Cyber Security

CURRICULUM:

UNIT -I NETWORKING AND WEB TECHNOLOGY

Network Components - Network Basics - Network Communication -Web Technologies TCPIP - Web Services

UNIT-II INTRODUCTION TO CYBER SECURITY

Recent Cyber Attacks - Cyber Security Concepts - Layers of Cyber Security - Introduction to Application Security - Secure Coding OWASP Top 10 - Coding Practices Secure Design – Closure [Practical demos and code on OWASP vulnerabilities and how to mitigate them]

UNIT III FUNDAMENTALS OF INFORMATION SECURITY & FUNDAMENTALS OF CRYPTOGRAPHY

Why information security? - What is information security? - Data Security - Network security - Application Security – Closure. Why Cryptography? – Cryptography - Shared Key Cryptography – Illustration - Shared Key Cryptography - Public Key Cryptography – Illustration - Public Key Cryptography – Hashing -Digital Signature – Illustration - Digital Signature - Applications of cryptography – Conclusion [Algorithmic representation of cryptographic methods]

UNIT-IV THREAT MODELING & IDENTITY AND ACCESS MANAGEMENT

Basics of Threat Modeling - Learn Threat Modeling with a Use Case - Tool Walkthrough - MS Threat Modeling Tool – Assignment - Introduction to Identity and Access Management - Security Standards and Regulations: PCI DSS – ISMS - FIPS and NIST Special Publications – FISMA – GDPR – HIPAA – SOX – Conclusion - Identity Governance and Administration: Need for IGA & basics concepts - IGA Basic Concepts and Onboarding - IGA Governance - Identity Administration in IGA - What next?

UNIT-V JAVA SE 11 PROGRAMMER II: SECURE CODING IN JAVA SE 11 APPLICATIONS

Course Overview – Managing Denial of Service – Securing Information – Managing Data Integrity – Accessibility and Extensibility – Securing Objects – Serialization and Deserialization Security – JCA and its Principles – Provider Architecture – Engine Class – Key Pair Generation – Signature Management – Unsecure to Secure Object – Course Summary. [Demos of Secure Coding in Java]

Course Duration: 45 Hours

Test Projects:

The following industry use cases highlight the importance of cybersecurity across various industries to mitigate risks, protect assets, and ensure the continuity of operations in an increasingly digital and interconnected world:

1. **Finance Sector:** Protecting financial transactions, customer data, and sensitive information from cyber threats such as data breaches and financial fraud.

2. **Healthcare Industry:** Safeguarding patient records, medical devices, and health information systems from cyberattacks to ensure patient privacy and maintain the integrity of medical data.

3. **Government Agencies**: Securing government networks, infrastructure, and classified information from cyber threats to prevent espionage, data theft, and disruption of critical services.

4. **Retail and E-commerce**: Ensuring the security of online payment systems, customer databases, and e-commerce platforms to prevent credit card fraud, identity theft, and website defacement.

5. **Manufacturing Sector**: Protecting industrial control systems (ICS) and operational technology (OT) from cyber threats to prevent production disruptions, equipment damage, and intellectual property theft.

6. **Energy and Utilities**: Securing power grids, oil and gas pipelines, and renewable energy infrastructure from cyberattacks to prevent service outages, environmental damage, and potential safety hazards.

7. **Transportation and Logistics**: Protecting transportation networks, vehicle systems, and supply chain operations from cyber threats to ensure the safety of passengers, cargo, and critical infrastructure.

8. **Telecommunications**: Securing communication networks, mobile devices, and internet services from cyberattacks to protect user privacy, prevent service disruptions, and maintain network reliability.

9. **Education Institutions**: Safeguarding student records, academic systems, and online learning platforms from cyber threats to protect sensitive information and maintain the integrity of educational services.

10. **Hospitality**: Protecting guest information, reservation systems, and hotel networks from cyber threats to uphold the reputation of hospitality businesses and ensure customer satisfaction.

11. **Media and Entertainment**: Securing digital content, streaming platforms, and user accounts from cyber-attacks to protect intellectual property rights and maintain consumer trust.
12. **Legal Services**: Safeguarding sensitive client information, case files, and communication channels from cyber threats to maintain client confidentiality and uphold ethical standards.

13. **Nonprofit Organizations**: Protecting donor information, fundraising platforms, and mission-critical systems from cyber-attacks to maintain trust with donors and stakeholders.

14. **Real Estate**: Securing property management systems, client data, and financial transactions from cyber threats to protect sensitive information and maintain business operations.

15. **Technology Companies**: Defending software development processes, intellectual property, and customer data from cyber-attacks to maintain the integrity of products and services and ensure customer trust.