CBTnuggets

Certification Guide

Security

Table of Contents

How to Succeed in Security

The security career field has boomed recently with demand high and investment pouring into the sector. Gartner predicts that security spending will increase to $170.4 billion in 2022 as companies move beyond simple prevention to advanced offensive security methods. Inevitably, a portion of the money will go to fill the acute shortage of qualified security professionals. Independent research suggests 1.8 cybersecurity positions will go unfilled worldwide in 2022. Meanwhile, cyber threats are showing no signs of slowing.

The numbers are staggering, but the massive shortage of qualified professionals is not necessarily due to lack of interest or investment. Quite simply, it just takes longer to train cybersecurity professionals. It's been said there's no such thing as an entry-level security professional. When someone enters the cybersecurity field, it's typically on the back of five to seven years of experience, and there's a reason for that.

Security professionals need to know everything — networking, system administration, and even programming. To prevent a breach, security professionals need to know every attack vector — technological and social, new and old. To combat breaches, pen testers need to think like a hacker. To clean up after a breach, forensic analysts need to know where to find clues about the cause and how to patch the holes. If that seems daunting, don't worry. Security professionals aren't made overnight. Instead, they're developed throughout a career in IT.

Looking at the most difficult security exams, like the OSCP or CISSP, the depth and breadth of required knowledge is intimidating. These are specialized exams for specialized roles that attract experienced security professionals. Most security professionals specialize in one area of IT, and then specialize in security. Security professionals need to know everything, but not immediately.

A Look at Security Career Progression

Long before an IT professional heads down a specialization path like analysis, pen testing, or risk management, they acquire basic security skills throughout the normal course of their career. The easiest way to get into IT security isn't necessarily with security certifications (though it helps). Instead, the best way to start down the security path is with basic certifications like CompTIA Network+, Cisco CCNA, or even a Microsoft MCSA. More important than security knowledge are fundamental network and system skills.

With those foundational skills acquired, it's time to specialize — and there are certifications specific to each stage of a career. A look at the requirements for one foundational security certification, shows where IT professionals looking to get into security can start.

Entry-level: Security fundamentals

There's only one true foundational security certification — CompTIA Security+. As it should be, this exam is basic at best and very broad. Here are the exam objectives:

- 1.0 Threats, Attacks, and Vulnerabilities - 21%
- 2.0 Technologies and Tools - 22%
- 3.0 Architecture and Design - 15%
- 4.0 Identity and Access Management - 16%
- 5.0 Risk Management - 14%
- 6.0 Cryptography and PKI - 12%

Note that nearly half the exam — the first two domains — simply validates terms and tools. The exam then offers a broad introduction to the other aspects of security. As with all certifications, its difficulty is relative to the experience level of the test taker. For someone just getting into IT, Security+ introduces a whole new vocabulary and reinforces that information through scenario-based test questions. In this way, it's a perfect starting point for anyone interested in getting into security. However, the serious security stuff starts appearing throughout many certifications that aren't necessarily security-specific.

Advanced Basics: 2 to 3 years

Security is baked into most IT certifications. Most people think they need advanced or expert security certifications to specialize, but security topics are covered in the most entry-level networking and system administration certifications. For instance, networking professionals should expect about 11 percent of questions on the CCNA to be about infrastructure security. Cloud professionals can expect nearly a quarter of the AWS

Certified Solutions Architect - Associate exam to be security-related.
Security is everyone's job, and IT professionals will get plenty of dedicated security experience — even as generalists in a support role or early-career network or systems administrators. Many decide to specialize from this initial exposure to security responsibilities. When that time comes, it's time to get certified.

Security Specialization: 3 to 7 years

At this point, most security professionals have already assumed many of the responsibilities they'll need to build a great security resume. That also means it's time to get certified.

Security certifications are either offered by security appliance vendors like Palo Alto or Cisco, or professional organizations dedicated to security like (ISC)2. In either case, these certifications are specialized and often require at least five years of experience. AWS offers the AWS Certified Security - Specialty certification, which requires five years of IT security experience and at least two years securing AWS workloads. Similarly, Cisco has a security track, which right now starts at the CCNA level, but will soon be a professional (or mid-career) certification. The next steps are highly individualized. Security is a huge career field with many potential career paths.

IT Security Career Paths

Security jobs are often a continuation of the skills acquired throughout a career. For instance, network administrators may become analysts or pen testers. Developers may become security engineers. Systems administrators may turn to application or systems security. Again, that's because security professionals are often specialists in both one career field and also security. Here are some common security career paths.

Cybersecurity Analyst

By most accounts, analysts do pretty boring work. Analysts do two things: discover and detect cyberattacks. What discovering threats means is dependent on the requirements of the company, but it most often means digging into log files to find threats and then implementing security policies to prevent attacks based on their signatures. Security policies can be implemented through a security appliance or software, or through custom-built automation.

IT professionals looking to become cybersecurity analysts need a well-rounded set of technical skills because they rely on their experience to know what to look for. Cybersecurity analysts are technicians, which mean they need qualified technical skills like Windows administration, desktop support, networking, and probably proficiency with at least one programming language. Analysts may spend days auditing SSL certificates or combing through logs. It's monotonous but important work that's performed on the frontline of an attack.

Security certifications: CompTIA CySA+, CCNA CyberOps
Typical background: Systems administrator, network administration

Security Engineer

Engineers play a different role than analysts. While analysts identify security issues and detect attacks, engineers set up defenses and prevent disruption to services in the event of an attack. Most often, engineers implement the security measures that come down from the security architect (or similar security manager). It may be building reporting and logging features, or implementing security hardware. As is the case with most security positions, no two security engineer jobs are the same, but most engineers should have a wide set of skills like networking, Active Directory, server technologies, firewalls, light pen testing, and scripting.

Security certifications: AWS Security, CCNP Security
Typical background: Systems administrator, network administration, software engineer

Security Architect

Architect roles will have different responsibilities depending on the company. Some architects are still deeply hands-on with the technology, acting more like senior engineers. Other architects operate more as managers. As managers, architects evaluate security solutions, sell their benefits to top management, and then work with engineers to implement the solutions. Whether they are still hands-on or managerial, architects are senior technicians with plenty of time in the trenches as an engineer.

Security certifications: CCIE Security, CISSP
Typical background: Systems administrator, network administration, software engineer

Penetration Tester

With all the recent high-profile breaches, pen testing has grown in popularity. Networking, systems administration, Linux, and scripting feature strongly in the OSCP exam tasks, which is a good proxy for the skills required in the field. Pen testers often rely on previous experience to look for vulnerabilities. For instance, a pen tester may draw on their experience hardening servers in a previous role as a system administrator to know where to look for misconfigurations. For that reason, the best pen testers didn't start out as pen testers. They started out as generalists or networking professionals.

Security certifications: CompTIA PenTest+, OSCP
Typical background: Systems administrator, network administration, software engineer, security analyst

Security Executive

In 2019, while most companies struggled to find qualified technical cybersecurity professionals, few security executive positions went unfilled. That may be due to the sheer quantity of technical professionals demanded by the market. In any case, security executives are managers and communicators who look at systems from the perspective of security. Many C-level and managerial security professionals work their way up from technical positions. Certifications like the CISSP validate the considerable technical experience typically required for these positions.

Security certifications: CISSP
Typical background: Software engineer, security engineer, security architect

Other Security Job Roles

The job titles listed here are broad, and represent the most common ones an aspiring security professional will find and pursue. As security professionals progress, they'll find the other subsets of information and cybersecurity roles that exist and determine whether they're a good fit.

Specialists. Anyone whose even glanced at a job site knows there are plenty of specialized positions out there. There are security professionals who specialize in cloud, mobile, IoT, or the dozens of other specialist analyst or engineer positions. Some of these specialized roles have certifications associated with them — many do not. Specialists rely on their own experience and research to enter and remain current in their narrow well of expertise.

Incident handlers. There's an entire subset of security jobs that show up only in the event of a major security event, like incident handlers, forensics, and other Computer Security Incident Response Team (CSIRT) members. These are exciting jobs that may be dedicated staff, or activate in the event of an incident. Security professionals in this subfield often work for a government agency or cybersecurity firm. Otherwise, CSIRT members will have a primary role as an engineer or analyst except when something happens.

Cybersecurity researchers. There's also the growing field of malware analysts and security researchers who reverse engineer malware, trace threats back to their origins, and set honeypots. They may work at a large company, but most often they'll be employed by a nonprofit, cybersecurity firm, or a government agency.

Compliance and governance. Compliance is thankless work, but also essential for companies beholden to a particular framework for certification. These job titles often refer to policy, governance, or compliance. This subset of security professionals enforce compliance standards with the NIST, DISA, ITIL, or PCI framework.

Using this Certification Guide

Despite the demand for security professionals, security is a difficult career field to break into. That's because it's difficult to gain security experience if companies won't hire someone without security experience. Most people in this field must start assuming security responsibilities in their day-to-day roles before specializing. With that experience and certification, anyone can build the resume they need to land their first security job.

In this certification guide, we've listed every certification for the top networking vendors — Cisco, Palo Alto, (ISC)2, Check Point, Offensive Security, and CompTIA. A notable exception is GIAC certifications, which will be in a future version of this certification guide.

Each chapter is ordered from foundational to specialized expert. Choose your path based on your career goals, experience level, and stated prerequisites.

CBTnuggets

Palo Alto Certifications

Palo Alto Networks is recognized around the world as a leading provider of cybersecurity products. Palo Alto Networks certification validates an IT professional's knowledge and skills in security management using Palo Alto products. It is a valuable credential for those seeking advancement in the field of IT security. The aim of the Palo Alto certification path is to give IT professionals the opportunity to demonstrate the skills required to secure their systems and network.

The Palo Alto certifications exams include three levels of certification, designed to take the learner from beginner to expert:

- **Associate**
- **Administrator**
- **Engineer**

Palo Alto Network Certifications

Palo Alto certification currently includes the PCCSA, PCNSA, and PCNSE exams. According to Palo Alto, the focus is on the critical skills required to develop infrastructure, mitigate threats, and prevent successful cyberattacks. Certified professionals will have an understanding of how to use Palo Alto hardware and software to protect IT assets from attack.

