Course Title:

Cyber Security First Responder

Duration:

8-12 sessions with certain practical labs.

Class Format Options:

Instructor-led classroom Live Training.

Who Should Attend

- IT administrators
- Data Base administrators
- Web site administrators
- Programmers
- Fresh IT graduate

Student Material:

Student Workbook

Prerequisites:

None- This is an entry-level course

Cyber Security First Responder

Every organization is responsible for ensuring Cyber Security. The ability to protect its information systems from impairment or even theft is essential to success. Implementing effective security measures will not only offer liability protection; it will additionally increase efficiency and productivity.

Cyber security is a high priority for business and all employees must be aware of how to implement protective measures.

With the **Cyber Security First Responder training**course participants will understand the different types of malware and security Common attack and defense strategies for software, web applications, networks, operating systems, and cryptographic.

The challenges will be examined both from the attacker's perspective (how systems are exploited) and the defender's perspectives (how to secure systems or respond to threats).

Cyber Zones developed this outstanding training course to those IT users or users that doesn't have any technical knowledge regarding IT in general.

Cyber Security First Respondertraining course covers the most important areas that each computer/mobile phone users should know and is designed to give you a foundational look at today's cybersecurity landscape and how to evaluate and manage security protocol in information processing systems. They will also understand the basic concepts associated with Cyber Security and what a company needs to stay secure.

The following are covered withinCyber Security First Responder:

- BLUE Team vs RED Team
- Difficulties in Defending against Attacks
- Information Security
- Types of Attacks
- Attackers Methodology
- Five fundamental security principles
- Virtualization Definition and Attacks
- Software-Based Attacks
- Hardware-Based Attacks
- NAS vs SAN
- Cell Phones Definition and Attacks
- Denial-of-Service and Distributed Denial-of-Service
- OSI model
- Address Resolution Protocol
- Defense against attacks
- IDS Vs IPS
- Security Control Decision Classification
- Protecting Systems
- Identifying Vulnerabilities
- Penetration Testing Terminology
- Network Defenses
- Access Control Fundamentals
- Password Definition,attacks, crackers, and Polices
- Authentication and Access Control Terminology
- Authentication, Authorization, and Accounting
- Remote Access Services (RAS)
- Cryptography

- Risk management and Security policies/ procedures
- Network Vulnerabilities and Attacks
- Cisco Systems Endpoint Security Solutions
- NAC Appliance Process
- Hacking Tools examples
- Basic Incident handling
- Basic Digital Forensics

Upon Completion Trainees will:

- Explain basic cyber security terminology; have skills for keeping up to date on cyber security issues; and be able to identify information assets.
- Explain the difference between awareness, education and training
- Describe various basic security practices (e.g. firewalls, account controls, file privacy, etc.)
- Describe basic authentication mechanisms; have skills to improve their password security; and be aware of alternative authentication methods.
- Differentiate between various security threats and computer attacks
- Identify several techniques appropriate to provide basic protection of a small computer and/or small network
- Describe basic incident response techniques
- Identify potential threats to wireless networks
- describe the role of computers and networks in a security context
- identify computer system threats and evaluate their impact
- Demonstrate understanding of firewalls, virtual private networks and network intrusion detection and prevention technologies.
- discuss the effectiveness of various cryptographic techniques and their impact on security, how it has evolved, and some key encryption techniques used today.
- develop basic organizational security policies; anddemonstrate how defense in depth can be used to implement security.
- Identify main malware types; awareness of different malware propagation methods

Training Course Completion

The training course should have a clearly stated end date that is identified before the training begins, At the end of the training course, **Cyber Zones** will:

Give an attendance certificate from **Cyber Zones.**