€TRAINING

Cyber Security Specialist

Cyber Security Specialist

Introduction:

This training program offers comprehensive instruction in protecting computer systems, networks, and data from cyber threats. At the end of this program, attendees will be equipped with the skills necessary to secure digital assets, mitigate cyber risks, and safeguard organizations against cyber attacks.

Program Objectives:

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

- Use Neuro-Linguistic Programing NLP to deliver messages that will change the way employees work and think about security.
- Examine the area of wireless security protocols, their security attributes, and their potential insecurities within the organization, and in public spaces.
- Illustrate how penetration testing and ethical hacking enhance organizational security.
- Evaluate and apply two of the most important aspects in the modern day of cyber-adversity: Open Source Intelligence OSINT and cyber threat intelligence.
- Apply information security standards to their organization and its critical assets.
- Identify the threats presented by viruses, malware, active code, and Active Persistent Threats APT and consider the different mitigating options.
- Formulate and manage effective cybersecurity teams, and apply the Computer Security Incident Response Team CSIRT framework, tools, and capabilities to deliver cost-effective and robust solutions to protect the organization.

Targeted Audience:

- IT professionals.
- Security professionals.
- Auditors.
- Site administrators.
- General management.
- Employees tasked with managing and protecting the integrity of the network infrastructure.

Program Outlines:

Unit 1:

Fundamentals of Cybersecurity

- Introduction to cybersecurity principles and concepts.
- Understanding common cyber threats and attack vectors.
- Exploring different types of malware and their characteristics.
- Overview of encryption techniques and their role in securing data.
- Introduction to cybersecurity laws, regulations, and compliance standards.

Unit 2:

Network Security:

- Understanding network architecture and protocols.
- Implementing network security measures such as firewalls, intrusion detection systems IDS, and intrusion prevention systems IPS.
- Securing wireless networks and mitigating wireless security risks.
- Conducting network vulnerability assessments and penetration testing.
- Implementing secure network configuration best practices.

Unit 3:

Cyber Threat Intelligence and Incident Response:

- Introduction to cyber threat intelligence CTI and its importance in cybersecurity.
- Establishing an incident response plan and defining roles and responsibilities.
- Detecting and responding to security incidents in real-time.
- Conducting forensic analysis and digital evidence collection.
- Post-incident analysis and lessons learned for continuous improvement.

Unit 4:

Identity and Access Management IAM:

- Understanding the principles of identity and access management IAM.
- Implementing authentication mechanisms such as passwords, biometrics, and multi-factor authentication MFA.
- Managing user access rights and permissions to systems and data.
- Implementing IAM best practices for privileged account management.
- Monitoring and auditing user activities to detect unauthorized access attempts.

Unit 5:

Secure Software Development and Application Security:

- Understanding secure software development lifecycle SDLC methodologies.
- Implementing secure coding practices to prevent common software vulnerabilities such as injection flaws, XSS, and CSRF.
- Conducting code reviews and security testing static analysis, dynamic analysis to identify and mitigate security flaws.
- Securing web applications, APIs, and mobile applications.
- Implementing secure deployment and configuration management practices for software and applications.