Palo Alto offers three professional certifications available for demonstrating network security skills:

- **Palo Alto Networks Certified Cybersecurity Associate (PCCSA)**
- **Palo Alto Networks Certified Network Security Administrator (PCNSA)**
- **Palo Alto Networks Certified Network Security Engineer (PCNSE)**

Palo Alto Networks Certified Cybersecurity Associate (PCCSA)

The Palo Alto Networks Certified Cybersecurity Associate certification is designed for IT professionals who are just beginning in the field of cybersecurity. The PCCSA is the lowest level in the Palo Alto Networks certification path, and validates knowledge in these areas:

- **Cybersecurity Landscape**
- **Cyberthreats and the Cyber-Attack Lifecycle**
- **Cyberattack Techniques and Types**
- **Wireless Threats and Advanced Threats**
- **Cloud Security and Data Center Security**
- **Network Security Technology**
- **Packet Encapsulation and Lifecycle**
- **Malware Analysis**

Required exam: Earning the PCSSA certification requires passing one exam — the Palo Alto Networks Certified Cybersecurity Associate exam.
Prerequisites: None.
Recommended experience: Palo Alto Networks recommends a basic understanding of networking and cybersecurity and up-to-date knowledge on cyber threats prior to attempting this certification exam.

Palo Alto Networks Certified Network Security Administrator (PCNSA)

The Palo Alto Networks Certified Network Security Administrator certification is designed for IT professionals who use Palo Alto Networks next-generation firewalls. The PCNSA certification validates a candidate's understanding of these security administration tasks:

- **Next-Generation Security Platform and Architecture**
- **Firewall Configuration**
- **Security and NAT Policies**
- **App-ID™**
- **Content-ID™**
- **LO ALTO NETWORKS PCNSA FAQ 3**
- **User-ID™**
- **URL Filtering**
- **Monitoring and Reporting**
- **Security Best Practices**

Required exam: Earning the PCNSA certification requires passing one exam — the Certified Network Security Administrator exam.
Prerequisites: The PCCSA is not specified as a prerequisite for PCNSA, but it is highly recommended.
Recommended experience: Palo Alto recommends advanced knowledge of networking and cybersecurity and considerable experience deploying Palo Alto firewalls prior to attempting this certification exam.

Palo Alto Networks Certified Network Security Engineer (PCNSE)

The Palo Alto Networks Certified Network Security Engineer (PCNSE) certification is designed for IT professionals with considerable experience and expertise in Palo Alto Networks technologies.
The PCNSE certification validates a candidate's understanding of these security administration tasks:

- **Security Management Concepts**
- **Deployment and Configuration of Palo Alto Hardware and Software**
- **Management and Operation of Security Platforms**
- **Troubleshooting of Network Security Issues**

Required exam: Earning the PCNSE certification requires passing one exam — the Certified Network Security Engineer exam.
Prerequisites: None. The PCCSA and PCNSA are not specified as prerequisites for the PCNSE, but they are recommended.
Recommended experience: Palo Alto Networks recommends advanced knowledge of networking and cybersecurity and extensive experience designing, deploying, configuring, maintaining and troubleshooting the vast majority of Palo Alto Networks Operating Platform implementations.

How Much Does It Cost to Get Palo Alto Certified?

Palo Alto Networks certification exams are proctored by the testing company Pearson VUE. The cost of these exams is significantly less than many other IT certifications we've discussed. The certification system has a simple pricing scheme. The PCCSA costs $100, the PCNSA costs $140, and the PCNSE costs $160.

Palo Alto Recertification and Renewal

Like Check Point, Palo Alto Networks certifications expire after two years (24 months). But you can keep the PCCSA certification valid by taking any of the three certifications. To recertify with the PCNSA, you can take either the PCNSA again or take PCNSE. The PCNSE can only be recertified by retaking the PCNSE exam.

Palo Alto Certification Salary and Career Information
According to Payscale, IT professionals with a Palo Alto Networks Certified Network Security Engineer (PCNSE) certification can expect to earn around $93,000 per year. No figures are available on Payscale for the PCCSA or PCNSA. Those with PCCSA or PCNSA might expect to make a bit less than with the PCNSE, but a lot depends on the level of experience.

Payscale lists the following average salaries for the PCNSE (in USD):

- Network Security Engineer: $110,000
- Network Engineer: $71,899
- Network Architect: $122,607
- Security Consultant, (Computing / Networking / Information Technology): $102,750
- Senior Security Consultant: $147,395
- Security Engineer: $87,500
- Sr. Network Engineer: $115,000

Palo Alto Networks certifications may be among the easier certifications to get for those trying to break into the information security field. And the price is very low compared to other certifications. Of course, many people seek certifications because they are already working on a certain product.

Your decision to pursue Palo Alto certification may depend on whether you believe that you will be working on Palo Alto Networks certifications in your career as an IT professional. Considering the earnings potential and opportunities for Palo Alto Networks certified IT professionals, it's well worth considering.

CBTnuggets

Palo Alto Networks Certification Training

As of September 2019, CBT Nuggets offers the following Palo Alto Networks training from Keith Barker.

- **Getting Started with Palo Alto Firewalls v8.x**
- **Using Palo Alto v8.x Advanced Features**
- **Palo Alto Networks Firewall**

Please note that we constantly update our training library, so check regularly for new Palo Alto training.

In addition to quality, entertaining video training created by expert-level trainers, CBT Nuggets provides everything a learner needs to study for IT certification exams, including virtual labs, supplemental files, practice exams, and access to a robust Learner Community.

All CBT Nuggets training provides learners with custom virtual labs or supplemental files to learn technical concepts alongside the video training. Virtual labs were designed by experts to help learners gain hands-on experience in a sandbox environment. Supplemental files include practice commands, configuration files, and network diagrams — everything a learner needs to study for a certification exam.

CBT Nuggets learners should also take advantage of the Kaplan® IT Training Practice Exams included with a subscription to CBT Nuggets. Practice exams can either be taken timed or untimed, and provide a good baseline for learners to test their knowledge. Additionally, Kaplan® IT Training Practice Exams evaluate a learner's strengths and weaknesses, so they know where to focus their attention while studying.

CBTnuggets

Offensive Security Certifications

Network security is one of the most important aspects of information technology. That's because there are so many bad guys who don't mind infiltrating and pilfering vulnerable networks if they can. Security certifications like Offensive Security, which focuses on penetration testing, arose in response to the growing worldwide threats to IT infrastructure and the demand for professionals who can defend against them.

The internet consensus is that Offensive Security certifications are among the most difficult and highly respected in the business. These professional certifications will improve your IT security resume and show prospective employers that you know something about combating security threats — and that you can do something about it.

Where to Start with Offensive Security Certifications

The Offensive Security certification path is not necessarily tiered. You could take each one individually as long as you complete the required course first, and none of the certifications has another exam as a prerequisite. That said, you might consider the OSCP the "entry-level" exam, and the OSEE as the most advanced. Kali Linux certification is another good option for those who want to brush up on their Linux skills and learn the particulars of the Kali distribution.

What is Kali Linux?

Most Offensive Security certifications recommend knowledge of Kali Linux. Kali Linux is a Debian-based distribution of the Linux operating system that is focused on penetration testing and ethical hacking. The distribution was developed by founder Matt Aharoni and two of his colleagues, and first released in March 2013. It includes hundreds of tools that an IT professional performing penetration testing might need. There is nothing special about the Kali Linux distribution. That is to say, everything on it — the Linux kernel, the utilities, the applications — is available on the open-source market. For instance, Nmap is a piece of software that scans ports, and Wireshark is a network packet analyzer.

Categories of tools listed on the Kali website include:

- **Information Gathering**
- **Vulnerability Analysis**
- **Wireless Attacks**
- **Web Applications**
- **Stress Testing**
- **Forensics Tools**
- **Sniffing & Spoofing**
- **Password Attacks**

It's just that Kali Linux is a curated distribution that includes a certain set of software tools for white-hat hackers. (Now, whether these can be used for nefarious purposes is not the subject of this article.)

Kali Linux is an integral part of the Offensive Security certification training and testing program. Candidates will need to be thoroughly familiar with it for the grueling exam sessions. So, it may be a good idea to play around with it before starting the training.

Offensive Security Certifications

The Offensive Security certification program includes five hands-on tests that require candidates to show they can handle real-world problems. The Offensive Security Certified Professional (OSCP) certification covers general security issues and is usually the entry exam for test-takers. Two exams approach security from different angles: cracking the perimeter and Windows exploitation. The two others deal with specific areas, web attacks, and wireless security.

Offensive Security offers five certifications:

- **Offensive Security Certified Professional (OSCP)**
- **Offensive Security Certified Expert (OSCE)**
- **Offensive Security Web Expert (OSWE)**
- **Offensive Security Wireless Professional (OSWP)**
- **Offensive Security Exploitation Expert (OSEE)**

PENETRATION TESTING

Offensive Security Certified Professional (OSCP)

The Offensive Security Certified Professional (OSCP) certification is designed for network security professionals who want to demonstrate how well they deal with network security vulnerabilities. The OSCP certification validates a candidate's ability to execute these methods and attacks:

- **Use multiple operating systems and services to gather and enumerate targets**
- **Write basic scripts and tools to aid in pentesting**
- **Analyze, correct, modify, cross-compile and port exploit code**
- **Conduct remote and client-side attacks**
- **Exploit XSS, SQL injection, and other web application vulnerabilities**
- **Deploy tunneling techniques to bypass firewalls**

Required exam: Earning the OSCP requires passing one exam — the 24-hour, proctored OSCP exam.
Prerequisite: Prior to attempting this certification, Offensive Security requires taking the Penetration Testing with Kali Linux (PwK) course, which is included in the OSCP course bundle.
Recommended experience: Offensive Security recommends reasonable Linux skills, familiarity with Bash scripting, basic Perl or Python skills, and a solid understanding of TCP/IP and networking prior to attempting this exam.

PENETRATION TESTING

Offensive Security Certified Expert (OSCE)

The Offensive Security Certified Expert (OSCE) certification is designed for network security professionals who want to demonstrate how well they can deal with network security vulnerabilities, including some of the most troublesome exploits. While the OSCP focuses on pentesting, the OSCE takes an in-depth look at many of the specific exploits that hackers use to infiltrate systems. These include buffer overflows and the types of issues covered in the OWASP Top Ten list. The OSCE certification validates a candidate's ability to execute these methods and attacks:

- **Intelligent fuzz-testing**
- **Analyze, correct, modify, and port exploit code**
- **Craft binaries to evade antivirus software**

Required exam: Earning the OSCE certification requires passing one exam — the 48-hour, proctored OSCE exam.
Prerequisite: Prior to attempting this certification, Offensive Security requires taking the Cracking the Perimeter (CTP) course, which is included in the OSCE course bundle.
Recommended experience: Offensive Security recommends reasonable Linux skills, familiarity with Bash scripting, basic Perl or Python skills, and a solid understanding of TCP/IP and networking prior to attempting this exam.

