CCNA Cybersecurity Certification Guide

Top Cisco resources to plan and prepare for certification

Get started

Table of contents

Cybersecurity certification overview: Your gateway to a career in cybersecurity

Unlock your career potential and drive success

Today, every organization needs security expertise to protect against threats, and the demand for skilled professionals is soaring. The cybersecurity field is projected to grow by 33% for information security analysts between 2023 and 2033,[1] with a 12% increase in cybersecurity job postings in the past year alone.[2] This high-energy field is where dedicated teams guard business-critical infrastructure, protect digital assets, and respond to attacks in real time.

How can you get started in this fast-growing career? Earn your CCNA Cybersecurity (Cybersecurity Associate) certification. It's from Cisco, a recognized leader in security solutions and certifications, and it validates the day-to-day, tactical knowledge and skills that Security Operations Center (SOC) teams need to detect and respond to cybersecurity threats.

This certification gives you a deep understanding of the fundamentals of cybersecurity operations and prepares you for associate-level job roles with SOC teams worldwide.

1 Occupational Outlook Handbook U.S. Bureau of Labor Statistics, April 25, 2025
https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
2 Cybersecurity jobs on the rise as US industries navigate economic uncertainty. World Economic Forum, June 25, 2025
https://www.weforum.org/stories/2025/06/cybersecurity-jobs-rise-us-industries-navigate-economic-uncertainty/

Unlock your career potential and drive success

The CCNA Cybersecurity (Cybersecurity Associate) certification might be the one for you if:

- You want to specialize in cybersecurity
- You like working in a high-stakes environment and responding to challenges in real time
- You can apply your analytical skills to stay a step ahead of cybercrime

Here are some job titles this certification can help prepare you for:

- Security Operations Center (SOC) analyst
- Cybersecurity engineer
- IT security operations specialist

The network needs you

The network is under constant assault—and it needs you.

Get started today

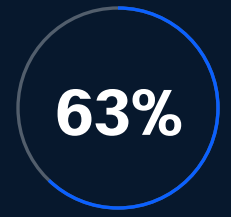
Why certify? Elevate your career.

Certifications are powerful catalysts for personal and professional growth, offering tangible benefits. According to the latest Pearson VUE 2025 Value of IT Certification Candidate report, certifications help to:

Boost your confidence and opportunities

of respondents have reported gaining confidence in their abilities to pursue new job opportunities.

Grow your career and salary



of certified professional respondents receive or anticipate promotions, 32% see salary increases, with 31% of those raises exceeding 20%.

Why Cisco? Build on excellence.

Cisco certifications are the recognized gold standard, bringing significant value to individuals and the organizations that employ them. And employers, including Fortune 500 companies, know it.

From entry to expert, Learn with Cisco is with you

Cisco best-in-class training helps you gain the skills employers are looking for. Our certifications are available in multiple levels of expertise and for various professional areas. Whether you're just starting out or advancing to expert level, Learn with Cisco is with you every step of the way in your entry-to-expert tech learning journey.

Highlight your accomplishments at every milestone

Our digital badges program, certificates of training completion, and certifications give you the tools to highlight your professional achievements every step of the way. Share on social, resumes, and digital profiles to prove the knowledge you've gained and stand out in the technologies of your choice.

Earn top salaries

Cisco certifications consistently rank among the highest-paying in the IT industry. The in-demand skills gained from these certifications in networking and security allow professionals to command top salaries.[1]

Source: [1]19th EDITION 2024-2025 IT Skills and Salary Report by Skillsoft

Certifications matter to employers

Skillsoft's Global Knowledge 2024 IT Skills and Salary Report examined data from thousands of IT professionals and confirmed that certified staff add value to an organization. In fact, 49% of IT decision-makers say that certified staff add value by closing organizational skill gaps and by spending less time on troubleshooting issues.

