CBTnuggets

Certification Guide

Security

Table of Contents

How to Succeed in Security	3
Palo Alto Certifications	11
OffSec Certifications	19
(ISC)² Certifications	33
Check Point Certifications	47
CompTIA Certifications	53
Cisco Certifications	76

Last updated 10/1/2024

CBTnuggets

How to Succeed in Security

The security career field has boomed recently with demand high and investment pouring into the sector. Gartner forecasts that security spending will rise to $203.8 billion in 2025 as companies shift from basic prevention to more advanced offensive security strategies. A significant portion of this investment will address the critical shortage of skilled security professionals. Independent research indicates that 3.9 million cybersecurity positions will remain unfilled globally in 2025. Meanwhile, cyber threats continue to escalate with no signs of abating.

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, systems 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 specializes in areas like analysis, penetration testing, or risk management, they build foundational security skills throughout their career. Surprisingly, the easiest way to break into IT security isn't necessarily through security certifications (though they definitely help). Instead, the best way to start is by earning essential certifications like CompTIA Network+, Cisco CCNA, or Microsoft's Azure Fundamentals. More important than security knowledge at this stage are solid networking and system administration skills.

Once you've mastered those foundational skills, it's time to specialize — and there are certifications tailored to each career stage. For example, taking a look at the prerequisites for a foundational security certification shows where aspiring IT security professionals 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 General Security Concepts** - 12%
- **2.0 Threats, Vulnerabilities, and Mitigations** -22%
- **3.0 Security Architecture** - 18%

- **4.0 Security Operations** - 28%
- **5.0 Security Program Management and Oversight** - 20%

Like all certifications, the difficulty of Security+ depends on the test taker's experience level. For someone new to IT, Security+ introduces a lot of new terminology and reinforces it with scenario-based questions, making it a great starting point for anyone interested in security. However, serious security concepts start to show up even in certifications that aren't strictly focused on security.

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 systems administration certifications.

For instance, networking professionals should expect about 15 percent of questions on the CCNA to be about infrastructure security. Cloud professionals can expect nearly a third 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

By this stage, most security professionals have already taken on responsibilities that will help build a strong security resume. That also means it's time to get certified.

Security certifications are typically offered either by security vendors like Palo Alto or Cisco, or by professional organizations such as (ISC)². These certifications are often specialized and typically require several years of experience. For example, AWS offers the AWS Certified Security – Specialty certification, which requires five years of IT

security experience and at least two years securing AWS workloads. Cisco's security track includes the Cisco Certified CyberOps Associate as an entry-level certification. From there, the path forward is highly individualized — security is a broad field with numerous career paths to explore.

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 one career field and also security. Here are some common security career paths.

Cybersecurity Analyst

By most accounts, cybersecurity analysts do some of the more routine work in the field. Their main responsibilities are discovering and detecting cyberattacks. What "discovering threats" means can vary based on the company, but it typically involves digging into log files, identifying threats, and implementing security policies to prevent attacks based on known signatures. These policies might be enforced through security appliances, software, or even custom-built automation solutions.

IT professionals aiming to become cybersecurity analysts need a well-rounded set of technical skills, as they rely heavily on their experience to know what to look for. Cybersecurity analysts are hands-on technicians, so they need strong technical expertise in areas like Windows administration, desktop support, networking, and proficiency in at least one programming language. Analysts might spend days auditing SSL certificates or combing through log files — it's repetitive but crucial work, forming the frontline defense against attacks.

Security certifications: CompTIA CySA+, Cisco Certified CyberOps Associate

Typical background: Systems administrator, network administration

Security Engineer

Engineers play a different role than analysts. While analysts identify security issues and detect attacks, engineers are responsible for setting up defenses and minimizing service disruption in the event of an attack. Typically, engineers implement the security measures designed by security architects or similar security managers. This could involve building reporting and logging systems or deploying security hardware. Like many security roles, no two security engineer jobs are exactly alike, but most engineers need a broad skill set. This often includes networking, Active Directory, server technologies, firewalls, light penetration testing, and scripting.

Security certifications: AWS Security, CCNP Security

Typical background: Systems administrator, network administration, software engineer

Security Architect

Architect roles vary depending on the company. Some architects remain deeply hands-on, functioning almost like senior engineers, while others take on more managerial responsibilities. As managers, architects evaluate security solutions, present their benefits to upper management, and collaborate with engineers to implement them. Whether they're hands-on or managerial, architects are senior-level professionals with extensive experience in the trenches as engineers.

Security certifications: CCIE Security, CISSP

Typical background: Systems administrator, network administration, software engineer

Penetration Tester

With recent high-profile breaches, penetration testing has gained significant attention. Skills like networking, systems administration, Linux, and scripting are heavily featured in the OSCP exam, which serves as a good benchmark for what's needed in the field. Pen testers often rely on their previous experience to identify vulnerabilities. For example, a pen tester who previously worked as a systems administrator may use that knowledge to spot server misconfigurations. That's why the best pen testers rarely start out in pen testing; they typically begin as generalists or networking professionals.

Security certifications: CompTIA PenTest+, OSCP

Typical background: Systems administrator, network administration, software engineer, security analyst

Security Executive

In recent years, while companies have struggled to find enough qualified technical cybersecurity professionals, executive-level security positions have generally been easier to fill. This may be due to the high demand for technical roles in the market. Security executives are managers and communicators who view systems through a security-focused lens. Many C-level and managerial security professionals rise through the ranks from technical roles. Certifications like CISSP validate the extensive technical experience typically required for these leadership positions.

Security certifications: CISSP

Typical background: Software engineer, security engineer, security architect

Other Security Job Roles

The job titles mentioned here are broad and represent the most common roles an aspiring security professional will encounter. As professionals advance, they'll discover other subsets of information and cybersecurity roles and determine if they're a good fit.

Specialists. A quick glance at any job board reveals a wide range of specialized positions. There are security professionals focused on areas like cloud, mobile, IoT, and various other niches within analyst or engineer roles. Some of these specialized fields have certifications tied to them, while many do not. Specialists often rely on their experience and ongoing research to stay current in their specific areas of expertise.

Incident Handlers. There's a whole subset of security jobs that only come into play during major security events, such as incident handlers, forensics experts, and other members of Computer Security Incident Response Teams (CSIRTs). These are high-intensity roles that can be full-time positions or activated when an incident occurs. Many professionals in this field work for government agencies or cybersecurity firms, while others may have primary roles as engineers or analysts until an event requires their expertise.

Cybersecurity Researchers. The field of malware analysts and security researchers is growing rapidly. These professionals reverse-engineer malware, trace threats back to their sources, and set up honeypots. While some may work for large corporations, most are employed by nonprofit organizations, cybersecurity firms, or government agencies.

