

Cisco CCST Cybersecurity (100-160)

This entry-level Cisco Certified Support Technician (CCST) Cybersecurity training prepares entry-level cybersecurity professionals to operate, maintain, troubleshoot, and configure the Cisco devices and software that keep devices and networks secure. This course prepares you for the CCST Cybersecurity exam, which is needed to earn your CCST Cybersecurity certification from Cisco.

[CBT Nuggets course material](#) →

WEEK 1

Essential Security Principles

152 min.

Vulnerabilities	12
Types of Vulnerabilities	13
Exploits, Risks, and Threats	11
Attack Vectors and Defense-in-Depth	9
Types of Attackers and Code of Ethics	8
Reasons for Attacks	4
Validation	5

Common Threats and Vulnerabilities

Types of Malware	20
Symptoms of Malware	11
Common Attacks Part 1	13
Common Attacks Part 2	6
Password Attacks	6
Social Engineering Attacks	8
Validation	5

Access Management Principles

Authentication	10
Authorization and Accounting	11

WEEK 2

156 min.

Password Management	18
National Institute of Standards and Technology (NIST) Recommendations	7
RADIUS	6
Validation	7

States of Data and Appropriate Encryption

What is Encryption?	8
Encryption of Data at Rest	15
Encryption of Data in Transit	10
Data in Use	9
Validation	6

Types of Encryption, Protocols that Use Encryption

Symmetric Encryption	19
Asymmetric Encryption	10
Summary of Algorithms	10
Hashing Data	14
Validation	5

TCP/IP Protocol Vulnerabilities

The TCP Protocol	12
------------------	----

WEEK 3

162 min.

The IP Protocol	1
Protocol Vulnerabilities	18
UDP and Additional Protocols	12
Validation	1

Network Addresses and Security

Introduction	1
Understanding Binary and Decimal Notation	9
Calculate a Subnet Mask Result	9
Understanding Switch and Router Functions	9
Public vs Private Addresses	9

Network Address Translation	5
IPv6 Addressing	6
Validation	4

Describe Network Infrastructure and Technologies

Network Architecture Requirements	1
Network Architecture: Fault Tolerance	8
Network Architecture: Scalability	5
Network Architecture: QoS, Security	13
DMZ and Proxy	8
Honeypot	3
Virtualization Overview	10
Virtualization Demo	8
Your Invisible Friend: The Cloud	7
Explore the Cloud	15

WEEK 4

152 min.

Validation	1
------------	---

Set Up a Secure Wireless SoHo Network

SoHo Introduction	2
Device Requirements	8
Purpose and Availability Requirements	7
Wireless Bands and Channels	12
Wireless Protocols	7
Elements of a SoHo Network	10
Configure a Wireless SoHo Network	22
Validation	1

Implement Secure Access Technologies

Introduction	1
Access Control List Overview	5
ACL Implementations	5
ACL Demonstration	10
Firewall Essentials	5
Other Firewall Types	7
Network Access Control (NAC)	18
Virtual Private Network (VPN)	7
Validation	1

The Windows Interface, File System, & Command Line

Windows Installed Base and Support	9
The Windows User Interface	14

WEEK 5

152 min.

The Windows File System	11
Implement the Command Line	18
Validation	6

Secure the Windows OS with Defender and Firewall

Microsoft Defender Overview	6
Microsoft Defender Demonstration	15
Windows Host-Based Firewall	20
Validation	12

PowerShell and CLI for Linux and macOS

Introduction to PowerShell	15
PowerShell Examples	8

Introduction to Linux	4
Linux Terminal Overview	5
Bash File Management Commands	16
Network Commands	11
Linux Programs from the CLI	5

WEEK 6

161 min.

Validation	1
------------	---

File Permissions, macOS and Linux Firewalls

Windows File and Directory Permissions	13
Linux and macOS File and Directory Permissions	10
Configure macOS Firewall	9
Configure Linux Firewall	9
Validation	13

Security Systems and Asset Management

Hardware Inventory	13
Using Intune to Track Assets	4
Manage Software	8
Manage an Android Device	9
Configuration Management	8
Configuration Management with Configuration Profile	4
Validation	4

Regulatory Compliance and Backups

Introduction	1
Regulatory Compliance: GDPR	1

Regulatory Compliance - PCI DSS	3
Regulatory Compliance: HIPPA	9
Backup Purpose	12
Backup Media, Types, and Frequency	10
Backup Products	9
Validation	11

WEEK 7

Implement Software and Hardware Updates **151 min.**

Types of Windows Updates	14
Client-Side Windows Update Settings	13
Windows Server Update Services (WSUS)	7
Updates via Intune	9
Software, Driver, and Firmware Updates	12
Validation	2

Interpret System Logs

Event Viewer Overview	1
Manage Event Viewer	11
Event Viewer Examples	5
Event Viewer Tools	5
Syslog	5
Validation	9

Linux and macOS Antimalware, Handling Malware

Does Linux Need Antimalware?	8
Linux Targets	8
Linux Attacks: Ransomware and Cryptojacking	4
Linux Attacks: State-Sponsored, File-less, and IoT	7

macOS and Security	9
XProtect in Action	3
Scan Logs and Malware Remediation	8
Validation	11

WEEK 8

Vulnerability Management **154 min.**

Intro	1
OS and Network Vulnerabilities	4
Common Vulnerabilities and Exposure (CVEs)	10
Scanning Networks Using Nmap and Zenmap	13
Managing Ubuntu Firewall Ports	10
Configuring SSH	5
Skill Validation	3

Compliance Frameworks

Introducing Compliance Frameworks	1
Complying With PCI DSS	10
Complying With HIPAA	3
Complying With FERPA	4
Complying With GDPR	6
Working With ISO 27001 and NIST Templates	13
Compliance Laws and Standards	1
Skill Validation	3

Risk Management

Intro	1
Vulnerability vs Risk	8
Determine Risk Rankings	9

Exploring Insider Risks Policies	16
Complete Policy Review	3
Skill Validation	1
Review	4

Incident Handling

Intro	1
SIEM vs SOAR	7
NIST SP 800-61	6
Exploring Azure Sentinel	11

WEEK 9

20 min.

Tactics and Techniques	14
Skill Validation	1
Validation Questions	1
Question Review	4