Course Code: 23CS0929 **R23**

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY : PUTTUR
(AUTONOMOUS)
Siddharth Nagar, Narayanavanam Road – 517583
QUESTION BANK (DESCRIPTIVE)

Subject with Code: Cybersecurity & AI-driven Threat Detection (23CS0929)
Course & Branch: B. Tech –CSM & CAI
Regulation: R23 **Year & Sem:** III - B.Tech & II-Sem

UNIT – I
Fundamentals of Cybersecurity

1	**a)**	Define CIA Triad?	**[L1][CO1]**	**[2M]**
	b)	What is a vulnerability?	**[L1][CO1]**	**[2M]**
	c)	Define malware?	**[L1][CO1]**	**[2M]**
	d)	What is access control?	**[L1][CO1]**	**[2M]**
	e)	Name some cybersecurity frameworks.	**[L1][CO1]**	**[2M]**
2	Explain the types of Attacks in detail.		**[L3][CO1]**	**[10M]**
3	**a)**	What is phishing? Explain elaborately.	**[L2][CO1]**	**[5M]**
	b)	Describe phishing types and prevention methods.	**[L2][CO1]**	**[5M]**
4	Differentiate between virus, worm, ransomware, and rootkit.		**[L4][CO1]**	**[10M]**
5	List and explain common threats and vulnerabilities in cybersecurity.		**[L3][CO1]**	**[10M]**
6	**a)**	Explain DDoS attack.	**[L2][CO1]**	**[5M]**
	b)	Define DDoS attack mitigation techniques.	**[L2][CO1]**	**[5M]**
7	**a)**	Describe the steps involved in risk assessment.	**[L2][CO1]**	**[5M]**
	b)	Explain vulnerability management.	**[L2][CO1]**	**[5M]**
8	What are symmetric, asymmetric encryption and hashing? How are they used?		**[L3][CO1]**	**[10M]**
9	Explain the purpose of NIST, ISO 27001, and OWASP frameworks.		**[L3][CO1]**	**[10M]**
10	What are insider threats? How can they be prevented?		**[L4][CO1]**	**[10M]**

Course Code: 23CS0929 **R23**

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY : PUTTUR
(AUTONOMOUS)
Siddharth Nagar, Narayanavanam Road – 517583
QUESTION BANK (DESCRIPTIVE)

Subject with Code: Cybersecurity & AI-driven Threat Detection (23CS0929)
Course & Branch: B.Tech – CSM & CAI
Regulation: R23 **Year & Sem:** III - B.Tech & II-Sem

UNIT – II
Machine Learning for Cyber Threat Detection

1	a)	Define supervised learning.	[L1][CO2]	[2M]
	b)	What is a feature in ML?	[L1][CO2]	[2M]
	c)	Name two ML algorithms.	[L1][CO2]	[2M]
	d)	Define accuracy in ML.	[L1][CO2]	[2M]
	e)	What is clustering?	[L1][CO2]	[2M]
2	a)	Describe different types of malware attacks such as viruses, worms, Trojans, and ransomware.	[L2][CO2]	[5M]
	b)	Explain how they affect computer systems.	[L2][CO2]	[5M]
3	a)	Evaluate the effectiveness of security policies in protecting organizational assets?	[L5][CO2]	[5M]
	b)	Compare and analyze different types of cyber attacks such as DoS, DDoS, and Man-in-the-Middle attacks.	[L4][CO2]	[5M]
4		Differentiate supervised and unsupervised learning with examples.	[L4][CO2]	[10M]
5		Give examples of feature engineering for cyber threat detection.	[L3][CO2]	[10M]
6	a)	Explain SVM, Random Forest, and KNN briefly.	[L3][CO2]	[5M]
	b)	Compare K-means and DBSCAN clustering.	[L4][C02]	[5M]
7	a)	Define accuracy, precision, ROC, and F1-score.	[L1][CO2]	[5M]
	b)	What are challenges in ML-based threat detection?	[L4][CO2]	[5M]
8	a)	Describe a phishing detection scenario using ML.	[L3][CO2]	[5M]
	b)	Outline the ML workflow for cyber threat detection.	[L2][CO2]	[5M]
9		Design a basic cybersecurity strategy for a small organization, addressing threats, access control, data protection, and incident response.	[L6][CO2]	[10M]
10		How does normalization improve ML performance?	[L2][CO2]	[10M]

