CompTIA Security+ Certification Training (SYO-601)

O que você aprenderá nesta formação

A formação CompTIA Security+ fornece o conhecimento básico necessário para o planejamento, a implementação e a manutenção da segurança da informação em um formato independente de fornecedor, incluindo gerenciamento de risco, segurança de host e de rede, sistemas de autenticação e controle de acesso, criptografia e segurança organizacional. Esta formação prepara o participante para o exame de certificação **SY0-601**: CompTIA Security+, via material didático e laboratórios oficiais da CompTIA.

A certificação Security+ é considerada o nível mínimo de certificação para todos os cargos de segurança de TI além do nível inicial. Esta formação oferece o conhecimento básico necessário para passar no exame e as habilidades necessárias para avançar para um cargo de segurança de nível intermediário. Esta certificação é compatível com o padrão ISO 17024 e aprovado pelo DoD (Departament of Defense) dos EUA para atender aos requisitos da diretiva 8140/8570.01-M. Mais de 2,3 milhões de exames CompTIA certificados pela ISO/ANSI foram entregues desde 1º de janeiro de 2011.

A quem se destina

- Administradores de rede e de sistemas
- Técnicos e analistas de segurança cibernética
- Engenheiros de rede e de cloud
- Pessoal das TICs interessado em seguir carreira em segurança cibernética

Metodologia, Duração, Preço

Formação via *virtual class* ou presencial com combinação de aulas expositivas e práticas, e simulado, com duração de cinco dias. Kz 997.000 por participante, incluindo um voucher para o exame **SY0-601**: CompTIA Security+.

Pré-requisitos

Recomenda-se de seis a nove meses de experiência em redes, incluindo configuração de parâmetros de segurança. Conhecimento equivalente às certificações CompTIA A+ e Network+ também é recomendado.

Conteúdo Programático

Lesson 1: Comparing Security Roles and Controls
Topic 1A: Compare and Contrast Information Security Roles
Topic 1B: Compare and Contrast Security Control and Framework Types

Lesson 2: Explaining Threat Actors and Threat Intelligence
Topic 2A: Explain Threat Actor Types and Attack Vectors
Topic 2B: Explain Threat Intelligence Sources

Lesson 3: Performing Security Assessments
Topic 3A: Assess Organizational Security with Network Reconnaissance Tools
Topic 3B: Explain Security Concerns with General Vulnerability Types
Topic 3C: Summarize Vulnerability Scanning Techniques
Topic 3D: Explain Penetration Testing Concepts

Lesson 4: Identifying Social Engineering and Malware
- Topic 4A: Compare and Contrast Social Engineering Techniques
- Topic 4B: Analyze Indicators of Malware-Based Attacks

Lesson 5: Summarizing Basic Cryptographic Concepts
- Topic 5A: Compare and Contrast Cryptographic Ciphers
- Topic 5B: Summarize Cryptographic Modes of Operation
- Topic 5C: Summarize Cryptographic Use Cases and Weaknesses
- Topic 5D: Summarize Other Cryptographic Technologies

Lesson 6: Implementing Public Key Infrastructure
- Topic 6A: Implement Certificates and Certificate Authorities
- Topic 6B: Implement PKI Management

Lesson 7: Implementing Authentication Controls
- Topic 7A: Summarize Authentication Design Concepts
- Topic 7B: Implement Knowledge-Based Authentication
- Topic 7C: Implement Authentication Technologies
- Topic 7D: Summarize Biometrics Authentication Concepts

Lesson 8: Implementing Identity and Account Management Controls
- Topic 8A: Implement Identity and Account Types
- Topic 8B: Implement Account Policies
- Topic 8C: Implement Authorization Solutions
- Topic 8D: Explain the Importance of Personnel Policies

Lesson 9: Implementing Secure Network Designs
- Topic 9A: Implement Secure Network Designs
- Topic 9B: Implement Secure Switching and Routing
- Topic 9C: Implement Secure Wireless Infrastructure
- Topic 9D: Implement Load Balancers

Lesson 10: Implementing Network Security Appliances
- Topic 10A: Implement Firewalls and Proxy Servers
- Topic 10B: Implement Network Security Monitoring
- Topic 10C: Summarize the Use of SIEM

Lesson 11: Implementing Secure Network Protocols
- Topic 11A: Implement Secure Network Operations Protocols
- Topic 11B: Implement Secure Application Protocols
- Topic 11C: Implement Secure Remote Access Protocols

Lesson 12: Implementing Host Security Solutions
- Topic 12A: Implement Secure Firmware
- Topic 12B: Implement Endpoint Security
- Topic 12C: Explain Embedded System Security Implications

Lesson 13: Implementing Secure Mobile Solutions
- Topic 13A: Implement Mobile Device Management
- Topic 13B: Implement Secure Mobile Device Connections

Lesson 14: Summarizing Secure Application Concepts
- Topic 14A: Analyze Indicators of Application Attacks
- Topic 14B: Analyze Indicators of Web Application Attacks
- Topic 14C: Summarize Secure Coding Practices
- Topic 14D: Implement Secure Script Environments
- Topic 14E: Summarize Deployment and Automation Concepts

Lesson 15: Implementing Secure Cloud Solutions
- Topic 15A: Summarize Secure Cloud and Virtualization Services
- Topic 15B: Apply Cloud Security Solutions
- Topic 15C: Summarize Infrastructure as Code Concepts

Lesson 16: Explaining Data Privacy and Protection Concepts
- Topic 16A: Explain Privacy and Data Sensitivity Concepts
- Topic 16B: Explain Privacy and Data Protection Controls

Lesson 17: Performing Incident Response
- Topic 17A: Summarize Incident Response Procedures
- Topic 17B: Utilize Appropriate Data Sources for Incident Response
- Topic 17C: Apply Mitigation Controls

Lesson 18: Explaining Digital Forensics
- Topic 18A: Explain Key Aspects of Digital Forensics Documentation
- Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition

Lesson 19: Summarizing Risk Management Concepts
- Topic 19A: Explain Risk Management Processes and Concepts
- Topic 19B: Explain Business Impact Analysis Concepts

Lesson 20: Implementing Cybersecurity Resilience
- Topic 20A: Implement Redundancy Strategies
- Topic 20B: Implement Backup Strategies
- Topic 20C: Implement Cybersecurity Resiliency Strategies

Lesson 21: Explaining Physical Security
- Topic 21A: Explain the Importance of Physical Site Security Controls
- Topic 21B: Explain the Importance of Physical Host Security Controls