CompTIA CASP+ Course Outline

ERIC REED

CYBERSECURITY TRAINING

PASS ON THE FIRST ATTEMPT!™

COMPANY OVERVIEW

For over 25 years, Eric Reed Cybersecurity Training has been a trusted leader in cybersecurity education, equipping more than 60,000 professionals with the skills needed to defend against emerging cyber threats. Our mission is to empower individuals and organizations with comprehensive, hands-on training that translates directly to real-world success. Recognized with multiple industry awards—including an unprecedented 10-time EC Council Instructor of the Year and 7-time Circle of Excellence honoree—we combine innovative delivery methods with a passion for excellence to ensure our students achieve certification success on the first attempt

COMPTIA CASP+

CompTIA Advanced Security Practitioner (CASP+) is a performance-based certification for experienced cybersecurity professionals focusing on enterprise security and risk management.

COURSE OBJECTIVES

- Design and implement advanced security solutions.
- Assess enterprise security risks and develop mitigation strategies.
- Secure cloud, mobile, and virtualization environments.
- Integrate cryptographic techniques into security policies.
- Manage security governance, risk, and compliance.

SALARY RANGE

CASP+ → $90,000 - $130,000

These figures are approximate and depend on location, experience, and job role. Higher salaries are usually seen in major tech hubs and with significant experience.

JOB ROLES

- **Senior Security Engineer**
- **Architect**

ONLINE LIVE LEARNING

ON-DEMAND LIVE LEARNING

ONLINE LIVE & ON-DEMAND LIVE

All the benefits of live, instructor-led training with the convenience of on-demand.

- **Online Live:** Attend our scheduled sessions in real time (Monday–Friday). Get immediate interaction with the instructor and fellow students.
- **On-Demand Live:** Access recordings of the most recent live sessions on your own schedule, while still having direct instructor support.
- **Flexible Scheduling:** Choose a structured approach—one-week bootcamp (M–F), two nights a week for five weeks, or every Saturday for five weeks. Need more wiggle room? Adjust any schedule to fit your lifestyle!

★★★★★

"It's was a great class that covered all aspects of security. Most importantly, I appreciate the fact that you are giving up your own time to assist us and maintain a sharedrive with the latest security tools and informative papers even after the class is over. I was able to pass the test after one week of attending the training."

-Shadi Ehalabi

WWW.LINKEDIN.COM/IN/ERICREEDLIVE/

Contact Us

(707) 722-7333

info@ericreedlive.com

1401 61st St S
Gulfport, FL 33707

CompTIA CASP+ Course Outline

COMPTIA CASP+ OVERVIEW

1 - Supporting IT Governance and Risk Management

Identify the Importance of IT Governance and Risk Management

Assess Risk

Mitigate Risk

Integrate Documentation into Risk Management

2 - Leveraging Collaboration to Support Security

Facilitate Collaboration across Business Units

Secure Communications and Collaboration Solutions

3 - Using Research and Analysis to Secure the Enterprise

Determine Industry Trends and Their Effects on the Enterprise

Analyze Scenarios to Secure the Enterprise

4 - Integrating Advanced Authentication and Authorization Techniques

Implement Authentication and Authorization TechnologiesImplement

Advanced Identity and Access Management

5 - Implementing Cryptographic Techniques

Select Cryptographic Techniques

Implement Cryptography

6 - Implementing Security Controls for Hosts

Select Host Hardware and Software

Harden Hosts

Virtualize Servers and Desktops

Protect Boot Loaders

7 - Implementing Security Controls for Mobile Devices

Implement Mobile Device Management

Address Security and Privacy Concerns for Mobile Devices

8 - Implementing Network Security

Plan Deployment of Network Security Components and Devices

Plan Deployment of Network-Enabled Devices

Implement Advanced Network Design

Implement Network Security Controls

CompTIA CASP+ Course Outline

9 - Implementing Security in the Systems and Software Development Lifecycle

Implement Security throughout the Technology Lifecycle

Identify General Application Vulnerabilities

Identify Web Application Vulnerabilities

Implement Application Security Controls

10 - Integrating Assets in a Secure Enterprise Architecture

Integrate Standards and Best Practices in Enterprise Security

Select Technical Deployment Models

Integrate Cloud-Augmented Security Services

Secure the Design of the Enterprise Infrastructure

Integrate Data Security in the Enterprise Architecture

Integrate Enterprise Applications in a Secure Architecture

11 - Conducting Security Assessments

Select Security Assessment Methods

Perform Security Assessments with Appropriate Tools

12 - Responding to and Recovering from Incidents

Prepare for Incident Response and Forensic Investigations

Conduct Incident Response and Forensic Analysis