Course Code: 23CS0929 **R23**

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY : PUTTUR
(AUTONOMOUS)
Siddharth Nagar, Narayanavanam Road – 517583
QUESTION BANK (DESCRIPTIVE)

Subject with Code: Cybersecurity & AI-driven Threat Detection (23CS0929)
Course & Branch: B.Tech – CSM & CAI
Regulation: R23 **Year & Sem:** III - B.Tech & II-Sem

UNIT – III
Deep Learning in Threat Intelligence

1	**a)**	Define DNN.	**[L1][CO3]**	**[2M]**
	b)	What is RNN?	**[L1][CO3]**	**[2M]**
	c)	Explain autoencoder.	**[L1][CO3]**	**[2M]**
	d)	Define CNN.	**[L1][CO3]**	**[2M]**
	e)	What is an adversarial attack?	**[L1][CO3]**	**[2M]**
2	**a)**	Explain the role of Deep Neural Networks (DNNs) in cybersecurity.	**[L2][CO3]**	**[5M]**
	b)	Discuss how deep learning differs from traditional machine learning approaches in threat detection.	**[L3][CO3]**	**[5M]**
3	Illustrate how Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks can be applied to analyze system logs and network traffic for intrusion detection?		**[L4][CO3]**	**[10M]**
4	Analyze the advantages and limitations of using RNNs and LSTMs for sequential log data in cybersecurity applications.		**[L4][CO3]**	**[10M]**
5	**a)**	Describe the architecture of Convolutional Neural Networks (CNNs).	**[L2][CO3]**	**[05M]**
	b)	Explain Convolutional Neural Networks (CNNs) use in malware classification through binary analysis.	**[L2][CO3]**	**[05M]**
6	Compare CNN-based malware detection techniques with traditional static and dynamic malware analysis methods?		**[L4][CO3]**	**[10M]**
7	Evaluate the impact of adversarial attacks on AI-based security systems. Discuss common attack techniques and their consequences.		**[L5][CO3]**	**[10M]**
8	Describe a case study using LSTM for anomaly detection.		**[L2][CO3]**	**[10M]**
9	Compare ML vs. DL in cyber threat detection.		**[L4][CO3]**	**[10M]**
10	Outline the deep learning workflow in threat intelligence.		**[L6][CO3]**	**[10M]**

Course Code: 23CS0929 **R23**

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY : PUTTUR
(AUTONOMOUS)
Siddharth Nagar, Narayanavanam Road – 517583
QUESTION BANK (DESCRIPTIVE)

Subject with Code: Cybersecurity & AI-driven Threat Detection (23CS0929)
Course & Branch: B.Tech – CSM & CAI
Regulation: R23 **Year & Sem:** III - B.Tech & II-Sem

