SC110 CompTIA Security+

Kurzbeschreibung:

In der 5-tägigen Schulung **SC110 CompTIA Security+** lernen Sie die grundlegenden Kenntnisse im Bereich der IT-Sicherheit und erhalten eine herstellerneutrale Zertifizierung von CompTIA. Der inhaltliche Schwerpunkt liegt auf generellen Sicherheitskonzepten für Zugangskontrolle, Authentifizierung und Abwehr externer Angriffe. Sie werden in diesem Workshop auch Sicherheitsaspekte für Kommunikation und Infrastruktur kennenlernen sowie die Grundlagen der Verschlüsselung, die für die erfolgreiche Absolvierung des Exams erforderlich sind. Diese Zertifizierung richtet sich an IT-Profis, die ihre Fähigkeiten offiziell bestätigen lassen möchten oder grundlegende Kenntnisse im Bereich IT-Sicherheit erwerben wollen.

Kurssprache: Wahlweise Deutsch oder Englisch
Kursunterlagen: Englisch
Prüfungssprache: Englisch

Zielgruppe:

Die Schulung **SC110 CompTIA Security+** richtet sich sowohl an System- und Netzwerkadministratoren, als auch an IT-Sicherheitsverantwortliche in einem Unternehmen.

Voraussetzungen:

Es werden folgende Vorkenntnisse empfohlen:

- zwei Jahre Erfahrung in der IT Administration mit Schwerpunkt Security
- Verständnis von Betriebssystemen und Kenntnisse von Windows-basierten Systemen wie Windows 7 oder Windows 8.1
- Fähigkeit, grundlegende Netzwerkkomponenten und ihre Rollen zu identifizieren, einschließlich Routern, Switches, Firewalls und Serverrollen. Erfahrungen in der Konfiguration von Firewalls sind vorteilhaft.
- Grundverständnis von drahtlosen Netzwerken
- Grundverständnis des OSI Modells und TCP/IP einschließlich IPv4 Subnetting

Sonstiges:

Dauer: 5 Tage

Preis: 2390 Euro plus Mwst.

Ziele:

- Bewerten Sie den Sicherheitsstatus einer Unternehmensumgebung und empfehlen und implementieren Sie geeignete Sicherheitslösungen
- Überwachen und sichern Sie hybride Umgebungen, einschließlich Cloud, Mobile und IoT
- Arbeiten Sie mit einem Bewusstsein für geltende Gesetze und Richtlinien, einschließlich der Grundsätze der Governance, des Risikos und der Compliance
- Identifizieren, Analysieren und Reagieren auf Sicherheitsereignisse und -vorfälle

Die CompTIA Secirity+ Zertifizierungsprüfung besteht aus maximal 90 Fragen, die in 90 Minuten beantwortet werden müssen. Sie brauchen ein Ergebnis von mindestens 750 Punkten (auf einer Skala von 100-900), um die Prüfung zu bestehen.

Die Prüfung können Sie in einem Pearson VUE Testzentrum oder online ablegen.

Inhalte/Agenda:

- ♦ **General Security Concepts**
  - ♦ ◊ Various types of security controls
  - ◊ Fundamental security concepts
  - ◊ The importance of change management processes and the impact to security
  - ◊ The importance of using appropriate cryptographic solutions
- ♦ **Threats, Vulnerabilities, and Mitigations**
  - ♦ ◊ Common threat actors and motivations
  - ◊ Common threat vectors and attack surfaces
  - ◊ Various types of vulnerabilities
  - ◊ Analyze indicators of malicious activity
  - ◊ The purpose of mitigation techniques used to secure the enterprise
- ♦ **Security Architecture**
  - ♦ ◊ Security implications of different architecture models
  - ◊ Apply security principles to secure enterprise infrastructure
  - ◊ Concepts and strategies to protect data
  - ◊ The importance of resilience and recovery in security architecture
- ♦ **Security Operations**
  - ♦ ◊ Apply common security techniques to computing resources
  - ◊ The security implications of proper hardware, software, and data asset management
  - ◊ Various activities associated with vulnerability management
  - ◊ Security alerting and monitoring concepts and tools
  - ◊ Modify enterprise capabilities to enhance security
  - ◊ Implement and maintain identity and access management
  - ◊ The importance of automation and orchestration related to secure operations
  - ◊ Appropriate incident response activities
  - ◊ Use data sources to support an investigation
- ♦ **Security Program Management and Oversight**
  - ♦ ◊ Elements of effective security governance
  - ◊ Elements of the risk management process
  - ◊ The processes associated with third-party risk assessment and management
  - ◊ Elements of effective security compliance
  - ◊ Types and purposes of audits and assessments
  - ◊ Implement security awareness practices
  - ♦ ◊