SC260 CompTIA SecurityX

Kurzbeschreibung:

Während Führungskräfte im Bereich Cybersicherheit bestimmen, welche Cybersicherheitsrichtlinien und -rahmenwerke umgesetzt werden können, wissen SecurityX-zertifizierte Experten (vormals CASP+), wie die Umsetzung der Lösungen innerhalb dieser Richtlinien und Rahmenwerke erfolgen kann.

Im Unterschied zu anderen Zertifizierungen deckt SecurityX sowohl die Sicherheitsarchitektur als auch die Technologie ab. In unserem Kurs **SC260 CompTIA SecurityX** werden Sie auf die SecurityX Zertifizierung vorbereitet. SecurityX ist die einzige praxisorientierte, leistungsbasierte Zertifizierung für Praktiker - nicht Manager - auf dem fortgeschrittenen Kompetenzniveau der Cybersicherheit, die technische Führungskräfte in die Lage versetzt, die Cyber-Bereitschaft eines Unternehmens zu bewerten und die richtigen Lösungen zu entwickeln und zu implementieren, um sicherzustellen, dass das Unternehmen auf den nächsten Angriff vorbereitet ist.

SecurityX umfasst technische Fähigkeiten in On-Premise-, Cloud- und Hybrid-Umgebungen, Governance-, Risiko- und Compliance-Fähigkeiten, die Bewertung der Cybersicherheitsbereitschaft eines Unternehmens und die Leitung technischer Teams zur Implementierung unternehmensweiter Cybersicherheitslösungen.

Zielgruppe:

Der Kurs **SC260 CompTIA SecurityX** ist geeignet für:

- IT-Professionals
- IT Specialist INFOSEC
- Cybersecurity Risk Manager
- Cybersecurity Risk Analyst
- Cyber Security / IS Professional
- Information Security Analyst
- Security Architect

Voraussetzungen:

Um den Inhalten und dem Lerntempo des Kurses **SC260 CompTIA SecurityX** gut folgen zu können, sind folgende Voraussetzungen notwendig:

- Mindestens zehn Jahre allgemeine praktische IT-Erfahrung, davon mindestens fünf Jahre umfassende praktische Erfahrung im Bereich Sicherheit.

Wir empfehlen die vorherige Teilnahme an unserem Kurs SC110 CompTIA Security+.

Sonstiges:

Dauer: 5 Tage

Preis: 2690 Euro plus Mwst.

Ziele:

Im Kurs **SC260 CompTIA SecurityX** erlernen Sie fortgeschrittene Methoden der Informationssicherheit, um Bedrohungen gezielt zu bekämpfen. Der offizielle Zertifikatslehrgang vermittelt Ihnen ein fundiertes Verständnis von fortgeschrittenen Sicherheitskonzepten, -methoden und -implementierungen, die zur Stärkung der Cybersicherheit auf Unternehmensebene beitragen. Der Workshop versetzt die Teilnehmenden in die Lage, komplexe Sicherheitsszenarien zu analysieren und wirksame Sicherheitsmaßnahmen im Unternehmensumfeld anzuwenden.

Erwerben Sie umfassende Kenntnisse, um als Experte für Informationssicherheit zu agieren und strategische Sicherheitsentscheidungen zu treffen, um Ihre Organisation vor komplexen Bedrohungen zu schützen. Der Kurs bereitet Sie gezielt auf die SecurityX Zertifizierungsprüfung vor und bietet Ihnen die Möglichkeit, Ihre Cybersicherheitskompetenzen nach international anerkannten Standards zu validieren.

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

Inhalte/Agenda:

- ♦ **Security Architecture**
  - ♦ ◊ Analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network
    ◊ Analyze the organizational requirements to determine the proper infrastructure security design
    ◊ Integrate software applications securely into an enterprise architecture
    ◊ Implement data security techniques for securing enterprise architecture
    ◊ Analyze the security requirements and objectives to provide the appropriate authentication and authorization controls
    ◊ Set of requirements, implement secure cloud and virtualization solutions
    ◊ Cryptography and public key infrastructure (PKI) support security objectives and requirements
    ◊ Impact of emerging technologies on enterprise security and privacy
- ♦ ◊
- ♦ **Security Operations**
  - ♦ ◊ Perform threat management activities
    ◊ Analyze indicators of compromise and formulate an appropriate response
    ◊ Aerform vulnerability management activities
    ◊ Use the appropriate vulnerability assessment and penetration testing methods and tools
    ◊ Analyze vulnerabilities and recommend risk mitigations
    ◊ Use processes to reduce risk
    ◊ Incident, implement the appropriate response
    ◊ The importance of forensic concepts
    ◊ Use forensic analysis tools
- ♦ ◊
- ♦ **Security Engineering and Cryptography**
  - ♦ ◊ Apply secure configurations to enterprise mobility
    ◊ Configure and implement endpoint security controls
    ◊ Considerations impacting specific sectors and operational technologies
    ◊ Cloud technology adoption impacts organizational security
    ◊ Business requirement, implement the appropriate PKI solution
    ◊ Business requirement, implement the appropriate cryptographic protocols and algorithms
    ◊ Troubleshoot issues with cryptographic implementations
- ♦ ◊
- ♦ **Governance, Risk, and Compliance**
  - ♦ ◊ Given a set of requirements, apply the appropriate risk strategies
    ◊ The importance of managing and mitigating vendor risk
    ◊ Compliance frameworks and legal considerations, and their organizational impact
    ◊ The importance of business continuity and disaster recovery concepts
    ♦ ◊