Certified professionals also see their added value:

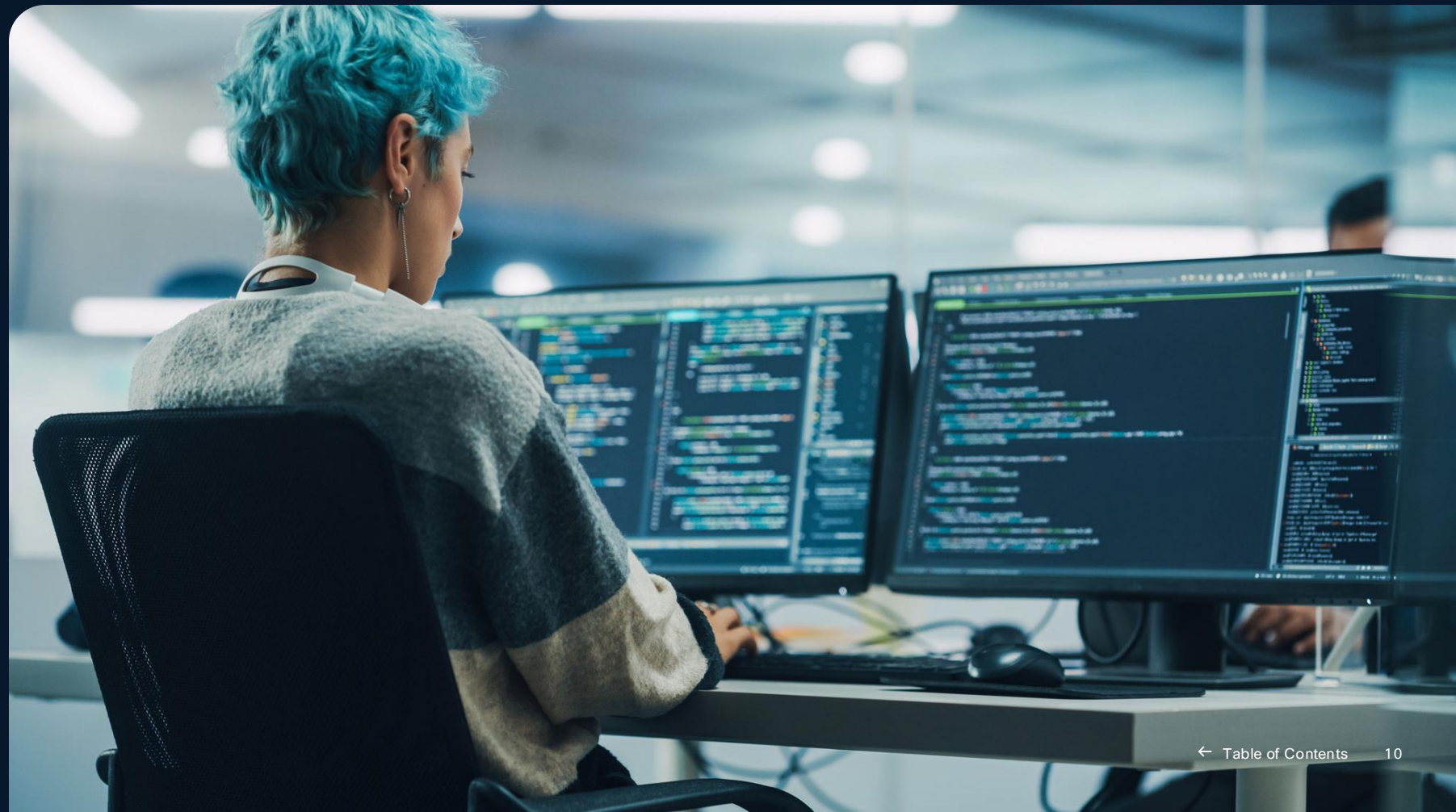
60% of certified professionals believe the quality of their work has improved

48% reported being more engaged in their work

43% are faster at performing their jobs

By choosing CCNA Cybersecurity, you become a highly valuable, innovative, and productive asset, securing your place in the industry and contributing directly to organizational success.