Compliance and Governance. Compliance may not be glamorous, but it's crucial for organizations that need to adhere to specific regulatory frameworks. Job titles in this area often focus on policy, governance, or compliance. These professionals enforce standards based on frameworks like NIST, DISA, ITIL, or PCI, ensuring organizations meet certification and regulatory requirements.

Using this Certification Guide

Despite the high demand for security professionals, breaking into the field can be challenging. It's often difficult to gain security experience when companies are hesitant to hire someone without it. Most people in this industry start by taking on security responsibilities in their existing roles before fully specializing. With that experience and relevant certifications, anyone can build a resume that stands out and land their first security job.

In this certification guide, we've listed certifications from top networking vendors like Cisco, Palo Alto, (ISC)2, Check Point, Offensive Security, and CompTIA. Two notable exceptions are GIAC and Fortinet certifications, which will be in a future version of this certification guide.

Each chapter is organized from foundational to expert-level certifications, so you can choose your path based on your career goals, experience level, and the stated prerequisites.

Palo Alto Certifications

Palo Alto Networks is globally recognized as a leading provider of cybersecurity solutions. Their certifications validate an IT professional's expertise in security management using Palo Alto products, making it a valuable credential for those looking to advance in IT security. The Palo Alto certification path is designed to help professionals demonstrate their ability to secure systems and networks effectively.

Palo Alto certification exams are organized into four categories, each tailored to help IT professionals gain expertise in their chosen security niche. These categories include:

- **Cloud Security**
- **Cybersecurity Fundamentals**
- **Network Security**
- **Security Operations**

Palo Alto Network Certifications

Palo Alto Networks certifications include the Palo Alto Networks Certified Cybersecurity Associate (PCCSA), Certified Network Security Administrator (PCNSA), and Certified Network Security Engineer (PCNSE) exams. These certifications focus on essential skills for building secure infrastructure, mitigating threats, and defending against cyberattacks. Certified professionals will be equipped to use Palo Alto hardware and software to protect IT assets effectively.

Palo Alto Networks offers seven professional certifications that demonstrate network security skills:

- Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)
- Palo Alto Networks Certified Network Security Administrator (PCNSA)
- **Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA)**
- **Palo Alto Networks Prisma Certified Cloud Security Engineer (PCCSE)**
- **Palo Alto Networks Certified Security Automation Engineer (PCSAE)**
- **Palo Alto Networks Certified Software Firewall Engineer (PCSFE)**
- Palo Alto Networks Certified Network Security Engineer (PCNSE)

[PALO ALTO ENTRY-LEVEL]

Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)

The Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET) certification is designed to provide an introductory examination of cybersecurity fundamentals. This entry-level exam aligns with the National Institute of Standards and Technology/National Initiative for Cybersecurity Education (NIST/NICE) workforce framework, ensuring that those who pass it are well-versed in current cybersecurity policies and foundational knowledge. The topics covered include:

- **Fundamentals of Cybersecurity**
- **Network Security Components**
- **Cloud Technologies**
- **Elements of Security Operations**

Required exam: Earning the Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET) certification requires passing one exam — the Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET) certification exam.

Prerequisites: None.

Recommended experience: Palo Alto recommends introductory knowledge of networking and cybersecurity concepts. Real-world experience with Palo Alto Networks technology is a plus.

[PALO ALTO INTERMEDIATE]

Palo Alto Networks Certified Network Security Administrator (PCNSA)

The Palo Alto Networks Certified Network Security Administrator (PCNSA) is designed for IT professionals who are starting their journey in cybersecurity. The PCNSA covers a broad range of security administration topics, including:

- **Device Management and Services**
- **Managing Objects**
- **Policy Evaluation**
- **Management Securing Traffic**

Required exam: Earning the Palo Alto Networks Certified Network Security Administrator (PCNSA) certification requires passing one exam — the Palo Alto Networks Certified Network Security Administrator (PCNSA) exam.
Prerequisites: None. The PCCSE and PCNSE are not specified as prerequisites for the PCNSA, but they are recommended.
Recommended experience: Candidates should have an understanding of networking concepts, such as IP addressing and TCP/IP, along with hands-on experience with Palo Alto Networks firewalls and network security administration. Practical experience and familiarity with core security concepts are recommended.

[PALO ALTO INTERMEDIATE]

Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA)

The Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) is aimed at IT professionals focused on detecting and responding to cyber threats. It covers key topics such as:

- **Threats and Attacks**
- **Prevention and Detection**
- **Investigation**
- **Remediation**
- **Threat Hunting**
- **Reporting**

- **Architecture**

Required exam: Earning the Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) certification requires passing one exam — the Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) exam.

Prerequisites: None.

Recommended experience: It is recommended that candidates have a foundational understanding of cybersecurity concepts and network security practices to succeed in the exam.

[PALO ALTO INTERMEDIATE]

Palo Alto Networks Prisma Certified Cloud Security Engineer (PCCSE)

The Palo Alto Networks Prisma Certified Cloud Security Engineer (PCCSE) certification is designed for cloud security specialists looking to deepen their technical expertise in Prisma Cloud. This certification validates the skills needed to onboard, deploy, and manage all aspects of Prisma Cloud. It ensures that candidates have a solid understanding of key security administration tasks, including:

- **Cloud Security Posture Management (CSPM)**
- **Cloud Workload Protection (CWP)**
- **Install, Upgrade, and Backup / Prisma Cloud**
- **Cloud Network Security and Identity-Based Microsegmentation Enterprise Edition**
- **Prisma Cloud Code Security (PCCS)**
- **Identity and Access Management (IAM) / Prisma Cloud Data Security (PCDS)**

Required exam: Earning the Palo Alto Networks Prisma Certified Cloud Security Engineer (PCCSE) certification requires passing one exam — the Palo Alto Networks Prisma Certified Cloud Security Engineer (PCCSE) exam.

Prerequisites: None.

Recommended experience: It is recommended that candidates have a foundational understanding of Prisma Cloud, as well as experience with containers, cloud architecture and cloud computing.

[PALO ALTO INTERMEDIATE]

Palo Alto Networks Certified Security Automation Engineer (PCSAE)

The Palo Alto Networks Certified Security Automation Engineer (PCSAE) certification is designed for IT professionals with significant experience in Palo Alto Networks technologies and a solid understanding of security automation techniques. This certification validates a candidate's understanding of these security administration tasks:

- **Playbook Development**
- **Incident Objects**
- **Automations, Integrations, and Related Concepts**
- **Content Management and Solution Architecture**
- **UI Workflow, Dashboards, and Reports**
- **Threat Intel Management**

Required exam: Earning the Palo Alto Networks Certified Security Automation Engineer (PCSAE) certification requires passing one exam — the Palo Alto Networks Certified Security Automation Engineer (PCSAE) exam.
Prerequisites: None.
Recommended experience: Candidates should have the equivalent of three years experience with incident response processes and security incident management, as well as fundamental knowledge of Cortex XSOAR.

