REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
*"Training You Can Really Use"*

# CompTIA Cybersecurity Analyst (CySA+)

## Duration: 5 Days

## Method: Instructor-Led Training (ILT) | Live Online Training

***Certification:*** *CompTIA Cybersecurity Analyst (CySA+) —*
***Exam:*** *CS0-002*

## Course Description

Attackers have learned to evade traditional signature-based solutions, such as firewalls and anti-virus software. An analytics-based approach within the IT security industry is increasingly important for organizations. This course teaches participants how to apply behavioural analytics to networks to improve the overall state of security. It will do so through identifying and combating malware and advanced persistent threats (APTs), resulting in enhanced threat visibility across a broad attack surface. The certification will validate an IT professional's ability to proactively defend and continuously improve the security of an organization.

## Target Audience

This course is intended for:

- IT professionals with (or seeking) job roles such as
- IT Security Analyst,
- Security Operations Center (SOC) Analyst,
- Vulnerability Analyst,
- Cybersecurity Specialist,
- Threat Intelligence Analyst
- Application Security Analyst
- Compliance Analyst
- Security Engineer.
- Professionals who wish to attain this intermediate-level certificate.

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
*"Training You Can Really Use"*

## Prerequisites

To attend this course, candidates must have:

- Minimum of four (4) years of hands-on information security or related experience.
- Obtained the *Network*+ and *Security*+ certificates or have equivalent knowledge such as:
  - Knowledge of basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers)
  - Understanding of TCP/IP addressing, core protocols, and troubleshooting tools
  - Network attack strategies and defences
  - Knowledge of the technologies and uses of cryptographic standards and products
  - Network- and host-based security technologies and practices

## Exam Details

| | |
|---|---|
| **Exam Code:** | • CS0-002 |
| **Length of Exam:** | • 165 mins |
| **Number of Questions:** | • 85 |
| **Passing Score:** | • 750 out of 900 |
| **Question Format:** | • Multiple Choice and Performance-Based |

## Course Objectives

Upon successful completion of this course, attendees will be able to:

- Leverage intelligence and threat detection techniques.
- Analyse and interpret data.
- Identify and address vulnerabilities.
- Suggest preventative measures.
- Effectively respond to and recover from incidents.

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
*"Training You Can Really Use"*

# Course Topics

## Module 1: Threat and Vulnerability Management

- Explain the Importance of Threat Data and Intelligence
  - Intelligence Sources
  - Indicator Management
  - Threat Classification
  - Threat Actors
  - Intelligence Cycle
  - Commodity Malware
  - Information Sharing and Analysis Communities
- Utilize Threat Intelligence to Support Organizational Security
  - Attack Frameworks
  - Threat Research
  - Threat Modelling Methodologies
  - Threat Intelligence Sharing with Supported Functions
- Perform Vulnerability Management Activities
  - Vulnerability Identification
  - Validation
  - Remediation/Mitigation
  - Scanning Parameters and Criteria
  - Inhibitors to Remediation
- Analyse 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 Tools
- 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
  - Bustling Automation Systems
  - Vehicles and Drones
  - Workflow and Process Automation Systems
  - Industrial Control System
  - Supervisory Control 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
- Implement Controls to Mitigate Attacks and Software Vulnerabilities
  - Attack Types
  - Vulnerabilities

# Course Topics *Continued*

## Module 2: Software and Systems Security

- 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 Defence
- 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
  - eFuse
  - Unified Extensible Firmware Interface (UEFI)
  - Trusted Foundry
  - Secure Processing
  - Anti-Tamper
  - Self-Encrypting Drive
  - Trusted Firmware Updates
  - Measured Boot and Attestation
  - Bus Encryption

# Course Topics *Continued*

## Module 3: Security Operations and Monitoring

- Analyse 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
- 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

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
*"Training You Can Really Use"*

# Course Topics *Continued*

## Module 4: Incident Response

- Explain the Importance of The Incident Response Process
  - Communication Plan
  - Factors Contributing to Data Criticality
  - Response Coordination with Relevant Entities
- Apply the Appropriate Incident Response Procedure
  - Preparation
  - Detection and Analysis
  - Containment
  - Eradication and Recovery
  - Post-Incident Activities
- Given an Incident, Analyse Potential Indicators of Compromise
  - Network-Related
  - Host-Related
  - Application-Related
- Utilize Basic Digital Forensics Techniques
  - Network
  - Endpoint
  - Mobile
  - Cloud
  - Virtualization
  - Legal Hold
  - Procedures
  - Hashing
  - Carving
  - Data Acquisition

## Module 5: Compliance and Assessment Vulnerability Management

- Understand the Importance of Data Privacy and Protection.
  - Privacy Vs. Security
  - Non-Technical Controls
  - Technical Controls
- 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 Assessment

## LABS INCLUDED