Course Description:

The Cybersecurity II course provides a comprehensive overview of key concepts and practices in cybersecurity. Students learn to identify and mitigate common threats and vulnerabilities, including malware, ransomware, and social engineering attacks. The course covers critical access management, encryption methods, and network security, with a focus on securing wireless networks, implementing firewalls, and VPN technologies. Participants also explore endpoint security, vulnerability management, risk assessment, and the principles of disaster recovery and business continuity planning. Additionally, students gain practical skills in incident handling, digital forensics, and monitoring security events, ensuring they are prepared to respond to cybersecurity incidents and comply with regulatory frameworks.

Module	Objectives
Module 1: Essential Security Principles	• Understand the significance of the CIA triad in maintaining confidentiality, integrity, and availability of data, systems, services, and networks.
	• Define common security terms used in cybersecurity, including vulnerabilities, threats, exploits, and risks.
	• Explore various types of attackers and their reasons for attacks.
	• Examine the importance of creating and adhering to a code of ethics as an essential security measure.
	• Explain common threats such as malware variants, DDoS and Man-in-the-Middle attacks, and vulnerabilities associated with Internet of Things (IoT) devices worldwide.
	• Explore other threats like insider threats, different social engineering tactics, physical attacks, and Advanced Persistent Threats (APTs), and why they are a growing concern for cybersecurity.

Module 2: Access Management Basics	• Understand the importance of the Authentication, Authorization, and Accounting (AAA) security framework.
	• Explain the importance of multifactor authentication (MFA) and password policies and understand the RADIUS protocol.
	• Explain the concepts of encryption and decryption, including the different types of encryptions.
	• Examine the application of certificates and public key infrastructure (PKI) in identity authentication and protection.
	• Explore hashing algorithms and when they are used.

Module 3: Basic Network Security Concepts	• Learn about the common TCP/IP protocols, their vulnerabilities, and ways to mitigate them.
	• Understand how network addresses impact network security.
	• Explore various network infrastructures and technologies.
	• Learn about secure access technologies.
	• Understand how to set up secure wireless SOHO networks.

Module 4: Endpoint Security Concepts Part I	• Understand operating system security concepts and learn about Windows Defender, PowerShell, and NTFS permissions.
	• Learn about Linux and macOS endpoint security concepts.
	• Explore various endpoint tools, including netstat, nslookup, and tcpdump.
	• Understand the significance of asset management, program deployment, and data backups in satisfying endpoint security policies.
	• Learn about BYOD security policies and endpoint regulatory compliance, including PCI DSS, HIPAA, and GDPR.
	• Understand operating system security concepts and learn about Windows Defender, PowerShell, and NTFS permissions.

Module 5 Endpoint Security Concepts Part II	• Implement hardware and software updates using Windows Update.
	• Understand and interpret system logs using Windows Event Viewer.
	• Demonstrate familiarity with malware removal, including scanning systems, scan log reviews, and malware remediation.

Module 6: Vulnerability Assessment and Risk Management Part I	• Explore the key concepts of vulnerability management, including identification, management, and mitigation strategies.
	• Examine active and passive reconnaissance techniques and learn about various testing methods such as port scanning and automation.
	• Explore threat intelligence techniques and learn about the uses and limitations of vulnerability databases, including Common Vulnerabilities and Exposures (CVEs).
	• Learn about industry-standard tools for assessing vulnerabilities and understand the role of cybersecurity reports, news, and subscription services in threat identification.
	• Understand collective, ad hoc, and automated threat intelligence.
	• Learn about the significance of documenting information proactively before, during, and after cybersecurity incidents, including ways to secure, share, and update the documentation.

Module 7: Vulnerability Assessment and Risk Management Part II	• Learn about risk identification, risk prioritization, risk levels, and risks associated with specific data types and classifications.
	• Understand the fundamental concepts of risk management and learn about its strategies.
	• Understand how security assessments of IT systems contribute to risk mitigation.
	• Learn about various disasters and understand the significance of disaster recovery plans.
	• Explore various types of backups and learn about the business continuity plan.

Module 8: Incidents Handling	• Monitor security events and know when escalation is required
	• Explain digital forensics and attack attribution processes
	• Explain the impact of compliance frameworks on incident handling
	• Describe the elements of cybersecurity incident response