PENETRATION TESTING

Offensive Security Web Expert (OSWE)

The Offensive Security Web Expert (OSWE) certification is designed for network security professionals who want to demonstrate proficiency in auditing of web application code for vulnerabilities, and it is meant to test a candidate's ability to recognize and thwart various web application exploits. This is the newest exam in the Offensive Security portfolio.

The OSWE certification validates a candidate's ability to execute these methods and attacks:

- **Web application code auditing**
- **Audit code to find vulnerabilities**
- **Develop exploits for vulnerable web applications**
- **Analyze of public exploit code**
- **Bypass sanitization filters**

Required exam: Earning the OSWE requires passing one exam — the OSWE exam.
Prerequisite: Prior to attempting this certification, Offensive Security requires taking the Advanced Web Attacks and Exploitation (AWAE) course, which is included in the OSWE course bundle.
Recommended experience: Offensive Security recommends an understanding of web applications, reasonable Linux skills, familiarity with Bash scripting, basic Perl or Python skills, and a solid understanding of TCP/IP and networking prior to attempting this exam.

PENETRATION TESTING

Offensive Security Wireless Professional (OSWP)

The Offensive Security Wireless Professional certification is designed for network security professionals who want to demonstrate their ability to audit 802.11 wireless networks and identify vulnerabilities. Candidates should also be able to simulate attacks themselves. The OSWP certification validates a candidate's ability to execute these methods and attacks:

- **Wireless information gathering**
- **Circumvention wireless network access restrictions**
- **Cracking WEP, WPA, and WPA2 implementations**
- **Man-in-the-Middle attacks**

Required exam: Earning the OSWP certification requires passing one exam — the 4-hour, proctored OSWP exam.
Prerequisite: Prior to attempting this certification, Offensive Security requires taking the Offensive Security Wireless Attacks (WiFu) course, which is included in the OSWP course bundle.
Recommended experience: Offensive Security recommends a good understanding of 802.11 wireless networking, reasonable Linux skills, familiarity with Bash scripting, basic Perl or Python skills, and a solid understanding of TCP/IP and networking prior to attempting this exam.

PENETRATION TESTING

Offensive Security Exploitation Expert (OSEE)

The Offensive Security Exploitation Expert (OSEE) certification is designed for network security professionals who want to demonstrate their ability to research and create exploits through reverse engineering, assembly, and disassembly. The OSEE certification validates a candidate's ability to execute these methods and attacks:

- **Develop sophisticated exploits**
- **Create custom shellcode**
- **Evade DEP and ASLR protections**
- **Perform precision heap sprays**
- **Kernel Pool Exploitation**
- **NX/ASLR Bypass**

Required exam: Earning the OSEE requires passing one exam — the 72-hour OSEE exam.
Prerequisite: Prior to attempting this certification, Offensive Security requires taking the live, hands-on Advanced Windows Exploitation (AWE) course, which is administered every year at the Black Hat USA conference in Las Vegas.
Recommended experience: Offensive Security recommends an expert-level understanding of Windows, Linux, Bash scripting, basic Perl or Python skills, and a full understanding of TCP/IP and networking prior to attempting this exam.

How Much Does It Cost to Get Certified?

Offensive Security certification cost is all wrapped up in packages. Training and testing are purchased as one unit. It's not possible to take a course at an external provider, or sit for the test at an external testing company. Offensive Security certification exam cost is $800 for OSCP, $1,200 for OSCE, $1,400 for OSWE, and $450 for OSWP.

Offensive Security Recertification and Renewal

Offensive Security does not address this directly on their website, but the consensus from reputable sources on the internet is that their certifications do not expire and do not need renewal. Part of the reason may be that the course and exam focus on methods and strategies in security mitigation rather than specific technologies, which may change annually.

Penetration Tester Salary and Career Information

The average OSCP salary according to Payscale is $91,000. They list the following roles and salaries for OSCP-certified IT professionals (in USD):

- **Penetration Tester: $90,262**
- **Security Engineer: $97,151**
- **Security Consultant: $79,456**
- **Information Security Analyst: $74,950**
- **Cyber Security Engineer: $97,727**
- **Information Security Engineer: $98,870**
- **Senior Security Consultant: $107,351**

For an average penetration testing salary, Indeed puts the figure at $116,272. The earnings potential and job opportunities for a penetration tester in general, and an Offensive Security-certified individual in particular, both look pretty good.

Doing shift work in IT helpdesk or NOC jobs can be grueling enough. But from what these marathon exams look like, the penetration testing profession must be pretty demanding. You may be expected to get "wired in" and stay with an issue until you figure it out. What about sleep, you ask? Sleep's for babies they say — obviously not for dedicated penetration testers.

CBTnuggets

Offensive Security Training

CBT Nuggets doesn't offer Offensive Security certification training. However, every Offensive Security exams requires a strong foundation in networking, security, and Kali LInux. CBT Nuggets trainer Keith Barker has created the following Kali Linux and security training:

- **CompTIA Network+**
- **CompTIA Security+**
- **Penetration Testing Training with Kali Linux Tools**

All CBT Nuggets training either provides learners with custom virtual labs and supplemental files to learn technical concepts alongside the video training. Virtual labs were designed by experts to help learners gain hands-on experience in a sandbox environment.

CBT Nuggets learners should also take advantage of the Kaplan® IT Training Practice Exams included with a subscription to CBT Nuggets. Practice exams can either be taken timed or untimed, and provide a good baseline for learners to test their knowledge.

Additionally, Kaplan® IT Training Practice Exams evaluate a learner's strengths and weaknesses, so they know where to focus their attention while studying. Being successful taking certification exams requires quality instruction, hands-on experience, and practice with the exam itself.

CBTnuggets

(ISC)² Certifications

Cybersecurity is one of the highest priority issues facing enterprises today. Organizations face threats from all angles — data breaches, IoT device vulnerabilities, mobile malware, and more. What's more, there's a widening shortage of cybersecurity professionals.

(ISC)² is a not-for-profit organization focused on cybersecurity training and professional certification. (ISC)² certification programs are arguably the most comprehensive set of cybersecurity certifications in the industry. Here's the full list of (ISC)2 certifications:

- **(ISC)² CISSP - Certified Information Systems Security Professional**
- **(ISC)² SSCP - Systems Security Certified Practitioner**
- **(ISC)² CCSP - Certified Cloud Security Professional**
- **(ISC)² CAP - Certified Authorization Professional**
- **(ISC)² CSSLP - Certified Secure Software Lifecycle Professional**
- **(ISC)² HCISSP - HealthCare Information Security and Privacy Practitioner**
- **(ISC)² CISSP Concentrations**
- **Architecture: CISSP-ISSAP**
- **Engineering: CISSP-ISSEP**
- **Management: CISSP-ISSMP**

(ISC)² Certification Process

(ISC)² certifications are recognized worldwide as symbols of excellence in IT security. (ISC)² CISSP and (ISC)² CCSP certifications in particular are highly prized by employers and IT professionals alike. (ISC)² certifications provide employers with proof that potential employees have the cybersecurity skills and expertise needed to protect their enterprise systems, networks, and information.

(ISC)² has a rigorous multi-step process for candidates to achieve certification:

- **Satisfy designated work experience**
- **Take and pass a certification exam**
- **Complete the (ISC)² endorsement process**
- **Agree to support the (ISC)² Code of Ethics**
- **Pay initial (ISC)² Annual Maintenance Fee (AMF)***

*Members only pay a single AMF regardless of how many certifications they earn.

The (ISC)² certification path has an on-ramp for professionals who don't have the work experience prerequisite to becoming certified. Through the Associate of (ISC)² program, candidates can take any (ISC)² certification exam without the required work experience.

Associate of (ISC)² Designation

Work experience requirements for (ISC)² certifications are extensive and are policed rigorously. The requirements are set high — five (5) years for the CISSP and CCSP, four (4) years for the CSSLP, and two (2) years for CAP and HCISSP — in order to ensure the most experienced candidates for (ISC)² certification.

Recognizing the "chicken and the egg" nature of work experience, (ISC)² created the Associate of (ISC)² desigation. Through the Associate of (ISC)² program, candidates can take any (ISC)² certification exam without the required work experience.

Upon passing the exam, the person is eligible to become an Associate of (ISC)², as they work to gain the work experience required to become fully certified. Employers recognize that the Associate of (ISC)² has value and are consequently open to employment candidates who have earned this designation.

(ISC)² Certifications

(ISC)² has a broad portfolio of security certifications that are aligned with the (ISC)² Common Body of Knowledge (CBK) — a compendium of cybersecurity domain topics, which is updated annually to reflect the latest in IT security knowledge and practices.

(ISC)² offers six certifications:

- **Certified Information Systems Security Professional (CISSP)**
- **Systems Security Certified Practitioner (SSCP)**
- **Certified Cloud Security Professional (CCSP)**
- **Certified Authorization Professional (CAP)**
- **Certified Secure Software Lifecycle Professional (CSSLP)**
- **HealthCare Information Security and Privacy Practitioner (HCISSP)**

An important aspect of (ISC)² certification is that in addition to passing the required examination(s), there is an absolute requirement that individuals have prescribed years of relevant paid work experience in domain(s) in the Common Body of Knowledge (CBK).

(ISC)2 CERTIFICATION

(ISC)² Certified Information Systems Security Professional (CISSP)

The (ISC)² Certified Information Systems Security Professional (CISSP) is one of the most valued certifications available to IT security professionals. The (ISC)² CISSP validates a candidate's knowledge in eight security domains:

- **Security and Risk Management**
- **Asset Security**
- **Security Architecture and Engineering**
- **Communication and Network Security**
- **Identity and Access Management (IAM)**
- **Security Assessment and Testing**
- **Security Operations**
- **Software Development Security**

Required exam: Earning the (ISC)² CISSP certification requires passing one exam — the CISSP exam.
Prerequisites: Candidates who pass the CISSP exam, but do not have the required work experience, will become an Associate of (ISC)².
Required experience: Candidates must have a minimum of five (5) years cumulative paid work experience. Candidates may satisfy one year of the required experience with a four-year college degree or equivalent credential.

The (ISC)² CISSP meets the requirements of U.S. Department of Defense (DoD) Directive 8570.1.

