Official ISC2 Systems Security Certified Practitioner (SSCP) Training

Duration: 5 Days **Course Code: SSCP** **Delivery Method: Virtual Learning**

Overview:

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. The broad spectrum of topics included in the SSCP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security.

Successful candidates are competent in the following seven domains: Security Operations and Administration Access Controls Risk Identification, Monitoring and Analysis Incident Response and Recovery Cryptography Network and Communications Security Systems and Application Security

Please noteTo register for the new (ISC)2 exam, you will need a Pearson VUE exam voucher. This exam voucher is not included in the course price.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

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 EngineerSystems AdministratorSecurity AnalystSystems EngineerSecurity Consultant/SpecialistSecurity AdministratorSystems/Network AnalystDatabase Administrator

Objectives:

- **After completing this course you should be able to:**
- Understand the different Access Control systems and how they should be implemented to protect the system and data using the different levels of confidentiality, integrity, and availability.
- Understand the processes necessary for working with management and information owners, custodians, and users so that proper data classifications are defined. This will ensure the proper handling of all hard copy and electronic information as it is applied by the Security Operations and Administration.
- The Risk Identification, Monitoring, and Analysis Domain identifies the how to identify, measure, and control losses associated with adverse events. You will review,analyze, select, and evaluate safeguards for mitigating risk.
- Identify how to handle Incident Response and Recovery using consistent, applies approaches including the use of the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) concepts in order to mitigate damages, recover business operations, and avoid critical business interruption; and emergency response and post-disaster recovery.
- Identify and differentiate key cryptographic concepts and how to apply them, implement secure protocols, key management concepts, key administration and validation, and Public Key Infrastructure as it applies to securing communications in the presence of third parties.
- Define and identify the Networks and Communications Security needed to secure network structure, data transmission methods, transport formats, and the security measures used to maintain integrity, availability, authentication, and confidentiality of the information being transmitted.
- The Systems and Application Security section identifies and defines technical and non-technical attacks and how an organization can protect itself from these attacks including the concepts in endpoint device security, cloud infrastructure security, securing big data systems, and securing virtual environments.

Prerequisites:

- One year working in the Information Security arena, covering at least one of the domains from the SSCP CBK.
- G005 - CompTIA Network+

Testing and Certification

- Length of exam 3 hours
- Number of items 125
- Item format Multiple choice
- Passing grade 700 out of 1000 points
- Language availability English, Japanese and Brazilian Portuguese
-
- Security Operations and Administration 16%
- Access Controls 15%
- Risk Identification, Monitoring and Analysis 15%
- Incident Response and Recovery 14%
- Cryptography 9%
- Network and Communications Security 16%
- Systems and Application Security 15%

Total100%

Content:

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 the 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
- Analyse 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 the 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 analyse malicious code and activity
- Implement and operate endpoint device security
- Operate and configure cloud security
- Secure big data systems

Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A,First Floor, Office F68, Dubai, UAE