UNIT-IV

Real-Time Threat Detection and SIEM Systems

1	**a)**	Define SIEM.	**[L1][CO4]**	**[2M]**
	b)	What is TIP?	**[L2][CO4]**	**[2M]**
	c)	Define log analysis.	**[L1][CO4]**	**[2M]**
	d)	Name SIEM tools.	**[L1][CO4]**	**[2M]**
	e)	What is packet inspection?	**[L2][CO4]**	**[2M]**
2	**a)**	Explain the concept of Security Information and Event Management (SIEM) and its role in modern cybersecurity operations.	**[L2][CO4]**	**[5M]**
	b)	Describe the process of log collection, normalization, and correlation in SIEM systems for real-time alerting.	**[L2][CO4]**	**[5M]**
3	Explain real-time alert generation in SIEM tools with an example and describe the role of Threat Intelligence Platforms (TIPs) in improving threat detection.		**[L3][CO4] [10M]**	
4	**a)**	Explain the role of TIPs in SIEM..	**[L2][CO4]**	**[5M]**
	b)	How does AI enhance SIEM capabilities.	**[L2][CO4]**	**[5M]**
5	Explain how Machine Learning models are used in threat detection and describe the concept of event correlation in SIEM systems.		**[L3][CO4] [10M]**	
6	**a)**	What are the challenges in real-time threat detection?	**[L4][CO4]**	**[5M]**
	b)	Describe the key functions and responsibilities of a Security Operations Center (SOC).	**[L2][CO4]**	**[5M]**
7	**a)**	Explain AI-driven SOC functionalities.	**[L3][CO4]**	**[5M]**
	b)	Compare signature-based detection with anomaly-based detection in the context of SIEM and network monitoring.	**[L4][CO4]**	**[5M]**
8	**a)**	Analyze the role of AI in detecting Advanced Persistent Threats (APTs) using SIEM data.	**[L4][CO4]**	**[5M]**
	b)	Design a real-time alerting mechanism using SIEM and AI techniques for a large enterprise network.	**[L6][CO4]**	**[5M]**
9	Explain how ELK Stack processes and visualizes security logs for threat monitoring.		**[L2][CO4]**	**[10M]**
10	Analyze how false positives impact SOC efficiency and explain how AI can help reduce alert fatigue		**[L4][CO4]**	**[10M]**

Course Code: 23CS0929 **R23**

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY : PUTTUR
(AUTONOMOUS)
Siddharth Nagar, Narayanavanam Road – 517583
QUESTION BANK (DESCRIPTIVE)

Subject with Code: Cybersecurity & AI-driven Threat Detection (23CS0929)
Course & Branch: B. Tech – CSM & CAI
Regulation: R23 **Year & Sem:** III - B.Tech & II-Sem

UNIT-V

Ethical Hacking, Privacy, and Legal Aspects

1	**a)**	Define ethical hacking.	**[L1][CO5]**	**[2M]**
	b)	What is GDPR?	**[L1][CO5]**	**[2M]**
	c)	Name some laws related to cybersecurity.	**[L1][CO5]**	**[2M]**
	d)	Define AI bias.	**[L1][CO6]**	**[2M]**
	e)	Explain Zero Trust.	**[L1][CO6]**	**[2M]**
2		Explain the role of Artificial Intelligence in penetration testing and discuss how AI-based tools automate vulnerability scanning and exploitation.	**[L3][CO5]**	**[10M]**
3	**a)**	Analyze the advantages and risks of using AI-driven penetration testing tools compared to traditional methods.	**[L4][CO5]**	**[5M]**
	b)	Describe the concepts of Red Team and Blue Team and explain their significance in cybersecurity simulations.	**[L2][CO5]**	**[5M]**
4	**a)**	Compare Red Team vs. Blue Team exercises in terms of objectives, tools used, and outcomes	**[L2][CO5]**	**[5M]**
	b)	Explain the key principles of data privacy regulations such as GDPR and HIPAA	**[L4][CO5]**	**[5M]**
5		Explain how organizations ensure compliance with data protection laws in AI-based security systems and discuss the importance of Zero Trust architecture in future cybersecurity.	**[L5][CO6]**	**[10M]**
6	**a)**	Analyze how AI-driven Security Operations Centers (AI SOCs) improve threat detection and incident response.	**[L4][CO6]**	**[5M]**
	b)	Illustrate the working of federated threat detection and explain how it helps in preserving data privacy.	**[L3][CO6]**	**[5M]**
7		Analyze ethical challenges in automated AI-based cybersecurity decision-making and evaluate the impact of AI bias and fairness on security systems.	**[L5][CO6]**	**[10M]**
8	**a)**	Define ethical hacking. List any four objectives of ethical hacking.	**[L1][CO6]**	**[5M]**
	b)	What is penetration testing? Name the different phases of penetration testing.	**[L1][CO6]**	**[5M]**
9		Explain fairness in AI decision-making with a simple example from cybersecurity.	**[L2][CO6]**	**[10M]**
10	**a)**	Explain the role of AI in future Security Operations Centers (AI SOC).	**[L2][CO6]**	**[5M]**
	b)	What is federated threat detection? State its main advantages.	**[L1][CO6]**	**[5M]**