[PALO ALTO ADVANCED]

Palo Alto Networks Certified Software Firewall Engineer (PCSFE)

The Palo Alto Networks Certified Software Firewall Engineer (PCSFE) certification is designed for IT professionals who have experience with Palo Alto Networks' software firewalls and are looking to deepen their expertise. This certification validates a candidate’s ability to deploy, configure, and manage software-based firewalls across various environments, ensuring optimal security and performance. Candidates will verify knowledge in the following areas:

- **Software Firewall Fundamentals**
- **Securing Environments with Software Firewalls**
- **Deployment Architecture**
- **Automation and Orchestration**

- **Technology Integration**
- **Troubleshooting**
- **Management Plugins and Log Forwarding**

Required exam: Earning the Palo Alto Networks Certified Software Firewall Engineer (PCSFE) certification requires passing one exam — the Palo Alto Networks Certified Software Firewall Engineer (PCSFE) exam.
Prerequisites: None.
Recommended experience: Candidates should have about five years of experience in networking or security, with at least a year working in virtualized or cloud environments. They should also have 6–12 months of hands-on experience deploying and configuring Palo Alto Networks next-generation firewalls.

[PALO ALTO ADVANCED]

Palo Alto Networks Certified Network Security Engineer (PCNSE)

The Palo Alto Networks Certified Network Security Engineer (PCNSE) certification is designed for IT professionals with extensive experience and expertise in Palo Alto Networks technologies. This certification validates a candidate's ability to perform key security administration tasks, including deploying, managing, and troubleshooting Palo Alto Networks solutions.Candidates will verify knowledge in the following areas:

- **Core Concepts**
- **Deploy and Configure Core Components**
- **Deploy and Configure Features and Subscriptions**
- **Deploy and Configure Firewalls Using Panorama**
- **Manage and Operate**
- **Troubleshooting**

Required exam: Earning the Palo Alto Networks Certified Network Security Engineer (PCNSE) certification requires passing one exam — the Palo Alto Networks Certified Network Security Engineer (PCNSE) exam.
Prerequisites: None.
Recommended experience: It's recommended that candidates for the PCNSE have 3-5 years of experience in networking or security, with hands-on experience using Palo Alto Networks products. Familiarity with deploying, managing, and troubleshooting Palo Alto Networks next-generation firewalls is key to success.

How Much Does It Cost to Get Palo Alto Certified?

Palo Alto Networks certification exams are administered by Pearson VUE. The pricing is straightforward and competitive compared to many other IT certifications. The PCCSA exam costs $110, the PCNSA is priced at $175, and the PCNSE costs $200.

Palo Alto Recertification and Renewal

Palo Alto Networks certifications are valid for two years (24 months). To keep your certification current, you need to renew it by passing the exam again every two years. For recertification with the PCNSA, you can either retake the PCNSA exam or opt for the PCNSE exam. However, the PCNSE certification can only be renewed by retaking the PCNSE exam.

Palo Alto Certification Salary and Career Information

IT professionals with a Palo Alto Networks Certified Network Security Engineer (PCNSE) certification can expect to earn around $114,000 per year. While there aren't specific figures available on Payscale for the PCCSA or PCNSA, these certifications typically command slightly lower salaries than the PCNSE, though this can vary based on experience. Here are the current average salaries for the PCNSE, according to Payscale (in USD):

- **Network Security Engineer: $114,000**
- **Network Engineer: $75,000**
- **Network Architect: $128,000**
- **Security Consultant: $106,000**
- **Senior Security Consultant: $152,000**

- **Security Engineer: $92,000**
- **Senior Network Engineer: $120,000**

Palo Alto Networks certifications are often considered a more accessible entry point for those looking to break into the information security field, with a relatively low cost compared to other certifications.

Many individuals pursue these certifications because they are working with Palo Alto Networks products. Ultimately, your decision to pursue Palo Alto certification should align with your career goals and whether you anticipate working with their technologies. Given the potential earnings and career opportunities, it's definitely worth considering.

Palo Alto Networks Certification Training

CBT Nuggets offers a comprehensive range of courses focused on Palo Alto Networks. Check out CBT Nuggets' Palo Alto Networks courses here. We continually update our training library, so be sure to check regularly for the latest Palo Alto training.

In addition to engaging video training created by expert trainers, CBT Nuggets provides everything you need to prepare for IT certification exams. This includes virtual labs, supplemental files, practice exams, and access to a robust Learner Community.

Our training features custom virtual labs and supplemental files designed to help you grasp technical concepts alongside the video content. Virtual labs offer hands-on experience in a sandbox environment, while supplemental files include practice commands, configuration files, and network diagrams — all essential for certification exam preparation. Additionally, CBT Nuggets learners can benefit from the CyberVista® IT training practice exams included with a subscription. These practice exams, available both timed and untimed, offer a valuable way to assess your knowledge and identify areas for improvement, helping you focus your study efforts effectively.

OffSec Certifications

Network security is a crucial element of information technology, especially with the persistent threat from cybercriminals targeting vulnerable networks. To combat these threats and meet the demand for skilled security professionals, OffSec certifications have emerged as key credentials. Known for their difficulty and high respect in the industry, OffSec certifications focus on advanced penetration testing and security practices.

These certifications are widely recognized for their rigor and can significantly enhance your IT security resume. They demonstrate to potential employers your expertise in addressing and mitigating security threats effectively. If you're aiming to elevate your credentials and show your capability in network security, OffSec certifications are a top choice. OffSec offers certifications in the following areas:

- **Security Essentials**
- **Security Operations**
- **Penetration Testing**
- **Threat Hunting**
- **Web Application Security**
- **Exploit Development**

What is Kali Linux?

Most OffSec certifications recommend a solid understanding of Kali Linux. Kali Linux is a Debian-based distribution specifically designed for penetration testing and ethical hacking. Originally developed by founder Mati Aharoni and his team, it was first released

in March 2013 and comes packed with hundreds of tools used by IT professionals for security testing.

While Kali Linux brings everything together in one distribution, there's nothing exclusive about it—everything, from the Linux kernel to the utilities and applications, is open source. For example, Nmap is a well-known port scanner, and Wireshark is a popular network packet analyzer, both of which are included in the Kali toolset.

Where to Start with OffSec Certifications

The OffSec certification path isn't strictly tiered, meaning you can pursue each certification individually, provided you complete the required course beforehand. There are no prerequisites in terms of other exams for any of the certifications. The OffSec CyberCore (OSCC) is the most approachable certification offered, aimed at learners who are new to cybersecurity. At the other end of the spectrum, the OffSec Exploitation Expert (OSEE) certification is seen as the most advanced. Additionally, if you're looking to refine your Linux skills and leverage Linux for penetration testing, the OffSec Certified Professional (OSCP & OSCP+) certification is a solid option.