Cybersecurity Operations Fundamentals (CBROPS) exam study guide



Exam topics

Already decided to get certified, and want to get started? Exam topics are the best place to kickstart your studies. They tell you what to focus on, including how much weight is placed on each topic in the 200-201 CBROPS v1.2 Exam.

1.0 Security Concepts

1.1 Describe the CIA triad

1.2 Compare security deployments

1.3 Describe security terms

1.4 Compare security concepts

1.5 Describe the principles of the defense-in-depth strategy

1.6 Describe terms as defined in CVSS

1.7 Identify the challenges of data visibility (network, host, and cloud) in detection

1.8 Identify potential data loss from traffic profiles

1.9 Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs

1.10 Compare rule-based detection vs. behavioral and statistical detection

Exam topics

Walk through security monitoring. This domain is where you learn to see and respond to threats in a network. It's the core of a cybersecurity professional's job—identifying, analyzing, and mitigating attacks before they cause serious damage.

2.0 Security Monitoring

2.1 Compare attack surface and vulnerability

2.2 Identify the types of data provided by these technologies

2.3 Describe the impact of these technologies on data visibility

2.4 Describe the uses of these data types in security monitoring

2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle

2.6 Describe web application attacks, such as SQL injection, command injections, and cross-site scripting

2.7 Describe social engineering attacks

2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware

2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies

2.10 Describe the impact of certificates on security (includes PKI, public / private crossing the network, asymmetric / symmetric)

2.11 Identify the certificate components in a given scenario

Exam topics

This is where you walk through the forensics of a compromised system. You'll learn how to analyze the data on an individual device, from identifying malicious activity in system logs to interpreting the output of malware analysis tools.

20%

3.0 Host-based Analysis

3.1 Describe the functionality of these endpoint technologies in regard to security monitoring utilizing rules, signatures, and predictive AI

3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario

3.3 Describe the role of attribution in an investigation

3.4 Identify type of evidence used based on provided logs

3.5 Compare tampered and untampered disk image

3.6 Interpret operating system, application, or command line logs to identify an event

3.7 Interpret the output report of a malware analysis tool such as a detonation chamber or sandbox

Exam topics

Learn to analyze a variety of data sources, from raw network packets to filtered logs, to identify and investigate malicious activity. Put your detective skills to work, uncovering the story behind an attack as it unfolds across the network.

20%

4.0 Network Intrusion Analysis

4.1 Map the provided events to source technologies

4.2 Compare impact and no impact for these items

4.3 Compare deep packet inspection with packet filtering and stateful firewall operation

4.4 Compare inline traffic interrogation and taps or traffic monitoring

4.5 Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic

4.6 Extract files from a TCP stream when given a PCAP file and Wireshark

4.7 Identify key elements in an intrusion from a given PCAP file

4.8 Interpret the fields in protocol headers as related to intrusion analysis

4.9 Interpret common artifact elements from an event to identify an alert

4.10 Interpret basic regular expressions

Exam topics

This is the framework that guides an organization's response to an attack. You'll learn about the crucial role of management concepts and a well-defined incident response plan, ensuring the right people do the right things at the right time.

15%

5.0 Security Policies and Procedures

5.1 Describe management concepts

5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61

5.3 Apply the incident handling process such as NIST.SP800-61 to an event

5.4 Map elements to these steps of analysis based on the NIST.SP800-61

5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP800-61)

