

# CCST

Cisco® Certified  
Support Technician

# STUDY GUIDE

**CYBERSECURITY EXAM**

Includes one year of FREE access after activation to the  
interactive online learning environment and study tools:

**Custom practice exam**

**100 electronic flashcards**

**Searchable key term glossary**

TODD LAMMLE  
JON BUHAGIAR  
DONALD ROBB  
TODD MONTGOMERY

 **SYBEX**  
A Wiley Brand



# CCST

## Cisco<sup>®</sup> Certified Support Technician

### Study Guide

### Cybersecurity Exam



Todd Lammle  
Jon Buhagiar  
Donald Robb  
Todd Montgomery

 **SYBEX<sup>®</sup>**  
A Wiley Brand

Copyright © 2025 by John Wiley & Sons Inc. All rights reserved, including rights for text and data mining and training of artificial intelligence technologies or similar technologies.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.  
Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at [www.copyright.com](http://www.copyright.com). Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

The manufacturer's authorized representative according to the EU General Product Safety Regulation is Wiley-VCH GmbH, Boschstr. 12, 69469 Weinheim, Germany, e-mail: [Product\\_Safety@wiley.com](mailto:Product_Safety@wiley.com).

Trademarks: Wiley and the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

**Limit of Liability/Disclaimer of Warranty:** While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002. For product technical support, you can find answers to frequently asked questions or reach us via live chat at <https://sybexsupport.wiley.com>.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at [www.wiley.com](http://www.wiley.com).

*Library of Congress Control Number applied for:*

Paperback ISBN: 9781394207350  
ePDF ISBN: 9781394207374  
ePub ISBN: 9781394207367

Cover Image: © Jeremy Woodhouse/Getty Images  
Cover Design: Wiley



# Contents at a Glance

<i>Acknowledgments</i>		<i>xix</i>
<i>About the Authors</i>		<i>xxi</i>
<i>Introduction</i>		<i>xxiii</i>
<i>Assessment Test</i>		<i>xxxiii</i>
<i>Answer to Assessment Test</i>		<i>xxxviii</i>
<b>Chapter 1</b>	Security Concepts	1
<b>Chapter 2</b>	Network Security Devices	27
<b>Chapter 3</b>	IP, IPv6, and NAT	57
<b>Chapter 4</b>	Network Device Access	115
<b>Chapter 5</b>	Secure Access Technology	143
<b>Chapter 6</b>	OS Basics and Security	179
<b>Chapter 7</b>	Endpoint Security	225
<b>Chapter 8</b>	Risk Management	265
<b>Chapter 9</b>	Vulnerability Management	293
<b>Chapter 10</b>	Disaster Recovery	327
<b>Chapter 11</b>	Incident Handling	357
<b>Chapter 12</b>	Digital Forensics	377
<b>Chapter 13</b>	Incident Response	391
<b>Appendix A</b>	Answers to Review Questions	417
<i>Index</i>		<i>439</i>



# Contents

<i>Acknowledgments</i>	<i>xix</i>	
<i>About the Authors</i>	<i>xxi</i>	
<i>Introduction</i>	<i>xxiii</i>	
<i>Assessment Test</i>	<i>xxxiii</i>	
<i>Answer to Assessment Test</i>	<i>xxxviii</i>	
<b>Chapter 1</b>	<b>Security Concepts</b>	<b>1</b>
	Technology-Based Attacks	2
	Denial of Service (DoS)/Distributed Denial of Service (DDoS)	3
	The Ping of Death	3
	Distributed DoS (DDoS)	3
	Botnet/Command and Control	3
	Traffic Spike	4
	Coordinated Attack	4
	Friendly/Unintentional DoS	4
	Physical Attack	5
	Permanent DoS	5
	Smurf	5
	SYN Flood	5
	Reflective/Amplified Attacks	7
	On-Path Attack (Previously Known as Man-in-the-Middle Attack)	8
	DNS Poisoning	8
	VLAN Hopping	9
	ARP Spoofing	10
	Rogue DHCP	10
	IoT Vulnerabilities	11
	Rogue Access Point (AP)	11
	Evil Twin	12
	Ransomware	12
	Password Attacks	12
	Brute-Force	13
	Dictionary	13
	Advanced Persistent Threat	13
	Hardening Techniques	13
	Changing Default Credentials	14
	Avoiding Common Passwords	14
	DHCP Snooping	14