OffSec offers twelve professional certifications that demonstrate network security skills:

- **OffSec CyberCore (OSCC)**
- **Kali Linux Certified Professional (KLCP)**
- **OffSec Certified Professional (OSCP & OSCP+)**
- **OffSec Wireless Security Professional (OSWP)**
- **OffSec Experienced Penetration Tester (OSEP)**
- **OffSec Web Assessor (OSWA)**
- **OffSec Web Expert (OSWE)**
- **OffSec Defense Analyst (OSDA)**
- **OffSec Certified Threat Hunters (OSTH)**
- **OffSec Exploit Developer (OSED)**
- **OffSec macOS Researcher (OSMR)**
- **OffSec Exploitation Expert (OSEE)**

[OFFSEC ENTRY-LEVEL]

OffSec CyberCore (OSCC)

OffSec's CyberCore is a good starting point if you're looking to break into cybersecurity, whether you're a recent graduate or an IT professional looking to switch to a cybersecurity role. It verifies essential skills in both offensive and defensive security, with topics such as:

- **Anatomy of Cybersecurity**
- **Cybersecurity Frameworks and Standards**
- **Cybersecurity Roles**
- **Linux Basics**
- **Windows Basics**
- **Data Transformation Fundamentals**
- **Python Scripting Fundamentals**
- **PowerShell Scripting Fundamentals**
- **Networking Fundamentals**

Required exam: Earning the OffSec CyberCore (OSCC) certification requires passing one exam — the OffSec CyberCore (OSCC) exam.
Prerequisites: Candidates must complete the SEC-100: CyberCore – Security Essentials course offered by OffSec before taking the OffSec CyberCore (OSCC) exam.
Recommended experience: It's recommended that candidates have basic computer literacy and familiarity with operating systems.

[OFFSEC ENTRY-LEVEL]

Kali Linux Certified Professional (KLCP)

This Kali Linux Certified Professional (KLCP) course is designed for cybersecurity professionals, system administrators, and penetration testers who want to enhance their skills with Kali Linux. It is suitable for those who have a foundational understanding of networking and some familiarity with the Linux command line. The topics covered in the KLCP include:

- **Kali Linux Fundamentals**
- **Getting Started with Kali Linux**

- **Installing Kali Linux**
- **Configuring Kali Linux**
- **Troubleshooting**
- **Securing and Monitoring Kali Linux**
- **Debian Package Management**
- **Advanced Usage**
- **Kali Linux in the Enterprise**

Required exam: Earning the Kali Linux Certified Professional (KLCP) certification requires passing one exam — the OffSec CyberCore (OSCC) exam.

Prerequisites: Candidates must take the PEN-103 course offered by OffSec before taking the Kali Linux Certified Professional (KLCP) exam.

Recommended experience: A basic understanding of Linux and networking concepts is recommended, but not required.

[OFFSEC INTERMEDIATE]

OffSec Certified Professional (OSCP & OSCP+)

The OSCP+ and OSCP certifications are aimed at cybersecurity experts who want to validate their skills in ethical hacking and penetration testing. This certification is pertinent for roles like penetration testers, security analysts, and consultants, showcasing their capability to perform thorough security evaluations. Candidates will verify knowledge in the following areas:

- **Introduction to Cybersecurity**
- **Report Writing for Penetration Testers**
- **Information Gathering**
- **Vulnerability Scanning**
- **Introduction to Web Applications**
- **Common Web Application Attacks**
- **SQL Injection Attacks**
- **Client-Side Attacks**
- **Locating Public Exploits**
- **Fixing Exploits**

Required exam: Earning the OffSec Certified Professional (OSCP & OSCP+) certification requires passing one exam — the OffSec Certified Professional (OSCP & OSCP+) exam.
Prerequisites: Candidates must take the PEN-200: Penetration Testing with Kali Linux course offered by OffSec before taking the OSCP & OSCP+ exam.
Recommended experience: A solid foundation in TCP/IP networking, basic scripting abilities, familiarity with Linux and Windows operating systems are all strongly recommended.

[OFFSEC INTERMEDIATE]

OffSec Wireless Security Professional (OSWP)

The OffSec Wireless Professional (OSWP) certification is geared towards network security experts who want to showcase their skills in auditing 802.11 wireless networks and spotting vulnerabilities. Candidates are expected to be capable of simulating attacks as well. The OSWP certification confirms a candidate's proficiency in executing these knowledge areas:

- **IEEE 802.11**
- **Wireless Networks**
- **Wi-Fi Encryption**
- **Linux Wireless Tools, Drivers, and Stacks**
- **Wireshark Essentials**
- **Frames and Network Interaction**
- **Aircrack-ng Essentials**
- **Cracking Authentication Hashes**
- **Attacking WPS Networks**
- **Rogue Access Points**

Required exam: Earning the OffSec Wireless Security Professional (OSWP) certification requires passing one exam — the OffSec Wireless Security Professional (OSWP) exam.
Prerequisites: Candidates must take the PEN-210: Foundational Wireless Network Attacks course offered by OffSec before taking the OSWP exam.
Recommended experience: Candidates are strongly encouraged to have a familiarity using the Linux command line, a firm understanding of TCP/IP networking, and basic knowledge of wireless networking concepts.

[OFFSEC INTERMEDIATE]

OffSec Web Assessor (OSWA)

The OffSec Web Assessor OSWA is a 24-hour assessment designed for security professionals looking to verify their web application testing skills. Candidates will be tested in a hands-on, live lab environment, and are expected to demonstrate knowledge in the following areas:

- **Web Assessor Tools**
- **Cross-Site Scripting (XSS) Introduction, Discovery, Exploitation and Case Study**
- **Cross-Site Request Forgery (CSRF)**
- **Exploiting CORS Misconfigurations**
- **Database Enumeration**
- **SQL Injection (SQLi)**
- **Directory Traversal**
- **XML External Entity (XXE) Processing**
- **Server-Side Template Injection (SSTI)**
- **Server-Side Request Forgery (SSRF)**

Required exam: To earn the OffSec Web Assessor (OSWA) certification, you must pass the OffSec Web Assessor (OSWA) exam.
Prerequisites: Candidates must complete the WEB-200: Foundational Web Application Assessments with Kali Linux course offered by OffSec before taking the OSWA exam.
Recommended experience: Candidates should have a basic understanding of web development technologies such as HTML, CSS, and JavaScript, as well as networking fundamentals and the basics of the Linux operating system.

