Cyber Gate
ACADEMY

CySA+

COMPTIA CYSA+ CYBERSECURITY ANALYST COURSE

Course Overview

You have experience in the increasingly crucial field of information security, and now you're ready to take that experience to the next level. CompTIA® Advanced Security Practitioner (CASP) (Exam CAS-002) is the course you will need to take if your job responsibilities include securing complex enterprise environments. In this course, you will expand on your knowledge of information security to apply more advanced principles that will keep your organization safe from the many ways it can be threatened.

Today's IT climate demands individuals with demonstrable skills, and the information and activities in this course can help you develop the skill set you need to confidently perform your duties as an advanced security professional. This course is designed for IT professionals who want to acquire the technical knowledge and skills needed to conceptualize, engineer, integrate, and implement secure solutions across complex enterprise environments. This course can also benefit you if you intend to pass the CompTIA Advanced Security Practitioner (CAS-002) certification examination. What you learn and practice in this course can be a significant part of your preparation.

Course Duration

5 Days (40 Hours).

Target Audience

Individuals seeking the CompTIA Advanced Security Practitioner (CASP) certification (Exam CAS-002); IT professionals with a minimum of 10 years of experience in IT administration and at least five years of hands-on security in an enterprise environment.

During this course you should learn

1. Manage risk in the enterprise.
2. Integrate computing, communications, and business disciplines in the enterprise.
3. Use research and analysis to secure the enterprise.
4. Integrate advanced authentication and authorization techniques.
5. Implement cryptographic techniques.
6. Implement security controls for hosts.
7. Implement security controls for storage.
8. Analyze network security concepts, components, and architectures, and implement controls.
9. Implement security controls for applications.
10. Integrate hosts, storage, networks, and applications in a secure enterprise architecture.
11. Conduct vulnerability assessments.
12. Conduct incident and emergency responses.

Course Content

Lesson 1: Managing Risk

- Identify the Importance of Risk Management.
- Assess Risk.
- Mitigate Risk.
- Integrate Documentation into Risk Management.

Lesson 2: Integrating Computing, Communications, and Business Disciplines

- Facilitate Collaboration Across Business Units.
- Secure Communications and Collaboration Solutions.
- Implement Security Activities Throughout the Technology Life Cycle.

Lesson 3: Using Research and Analysis to Secure the Enterprise

- Determine Industry Trends and Effects on the Enterprise.
- Analyze Scenarios to Secure the Enterprise.

Lesson 4: Integrating Advanced Authentication and Authorization Techniques

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

Lesson 5: Implementing Cryptographic Techniques

- Describe Cryptographic Concepts.
- Choose Cryptographic Techniques.
- Choose Cryptographic Implementations.

Lesson 6: Implementing Security Controls for Hosts

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

Lesson 7: Implementing Security Controls for Enterprise Storage

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

Lesson 8: Analyzing and Implementing Network Security

- Analyze Network Security Components and Devices.
- Analyze Network-Enabled Devices.
- Analyze Advanced Network Design.
- Configure Controls for Network Security.

Lesson 9: Implementing Security Controls for Applications

- Identify General Application Vulnerabilities.
- Identify Web Application Vulnerabilities.
- Implement Application Security Controls.

Lesson 10. Integrating Hosts, Storage, Networks, and Applications in a Secure Enterprise Architecture

- Implement Security Standards in the Enterprise.
- Select Technical Deployment Models.
- Secure the Design of the Enterprise Infrastructure.
- Secure Enterprise Application Integration Enablers.

Lesson 11: Conducting Vulnerability Assessments

- Select Vulnerability Assessment Methods.
- Select Vulnerability Assessment Tools.

Lesson 12: Responding to and Recovering from Incidents

- Design Systems to Facilitate Incident Response.
- Conduct Incident and Emergency Responses.

Classroom Live Labs

- Lab 1: Integrate Documentation into Risk Management.
- Lab 2: Secure Communications and Collaboration Solutions.
- Lab 3: Analyze Scenarios to Secure the Enterprise.
- Lab 4: Implement Authentication and Authorization Technologies.
- Lab 5; Choose Cryptographic Techniques
- Lab 6: Harden Hosts.
- Lab 7: Virtualize Servers and Desktops.
- Lab 8: Protect Boot Loaders.
- Lab 9: Implement Secure Storage Controls.
- Lab 10: Configure Controls for Network Security.
- Lab 11: Implement Application Security Controls.
- Lab 12: Select Vulnerability Assessment Tools.
- Lab 13: Design Systems to Facilitate Incident Response.
- Lab 14: Conduct Incident and Emergency Responses.

Prerequisites

Attendees should meet the following prerequisites:

- Attendance in our Internetworking with TCP/IP and Switching in IP Networks courses is strongly recommended Security+ Prep Course.

Recommended prerequisites: G013 - CompTIA Security+

Course Agenda

Day 1	Lesson 1: Managing Risk. Lesson 2: Integrating Computing, Communications, and Business Disciplines. Lesson 3: Using Research and Analysis to Secure the Enterprise.
Day 2	Lesson 4: Integrating Advanced Authentication and Authorization Techniques. Lesson 5: Implementing Cryptographic Techniques.
Day 3	Lesson 6: Implementing Security Controls for Hosts. Lesson 7: Implementing Security Controls for Enterprise Storage. Lesson 8: Analyzing and Implementing Network Security.
Day 4	Lesson 9: Implementing Security Controls for Applications. Lesson 10: Integrating Hosts, Storage, Networks, and Applications in a Secure Enterprise Architecture.
Day 5	Lesson 11: Conducting Vulnerability Assessments. Lesson 12: Responding to and Recovering from Incidents.

Technical Requirement

1. Laptop with minimum 8GB Ram.
2. Connected Monitor for iLabs.
3. Hi speed Internet Connection as All the labs it will be accessed through EC-Council Cloud.

Exam Voucher Validity

It will be valid for 12month starting from the last day of the course.

Certification Expiry

It will be valid for 3 years.

YOUR TRUSTED DEFENDERS

ADDRESS

CyberGate Academy
ADPOLY, MBZ City

WEB

academy@cybergate.tech
training@cybergate.tech