Wissenhive

CompTIA CYSA+ Training Certification

CompTIA

CySA+

Table of Contents

About the Program

The CompTIA CYSA+ certification is an intermediate-level course specially designed for vulnerability analysts, IT security analysts, or threat intelligence analysts. It ensures that successful pupils have the proper skills and knowledge required to using and configuring threat detection tools, performing data analysis, and interpreting the result for identifying threats, vulnerabilities, and risks to businesses, organizations, and companies with the end goal of protecting and securing systems and applications within an organization.

- Improve employment opportunity in interviews
- Retention and acquisition for the best skill sets and resources
- Provide job retention prospects
- Can achieve a higher income in any industry.
- Proper and strong understanding about Softwares
- Wide career options such as educational, medical, and engineering fields, etc.

Key Training Features

- Ask Questions Real-Time and Interact with the Trainer Live
- Learner assistance and support - 24x7x365
- Flexible classes
- High-quality content created by industry experts
- Professionally designed Student Training Material
- High-Quality Audio-Video Lectures
- Lifetime Training Access
- Assessments

Training Options

- Self-paced Training
- Live Virtual Classes
- One on One Training

Why CompTIA CYSA+?

- Higher Paying Opportunities
- Gain Knowledge and Credibility
- Stand Out Among the Ordinary
- Knowledge of CYSA+ Best Practices
- Better Career Growth & Job Opportunities
- Better ROI with Flexibility
- Sharpen your IT Skillset

What will you learn?

- Threat and Vulnerability Management
- Software and Systems Security
- Compliance and Assessment
- Security Operations and Monitoring
- Incident Response

CompTIA
CySA+

Career Option with Salary Compensation

Security Engineer

- Minimum - $62,000
- Avg Salary - $93,000
- Maximum - $135,000

Security Analyst

- Minimum - $49,000
- Avg Salary - $69,000
- Maximum - $100,000

Technical Support Specialist

- Minimum - $37,000
- Avg Salary - $52,000
- Maximum - $14,000

Information Security Officer

- Minimum - $59,000
- Avg Salary - $92,000
- Maximum - $136,000

Average Intelligence

- Minimum - $45,000
- Avg Salary - $71,000
- Maximum - $106,000

Target Audience

- Security Analyst
- Security Engineer
- Threat hunter
- Threat intelligence analyst
- Incident response or handler
- Compliance analyst
- Application security analyst

Prerequisites

There are no particular prerequisites for the CompTIA CYSA+ certification course, but Wissenhive recommends at least having one of the following:

- 3-4 years of experience in information security or related field
- Having the quality of experience in cybersecurity and analysis
- CompTIA Security+ Certification Course
- CompTIA Network+ Certification Course

Course Details

Wissenhive's CompTIA CYSA+ certification training clarifies that the successful candidate has knowledge and skills for performing data analysis with the capability to detect and identify threats, risks, and vulnerabilities. They focus on securing organization applications and systems by configuring, managing, and utilizing threat-detection tools.

In this course, apprentices learn about the detailed concept of IT security, which includes

- Leverage intelligence and threat detection procedures
- Analyzing and interpreting data
- Identifying and addressing vulnerabilities
- Focusing on preventative measures
- In-depth knowledge about frameworks, controls, policies, and procedure

Course Curriculum:

1. Detailed introduction about course

2. Threat Management I

- 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

Course Curriculum:

1. Detailed introduction about course

2. Threat Management I

- 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

Course Curriculum:

3. Threat Management II

- 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

Course Curriculum:

4. 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
- 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

CompTIA CySA+

Course Curriculum:

5. 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

Course Curriculum:

6. 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

Contact us

WISSENHIVE E-LEARNING PRIVATE LIMITED

Noida

B-115, B Block, Sector 2,
Noida, Uttar Pradesh-201301

If you have any further questions or would like to chat with us, give us a call

Contact - sales@wissenhive.com

https://www.facebook.com/Wissenhive

https://www.linkedin.com/company/wissenhive/

https://www.instagram.com/wissenhive/

https://twitter.com/HiveWissen

https://in.pinterest.com/wissenhive/

https://www.youtube.com/channel/UCEaIUuf4czgsl9F0PTs0lDg

CompTIA CySA+