[OFFSEC INTERMEDIATE]

OffSec Threat Hunter (OSTH)

The OffSec Threat Hunter (OSTH) certification is designed for cybersecurity professionals who want to sharpen their skills in threat detection and analysis. This certification focuses on proactive threat hunting techniques, and how to identify and respond to potential security incidents before they escalate. You'll demonstrate knowledge of tools and concepts such as:

- **Threat Hunting Concepts and Practices**
- **Threat Actor Landscape Overview**
- **Communication and Reporting for Threat Hunters**
- **Hunting with Network Data**
- **Hunting on Endpoints**
- **Threat Hunting with IoCs**

Required exam: To earn the OffSec Threat Hunter (OSTH) certification, you must pass the OffSec Threat Hunter (OSTH) exam.
Prerequisites: Candidates are required to take the TH-200: Foundational Threat Hunting course offered by OffSec before attempting the OSTH exam.
Recommended experience: A solid foundation in TCP/IP networking, familiarity with Linux and Windows, and a basic understanding of cybersecurity concepts are strongly recommended.

[OFFSEC INTERMEDIATE]

OffSec Defense Analyst (OSDA)

The OffSec Defense Analyst (OSDA) certification is designed for cybersecurity professionals looking to enhance their skills in defense strategies and incident response. You'll gain practical, hands-on experience that prepares you to handle real-world security challenges and make informed decisions. This course covers key topics such as:

- **Attack Methodology**
- **Windows Endpoint**
- **Windows Server Side Attacks**
- **Windows Client-Side Attacks**
- **Windows Privilege Escalation**
- **Windows Persistence**
- **Linux Endpoint**
- **Linux Server Side Attacks**
- **Network Detections**
- **Antivirus Alerts and Evasion**

Required exam: To earn the OffSec Defense Analyst (OSDA) certification, you must pass the OffSec Defense Analyst (OSDA) exam.

Prerequisites: Candidates are required to take the SOC-200: Foundational Security Operations and Defensive Analysis course offered by OffSec before attempting the OSDA exam.

Recommended experience: A solid foundation in TCP/IP networking, familiarity with Linux and Windows, and basic cybersecurity concepts are all recommended for OSDA candidates.

[OFFSEC ADVANCED]

OffSec Experienced Penetration Tester (OSEP)

The OffSec Experienced Penetration Tester (OSEP) is a rigorous exam that takes place over 48-hours, and is designed to prove mastery in penetration testing. Skills are validated in a real-world lab environment, and include:

- **In-depth vulnerability analysis and exploitation**
- **Custom exploit development**
- **Bypassing modern security defenses**
- **Exploiting authentication and authorization flaws**
- **Attacking Active Directory and cloud environments**
- **Post-exploitation techniques for maintaining access and escalating privileges**

Required exam: To earn the OffSec Wireless Security Professional (OSWP) certification, you must pass the OffSec Wireless Security Professional (OSWP) exam.

Prerequisites: Candidates are required to take the PEN-300: Advanced Evasion Techniques and Breaching Defenses course offered by OffSec before attempting the OSEP exam. It is also recommended to have completed the PEN-200 (Penetration Testing with Kali Linux) course.

Recommended experience: Candidates should have a solid understanding of operating systems, networking, and scripting.

[OFFSEC ADVANCED]

OffSec Experienced Penetration Tester (OSEP)

The OffSec Experienced Penetration Tester (OSEP) is a rigorous exam that takes place over 48-hours, and is designed to prove mastery in penetration testing. Skills are validated in a real-world lab environment, and include:

- **In-depth vulnerability analysis and exploitation**
- **Custom exploit development**
- **Bypassing modern security defenses**
- **Exploiting authentication and authorization flaws**
- **Attacking Active Directory and cloud environments**
- **Post-exploitation techniques for maintaining access and escalating privileges**

Required exam: To earn the OffSec Wireless Security Professional (OSWP) certification, you must pass the OffSec Wireless Security Professional (OSWP) exam.
Prerequisites: Candidates are required to take the PEN-300: Advanced Evasion Techniques and Breaching Defenses course offered by OffSec before attempting the OSEP exam. It is also recommended to have completed the PEN-200 (Penetration Testing with Kali Linux) course.
Recommended experience: Candidates should have a solid understanding of operating systems, networking, and scripting.

[OFFSEC ADVANCED]

OffSec Web Expert (OSWE)

The OffSec Web Expert (OSWE) certification is aimed at network security professionals looking to showcase their skills in auditing web application code for vulnerabilities. This certification tests your ability to identify and defend against various web application exploits. The OSWE validates your capability to carry out a range of methods and attacks.

- **JavaScript Prototype Pollution**
- **Advanced Server-Side Request Forgery (SSRF)**
- **Web Security Tools and Methodologies**
- **Source Code Analysis**

- **Persistent Cross-Site Scripting**
- **Session Hijacking**
- **.NET Deserialization**
- **Remote Code Execution**
- **Blind SQL Injection**
- **Data Exfiltration**

Required exam: To earn the OffSec Web Expert (OSWE) certification, you must pass the OffSec Web Expert (OSWE) exam.

Prerequisites: Candidates are required to take the WEB-300: Advanced Web Attacks and Exploitation course offered by OffSec before attempting the OSWE exam.

Recommended experience: It is highly recommended that candidates be comfortable with at least one coding language, have familiarity with Linux, and possess experience in writing simple scripts and working with web proxies. Additionally, candidates should have a general understanding of web application attack vectors.

[OFFSEC ADVANCED]

OffSec Exploit Developer (OSED)

The OffSec Exploit Developer (OSED) exam is designed for cybersecurity professionals ready to demonstrate their skills in exploit development and vulnerability research. This challenging, hands-on assessment evaluates your ability to identify and exploit vulnerabilities in real-world scenarios. During the exam, you'll be required to demonstrate proficiency in the following areas:

- **WinDbg**
- **Stack Buffer Overflows**
- **Exploiting SEH Overflows**
- **IDA Pro**
- **Overcoming Space Restrictions**
- **Shellcode From Scratch**
- **Reverse-Engineering Bugs**
- **Stack Overflows and DEP/ASLR Bypass**
- **Format String Specifier Attacks**
- **Custom ROP Chains and ROP Payload Decoders**

Required exam: To earn the OffSec Exploit Developer (OSED) certification, you must pass the OffSec Exploit Developer (OSED) exam.

Prerequisites: Candidates are required to take the EXP-301: Windows User Mode Exploit Development course offered by OffSec before attempting the OSED exam.

Recommended experience: Candidates are encouraged to have a solid understanding of C programming, assembly language, Windows internals, and debugging tools like WinDbg and Immunity Debugger.

