL6	Creating
4	Explain about Intelligence driven security in detail. (15)	BTL5	Evaluating
5	Describe the role of providers of threat indicators and threat data feeds in detail..(15)	BTL5	Evaluating