5.6 Describe concepts as documented in NIST.SP800-86

5.7 Identify these elements used for network profiling

5.8 Identify these elements used for server profiling

5.9 Identify protected data in a network

5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

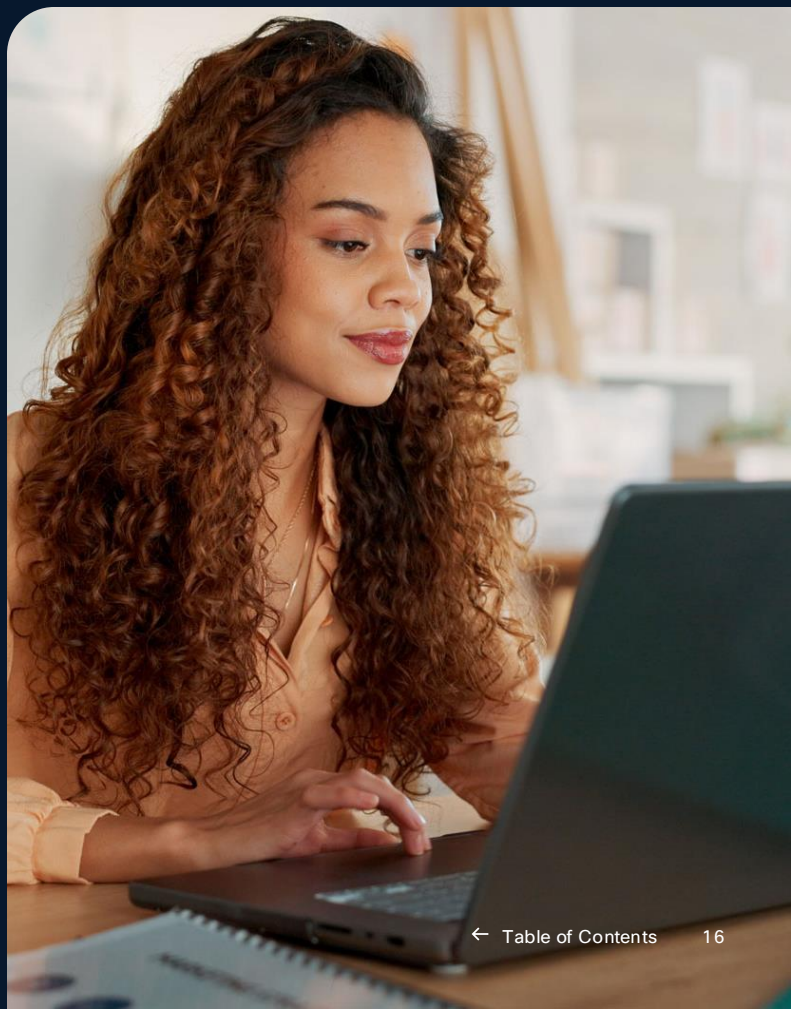
Pro tips

When the verb for a topic area is “describe,” you won’t need the same depth of knowledge for that topic as when the verbs are “configure,” “troubleshoot,” and “analyze.”

Download current 200-201 CBROPS Exam Topics

For a detailed review of all the exam topics, watch the Cisco Certified Cybersecurity Associate Training Videos. They are a fantastic resource for a deeper understanding of the material.

Watch the video series



Official training: Cisco Networking Academy

If you're a student or new to cybersecurity, this might be the best place for you to start. Find online courses, in-person learning, and certification-aligned pathways like Junior Cybersecurity Analyst to help begin, change, or propel your first career in cybersecurity. Did we mention it's free?

Choose from several no-cost training options to start learning:

Introduction to Cybersecurity

A foundational course where you'll explore the exciting field of cybersecurity and understand why cybersecurity is a future-proof career.

CyberOps Associate

This course prepares you for the Cisco CCNA Cybersecurity Certification, covering the core skills needed for a Security Operations Center (SOC) team.

Cybersecurity Essentials

Learn the skills to protect and defend an organization and launch your career in cyber.

Cisco Packet Tracer

A powerful network simulation tool that allows you to build and troubleshoot security scenarios in a virtual environment, giving you essential hands-on experience.

Official training: Cisco Certifications

Start here. Go anywhere. This is where the real work happens. You'll need two things: the exam topics as well as a strategy for learning, studying, and practicing. Learn with Cisco has everything you need to build upon what you already know.

Choose from several training options to help you prepare:

Instructor-led courses

For a guided, expert-led experience, use the Cisco Learning Locator to find courses, both in-person and virtual. The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) Learning Path is the official course to prepare you for the 200-201 CBROPS exam.

If books are your thing

Check out the Cisco Press Cisco Cybersecurity Associate CBROPS 200-201 Official Cert Guide.