(ISC)2 CERTIFICATION

(ISC)² Systems Security Certified Practitioner (SSCP)

The (ISC)² Systems Security Certified Practitioner (SSCP) is designed for IT administrators, managers, directors and network security professionals who have hands-on operational responsibility for security of their organization's data, systems, and networks. The (ISC)² SSCP validates a candidate's knowledge in seven security domains:

- **Access Controls**
- **Security Operations and Administration**
- **Risk Identification, Monitoring and Analysis**
- **Incident Response and Recovery**
- **Cryptography**
- **Network and Communications Security**
- **Systems and Application Security**

Required exam: Earning the (ISC)² SSCP certification requires passing one exam — the SSCP exam.
Prerequisites: Candidates who pass the SSCP exam, but do not have the required work experience will become an Associate of (ISC)². They then have two (2) years in which to gain the one year of required experience and be awarded the SSCP certification.
Required experience: Candidates must have a minimum of one (1) year cumulative work experience. Candidates who hold an accredited degree from a cybersecurity program may be deemed to have satisfied their one year work experience requirement.

(ISC)2 CERTIFICATION

(ISC)² Certified Cloud Security Professional (CCSP)

The (ISC)² Certified Cloud Security Professional (CCSP) is reported to be the industry's leading cloud security certification. The certification is designed for IT and security leaders who are responsible for cloud security architecture, design, operations, and service orchestration. The (ISC)² CCSP validates a candidate's knowledge in six security domains:

- **Architectural Concepts and Design Requirements**
- **Cloud Data Security**
- **Cloud Platform and Infrastructure Security**
- **Cloud Application Security**
- **Operations**
- **Legal and Compliance**

Required exam: Earning the (ISC)² CCSP certification requires passing one exam — the CCSP exam.
Prerequisites: Candidates who pass the CCSP exam, but do not have the required work experience, will become an Associate of (ISC)².
Required experience: Candidates must have a minimum of five (5) years cumulative work experience. The (ISC)² CISSP credential can be substituted for the entire CCSP work experience requirement. The CCSP CCSK can be substituted for the requirement for one year of experience.

(ISC)2 CERTIFICATION

(ISC)² Certified Authorization Professional (CAP)

The (ISC)² Certified Authorization Professional (CAP) is designed for IT security and information assurance practitioners in U.S. military, government contractors, as well as state and local government. The (ISC)² CAP validates a candidate's knowledge in seven security domains:

- **Information Security Risk Management Program**
- **Categorization of Information Systems (IS)**
- **Selection of Security Controls**
- **Implementation of Security Controls**
- **Assessment of Security Controls**
- **Authorization of Information Systems (IS)**
- **Continuous Monitoring**

Required exam: Earning the (ISC)² CAP certification requires passing one exam — the CAP exam.
Prerequisites: Candidates who pass the CAP exam, but do not have the required work experience will become Associates of (ISC)². They then have three (3) years in which to gain the two (2) years required experience and be awarded the CAP certification.
Required experience: Candidates must have a minimum of two (2) years cumulative work experience in one or more of the seven domains of the CAP CBK.

(ISC)2 CERTIFICATION

(ISC)² Certified Secure Software Lifecycle Professional (CSSLP)

The (ISC)² Certified Secure Software Lifecycle Professional (CSSLP) is designed for software development and security professionals who are responsible for applying best practices to each phase of the SDLC. The (ISC)² CSSLP validates a candidate's knowledge in eight security domains:

- **Secure Software Concepts**
- **Secure Software Requirements**
- **Secure Software Design**
- **Secure Software Implementation/Programming**
- **Secure Software Testing**
- **Secure Lifecycle Management**
- **Deployment, Operations, and Maintenance**
- **Supply Chain and Software Acquisition**

Required exam: Earning the (ISC)² CSSLP certification requires passing one exam — the CSSLP exam.
Prerequisites: Candidates who pass the CSSLP exam, but do not have the required work experience will become an Associate of (ISC)².
Required experience: Candidates must have a minimum of four (4) years cumulative paid full-time Software Development Lifecycle work experience in one or more of the eight domains of the CSSLP CBK. Candidates who hold an accredited four-year degree in IT related field may be deemed to have satisfied one (1) year of the four (4) year work experience requirement.

(ISC)2 CERTIFICATION

(ISC)² HealthCare Information Security and Privacy Practitioner (HCISSP)

The (ISC)² HealthCare Information Security and Privacy Practitioner (HCISPP) is designed for information security and health management professionals who are responsible for guarding patients' protected health information (PHI). The (ISC)² HCISPP validates a candidate's knowledge in seven security domains:

- **Healthcare Industry**
- **Information Governance in Healthcare**
- **Information Technologies in Healthcare**
- **Regulatory and Standards Environment**
- **Privacy and Security in Healthcare**
- **Risk Management and Risk Assessment**
- **Third-Party Risk Management**

Required exam: Earning the (ISC)² HCISPP certification requires passing one exam — the HCISPP exam.
Prerequisites: Candidates who pass the HCISPP exam, but do not have the required work experience will become an Associate of (ISC)². They then have three (3) years to gain the two (2) years of required experience and be awarded the HCISPP certification.
Required experience: Candidates must have a minimum of two (2) years cumulative paid work experience with at least one of those years in the healthcare industry.

How Much Does It Cost to Get (ISC)² Certified?

Your cost to be (ISC)² certified includes the (ISC)² certification exam cost, plus your $125 (ISC)² annual maintenance fee (AMF) for the three (3) years that the credential is valid. For example, in the Americas, the CISSP certification cost would be a total of $1074 — $699 for the exam plus $375 in AMFs.

(ISC)² exam prices are normally $599 in the Americas, with the CISSP exam costing $699 and the SSCP exam costing $249. Beyond the exam, you'll also need to budget for the costs involved in continuing professional education (CPE) credits needed to keep the certification valid.

Associates of (ISC)² are on a one-year certification cycle and are required to earn and submit 15 CPE credits each year — plus pay their $50 AMF.

Renewal of the CISSP certification requires a total of 120 CPE credits over the three-year certification cycle, with a recommended 40 credits per year. For holders of one or more of the CISSP concentration credentials — CISSP-ISSAP, CISSP-ISSEP, or CISSP-ISSMP — 20 CPE credits in the CISSP three-year cycle must be directly related to each concentration held.

For more information on CPE credits required to recertify and renew each (ISC)² certification, download the (ISC)² Continuing Professional Education Handbook.

(ISC)² Recertification and Renewal

(ISC)² certifications are valid for three years and may be renewed by earning and submitting continuing professional education (CPE) credits for each year of the three-year certification cycle. For each (ISC)² certification, there is a minimum number of CPE credits — with a suggested minimum number per year — required before the certification expires. Remember of course that holders must also be current with paying their annual maintenance fee (AMF).

(ISC)² Certification Salary and Career Information

There's never been a bad time to be in security, but with the shortage of cybersecurity professionals, now is a particularly good time to earn (ISC)² certification.

(ISC)² certification are highly regarded credentials for IT security professionals and this is reflected in (ISC)² certification salary expected. In Certification Magazine's last survey of certification salaries, eight (ISC)² certifications made the top 30 average salaries. The three CISSP Concentrations — CISSP-ISSEP,

CISSP-ISSAP, and CISSP-ISSMP — came in third, sixth and seventh, respectively. The (ISC)² Certified Secure Software Lifecycle Professional (CSSLP) came in fourth. Also in the Top 30 were the Certified Information Systems Security Professional (CISSP), the Certified Cloud Security Professional (CCSP), the HealthCare Information Security and Privacy Practitioner (HCISSP), and the Certified Authorization Professional (CAP).

A review of the certification data collected by PayScale, shows that even the Associate of (ISC)² credential is of value, with an average salary of $65,000. Moving along the (ISC)² certification path, an average salary of $74,000 is reported for holders of the System Security Certified Practitioner (SSCP) certification.

The premier (ISC)² Certified Information Systems Security Professional (CISSP) certification commands a $109,000 average salary, while the CISSP Concentrations have yearly salaries of $155,000 for management professionals (CISSP-ISSMP), $129,000 for security architects (CISSP-ISSAP), and $142,000 for security engineers (CISSP-ISSEP).

Government organizations and contractors are popular employers, which is not surprising given that Associate of (ISC)², SSCP, CISSP, the CISSP Concentrations (CISSP-ISSAP, CISSP-ISSEP, CISSP-ISSMP), and CSSLP are all DOD 8570-approved baseline certifications.

(ISC)² Certification Training

Good luck to you as you start on your (ISC)² certification path. CBT Nuggets has video training that supports the (ISC)² certification programs for the (ISC)² CISSP, as well as the (ISC)² System Security Certified Practitioner (SSCP).

- **(ISC)2 CISSP training**

Our training does change occasionally, so be sure to check CBT Nuggets for new or updated (ISC)² certification training that's relevant to your personal goals.

CBTnuggets

Check Point Certification Guide

Check Point is recognized around the world as a leading provider of hardware and software security products. Check Point security certification validates an IT professional's knowledge and skills in security management using Check Point products. It is a valuable credential for those seeking advancement in the field of IT security.

The Check Point certification path includes four certifictions at three levels of certification that are designed to take learners' skill sets from beginner to expert:

- **Check Point Certified Security Administrator R80 (CCSA R80)**
- **Check Point Certified Security Expert R80 (CCSE R80)**
- **Check Point Certified Master R80 (CCSE R80)**
- **Check Point Managed Security Expert R77 (CCSME R77)**

Check Point Certifications

The Check Point certification system is currently in transition from R77 to R80. Levels for R80 include CCSA, CCSE, and CCMSE. There may be some confusion between the Checkpoint and Pearson Vue websites, but those wishing to pursue Check Point certifications going forward should focus on the new R80 exams.

Check Point offers four certifications:

- **Check Point Certified Security Administrator R80 (CCSA R80)**
- **Check Point Certified Security Expert R80 (CCSE R80)**
- **Check Point Certified Master R80 (CCSE R80)**
- **Check Point Managed Security Expert R77 (CCSME R77)**

CHECK POINT ADMINISTRATOR

Check Point Certified Security Administrator R80 (CCSA R80)

The Check Point Certified Security Administrator (CCSA) R80 certification is designed for IT professionals with a basic understanding of Check Point implementations. The CCSA is the lowest level on the Check Point certification path, and it deals with various security administration tasks on Check Point hardware and software. The CCSA R80 certification validates a candidate's understanding of these Check Point topics and skills:

- **Check Point Technology Overview**
- **Security Policy Management**
- **Traffic Monitoring**
- **Network Address Translations**
- **Basic Concepts of VPN**
- **Managing User Access**
- **Working with ClusterXL**
- **Administrator Task Implementation**

Required exam: Earning the CCSA R80 certification requires passing one exam — CCSA R80 (156-215.80).
Prerequisites: None.
Recommended experience: Check Point recommends 6 to 12 months of hands-on experience with Check Point products, and a good understanding of networking and TCP/IP before attempting this exam.

