O.P.Code: 23CS0929	R23	H.T.No.									

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR
(AUTONOMOUS)
B.Tech. III Year II Semester Regular Examinations April-2026
CYBERSECURITY & AI DRIVEN THREAT DETECTION
(Common to CSM & CAI)

Time: 3 Hours **Max. Marks: 70**

PART-A
(Answer all the Questions **10 x 2 = 20** Marks)

1	a	Define CIA Triad.	CO1	L1	2M
	b	What is access control?	CO1	L1	2M
	c	What is a feature in ML?	CO2	L1	2M
	d	Define supervised learning.	CO2	L1	2M
	e	Define DNN.	CO3	L1	2M
	f	What is RNN?	CO3	L1	2M
	g	Define log analysis.	CO4	L1	2M
	h	Name SIEM tools.	CO4	L1	2M
	i	Name some laws related to cybersecurity.	CO5	L1	2M
	j	Define AI bias.	CO5	L1	2M

PART-B
(Answer all Five Units **5 x 10 = 50** Marks)

UNIT-I

2	a	Explain DDoS attack.	CO1	L2	5M
	b	Define DDoS attack mitigation techniques.	CO1	L2	5M
		OR			
3	a	Describe the steps involved in risk assessment.	CO1	L2	5M
	b	Explain vulnerability management.	CO1	L2	5M

UNIT-II

4	a	Evaluate the effectiveness of security policies in protecting organizational assets.	CO2	L5	5M
	b	Compare and analyze different types of cyber attacks such as DoS, DDoS, and Man-in-the-Middle attacks.	CO2	L4	5M
		OR			
5	a	Explain SVM, Random Forest, and KNN briefly.	CO2	L3	5M
	b	Compare K-means and DBSCAN clustering.	CO2	L4	5M

UNIT-III

6	a	Illustrate how Recurrent Neural Networks (RNNs) can be applied to analyze system logs and network traffic for intrusion detection.	CO3	L4	5M
	b	Analyze the advantages and limitations of using LSTMs for sequential log data in cybersecurity applications.	CO3	L4	5M
		OR			
7	a	Describe the architecture of Convolutional Neural Networks (CNNs).	CO3	L2	6M
	b	Explain Convolutional Neural Networks (CNNs) use in malware classification through binary analysis.	CO3	L2	4M

UNIT-IV

8	a	Explain the concept of Security Information and Event Management (SIEM) and its role in modern cybersecurity operations.	CO4	L2	6M
	b	Describe the process of log collection, normalization, and correlation in SII systems for real-time alerting.	CO4	L2	4M
		OR			
9	a	What are the challenges in real-time threat detection?	CO4	L4	5M
	b	Describe the key functions and responsibilities of a Security Operations Center (SOC).	CO4	L2	5M

UNIT-V

10	a	Explain the role of Artificial Intelligence in penetration testing.	CO5	L3	5M
	b	Discuss how AI-based tools automate vulnerability scanning and exploitation.	CO5	L3	5M
		OR			
11	a	Explain how organizations ensure compliance with data protection laws in AI-based security systems	CO5	L5	5M
	b	Discuss the importance of Zero Trust architecture in future cybersecurity.	CO5	L5	5M

***** END *****