CERTIFICATION GUIDE

CompTIA CySA+

What is it?

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

Why is it different?

- CySA+ is the only intermediate high-stakes cybersecurity analyst certification with performance-based questions covering security analytics, intrusion detection and response. High-stakes exams are proctored at a Pearson VUE testing centre 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 organisations. The behavioural 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 organisation.
- Configure and use threat-detection tools.
- Secure and protect applications and systems within an organisation.

Exam #
CS0-001

Release Date
February 2017

Languages
English, Japanese and Simplified Chinese

CE Required?
Yes

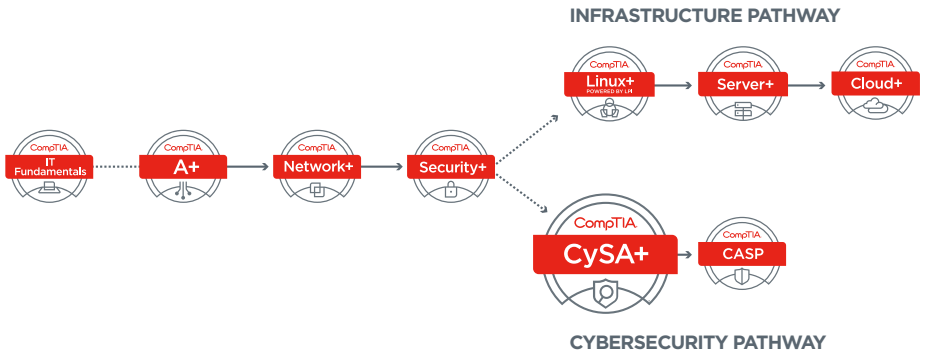
Accreditation
Accredited by ANSI to show compliance with the ISO 17024 Standard. It is also approved by the DoD for Directive 8140/8570.01-M.

How does CySA+ Compare to Alternatives?

	CompTIA CySA+	CEH Certified Ethical Hacker	GCIA
Certification	**CySA+**	**EC-Council Certified Ethical Hacker (CEH)**	**GIAC Certified Intrusion Analyst (GCIA)**
Performance-based Questions	Yes	No	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	No specific training requirement

CompTIA Certification Pathway

CompTIA certifications align with the skillsets needed to support and manage IT infrastructure. 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

Technical Areas Covered in the Certification

Threat Management
27%

- Apply environmental reconnaissance techniques using appropriate tools and processes.
- Analyse the results of a network reconnaissance.
- Implement or recommend the appropriate response and countermeasure to a network-based threat.
- Explain the purpose of practices used to secure a corporate environment.

Vulnerability Management
26%

- Implement an information security vulnerability management process.
- Analyse the output resulting from a vulnerability scan.
- Compare and contrast common vulnerabilities found in an organisation.

Cyber-Incident Response
23%

- Distinguish threat data or behaviour to determine the impact of an incident.
- Prepare a toolkit and use appropriate forensics tools during an investigation.
- Explain the importance of communication during the incident response process.
- Analyse common symptoms to select the best course of action to support incident response.
- Summarise the incident recovery and post-incident response process.

Security Architecture and Tool Sets
24%

- Explain the relationship between frameworks, common policies, controls, and procedures.
- Use data to recommend remediation of security issues related to identity and access management.
- Review security architecture and make recommendations to implement compensating controls.
- Use application security best practices while participating in the Software Development Life Cycle (SDLC).
- Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies.

"We're coming up on catastrophic conditions – if we're not already there – in the labour 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

Organisations 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

CompTIA's International Security Snapshot reports that **73 percent of companies surveyed had at least one security breach/incident in the past 12 months.**

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).[2]

Top 10 Best Technology Job

A career in information security analysis **ranked seventh** on U.S. News and World Report's list of the 100 best technology jobs for 2017.

*** 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. International Trends in Cybersecurity, CompTIA, 2016

CompTIA