

OUR LEARNING EXCLUSIVE

- Custom exam prep software and materials
- Exam delivery in the classroom, with a **98% success rate**
- Course-specific thinQtank® Learning publications to keep the learning engaging
- Extended hours of training, including immersive hands-on exercises
- **We do not teach the test.** We always deliver valuable hands-on experience
- All reading material and study guides sent to you when you register
- Every course taught by certified instructors

TRAINING CAMP FORMAT

thinQtank® Learning delivers this course as an **instructor-led training camp**, with the exam sat in the classroom as part of the camp. Camps are scheduled by cohort rather than to a fixed calendar, and the balance of lecture and lab work is set to suit the group and the delivery method. Contact us for the schedule covering your dates.

PREREQUISITES

- **None.** Cisco sets no prerequisites for CCST — no prior certification, no minimum education, no required training
- Basic familiarity with computers and networks helps, but the course does not assume it
- Cisco suggests roughly 120 hours of study here against 70 for CCST Networking — this is the deeper of the two

TARGET AUDIENCE

- Career changers moving into security, who need a credential and a vocabulary
- Help desk and Tier 1 staff who are already first to see an incident
- Network and desktop technicians whose remit now includes security
- Students and school leavers aiming at a cybersecurity technician or analyst role
- Anyone planning CyberOps Associate who wants the fundamentals solid first

EXAM

100-160 — Cisco Certified Support Technician (CCST) Cybersecurity

Fifty minutes. **No prerequisites** — no prior certification, no minimum education, no required training.

Five topic areas, listed as the five course modules overleaf. **Cisco does not publish a question count, a passing score or domain weightings for this exam**, so we do not quote any.

Know the term before you sit it. A CCST earned on or after 15 July 2025 is valid for five years; one earned before that date does not expire. You recertify by passing any CCST, associate, professional or expert Cisco exam — so going on to CyberOps Associate renews this one as a side effect.

COURSE OVERVIEW

thinQtank® Learning offers an industry-unique training camp in which students earn the **Cisco Certified Support Technician (CCST) Cybersecurity** certification. As with all our Cisco training experiences, the exam is delivered in the classroom.

CCST Cybersecurity is where a security career starts. The principles the whole field rests on, the threats and attacks you will actually meet, how access and cryptography work, how a network and an endpoint are defended, how to assess a vulnerability and weigh the risk it carries — and what to do in the first hour of an incident. Cisco sets no prerequisites.

It is a credential in its own right and the first rung of Cisco's security ladder — the step before CyberOps Associate. Exam **100-160**, and the **voucher is available** at \$125 USD.

COURSE OBJECTIVES

Primary course objectives:

- Apply the essential security principles the field rests on — confidentiality, integrity and availability, in terms of real decisions
- Recognize common threats, attacks and vulnerabilities, and how each one works
- Explain access management: authentication, authorization and accounting
- Use cryptography correctly — what to encrypt, what to hash, and why
- Describe networking, addressing and the TCP/IP protocols from a security standpoint
- Identify the security role of each piece of network infrastructure
- Control network access, and explain what a firewall, VPN or NAC actually enforces
- Secure a small office or home office wireless network properly
- Use operating system tools to inspect and harden an endpoint
- Apply endpoint policies and standards, and explain why they exist
- Detect and remediate malware on a network and on an endpoint
- Run a vulnerability assessment and interpret what it returns
- Weigh and prioritize risk, rather than treating every finding as urgent
- Use threat intelligence to anticipate rather than react
- Explain disaster recovery and business continuity at a technician level
- Work an incident through detection, containment, eradication and recovery

WHAT YOU WILL BE ABLE TO DO

- Use the vocabulary of security correctly, in a room where it matters
- Recognize a threat or attack for what it is, and name the control that answers it
- Assess a vulnerability, score the risk, and say what should be done first
- Work an incident through its stages instead of reacting to it

DELIVERY METHODS

- Instructor-led training
- Immersive live-online training
- On-site and custom delivery

EXCLUSIVE LEARNING PACKAGE

- Hands-on labs on real network and endpoint kit
- Guided attack-and-defend exercises — see the threat, then answer it
- Vulnerability scanning and risk-scoring practice against systems we stand up
- Incident handling walk-throughs, run end to end
- CCST Cybersecurity video course
- CCST Cybersecurity reading plan and review guide
- CCST Cybersecurity certification practice exam

COURSE MODULES

01 Essential Security Principles

- Topic A: Security principles, and confidentiality, integrity and availability
- Topic B: Common threats, attacks and vulnerabilities
- Topic C: Access management — authentication, authorization, accounting
- Topic D: Cryptography, and what it is actually for
- Topic E: Security ethics, laws and regulations a technician meets

02 Basic Network Security Concepts

- Topic A: Networking, addressing and TCP/IP from a security standpoint
- Topic B: Network infrastructure and the security role of each device
- Topic C: Controlling network access — firewalls, VPNs and NAC
- Topic D: Secure protocols, and the insecure ones they replaced
- Topic E: Wireless SOHO security, done properly

03 Endpoint Security Concepts

- Topic A: Operating systems, and the tools that come with them
- Topic B: Hardening an endpoint
- Topic C: Endpoint policies and standards
- Topic D: Malware detection and remediation, network and endpoint
- Topic E: Logging, and knowing what a log is telling you

04 Vulnerability Assessment and Risk Management

- Topic A: Running a vulnerability assessment
- Topic B: Reading a scan result without panicking
- Topic C: Risk management — weighing, scoring and prioritizing
- Topic D: Threat intelligence, and using it to anticipate
- Topic E: Disaster recovery and business continuity

05 Incident Handling

- Topic A: The stages of incident handling
- Topic B: Detection and initial triage
- Topic C: Containment, eradication and recovery
- Topic D: Evidence, chain of custody and what not to touch
- Topic E: Post-incident review, and knowing when to escalate

WHERE THIS LEADS

- **CyberOps Associate** — the associate-level certification this course is the ground for, and the one Cisco names as the next step
- **A security role you can actually get.** Cybersecurity technician, cybersecurity analyst, Tier 1 help desk — the jobs CCST Cybersecurity was built for
- **CCST Networking** if the network security module is the one that caught your attention and you want the plumbing underneath it
- **Recertification handled by moving forward.** Passing any CCST, associate, professional or expert Cisco exam renews this certification, so the next course you take also keeps this one current
- **Ask us about the path.** We will map the next two certifications to the role you are aiming at, not to a catalog

TERMS

© 2026 thinQtank® Global, Inc. All rights reserved. The product or learning materials are protected by U.S. and intellectual property laws. thinQtank Global, thinQtank Learning and the Q-Man logo are registered trademarks of thinQtank Global, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

thinQtank Global, Inc. warrants that it will perform these training services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY THINQTANK GLOBAL, INC., OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. THINQTANK GLOBAL, INC. WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this training are copyrighted by thinQtank Global, Inc. ("Learning Materials"). thinQtank Global, Inc. grants the customer of this learning a license to use Learning Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of the technology covered herein. Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this training.