Practice exams

Before you take the live exam, a practice exam can help you identify any knowledge gaps or weaknesses. Consider the Cybersecurity Associate practice exam to perfect your skills.

Regardless of how you prepare for the exam, it's crucial to get hands-on experience in a lab environment. This is called "labbing." Your ability to execute critical tasks will be tested on the exam, so you need to practice. Lab early. Lab often. Then lab some more.

If you are just starting out, consider the Cisco Certified Support Technician (CCST) Cybersecurity certification exam. It's a great first step toward the CCNA Cybersecurity certification, and you can learn the skills for free with the Junior Cybersecurity Analyst Career Path.

Exam success

What to expect

CCNA certification exams are administered by our testing partner, Pearson VUE, as proctored exams. When you take the exam, you'll be in a controlled environment to ensure fairness and to give you the best, most consistent experience.

The 200-201 CBROPS v1.2 Exam tests a candidate's knowledge of security concepts, monitoring, host-based analysis, network intrusion analysis, and security policies. The official course, Understanding Cisco Cybersecurity Operations Fundamentals, helps candidates prepare for this exam.

Cisco performance-based testing gives you an experience that best replicates a true lab environment. As a result, the number of questions on your exam may vary. To find out more about this testing experience, read our Performance-Based Lab Exam Items Build Opportunities blog.

Please note: The name of this certification and the exam are scheduled to change on February 3, 2026. Anyone holding the current certification will automatically receive the updated certification.

To view a walk-through demonstration of the various exam question types and how they function, check out the Cisco Certification Exam Tutorial Videos page.

Visit cisco.com/go/onlinetesting to perform a system check.

Ensure your exam success: Safeguard and Safeguard Plus

To help you build more confidence, Cisco Exam Safeguard offers two ways to help give passing your exam a backup plan. Register for your exam as usual, if you don't pass your first exam attempts, you can retake the exam at no additional cost. You'll get the peace of mind that comes from knowing you've invested in a second chance, whether you need it or not.

With Safeguard Plus, we also include the practice exam so you can practice as many times as you need to feel ready.

Learn more

Next steps

Next steps

The IT landscape evolves daily, and your CCNA Cybersecurity provides the core foundation to build your career. With your CCNA Cybersecurity, you'll be more knowledgeable and confident about all things cybersecurity, positioning you for a rewarding and lucrative career.

Here's how to leverage your certification and continue your growth:

Communicate your value

Use this guide and email template to let your manager know why training and certification is so beneficial for you—and for them. Ask your manager to sponsor your training to help transform your career, income, and skill set.

Explore further certifications

Your Cisco Certified Cybersecurity Associate certification is a gateway. Consider pursuing your Professional certification to deepen your expertise and open new doors.

Now’s the perfect time

The complexity of cyberthreats has evolved. Cybercriminals are weaponizing data. Ransomware is on the rise. And security breaches are increasing operating expenses at companies large and small.

These organizations all rely on Security Operations Center (SOC) teams to vigilantly watch security systems, rapidly detect breaches and respond quickly and effectively. To succeed, SOCs desperately need qualified cybersecurity professionals.

Which is why right now is the perfect time for you to launch your career in cybersecurity operations.

Beyond CCNA Cybersecurity

This certification is one of many steps you can take on your learning journey. With each step, you build your knowledge base—and your reputation—to become increasingly valuable to any IT organization.

Download certifications poster

Entry to expert learning journeys

Earning the certification you need can lead you to the career you want. It can also keep you competitive in a field where 92% of IT professionals hold certifications. The Cisco certification portfolio offers more options than ever before, empowering you to customize your learning path to meet your career needs, interests, and aspirations. Since every Cisco exam you pass earns you a certification, each of these milestones you reach tells a new chapter in your story.

