Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Security+ [SY0-501] Certification Training Course

Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Overview

The CompTIA Security+ [SY0-501] Certification is a universally recognized highly valuable credential for foundation level IT security skills. This CompTIA training validates your ability to apply knowledge of information security to real networks. It certifies an individual's ability to identify risks, perform risk management and mitigation activities, and ensure operational security of enterprise networks. CompTIA Security+ [SY0-501] Training at Koenig makes you proficient in core IT security concepts such as Cryptography, risk mitigation and risk management, identity management, security infrastructure, organizational systems, security systems, network access control among others.

Successful completion of Security plus training from Koenig and subsequently getting certified by CompTIA will help you gain skills required by employers all over the world to manage and maintain security of their information systems. You can demonstrate that you can not only apply knowledge about security tools, concepts, and procedures to respond to security threats, but you also have skills to anticipate risks and protect against them proactively.

Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Security+ [SY0-501]

Part 1: Threats, Attacks and Vulnerabilities

- Chapter 1: Malware and Indicators of Compromise
- Chapter 2: Attacks
- Chapter 3: Threat Actors
- Chapter 4: Vulnerability Scanning and Penetration Testing
- Chapter 5: Vulnerabilities and Impacts

Part 2: Technologies and Tools

- Chapter 6: Network Components
- Chapter 7: Security Tools and Technologies
- Chapter 8: Troubleshoot Common Security Issues
- Chapter 9: Deploy Mobile Devices Securely
- Chapter 10: Implementing Secure Protocols

Part 3: Architecture and Design

- Chapter 11: Architecture Frameworks and Secure Network Architectures
- Chapter 12: Secure Systems Design and Deployment
- Chapter 13: Embedded Systems
- Chapter 14: Application Development and Deployment
- Chapter 15: Cloud and Virtualization
- Chapter 16: Resiliency and Automation strategies
- Chapter 17: Physical Security Controls

Part 4: Identity and Access Management

- Chapter 18: Identity, Access and Accounts
- Chapter 19: Identity and Access Services
- Chapter 20: Identity and Access Management Controls

Part 5: Risk Management

- Chapter 21: Policies, Plans and Procedures
- Chapter 22: Risk Management and Business Impact Analysis Concepts
- Chapter 23: Incident Response, Disaster Recovery and Continuity of Operation
- Chapter 24: Digital forensics
- Chapter 25: Compare and contrast various types of controls

Chapter 26: Data Security and Privacy Practices

Email: info@certificationsmaster.com
WhatsApp us @ +919311619773

Part 6: Cryptography and PKI

- Chapter 27: Cryptography Concepts
- Chapter 28: Cryptography Algorithms Chapter 29: Wireless Security
- Chapter 30: Public Key Infrastructure