CHECK POINT EXPERT

Check Point Certified Security Expert R80 (CCSE R80)

The CCSE R80 certification is designed for IT professionals who know their way around Windows and UNIX servers, and know how to build, test and troubleshoot numerous deployment scenarios.
The CCSE R80 certification validates a candidate's understanding of these Check Point topics and skills:

- **Check Point Technology Overview**
- **Deployment Platforms and Security Policies**
- **Monitoring Traffic and Connections**
- **Network Address Translations**
- **User Management and Authentication**
- **Using SmartUpdate**
- **Implementing Identity Awareness**
- **Configuring VPN Tunnels**
- **Resolving Security Administration Issues**

Required exam: Earning the CCSE R80 certification requires passing one exam — CCSE R80 (156-315.80).
Prerequisites: Prior to attempting this certification, candidates must earn the CCSA R80 certification. Candidates who have already earned the CCSA R77 must still earn the CCSA R80 certification.
Recommended experience: Check Point recommends candidates have extensive hands-on experience with Check Point products, strong networking, Window, and UNIX server management skills, and a good understanding of security certificate management.

CHECK POINT MASTER

Check Point Certified Master R80 (CCSM R80)

The CCSM R80 certification is designed for IT professionals who have developed the highest skills in the management and implementation of Check Point products and technologies. Candidates should know how to approach common deployment scenarios and how to apply common troubleshooting practices.
The CCSM R80 certification validates a candidate's understanding of these Check Point topics and skills:

- **Policy Changes to Security Implementations**
- **UGI Client Connectivity**
- **Secure Internal Communications**
- **VPN Tunnel Interfaces**
- **IPv6 Deployment**
- **Check Point Commands**
- **Open Shortest Path First (OSPF)**
- **Network Address Translation (NAT)**
- **ClusterXL Debug File**

Required exam: Earning the CCSM R80 certification requires passing one exam — CCSM R80 (156-115.80).
Prerequisites: Prior to attempting this certification, candidates must earn either the CCSE R77 or CCSE R80 certification.
Recommended experience: Check Point recommends candidates have extensive hands-on experience with Check Point products, and advanced networking, server management, and security skills.

CHECK POINT EXPERT

Check Point Managed Security Expert R77 (CCMSE R77)

The CCMSE R77 certification is designed for experienced IT professionals who are interested in multi-domain security management. Candidates will need to be able to handle different deployment scenarios and implementation tasks. The CCMSE R77 certification certification validates a candidate's understanding of these Check Point topics and skills:

- **Multi-domain Security Management Installation and Configuration**
- **Common Deployment Scenarios**
- **Traffic Inspection Process**
- **Configuration of Domain Management Server (DMS) High Availability**
- **Configuration and Implementation of Global Policy**
- **Common Troubleshooting Practices**

Required exam: Earning the CCMSE R77 certification requires passing one exam — Multi-Domain Security Management with VSX (156-820.77).
Prerequisites: Prior to attempting this certification, candidates must earn the CCSE 75, CCSE R77, or CCSE R80 certification.
Recommended experience: Check Point recommends candidates have extensive hands-on experience with Check Point products, and advanced networking, server management, and security skills.

How Much Does It Cost to Get Check Point Certified?

Check Point certification exam cost depends on the exam taken and your location. In the U.S., the cost for the CCSA and CCSE exams is $250 each, and the CCSM exam costs $350 according to the Check Point website. All Check Point exams are multiple choice, contain as many as 90 questions, and have a 90-minute time limit.

Check Point Recertification and Renewal

Check Point certifications expire after only two (2) years. Certifications, like security, must be kept current to be truly effective, which is why we strongly encourage you to constantly refresh and keep your certification current.

Because the exams are updated so frequently, be prepared to retake exams when a new version comes out. For instance, currently there is a transition from R77 to R80. It is up to the individual learner to monitor the changes and updates to the Check Point certification system.

Check Point Certification Salary and Careers

According to Payscale, IT professionals with a Check Point Certified Security Administrator (CCSA) certification can expect to earn around $89,000 per year. A Check Point CCSE makes an average of $103,000 per year. Similar figures are not available for CCSM, but one might expect it to be even higher.

CBTNuggets considers the CCSA as one of the easier certifications to get for those trying to break into the information security field. And CCSA certification cost is reasonable compared to other certifications. Taking into account the earnings potential for Check Point certified IT professional, it's well worth considering.

Check Point Certification Training

CBT Nuggets current offers the following Check Point video training by trainer Keith Barker:

- Check Point CCSA R80
- Check Point CCSA GAiA 156-215.76

Keith has more than three decades experience in IT and holds numerous IT security certifications.

Please note that CBT Nuggets constantly updates its training content library, meaning learners should check regularly for new Check Point training.

In addition to quality, entertaining video training created by expert-level trainers, CBT Nuggets provides everything a learner needs to study for IT certification exams, including virtual labs, supplemental files, practice exams, and access to a robust Learner Community.

All CBT Nuggets training provides learners with custom virtual labs or supplemental files to learn technical concepts alongside the video training. Virtual labs were designed by experts to help learners gain hands-on experience in a sandbox environment. NuggetLab supplemental files include practice commands, configuration files, and network diagrams — everything a learner needs to study for a certification exam.

CBT Nuggets learners should also take advantage of the Kaplan® IT Training Practice Exams included with a subscription to CBT Nuggets. Practice exams can either be taken timed or untimed, and provide a good baseline for learners to test their knowledge. Additionally, Kaplan® IT Training Practice Exams evaluate a learner's strengths and weaknesses, so they know where to focus their attention while studying.

CBTnuggets

CompTIA Certification Guide

CompTIA is a non-profit organization with membership comprising more than 200 leading IT companies and 2,000 member companies.

As an IT industry trade organization, a CompTIA goal is to help ensure that there is a strong pool of IT professionals with the skills required to drive the adoption and use of information technologies in enterprises worldwide. CompTIA is the leading provider of vendor-neutral training and certification programs for those IT professionals, having issued more than two million certificates to date.

CompTIA certificate programs have been established for IT support, networking, security, open-source (Linux) development, and cloud. In addition to technical certifications, additional professional CompTIA certificate programs are available for business professionals, non-IT staff, and technical trainers.

This guide contains a comprehensive introduction to the various CompTIA certificate

programs, recommended CompTIA certification paths, the costs associated with CompTIA certificate programs, and insights into job opportunities related to the CompTIA certification list.

- **What is CompTIA Certification?**
- **CompTIA Core Certifications**
- **CompTIA Infrastructure Certifications**
- **CompTIA Cybersecurity Certifications**
- **Additional Professional CompTIA Certifications**
- **CompTIA Stackable Certifications**
- **How Much Does CompTIA Certification cost?**
- **CompTIA Recertification and Renewal**
- **CompTIA Certification Salary and Career Information**
- **How Do I Get a Copy of My CompTIA Certification?**
- **CompTIA Certification Training**

We'll also describe how CompTIA certifications — and in particular CompTIA Stackable Certifications — play a key role in IT career development.

What is CompTIA Certification?

Unlike vendor certifications, CompTIA certifications are vendor-neutral certifications, which means they can applied universally, regardless of vendor. For example, someone with CompTIA Network+ certification should apply their knowledge and skills to Cisco or Juniper networking technologies — at a basic level.

The CompTIA certification program encompasses certs in four categories:

- **CORE**
- **INFRASTRUCTURE**
- **CYBERSECURITY**
- **PROFESSIONAL**

In their CompTIA Certification Roadmap, CompTIA sees the three technical certification categories as a progression — as IT professionals build on their skills from Core to Infrastructure and then to Cybersecurity. A number of the certs on the CompTIA Certification list are U.S. Department of Defense-approved baseline certifications (DoD 8570.01-M). This can provide certified professionals with job opportunities in the Federal government sector.

CompTIA Core Certifications

CompTIA Core Certifications are for beginners and entry-level IT professionals. There are four CompTIA Core Certifications:

- **CompTIA IT Fundamentals+**
- **CompTIA A+**
- **CompTIA Network+**
- **CompTIA Security+**

CompTIA A+, CompTIA Network+, and CompTIA Security+ are all DoD 8570.01-M -approved certifications.

COMPTIA CORE

CompTIA IT Fundamentals+

CompTIA IT Fundamentals+ is designed for individuals who want to begin exploring a career in IT. It's also a good option for business, sales, and marketing professionals who work closely with systems and information technology.

The IT Fundamentals+ certification validates a candidate's understanding of these topics:

- **Computing**
- **IT infrastructure**
- **Software development**
- **Database use**

Required exam: Earning the CompTIA IT Fundamentals+ certification requires passing one exam — CompTIA IT Fundamentals+ (FC0-U61).
Prerequisites: None.
Recommended experience: CompTIA recommends this exam for advanced end users or individuals thinking about entering the IT field. That means you should feel comfortable using computer systems and networks.

COMPTIA CORE

CompTIA A+

The CompTIA A+ certification is designed for people who want to build a career in IT technical support and operations. The A+ certification validates a candidate's ability to:

- **Identify, use, and connect hardware components**
- **Install and support Windows OS**
- **Troubleshoot PC and mobile device issues**
- **Explain types of networks and connections**
- **Troubleshoot device and network issues**
- **Identify and protect against security vulnerabilities**
- **Install & configure laptops and other mobile devices**
- **Understand Mac OS, Linux, and mobile OS**

Required exams: Earning the CompTIA A+ certification requires passing two exams — CompTIA A+ 220-1001 and CompTIA A+ 220-1002.
Prerequisites: None.
Recommended experience: While there are no specific prerequisites for the exams, CompTIA recommends that candidates have 9 to 12 months hands-on experience with various mobile, desktop, and networking tasks.

COMPTIA CORE

CompTIA Network+

The CompTIA Network+ certification is designed for IT professionals with entry-level experience. Network+ is a common stepping stone common to move into network administration. Given that almost everything is networked, networking experience is a valuable asset for any IT professional. The Network+ certification validates the candidate's ability to:

- **Implement networking concepts**
- **Determine the appropriate cabling, device and storage technologies**
- **Use best practices to manage a network**
- **Summarize physical security, and common wired and wireless attacks**
- **Explain the network troubleshooting methodology**

Required exam: Earning the CompTIA Network+ certification requires passing one exam — CompTIA Network+ (N10-007).
Prerequisites: None.
Recommended experience: While are no specific prerequisites for the exam, CompTIA recommends that candidates have obtained CompTIA A+ certification and at least 9 to 12 months of networking experience.