Change Native VLAN	15
Patching and Updates	15
Upgrading Firmware	16
Defense in Depth	16
Social-Based Attacks	17
Social Engineering	17
Insider Threats	17
Phishing	18
Vishing	19
Smishing	20
Spear Phishing	20
Environmental	20
Tailgating	20
Piggybacking	21
Shoulder Surfing	21
Malware	21
Ransomware	21
Summary	22
Exam Essentials	23
Review Questions	24
<b>Chapter 2</b>	<b>Network Security Devices</b>
	<b>27</b>
Confidentiality, Integrity, and Availability (CIA)	28
Confidentiality	29
Integrity	29
Availability	29
Threats	29
Internal	29
External	30
Network Access Control	30
Posture Assessment	30
Guest Network	30
Persistent vs. Nonpersistent Agents	30
Honeypot	31
Wireless Networks	31
Wireless Personal Area Networks	31
Wireless Local Area Networks	32
Wireless Metro Area Networks	33
Wireless Wide Area Networks	33
Basic Wireless Devices	34
Wireless Access Points	34
Wireless Network Interface Card	36
Wireless Antennas	36

Wireless Principles	37
Independent Basic Service Set (Ad Hoc)	37
Basic Service Set	38
Infrastructure Basic Service Set	39
Service Set ID	40
Extended Service Set	40
Nonoverlapping Wi-Fi channels	42
2.4 GHz Band	42
5 GHz Band (802.11ac)	43
2.4 GHz / 5GHz (802.11n)	43
Wi-Fi 6 (802.11ax)	45
Interference	45
Range and Speed Comparisons	46
Wireless Security	46
Authentication and Encryption	46
WEP	48
WPA and WPA2: An Overview	48
Wi-Fi Protected Access	49
WPA2 Enterprise	49
802.11i	50
WPA3	50
WPA3-Personal	51
WPA3-Enterprise	51
Summary	52
Exam Essentials	53
Review Questions	54
<b>Chapter 3</b>	<b>57</b>
<b>IP, IPv6, and NAT</b>	<b>57</b>
TCP/IP and the DoD Model	58
The Process/Application Layer Protocols	60
Telnet	61
Secure Shell (SSH)	61
File Transfer Protocol (FTP)	62
Secure File Transfer Protocol (SFTP)	63
Trivial File Transfer Protocol (TFTP)	63
Simple Network Management Protocol (SNMP)	63
Hypertext Transfer Protocol (HTTP)	64
Hypertext Transfer Protocol Secure (HTTPS)	65
Network Time Protocol (NTP)	65
Domain Name Service (DNS)	65
Dynamic Host Configuration Protocol	
(DHCP)/Bootstrap Protocol (BootP)	66
Automatic Private IP Addressing (APIPA)	69

The Host-to-Host or Transport Layer Protocols	69
Transmission Control Protocol (TCP)	70
User Datagram Protocol (UDP)	72
Key Concepts of Host-to-Host Protocols	74
Port Numbers	74
The Internet Layer Protocols	78
Internet Protocol (IP)	79
Internet Control Message Protocol (ICMP)	82
Address Resolution Protocol (ARP)	85
IP Addressing	86
IP Terminology	86
The Hierarchical IP Addressing Scheme	87
Network Addressing	88
Class A Addresses	90
Class B Addresses	91
Class C Addresses	92
Private IP Addresses (RFC 1918)	92
IPv4 Address Types	93
Layer-2 Broadcasts	94
Layer-3 Broadcasts	94
Unicast Address	94
Multicast Address	95
When Do We Use NAT?	96
Types of Network Address Translation	98
NAT Names	99
How NAT Works	100
Why Do We Need IPv6?	101
IPv6 Addressing and Expressions	102
Shortened Expression	103
Address Types	104
Special Addresses	105
Summary	106
Exam Essentials	107
Review Questions	110
<b>Chapter 4</b>	<b>Network Device Access</b>
	<b>115</b>
Local Authentication	116
AAA Model	118
Authentication	118
Multifactor Authentication	119
Multifactor Authentication Methods	120

Authorization	122
Identity and Access Management	122
Least Privilege	123
Role-Based Access Control (RBAC)	123
Accounting	124
Common AAA Systems	125
Remote Authentication Dial-In User Service	125
Terminal Access Controller Access Control System Plus	126
Configuration of AAA	127
RADIUS Login Process	130
Password Policies	131
Account Lockout Policy	132
NAC Overview	133
802.1X	134
802.1X Components	134
NAC Process	135
Profiling	136
Posturing	136
Bring Your Own Device (BYOD)	136
Guest Network Isolation	137
Captive Portal	138
Summary	139
Exam Essentials	139

