CompTIA CSA+ (Cybersecurity Analyst)

Course Length: 5 days (virtual)

Click here to view the current class schedule!

Overview:

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 CSA+ identify and combat malware, and advanced persistent threats (APTs), resulting in enhanced threat visibility across a broad attack surface. CompTIA CSA+ is for IT professionals looking to gain the following security analyst skills:

- Configure and use threat detection tools.
- Perform data analysis.
- Interpret the results to identify vulnerabilities, threats and risks to an organization.

CSA+ certified skills are in-demand

Properly trained IT security staff who can analyze, monitor and protect cybersecurity resources are in high demand. The U.S. Bureau of Labor Statistics (BLS) predicts that information security analysts will be the fastest growing overall job category, with 37 percent overall growth between 2012 and 2022.

CSA+ is globally recognized

CompTIA CSA+ is ISO/ANSI 17024 accredited and is awaiting approval by the U.S. Department of Defense (DoD) for directive 8140/8570.01-M requirements.

CSA+ provides substantial earnings potential

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. According to the Bureau of Labor Statistics, the median pay for an information security analyst is $90,120 per year.

Target Student

The CompTIA CSA+ examination 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 the results to identify vulnerabilities, threats and risks to an organization with the end goal of securing and protecting applications and systems within an organization.

Prerequisite

The CompTIA CSA+ exam is an internationally targeted validation of intermediate-level security skills and knowledge. While there is no required prerequisite, the CompTIA CSA+ certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, "hands-on" focus on IT security analytics.

It is recommended for CompTIA CSA+ certification candidates to have the following:

- 3-4 years of hands-on information security or related experience
- Network+, Security+ or equivalent knowledge

Course Content

Threat Management

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

Vulnerability Management

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

Cyber Incident Response

- Given a scenario, distinguish threat data or behavior to determine the impact of an incident.
- Given a scenario, prepare a toolkit and use appropriate forensics 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 incident recovery and post-incident response process.

Security Architecture and Tool Sets

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