COMPTIA CORE

CompTIA Security+

The CompTIA Security+ certification validates the baseline cybersecurity skills required of IT administrators and security professionals. The Security+ certification validates the candidate's ability to:

- **Detect various types of threats, attacks and vulnerability**
- **Install, configure, and deploy network security components**
- **Implement a secure network architecture**
- **Install, configure, and manage identity and access services**
- **Implement risk management procedures to mitigate business impact**
- **Install and configure wireless security settings and implement public key infrastructure**

Required exam: Earning the CompTIA Security+ certification requires passing one exam — CompTIA Security+ (SY0-501).
Prerequisites: None.
Recommended experience: There are no specific prerequisites for the exam, although CompTIA recommends that candidates have obtained CompTIA Network+ certification and two years of experience in IT administration with a security focus.

CompTIA Infrastructure Certifications

The next level of the CompTIA certification program consists of the CompTIA Infrastructure Certifications. As the name suggests, these certs are related to key infrastructure technologies such as cloud computing, open source operating systems, and servers. There are three certs at this level:

- **CompTIA Cloud+**
- **CompTIA Linux+**
- **CompTIA Server+**

COMPTIA INFRASTRUCTURE

CompTIA Cloud+

The CompTIA Cloud+ certification validates that a certified professional has the expertise needed for a cloud data center job. Typical job titles that may require CompTIA Cloud+ certification include sysadmins, network administrator, cloud engineer, systems or network engineer, and data center manager. The Cloud+ certification validates the candidate's ability to:

- **Analyze system requirements to successfully execute workload migrations to the cloud**
- **Determine proper allocation of cloud resources**
- **Apply appropriate technologies and processes**
- **Implement appropriate security controls given requirements**
- **Troubleshoot capacity, automation, connectivity and security issues related to cloud implementations**

Required exam: Earning the CompTIA Cloud+ certification requires passing one exam — CompTIA Cloud+ (CV0-002).
Prerequisites: None.
Recommended experience: While there are no specific prerequisites for the exam, CompTIA recommends that candidates have at least 2 to 3 years of experience in system administration.

COMPTIA INFRASTRUCTURE

CompTIA Linux+

The CompTIA Linux+ certification is designed for IT professionals with hands-on experience configuring, monitoring, and supporting servers running major Linux distributions. The Linux+ certification validates the candidate's ability to:

- **Configure Linux kernel modules, network parameters, storage, cloud, and virtualization technologies**
- **Manage software and services**
- **Manage permissions and authentication, firewalls, and file management**
- **Troubleshoot user, app, and hardware issues**
- **Use Linux automation & scripting**

Required exams: Earning the CompTIA Linux+ certification requires passing one exam — CompTIA Linux+ (XK0-004).
Prerequisites: None.
Recommended experience: While there are no specific prerequisites for the exam, CompTIA recommends that candidates have CompTIA A+ and CompTIA Network+ certifications, as well as 12 months of experience in Linux administration.

COMPTIA INFRASTRUCTURE

CompTIA Server+

The CompTIA Server+ certification is designed for IT professionals with hands-on experience administering, troubleshooting, and securing those servers regardless of type or location. Server+ is the only vendor-neutral certification covering the major server platforms. The Server+ certification validates the candidate's ability to:

- **Configure and support server components**
- **Manage and maintain servers**
- **Support storage devices technologies, including capacity and growth planning**
- **Apply physical and network data security techniques**
- **Configure systems for network connectivity**
- **Understand disaster recovery and implement backup techniques**
- **Diagnose and resolve system hardware, software, connectivity, storage, and security issues**

Required exam: Earning the CompTIA Server+ certification requires passing one exam — CompTIA Server+ (SK0-004).
Prerequisites: None.
Recommended experience: While there are no specific prerequisites for the exam, CompTIA recommends that candidates have obtained CompTIA A+ certification and have 18 to 24 months of IT experience.

CompTIA Cybersecurity Certifications

CompTIA Cybersecurity certifications make up the final step of the CompTIA technical certification path. These certifications are for advanced and expert-level professionals. There are three certs at this tier:

- **CompTIA Cybersecurity Analyst (CySA+)**
- **CompTIA PenTest+**
- **CompTIA Advanced Security Practitioner (CASP+)**

CompTIA CySA+ and CASP+ are both DoD 8570.01-M-approved certifications.

COMPTIA CYBERSECURITY

CompTIA CySA+

The Cybersecurity Analyst (CySA+) certification is designed for cybersecurity professionals who use an analytics-based approach to identify and combat malware and advanced persistent threats (APTs). As hackers continue to evade traditional signature-based solutions such as firewalls, the IT security industry is moving toward an analytics-based approach.
The CySA+ certification validates the candidate's ability to:

- **Implement a vulnerability management process**
- **Perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization**
- **Configure and use threat-detection tools**
- **Secure and protect applications and systems within an organization**

Required exam: Earning the CompTIA CySA+ certification requires passing one exam — CompTIA CySA+ (CS0-001).
Prerequisites: None.
Recommended experience: While not required in order to take the CompTIA CySA+, CompTIA recommends that candidates either have a CompTIA Network+ or Security+ certification, or at least three years of hands-on experience in information security.

COMPTIA CYBERSECURITY

CompTIA PenTest+

The CompTIA PenTest+ certification is designed for intermediate-level cybersecurity professionals who are tasked with penetration testing to manage vulnerabilities on a network. The PenTest+ certification validates the candidate's ability to:

- **Plan a comprehensive compliance-based vulnerability assessment**
- **Perform a vulnerability scan and analyze results**
- **Exploit network, wireless, application, and RF-based vulnerabilities, summarize physical security attacks, and perform post-exploitation techniques**
- **Conduct information gathering exercises with various penetration testing tools**
- **Utilize report-writing and handling best practices**

Required exam: Earning the CompTIA PenTest+ certification requires passing one exam — CompTIA PenTest+ (PT0-001).
Prerequisites: None.
Recommended experience: While not required in order to take the CompTIA PenTest+ exam, CompTIA recommends that candidates have CompTIA Network+ or Security+ certification, and at least three years of hands-on information security or related experience.

CYBERSECURITY CERTIFICATION

CompTIA CASP+

The CompTIA CASP+ certification is designed for expert cybersecurity professionals who implement security solutions. While cybersecurity managers identify the cybersecurity policies and frameworks that need to be implemented, cybersecurity technical practitioners implement solutions within those policies and frameworks. The CASP+ certification validates the candidate's ability to:

- **Analyze security risks and frameworks that come along with specific industry threats**
- **Integrate network and security components and implement security controls**
- **Implement incident response and recovery procedures**
- **Integrate hosts, storage, networks and applications into a secure enterprise architecture**
- **Apply research methods to determine industry trends and their impacts to the enterprise**

Required exam: Earning the CompTIA CASP+ certification requires passing one exam — CompTIA CASP+ (CAS-003).
Prerequisites: None.
Recommended experience: CompTIA recommends that candidates have at least 10 years of IT administration experience, including at least five years of hands-on technical security experience.

Professional CompTIA Certifications

In addition to technical certifications, CompTIA offers certifications for non-technical professionals. The three professional certifications in the CompTIA certification path are:

- **CompTIA Project+**
- **CompTIA CTT+**
- **CompTIA Cloud Essentials**

COMPTIA PROFESSIONAL

CompTIA Project+

The CompTIA Project+ certification is designed for IT and project management professionals who need to manage smaller, less complex projects as part of their other job duties. There's a need for business professionals — within and outside of IT — who have the basic skills and knowledge to successfully manage small- to medium-sized projects.

The Project+ certification validates the candidate's ability to:

- **Manage the project life cycle**
- **Ensure appropriate communication**
- **Manage resources and stakeholders**
- **Maintain project documentation**

Required exam: Earning the CompTIA Project+ certification requires passing one exam — CompTIA Project+ (PK0-004).
Prerequisites: None.
Recommended experience: CompTIA recommends that candidates have at least 12 months of cumulative project management experience or equivalent education.

COMPTIA PROFESSIONAL

CompTIA CTT+

The CompTIA Certified Technical Trainer (CTT+) certification is designed for technical instructors. Education is an essential element in the successful roll-out and ongoing operation of any IT initiative. Effective training requires teachers who can use appropriate tools and techniques in physical and virtual learning environments.

Required exam: In order to become CompTIA CTT+ certified, candidates must pass two exams — one written and one performance-based:

- CTT+ Essentials (TK0-201) Exam, plus
- CTT+ Classroom Performance Based Exam (TK0-202), or
- CTT+ Virtual Classroom Performance Based Exam (TK0-203)

As part of the TK0-202 and TK0-203 exams, candidates must submit a video recording of their classroom training sessions for evaluation.

Recommended experience: CompTIA recommends that candidates have at least 6 to 12 months of training experience.

COMPTIA PROFESSIONAL

CompTIA Cloud Essentials

The CompTIA Cloud Essentials+ certification is designed to provide business professionals and non-IT staff an understanding of cloud computing fundamentals and the work involved to move to and govern the cloud. The Cloud Essentials+ exam validates the candidate's ability to:

- **Understand cloud principles and can aptly identify cloud networking concepts and storage techniques, and understand cloud design aspects**
- **Comprehend the financial aspects of engaging a cloud provider, as well as the business aspects of managing vendor relations in cloud adoptions**
- **Are able to explain aspects of operating within the cloud, such as data management, availability, and monitoring**
- **Understand risk management concepts related to cloud services and identify the importance and impacts of compliance in the cloud**

Required exam: Earning the CompTIA Cloud Essentials+ certification requires passing one exam — CompTIA Cloud Essentials (CLO-001).

Prerequisites: None.

Recommended experience: CompTIA recommends that candidates for the CompTIA Cloud Essentials exam have at least 6 to 12 months of exposure to cloud technologies.

CompTIA Stackable Certifications

CompTIA recognizes that IT pros build their technical proficiencies incrementally, gaining experience as they become established IT professionals.

As they progress in their careers, IT professionals can acquire multiple CompTIA certifications that combine to represent expertise in specific functional areas. CompTIA has formalized this "bundling of certs" as CompTIA Stackable Certifications. They have taken specific job functions and identified the stacks of certifications that are most relevant to each job.

The job functions are concentrated in one of two CompTIA certification pathways — Infrastructure and Cybersecurity — depending on the career direction an IT pro wants to take.

The job functions for the CompTIA Stackable Certifications are further categorized by the expected experience level of the job — specialist, professional, or expert:

- **Specialist:** Early-career IT professionals with 0–2 years of experience
- **Professional:** Mid-level IT professionals with 2–5 years of experience
- **Expert:** Established IT professionals with 5+ years of experience

Stackable Infrastructure Certifications

The CompTIA Infrastructure Career Pathway is for IT professionals who want to work with organizations' system and network infrastructures — servers, networks, data centers, cloud services, etc. There are five job functions that are represented by sets of CompTIA stackable certifications.

