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 →

STUDY PLAN

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

The Windows Interface, File System, & Command Line

WEEK 5 — **152 min.**

Secure the Windows OS with Defender and Firewall

PowerShell and CLI for Linux and macOS

WEEK 6 — **161 min.**

File Permissions, macOS and Linux Firewalls

Security Systems and Asset Management

Regulatory Compliance and Backups

WEEK 7 Implement Software and Hardware Updates 151 min.

Interpret System Logs

Linux and macOS Antimalware, Handling Malware

WEEK 8 Vulnerability Management 154 min.

Compliance Frameworks

Risk Management

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