Kore Infotech
Intelligent IT Solutions
Passionate People

Cyber Security Fundamentals

Cybersecurity is a growing and rapidly changing field. It is crucial that the central concepts that frame and define this pervasive field are understood by professionals who are involved and concerned with the security implications of Information Technologies (IT).

Cybersecurity Fundamentals is a platform to gain security knowledge and professional development to provide IT security and Cybersecurity professionals with the knowledge and technical skills to defend their organization from security breaches and cyber-attacks.

This course, offers a knowledge-based credential on the introductory concepts that frame and define the standards, guidelines and practices of the industry. It also provides an insight into the importance of Cybersecurity and the integral role of cybersecurity professionals.

Who Should Attend This Course:

IT security professionals new to Cybersecurity, IT oriented graduates and those IT professionals looking for a career change to Cybersecurity.

Pre-Requisites:

Few years of IT experience is needed to understand the content of this course.

Course Duration:

This course will be conducted over a period of 5 Days (9.30 am to 5.30 pm)

Objectives:

1. Understand basic cybersecurity concepts and definitions
2. Define network security architecture concepts
3. Recognize malware analysis concepts and methodology
4. Identify network defence and vulnerability assessment tools, including open source tools and their capabilities
5. Explain network systems management principles, models, methods, and tools
6. Distinguish system and application security threats and vulnerabilities
7. Classify types of incidents (categories, responses, and timelines for responses)
8. Outline disaster recovery and business continuity planning
9. Comprehend incident response and handling methodologies
10. Understand security event correlation tools and how different file types can be used for a typical behaviour
11. Identify the basic concepts, practices, tools, tactics, techniques and procedures for processing digital forensic data
12. Recognize new and emerging information technology and information security technologies

Kore Infotech
Intelligent IT Solutions
Passionate People

Course Content

1. **Cybersecurity Introduction And Overview**
   - 1.1. Cybersecurity architecture principles
   - 1.2. Cybersecurity definition
   - 1.3. Objectives of cybersecurity
   - 1.4. Key business and technology factors
   - 1.5. Cybersecurity roles and governance
   - 1.6. Domains of cybersecurity

2. **Cybersecurity Concepts**
   - 2.1. Risk management terms, concepts and frameworks
   - 2.2. Common attack types and vectors
   - 2.3. General process and attributes of cyber attacks
   - 2.4. Malware
   - 2.5. Framework and guidance for policies and procedures
   - 2.6. Cybersecurity control processes

3. **Security Architecture & Frameworks And Standards**
   - 3.1. Perimeter security concepts
   - 3.2. Security architectures
   - 3.3. Security frameworks
   - 3.4. Security Standards and Compliance
   - 3.5. The OSI model and TCP/IP communication protocol
   - 3.6. Defence in depth
   - 3.7. Firewall concepts and implementations
   - 3.8. Isolation and segmentation
   - 3.9. Intrusion detection and prevention systems
   - 3.10. Antivirus and anti-malware
   - 3.11. Encryption fundamentals, techniques and applications

4. **Security Of Networks, Systems, Applications And Data**
   - 4.1. Risk analysis, risk assessments and risk mitigation strategies
   - 4.2. Scanning, assessment and management of vulnerabilities
   - 4.3. Penetration testing
   - 4.4. Network management and configuration
   - 4.5. Port numbers and protocols
   - 4.6. Risk and controls for remote and wireless
   - 4.7. System hardening and virtualization
   - 4.8. Specialized systems (PLC/SCADA)
   - 4.9. Command line knowledge and tools
   - 4.10. System development life cycle (SDLC)
   - 4.11. OWASP top ten application security risk
   - 4.12. Data classification process and requirements

5. **Security Incident Response**
   - 5.1. Distinctions between events and incidents
   - 5.2. Incident categories and types
   - 5.3. Security event management & SIEM
   - 5.4. Key elements of incident response plans
   - 5.5. Legal requirements of investigation and evidence preservation
   - 5.6. Requirements for forensic investigations
   - 5.7. Business continuity planning and disaster recovery

6. **Security Of Emerging Technology**
   - 6.1. Trends in the current threat landscape
   - 6.2. Characteristics and targets of advanced persistent threats (APTs)
   - 6.3. Mobile device vulnerabilities, threats and risk
   - 6.4. BYOD and mobile devices
   - 6.5. Risk and benefits of cloud adoption