Current Technologies
Computer Learning Centers

CompTIA

6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

CompTIA Advanced Security Practioner (CASP+)

This course provides the knowledge needed to implement security solutions within an enterprise policy framework, using a vendor-neutral format. This includes risk and vulnerability management programs, organizational policies and training, applied cryptography, system security, network security, identity management, and incident response.

How you'll benefit

This class will help you:

- Learn knowledge of information security to apply more advanced principles that will keep your organization safe from the many ways it can be threatened.

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10%
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs Run up to Date Code for all our courses

Objectives

Upon completing this course, the student will be able to meet these objectives:

- Support IT governance in the enterprise with an emphasis on managing risk
- Leverage collaboration tools and technology to support enterprise security
- Use research and analysis to secure the enterprise
- Integrate advanced authentication and authorization techniques
- Implement cryptographic techniques
- Implement security controls for hosts
- Implement security controls for mobile devices
- Implement network security
- Implement security in the systems and software development lifecycle
- Integrate hosts, storage, networks, applications, virtual environments, and cloud technologies in a secure enterprise architecture
- Conduct security assessments
- Respond to and recover from security incidents

Course Duration

5 day

Course Price

$2,895.00

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Certification Exam

CAS-003

CompTIA Advanced Security Practioner (CASP+)

Who Should Attend

The job roles best suited to the material in this course are:

- This course is designed for IT professionals in the cybersecurity industry whose primary job responsibility is to secure complex enterprise environments. The target student should have real-world experience with the technical administration of these enterprise environments.

Perquisites

To fully benefit from this course, you should have the following knowledge:

- Students seeking CASP certification should have at least 10 years of experience in IT management, with at least 5 years of hands-on technical security experience.
- Knowledge of identity and access management (IAM) concepts and common implementations, such as authentication factors and directory services.
- Knowledge of cryptographic concepts and common implementations, such as Secure Sockets Layer/Transport Layer Security (SSL/TLS) and public key infrastructure (PKI).
- Knowledge of computer networking concepts and implementations, such as the TCP/IP model and configuration of routers and switches.
- Knowledge of common security technologies used to safeguard the enterprise, such as anti-malware solutions, firewalls, and VPNs.

Outline

Module 0: Introduction

- Course setup

Module 1: Risk management

- Security concepts
- Threats and vulnerabilities
- Risk assessment
- Risk management
- Summary: Cybersecurity fundamentals

Module 2: Vulnerability management

- Security research

CompTIA Advanced Security Practioner (CASP+)

- Vulnerability assessment
- Vulnerability management programs
- Summary: Vulnerability management

Module 3: Organizational security

- Security frameworks
- Security policies
- Controls and procedures
- Training and coordination
- Summary: Organizational Security

Module 4: Applied cryptography

- Cryptographic principles
- Public key infrastructure
- Cryptographic protocols
- Summary: Applied cryptography

Module 5: Secure systems integration

- Architecture integration
- Securing data
- Resilience and business continuity
- Fault tolerance and recovery
- Summary: Secure systems integration

Module 6: Integrated host security

- Securing hosts
- Mobile device security
- Virtual and cloud systems
- Summary: Securing hosts and data

Module 7: Secure development

- Software vulnerabilities

- Software development
- Summary: Secure development

Module 8: Network security architecture

- Packet flow
- Network security systems
- Network access technologies
- Summary: Network security architecture

Module 9: Secure network configuration

- Hardening networks
- Securing communications
- Summary: Secure network configuration

Module 10: Scanning and monitoring

- Reconnaissance techniques
- Active reconnaissance
- Network logging
- Data analysis
- Summary: Scanning and monitoring

Module 11: Identity management

- Identity systems
- Authentication technologies
- Summary: Identity management

Module 12: Incident response

- Incident response planning
- Incident response procedures
- Forensic toolkits
- Summary: Incident response
-