# CompTIA Cybersecurity Analyst (CySA+)

**Duration** : 5 Days

## Course Content

This course is intended for those wishing to qualify with CompTIA CySA+ Cybersecurity Analyst Certification. CompTIA's CySA+ Certification is an intermediate-level certificate for IT professionals with previous experience of working in the field of IT security. The CompTIA CySA+ examination is designed for IT security analysts, vulnerability analysts, or threat intelligence analysts. The exam will certify that the successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting applications and systems within an organization.

## Who Should Attend

CompTIA CySA+ certification is aimed at IT professionals with (or seeking) job roles such as IT Security Analyst, Security Operations Center (SOC) Analyst, Vulnerability Analyst, Cybersecurity Specialist, Threat Intelligence Analyst, and Security Engineer.

## Course Outline

### Threat Management

Cybersecurity Analysts

- Cybersecurity Roles and Responsibilities
- Frameworks and Security Controls
- Risk Evaluation
- Penetration Testing Processes

Reconnaissance Techniques

- The Kill Chain
- Open Source Intelligence
- Social Engineering
- Topology Discovery

- Service Discovery
- OS Fingerprinting

## Threat Management

Security Appliances

- Configuring Firewalls
- Intrusion Detection and Prevention
- Configuring IDS
- Malware Threats
- Configuring Anti-virus Software
- Sysinternals
- Enhanced Mitigation Experience Toolkit

Logging and Analysis

- Packet Capture
- Packet Capture Tools
- Monitoring Tools
- Log Review and SIEM
- SIEM Data Outputs
- SIEM Data Analysis
- Point-in-Time Data Analysis

## Vulnerability Management

Managing Vulnerabilities

- Vulnerability Management Requirements
- Asset Inventory
- Data Classification
- Vulnerability Management Processes
- Vulnerability Scanners
- Microsoft Baseline Security Analyzer
- Vulnerability Feeds and SCAP
- Configuring Vulnerability Scans
- Vulnerability Scanning Criteria
- Exploit Frameworks

Remediating Vulnerabilities

- Analyzing Vulnerability Scans
- Remediation and Change Control
- Remediating Host Vulnerabilities
- Remediating Network Vulnerabilities
- Remediating Virtual Infrastructure Vulnerabilities

Secure Software Development

- Software Development Lifecycle
- Software Vulnerabilities
- Software Security Testing
- Interception Proxies
- Web Application Firewalls
- Source Authenticity
- Reverse Engineering

## Cyber Incident Response

Incident Response

- Incident Response Processes
- Threat Classification
- Incident Severity and Prioritization
- Types of Data

Forensics Tools

- Digital Forensics Investigations
- Documentation and Forms
- Digital Forensics Crime Scene
- Digital Forensics Kits
- Image Acquisition
- Password Cracking
- Analysis Utilities

Incident Analysis and Recovery

- Analysis and Recovery Frameworks
- Analyzing Network Symptoms
- Analyzing Host Symptoms
- Analyzing Data Exfiltration
- Analyzing Application Symptoms

- Using Sysinternals
- Containment Techniques
- Eradication Techniques
- Validation Techniques
- Corrective Actions

## Security Architecture

Secure Network Design

- Network Segmentation
- Blackholes, Sinkholes, and Honeypots
- System Hardening
- Group Policies and MAC
- Endpoint Security

Managing Identities and Access

- Network Access Control
- Identity Management
- Identity Security Issues
- Identity Repositories
- Context-based Authentication
- Single Sign On and Federations
- Exploiting Identities
- Exploiting Web Browsers and Applications

Security Frameworks and Policies

- Frameworks and Compliance
- Reviewing Security Architecture
- Procedures and Compensating Controls
- Verifications and Quality Control
- Security Policies and Procedures
- Personnel Policies and Training