- **CompTIA IT Operations Specialist (CIOS)**
- **CompTIA Systems Support Specialist (CSSS)**
- **CompTIA Cloud Admin Professional (CCAP)**
- **CompTIA Network Infrastructure Professional (CNIP)**
- **CompTIA Linux Network Professional (CLNP)**

COMPTIA STACKABLE SPECIALIST

CompTIA IT Operations Specialist (CIOS)

The CompTIA IT Operations Specialist stackable certification is designed for IT operations specialists who regularly create and respond to tickets, maintain systems, and resolve customer issues.

Required exams: To earn the CIOS stackable certification, you must pass both CompTIA A+ and Network+ certifications.

COMPTIA STACKABLE SPECIALIST

CompTIA Systems Support Specialist (CSSS)

The CompTIA Systems Support Specialist stackable certification is designed for support specialists who support help desk operations and assist customers with issues related to hardware, software, and networks.

Required exams: To earn the CSSS stackable certification, you must earn both CompTIA A+ and Linux+ certifications.

COMPTIA STACKABLE PROFESSIONAL

CompTIA Network Infrastructure Professional (CNIP)

The CompTIA Network Infrastructure Professional stackable certification is designed for networking professionals who design and implement infrastructure projects.

Required exams: To earn the CNIP stackable certification, you must pass both CompTIA Network+ and Server+.

COMPTIA STACKABLE PROFESSIONAL

CompTIA Cloud Admin Professional (CCAP)

The CompTIA Cloud Admin Professional stackable certification is designed for IT professionals who regularly work with cloud service implementation and maintenance.

Required exams: To earn the CCAP stackable certification, you must earn both CompTIA Network+ and Cloud+ certifications.

COMPTIA STACKABLE PROFESSIONAL

CompTIA Linux Network Professional (CLNP)

The CompTIA Linux Network Professional stackable certification is designed for IT professionals that regularly support and monitor systems that operate on Linux.

Required exams: To earn the CLNP stackable certification, you must earn both CompTIA Network+ and Linux+ certifications.

CompTIA Cybersecurity Career Pathway

The CompTIA Cybersecurity Career Pathway is aimed at IT professionals who choose to specialize in the field of cybersecurity. There are seven sets of CompTIA stackable certifications for cybersecurity.

- **CompTIA Secure Infrastructure Specialist (CSIS)**
- **CompTIA Secure Cloud Professional (CSCP)**
- **CompTIA Security Analytics Professional (CSAP)**
- **CompTIA Network Vulnerability Assessment Professional (CNVP)**
- **CompTIA Network Security Professional (CNSP)**

COMPTIA STACKABLE SPECIALIST

CompTIA Secure Infrastructure Specialist (CSIS)

The CompTIA Secure Infrastructure Specialist stackable certification is designed for security professionals who primarily support hardware and software systems.

Required exams: To earn the CSIS stackable certification, you must earn CompTIA A+, Network+ and Security+ certifications.

COMPTIA STACKABLE PROFESSIONAL

CompTIA Secure Cloud Professional (CSCP)

The CompTIA Secure Cloud Professional stackable certification is designed for security professionals that primarily work with cloud applications and services.

Required exams: To earn the CSCP stackable certification, you must pass CompTIA Security+ and Cloud+ certifications.

COMPTIA STACKABLE PROFESSIONAL

CompTIA Security Analytics Professional (CSAP)

The CompTIA Security Analytics Professional stackable certification validates that security professionals can monitor for security events and enact measures to protect their network and systems.

Required exams: To earn the CSAP stackable certification, you must earn the CompTIA Security+ and CySA+ certifications.

COMPTIA STACKABLE PROFESSIONAL

CompTIA Network Vulnerability Assessment Professional (CNVP)

The CompTIA Network Vulnerability Assessment Professional stackable certification validates that security professionals can scan applications and systems for vulnerabilities.

Required exams: To earn the CNVP stackable certification, you must earn the CompTIA Security+ and PenTest+ certifications.

COMPTIA STACKABLE PROFESSIONAL

CompTIA Network Security Professional (CNSP)

The CompTIA Network Security Professional stackable certification validates that security professionals can monitor networks for threats and vulnerabilities, as well as actively respond to those threats.

Required exams: To earn the CNSP stackable certification, you must pass CompTIA Security+, PenTest+, and CySA+ certifications.

COMPTIA STACKABLE EXPERT

CompTIA Security Analytics Expert (CSAE)

The CompTIA Security Analytics Expert stackable certification validates that security professionals can research and find vulnerabilities through data — and then engineer solutions.

Required exams: To earn the CSAE stackable certification, you must earn CompTIA Security+, CySA+, and CASP certifications.

COMPTIA STACKABLE EXPERT

CompTIA Security Infrastructure Expert (CSIE)

The CompTIA Security Infrastructure Expert stackable certification validates that security professionals can lead and manage every element of security infrastructure for large, complex organizations.

Required exams: To earn the CSIE stackable certification, you must earn CompTIA Security+, CySA+, PenTest+, and CASP certifications.

Getting Your CompTIA Stackable Certifications

When you complete the set of CompTIA certifications that represent a particular CompTIA Stackable Certification, you will be automatically granted the relevant stackable certification(s). These will be found in the Stackable Certifications tab on your CompTIA certification account. You'll be able to download the stackable certification logo for your personal professional use.

Stackable certifications require active continuing education (CE) certifications. Good-for-life certification holders may earn these stackable certifications by re-certifying and validating that their skills are up to date.

How Much Does CompTIA Certification Cost?

CompTIA certification exams range in cost between $219 and $349, depending on the exam. For CompTIA A+, you must pass two exams for a total cost of $438. For CompTIA Security+, the single CompTIA certification exam costs $339. The cost for the CompTIA Network+ exam is $319.

How Do I Get a Copy of My CompTIA Certification?

What happens if you need verification of your CompTIA certification(s) for a job application, for your resume, or to submit to a potential client? Through your CompTIA certification account (login here if you have one) CompTIA provides two ways to provide proof of your certs:

- **Download a PDF Certificate:** You can download a PDF certificate that contains a URL and verification code that can be used to authenticate your certification.
- **Create a Transcript:** You can create a customized certification transcript which will be sent by email to a designated recipient.

CompTIA Recertification and Renewal

CompTIA certifications earned since 2011 are valid for three years from the date of original certification. They must be renewed before their expiration date. CompTIA recertification and renewal comes under the auspices of the CompTIA Continuing Education (CE) program. You must be enrolled in that program to renew a certification.

There are a number of ways to renew a certification. You can simply recertify by paying for, and taking, the most recent version of the relevant CompTIA certification exam(s). Here are some of the other ways to renew a CompTIA certification:

- **Complete a CompTIA CertMaster CE course.** CertMaster CE e-learning courses are available for A+, Network+, and Security+. When you complete the course, you'll automatically earn Continuing Education Units (CEU) for the exam in your CompTIA certification account. CertMaster CE e-learning courses cost between $129 and $199.
- **Earn a higher-level CompTIA certification.** If you earn or renew a qualifying higher-level CompTIA certification, your existing CompTIA certifications are renewed.
- **Earn a non-CompTIA IT industry certification.** If you earn or renew a qualifying non-CompTIA IT industry certification, you'll earn Continuing Education Units (CEU) that can apply toward the renewal requirements for your existing CompTIA certification. For example, earning a Cisco CCNA Security cert gives you the 50 CEUs you need for CompTIA Security+ certification renewal.
- **Earn other CEUs.** You can earn CEUs to apply to recertification through a number of different avenues. These include taking training and higher education, participating in IT Industry activities, publishing articles or white papers, or even submitting relevant work experience.

Is a CompTIA Certification a Lifetime Certification?

As of January 1, 2011, CompTIA ended lifetime certifications. CompTIA certifications earned since that date are valid for three years only and are then subject to renewal and recertification as described above. CompTIA A+, CompTIA Network+ or CompTIA Security+ certifications earned before 2011 are considered good-for-life (GFL) and do not expire. Note that GFL certs are not valid for CompTIA stackable certifications. If you want to bring your certification current, you'll need to pass the current version of the exam. You'll then have two certs: your GFL certification and the new CE one.

CompTIA Certification Salary and Career Information

PayScale reports the following average salaries (USD) for employees holding particular CompTIA certifications:

- **CompTIA A+ salary:** $59,000
- **CompTIA Server+:** $63,000
- **CompTIA Network+:** $64,000
- **CompTIA Project+:** $67,000
- **CompTIA Linux+:** $70,000
- **CompTIA Security+:** $73,000
- **CompTIA CTT+:** $74,000
- **CompTIA Cloud+:** $76,000
- **CompTIA Advanced Security Practitioner (CASP):** $86,000

CompTIA certification will be just one indicator of the value that you bring to the table. Other factors will play a big part in how much a job will pay. For example, although the average salary for CompTIA A+ is $59,000, PayScale reports salaries up to $91,000 for A+ certified professionals in Washington D.C.

Not surprisingly, given CompTIA's inclusion in the US Department of Defense (DoD) baseline certifications, the US military and Federal Government contractors are popular employers for CompTIA certification holders.

CompTIA Certification Training

CBT Nuggets offers a variety of training that maps to CompTIA certification exams, ranging from A+ to Cloud+.

- **Core Series**
  - CompTIA Network+ (N10-007)
  - CompTIA Security+ (SY0-501)
  - CompTIA A+ 220-1001
  - CompTIA A+ 220-1002
- **Infrastructure Series**
  - CompTIA Cloud+ (CV0-002)
  - LPI Linux LPIC-1 101 and CompTIA Linux+
- **Cybersecurity Series**
  - CompTIA CySA+ (CS0-001)
- **Additional Professional Series**
  - CompTIA Project+ (PK0-004)
  - CompTIA Cloud Essentials (CLO-001)

Our training changes from time-to-time as we support the CompTIA certification roadmap. So be sure to check CBT Nuggets for new and updated training relevant to your personal CompTIA certification goals.

CBTnuggets

Cisco Security Certifications

Security is one of the most sought after skills you can have in IT right now — and there are plenty of security certifications you could pursue. Network administrator or engineers working in a Cisco shop will find a good match between these Cisco security certifications and their existing networking skills. Many threats may be in the application layer, but defense starts at the network layer.

New Cisco Certification Program

Cisco announced major changes to their certification program at Cisco Live! 2019. On February 23, 2020, nine CCNAs will retire, Cisco certifications will no longer have prerequisites, and it will require passing fewer exams to earn Cisco Professional-level exams.

