Cisco Certified CyberOps Certification Guide

Top Cisco resources to plan and prepare for certification

Get started

Table of Contents

02 Overview

04 Certifications path

06 Vocabulary

07 Training options

09 Exam overview

10 Resources

11 Next steps

©2024 Cisco and/or its affiliates. All rights reserved.

Cisco Certified CyberOps Associate is about preparing you for the SOC

Today, every organization needs security expertise, before, during, and after an attack. Which is why the demand for cybersecurity operations (CyberOps) personnel keeps skyrocketing. Worldwide spending on cyber security is expected to hit a not-so-modest $215 billion in 2024, a 14.3% jump from the previous year[1]. CyberOps teams guard business-critical infrastructure and applications. In real time, they protect digital assets, defend against threats, and respond to attacks.

How do you get started in a career in this exciting, high-energy field? Earn your Cisco Certified CyberOps Associate certification. It's from Cisco, a leading, recognized provider of 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, skills, and procedures. And the process couldn't be simpler: Take one training course and pass one exam—and you're on your way to associate-level job roles with SOC teams worldwide.

1. CYBERSECURITY DIVE, Cyber investments on pace to reach $215B in 2024: Gartner., https://www.cybersecuritydive.com/news/cyber-spending-gartner-moodys/695343/, November 14, 2023.

©2024 Cisco and/or its affiliates. All rights reserved.

The Cisco Certified CyberOps Associate certification might be the one for you if:

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

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

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

And while you build your skills, you're also building your income. Here's proof. Skillsoft's Global Knowledge 2023 IT Skills and Salary Report examined data from thousands of IT professionals. Eighteen percent estimated that the annual value of being certified is $30,000 or more.

Training and certifications pay off– and organizations know it. Over 35% of respondents listed a boost in productivity as the top benefit of a certified staff. Even more, 34% of respondents believe that certifications close organizational skill gaps[2]. That makes certified candidates stand out in a pool of applicants during the hiring process.

The network is under constant assault–and it needs you. Cybersecurity is full of rewarding, meaningful, challenging work. Earning your Cisco Certified CyberOps Associate certification can help your résumé stand out and give you a foot in the door.

2. Skillsoft, The 20 top-paying certifications going into 2024. , https://www.skillsoft.com/blog/top-paying-it-certifications, November 14, 2023.

©2024 Cisco and/or its affiliates. All rights reserved.

Look ahead - certification tracks

As you can see, a Cisco Certified CyberOps Associate 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 poster

©2024 Cisco and/or its affiliates. All rights reserved.

Cisco certifications are available in multiple levels of expertise and various professional areas.

Earning the Cisco CyberOps certifications you need can lead you to the career you want. And you'll be more competitive in a field where 92 percent of IT professionals hold certifications.

Cisco's certification portfolio offers more options than ever, empowering you to customize your learning path to your career, interests, and aspirations. Since every Cisco exam you pass earns you a certification, each milestone tells a new chapter in your story.

Here are the different levels of Cisco certifications you can earn:

Associate →

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

Professional →

Focus on a core technology track to sharpen your specialized expertise

©2024 Cisco and/or its affiliates. All rights reserved.

Vocabulary

If you're just starting out on your Cisco Certified CyberOps Associate certification journey, get to know these key terms:

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.

Encryption

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

Decryption

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

Firewall

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

Intrusion Detection System (IDS)

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

Intrusion Prevention System (IPS)

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

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.

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.

©2024 Cisco and/or its affiliates. All rights reserved.

Digital certificate

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

Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

Protocols for establishing authenticated and encrypted links between networked computers.

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.

Security Information and Event Management (SIEM)

Solutions that provide real-time analysis of security alerts generated by applications and network hardware.

Two-Factor Authentication (2FA)

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

Phishing

A cybercrime in which a target or targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data.

Malware

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

Ransomware

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

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 Attack (DDoS)

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

©2024 Cisco and/or its affiliates. All rights reserved.

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.

Penetration testing

A simulated cyber attack against your computer system to check for exploitable vulnerabilities.

Zero-day exploit

A cyber attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator.

Patch management

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

Security Operations Center (SOC)

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

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.

©2024 Cisco and/or its affiliates. All rights reserved.

Training options

This is where the real work happens. You'll need two things: the exam topics, and a strategy for learning, studying, and practicing.

The Cisco Certified CyberOps Associate certification exam topics is the basis for the exam. They define the contents of both the exam and the official training course, and it should be your roadmap for studying. If you can successfully complete the tasks defined for each topic, you're ready for the exam.

There are no formal prerequisites for the Cisco CyberOps Associate certification, but you should understand the exam topics before taking the exam—and develop a strategy for how you're going to master them.

Keep in mind: 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 "design."

©2024 Cisco and/or its affiliates. All rights reserved.

Here are several training options to help you prepare:

- The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) Learning Path teaches you what you need to know to become a contributing member of a Cybersecurity Operations Center (SOC) team—all while preparing you for the Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS) exam.

