CompTIA

CompTIA CySA+ Certified Professionals Defend With Confidence

The skills that today's security analysts need to protect organizations are different than the skills they had just a few years ago. CompTIA Cybersecurity Analyst (CySA+) certification has evolved to help organizations address, monitor and respond to threats and manage risk. Specifically, candidates will gain skills in security operations, vulnerability management, incident response and management and reporting and communication. Professionals certified with CompTIA CySA+ are able to confidently lead incident detection, prevention and response in job roles like security analyst, security operations center (SOC) analyst, incident response analyst, vulnerability management analyst, security engineer and threat hunter.

CompTIA CySA+ (CS0-003) has been updated to reflect the latest in security analyst techniques, such as automated incident response, threat intelligence, cloud-based tools and communication processes. Upon passing the exam, successful candidates will be able to:

- Detect and analyze indicators of malicious activity
- Understand threat hunting and threat intelligence concepts
- Use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities
- Perform incident response processes
- Understand reporting and communication concepts related to vulnerability management and incident response activities

CompTIA CySA+

CompTIA CySA+ is accredited by ANSI as meeting the ISO 17024 standard. It is compliant with government regulations under the Federal Information Security Management Act (FISMA).

Exam Objectives Comparison

The following table aligns exam objectives from CS0-003 and CS0-002 for comparison. Skills are aligned by best match.

CS0-003	Equivalent CS0-002	MAPPING
1.1 Explain the importance of system and network architecture concepts in security operations.	2.1 Given a scenario, apply security solutions for infrastructure management.	Gap
1.1 Explain the importance of system and network architecture concepts in security operations.	3.2 Given a scenario, implement configuration changes to existing controls to improve security.	Gap
1.2 Given a scenario, analyze indicators of potentially malicious activity.	4.3 Given an incident, analyze potential indicators of compromise.	Maps
1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity.	1.4 Given a scenario, analyze the output from common vulnerability assessment tools.	Gap
1.4 Compare and contrast threat-intelligence and threat-hunting concepts.	1.1 Explain the importance of threat data and intelligence.	Gap
1.4 Compare and contrast threat-intelligence and threat-hunting concepts.	1.2 Given a scenario, utilize threat intelligence to support organizational security.	Maps
1.4 Compare and contrast threat-intelligence and threat-hunting concepts.	3.3 Explain the importance of proactive threat hunting.	Maps
1.5 Explain the importance of efficiency and process improvement in security operations.	3.4 Compare and contrast automation concepts and technologies.	Maps
2.1 Given a scenario, implement vulnerability scanning methods and concepts.	1.3 Given a scenario, perform vulnerability management activities	Maps
2.2 Given a scenario, analyze output from vulnerability assessment tools.	1.4 Given a scenario, analyze the output from common vulnerability assessment tools.	Maps
2.3 Given a scenario, analyze data to prioritize vulnerabilities.	n/a	New Content
2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.	1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities.	Maps
2.5 Explain concepts related to vulnerability response, handling, and management.	n/a	New Content
3.1 Explain concepts related to attack methodology frameworks.	1.2 Given a scenario, utilize threat intelligence to support organizational security.	Gap
3.2 Given a scenario, perform incident response activities.	4.2 Given a scenario, apply the appropriate incident response procedure.	Maps
3.3 Explain the preparation and post-incident activity phases of the incident management life cycle.	4.2 Given a scenario, apply the appropriate incident response procedure.	Gap
4.1 Explain the importance of vulnerability management reporting and communication.	n/a	New Content
4.2 Explain the importance of incident response reporting and communication.	4.1 Explain the importance of the incident response process.	Maps