CYBERSECURITY

(Creating Best of Minds)

Professional Certificate in Cybersecurity

Course Code: IT_CT_I_0001/25

Duration: 40 Hours

Delivery Format: Hybrid

Target Audience:

- Aspiring Cybersecurity Professionals: Ideal for beginners or those looking to start a career in cybersecurity.
- IT Professionals: For those wanting to deepen their cybersecurity knowledge.
- Network Administrators & Security Engineers: Focused on securing network infrastructures and systems.
- Business Leaders & Managers: Professionals responsible for protecting organizational assets.

Program Objectives:

- Understand Cybersecurity Basics: Recognize the importance of cybersecurity and common threats.
- Secure Networks: Apply knowledge of firewalls, VPNs, and network security in real scenarios.
- Respond to Threats: Detect and handle cyber-attacks like malware, phishing, and social engineering.
- Implement Data Protection: Apply data encryption and loss prevention strategies.

- Manage Identity & Access: Set up systems for multi-factor authentication and access control.
- Understand Cloud Security: Secure cloud data and manage identity in cloud environments.
- Handle Incidents: Develop and practice an Incident Response Plan.
- Use Security Tools: Gain hands-on experience with network analysis and penetration testing tools.
- Explore Ethical Hacking: Understand penetration testing techniques to identify vulnerabilities.
- Prepare for Emerging Threats: Stay updated on future cybersecurity trends like IoT, AI, and blockchain.

Detailed Syllabus

Module 1: Introduction to Cybersecurity

Objective: To introduce the core concepts of cybersecurity and provide a foundation for understanding cybersecurity principles.

Topics:

Overview of Cybersecurity:

- Definition and importance of cybersecurity in modern organizations.
- Cybersecurity challenges faced by businesses today.
- Introduction to common cyber threats (e.g., viruses, ransomware, phishing, etc.).

Cybersecurity Frameworks:

- Understanding NIST, ISO, and other cybersecurity frameworks.
- Overview of policies, procedures, and standards in cybersecurity.

Activities:

- Basic understanding of setting up secure environments (passwords, user authentication).

Assessments:

- Quiz on basic cybersecurity concepts.
- Assignment on identifying common cyber threats and security frameworks.

Module 2: Network Security Fundamentals

Objective: To provide a strong foundation in network security principles and the use of security tools.

Topics:

Network Security Basics:

- Types of networks: LAN, WAN, VPN, and cloud networks.
- Network components: Routers, firewalls, switches, and their roles in security.

Firewalls and VPNs:

- What are firewalls? Types and functions (stateful, stateless, next generation).
- Setting up VPNs and their role in securing remote connections.

Intrusion Detection and Prevention Systems (IDPS)

Activities:

- Configuring basic firewall settings on a router.
- Setting up a VPN for secure remote access.

Assessments:

- Assignment on network security concepts and firewall configurations.
- Practical assessment on setting up a secure VPN connection.

Module 3: Threats and Attacks in Cybersecurity

Objective: To develop the ability to recognize, classify, and understand various cyber threats and attacks.

Topics:

Types of Cyber Attacks:

- Malware (viruses, worms, trojans, ransomware).
- Phishing, spear phishing, and social engineering.
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks.

Case Studies:

- Overview of high-profile cyber-attacks (e.g., Target, Sony, etc.).

Activities:

- Simulated phishing attacks (phishing email awareness training).

- Identifying malware in files and websites.

Assessments:

- Report on a chosen cyber-attack case study.
- Assessment on identifying and classifying different types of cyber threats.

Module 4: Data Protection and Privacy

Objective: To gain expertise in data protection laws, regulations, and encryption techniques.

Topics:

Data Protection Laws & Regulations:

- GDPR, HIPAA, CCPA, and other privacy laws.
- Understanding data classification and protection principles.

Encryption Basics:

- Symmetric vs. asymmetric encryption.
- How SSL/TLS certificates work.

