CSX Cybersecurity Practitioner (CSx-P)

Introduction

ISACA's Cybersecurity Practitioner Certification (CSX-P) focuses on the objective of Identification and Protection in the Cybersecurity domain. Candidates who register for this credential will learn how to apply industry-developed, experience-based strategies to identify specific internal and external network threats.

Additionally, candidates will learn about the fundamentals, methods, and tools associated with implementing cybersecurity controls to protect a system from potential threats.

Also, as understudies total the course, they are granted proceeding with proficient instruction (CPE) credits which are material to the upkeep of their expert affirmations.

Course Highlights

This course teaches you about core aspects such as:

- Identification, assessment, and evaluation of assets, threats, and vulnerabilities in internal and external networks
- Implementation of cybersecurity controls to protect a system from identified threats
- Detection of network and system incidents, events, and compromise indicators, along with an assessment of potential damage
- Execution of incident response plans and mitigation of cyber incidents
- Recovery from incidents and disasters, including post-incident-response documentation and implementation of continuity plans

Course Outline

MODULE 1: Business and Security Environment (ID)

- Business Environment
  - Digital Infrastructure
  - Enterprise Architecture
  - Data and Digital Communication
- Security Environment
  - Network
  - Operating Systems
  - Applications
  - Virtualization and Cloud

MODULE 2: Operational Security Readiness (PR)

- Protection
  - Digital and Data Assets
  - Ports and Protocols
  - Protection Technologies
  - Identity and Access Management
  - Configuration Management

- Preparedness
    - Threat Modeling
    - Contingency Planning
    - Security Procedures

MODULE 3: Threat Detection and Evaluation (DE)

- Monitoring
    - Vulnerability Management
    - Security Logs and Alerts
    - Monitoring Tools and Appliances
    - Use Cases
    - Penetration Testing

- Analysis
    - Network Traffic Analysis
    - Packet Capture and Analysis
    - Data Analysis
    - Research and Correlation

MODULE 4: Incident Response and Recovery (RS&RC)

- Incident Handling
    - Notifications and Escalation
    - Digital Forensics

- Mitigation
    - Containment
    - Attack Countermeasures
    - Corrective Actions

- Restoration
    - Security Functions Validation
    - Incident Analysis and Reporting
    - Lessons Learned and Process Improvement

Prerequisites

- Network Scanning
- Specialized Port Scans
- Network Topologies
- Network Log Analysis
- Centralized Monitoring
- Hotfix Distribution
- Vulnerability Scanning
- Traffic Monitoring
- Compromise Indicators
- False Positive Identification
- Packet Analysis
- User Account Controls

Target Audience

CSX Cybersecurity Practitioner Certification Prep Course is intended for professionals established in the cybersecurity field — with a minimum of one to five years of experience. Y

ou should already be able to demonstrate proficiency in the following areas:

- Network Scanning
- Specialized Port Scans
- Network Topologies
- Network Log Analysis
- Centralized Monitoring
- Hotfix Distribution

- Vulnerability Scanning
- Traffic Monitoring
- Compromise Indicators
- False Positive Identification
- Packet Analysis
- User Account Controls

Duration

- 40 hours certification course