Here are the different levels of Cisco certifications to choose from:

Entry

Validates your skills and qualifications for entry-level IT roles

Associate

Proof that you've mastered the essentials to build your IT career

Professional

A core technology track to sharpen your specialized expertise

Expert

The most prestigious certification you can earn

Specialist

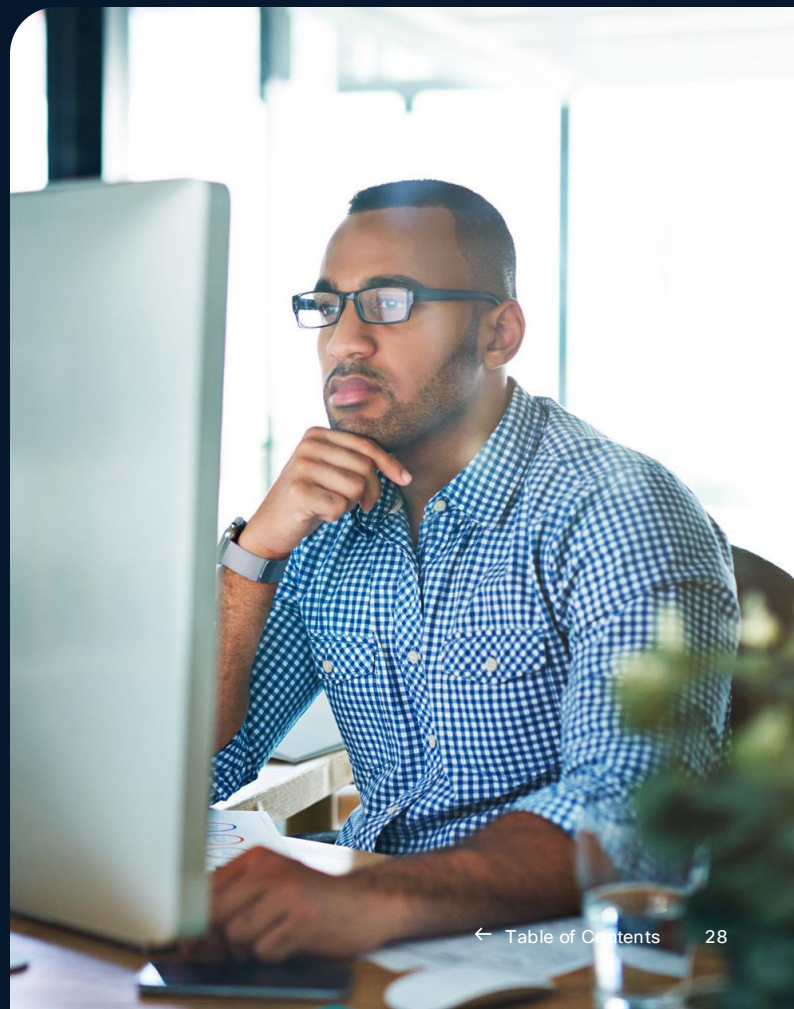
Advanced networking knowledge in tech such as security, data center, or video

Resources to help your studies

Study toolkit

We have many resources to help your progress. We encourage you to sign up for the Cisco Learning Network to be able to access learning resources, including videos, learning plans, and more.

We've also provided a vocabulary list to help your studies.



Vocabulary

Knowing these key vocabulary terms will help you on your CCNA Cybersecurity certification journey.

Access Control List (ACL)

A list of permissions attached to an object specifying which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

Authentication

Verifying the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Authorization

The process of giving someone permission to do or have something in a network.

Backdoor [Method or attack type]

A covert method by which hackers bypass an organization's standard security protocols in order to gain unauthorized privileged access to a system, network or application. Once a backdoor is in place, attackers can remotely access the affected system, exfiltrate data, install additional malware, or use the compromised system to launch attacks on other networks.

Biometrics

An automated authentication method that verifies a user's identity using their unique biological characteristics such as fingerprints, voices, retinas, and facial features.

Vocabulary

Blue Team

The group of security professionals who perform defensive cybersecurity tasks, including identifying security risks and threats, evaluating the current state of security readiness, and defending against real or simulated attacks in an enterprise network environment.

