Rhythex Consulting
Information Security, Audit & Assurance

TRAINING

CYBERSECURITY FUNDAMENTALS (CSX)

Why become a cybersecurity professional? The protection of information is a critical function for all enterprises. Cybersecurity is a growing and rapidly changing field, and it is crucial that the central concepts that frame and define this increasingly pervasive field are understood by professionals who are involved and concerned with the security implications of Information Technologies (IT). The CSX Fundamental Course is designed for this purpose, as well as to provide insight into the importance of cybersecurity, and the integral role of cybersecurity professionals. This course will also cover four key areas of cybersecurity:

1) cybersecurity architecture principles,

2) security of networks, systems, applications and data,

3) incident response,

4) the security implications of the adoption of emerging technologies.

Designed as a foundational course, it will also prepare learners for the CSX Fundamental Exam.

AREAS OF COVERAGE:

At the conclusion of the course, attendees will be able to:

- Understand basic cybersecurity concepts and definitions
- Apply cybersecurity architecture principles
- Identify components of a cybersecurity architecture
- Define network security architecture concepts including:
  - topology
  - protocols
  - components
  - principles
- Understand malware analysis concepts and methodology
- Recognize the methodologies and techniques for detecting host-and-network-based intrusions via intrusion detection technologies
- Identify computer network defense (CND) and vulnerability assessment tools, including open source tools and their capabilities

- Understand system hardening
- Apply penetration testing principles, tools, and techniques
- Define network systems management principles, models, methods, and tools
- Understand remote access technology and systems administration concepts
- Recognize the Unix command line
- Distinguish system and application security threats and vulnerabilities
- Recognize system lifecycle management principles, including software security and usability
- Understand the local specialized system requirements for safety, performance, and reliability
- Define types of incidents (categories, responses, and timelines for responses)
- Outline disaster recovery and business continuity planning
- Understand incident response and handling methodologies
- Understand security event correlation tools, and how different file types can be used for atypical behavior
- Recognize investigative implications of hardware, operating systems, and network technologies
- Be aware of the basic concepts, practices, tools, tactics, techniques, and procedures for processing digital forensic data
- Identify network traffic analysis methods
- Recognize new and emerging information technology and information security technologies including:
    - The current threat landscape
    - Mobile devices
    - Cloud computing and storage

IN DETAILS

Who Should Attend: The target audience for this course includes:

- Zero to three years' cybersecurity experience.
- Audit, risk, compliance, information security, government and legal professionals with a familiarity of basic IT/IS concepts who:
    - are new to cybersecurity
    - are interested in entering the field of cybersecurity
    - are interested in the ISACA Cybersecurity Certification
- This course would be appropriate for students and recent graduates

What: **2-Days training course in an online or on-site style setting**

How Much: $400