<b>Chapter 5</b>	<b>Secure Access Technology</b>	<b>143</b>
	Access Control Lists	144
	Standard Access Lists	147
	Wildcard Masking	148
	Extended Access Lists	150
	Firewalls	155
	Encryption	156
	Symmetrical Encryption Keys	158
	The Data Encryption Standard (DES)	158
	Triple Data Encryption Standard (3DES)	158
	The Advanced Encryption Standard (AES)	159
	Hashes	159
	MD5	159
	SHA	159
	Virtual Private Networks	160
	Benefits of VPNs	161
	Enterprise- and Provider-Managed VPNs	161
	Introduction to Cisco IOS IPsec	164

	IPsec Transforms	165
	Security Protocols	165
	Encryption	166
	GRE Tunnels	168
	GRE over IPsec	168
	Cisco DMVPN (Cisco Proprietary)	169
	Cisco IPsec VTI	169
	Public Key Infrastructure	169
	Certification Authorities	170
	Certificate Templates	172
	Certificates	172
	Summary	174
	Exam Essentials	174
	Review Questions	176
<b>Chapter 6</b>	<b>OS Basics and Security</b>	<b>179</b>
	Operating System Security	180
	Windows	180
	Windows Defender Firewall	180
	Scripting	184
	Security Considerations	190
	NTFS vs. Share Permissions	191
	Shared Files and Folders	195
	User Account Control	198
	Windows Update	202
	Application Patching	203
	Device Drivers	204
	macOS/Linux	204
	System Updates/App Store	206
	Patch Management	206
	Firewall	207
	Permissions	211
	Driver/Firmware Updates	213
	Operating System Life Cycle	214
	System Logs	214
	Event Viewer	214
	Audit Logs	215
	Syslog	216
	Syslog Collector	216
	Syslog Messages	217
	Logging Levels/Severity Levels	218
	Identifying Anomalies	218
	SIEM	220



	Summary	221
	Exam Essentials	221
	Review Questions	223
<b>Chapter 7</b>	<b>Endpoint Security</b>	<b>225</b>
	Endpoint Tools	226
	Command-Line Tools	226
	netstat	227
	nslookup	227
	dig	228
	ping	229
	tracert	229
	tcpdump	230
	nmap	231
	gpresult	232
	Software Tools	232
	Port Scanner	232
	iPerf	233
	IP Scanner	234
	Endpoint Security and Compliance	234
	Hardware Inventory	235
	Asset Management Systems	235
	Asset Tags	236
	Software Inventory	236
	Remediation	237
	Considerations	238
	Destruction and Disposal	238
	Low-Level Format vs. Standard Format	239
	Hard Drive Sanitation and Sanitation Methods	239
	Overwrite	240
	Drive Wipe	240
	Physical Destruction	241
	Data Backups	241
	Regulatory Compliance	243
	BYOD vs. Organization-Owned	243
	Mobile Device Management (MDM)	244
	Configuration Management	244
	App Distribution	245
	Data Encryption	245
	Endpoint Recovery	248
	Endpoint Protection	248

Cloud-Based Protection	250
Reviewing Scan Logs	250
Malware Remediation	254
Identify and Verify Malware Symptoms	254
Quarantine Infected Systems	254
Disable System Restore in Windows	255
Remediate Infected Systems	256
Schedule Scans and Run Updates	258
Enable System Restore and Create a	
Restore Point in Windows	260
Educate the End User	261
Summary	261
Exam Essentials	261
Review Questions	263

**Chapter 8 Risk Management 265**

Risk Management	266
Elements of Risk	267
Vulnerabilities	269
Threats	270
Exploits	270
Assets	270
Risk Analysis	271
Risk Levels	272
Risk Matrix	272
Risk Prioritization	274
Data Classifications	275
Risk Mitigation	277
Introduction	278
Strategic Response	279
Action Plan	279
Implementation and Tracking	280
Security Assessments	281
Vulnerability Assessment	281
Penetration Testing	282
Posture Assessment	282
Change Management Best Practices	283
Documented Business Processes	284
Change Rollback Plan (Backout Plan)	284
Sandbox Testing	284
Responsible Staff Member	285
Request Forms	285
Purpose of Change	286

Scope of Change	286
Risk Review	287
Plan for Change	287
Change Board	288
User Acceptance	289
Summary	289
Exam Essentials	290
Review Questions	291

