1. Course Details:

Course Code : ISAC-003
Course Title : CSX Practitioner Level 2: Detection
Course Duration : 5 Days

2. Course Overview:

- ISACA's Cybersecurity Nexus (CSX) certification program supports cybersecurity professionals throughout their career by assessing a participant'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.
- This official CSX Practitioner 2 course reviews the "Detect" domain. Participants will learn the basic concepts, methods and tools used to leverage cyber security controls to identify system events and non-event level incidents.CSX Practitioner 2 will help participants develop the ability to serve as a first responder, following established procedures, defined processes and working mostly with known problems on a single system.

3. Learning Outcomes:

Over the course of five days, participants will cover everything they need to know to succeed in the CSX Practitioner 2: Detection exam:

- Traffic Flow Analysis
- IR Resources
- Attack Types
- Attack Methods
- Network Access Control
- Virus Types
- Worm Variants
- Incident Identification Methodologies
- IP Reputation Databases
- Port Scanning
- Host Analysis

- Network Traffic Behavior
- Malware Functionality, Spyware
- Trojans
- NIST Roles
- ISO Designations
- Cert Designation
- CSIRT Roles

4. Course Contents:

Day 1

The first day of this official CSX Practitioner 2 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: Traffic Flow Analysis and IR Resources.

Lessons:

- Analyzing Network Traffic Using Monitors
- Monitoring Network Traffic
- Monitoring Schedule
- Searching for Indicators of Compromise
- Monitoring for False Positives

Labs:

- Using Snort and Wireshark to Analyze Traffic
- Monitoring Network Traffic

Day 2

Day 2 of this official course analyzes several topics while providing labs for Participants to gain practical experience. The lessons and labs found below are associated with the following topics: Attack Types, Attack Methods, Network Access Control, Virus Types, and Worm Variants.

Lessons:

- Escalate Potential Compromises
- Network Packet Analysis
- Malicious Activity and Anti-Virus
- Malicious Code and Activity Types
- Remediation Steps

Labs:

- Searching for Indicators of Compromise
- Monitoring for False Positives

Day 3

The third day of this training seminar focuses on several topics while also providing labs for Participants to gain practical experience. The lessons and labs found below are associated with the following topics: Incident Identification Methodologies, IP Reputation Databases, Port Scanning, Host Analysis, and Network Traffic Behavior.

Lessons:

- Assessing Available Event Information
- Performing Initial Analysis
- Identifying Potential Collection Sources
- Deploy the Data Collection Utility
- Using Event Correlation

Labs:

- Performing an Initial Attack Analysis
- Detect the Introduction and Execution of Malicious Activity
- Analyze and Classify Malware

Day 4

Just like the first three days of training, day 4 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: Malware Functionality, Spyware, Trojans, Rootkits, Viruses, and Backdoors.

Lessons:

- Using Established Baselines to Detect Anomalies
- Documenting Your Steps
- Initial Attack Analysis
- Determine the Initial Scope
- Identify if High-Risk Systems Were Affected

Labs:

- Event Log Collection

- Windows Event Log Manipulation
- Host Integrity Baselining

Day 5

On the final day of training for this official CSX Practitioner 2 course, 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: NIST Roles, ISO Designations, Cert Designation, and CSIRT Roles.

Lessons:

- Monitoring Controls
- Updating Cyber Security Controls
- Patch Management
- Verifying Identities and Credentials
- Cybersecurity Standards and Procedures

Labs:

- IDS Setup
- Personal Security Products
- Verifying Hotfixes
- Linux Users and Groups
- Core Impact Vulnerability Scan

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 2 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