1. Course Details:

Course Code : ISAC-004
Course Title : CSX Practitioner Level 3: Respond and Recover
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 in the following areas: Identify, Protect, Detect, Respond, and Recover.

- CSX Practitioner 3 reviews both the "Respond" and "Recover" domains. With course lecture reinforced with lab sequences, participants will learn how to apply a professional methodology to respond and recover from network incidents or disasters. Participants will discover how to contain an event and protect assets and infrastructure, and learn the components and procedures required for a comprehensive incident response plan.

3. Learning Outcomes:

After completing of ISACA CSX Practitioner III: Respond and Recover course training, participants will be proficient in following areas to perform their role as cybersecurity professional better with wider responsibility:

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

4. Course Contents:

Day 1

On the first day of training for this official CSX Practitioner 3 course, participants will learn about several topics while also participating in various labs to gain practical experience. The lessons and labs for this day of training relate to the following subjects: IR Reputation Databases, IR Procedure, and Real Time Blacklists.

Lessons:

- Defined Response Plan Execution
- Incident Response Escalation Procedures
- System Adverse Effects to Incident Response
- Network Isolation
- Disable User Accounts

Labs:

- Remove Trojan
- Open and Close Ports on Windows 10
- Disable User Accounts on Windows 10
- Block Incoming Traffic on Known Ports

Day 2

The second day of training for this course looks at several different topics while also providing labs for Participants to gain practical experience. The lessons and labs for this day of training relate to the following subjects: IR Procedure, IR Drafting, and IR Frameworks.

Lessons:

- Blocking Traffic
- Assess and Unplug
- System Configuration Changes and Supplemental Monitoring
- IR Documentation and Preservation
- Incident Report

Labs:

- Implement Single System Changes
- Conduct Supplemental Monitoring
- Create Custom Snort Rules

- Install EMET and Edit Host Files
- Comprehensive Assessment

Day 3

Day 3 of this course focuses on teaching Participants about several different topics while also providing them with labs for practical experience. The lessons and labs for day 3 of training relate to the following subjects: Business Unit Integration, Third Party Connection Mechanisms, Warm Site / Cold Site Configurations, and Data Preservation.

Lessons:

- Industry Best Practices
- Disaster Recovery and Business Continuity
- Cyber System Restoration
- Data Backup and Restoration Key Concepts

Labs:

- Patches and Updates

Day 4

On the fourth day of training for this official CSX Practitioner 3 course participants will learn about several topics while also participate in labs to gain practical experience on the material covered. The lessons and labs for this day of training listed below relate to the following subjects: Network Access Control, Data Loss Prevention, Network Backup Procedures, and Encryption Controls.

Lessons:

- Backup Site Preparation and Utilization
- Data Management
- Actualizing Data Backups and Recovery
- Implementing Patches and Updates

Labs:

- Data Backup and Recovery

Day 5

CSX Practitioner 3: Respond and Recover course, participants review several topics while also participating in labs to reinforce the material covered. The lessons and labs that are listed below for this day of training relate to the following subjects: NIST Procedures, ISO Procedures, Team Input, and AAR Generation.

Lessons:

- Ensuring Data Integrity
- Deficiency and Error Reporting
- Post-Incident Review
- Reset and Prep for Future Events
- Temporary Control and Fix Review and Implementation

Labs:

- Recovering Data and Data Integrity Checks

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 Practitioner3 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