Training: ISC2
ISC2 SSCP Certification Prep Course

TRAINING GOALS:

Official ISC2 SSCP CBK Training Seminar for the SSCP (Systems Security Certified Practitioner)

This course provides a comprehensive review of information security concepts and industry best practices, covering the following seven domains of the SSCP Common Body of Knowledge (CBK®):

- Domain 1: Security Operations and Administration
- Domain 2: Access Controls
- Domain 3: Risk Identification, Monitoring and Analysis
- Domain 4: Incident Response and Recovery
- Domain 5: Cryptography
- Domain 6: Network and Communications Security
- Domain 7: Systems and Application Security

Each participant in an authorized training ISC2 ***SSCP Certification Prep Course*** *held in Exclusive Networks will receive a free SSCP Certification Exam voucher.*

Course objectives

At the end of this course, learners will be able to:

- Describe security and the alignment of asset management to risk management.
- Appraise risk management options and the use of access controls to protect assets.
- Examine the field of cryptography to secure information and communication.
- Build a security posture by securing software, data, and endpoints.
- Apply network and communications security to establish a secure networked environment.
- Evaluate cloud and wireless security.
- Prepare for incident detection and response.
- Implement appropriate measures that contribute to the maturation of risk management.

Intended audience

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

This course is for individuals planning to pursue the SSCP certification. The 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.

The SSCP is intended for professionals who have a minimum of one year cumulative work experience in one or more of the seven domains of the SSCP CBK. A one-year prerequisite pathway will be granted for candidates who receive a degree (bachelor's or master's) in a cybersecurity program.

- Prior to taking this course the learner should have experience, skills, or knowledge obtained while serving in the following roles:
- Network Security Engineer
- IT/Systems/Network Administrator
- Security Analyst
- Systems Engineer
- Security Consultant/Specialist
- Security Administrator
- Systems/Network Analyst
- Database Administrator
- Individuals operating in a security operations center (SOC) environment performing the role of incident handler, SIEM, forensics specialist, threat intel researcher, etc.

CONSPECT:

- Introducing Security and Aligning Asset Management to Risk Management
  - Classify information security and security concepts.
  - Summarize components of the asset management lifecycle .
  - Identify common risks and vulnerabilities.
  - Provide examples of appropriate risk treatment.
- Understanding Risk Management Options and the Use of Access Controls to Protect Assets
  - Provide examples of functional security controls and policies for identified scenarios.
  - Classify various access control models.
  - Identify components of the identity management lifecycle.
- Cryptography
  - Identify the fundamental concepts of cryptography driving requirements and benefits.
  - Recognize symmetric encryption methods.
  - Use asymmetric encryption methods.
  - Examine Public-Key Infrastructure (PKI) systems and certificates.
  - Summarize fundamental key management terms and concepts.

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Recognize how to implement secure protocols.
- Review methods of cryptanalytic attack.

- Securing Software, Data, and Endpoints
  - Discuss software systems and application security.
  - Recognize data security concepts and skills.
  - Identify malicious code and countermeasures.
  - Evaluate Mobile Device Management (MDM) and security issues with mobile and autonomous endpoints.
  - Review attacks and countermeasures for virtual machines.
- Network and Communications Security
  - Recognize layers of the OSI Model, their functions, and attacks present at each layer.
  - Identify commonly used ports and protocols.
  - Select appropriate countermeasures for various network attacks.
  - Summarize best practices for establishing a secure networked environment.
- Cloud and Wireless Security
  - Recall cloud security concepts and configurations.
  - Recognize types of virtualization and cloud security considerations.
  - Summarize the types of telecommunications and network access controls.
- Incident Detection and Response
  - Review the steps for monitoring, incident detection, and data loss prevention using all source intelligence.
  - Identify the elements of an incident response policy and members of the incident response team (IRT).
  - Classify the SSCP's role in supporting forensic investigations.
- Maturing Risk Management
  - Identify operational aspects of change management.
  - Summarize physical security considerations.
  - Design a security education and awareness strategy.
  - Recognize common security assessment activities.
  - Classify the components of a business continuity plan and disaster recovery plan.

REQUIREMENTS:

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

A candidate who doesn’t have the required experience to become an SSCP may become an Associate

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

of ISC2 by successfully passing the SSCP examination. The Associate of ISC2 will then have two years to earn the one year required experience.

Part-time work and internships may also count towards your experience.

Valid experience includes information systems security-related work performed, or work that requires information security knowledge and involves direct application of that knowledge. Experience must fall within one or more of the seven domains of the ISC2 SSCP CBK:

- Domain 1. Security Operations and Administration
- Domain 2. Access Controls
- Domain 3. Risk identification, Monitoring, and Analysis
- Domain 4. Incident Response and Recovery
- Domain 5. Cryptography
- Domain 6. Network and Communications Security
- Domain 7. Systems and Application Security

More information https://www.isc2.org/Certifications/SSCP/experience-requirements

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by ISC2 (course completion).

In order to complete the course, receive a certificate of completion and earn ISC2 continuing professional education (CPE) credits, learners must:

- Complete all learning activities within the course.
- Complete a course evaluation.
- Score 70% or higher on the end-of-chapter quizzes and final assessment.

A Certificate of Completion will be provided in class by your instructor once you have completed a course by meeting all the requirements. Please retain the certificate of completion as proof of credits earned.

This course will help prepare you also for the SSCP certification exam available at Pearson VUE test centers.

Each participant in an authorized training ISC2 ***SSCP Certification Prep Course*** *held in Exclusive Networks will receive a free SSCP Certification Exam voucher.*

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

TRAINER:

ISC2 Authorized Instructor

ADDITIONAL INFORMATION:

Participating in this training you get 40 CPE (Continuing Professional Education) credits.

CPE credits for ISC2 credentials must be self-reported by members and associates through the ISC2 CPE Portal accessible via www.isc2.org using your member login credentials.

CPE credits earned for this course may be eligible for continuing professional education credits for non-ISC2 certifications. Please visit the continuing education requirements established by the credentialing organization for eligibility.

For specific questions related to your CPE credits or the CPE portal please contact member support - membersupport@isc2.org.

The Official ISC2 CBK Training Seminar for the SSCP has earned ACE CREDIT. Students who complete the course can apply for two hours of lower division credit at participating universities and colleges. For more information https://www.acenet.edu/national-guide/Pages/default.aspx

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310