1. Course Details:

Course Code : ISAC-002
Course Title : CSX Practitioner Level 1: Identification and Protection
Course Duration : 5 Days

2. Course Overview:

- ISACA's Cybersecurity Nexus (CSX) certification program supports cybersecurity professionals throughout their career by assessing a candidate's abilities and skills at three progressive technical skill levels. Levels are differentiated by skills, not by years of experience. Each technical skill level is assessed utilizing a vendor-neutral set of performance-based exams measuring a candidate's technical skills, abilities and performance.

3. Learning Outcomes:

- Provide participants with an environment to discuss and practice methods implemented by cybersecurity professionals in the Identify and Protect domains
- Ensure participants develop into complimentary team members for enterprises who are workforce ready

4. Course Contents:

Day 1

The first day of this official CSX Practitioner 1 course reviews several topics while also providing labs for participants to gain practical experience. The lessons and labs found below are associated with the following topics: C.I.A., Active / Passive Scanning, Availability / Authenticity, Asset Classification, Network Devices, and OSI Model:

Lessons:

- Hardware and Software Identification and Documentation
- Network Reconnaissance and Scanning
- Sensitive Information Discovery
- Asset Validation and Rogue Devices

Labs:

- Preliminary Scanning
- Additional Scanning Options
- Scanning from Windows

Day 2

Day 2 of this official course reviews several topics while also providing labs for participants to gain practical experience. The lessons and labs found below are associated with the following topics: Scanning, Enumeration, Penetration Training, and Fingerprinting.

Lessons:

- Network Topology Documentation
- Vulnerability Assessment Process
- Patching and Configuration Vulnerability Scanners
- Vulnerability Scanning
- Vulnerability Scanning Analysis

Labs:

- Specialized Linux Port Scans
- Sensitive Information identification
- Network Topology Generation
- Vulnerability Scanner Set-up and Configuration
- Vulnerability Scanner Set-up and Configuration, Pt. 2

Day 3

Day 3 of this CSX Practitioner 1 training course reviews several topics while also providing labs for participants to gain practical experience. The lessons and labs found below are associated with the following topics: Cryptographic Controls, NSIT / ISO Documentation, Network / Host Prevention Systems, Internal Log Processes, and External Documentation.

Lessons:

- Implementing Specified Cyber Security Controls
- Cyber Security Procedure Execution
- Configuring Cyber Security Controls
- Validating Configurations

Labs:

- System Hardening
- Firewall Setup and Configuration

Day 4

The fourth day of training for this course reviews several topics while also providing labs for participants to gain practical experience. The lessons and labs found below are associated with the following topics: Host Logs, Activity Logs, Network Logs, Firewall Logs, IDS Logs, and Encryption.

Lessons:

- Documenting Configuration Changes
- Testing New Controls
- Collecting Event Data
- Sending and Receiving Event Data
- Verifying the Effectiveness of Controls

Labs:

- Log Analysis
- Centralized Monitoring
- Microsoft Baseline Analyzer

Day 5

In the final day of this official CSX Practitioner 1 training seminar, participants review several topics while also participating in various labs to gain practical experience. The lessons and labs found below are associated with the following topics: Non-Repudiation, Multiple Factor Authentication, Information Classification, File System Access Control Mechanisms, Mobile Device Management Policy, and Remote Access Solutions.

Lessons:

- Hardware and Software Identification and Documentation
- Network Reconnaissance and Scanning
- Sensitive Information Discovery
- Asset Validation and Rogue Devices

Labs:

- Preliminary Scanning

- Additional Scanning Options
- Scanning from Windows

5. Our Methodology:

- Make coaching and monitoring innovative and using modern
- Media training also using on the go training by using interactive means and focusing on
- The exercises, practical applications and real situations study.
- Live delivery method, instructor-led training.
- Experienced consultant, trainers, and professional.
- Qualified trainer with high-level experience

6. Attendance Reports:

- Send daily attendance reports to trainingdep
- Send full attendance report to training dep. by the end of thecourse
- Attend 100 % from the course days also providedaily
- Issue attendance certificate for participant who attend minimum 80% from the course duration

7. Pre/Post Reports:

- Pre- assessment before starting training.
- Post assessment after finish training
- Full report for the deferent between Pre-& Post assessment

8. Who Should Attend?

The CSX Practitioner course is intended for professionals with roles focusing on cyber security – with a minimum of one to five years of experience. Participants who register for this course should be proficient in the following areas:

- Network Scanning
- Specialized Port Scans
- Network Topologies
- Network Log Analysis
- Centralized Monitoring
- Vulnerability Scanning

- Traffic Monitoring
- Compromise Indicators
- False Positive Identification
- Packet Analysis