

Systems Security Certified Practitioner (SSCP)

ID SSCP Preis CHF 4'940.– (exkl. MwSt.) Dauer 5 Tage

Zielgruppe

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

Empfohlenes Training für die Zertifizierung zum

Systems Security Certified Practitioner (SSCP)

Voraussetzungen

Candidates must have a minimum of 1 year cumulative work experience in 1 or more of the 7 domains of the SSCP CBK. A 1 year prerequisite pathway will be granted for candidates who received a degree (bachelors or masters) in a cybersecurity program.

A candidate that doesn't have the required experience to become an SSCP may become an Associate of ISC2 by successfully passing the SSCP examination. The Associate of ISC2 will then have 2 years to earn the 1 year required experience.

Kursziele

The Systems Security Certified Practitioner (SSCP) is the ideal certification for those with proven technical skills and practical, hands-on security knowledge in operational IT roles. It provides confirmation of a practitioner's ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability.

Kursinhalt

Domain 1: Access Controls

- Implement and maintain authentication methods
- Support internetwork trust architectures
- Participate in the identity management lifecycle
- Implement access controls

Domain 2: Security Operations and Administration

- Comply with codes of ethics
- Understand security concepts
- Document, implement, and maintain functional security controls
- Participate in asset management
- Implement security controls and assess compliance
- Participate in change management
- Participate in security awareness and training
- Participate in physical security operations (e.g., data center assessment, badging)

Domain 3: Risk Identification, Monitoring, and Analysis

- Understand the risk management process
- Perform security assessment activities
- Operate and maintain monitoring systems (e.g., continuous monitoring)
- Analyze monitoring results

Domain 4: Incident Response and Recovery

- Support incident lifecycle
- Understand and support forensic investigations
- Understand and support Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) activities

Domain 5: Cryptography

- Understand fundamental concepts of cryptography
- Understand reasons and requirements for cryptography
- Understand and support secure protocols
- Understand Public Key Infrastructure (PKI) systems

Domain 6: Network and Communications Security

- Understand and apply fundamental concepts of networking
- Understand network attacks and countermeasures (e.g., DDoS, man-in-the-middle, DNS poisoning)
- Manage network access controls
- Manage network security

- Operate and configure network-based security devices
- Operate and configure wireless technologies (e.g., bluetooth, NFC, WiFi)

Domain 7: Systems and Application Security

- Identify and analyze malicious code and activity
- Implement and operate endpoint device security
- Operate and configure cloud security
- Operate and secure virtual environments

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer GmbH

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>