Data Loss Prevention (DLP)

Activities:

- Hands-on with encryption software.
- Setting up data classification and basic encryption on files.

Assessments:

- Essay on the importance of data protection laws.
- Practical assignment on implementing data encryption.

Module 5: Identity and Access Management (IAM)

Objective: To become proficient in managing digital identities and controlling access to systems and data.

Topics:

Identity Management:

- How identity management systems control access (Single Sign-On (SSO), Multi-Factor Authentication (MFA)).
- Role-based access control (RBAC).

Authentication vs Authorization:

- Different methods of authentication (passwords, biometrics, tokens).

Activities:

- Setting up MFA and SSO for a service.
- Configuring user access and permissions in a system.

Assessments:

- Case study on implementing an IAM system.
- Practical assessment on configuring user access controls.

Module 6: Cloud Security

Objective: To provide an understanding of the unique security challenges and best practices in cloud computing.

Topics:

Cloud Computing Overview:

- Types of cloud models: IaaS, PaaS, SaaS.
- Security challenges in cloud environments.

Cloud Security Best Practices:

- Securing cloud data, identity management, and application security.
- Shared Responsibility Model in cloud security.

Activities:

- Securing data in the cloud (AWS, Google Cloud, or Azure).
- Configuring access and security settings in a cloud environment.

Assessments:

- Report on cloud security challenges and solutions.
- Practical assignment on securing cloud resources.

Module 7: Incident Response and Cybersecurity Policies

Objective: To develop skills in incident handling and creating effective cybersecurity policies.

Topics:

Incident Response (IR):

- Stages of incident response: Detection, containment, eradication, recovery, and lessons learned.
- How to build an Incident Response Plan (IRP).

Cybersecurity Policies:

- Best practices for building organizational cybersecurity policies.
- Risk management and cyber risk assessment.

Activities:

- Developing a basic Incident Response Plan.
- Simulating an IR scenario and walk-through.

Assessments:

- Development of a comprehensive Incident Response Plan.
- Presentation on cybersecurity policies and risk management.

Module 8: Security Tools and Practical Applications

Objective: To gain hands-on experience with security tools used in real-world cybersecurity practices.

Topics:

Security Tools Overview:

- Antivirus software, firewalls, VPNs, and endpoint protection.
- Intrusion detection systems (IDS), network monitoring, and vulnerability scanners.

Hands-on with Security Tools:

- Using Wireshark for network analysis.
- Exploring Kali Linux for penetration testing.

Activities:

- Running vulnerability scans on a network.
- Using security tools to analyze network traffic.

Assessments:

- Report on network traffic analysis using Wireshark.
- Practical assessment on performing vulnerability scans.

Module 9: Ethical Hacking & Penetration Testing Basics

Objective: To introduce the concepts and techniques of ethical hacking and penetration testing.

Topics:

Ethical Hacking Overview:

- Understanding penetration testing, its methodologies (OSCP, CEH).
- Tools used in penetration testing (Nmap, Metasploit).

Penetration Testing Lifecycle:

- Reconnaissance, scanning, exploitation, post-exploitation.

Activities:

- Hands-on with Nmap and basic scanning techniques.
- Understanding and performing vulnerability assessments.

Assessments:

- Report on a penetration testing exercise.
- Practical assessment on using Nmap for network scanning.

Module 10: Emerging Threats and Future Trends in Cybersecurity

Objective: To explore the latest trends and future challenges in the field of cybersecurity.

Topics:

Cybersecurity in the Age of IoT, AI, and Blockchain:

- Security challenges in IoT devices.
- Impact of Artificial Intelligence and Machine Learning on cybersecurity.
- Blockchain and its role in secure transactions.

Future Trends in Cybersecurity:

- The growing need for Zero Trust Security Models.
- Cybersecurity workforce development and skills gap.

Activities:

- Simulated IoT network security analysis.
- Exploring cybersecurity career paths and certifications.

Assessments:

- Essay on the future of cybersecurity.
- Presentation on emerging cybersecurity threats.