Cybersecurity Analyst
Exam CS0-002

Overview

The CompTIA Cybersecurity Analyst (CySA+) certification verifies that successful candidates have the knowledge and skills required to leverage intelligence and threat detection techniques, analyze and interpret data, identify and address vulnerabilities, suggest preventative measures, and effectively respond to and recover from incidents.

Course Length
5 days

Target Student

IT professionals looking to gain IT security analyst skills, and those following the CompTIA recommended skills pathway to achieve cybersecurity mastery, should consider earning the CompTIA CSA+ vendor-neutral certification.

Prerequisites

Network+, Security+ or equivalent knowledge. Minimum of 4 years of hands-on information security or related experience.

Course Objectives

In this course, It will validate an IT professional´s ability to proactively defend and continuously improve the security of an organization. CySA+ will verify the successful candidate has the knowledge and skills required to:

- Leverage intelligence and threat detection techniques.
- Analyze and interpret data.
- Identify and address vulnerabilities.

- Suggest preventative measures.
- Effectively respond to and recover from incidents.

Course Contents

1.0 Threat and Vulnerability Management.

- Explain the importance of threat data and intelligence.
  - Intelligence sources
  - Confidence levels
  - Indicator management
  - Threat classification
  - Threat actors
  - Intelligence cycle
  - Commodity malware
  - Information sharing and analysis communities

- Given a scenario, utilize threat intelligence to support organizational security.
  - Attack frameworks
  - Threat research
  - Threat modeling methodologies
  - Threat intelligence sharing with supported functions

- Given a scenario, perform vulnerability management activities.
  - Vulnerability Identification
  - Validation
  - Remediation/mitigation
  - Scanning parameters and criteria
  - Inhibitors to remediation

- Given a scenario, analyze the output from common vulnerability assessment tools.
  - Web application scanner
  - Infrastructure vulnerability scanner

- Software assessment tools and techniques
- Enumeration
- Wireless assessment tools
- Cloud Infrastructure assessment

- Explain the threats and vulnerabilities associated with specialized technology.
  - Mobile
  - Internet of Things (IoT)
  - Embedded
  - Real-time operating system (RTOS)
  - System-on-Chip (SoC)
  - Field programmable gate array (FPGA)
  - Physical access control
  - Building automation systems
  - Vehicles and drones
  - Workflow and process automation systems
  - Industrial control system
  - Supervisory and data acquisition (SCADA)

- Explain the threats and vulnerabilities associated with operating in the cloud.
  - Cloud service models
  - Cloud deployment models
  - Function as a Service (FaaS)/ serverless architecture
  - Infrastructure as code (IaC)
  - Insecure application programming Interface (API)
  - Improper key management
  - Unprotected storage
  - Logging and monitoring

- Given a scenario, implement controls to mitigate attack and software vulnerabilities.
  - Attack types
  - Vulnerabilities

2.0 Software and Systems Security

- Given scenario, apply security solutions for infrastructure management.
  - Cloud vs. on-premises
  - Asset management
  - Segmentation
  - Network architecture
  - Change management
  - Virtualization
  - Containerization
  - Identity and access management
  - Cloud access security broker (CASB)
  - Honeypot
  - Monitoring and logging
  - Encryption
  - Certificate management
  - Active defense

- Explain software assurance best practices.
  - Platforms
  - Software development life cycle (SDLC) integration
  - DevSecOps
  - Software assessment methods
  - Secure coding best practices
  - Static analysis tools
  - Dynamic analysis tools
  - Formal methods for verification of critical software
  - Service-oriented architecture

- Explain hardware assurance best practices.
  - Hardware root of trust
  - sFuse
  - Unified Extensible Firmware Interface (UEFI)
  - Trusted foundry

- Secure processing
- Anti-tamper
- Self-encrypting drive
- Trusted firmware updates
- Measured boot and attestation
- Bus encryption

3.0 Security Operations and Monitoring

- Given a scenario, analyze data as part of security monitoring activities.
  - Heuristics
  - Trend analysis
  - Endpoint
  - Network
  - Log review
  - Impact analysis
  - Security Information and event management (SIEM) review
  - Query writing
  - E-mail analysis

- Given a scenario, implement configuration changes to existing controls to improve security.
  - Permissions
  - Whitelisting
  - Blacklisting
  - Firewall
  - Intrusion prevention system (IPS) rules
  - Data loss prevention (DLP)
  - Endpoint detection and response (EDR)
  - Network access control (NAC)
  - Sinkholing
  - Malware signatures
  - Sandboxing

- Port security

- Explain the importance of proactive threat hunting.
  - Establishing a hypothesis
  - Profiling threat actors and activities
  - Threat hunting tactics
  - Reducing the attack surface area
  - Bundling critical assets
  - Attack vectors
  - Integrated intelligence
  - Improving detection capabilities

- Compare and contrast automation concepts and technologies.
  - Workflow orchestration
  - Scripting
  - Application programming Interface (API) Integration
  - Automated malware signature creation
  - Data enrichment
  - Threat feed combination
  - Machine learning
  - Use of automation protocols and standards
  - Continuous Integration
  - Continuous deployment/delivery

4.0 Incident Response

- Explain the importance of the incident response process.
  - Communication plan
  - Response coordination with relevant entities
  - Factors contributing to data criticality

- Given a scenario, apply the appropriate incident response procedure.
  - Preparation

- Detection and analysis
- Containment
- Eradication and recovery
- Post-incident activities

- Given an incident, analyze potential indicators of compromise.
  - Network-related
  - Host-related
  - Application-related

- Given a scenario, utilize basic digital forensics techniques.
  - Network
  - Endpoint
  - Mobile
  - Cloud
  - Virtualization
  - Legal hold
  - Procedures
  - Hashing
  - Carving
  - Data acquisition

5.0 Compliance and Assessment

- Understand the importance of data privacy and protection.
  - Privacy vs. security
  - Non-technical controls
  - Technical controls

- Given a scenario, apply security concepts in support of organizational risk mitigation.
  - Business impact analysis
  - Risk identification process
  - Risk calculation

- Communication of risk factors
- Risk prioritization
- Systems assessment
- Documented compensating controls
- Training and exercises
- Supply chain assessment

- Explain the importance of frameworks, policies, procedures, and controls.
  - Frameworks
  - Policies and procedures
  - Category
  - Control type
  - Audits and assessments

Certification Information

- Exam CS0-002