CompTIA Cybersecurity Analyst (CySa+) Certification Course

TRAINING

Empower Your Cyber Defense: Elevate Your Career with CompTIA CySA+ Certification

Online

Monday - Friday, September 23 - 27, 2024 | 9AM - 5PM EST

PUBLIC SECTOR NETWORK

Certified B Corporation

Overview

In an era dominated by sophisticated cyber threats, the demand for advanced cybersecurity practitioners has soared to unprecedented heights. The CompTIA Cybersecurity Analyst (CySA+) certification emerges as a critical milestone for IT professionals dedicated to the art and science of proactive cyber defense. This globally recognized credential not only validates your expertise in cybersecurity analytics but also your ability to apply behavioral analytics to networks and devices to prevent, detect, and combat cybersecurity threats.

The CySA+ certification is meticulously designed to bridge the gap between foundational security knowledge and hands-on operational skills. It equips candidates with the ability to analyze and interpret data, identify vulnerabilities, suggest preventative measures, and effectively respond to and recover from incidents. The course covers essential domains such as threat management, vulnerability management, cyber incident response, and security architecture and toolsets, providing a comprehensive understanding of the cybersecurity landscape.

Course Inclusions:

By obtaining the CySA+ certification, you position yourself at the forefront of cybersecurity defense, capable of leveraging cutting-edge analytical tools and techniques to safeguard organizations from potential threats. Whether you're an IT professional seeking to specialize in cybersecurity analytics, or a security practitioner aiming to validate your skills, CySA+ offers a robust pathway to enhancing your career and contributing to a safer digital environment.

Elevate your career and join the ranks of proactive cybersecurity defenders with the CompTIA CySA+ certification. Your journey towards becoming a cybersecurity analyst starts here—equip yourself with the skills to analyze, secure, and protect the digital world.

Learning Objectives

Security Operations

- Improve processes in security operations and differentiate between threat intelligence and threat hunting concepts.
- Identify and analyze malicious activity using the appropriate tools and techniques.

Vulnerability Management

- Implement and analyze vulnerability assessments, prioritize vulnerabilities and make recommendations on mitigating attacks and vulnerability response.

Incident Response and Management

- Apply updated concepts of attack methodology frameworks, perform incident response activities and understand the incident management lifecycle.

Reporting and Communication

- Apply communication best practices in vulnerability management and incident response as it relates to stakeholders, action plans, escalation, and metrics.

Who Attends

- Cybersecurity Analyst
- Security Operations Center (SOC) Analyst
- Vulnerability Analyst
- Threat Intelligence Analyst
- Security Engineer
- Cybersecurity Specialist
- Incident Response or Handler
- Compliance Analyst
- Information Security Analyst
- Network Security Engineer
- IT Auditor
- Forensic Analyst
- Security Consultant

Explore the Key Sessions

This program will be delivered across 5 days from September 23 to September 27, 2024, 9am to 5pm EST with breaks for morning tea, lunch and afternoon tea.

CompTIA Cybersecurity Analyst Modules Breakdown:

Threat and Vulnerability Management

- Identifying and analyzing vulnerabilities to understand the potential impacts on information systems.
- Conducting environmental reconnaissance and intelligence gathering to identify potential threats.
- Utilizing threat data and intelligence to support organizational security and to inform risk management decisions.
- Implementing vulnerability management processes to identify, assess, prioritize, and respond to vulnerabilities.
- Understanding the principles of threat classification and the methodologies used for threat modeling.

Software and Systems Security

- Applying security solutions for infrastructure management and the securing of software applications.
- Understanding the importance of secure coding practices and the implementation of software security improvements.
- Assessing and mitigating the security impact of acquired software and systems.
- Implementing secure configuration and patch management processes to protect systems and software.
- Understanding common software vulnerabilities and attacks and how to prevent them.

Pricing for Public Courses

Early Bird 1	Early Bird 2	Standard
$2,590 CAD	$2,790 CAD	$2,990 CAD

Security Operations and Monitoring

- Analyzing security and event logs to identify and track security incidents.
- Implementing configuration changes to improve security and compliance with organizational policies.
- Utilizing security monitoring tools and techniques to detect and mitigate potential threats.
- Conducting continuous security monitoring activities to ensure the integrity and availability of IT systems.
- Understanding the principles of network intrusion detection and the use of SIEM (Security Information and Event Management) technologies.

Incident Response

- Understanding the incident response process, from detection to recovery and post-incident analysis.
- Developing and implementing incident response plans and policies to manage security incidents effectively.
- Conducting forensic analysis to identify the source of security breaches and to gather evidence.
- Coordinating response efforts to minimize impact and restore operations quickly.
- Communicating incident status and risk assessments to stakeholders in a clear and timely manner.

Compliance and Assessment

- Understanding legal and regulatory requirements related to information security and cybersecurity.
- Conducting security assessments to identify compliance gaps and to assess the effectiveness of security controls.
- Implementing policies and procedures to ensure compliance with data protection laws and industry standards.
- Understanding the role of ethics in cybersecurity operations and the handling of sensitive data.
- Preparing and maintaining documentation related to compliance audits and security assessments.