**Chapter 9 Vulnerability Management 293**

Vulnerabilities	294
Vulnerability Identification	294
Management	295
Mitigation	297
Active and Passive Reconnaissance	298
Port Scanning	298
Vulnerability Scanning	299
Packet Sniffing/Network Traffic Analysis	300
Brute-Force Attacks	301
Open-Source Intelligence (OSINT)	302
DNS Enumeration	302
Social Engineering	303
Testing	304
Port Scanning	304
Automation	304
Threat Intelligence	305
Vulnerability Databases	308
Limitations	309
Assessment Tools	310
Recommendations	312
Reports	314
Security Reports	314
Cybersecurity News	314
Subscription-based	315
Documentation	316
Updating Documentation	316
Security Incident Documentation	317
Documenting the Incident	318
Following the Right Chain of Custody	319
Securing and Sharing of Documentation	319
Reporting the Incident	320
Recovering from the Incident	321
Documenting the Incident	321

	Reviewing the Incident	321
	Documentation Best Practices for Incident Response	322
	Summary	322
	Exam Essentials	323
	Review Questions	324
<b>Chapter 10</b>	<b>Disaster Recovery</b>	<b>327</b>
	Disaster Prevention and Recovery	328
	Data Loss	329
	File Level Backups	329
	Image-Based Backups	332
	Critical Applications	332
	Network Device Backup/Restore	332
	Data Restoration Characteristics	333
	Backup Media	333
	Backup Methods	335
	Backup Testing	336
	Account Recovery Options	336
	Online Accounts	336
	Local Accounts	336
	Domain Accounts	337
	Facilities and Infrastructure Support	338
	Battery Backup/UPS	338
	Power Generators	339
	Surge Protection	339
	HVAC	340
	Fire Suppression	342
	Redundancy and High Availability	
	Concepts	343
	Switch Clustering	343
	Routers	344
	Firewalls	345
	Servers	345
	Disaster Recovery Sites	345
	Cold Site	345
	Warm Site	346
	Hot Site	346
	Cloud Site	346
	Active/Active vs. Active/Passive	346
	Multiple Internet Service Providers/Diverse Paths	347
	Testing	348
	Tabletop Exercises	349
	Validation Tests	349

	Disaster Recovery Plan	350
	Business Continuity Plan	352
	Summary	352
	Exam Essentials	353
	Review Questions	354
<b>Chapter 11</b>	<b>Incident Handling</b>	<b>357</b>
	Security Monitoring	358
	Security Information and Event Management (SIEM)	359
	Hosting Model	359
	Detection Methods	359
	Integration	360
	Cost	360
	Security Orchestration, Automation, and Response (SOAR)	361
	Orchestration vs. Automation	362
	Regulations and Compliance	362
	Common Regulations	363
	Data locality	363
	Family Educational Rights and Privacy Act (FERPA)	364
	Federal Information Security Modernization Act (FISMA)	365
	Gramm–Leach–Bliley Act	366
	General Data Protection Regulation (GDPR)	368
	Health Insurance Portability and Accountability Act	369
	Payment Card Industry Data Security Standard (PCI-DSS)	370
	Reporting	371
	Notifications	372
	Summary	372
	Exam Essentials	373
	Review Questions	374
<b>Chapter 12</b>	<b>Digital Forensics</b>	<b>377</b>
	Introduction	378
	Forensic Incident Response	378
	Attack Attribution	379
	Cyber Kill Chain	380
	MITRE ATT&CK Matrix	381
	Diamond Model	382
	Tactics, Techniques, and Procedures	383
	Artifacts and Sources of Evidence	383
	Evidence Handling	384
	Preserving Digital Evidence	384
	Chain of Custody	385

	Summary	385
	Exam Essentials	387
	Review Questions	388
<b>Chapter 13</b>	<b>Incident Response</b>	<b>391</b>
	Incident Handling	392
	What Are Security Incidents?	393
	Ransomware	393
	Social Engineering	393
	Phishing	393
	DDoS Attacks	394
	Supply Chain Attacks	394
	Insider Threats	394
	Incident Response Planning	394
	Incident Response Plans	394
	Incident Response Frameworks	395
	Incident Preparation	396
	Risk Assessments	397
	Detection and Analysis	397
	Containment	397
	Eradication	397
	Recovery	398
	Post-incident Review	398
	Lessons Learned	398
	Creating an Incident Response Policy	399
	Document How You Plan to Share Information with	
	Outside Parties	400
	Interfacing with Law Enforcement	401
	Incident Reporting Organizations	401
	Handling an Incident	401
	Preparation	401
	Preventing Incidents	403
	Detection and Analysis	404
	Attack Vectors	404
	Signs of an Incident	405
	Precursor and Indicator Sources	406
	Containment, Eradication, and Recovery	406
	Choosing a Containment Strategy	406
	Evidence Gathering and Handling	407
	Attack Sources	409
	Eradication and Recovery	409

