



CASP Boot Camp

Cyber Security's CompTIA CASP Boot Camp is a comprehensive 5 day course that helps students certify the skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. Students will apply critical thinking and judgment across a spectrum of security disciplines to propose and implement solutions that map to enterprise drivers.

The CompTIA Advanced Security Practitioner (CASP) certification is a vendor-neutral credential. The CASP exam is an internationally targeted validation of advanced-level security skills and knowledge. While there is no required prerequisite, the CASP certification is intended to follow Security+ or equivalent experience and has a technical, "hands-on" focus at the enterprise level.



The goal of this CompTIA Authorized CASP Boot Camp Training course is to provide IT Professionals with the most comprehensive accelerated learning environment for the CompTIA Advanced Security Practitioner (CASP) exam.

SYLABUS:

Managing Risk

- o Identify the Importance of Risk Management
- o Assess Risk
- o Mitigate Risk

Integrate Documentation into Risk Management

- o Integrating Computing, Communications, and Business Disciplines
- o Facilitate Collaboration Across Business Units
- o Secure Communications and Collaboration Solutions
- o Implement Security Activities Throughout the Technology Life Cycle

Using Research and Analysis to Secure the Enterprise

- o Determine Industry Trends and Effects of the Enterprise
- o Analyze Scenarios to Secure the Enterprise

Integrating Advanced Authentication and Authorization

- o Implement Authentication and Authorization Technologies
- o Implement Advanced Identity Management

Implementing Cryptographic Techniques

- o Describe Cryptographic Concepts
- o Choose Cryptographic Techniques
- o Choose Cryptographic Implementations

• Implementing Security Controls for Hosts

- o Select Host Hardware and Software
- o Harden Hosts
- o Virtualize Servers and Desktops
- o Implement Cloud Augmented Security Services
- o Protect Boot Loaders

o Implementing Security Controls for Enterprise Storage

- o Identify Storage Types and Protocols
- o Implement Secure Storage Controls



More...

- **Analyzing and Implementing Network Security**
 - o Analyze Network Security Components and Devices
 - o Analyze Network-Enabled Devices
 - o Analyze Advanced Network Design
 - o Configure Controls for Network Security
- **Implementing Security Controls for Applications**
 - o Identify General Application Vulnerabilities
 - o Identify Web Application Vulnerabilities
 - o Implement Application Security Controls
- **Integrating Hosts, Storage, Networks, and Applications in a Secure Enterprise Architecture**
 - o Implement Security Standards in the Enterprise
 - o Select Technical Deployment Models
 - o Secure the Design of the Enterprise Infrastructure
 - o Secure Enterprise Application Integration Enablers
- **Conducting Vulnerability Assessments**
 - o Select Vulnerability Assessment Methods
 - o Select Vulnerability Assessment Tools
- **Responding to and Recovering from Incidents**
 - o Design Systems to Facilitate Incident Response
 - o Conduct Incident and Emergency Responses



CONTACT US :