SSCP: Systems Security Certified Practitioner

Duration: 4 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

SSCP certification demonstrates you have the advanced technical skills and knowledge to implement, monitor and administer IT infrastructure using security best practices, policies and procedures established by the cybersecurity experts at (ISC)².

Prove your skills, advance your career, and gain the support of a community of cybersecurity leaders here to help you throughout your career.

Attend SSCP certification course and get prepared to pass the exam and become a Systems Security Certified Practitioner. This course will provide you with in-depth coverage on the skills and concepts in the seven domains of systems security including Access Controls, Security Operations and Administration, Incident Response, Cryptography and Network Security among others.

SKILLS COVERED

After completing this course, students will be able to:

- Prepare for and pass the SSCP Exam
- Implement authentication mechanisms
- Document and operate security controls
- Perform security assessment activities
- Understand security issues related to networks

WHO SHOULD ATTEND?

The SSCP is ideal for IT administrators, managers, directors and network security professionals responsible for the hands-on operational security of their organization's critical assets, including those in the following positions:

- Network Security Engineer
- Systems Administrator
- Security Analyst
- Systems Engineer
- Security Consultant/Specialist
- Security Administrator
- Systems/Network Analyst
- Database Administrator

PREREQUISITES

Minimum of one-year full-time experience in one of the domains covered in the SSCP exam.

MODULES

Module 1: Access Controls

- Implement authentication mechanisms
- Operate internetwork trust architectures
- Participate in the identity-management lifecycle
- Implement access controls

Module 2: Security Operations and Administration

- Understand and comply with code of ethics
- Understand security concepts
- Document and operate security controls
- Participate in asset management

- Implement and assess compliance with controls
- Participate in change management
- Participate in security awareness and training
- Participate in physical security operations

Module 3: Risk Identification, Monitoring, and Analysis

- Understand the risk management process
- Perform security assessment activities
- Operate and maintain monitoring systems
- Analyze monitoring results

Module 4: Incident Response and Recovery

- Participate in incident handling
- Understand and support forensic investigations
- Understand and support BCP and DRP

Module 5: Cryptography

- Understand and apply fundamental concepts of cryptography
- Understand requirements for cryptography
- Understand and support secure protocols
- Operate and implement cryptographic systems

Module 6: Networks and Communications Security

- Understand security issues related to networks
- Protect telecommunications technologies
- Control network access
- Manage LAN-based security
- Operate and configure network-based security devices
- Implement and operate wireless technologies

Module 7: Systems and Application Security

- Identify and analyze malicious code and activity
- Implement and operate endpoint device security
- Operate and configure cloud security
- Secure big data systems

END OF PAGE