	Post-incident Activity	410
	Using Collected Incident Data	411
	Evidence Retention	412
	Summary	412
	Exam Essentials	412
	Review Questions	414
<b>Appendix A</b>	<b>Answers to Review Questions</b>	<b>417</b>
	Chapter 1: Security Concepts	418
	Chapter 2: Network Security Devices	419
	Chapter 3: IP, IPv6, and NAT	420
	Chapter 4: Network Device Access	422
	Chapter 5: Secure Access Technology	424
	Chapter 6: OS Basics and Security	425
	Chapter 7: Endpoint Security	426
	Chapter 8: Risk Management	428
	Chapter 9: Vulnerability Management	429
	Chapter 10: Disaster Recovery	431
	Chapter 11: Incident Handling	432
	Chapter 12: Digital Forensics	434
	Chapter 13: Incident Response	435
<i>Index</i>		439





# Acknowledgments

There were many people who helped us build the new Cisco certification books in 2023 and 2024. First, Kenyon Brown helped us put together the direction for the books and managed the internal editing at Wiley, so thank you, Ken. Kim Wimpsett was the development editor and worked diligently for many months keeping these books moving along.

We also thank content refinement specialist Sowmini Durairaj, the copyeditor Lori Martinsek, the proofreader Tiffany Taylor, and the indexer Tom Dinse.



# About the Authors

**Todd Lammler** is the authority on Cisco certification and internetworking and is Cisco certified in most Cisco certification categories. He is a world-renowned author, speaker, trainer, and consultant. Todd has three decades of experience working with LANs, WANs, and large enterprise licensed and unlicensed wireless networks, and lately he's been implementing large Cisco Security networks using Firepower/FTD and ISE.

His years of real-world experience are evident in his writing; he is not just an author but an experienced networking engineer with very practical experience from working on the largest networks in the world, at such companies as Xerox, Hughes Aircraft, Texaco, AAA, Cisco, and Toshiba, among many others.

Todd has published over 130 books, including the very popular *CCNA: Cisco Certified Network Associate Study Guide*, *CCNA Wireless Study Guide*, *CCNA Data Center Study Guide*, and *CCNP Security*—among over a hundred more—all from Sybex. He runs an international consulting and training company based in northern Idaho where he spends his free time in the mountains playing with his golden retrievers.

You can reach Todd through his website at [www.lammler.com](http://www.lammler.com).

**Jon Buhagiar**, BS/ITM, MCSE, CCNA, is an information technology professional with two decades of experience in higher education and the private sector.

Jon currently serves as supervisor of network operations and is currently the director of information technology at RareMed Solutions, Pittsburgh Technical College. In this his role, he manages projects related to the IT infrastructure and cloud services that serve multiple pharmacies operated by RareMed Solutions. In addition, he is responsible for the technology that support hundreds of care specialists that raise the quality of life for many patients all over the world.

He was previously the supervisor of network operations at Pittsburgh Technical College, where he managed the data center, network infrastructure operations, and IT operations and was involved in the management of projects supporting the quality of education at the College. He also served as an adjunct instructor in the College's School of Information Technology department, where he has taught courses for Microsoft and Cisco certification. Jon has been an instructor for 20+ years at several colleges in the Pittsburgh area, since the introduction of the Windows NT MCSE in 1998.

Jon earned a bachelor of science degree in information technology management from Western Governors University. He also achieved an associate degree in business management from Pittsburgh Technical College. His most recent certifications include Windows Server 2016 Microsoft Certified Solutions Expert (MCSE) and Cisco Certified Network Associate (CCNA). Other certifications include CompTIA Network+, CompTIA A+, and CompTIA Project+.

In addition to his professional and teaching roles, Jon has authored many books with Wiley Sybex over the past 10 years, including the Second Edition *CCNA Certification Practice Tests 200-301* (Sybex 2023) *Comp-TIA Network+ Study Guide: Exam N10-009* (Sybex Study Guide), along with Todd Lammler (Sybex 2024). Jon has spoken at several

conferences about spam and email systems. He is an active radio electronics hobbyist and has held a ham radio license for the past 20 years, KB3KGS. He experiments with electronics and has a strong focus on the Internet of Things (IoT).

**Donald Robb**, widely recognized online as “The Packet Thrower,” brings over two decades of experience in the IT industry. His career has spanned a diverse array of roles, beginning with help desk support and evolving into a position as one of the most respected consultants in the field. Donald has honed expert-level skills across various IT domains, including networking, security, collaboration, data center management, wireless technologies, and service providers. His depth of knowledge and technical expertise have made him a sought-after professional in the industry.