Botnet

A network of internet-connected devices (computers, IoT devices, smartphones, or servers) infected with malware and controlled by a hacker without the owner's knowledge. The infected devices, often referred to as "zombies," are used to carry out malicious activities such as DDoS attacks, data theft, and cryptocurrency mining.

Brute Force Attack [Attack type]

Hacking method using a trial-and-error approach of guessing passwords, login credentials, and encryption keys to gain unauthorized access to a system or data.

Cryptography

The practice of information hiding and verification using protocols, algorithms, and methodologies to securely prevent unauthorized access or use of sensitive data. Two key cryptographic methods are encryption, used to transform plaintext data into an unreadable format, and decryption, used to restore encrypted data back into its original usable form.

Data poisoning [AI term attack type]

An emerging type of attack where a hacker deliberately corrupts or manipulates the training data used to develop machine learning (ML) or artificial intelligence (AI) models by injecting misleading or incorrect information into the training dataset causing the model to produce inaccurate outputs or learn biased patterns.

Decryption

The process of converting encrypted data back into its original form so it can be understood.

Deepfakes

An elaborate form of synthetic media using AI and machine learning (ML) techniques to fabricate or manipulate audio, video, or images that appear convincingly real. Deepfakes pose several cybersecurity implications including bypassing biometric security, identity theft, social engineering attacks, disinformation campaigns, and blackmail or extortion.

Denial-of-Service (DoS) /
Distributed Denial-of-Service (DDoS)

Cyberattacks designed to overwhelm a network or service with traffic, making it unavailable to users. A DoS is launched from a single source, while a DDoS attack involves multiple sources.

Vocabulary

Denial-of-Service Attack (DoS)

An interruption of an authorized user's access to any system or network, typically one caused with malicious intent.

Distributed Denial-of-Service attach (DDoS)

A type of attack where multiple compromised systems are used to target a single system causing a Denial of Service (DoS) attack.

Digital certificate

An electronic document used to prove the ownership of a public key.

Digital forensics

The practice of investigating cyberattacks and incidents by collecting, analyzing, and preserving digital evidence to understand the nature of an attack, identify perpetrators, and prevent future incidents.

Ethical hacking

The practice of attempting to gain unauthorized access to computer systems, applications, or data conducted by authorized security individuals using the strategies and actions of malicious attackers. Ethical hacking helps to identify security vulnerabilities that can then be resolved before a malicious attacker has the opportunity to exploit them.

Encryption

The process of converting data into a coded form to prevent unauthorized access.

Exploit

A piece of code that takes advantage of a vulnerability in a system, application or network allowing an attacker to perform unauthorized actions, such as gaining control over a system or stealing data.

Firewall

A network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.

Incident response

The methodology an organization uses to respond to and manage a cyber-attack. An incident response plan includes a policy that defines in specific terms what constitutes an incident and provides a step-by-step process to be followed during an incident.

Intrusion Detection System (IDS)

A device or software application that monitors a network or systems for malicious activity or policy violations.

Vocabulary

Intrusion Prevention System (IPS)

A form of network security that works to detect and prevent identified threats.

Logic Bomb [Attack type]

A type of malware code imbedded within a software or systems that is designed to activate and execute a malicious function when specified conditions are met. Triggers can be time-based, event-driven, user actions, or system conditions.

Malware

Software designed to disrupt, damage, or gain unauthorized access to a computer system.

Man-in-the-Middle (MitM) Attack [Attack type]

A cyberattack where an attacker intercepts and potentially alters the communication between two parties who believe they are directly communicating with each other. The attacker can eavesdrop on the conversation or manipulate the data being exchanged without the knowledge of either party.

Patch management

The process of managing a network of computers by regularly performing system patches and updates to improve security and functionality.

Penetration testing

A simulated cyberattack conducted on a computer system, network, or web application to evaluate its security. The main goal is to identify vulnerabilities that could be exploited by attackers and provide insights on improving the system's defenses. Also referred to as pen testing.

