

# 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.

## Why is it different?

- CompTIA CySA+ is the only intermediate high-stakes cybersecurity analyst certification exam taken at a Pearson VUE testing center with both hands-on, performance-based questions and multiple-choice, to ensure each candidate possesses the skills, knowledge, and ability to address security analytics, intrusion detection and response. High-stakes exams are proctored at a Pearson VUE testing center in a highly secure environment.
- CySA+ is the most up-to-date security analyst certification that covers advanced persistent threats in a post-2014 cybersecurity environment.

## About the exam

As attackers have learned to evade traditional signature-based solutions, such as firewalls, an analytics-based approach within the IT security industry is increasingly important for most organizations. The behavioral analytics skills covered by CySA+ identify and combat malware, and advanced persistent threats (APTs), resulting in enhanced threat visibility across a broad attack surface. CompTIA CySA+ is for IT professionals looking to gain the following security analyst skills:

- Perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization.
- Configure and use threat-detection tools.
- Secure and protect applications and systems within an organization.



### Exam #

CS0-001

### Release Date

February 2017

### Languages

English, Japanese and Simple Chinese




### CE Required?

Yes

### Accreditation

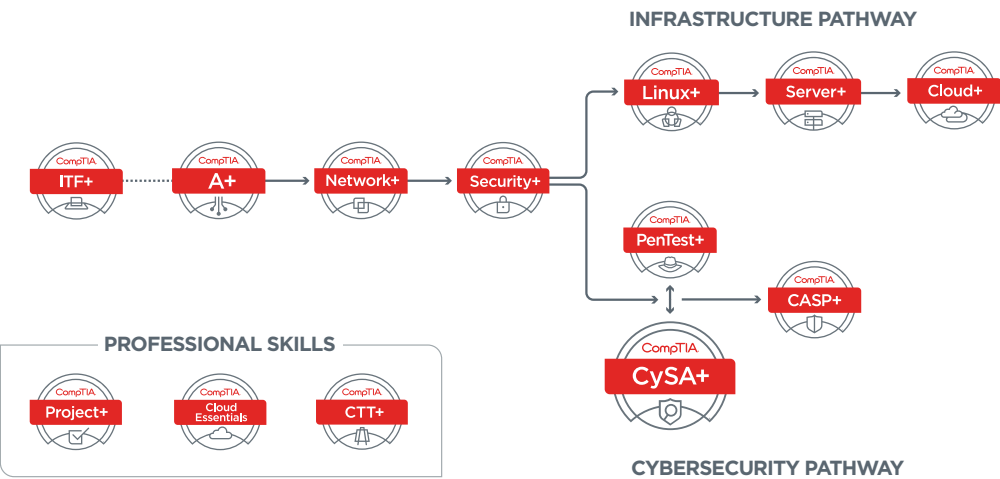
Accredited by ANSI to show compliance with the ISO 17024 Standard. It is also approved by the DoD for Directive 8140/8570.01-M.

How does CySA+ Compare to Alternatives?

			
Certification	CySA+	EC-Council Certified Ethical Hacker (CEH)	GIAC Certified Intrusion Analyst (GCIA)
Performance-based Questions	Yes	No A second exam, CEH (Practical) offers performance-based questions	No
Exam Length	1 exam, 90 questions, 165 min	1 exam, 4 hrs	1 exam, 5 hrs
Experience Level	Intermediate	Intermediate	Intermediate
Exam Focus	Security analytics, intrusion detection and response	Penetration testing	Intrusion detection
Pre-requisites	Network+, Security+ or equivalent knowledge plus a minimum of 3 to 4 years of hands-on information security or related experience recommended	CEH Training, 2 years information security experience, Endorsement	None

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

- IT Security Analyst
- Security Operations Center (SOC) Analyst
- Vulnerability Analyst
- Cybersecurity Specialist
- Threat Intelligence Analyst
- Security Engineer
- Cybersecurity Analyst
- Security architect

## Technical Areas Covered in the Certification

<p>Threat Management <b>27%</b></p> <ul style="list-style-type: none"><li>• Apply environmental reconnaissance techniques using appropriate tools and processes</li><li>• Analyze the results of a network reconnaissance</li><li>• Implement or recommend the appropriate response and countermeasure to a network-based threat</li><li>• Explain the purpose of practices used to secure a corporate environment</li></ul>	<p>Vulnerability Management <b>26%</b></p> <ul style="list-style-type: none"><li>• Implement an information security vulnerability management process</li><li>• Analyze the output resulting from a vulnerability scan</li><li>• Compare and contrast common vulnerabilities found in an organization</li></ul>
<p>Cyber-Incident Response <b>23%</b></p> <ul style="list-style-type: none"><li>• Distinguish threat data or behavior to determine the impact of an incident</li><li>• Prepare a toolkit and use appropriate forensics tools during an investigation</li><li>• Explain the importance of communication during the incident response process</li><li>• Analyze common symptoms to select the best course of action to support incident response</li><li>• Summarize the incident recovery and post-incident response process</li></ul>	<p>Security Architecture and Tool Sets <b>24%</b></p> <ul style="list-style-type: none"><li>• Explain the relationship between frameworks, common policies, controls, and procedures</li><li>• Use data to recommend remediation of security issues related to identity and access management</li><li>• Review security architecture and make recommendations to implement compensating controls</li><li>• Use application security best practices while participating in the Software Development Life Cycle (SDLC)</li><li>• Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies</li></ul>

“We’re coming up on catastrophic conditions – if we’re not already there – in the labor market in terms of the gap between companies unable to find or breed (internally) or have sufficient talent available to them to do what they want to do.”

### David Foote

Co-founder of IT employment research firm Foote Partners

## 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
- Japan Business Systems (JBS)
- Federal Reserve Bank of Chicago
- Washington State Patrol
- KirkpatrickPrice
- Integra
- Dell SecureWorks
- Linux Professional Institute
- Boulder Community Health
- Western Governors University
- BlacKnight Cyber Security International
- Summit Credit Union

## 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 **37 percent overall growth between 2012 and 2022**.<sup>1</sup>

**Growing Priority** Of managers responsible for security in the 12 countries covered by CompTIA's International Trends in Cybersecurity survey, **8 out of 10** expect security to become an even higher priority over the next two years (79 percent net of moderately higher and significantly higher).<sup>2</sup>

## 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 Information Security 2015

2. International Trends in Cybersecurity, CompTIA, 2016

© 2019 CompTIA Properties, LLC, used under license by CompTIA Certifications, LLC. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA Certifications, LLC. CompTIA is a registered trademark of CompTIA Properties, LLC in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA Properties, LLC or of their respective owners. Reproduction or dissemination prohibited without written consent of CompTIA Properties, LLC. Printed in the U.S. 06197-Jan2019