CompTIA Cybersecurity Analyst CySA+ Certification Training

Category: Networking & Security | **Vendor:** CompTIA

Duration: 40.00 hours (5 days) **32.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	CompTIA CySA+
Related Exam:	CS0-003

Course Overview

When attacks slip through unnoticed, the results are costly: data breaches, regulatory fines, downtime, and lost customer trust. And the demand for skilled defenders has never been higher, with the U.S. Bureau of Labor Statistics projecting a 33% growth in Information Security Analyst jobs from 2023 to 2033, far outpacing most careers. Without trained analysts, organizations are left vulnerable. CompTIA Cybersecurity Analyst (CySA+) training equips you with the skills employers demand, including threat detection, log analysis, and incident response. This hands-on certification course prepares you to identify vulnerabilities, stop attacks before they spread, and keep critical systems secure. This instructor-led course prepares you to proactively defend systems using behavioral analytics, threat intelligence, and hands-on investigation tools. You'll gain real-world experience managing vulnerabilities, analyzing SIEM output, investigating incidents, and preparing for forensic analysis—all while developing the knowledge needed to pass the CompTIA CySA+ certification exam (CS0-002 or CS0-003). The CySA+ certification is also DoD 8570/8140 approved, making this course an excellent choice for military, civilian, and contractor personnel who require compliance with Department of Defense cybersecurity workforce standards.

About This Course

When attacks slip through unnoticed, the results are costly: data breaches, regulatory fines, downtime, and lost customer trust. And the demand for skilled defenders has never been higher, with the U.S. Bureau of Labor Statistics projecting a 33% growth in Information Security Analyst jobs from 2023 to 2033, far outpacing most careers. Without trained analysts, organizations are left vulnerable. CompTIA Cybersecurity Analyst (CySA+) training equips you with the skills employers demand, including threat detection, log analysis, and incident response. This hands-on certification course prepares you to identify vulnerabilities, stop attacks before they spread, and keep critical systems secure. This instructor-led course prepares you to proactively defend systems using behavioral analytics, threat intelligence, and hands-on investigation tools. You'll gain real-world experience managing vulnerabilities, analyzing SIEM output, investigating incidents, and preparing for forensic analysis—all while developing the knowledge needed to pass the CompTIA CySA+ certification exam (CS0-002 or CS0-003). The CySA+ certification is also DoD 8570/8140 approved, making this course an excellent choice for military, civilian, and contractor personnel who require compliance with Department of Defense cybersecurity workforce standards.

Who Should Attend

This course is ideal for cybersecurity analysts, SOC analysts, incident responders, threat hunters, and IT professionals responsible for protecting information systems. It's also suitable for those seeking to transition into a security operations role and validate skills in threat detection, log analysis, and response.

As a DoD-approved course, it is also valuable for anyone in the Department of Defense (DoD)—military, civilian, or contractor—who needs to develop or validate skills in threat detection, security monitoring, log analysis, and incident response capabilities.

Prerequisites & Entry Requirements

General Prerequisites:

Network+, Security+ or equivalent knowledge. Minimum of 4 years of hands-on experience as an incident response analyst or security operations center (SOC) analyst, or equivalent experience.

Learning Outcomes

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

Assess information security risk in computing and network environments. Analyze reconnaissance threats to computing and network environments. Analyze attacks on computing and network environments. Analyze post-attack techniques on computing and network environments. Implement a vulnerability management program. Collect cybersecurity intelligence. Analyze data collected from security and event logs. Perform active analysis on assets and networks. Respond to cybersecurity incidents. Investigate cybersecurity incidents. Address security issues with the organization's technology architecture.

Detailed Course Outline

Module 1: Assessing Information Security Risk

- Understand the importance of risk management
- Perform risk assessments across systems and networks
- Apply risk mitigation strategies
- Integrate documentation into the risk management process

Module 2: Analyzing Reconnaissance Threats to Computing and Network Environments

- Evaluate the impact of reconnaissance activities
- Assess the risks posed by social engineering attacks

Module 3: Analyzing Attacks on Computing and Network Environments

- Analyze the impact of system hacking attempts
- Evaluate the effects of web-based attacks
- Assess malware threats and their consequences
- Understand hijacking and impersonation attacks
- Analyze Denial-of-Service (DoS) incidents
- Examine mobile security threats
- Explore cloud security risks

Module 4: Analyzing Post-Attack Techniques

- Identify command and control methods
- Assess techniques for maintaining persistence
- Analyze lateral movement and pivoting strategies
- Understand data exfiltration methods
- Examine anti-forensics techniques

Module 5: Managing Vulnerabilities in the Organization

- Implement a comprehensive vulnerability management plan
- Identify and assess common system and application vulnerabilities
- Conduct vulnerability scans effectively
- Perform penetration testing on network assets

Module 6: Collecting Cybersecurity Intelligence

- Set up platforms for collecting and analyzing security intelligence
- Gather data from network-based intelligence sources
- Collect intelligence from host-based sources

Module 7: Analyzing Log Data

- Utilize common tools to analyze log files
- Leverage SIEM (Security Information and Event Management) tools for deeper analysis

Module 8: Performing Active Asset and Network Analysis

- Investigate incidents using Windows-based tools
- Analyze events using Linux-based tools
- Perform basic malware analysis
- Examine indicators of compromise (IOCs)

Module 9: Responding to Cybersecurity Incidents

- Deploy an effective incident response architecture
- Mitigate active threats
- Prepare your CSIRT team for forensic investigation

Module 10: Investigating Cybersecurity Incidents

- Apply a structured forensic investigation plan
- Securely collect and analyze electronic evidence
- Conduct post-investigation follow-up and reporting

Module 11: Addressing Security Architecture Issues

- Resolve identity and access management (IAM) problems
- Integrate security considerations throughout the Software Development Life Cycle (SDLC)

□□ Certification Path

CompTIA CySA+

Exam: CS0-003

Upcoming Schedule

Available training dates for CompTIA Cybersecurity Analyst CySA+ Certification Training:

Start Date	End Date	Location	Delivery	Price
16 Nov 2026	20 Nov 2026	Online	Virtual	€2,495.00
07 Dec 2026	11 Dec 2026	Online	Virtual	€2,495.00
11 Jan 2027	15 Jan 2027	Online	Virtual	€2,495.00

Frequently Asked Questions

Q: What delivery options are available for CompTIA Cybersecurity Analyst CySA+ Certification Training?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The CompTIA Cybersecurity Analyst CySA+ Certification Training course helps prepare you for the CompTIA CySA+ certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the CS0-003 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 5-day CompTIA Cybersecurity Analyst CySA+ Certification Training course provides up to 32.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the CompTIA Cybersecurity Analyst CySA+ Certification Training training?

The training takes place over 5 day(s), with each day lasting approximately 40.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for CompTIA Cybersecurity Analyst CySA+ Certification Training?

Yes, we provide corporate training, dedicated training, and closed classes for CompTIA Cybersecurity Analyst CySA+ Certification Training. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: Why choose Nexus Human for CompTIA Cybersecurity Analyst CySA+ Certification Training?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your CompTIA Cybersecurity Analyst CySA+ Certification Training training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 13/11/2026.