Course Outline

SSCP Certification Prep Course
Course SSCP-CPC: 5 days Instructor Led

About this course
The best way to combat an attack on an organization's information assets is to have qualified information security professionals with the appropriate practices and controls to implement, monitor and administer IT infrastructure to ensure data confidentiality, integrity and availability. This SSCP certification prep course validates student's ability to identify, evaluate, and prioritize potential threats, manage and mitigate threats through risk management concepts, assessment activities, and monitoring terminology, techniques and systems.

Gain skills to properly and promptly respond to a security incident or forensic investigation with incident handling processes and procedures such as Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP).
This updated edition covers the SSCP exam objectives effective as of November 2021. Much of the new and more advanced knowledge expected of an SSCP is now covered in a new chapter "Cross-Domain Challenges." If you're an information security professional or student of cybersecurity looking to tackle one or more of the seven domains of the SSCP, this course gets you prepared to pass the exam and enter the information security workforce with confidence.

Audience profile
- Network security engineer
- Security administrator
- Security analyst
- Systems engineer
- Network administrator
- Systems administrator
- Security specialist
- Systems/network analyst
- Security consultant
- Database administrator

At course completion
After completing this course, students will be able to:
- Security Operations and Administration
- Access Controls
- Risk Identification, Monitoring, and Analysis
- Incident Response and Recovery
- Cryptography
- Network and Communications Security
- Systems and Application Security

Course Outline

Chapter 1: The Business Case for Decision Assurance and Information Security
Chapter 2: Information Security Fundamentals
Chapter 3: Integrated Information Risk Management
Chapter 4: Operationalizing Risk Mitigation
Chapter 5: Communications and Network Security
Chapter 6: Identity and Access Control

SHI | TRAINING & ADOPTION

Course Outline

Chapter 7: Cryptography
Chapter 8: Hardware and Systems Security
Chapter 9: Applications, Data, and Cloud Security
Chapter 10: Incident Response and Recovery
Chapter 11: Business Continuity via Information Security and People Power
Chapter 12: Cross-Domain Challenges