

## Who should enroll

The training also provides foundational knowledge for all support technicians involved in the basic installation, operation, and verification of cyber & information security.

## The job roles best suited to the material in this training are:

- Information Security Analyst / Specialist
- IT Auditor
- Security System Administrator
- Penetration Tester
- Vulnerability Assessment Analyst
- Security Engineer
- Security Architect
- Cryptography Engineer

## Technology areas

- Network Security
- Cyber Security
- Information Security
- Vulnerability Analysis

## Training overview

### Objectives

- Identify the components of a cyber security and describe their basic characteristics
- Understand the latest threats
- Network Monitoring, Protocol Analysis, Vulnerability Analysis, Bug Bounty,
- Cryptography, Cryptanalysis and VPN's
- Security Recommendations & Measures

### Prerequisites

Before taking this training, you should have:

- Basic computer literacy
- Basic PC operating system navigation skills
- Basic Internet usage skills
- Basic IP address & Networking knowledge

- ❖ Introduction to Cyber Security
- ❖ Introduction to Threats
- ❖ OSI Layers, Protocols & Ports
- ❖ Footprinting
- ❖ Reconnaissance
- ❖ Enumeration
- ❖ Social Engineering
- ❖ Network Scanning & Monitoring
- ❖ Session Hijacking
- ❖ Brute Force Attack
- ❖ Vulnerability Analysis (Burp Suit, OWASP, Nikto, CMSeeek, WPScan)
- ❖ SQL Injection
- ❖ Pen Testing
- ❖ Wireless Security
- ❖ Cryptography & Cryptanalysis
- ❖ Network Security Devices
- ❖ Firewall, types and Inspection Techniques
- ❖ Security Recommendations, Countermeasures and Security baseline