CompTIA CySA+ Certification Course - TTCTCS00

Gain the tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur.

Duration: 5 Days
Skill Level: Intermediate
Available Format: Instructor-Led Online ; On Public Schedule

Gain the tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This is a comprehensive approach to security aimed at those on the front lines of defense. This course is designed to assist students in preparing for the CompTIA CySA+ - Cybersecurity Analyst+ (CS0-003) certification exam.

CompTIA's CySA+ is a global vendor-neutral certification covering intermediate-level knowledge and skills required by information security analyst job roles. It helps identify a cybersecurity professional's ability to proactively defend an organization using secure monitoring, threat identification, incident response and teamwork.

*Certification exam vouchers are available as an add-on for an additional fee.

What You'll Learn

Overview

Gain the tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This is a comprehensive approach to security aimed at those on the front lines of defense. This course is designed to assist students in preparing for the CompTIA CySA+ - Cybersecurity Analyst+ (CS0-003) certification exam.

CompTIA's CySA+ is a global vendor-neutral certification covering intermediate-level knowledge and skills required by information security analyst job roles. It helps identify a cybersecurity professional's ability to proactively defend an organization using secure monitoring, threat identification, incident response and teamwork.

*Certification exam vouchers are available as an add-on for an additional fee.

Objectives

- Explain the Importance of Security Controls and Security Intelligence
- Utilize Threat Data and Intelligence
- Analyze Security Monitoring Data
- Collect and Query Security Monitoring Data
- Utilize Digital Forensics and Indicator Analysis Techniques
- Apply Incident Response Procedures
- Apply Risk Mitigation and Security Frameworks
- Perform Vulnerability Management
- Apply Security Solutions for Infrastructure Management
- Understand Data Privacy and Protection
- Apply Security Solutions for Software Assurance
- Apply Security Solutions for Cloud and Automation

Audience

- IT Security Analyst
- Security Operations Center (SOC) Analyst
- Vulnerability Analyst
- Cybersecurity Specialist
- Threat Intelligence Analyst
- Security Engineer
- Individuals preparing for the CompTIA CySA+ - Cybersecurity Analyst+ (CS0-003) certification exam

Pre-Requisites

- At least two years (recommended) of experience in computer network security technology or a related field.
- The ability to recognize information security vulnerabilities and threats in the context of risk management.
- Foundation-level operational skills with some of the common operating systems for computing environments.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include, but are not limited to, basic authentication and authorization, resource permissions, and anti-malware mechanisms.
- Foundation-level understanding of some of the common concepts for network environments, such as routing and switching.
- Foundational knowledge of major TCP/IP networking protocols including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments. Safeguards include, but are not limited to, firewalls, intrusion prevention systems, and VPNs.

Agenda

Lessons:

- Understanding Vulnerability Response, Handling, and Management
- Exploring Threat Intelligence and Threat Hunting Concepts
- Explaining Important System and Network Architecture Concepts
- Understanding Process Improvement in Security Operations
- Implementing Vulnerability Scanning Methods
- Performing Vulnerability Analysis
- Communicating Vulnerability Information
- Explaining Incident Response Activities
- Demonstrating Incident Response Communication
- Applying Tools to Identify Malicious Activity
- Analyzing Potentially Malicious Activity
- Understanding Application Vulnerability Assessment
- Exploring Scripting Tools and Analysis Concepts
- Understanding Application Security and Attack Mitigation Best Practices
- Mapping Course Content to CompTIA CySA+ (CS0-003)

Hands-on Labs:

- Exploring the Lab Environment
- Configuring Controls
- Reviewing IoC and Threat Intelligence Sources
- Performing Threat Hunting
- Configuring Centralized Logging
- Performing System Hardening
- Assess Time Synch Errors
- Configuring Automation
- Performing Asset Discovery
- Performing Vulnerability Scanning
- Performing Passive Scanning
- Establishing Context Awareness
- Analyzing Vulnerability Reports
- Detecting Legacy Systems
- Performing Post-Incident Forensic Analysis
- Performing IoC Detection and Analysis
- Performing Playbook Incident Response
- Collecting Forensic Evidence
- Performing Root Cause Analysis
- Using Network Sniffers
- Researching DNS and IP Reputation
- Using File Analysis Techniques
- Analyzing Potentially Malicious Files
- Using Nontraditional Vulnerability Scanning Tools
- Performing Web Vulnerability Scanning
- Exploiting Weak Cryptography
- Performing and Detecting Directory Traversal and Command Injection
- Performing and Detecting Privilege Escalation
- Performing and Detecting XSS
- Performing and Detecting LFI/RFI
- Performing and Detecting SQLi
- Performing and Detecting CSRF
- Detecting and Exploiting Security Misconfiguration

For More Information

Please contact us or call 844-475-4559 toll free for more information about our training services (instructor-led, self-paced or blended), coaching and mentoring services, public course enrollment or questions, partner programs, courseware licensing options and more.