COMPTIA - CSA+

Duration: 5 days
Audience: Professionnel TI

Who is this training for?

This course is designed for IT security analysts, vulnerability analysts, or threat intelligence analysts. The exam will certify that the successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization, with the ultimate goal of securing and protecting applications and systems within an organization.

Training objectives

- Configure and use threat detection tools
- Analyze data and interpret results to identify vulnerabilities, threats, and risks
- Manage cybersecurity incidents and apply appropriate response processes
- Assess security architectures and recommend appropriate compensating controls

Summary

CompTIA Cybersecurity Analyst (CSA+) is an international, vendor-neutral professional IT certification that applies behavioral analytics to improve the overall state of IT security. It validates the knowledge and skills required to configure and use threat detection tools, perform data analysis, and interpret results to identify vulnerabilities, threats, and risks to an organization, with the ultimate goal of securing and protecting applications and systems within an organization. As attackers have learned to bypass traditional signature-based solutions such as firewalls, an analytics-based approach in the IT security industry has become extremely important and essential for most organizations. The behavioral analytics skills covered by the CompTIA CSA+ certification make it possible to identify and combat malware and advanced persistent threats (APTs), providing better visibility into threats across a broad attack surface by focusing on network behavior, including an organization’s internal network.

Course outline

Module 1 - Threat Management

- Given a scenario, apply environmental reconnaissance techniques using the appropriate tools and processes
- Given a scenario, analyze the results of network reconnaissance
- Given a network-based threat, implement or recommend the appropriate response and counter-measure
- Explain the purpose of practices used to secure an enterprise environment

Module 2 - Vulnerability Management

- Given a scenario, implement an information security vulnerability management process
- Given a scenario, analyze the results of a vulnerability scan
- Compare and contrast common vulnerabilities found in the following targets within an organization

Module 3 - Cybersecurity Incident Response

- Given a scenario, distinguish threat data or behaviors to determine the impact of an incident
- Given a scenario, prepare a toolkit and use the appropriate digital investigation tools during an investigation
- Explain the importance of communication during the incident response process
- Given a scenario, analyze common symptoms to select the best course of action to support incident response
- Summarize the recovery process after an incident and post-incident response

Module 4 - Security Architecture and Tool Sets

- Explain the relationship between frameworks, common policies, controls, and procedures
- Given a scenario, use data to recommend remediation measures related to identity and access management
- Given a scenario, review the security architecture and make recommendations for implementing compensating controls
-

Given a scenario, apply application security best practices as part of the software development lifecycle (SDLC)

- Compare and contrast the overall purpose of and reasons for using various cybersecurity tools and technologies

Approach and methodology

A practical and structured approach combining targeted theory and guided workshops.

Recommendations

- Hold the CompTIA Network+ certification or equivalent content
- Hold the CompTIA Security+ certification or equivalent content
- 3 to 4 years of hands-on experience in IT security or a related field

Certifications

CompTIA Cybersecurity Analyst (CSA+) — CS0-001 Exam

Legal notices

This course is offered in French; the course materials are in English.