[OFFSEC ADVANCED]

OffSec macOS Researcher (OSMR)

The OffSec macOS Researcher (OSMR) exam is designed for cybersecurity professionals who want to validate their expertise in macOS security research and exploitation. This hands-on assessment challenges you to demonstrate your ability to identify vulnerabilities and develop effective exploitation techniques specific to the macOS environment. The OSMR exam covers topics such as:

- **Introduction to macOS Internals**
- **Debugging, Tracing & Hopper**
- **Shellcoding in macOS**
- **Dylib Injection**
- **Mach and Mach Injection**
- **Hooking**
- **XPC Exploitation**
- **Sandbox Escape**
- **Attacking Privacy (TCC)**
- **Symlink Attacks**

Required exam: To earn the OffSec macOS Researcher (OSMR) certification, you must pass the OffSec macOS Researcher (OSMR) exam.

Prerequisites: Candidates are required to take the EXP-312: Advanced macOS Control Bypasses course offered by OffSec before attempting the OSMR exam.

Recommended experience: A solid understanding of macOS internals, C and Objective-C programming concepts, and debugging tools like LLDB is highly recommended.

[OFFSEC ADVANCED]

OffSec Exploitation Expert (OSEE)

The OffSec Exploitation Expert (OSEE) certification is the most challenging exam offered by OffSec. It is designed for seasoned cybersecurity professionals looking to showcase their advanced skills in exploit development and vulnerability research. Successfully passing the OSEE exam confirms your expertise in crafting custom exploits and handling complex security challenges. The 72-hour exam covers topics such as:

- **Bypass and evasion of user mode security mitigations such as DEP, ASLR, CFG, ACG and CET**
- **Advanced heap manipulations to obtain code execution along with guest-to-host and sandbox escapes**
- **Disarming WDEG mitigations and creating version independence for weaponization**
- **64-Bit Windows Kernel Driver reverse engineering and vulnerability discovery**
- **Bypass of kernel mode security mitigations such as kASLR, NX, SMEP, SMAP, kCFG and HVCI**

Required exam: To earn the OffSec macOS Researcher (OSMR) certification, you must pass theOffSec macOS Researcher (OSMR) exam.
Prerequisites: Although there are no formal prerequisites, OffSec recommends completing all 300-Level OffSec certifications before attempting the OSEE.
Recommended experience: Experience developing Windows exploits, operating a debugger, and familiarity with WinDBG, x86_64 assembly, IDA Pro, and basic C/C++ programming are all strongly recommended.

How Much Does It Cost to Get Certified?

OffSec certification costs are bundled into packages that include both training and testing, meaning you can't take a course through an external provider or sit the exam elsewhere. The course and exam bundles range between $799 and $2,599. Each plan is highly variable in regard to which courses you get access to, and for how long.

OffSec Recertification and Renewal

With the exception of the OSCC certification, OffSec certifications do not expire and remain valid indefinitely once earned. This likely reflects their emphasis on security mitigation methods and strategies rather than specific technologies, which can change annually.

Penetration Tester Salary and Career Information

The average salary for an OSCP-certified professional is approximately $101,000, according to Payscale. Here are the typical salaries for various roles held by OSCP-certified IT professionals (in USD):

- Penetration Tester: $100,994
- Security Engineer: $110,930
- Security Consultant: $90,804
- Information Security Analyst: $82,685
- Cyber Security Engineer: $103,414
- Information Security Engineer: $96,931
- Senior Security Consultant: $119,454

Indeed reports an average salary for penetration testers at $122,136, highlighting strong earnings potential and job opportunities for those in this field, especially for OffSec-certified professionals.

While positions in IT helpdesk or NOC can be tough, the intense nature of penetration testing exams reflects the demands of the profession. Dedicated penetration testers often find themselves fully immersed in complex problems, leading to the adage that "sleep's for babies" — a testament to the commitment required in this line of work.

OffSec Training

Every OffSec exam requires a strong foundation in networking, security, and Kali LInux. CBT Nuggets trainer Keith Barker created the following Kali Linux and security training:

- CompTIA Security+
- White Hat Hacking v10 Online Training

In addition to engaging video training created by expert trainers, CBT Nuggets provides everything you need to prepare for IT certification exams. This includes virtual labs, supplemental files, practice exams, and access to a robust Learner Community.

Our training features custom virtual labs and supplemental files designed to help you grasp technical concepts alongside the video content. Virtual labs offer hands-on experience in a sandbox environment, while supplemental files include practice commands, configuration files, and network diagrams—all essential for certification exam preparation.

Additionally, CBT Nuggets learners can benefit from the CyberVista® IT training practice exams included with a subscription. These practice exams, available both timed and untimed, offer a valuable way to assess your knowledge and identify areas for improvement, helping you focus your study efforts effectively.

(ISC)² Certifications

Cybersecurity remains one of the most critical concerns for organizations due to evolving threats like data breaches, IoT vulnerabilities, and malware. The need for skilled cybersecurity professionals is higher than ever, but the industry is also grappling with a growing talent gap.

(ISC)², a leading nonprofit in cybersecurity training and certification, offers some of the most respected certifications in the field. These certifications, such as CISSP and SSCP, are designed to address a wide range of cybersecurity roles, helping professionals build both general and specialized skills needed to combat modern cyber threats. Here's the full list of (ISC)2 certifications:

- **(ISC)² CC - Certified in Cybersecurity**
- **(ISC)² CCSP - Certified Cloud Security Professional**
- **(ISC)² CISSP - Certified Information Systems Security Professional**
- **(ISC)² CGRC - Governance, Risk and Compliance Certification**
- **(ISC)² ISSAP - Information Systems Security Architecture Professional**
- **(ISC)² ISSEP - Information Systems Security Engineering Professional**
- **(ISC)² ISSMP - Information Systems Security Management Professional**
- **(ISC)² CSSLP - Certified Secure Software Lifecycle Professional**
- **(ISC)² SSCP - Systems Security Certified 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. The (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 in order to ensure the most experienced candidates for (ISC)² certification;

- **CC - Entry-Level (no work experience required)**
- **CCSP - 5 years**

- **CISSP - 5 years**
- **CGRC - 2 years**
- **ISSAP - CISSP + 2 years or 7 years accumulative**
- **ISSEP - CISSP + 2 years or 7 years accumulative**
- **ISSMP - CISSP + 2 years or 7 years accumulative**
- **CSSLP - 4 years**
- **SSCP - 1 year**

Recognizing the "chicken and the egg" nature of work experience, $(ISC)^2$ created the Associate of $(ISC)^2$ designation. 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.

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 ENTRY-LEVEL]

(ISC)² Certified in Cybersecurity (CC)

The (ISC)² Certified in Cybersecurity (CC) is an entry-level certification aimed at preparing learners with the foundational knowledge, skills and abilities required for an entry- or junior-level role in the cybersecurity field. The (ISC)² CISSP validates a candidate's knowledge in five security domains:

- **Security Operations**
- **Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts**
- **Access Controls Concepts**
- **Network Security**
- **Security Operations**

Required exam: Earning the (ISC)² CC certification requires passing one exam — the CC exam.