The Cisco career certification program will still have five tiers of certifications —- Associate, Specialist, Professional, Expert, and Architect. Within each tier, networking professionals can either follow the popular enterprise track (equivalent to the previous R&S track) or specialize into five other areas as they progress. Cisco still offers specializations in the Associate, Professional, and Expert tracks. However, there are fundamental changes to the Cisco certification program:

No more prerequisites. Among those changes, Cisco rescinded all prerequisites for exams. You no longer have to earn a CCNA in order to attempt the CCNP. DevNet track. Until February 2020, CCENT or CCNA still serve as the entry point into the Cisco certification universe. On February 24, 2020, there will also be a DevNet, which emphasizes programming as well as networking skills. The DevNet track currently has an associate and professional-level certification exam. Cisco will add an expert-level exam soon equivalent to a CCIE.

CCNA retirements. Cisco will retire nine associate-level certifications in February 2020, replacing all nine with a single CCNA. Rather than specializing as an associate, networking professionals will specialize at the CCNP level. Those concentrations include Enterprise, Collaboration, Data Center, Security, and Service Provider.

Fewer CCNP exams. Until February 2020, CCNP certifications often require passing either three or four exams. On February 24, 2020, IT professionals only need to pass two exams — one core exam and one concentration exam — to earn their Professional-level certification. Additionally, the CCNP core exam for each also serves as the written exam for the CCIE in that track.

Easier to switch specialties. With the previous certification program, the process for networking professionals who wanted to switch between specialization tracks was fairly rigid. For instance, the CCNA R&S served as a prerequisite for several other CCNAs, but the CCNP requires that IT professionals earn the preceding CCNA in the track. For instance, someone who earns their CCNA Wireless and then wants to earn the CCNP Collaboration has to go back to earn the CCNA Collaboration.

New Cisco Security Certifications

In the new Cisco certification program, specialization happens at the professional-level rather than the associate-level. While there will no longer be a CCNA Security, the CCNA 200-301 exam will cover networking security fundamentals.

Cisco offers three security exams:

- **CCNA CyberOps**
- **CCNP Security**
- **CCIE Security**

Certification updates: These certification exams will be available February 24, 2020.

Despite all other CCNA certifications retiring, there are no changes to the associate-level CCNA CyberOps certification.

CISCO ASSOCIATE (NEW)

Cisco Certified Network Associate - CyberOps (CCNA CyberOps)

The CCNA CyberOps certification is designed for entry-level cybersecurity professionals. CCNA CyberOps is an approved certification under the DoD 8570.01-M framework in the CSSP Analyst and CCSP Incident Responder categories. The CCNA CyberOps certification validates a candidate's understanding of security topics, including:

- **Understanding and implementing access control modes**
- **Knowing the security impact of common cryptography methods**
- **Identifying common attack vectors and security vulnerabilities**
- **Mapping data types to compliance frameworks**
- **Analyzing data from security events**

Required exams: CCNA - CyberOps has two required exams — Understanding Cisco Cybersecurity Fundamentals (210-250 SECFND) and Implementing Cisco Cybersecurity Operations (210-255 SECOPS).
Prerequisites: None.
Recommended experience: While Cisco certifications no longer have formal prerequisites, Cisco recommends that candidates attempting the two CCNA - CyberOps exams have at least one year of experience in a security role.

CISCO PROFESSIONAL (NEW)

Cisco Certified Network Professional - Security (CCNP Security)

The CCNP Security certification is designed to test a security professional's ability to secure an organization's physical infrastructure, cloud services, endpoints, and network access. The CCNP - Security core exam validates a candidate's understanding of security topics, including:

- **Identifying common security vulnerabilities against on-prem and cloud environments**
- **Implementing appropriate access policies**
- **Configuring cloud logging and monitoring methods**
- **Ensuring email, internet gateway, and web security features are active**
- **Understanding benefits of various Cisco security products**

Required exams: The core exam for the CCNP Security certification is Implementing and Operating Cisco Security Core Technologies (300-701 SCOR). Candidates can then choose one of seven concentration exams:

- Securing Networks with Cisco Firepower Next Generation Firewall (300-710 SNCF)
- Securing Networks with Cisco Firepower Next-Generation IPS (300-710 SNCF)
- Implementing and Configuring Cisco Identity Services Engine (300-715 SISE)
- Securing Email with Cisco Email Security Appliance (300-720 SESA)
- Securing the Web with Cisco Web Security Appliance (300-725 SWSA)
- Implementing Secure Solutions with Virtual Private Networks (300-730 SVPN)
- Implementing Automation for Cisco Security Solutions (300-735 SAUTO)

Prerequisites: None.

Recommended experience: While Cisco certifications no longer have formal prerequisites, Cisco recommends that candidates who attempt this professional-level exam have three to five years experience implementing security solutions.

CISCO EXPERT (NEW)

Cisco Certified Internetwork Expert - Security (CCIE Security)

The CCIE Security certification is designed for IT professionals who secure all aspects of an organization's wired and wireless networks and cloud services. Candidates should expect to demonstrate an expert level of competency in these topics during their 8-hour hands-on lab:

- **Perimeter Security and Intrusion Prevention**
- **Secure Connectivity and Segmentation**
- **Infrastructure Security**
- **Identity Management, Information Exchange, and Access Control**
- **Advanced Threat Protection and Content Security**

Required exams: The written exam for the CCIE Security certification is Implementing and Operating Cisco Security Core Technologies (SCOR 300-701). CCIE candidates must then travel to a Cisco facility to take the CCIE Security v6.0 lab exam.
Prerequisites: None.
Recommended experience: While expert-level Cisco certifications don't have formal prerequisites, Cisco recommends that candidates attempting CCIE exams have five to seven years experience securing enterprise networks and systems.

Current Cisco Security Certifications

With Cisco certifications everything starts with networking. These Cisco security certifications start at the associate-level, which validates everything a networking professoinal will learn in their first year about networking and security. These certifications then progress to the professional and finally expert levels, which provide a good path forward for anyone who wants to create a career securing networks.

Cisco offers three security exams:

- **CCNA Cyber Ops**
- **CCNA Security**
- **CCNP Security**
- **CCIE Security**

Note: All listed CCNAs (except for the CCNA - CyberOps) will retire February 24, 2020.

CISCO ASSOCIATE (CURRENT)

Cisco Certified Network Associate - Security (CCNA Security)

The CCNA Security certification is designed for IT professionals who develop security infrastructure, recognize vulnerabilities, and mitigate security threats. The CCNA Security certification validates a candidate's understanding of security topics, including:

- **SIEM Technology**
- **Cloud & Virtual Network Topologies**
- **BYOD (Bring Your Own Device)**
- **Identity Services Engine (ISE)**
- **802.1x Authentication**
- **Cisco FirePOWER Next Generation IPS**
- **Cisco Advanced Malware Protection**

Required exam: Earning the CCNA Security requires passing one exam — Implementing Cisco Network Security (210-260 IINS).
Prerequisites: Prior to attempting this certification, candidates must earn the CCENT, CCNA R&S, or any CCIE certification.
Recommended experience: Cisco recommends that candidates attempting this associate-level exam have at least one year of experience in an IT role.

CISCO ASSOCIATE (CURRENT)

Cisco Certified Network Associate - CyberOps (CCNA CyberOps)

The CCNA CyberOps certification is designed for entry-level cybersecurity professionals. CCNA CyberOps is an approved certification under the DoD 8570.01-M framework in the CSSP Analyst and CCSP Incident Responder categories. The CCNA CyberOps certification validates a candidate's understanding of security topics, including:

- **Understanding and implementing access control modes**
- **Knowing the security impact of common cryptography methods**
- **Identifying common attack vectors and security vulnerabilities**
- **Mapping data types to compliance frameworks**
- **Analyzing data from security events**

Required exams: CCNA - CyberOps has two required exams — Understanding Cisco Cybersecurity Fundamentals (210-250 SECFND) and Implementing Cisco Cybersecurity Operations (210-255 SECOPS).
Prerequisites: None.
Recommended experience: While Cisco certifications no longer have formal prerequisites, Cisco recommends that candidates attempting the two CCNA - CyberOps exams have at least one year of experience in a security role.

Cisco networking gear is everywhere. Its routers, switches, and even phones are found in most office environments. For IT professionals who specialize in network administration, it's more likely than not that you'll work in a Cisco environment at some point. That's why Cisco certifications are so popular and highly valued. Cisco certifications validate the knowledge and skills IT professionals need to be successful in managing and maintaining Cisco technologies.

CBTnuggets

CISCO PROFESSIONAL (CURRENT)

Cisco Certified Network Professional - Security (CCNP Security)

The CCNP Security certification is designed for networking engineers who deploy, support and troubleshoot firewalls, VPNS, and IDS/IPS solutions. The CCNP Security certification validates a candidate's understanding of security topics, including:

- **Content Security**
- **Network Threat Defense**
- **Cisco FirePOWER Next-Generation IPS (NGIPS)**
- **Security Architectures**
- **Troubleshooting, Monitoring, and Reporting**

Required exams: Earning the CCNP Security requires passing four exams:

- Implementing Cisco Secure Access Solutions (300-208 SISAS)
- Implementing Cisco Edge Network Security Solutions (300-206 SENSS)
- Implementing Cisco Secure Mobility Solutions (300-209 SIMOS)
- Implementing Cisco Threat Control Solutions (300-210 SITCS)

Prerequisites: Prior to attempting this certification, candidates must earn the CCNA Security, or any CCIE.

Recommended experience: Cisco recommends that candidates attempting this professional-level exam have at least three years of experience in an IT role.

CISCO EXPERT (CURRENT)

Cisco Certified Internetwork Expert - Security (CCIE Security)

The CCIE Security certification is designed for IT professionals who secure all aspects of an organization's wired and wireless networks and cloud services. Candidates should expect to demonstrate an expert level of competency in these topics during their 8-hour hands-on lab:

- **Perimeter Security and Intrusion Prevention**
- **Secure Connectivity and Segmentation**
- **Infrastructure Security**
- **Identity Management, Information Exchange, and Access Control**
- **Advanced Threat Protection and Content Security**

Required exams: The written exam for the CCIE Security certification is 400-251 CCIE Security. CCIE candidates must then travel to a Cisco facility to take the CCIE Security lab exam.

Prerequisites: None.

Recommended experience: While expert-level Cisco certifications don't have formal prerequisites, Cisco recommends that candidates attempting CCIE exams have five to seven years experience securing enterprise networks and systems.