Pharming [Attack type]

A type of large-scale cyberattack in which hackers redirect users from legitimate websites such as online banking, retail shopping, and social media to fraudulent websites with the goal of collecting sensitive data such as login credentials and financial information.

Phishing [Attack type]

A cybercrime where the attacker posing as a legitimate institution or entity sends email to an individual or group with the intent of stealing the target's personal information such as usernames, passwords, credit card details, social security numbers, or other sensitive data. Phishing relies on evoking a sense of urgency that compels the victim to take immediate action by clicking on a malicious link or attachment in the message. Related forms of phishing include smishing (SMS), vishing (voice) messaging.

Vocabulary

Public Key Infrastructure (PKI)

A set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

Purple Team

A collaborative effort between members of the Red Team (offensive) and Blue Team (defensive) working in unison to simulate attacks and test defenses with the goal of enhancing an organization's security communication and effectiveness.

Ransomware

A type of malicious software designed to block access to a computer system until a sum of money is paid.

Reconnaissance

The preliminary phase where attackers gather information about a target system or network to identify potential vulnerabilities and plan their attack strategy.

Red Team

The group of security professionals who perform offensive cybersecurity tasks intended to emulate a potential adversary's behavior, including TTPs (tools, tactics and procedures), social engineering, ethical hacking, pen testing, and exploitation with the goal of identifying security vulnerabilities in the network environment.

Rootkit

A type of malicious software that enables unauthorized users to gain access and control of the host's system, network, and devices while concealing its existence from detection.

Social Engineering

Cybercriminal tactics using psychological manipulation to gain a target user's trust and coerce them into divulging confidential information or providing unauthorized access to systems or data.

Security Operations Center (SOC)

A centralized unit that deals with security issues on an organizational and technical level.

Vocabulary

Spoofing

A tactic where an attacker disguises their identity or communication to appear as an authorized, trusted source, typically to deceive systems or individuals into providing sensitive information or access.

Supply Chain Attack

A cyberattack that targets an organization by exploiting the vulnerabilities of trusted third parties and vendors in its supply network, such software providers or hardware manufacturers, to gain unauthorized access to its systems and data.

Threat Actor

An individual or group that conducts malicious activities or cyberattacks against organizations or systems, often with the intent to steal data, disrupt operations, or cause harm.

Threat Hunting

The proactive process of searching through networks and systems to detect and isolate advanced threats that evade automated security solutions. It involves identifying indicators of compromise and suspicious activities to protect against potential cyberattacks.

Two-Factor Authentication (2FA)

A security process in which the user provides two different authentication factors to verify themselves.

Virtual Private Network (VPN)

A service that allows you to connect to the internet via a server run by a VPN provider, creating a secure connection.

Vulnerability

A weakness in a system that can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system.

Zero-day exploit

A cyberattack that targets a software vulnerability unknown to the software's developers or the public. Since there is no available fix at the time of the attack, these exploits can be particularly damaging and are often used to compromise systems before the vulnerability is patched.

Additional resources

Other cybersecurity resources include:

Cybersecurity Associate Certification Overview

Download 200-201 CBROPS Exam Topics

Cybersecurity Certifications Community

Cisco Certified Cybersecurity Associate Training Videos

Cisco Learning Blog

Cisco Certification Blogs

Stay connected through:

Cisco Learning Network

Cisco Networking Academy

Cisco U

Use code CBROPS40 to save 40% on your purchase of the Cisco Cybersecurity Associate CBROPS 200-201 Official Cert Guide or Premium Edition eBook at: ciscopress.com/CBROPS

Discount code CBROPS40 confers a 40% discount off the list price of ISBNs 0-13-680783-6 and 978-0-13-680783-4, when purchased on ciscopress.com. Apply discount code during checkout to receive savings. Ineligible titles include book + eBook bundles, book/eBook + video bundles, Rough Cuts, O'Reilly Online Learning, or individual video lessons. Discount code may not be combined with any other offer and is not redeemable for cash. Discount offer expires 11:59 p.m. EST December 31, 2025. Offer subject to change.


CISCO