CERTIFICATION GUIDE

CompTIA CySA+

What is it?

CompTIA Cybersecurity Analyst (CySA+) is an IT workforce certification that applies behavioral analytics to networks and devices to prevent, detect and combat cybersecurity threats through continuous security monitoring.

Why is it different?

- CompTIA CySA+ is the only intermediate high-stakes cybersecurity analyst certification with both hands-on, performance-based questions and multiple-choice questions.
- CySA+ focuses on the candidates ability to not only proactively capture, monitor, and respond to network traffic findings, but also emphasizes software and application security, automation, threat hunting, and IT regulatory compliance, which affects the daily work of security analysts.
- CySA+ covers the most up-to-date core security analyst skills and upcoming job skills used by threat intelligence analysts, application security analysts, compliance analysts, incident responders/handlers, and threat hunters, bringing new techniques for combating threats inside and outside of the Security Operations Center (SOC).

About the exam

As 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. CompTIA CySA+ applies behavioral analytics to networks to improve the overall state of security through identifying and combating malware and advanced persistent threats (APTs), resulting in an enhanced threat visibility across a broad attack surface. 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

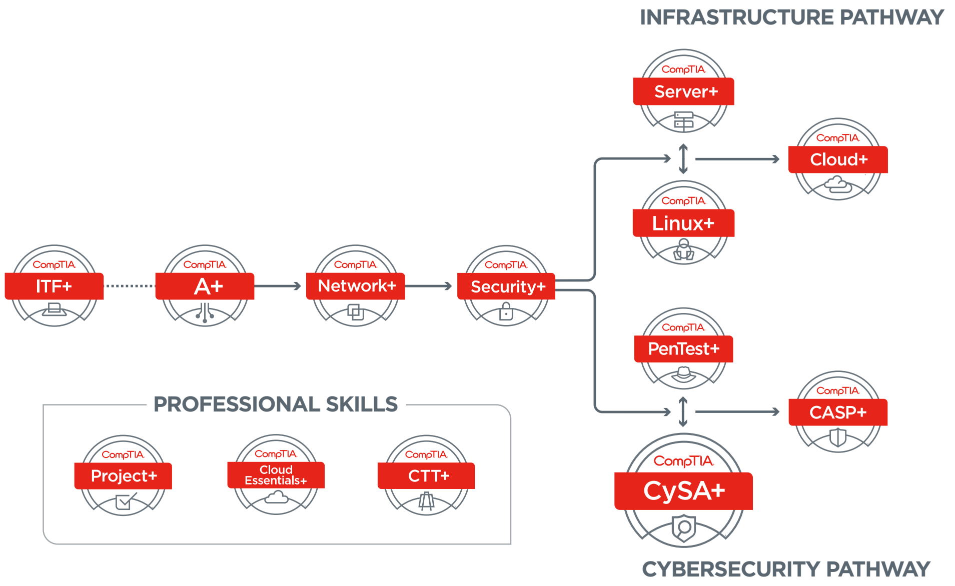
Exam #	CS0-002
Release Date	April 2020
Languages	English and Japanese
CE Required?	Yes
Accreditation	Accredited by ANSI to show compliance with the ISO 17024 Standard. It is also approved by the DoD for Directive 8140/8570.01-M.

How does CySA+ Compare to Alternatives?

Certification	CySA+	EC-Council Certified Security Analyst (ECSA)	GIAC Continuous Monitoring Certification (GMON)	ISACA Certified Information Systems Auditor (CISA)
Performance-based Questions	Yes	No	No	No
Exam Length	1 exam, 165 minutes	1 exam, 4 hours	1 exam, 3 hours	1 exam, 4 hours
Experience Level	Intermediate	Intermediate	Intermediate	Advanced
Exam Focus	Security analytics, intrusion detection and response	Pen testing Methodology	Defensible security and continuous security monitoring	Auditing and vulnerability assessment
Prerequisites	Recommended Network+, Security+ or equivalent knowledge plus a minimum of 4 years of hands-on experience in a technical cybersecurity job role	Attend approved training or 2 years of working experience in a related InfoSec domain	Must have a basic understanding of network protocols and devices and experience with Linux	5 years of professional information systems auditing, control or security work experience

CompTIA Certification Pathway

CompTIA certifications align with the skillsets needed to support and manage cybersecurity. Enter where appropriate for you. Consider your experience and existing certifications or course of study.