Currently, Donald is a principal network architect for Walt Disney Studios. In this role, he serves as a subject matter expert on various technologies, playing a critical role in shaping the company’s network architecture and ensuring its reliability and performance. His work involves leading the design and implementation of complex networks and guiding teams and stakeholders through the technical intricacies of modern IT infrastructures.

Over the years, Donald has collaborated with major industry vendors and smaller, specialized companies, earning many advanced certifications along the way. His achievements include becoming a double JNCIE and obtaining most of Cisco’s professional-level certifications, demonstrating his deep technical proficiency and commitment to continuous learning. His expertise has also been recognized through his selection as a Cisco Champion for four consecutive years, an honor awarded to top influencers in the networking community.

In addition to his hands-on work in the field, Donald has made significant contributions to IT education. He has had the privilege of working alongside Todd Lammle, a legendary figure in the IT world, coauthoring several books and developing courses that have helped countless professionals advance their careers. Through his extensive experience, certifications, and educational efforts, Donald Robb has solidified his reputation as a leading authority in the IT industry.

**Todd Montgomery** has been in the networking industry for more than 40 years. Todd holds many Cisco, AWS, CompTIA, and Juniper certifications. Todd has spent most of his career in the field working on-site in data centers throughout North America and around the world.

He has worked on the most advanced networks of equipment manufacturers, systems integrators, and end users in the data center and cloud computing environments of the private sector, service providers, and the government sector. Todd most recently worked as a data center network automation engineer in Austin, Texas, involved in network implementation and support of emerging data center technologies and AWS public cloud services.

# Introduction

Welcome to the exciting world of security and your path toward Cisco certification. If you've picked up this book because you want to improve yourself and your life with a better, more satisfying, and secure job, you've chosen well!

Whether you're striving to enter the thriving, dynamic security sector or seeking to enhance your skill set and advance your position within it, being Cisco certified can seriously stack the odds in your favor to help you attain your goals. This book is a great start.

Cisco certifications are powerful instruments of success that also markedly improve your grasp of all things internetworking. As you progress through this book, you'll gain a strong, foundational understanding of security that reaches far beyond Cisco devices. And when you finish this book, you'll be ready to tackle the next step toward Cisco certification.

Essentially, by beginning your journey toward becoming Cisco certified, you're proudly announcing that you want to become an unrivaled security expert, a goal that this book will help get you underway to achieving.

Congratulations in advance for taking the first step toward your brilliant future!



---

To find your included bonus material, as well as additional Todd Lammle videos, and extra practice questions, please see [www.lammle.com/ccst](http://www.lammle.com/ccst).

## Cisco's CCST Certifications

It used to be that to secure the holy grail of Cisco certifications—the CCIE—you passed only one written test before being faced with a grueling, formidable hands-on lab. This intensely daunting, all-or-nothing approach made it nearly impossible to succeed and predictably didn't work out too well for most people.

Cisco responded to this issue by creating a series of new certifications, which not only created a sensible, stepping-stone-path to the highly coveted CCIE prize, but it also gave employers a way to accurately rate and measure the skill levels of prospective and current employees.

The CCNA and CCNP exams were then created as a stepping stone, and they are still the most popular certifications in the world. This exciting paradigm shift in Cisco's certification path truly opened doors that few were allowed through before!

Now Cisco has reached down and created a new introduction level certification program, below the CCNA, called the Cisco Certified Support Technician (CCST). There are two exams, two certs, called Network and Cybersecurity.

CCST Networking certification validates an individual's skills and knowledge of entry-level networking concepts and topics. The certification demonstrates foundational

knowledge and skills needed to show how networks operate, including the devices, media, and protocols that enable network communications.

The Cisco Certified Support Technician (CCST) Networking certification is also a first step toward working on achieving your CCNA Certification.

The Cisco Certified Support Technician (CCST) Cybersecurity certification validates a candidate's skills and knowledge of entry-level cybersecurity concepts and topics, including security principles, network security and endpoint security concepts, vulnerability assessment and risk management, and incident handling.

The Cisco Certified Support Technician (CCST) Cybersecurity certification is also a first step toward CyberOps Associate certification.

This book is a powerful tool to get you started in your Cisco certification studies, and it's vital to understand that material in it before you go on to conquer any other certifications!



Exam policies can change from time to time. We highly recommend that you check both the Cisco and Pearson VUE sites for the most up-to-date information when you begin your preparation, when you register, and again a few days before your scheduled exam date.

