

Course Training

Cisco Certified Support Technician (CCST Cyber Security [100-160])

Course Content

Building a solid foundation in cybersecurity with the Cisco Certified Support Technician (CCST) course. This certification training is ideal for beginners seeking basic knowledge in cyber security. Additionally, the CCST certification serves as a stepping stone toward the CyberOps Associate certification.

It covers essential topics such as security principal network security endpoint security, vulnerability assessment, risk management, and incident handling, security policy and procedures, network monitoring and analysis.

Course Objectives

- Essential Security Principal
- Basic Networking Security Concepts
- Endpoint Security Concepts
- Vulnerability Assessment and Risk Management Incident Handling
- Incident Handling

Course Prerequisite

Cisco CCST Networking Certification, a basic understanding of how to use a computer and browse the internet.

Who should attend

- High school, secondary, and immediate post-secondary students
- Entry Level Cybersecurity
- Entry Level Network Security
- Entry Level IT Specialists
- Entry Level Network Administrator

Course Outline

- Define essential security principles
- Explain access management principles
- Explain encryption methods and applications
- Describe TCP/IP protocol vulnerabilities
- Explain how network addresses impact network security
- Describe network infrastructure and technologies
- Set up a secure wireless SoHo network
- Implement secure access technologies
- Describe operating system security concepts
- Demonstrate familiarity with appropriate endpoint tools that gather security assessment information
- Verify that endpoint systems meet security policies and standards
- Implement software and hardware updates
- Interpret system logs
- Demonstrate familiarity with malware removal
- Explain vulnerability management
- Use threat intelligence techniques to identify potential network vulnerabilities
- Explain risk management
- Explain the importance of disaster recovery and business continuity planning
- Monitor security events and know when escalation is required
- Explain digital forensics and attack attribution processes
- Explain the impact of compliance frameworks on incident handling
- Describe the elements of cybersecurity incident response