CompTIA

PhoenixTS

CS0-002 vs CS0-001 Exam Objective Comparison

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. CySA+ will validate an IT professional's ability to proactively defend and continuously improve the security of an organization.

In response to a rapidly evolving cybersecurity environment, the updated CompTIA CySA+ (CS0-002) covers the most up-to-date core cybersecurity analyst skills while emphasizing software and application security, automation, threat hunting, and IT regulatory compliance.

CompTIA CySA+

Exam Objectives

The following table aligns exam objectives from CS0-001 to CS0-002 for comparison. Skills are aligned by best match. Exam objectives are listed multiple times to indicate broader coverage.

CS0-002	CS0-001
1.1 Explain the importance of threat data and intelligence.	3.1 Given a scenario, distinguish threat data or behavior to determine the impact of an incident.
1.2 Given a scenario, utilize threat intelligence to support organizational security.	n/a
1.3 Given a scenario, perform vulnerability management activities	1.1 Given a scenario, distinguish threat data or behavior to determine the impact of an incident.
1.4 Given a scenario, analyze the output from common vulnerability assessment tools.	1.2 Given a scenario, analyze the results of a network reconnaissance.
1.5 Explain the threats and vulnerabilities associated with specialized technology.	2.3 Compare and contrast common vulnerabilities found in the following targets within an organization.
1.6 Explain the threats and vulnerabilities associated with operating in the cloud.	n/a
1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities.	2.3 Compare and contrast common vulnerabilities found in the following targets within an organization.
1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities.	4.2 Given a scenario, use data to recommend remediation of security issues related to identity and access management.
2.1 Given a scenario, apply security solutions for infrastructure management.	1.3 Given a network-based threat, implement or recommend the appropriate response and countermeasure.
2.1 Given a scenario, apply security solutions for infrastructure management.	1.4 Explain the purpose of practices used to secure a corporate environment.
2.1 Given a scenario, apply security solutions for infrastructure management.	4.2 Given a scenario, use data to recommend remediation of security issues related to identity and access management.
2.2 Explain software assurance best practices.	4.4 Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC).
2.3 Explain hardware assurance best practices.	n/a
3.1 Given a scenario, analyze data as part of security monitoring activities.	1.2 Given a scenario, analyze the results of a network reconnaissance.
3.2 Given a scenario, implement configuration changes to existing controls to improve security.	1.3: Given a network-based threat, implement or recommend the appropriate response and countermeasure.
3.2 Given a scenario, implement configuration changes to existing controls to improve security.	4.3 Given a scenario, review security architecture and make recommendations to implement compensating controls.
3.3 Explain the importance of proactive threat hunting.	n/a
3.4 Compare and contrast automation concepts and technologies.	n/a
4.1 Explain the importance of the incident response process.	3.1 Given a scenario, distinguish threat data or behavior to determine the impact of an incident.
4.1 Explain the importance of the incident response process.	3.3 Explain the importance of communication during the incident response process.
4.2 Given a scenario, apply the appropriate incident response procedure.	3.5 Summarize the incident recovery and post-incident response process.
4.3 Given an incident, analyze potential indicators of compromise.	3.4 Given a scenario, analyze common symptoms to select the best course of action to support incident response.
4.4 Given a scenario, utilize basic digital forensics techniques.	n/a
5.1 Understand the importance of data privacy and protection.	n/a
5.2 Given a scenario, apply security concepts in support of organizational risk mitigation.	1.4 Explain the purpose of practices used to secure a corporate environment.
5.3 Explain the importance of frameworks, policies, procedures, and controls.	4.1 Explain the relationship between frameworks, common policies, controls, and procedures.