## Tips for Taking the CCST Cybersecurity Exam

Here are some general tips for taking your exam successfully (assuming you are going in person as online testing is available as well):

- This is not like the CCNA or other Cisco certification tests that are available on [www.vue.com](http://www.vue.com). You need to instead go to <https://www.certipoint.com/locator> to both register and pay for your exam. You can take the exams in person at a center, or in your home or office, under direct video and audio supervision. For exams at home information and to sign up, call (800) 589-6871.
- Bring two forms of ID with you. One must be a photo ID, such as a driver's license. The other can be a major credit card or a passport. Both forms must include a signature.
- Arrive early at the exam center so you can relax and review your study materials, particularly tables and lists of exam-related information. After you are ready to enter the testing room, you will need to leave everything outside; you won't be able to bring any materials into the testing area.
- Read the questions carefully. Don't be tempted to jump to an early conclusion. Make sure you know exactly what each question is asking.
- Don't leave any unanswered questions. Unanswered questions are scored against you. There will be questions with multiple correct responses. When there is more than one correct answer, a message at the bottom of the screen will prompt you to either "choose two" or "choose all that apply." Be sure to read the messages displayed to know how many correct answers you must choose.

- When answering multiple-choice questions you're not sure about, use a process of elimination to get rid of the obviously incorrect answers first. Doing so will improve your odds if you need to make an educated guess.

## Who Should Read This Book?

You—if want to pass the CCST Cybersecurity exam and pass it confidently! This book is chock-full of the exact information you need and directly maps to CCST Cybersecurity exam objectives, so if you use it to study for the exam, your odds of passing shoot way up.

And in addition to including every bit of knowledge you need to learn to pass the exam, We have included some really great tips and solid wisdom throughout the chapters, to equip you even further to successfully work in the real IT security world.

## What's Included in the Book

We have included several study tools throughout the book:

**Assessment Test** At the end of this introduction is an assessment test that you can use to check your readiness for the exam. Take this test before you start reading the book; it will help you determine the areas you might need to brush up on. The answers to the assessment test questions appear on a separate page after the last question of the test. Each answer includes an explanation and a note telling you the chapter in which the material appears.

**Objective Map and Opening List of Objectives** In this introduction you'll find a detailed exam objective map showing you where each of the exam objectives is covered in this book. In addition, each chapter opens with a list of the exam objectives it covers. Use these to see exactly where each of the exam topics is covered.

**Exam Essentials** Each chapter, just after the summary, includes a number of exam essentials. These are the key topics you should take from the chapter in terms of areas to focus on when preparing for the exam.

**Chapter Review Questions** To test your knowledge as you progress through the book, there are review questions at the end of each chapter. As you finish each chapter, answer the review questions, and then check your answers—the correct answers and explanations are in the Appendix. You can go back to reread the section that deals with each question you got wrong to ensure that you correctly answer the next time you're tested on the material.

## Interactive Online Learning Environment and Test Bank

The interactive online learning environment that accompanies CCST Cybersecurity provides a test bank with study tools to help you prepare for the certification exam—and increase your chances of passing it the first time! The test bank includes the following tools:

**Sample Tests** All of the questions in this book are provided, including the assessment test, which you'll find at the end of this introduction, and the chapter tests that include the review questions at the end of each chapter. In addition, there is a practice exam. Use these questions to test your knowledge of the study guide material. The online test bank runs on multiple devices.

**Flashcards** Approximately 100 questions are provided in digital flashcard format (a question followed by a single correct answer). You can use the flashcards to reinforce your learning and provide last-minute test prep before the exam.

**Other Study Tools** A glossary of key terms from this book and their definitions are available as a fully searchable PDF.



Go to <http://www.wiley.com/go/sybextestprep> to register and gain access to this interactive online learning environment and test bank with study tools.

## How to Use This Book

If you want a solid foundation for the serious effort of preparing for the Cisco CCST Cybersecurity exam, then look no further because we have spent countless hours putting together this book with the sole intention of helping you pass it!

This book is loaded with valuable information, and you will get the most out of your study time if you understand how I put the book together. Here's a list that describes how to approach studying:

1. Take the assessment test immediately following this introduction. (The answers are at the end of the test, but no peeking!) It's okay if you don't know any of the answers—that's what this book is for. Carefully read over the explanations for any question you get wrong and make note of the chapters where that material is covered.
2. Study each chapter carefully, making sure you fully understand the information and the exam objectives listed at the beginning of each one. Again, pay extra-close attention to any chapter that includes material covered in questions you missed on the assessment test.
3. Answer all the review questions related to each chapter. Specifically note any questions that confuse you and study the corresponding sections of the book again. And don't just skim these questions—make sure you understand each answer completely.
4. Before you take your test, be sure to visit my website for questions, videos, audios, and other useful information.
5. Test yourself using all the electronic flashcards. This is a brand-new and updated flashcard program to help you prepare for the latest Cisco CCST Cybersecurity exam, and it is a great study tool.