Prerequisites: None

Recommended experience: This certification has no recommended experience - it is aimed at people with the passion and drive to enter the field of cybersecurity.

[(ISC)² INTERMEDIATE]

(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:

- **Cloud Concepts, Architecture and Design**
- **Cloud Data Security**
- **Cloud Platform & Infrastructure Security**
- **Cloud Application Security**
- **Cloud Security Operations**
- **Legal, Risk 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; three (3) years must be in information security, and one (1) year must be in one or more of the six current CCSP Domains. There are some circumstances in which work experience can be substituted;

- A bachelors or masters degree in computer science, information technology (IT) or related fields may substitute up to one year of required experience.
- An additional credential from the ISC² approved list may be substituted for one year of experience in one or more of the six domains of the CCSP Exam Outline.
- An active CISSP credential can be substituted for the entire CCSP work experience requirement.
- Part-time work and internships may also count towards the experience requirements.
- The Cloud Security Alliance's Certificate of Cloud Security Knowledge (CCSK) can be substituted for one year of required experience in one or more of the six CCSP domains.

The (ISC)² CCSP meets the requirements of the U.S. Department of Defense (DoD) Directive 8140.03.

[(ISC)² INTERMEDIATE]

(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 in two or more of the eight domains of the ISC² CISSP Common Body of Knowledge (CBK). Candidates may satisfy one year of the required experience with a four-year bachelors or masters in computer science, information technology (IT) or related fields. One year of work experience may also be satisfied by holding an approved credential from the ISC² approved list.

The (ISC)² CISSP meets the requirements of the U.S. Department of Defense (DoD) Directive 8140.03.

[(ISC)² ADVANCED]

(ISC)² Governance, Risk and Compliance Certification (CGRC)

The (ISC)² Governance, Risk and Compliance Certification (CGRC) is designed for IT, information security and information assurance professionals who work in Governance, Risk and Compliance (GRC) roles. Gaining this certification demonstrates advanced technical knowledge and skills in protecting, authorizing and maintaining information systems within various risk management frameworks.

The (ISC)² CGRC validates a candidate's knowledge in seven security domains:

- **Security and Privacy Governance, Risk Management, and Compliance Program**
- **Scope of the System**
- **Selection and Approval of Framework, Security, and Privacy Controls**
- **Implementation of Security and Privacy Controls**
- **Assessment/Audit of Security and Privacy Controls**
- **System Compliance**
- **Compliance Maintenance**

Required exam: Earning the (ISC)² CGRC certification requires passing one exam — the CGRC exam.
Prerequisites: Candidates who pass the CGRC exam, but do not have the required work experience, will become an Associate of (ISC)².

Required experience: Candidates must have a minimum of two (2) years cumulative, full-time work experience in one or more of the seven domains of the current CGRC exam outline. Part-time work and internships may also count towards the experience requirement.

The (ISC)² CGRC meets the requirements of the U.S. Department of Defense (DoD) Directive 8140.03.

[(ISC)² ADVANCED]

(ISC)² Information Systems Security Architecture Professional (ISSAP)

The (ISC)² Information Systems Security Architecture Professional (ISSAP) certification is designed to prove expertise in developing, designing and analyzing security solutions across an organization. It also demonstrates the ability to give risk-based guidance to senior management in pursuing and achieving organizational goals.

The (ISC)² ISSAP validates a candidate's knowledge in six security domains:

- **Architect for Governance, Compliance and Risk Management**
- **Security Architecture Modeling**
- **Infrastructure Security Architecture**
- **Identity and Access Management (IAM) Architecture**
- **Architect for Application Security**
- **Security Operations Architecture**

Required exam: Earning the (ISC)² ISSAP certification requires passing two exams — the CISSP and ISSAP exams. See below for exceptions.
Prerequisites: CISSP or relevant experience.
Required experience: Candidates must hold a CISSP certification in good standing and have two (2) years cumulative, full-time experience in one or more of the six domains of the current ISSAP exam outline. Alternatively, candidates may satisfy the required experience with a minimum of seven (7) years cumulative, full-time experience in two or more of the current ISSAP domains. Earning a bachelors or masters degree in computer science, information technology (IT) or related fields or an additional credential from the ISC² approved list may satisfy one year of the required experience. Part-time work and internships may also count towards the experience requirement.

The (ISC)² ISSAP meets the requirements of the U.S. Department of Defense (DoD) Directive 8140.03.

[(ISC)² ADVANCED]

(ISC)² Information Systems Security Engineering Professional (ISSEP)

The (ISC)² Information Systems Security Engineering Professional (ISSEP) certification is designed for experienced cybersecurity professionals who specialize in applying security engineering principles and practices. It demonstrates expertise in integrating security into projects, applications, business processes, and information systems, showcasing the ability to manage and implement secure systems throughout their lifecycle.

The (ISC)² ISSEP validates a candidate's knowledge in five security domains:

- **Systems Security Engineering Foundations**
- **Risk Management**
- **Security Planning and Design**
- **Systems Implementation, Verification and Validation**
- **Secure Operations, Change Management and Disposal**

Required exam: Earning the (ISC)² ISSEP certification requires passing two exams — the CISSP and ISSEP exams. See below for exceptions.
Prerequisites: CISSP or relevant experience.
Required experience: Candidates must hold a CISSP certification in good standing and have two (2) years cumulative, full-time experience in one or more of the six domains of the current ISSEP exam outline. Alternatively, candidates may satisfy the required experience with a minimum of seven (7) years cumulative, full-time experience in two or more of the current ISSEP domains. Earning a bachelors or masters degree in computer science, information technology (IT) or related fields or an additional credential from the ISC² approved list may satisfy one year of the required experience. Part-time work and internships may also count towards the experience requirement.

The (ISC)² ISSEP meets the requirements of the U.S. Department of Defense (DoD) Directive 8140.03.

[(ISC)² ADVANCED]

(ISC)² Information Systems Security Management Professional (ISSMP)

The (ISC)² Information Systems Security Management Professional (ISSMP) certification is designed for experienced cybersecurity professionals who focus on the management and leadership aspects of information security programs. It demonstrates advanced knowledge in establishing, presenting, and governing information security policies and procedures, as well as aligning security initiatives with organizational goals.

