a: 10B Hesse Bay, Regina, SK S4R 7Z9 | t: 306.525.0537
e: apptraining@microagesask.com | w: microage.ca/regina

CompTIA Security+ Certification

Who Should Attend

This course is designed for information technology (IT) professionals who have networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks; familiarity with other operating systems, such as macOS®, Unix®, or Linux®; and who want to further a career in IT by acquiring foundational knowledge of security topics or using CompTIA Security+ as the foundation for advanced security certifications or career roles. This course is also designed for students who are seeking the CompTIA Security+ certification and who want to prepare for the CompTIA Security+ SY0-601 Certification Exam.

Course Objectives

In this course, students will use fundamental security principles to install and configure cybersecurity controls and participate in incident response and risk mitigation. Students will: - Compare and contrast attacks. - Compare and contrast security controls. - Use security assessment tools. - Explain basic cryptography concepts. - Implement a public key infrastructure. - Implement identity and access management controls. - Manage access services and accounts. - Implement a secure network architecture. - Install and configure security appliances. - Install and configure wireless and physical access security. - Deploy secure host, mobile, and embedded systems. - Implement secure network access protocols. - Implement secure network applications. - Explain risk management and disaster recovery concepts. - Describe secure application development concepts. - Explain organizational security concepts.

Agenda

1 - Comparing Security Roles and Security Controls

- Compare and Contrast Information Security Roles
- Compare and Contrast Security Control and Framework Types

2 - Explaining Threat Actors and Threat Intelligence

- Explain Threat Actor Types and Attack Vectors
- Explain Threat Intelligence Sources

3 - Performing Security Assessments

- Assess Organizational Security with Network Reconnaissance Tools
- Explain Security Concerns with General Vulnerability Types
- Summarize Vulnerability Scanning Techniques
- Explain Penetration Testing Concepts

4 - Identifying Social Engineering and Malware

- Compare and Contrast Social Engineering Techniques
- Analyze Indicators of Malware-Based Attacks

5 - Summarizing Basic Cryptographic Concepts

- Compare and Contrast Cryptographic Ciphers
- Summarize Cryptographic Modes of Operation
- Summarize Cryptographic Use Cases and Weaknesses
- Summarize Other Cryptographic Technologies

6 - Implementing Public Key Infrastructure

- Implement Certificates and Certificate Authorities
- Implement PKI Management

7 - Implementing Authentication Controls

- Summarize Authentication Design Concepts
- Implement Knowledge-Based Authentication
- Implement Authentication Technologies
- Summarize Biometrics Authentication Concepts

8 - Implementing Identity and Account Management Controls

- Implement Identity and Account Types
- Implement Account Policies
- Implement Authorization Solutions
- Explain the Importance of Personnel Policies

9 - Implementing Secure Network Designs

- Implement Secure Network Designs
- Implement Secure Switching and Routing
- Implement Secure Wireless Infrastructure
- Implement Load Balancers

10 - Implementing Network Security Appliances

- Implement Firewalls and Proxy Servers
- Implement Network Security Monitoring
- Summarize the Use of SIEM

11 - Implementing Secure Network Protocols

- Implement Secure Network Operations Protocols
- Implement Secure Application Protocols
- Implement Secure Remote Access Protocols

12 - Implementing Host Security Solutions

- Implement Secure Firmware
- Implement Endpoint Security
- Explain Embedded System Security Implications

13 - Implementing Secure Mobile Solutions

- Implement Mobile Device Management
- Implement Secure Mobile Device Connections

14 - Summarizing Secure Application Concepts

- Analyze Indicators of Application Attacks
- Analyze Indicators of Web Application Attacks
- Summarize Secure Coding Practices
- Implement Secure Script Environments
- Summarize Deployment and Automation Concepts

15 - Implementing Secure Cloud Solutions

- Summarize Secure Cloud and Virtualization Services
- Apply Cloud Security Solutions
- Summarize Infrastructure as Code Concepts

16 - Explaining Data Privacy and Protection Concepts

- Explain Privacy and Data Sensitivity Concepts
- Explain Privacy and Data Protection Controls

17 - Performing Incident Response

- Summarize Incident Response Procedures
- Utilize Appropriate Data Sources for Incident Response
- Apply Mitigation Controls

18 - Explaining Digital Forensics

- Explain Key Aspects of Digital Forensics Documentation
- Explain Key Aspects of Digital Forensics Evidence Acquisition

19 - Summarizing Risk Management Concepts

- Explain Risk Management Processes and Concepts
- Explain Business Impact Analysis Concepts

20 - Implementing Cybersecurity Resilience

- Implement Redundancy Strategies
- Implement Backup Strategies
- Implement Cybersecurity Resiliency Strategies

21 - Explaining Physical Security

- Explain the Importance of Physical Site Security Controls
- Explain the Importance of Physical Host Security Controls