SC210-EN ISC2 CISSP Preparation

Kurzbeschreibung:

In the **SC210-EN ISC2 CISSP Preparation** course, participants acquire comprehensive knowledge and skills that are necessary for the strategic and technical implementation of information security. At the same time, they are prepared for the CISSP ISC2 certification exam. In our intensive 5-day course, the contents of the eight domains of the Common Body of Knowledge (CBK) are taught. The CBK is a compendium that bundles proven security methods (best practices), technologies, theories, models and concepts.

The CISSP is the first certification accredited by ANSI as ISO Standard 17024:2003 in the field of information security and offers not only an objective assessment of competence, but also a globally recognised standard of performance. The course material is presented in a practical, concrete and understandable way using examples on the whiteboard and flipchart.

Accompanying the course, the books "ISC2 CISSP Official Study Guide" and "ISC2 CISSP Official Practice Tests" are provided free of charge.

Zielgruppe:

The workshop **SC210-EN ISC2 CISSP Preparation** is ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles, including those in the following positions:

- Chief Information Security Officer
- Chief Information Officer
- Director of Security
- IT Director/Manager
- Security Manager
- Security Architect
- Network Architect
- Security Systems Engineer
- Security Consultant

A solid understanding of common security mechanisms and several years of experience with general IT principles in at least two or more of the eight domains is recommended.

Voraussetzungen:

Basically, anyone interested in IT security, information technology and IT processes can aim for the CISSP certification in order to validate their knowledge at an internationally recognised level. However, in order to cover the broad scope of the CBK in a meaningful way within one week, knowledge in several areas of IT is an advantage. A willingness to engage with the content beyond the course - for example in the form of in-depth online questionnaires - is essential.

Although no training or studies are required to take the exam, proof of at least five years of relevant professional experience in at least two of the CBK subject areas (or 4 years of experience plus a relevant university degree) is mandatory after successful completion of the exam in order to obtain the certificate. Proof of the above-mentioned relevant professional experience is required in the form of an "endorsement" by a

CISSP (e.g. by the trainer) in order to subsequently apply for the certificate from the ISC2.

Sonstiges:

Dauer: 5 Tage

Preis: 3450 Euro plus Mwst.

Ziele:

The eight domains of the Common Body of Knowledge (CBK) are described as "a mile wide and an inch thick". Intensive preparation for the content and process of the CISSP (Certified Information Systems Security Professional) exam, including discussion of all relevant subject areas, means that participants are taught a wide range of technical expertise, process knowledge and architectures in quick succession.
Particular attention is paid to the newly added topics of "BYOD", Software Defined Networks and Cloud Identity Services.

Inhalte/Agenda:

- ♦ **Domain 1: Security and Risk Management**
  - ♦ ◊ Security concepts
  - ◊ Compliance, legal and regulatory requirements
  - ◊ Standards and Frameworks
  - ◊ Risk Management
  - ◊ Business Continuity

- ♦ **Domain 2: Asset Security**
  - ♦ ◊ Security models and frameworks
  - ◊ Asset management
  - ◊ Classification

- ♦ **Domain 3: Security Architecture and Engineering**
  - ♦ ◊ Understand the fundamental concepts of security models
  - ◊ Research, implement and manage engineering processes using secure design principles
  - ◊ Select and determine cryptographic solutions
  - ◊ Security principles

- ♦ **Domain 4: Communication and Network Security**
  - ♦ ◊ Topologies
  - ◊ Technologies
  - ◊ Protocols
  - ◊ Attacks
  - ◊ Security measures

- ♦ **Domain 5: Identity and Access Management (IAM)**
  - ♦ ◊ Identity Management
  - ◊ Access Control

- ♦ **Domain 6: Security Assessment and Testing**
  - ♦ ◊ Design and validate assessment, test, and audit strategies
  - ◊ Vulnerability assessment
  - ◊ Penetration testing

- ♦ **Domain 7: Security Operations**
  - ♦ ◊ Secure operation and maintenance
  - ◊ Incidence Response
  - ◊ Disaster Recovery Planning

- ♦ **Domain 8: Software Development Security**
  - ♦ ◊ Understand and integrate security in the Software Development Life Cycle
  - ◊ Web applications and mobile applications
  - ◊ Malware and attacks on applications
  - ◊ IoT und ICS

- ♦ **There will also be a review and Q&A sessions, as well as tips and learning methods.**
  - ♦