CERTIFIED CYBERSECURITY PRACTITIONER

CSX-P

Duration: 5 days; Instructor-led

OVERVIEW

The CSX-P: Certified Cybersecurity Practitioner was named 2016 Top Professional Certification program by the SC Magazine Awards and remains the first and only comprehensive performance certification testing one's ability to perform globally validated cybersecurity skills spanning five security functions – Identify, Protect, Detect, Respond, and Recover.

This course is ideal for professionals with up to five years of experience in a cybersecurity role and an intermediate technical skillset and is conducted in an adaptive, live cyber lab environment, enabling students to build critical technical skills by learning complex concepts and practice applying industry-leading methods. They will learn to utilize the latest open-source tools within actual, real-world scenarios.

CSXP requires candidates demonstrate critical cybersecurity skills in a live, virtual environment assessing candidates' analytical ability to identify and resolve network and host cybersecurity issues by applying foundational cybersecurity knowledge and skills required of an evolving cyber first responder.

OBJECTIVES

The ISACA CSX Practitioner (CSXP) certification verifies that successful candidates have the knowledge and skills required to identify and remediate vulnerabilities; configure and implement protective technologies; and detect, respond, and recover from incidents. The ISACA CSX Practitioner examination is a performance examination consisting of 30 items aligned to the Exam Content Outline (see topics below). This 4-hour exam contains no multiple-choice questions or simulations and intentionally restricts access to the internet.

- Business and Security Environment (23%)
- Operational Security Readiness (23%)
- Threat Detection and Evaluation (27%)
- Incident Response and Recovery (27%)

PREREQUISITES

CSXP candidates should hold at least one of the following certifications: CISA, CRISC, CISM, CGEIT, ECSA, CEH, LPT, GCIH, OSCP, GPEN, CySA+, CISSP, CSX Penetration Testing Overview (CPTO), or CSX Cybersecurity Fundamentals

Or,

If the candidate does not hold at least one of the above certifications, it is recommended that they have 3 years of experience in 3 or more of the 5 CSX-P cybersecurity domains which align with those of the globally accepted NIST Cybersecurity Framework: Identify, Protect, Detect, Respond and Recover.

AUDIENCE

Professionals established in the cybersecurity field with at least 1 to 3 years' experience.

COURSE CONTENTS

Module 1: Identify

Lab:

- Asset Identification
- Data Flow Identification
- Enterprise Asset Identification
- Data Flow Analysis
- Enterprise Data Flow Analysis
- Identify Challenge

Associated Topics:

- Network infrastructure analysis
- Digital asset analysis
- Network topology construction
- Network topology diagrams
- Data flow identification and mapping
- Tools used to construct a network topology diagram
- Tools used to identify data flow
- Importance of security review
- Gap analysis and its usage
- Security policies and procedures
- Development process for policies and procedures
- Information Sharing
- Importance of understanding legal and regulatory requirements
- Threat modeling

Module 2: Protect

Lab:

- Firewall Setup
- Backup and Restore Points
- File System Protections
- OS Baseline
- Protect Challenge

Associated Topics:

- Vulnerability scanning
- Vulnerability scanning personnel
- Vulnerability scanning tools
- Configuring monitoring systems and alert criteria
- Implementing, configuring, and monitoring security tools and systems

- Developing use cases for security monitoring
- Incident response plan development
- Incident response plan testing
- Incorporation of security considerations into business functions
- Monitoring user access, privileges, and permissions
- Monitoring compliance with security procedures and requirements
- Development of security training
- Evaluating security configurations against established configuration standards and baselines

Module 3: Detect

Lab:

- Sec Onion Setup and Testing
- Snort Rules
- Event Detection
- Data and Network Analysis
- Vulnerability Analysis
- Detect Challenge

Associated Topics:

- Assessing threat level and potential impact of anomalous behavior and security events
- Researching, analyzing, and correlating system activity and security events
- Monitoring and analyzing outputs from security tools, systems, and logs
- Analyzing malicious activity to determine weaknesses and exploitation methods

Module 4: Respond

Lab:

- Incident Correlation
- Network Forensics
- Malware Investigation and Evaluation
- Response Challenge

Associated Topics:

- Notifying appropriate incident response teams according to established protocols
- Identifying and implementing appropriate containment measures, countermeasures, and corrective actions
- Collecting and preserving digital evidence according to relevant regulations and laws
- Conducting post-incident analysis
- Communicating and documenting notifications and outcomes of incident response

Module 5: Recover

Lab:

- Re-Imaging
- Restore Points

Associated Topics:

- Validating whether restored systems meet security requirements
- Updating security plans and procedures following incident response