€TRAINING

Cyber Security

Cyber Security

Introduction:

Cybersecurity involves protecting systems, networks, and data from digital attacks, theft, and damage through a combination of technologies, processes, and practices. It ensures the confidentiality, integrity, and availability of information in an increasingly connected world. This training program is designed to equip participants with comprehensive knowledge and skills to safeguard digital assets and mitigate cyber threats.

Program Objectives:

At the end of this program, participants will be able to:

- Explore the fundamental concepts of cyber security and its significance in safeguarding organizational assets.
- Identify various cyber threats and vulnerabilities and evaluate associated risks.
- Utilize defensive strategies to enhance network, application, and endpoint security.
- Develop and perform effective incident response and management plans.
- Align cyber security practices with regulatory requirements and governance standards.

Target Audience:

- IT professionals and network administrators.
- Cyber security analysts and incident responders.
- Managers and executives responsible for IT governance.
- System administrators and technical support staff.

Program Outline:

Unit 1:

Introduction to Cyber Security:

- Cyber Security Fundamentals.
- Importance of Cyber Security in Modern Organizations.
- Threat Landscape Overview.

- Cyber Security Terminology and Concepts.
- Legal and Ethical Considerations in Cyber Security.

Unit 2:

Cyber Threats and Vulnerabilities:

- Types of Cyber Threats: Malware, Phishing, DDoS.
- Vulnerability Assessment and Management techniques,
- Exploitation Techniques.
- Social Engineering and Insider Threats.
- Attack Surfaces and Risk Assessment Process.

Unit 3:

Defensive Strategies:

- Network Security Principles.
- Endpoint Protection and Security.
- Encryption Techniques and Applications.
- Access Control and Identity Management.

Unit 4:

Incident Response and Management:

- Incident Response Frameworks: NIST and SANS.
- Incident Detection and Analysis Tools.
- Incident Containment and Eradication.
- Post-Incident Recovery.
- Cyber Security Incident Response Plan CSIRP.

Unit 5:

Compliance and Governance:

- Regulatory Requirements: GDPR and HIPAA
- Cyber Security Standards and Frameworks: ISO 27001 and NIST CSF.
- Role of Compliance in Cyber Security.
- Auditing and Monitoring for Compliance on Regular Bases.
- Cyber Security Policies and Procedures.