THE LEARNING CENTER
A TECHNICAL TRAINING INSTITUTION

CompTIA Advanced Security Practitioner (CASP+) meets the growing demand for advanced IT security in the enterprise. Recommended for IT professionals with at least 5 years of experience, CASP+ certifies critical thinking and judgment across a broad spectrum of security disciplines and requires candidates to implement clear solutions in complex environments. The current landscape of cybersecurity requires specialized skills to troubleshoot via customized hacks and build solid solutions. Each hack is unique and must be combated with master-level security skills and experience.

CompTIA CASP+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

The new CompTIA CASP+ CAS-004 exam is available as of October 6, 2021

Our unique model follows a streamlined approach to workforce development and skills attainment

Assess: Assess each student to determine existing skill sets

Educate: Deliver goal-specific training utilizing all delivery modalities

Mentor: Expose students to instructors and mentors with front-line IT and cybersecurity experience

Certify: Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate: Validate student abilities through performance analytics and real-world exercises hosted on a cyber range

Exam Objectives: CAS-004

Security Architecture	29%
Security Operations	30%
Security Engineering and Cryptography	26%
Governance, Risk, and Compliance	15%

Course Outline:

Chapter 1: Design a Secure Network Architecture
Chapter 2: Integrating Secure Applications into the Enterprise
Chapter 3: Enterprise Data Security including Secure Cloud and Virtualization Solutions
Chapter 4: Deploying Enterprise Authentication and Authorization Controls
Chapter 5: Threat and Vulnerability Management
Chapter 6: Vulnerability Assessment and Penetration Methods and Tools
Chapter 7: Risk Mitigation Controls
Chapter 8: Implementing Incident Response and Forensics Procedures
Chapter 9: Enterprise Mobility and Endpoint Security Controls
Chapter 10: Security Considerations Impacting Specific Sectors and Operational Technologies
Chapter 11: Implementing Cryptographic Protocols and Algorithms
Chapter 12: Implementing Appropriate PKI Solutions, Cryptographic Protocols, and Algorithms for Business Needs
Chapter 13: Applying Appropriate Risk Management Strategies
Chapter 14: Compliance Frameworks, Legal Considerations, and their Organizational Impact
Chapter 15: Business Continuity and Disaster Recovery Concepts

Included

40 hours of instructor-led training sessions
CompTIA authorized textbook and class materials
Practice questions and exam study tips