€TRAINING

Cyber Security

Cyber Security

Introduction:

This training program is designed to equip participants with comprehensive knowledge and practical skills to safeguard digital assets and mitigate cyber threats. It empowers them to protect organizational data integrity, confidentiality, and availability.

Program Objectives:

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

- Understand fundamental concepts of cyber security.
- Identify common cyber threats and vulnerabilities.
- Implement preventive measures and defensive strategies.
- Conduct effective incident response and management.
- Enhance organizational resilience against cyber attacks.
- Ensure compliance with regulatory requirements.

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.
- Professionals interested in enhancing cyber security knowledge and skills.

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.
- Exploitation Techniques.
- Social Engineering and Insider Threats.
- Attack Surfaces and Risk Assessment.

Unit 3:

Defensive Strategies:

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

Unit 4:

Incident Response and Management:

- Incident Response Frameworks NIST, SANS.
- Incident Detection and Analysis.
- Incident Containment and Eradication.
- Post-Incident Recovery and Lessons Learned.
- Cyber Security Incident Response Plan CSIRP.

Unit 5:

Compliance and Governance:

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