I tell you no lies—learning every bit of the material in this book is going to require applying yourself with a good measure of discipline. So try to set aside the same time period every day to study, and select a comfortable and quiet place to do so. If you work hard, you will be surprised at how quickly you learn this material.

## What Does This Book Cover?

This book covers everything you need to know to solidly prepare you for getting into your CCST studies. Be advised that just because much of the material in this book won't be official Cisco CCST objectives in the future doesn't mean you won't be tested on it. Understanding the foundational, real-world cybersecurity information and skills offered in this book is critical to your certifications and your career!

So, as you move through this book, here's a snapshot of what you'll learn chapter by chapter:

**Chapter 1: Security Concepts** In this chapter you will begin learning basic security concepts. The security concepts include vulnerabilities, threats, exploits, as well as the difference between these concepts. You will then learn about common threats and vulnerabilities, such as malware, ransomware, and other common tactics.

**Chapter 2: Network Security Devices** This chapter will describe network infrastructure and technologies that support network security, such as virtualization, honeypots, intrusion detection systems (IDS), and many other devices.

**Chapter 3: Network Security Concepts** Chapter 3 will cover a lot of common network concepts that you would find in the CCST Networking certification. However, the concepts will be explained and highlighted as they pertain to network security.

**Chapter 4: Network Device Access** This chapter will explain the difference between authentication, authorization, and accounting (AAA) that is used with Remote Authentication Dial-In User Service (RADIUS), as well as multifactor authentication (MFA), and password policies.

**Chapter 5: Secure Access Technology** This chapter will cover the various technologies that allow you to secure communications over an insecure network, such as access control lists (ACLs), firewalls, Virtual Private Network (VPN) connections, and Network Access Control (NAC). Encryption types and the protocols that use them will also be covered.

**Chapter 6: OS Basics and Security** This chapter will focus on the various operating systems and their various security features, such as Windows Defender, host-based firewalls, and file and directory permissions. In addition this chapter will cover the importance of software and hardware updates. To round this topic of operating system security, system logs will be covered in entirety.

**Chapter 7: Endpoint Security** This Chapter will take a deep dive into endpoint security, such as the various built-in tools that can help us collect data. This chapter will also cover the basics of hardware and software inventory, program deployments, data backups, regulatory compliance, and bring your own device (BYOD) strategies.

**Chapter 8: Vulnerability Management** Chapter 8 will focus on risk management strategies, such as risk ranking, approaching risk management, risk mitigations strategies, risk associated with data types, and the levels of risk. In addition, this chapter will give you a fundamental understanding of how to identify risk and mitigate risk.

**Chapter 9: Vulnerability Management** This chapter explains the various ways that you can manage vulnerabilities in your organization, such as identification, management, and mitigation. Threat intelligence techniques are also covered that explain how the industry catalogs vulnerabilities, identifies trends, and mitigates vulnerabilities.

**Chapter 10: Disaster Recovery** This chapter explains disaster recovery for business continuity and recovery. The chapter will cover how disasters might happen, what to do when it happens and the planning around disasters to get your organization operating again.

**Chapter 11: Incident Handling** This chapter explains how security events are found with the help of Security Information and Event Management (SIEM) systems. The chapter will also explain the importance of security orchestration, automation, and response (SOAR) systems to help automate and orchestrate a remediation to an event. Common compliance frameworks for incident handling are also explained along with their reporting and notification requirements.

**Chapter 12: Digital Forensics** This chapter will explain digital forensics and the attack attribution processes. Some of the concepts covered will be Cyber Kill Chain, MITRE ATT&CK Matrix, and tactics, techniques, procedures (TTPS), as well as evidence and the proper handling of evidence.

**Chapter 13: Incident Response** The last chapter will describe the elements of a cybersecurity incidence response. This chapter will include the National Institute of Standards and Technology (NIST) standard for incident response, and how to implement a policy, plan, and the various procedural elements.

## Exam Objectives

Speaking of objectives, you're probably pretty curious about those, right? Cisco asked groups of IT professionals to fill out a survey rating the skills they felt were important in their jobs, and the results were grouped into objectives for the exam.

This is a list of objectives and which chapter the objectives are covered in. Remember that a single objective can be covered in multiple chapters.