Top CySA+ Job Roles

- Security analyst
  - – Tier II SOC analyst
  - – Security monitoring
- Threat intelligence analyst
- Security engineer
- Application security analyst
- Incident response or handler
- Compliance analyst
- Threat hunter

Technical Areas Covered in the Certification

Threat and Vulnerability Management

22%

- Explain the importance of threat data and intelligence
- Utilize threat intelligence to support organizational security
- Perform vulnerability management activities
- Analyze the output from common vulnerability assessment tools
- Explain the threats and vulnerabilities associated with specialized technology and operating in the cloud
- Implement controls to mitigate attacks and software vulnerabilities

Software and Systems Security

18%

- Apply security solutions for infrastructure management
- Explain software & hardware assurance best practices

Security Operations and Monitoring

25%

- Analyze data as part of security monitoring activities
- Implement configuration changes to existing controls to improve security
- Explain the importance of proactive threat hunting
- Compare and contrast automation concepts and technologies

Incident Response

22%

- Explain the importance of the incident response process
- Apply the appropriate incident response procedure
- Analyze potential indicators of compromise
- Utilize basic digital forensics techniques

Compliance and Assessment

13%

- Understand the importance of data privacy and protection
- Apply security concepts in support of organizational risk mitigation
- Explain the importance of frameworks, policies, procedures, and controls

Organizations that have contributed to the development of CySA+

- U.S. Department of Defense (DoD)
- U.S. Department of Veterans Affairs
- U.S. Navy
- Northrop Grumman
- Target
- RICOH USA
- Netflix
- Johns Hopkins University Applied Physics Laboratory
- University of Maryland University College
- Kirkpatrick Price
- Integra
- Dell SecureWorks
- Splunk
- BlacKnight Cyber Security International
- Summit Credit Union
- Paylocity
- Japan Business Systems (JBS)
- Linux Professional Institute

Research and Statistics

Fastest-Growing Job Category

The U.S. Bureau of Labor Statistics predicts that information security analysts will be the fastest-growing job category, with **32 percent overall growth between 2018 and 2028.**

Growing Priority

Cybersecurity is now a critical function that demands unique handling and all signs point to security eventually becoming a concentrated discipline, with a combination of internal and external resources to set strategy, execute tactics and manage metrics. The net result will be a greater specialization of skills, a broader approach to methodology, and a better connection between cybersecurity and business success.[1]

Learn with CompTIA

Official CompTIA Content is the only study material exclusively developed by CompTIA for the CompTIA certification candidate; no other content library covers all exam objectives for all certifications. CompTIA eBooks and CertMaster Products have been developed with our Official CompTIA Content to help you prepare for your CompTIA certification exams with confidence. Learners now have everything they need to learn the material and ensure they are prepared for the exam and their career.

Whether you are just starting to prepare and need comprehensive training with CertMaster Learn, need a final review with CertMaster Practice, or need to renew your certification upon expiration with CertMaster CE, CertMaster's online training tools have you covered.

What does it mean to be a "high stakes" exam?

An extraordinarily high level of rigor is employed in developing CompTIA certifications. Each question created for a CompTIA exam undergoes multiple layers of quality assurance and thorough psychometric statistical validation, ensuring CompTIA exams are highly representative of knowledge, skills and abilities required of real job roles. This is why CompTIA certifications are a requirement for many professionals working in technology. Hiring managers and candidates alike can be confident that passing a CompTIA certification exam means competence on the job. This is also how CompTIA certifications earn the ANSI/ISO 17024 accreditation, the standard for personnel certification programs. Over 1.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

What does it mean to be a "vendor-neutral" exam?

All CompTIA certification exams are vendor-neutral. This means each exam covers multiple technologies, without confining the candidate to any one platform. Vendor-neutrality is important because it ensures IT professionals can perform important job tasks in any technology environment. IT professionals with vendor-neutral certifications can consider multiple solutions in their approach to problem-solving, making them more flexible and adaptable than those with training in just one technology.

What is a Performance Certification?

CompTIA performance certifications validate the skills associated with a particular job or responsibility. They include simulations that require the test taker to demonstrate multi-step knowledge to complete a task. CompTIA has a higher ratio of these types of questions than any other IT certifying body.

[1] CompTIA, Trends in Cybersecurity: Building Effective Security Teams, 2019