CompTIA Security+ 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 SECURITY+

CompTIA Security+ is an entry-level cybersecurity certification covering essential security concepts, risk management, and network security. It is suitable for security analysts and SOC analysts.

COURSE OBJECTIVES

- Identify and mitigate security threats and vulnerabilities.
- Implement security controls and risk management strategies.
- Configure secure network architectures and protocols.
- Manage identity, access control, and authentication methods.
- Respond to security incidents and perform forensic analysis.

SALARY RANGE

Sec+ → $75,000 - $115,000

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

- **Security Analyst**
- **SOC Analyst**

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 Security+ Course Outline

COMPTIA SECURITY+ OVERVIEW

1 - Summarize Fundamental Security Concepts

Security Concepts

Security Controls

2 - Compare Threat Types

Threat Actors

Attack Surfaces

Social Engineering

3 - Explain Cryptographic Solutions

Cryptographic Algorithms

Public Key Infrastructure

Cryptographic Solutions

4 - Implement Identity and Access Management

Authentication

Authorization

Identity Management

5 - Secure Enterprise Network Architecture

Enterprise Network Architecture

Network Security Appliances

Secure Communications

6 - Secure Cloud Network Architecture

Cloud Infrastructure

Embedded Systems and Zero Trust Architecture

7 - Explain Resiliency and Site Security Concepts

- Asset Management

- Redundancy Strategies

- Physical Security

8 - Explain Vulnerability Management

Device and OS Vulnerabilities

Application and Cloud Vulnerabilities

Vulnerability Identification Methods

Vulnerability Analysis and Remediation

CompTIA Security+ Course Outline

9 - Evaluate Network Security Capabilities

Network Security Baselines

Network Security Capability Enhancement

10 - Assess Endpoint Security Capabilities

Implement Endpoint Security

Mobile Device Hardening

11 - Enhance Application Security Capabilities

Application Protocol Security Baselines

Cloud and Web Application Security Concepts

12 - Explain Incident Response and Monitoring Concepts

Incident Response

Digital Forensics

Data Sources

Alerting and Monitoring Tools

13 - Analyze Indicators of Malicious Activity

Malware Attack Indicators

Physical and Network Attack Indicators

Application Attack Indicators

14 - Summarize Security Governance Concepts

Policies, Standards, and Procedures

Change Management

Automation and Orchestration

15 - Explain Risk Management Processes

Risk Management Processes and Concepts

Vendor Management Concepts

Audits and Assessments

16 - Summarize Data Protection and Compliance Concepts

Data Classification and Compliance

Personnel Policies