  Add the CyberOps Associate practice exam to identify any knowledge gaps or weakness that you should focus on before taking the live exam and you've got the perfect exam prep pairing.

- Use the Cisco Learning Locator to find instructor-led courses, both in-person and virtual.
- If books are your thing, check out the Cisco Press Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, a perfect addition to your self-study plan.

There are no formal prerequisites for the Cisco CyberOps Associate certification, but you should understand the exam topics before taking the exam—and develop a strategy for how you're going to master them.

Check out the following options to help you get started:

- Validate your skills and knowledge of entry-level cybersecurity concepts and topics with the Cisco Certified Support Technician (CCST) Cybersecurity certification exam. It's a great first step toward the Cisco Certified CyberOps Associate certification.
- Learn the skills you need to prepare for CCST with the Junior Cybersecurity Analyst Career Path. It's free.

Regardless of how you prepare for the exam, it's crucial for you to get your hands on the gear to practice. This is called "labbing," as in "practicing in a lab environment." 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.

©2024 Cisco and/or its affiliates. All rights reserved.

Exam overview

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

During the exam, it will be just you and your knowledge and experience versus the test. Keep track of the time, read each question carefully, answer each one (and if you don't know the answer, try to eliminate one or more options and then guess), and keep moving to the end.

After you pass the exam, you can link your digital certification badge to all your social media profiles to tell the world what you've achieved.

And, you can take certification exams online, so you can stay on track, even when you can't travel to a testing center.

Perform a system check before taking your exam.

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.

200-201 CBROPS v1.1 Exam Topics

©2024 Cisco and/or its affiliates. All rights reserved.

Resources

CyberOps Associate Essentials →

Still thinking about getting certified? Select CyberOps Associate Essentials for more details about the program. It will help you make the best decision.

CyberOps Associate Prep →

Already decided to get certified, and want to start studying? Select CyberOps Associate Prep to find the ultimate resources to develop your self-study plan.

Other CyberOps resources include:

- Cisco Certified CyberOps Associate Training Videos
- Cisco Learning Blog
- Cisco Certification Blogs
- CyberOps Associate Certification
- Download 200-301CBROPS v1.1. Exam Topics
- CyberOps Certifications Community

Stay connected through:

- LinkedIn
- Facebook
- X, formerly known as Twitter
- Cisco Learning Network
- Instagram
- Cisco YouTube Channel

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

©2024 Cisco and/or its affiliates. All rights reserved.

Now's the perfect time

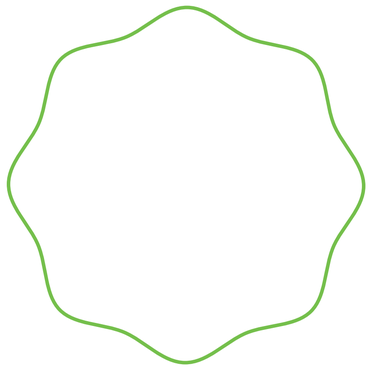
The complexity of cyberthreats has evolved. Cybercriminals are weaponizing data. Ransomware is on the rise. And security breaches are increasing operating expenses at companies large and small.

These organizations all rely on 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.

With the Cisco Certified CyberOps Associate certification, you can secure your position in this new, fast-paced era of cybersecurity. It prepares you to begin a career working as a highly in-demand associate-level cybersecurity analysts within SOCs.

If you're starting your cybersecurity journey with a CCNA certification, we have great news for you! As a foundational cert, CCNA establishes a solid baseline for IT pros who want to build upon their knowledge with new security skills. In fact, most of your skills and knowledge already overlap.



©2024 Cisco and/or its affiliates. All rights reserved.

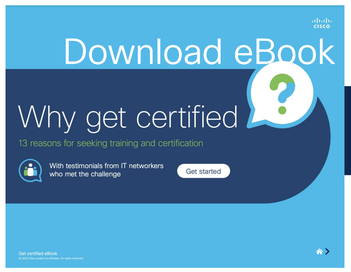
Next steps

Use this email template to let your manager know why training and certification is so beneficial for you–and for them. Get the help you need to transform your career, your income, and your skill set.

Next, get help on your CyberOps Associate Certification self-study plan directly from Cisco for FREE. Sign up for the CyberOps Associate Prep On Demand program. You'll gain access to all kinds of resources to help you succeed, including webinars focused on exam topics, a learning map, a practice quiz, access to Cisco subject matter experts, and more.

Take these important next steps to master the essentials to prevent, detect, and respond to cybersecurity threats and breaches. You'll upgrade your resume, with training and certification on cybersecurity operations. And you'll boost your confidence by gaining real-world knowledge.

Ask your manager to sponsor your training. Once they understand the benefits to your organization, they will be eager to learn more and support you with next steps.



Download e-book

©2024 Cisco and/or its affiliates. All rights reserved.