The (ISC)² ISSMP validates a candidate's knowledge in six security domains:

- **Leadership and Business Management**
- **Systems Lifecycle Management**
- **Risk Management**
- **Threat Intelligence and Incident Management**
- **Contingency Management**
- **Law, Ethics, and Security Compliance Management**

Required exam: Earning the (ISC)² ISSMP certification requires passing two exams — the CISSP and ISSMP exams. See below for exceptions.
Prerequisites: CISSP or relevant experience.
Required experience: Candidates must hold a CISSP certification in good standing and have two (2) years cumulative, full-time experience in one or more of the six domains of the current ISSMP exam outline. Alternatively, candidates may satisfy the required experience with a minimum of seven (7) years cumulative, full-time experience in two or more of the current ISSMP domains. Earning a bachelors or masters degree in computer science, information technology (IT) or related fields or an additional credential from the ISC² approved list may satisfy one year of the required experience. Part-time work and internships may also count towards the experience requirement.

The (ISC)² ISSMP meets the requirements of the U.S. Department of Defense (DoD) Directive 8140.03.

[(ISC)² ADVANCED]

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

The (ISC)² Certified Secure Software Lifecycle Professional (CSSLP) certification is designed for software development and security professionals who are responsible for applying best practices to each phase of the Software Development Lifecycle (SDLC). It demonstrates expertise in building, deploying, and maintaining secure software that mitigates vulnerabilities and addresses security risks.

The (ISC)² CSSLP validates a candidate's knowledge in eight security domains:

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

Required exam: Earning the (ISC)² CSSLP certification requires passing one exam — the CSSLP.
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 work experience in one or more of the eight domains of the ISC² CSSLP Common Body of Knowledge (CBK). Candidates may satisfy one year of the required experience with a four-year bachelors or masters degree in computer science, information technology (IT) or related fields. Part-time work and internships may also count towards the experience requirement.

The (ISC)² CSSLP meets the requirements of the U.S. Department of Defense (DoD) Directive 8140.03.

[(ISC)² INTERMEDIATE]

(ISC)² Systems Security Certified Practitioner (SSCP)

The (ISC)² Systems Security Certified Practitioner (SSCP) is a globally recognized IT security administration and operations certification 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:

- **Security Concepts and Practices**
- **Access Controls**
- **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.
Prerequisites: Candidates who pass the SSCP exam, but do not have the required work experience, will become an Associate of (ISC)².
Required experience: Candidates must have a minimum of one (1) year full-time experience in one or more of the domains of the current SSCP exam outline. Candidates may satisfy one year of the required experience with a four-year bachelors or masters degree in computer science, information technology (IT) or related fields. Part-time work and internships may also count towards the experience requirement.

The (ISC)² SSCP meets the requirements of the U.S. Department of Defense (DoD) Directive 8140.03.

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 (ISC)² annual maintenance fee (AMF) for the three years that the credential is valid. As a certified member you only pay a single AMF regardless of how many certifications you hold. AMFs are as follows;

- **$135 for members who hold CISSP, SSCP, CCSP, CGRC, CSSLP, ISSAP, ISSEP or ISSMP certifications**
- **$50 for members who hold the CC certification**
- **$50 for Associates of (ISC)² which is due upon the anniversary of achieving associate status**

For example, in the Americas, the CISSP certification cost would be a total of $884 — $749 for the exam plus the $135 AMF.

(ISC)² exam prices are normally $599 in the Americas, with the CISSP exam costing $749, the SSCP exam costing $249 and the CC exam costing $199. 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.

(ISC)² Recertification and Renewal

(ISC)² certifications are valid for three years and may be renewed by earning and submitting 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 AMF.

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 Certification Salary and Career Information

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

(ISC)² certifications are highly regarded credentials, and this is reflected in (ISC)² certification expected salaries. In *Certification Magazine*'s 2023 survey of certification salaries, five of the currently available (ISC)² certifications made the Top 75 average salaries. Two of their certifications made the top 15, with the CISSP ranking at ninth and the CCSP ranking at 13th. Also in the Top 75 were the CSSLP, the SSCP and the CC.

A review of the certification data collected by PayScale shows that even the Associate of (ISC)² credential is of value, with an average annual salary of $77,000. Moving along the (ISC)² certification path, holders of a SSCP credential can earn an average salary of $83,000.

The premier (ISC)² Certified Information Systems Security Professional (CISSP) certification commands an average salary of $130,000, while the CISSP Concentrations have yearly salaries of $120,000 for management professionals (ISSMP), $125,000 for security architects (ISSAP), and $136,000 for security engineers (ISSEP).

Government organizations and contractors are popular employers, which is not surprising given that all the (ISC)² certifications (except the CC certification) are U.S. Department of Defense (DoD) Directive 8140.03 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 CC, CCSP, CISSP and the SSCP.

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.

Check Point Certifications

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 certifications at three levels of certification that are designed to take learners' skill sets from beginner to expert:

- **Check Point Certified Security Administrator (CCSA R81.20)**
- **Check Point Certified Security Expert (CCSE R81.20)**
- **Check Point Certified Security Master (CCSM)**
- **Check Point Certified Security Master Elite (CCSME)**

[CHECK POINT ENTRY-LEVEL]

Check Point Certified Security Administrator (CCSA R81.20)

The Check Point Certified Security Administrator (CCSA) certification is designed for IT professionals with a basic understanding of Check Point implementations. It is the lowest level on the Check Point certification path and covers various security administration tasks on Check Point hardware and software.

The CCSA certification validates a candidate's understanding of these Check Point topics and skills:

- **Fundamental Check Point Technology knowledge**
- **Network Security**
- **System Administration**
- **Network Fundamentals**
- **Basic Concepts of VPN**
- **Managing User Access**
- **TCP/IP Networking**
- **Unix-like and/or Windows OS**

Required exam: Earning the CCSA certification requires passing one exam — CCSA (Exam 156-215.81.20).
Prerequisites: None are required. However, candidates must complete a three-day course.
Recommended experience: Check Point recommends exam takers have 6 to 12 months of hands-on experience with Check Point products and a good understanding of networking and TCP/IP.

[CHECK POINT INTERMEDIATE]

Check Point Certified Security Expert (CCSE R81.20)

The Check Point Certified Security Expert (CCSE) certification is designed for IT professionals who know their way around Windows and UNIX servers and already have significant experience in Check Point system support. Candidates should also know how to design, maintain, optimize, and protect an enterprise network from even the most aggressive cyber threats. Preparation for the Check Point Certified Security Expert certification enables IT professionals to configure gateways, firewalls, VPNs, and content security software.

The CCSE 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 certification requires passing one exam — CCSE (Exam 156-315.81.20).
Prerequisites: Candidates must earn the CCSA certification prior to attempting this certification. Candidates earning the R77 or prior CCSE must restart with the CCSA exam.
Recommended experience: Check Point recommends that candidates have extensive hands-on experience with Check Point products, strong networking skills, Windows and UNIX server management skills, and a good understanding of security certificate management.

[CHECK POINT ADVANCED]

Check Point Certified Master (CCSM)

The Check Point Certified Master (CCSM) certification is designed for IT professionals who have developed the highest skills in managing and implementing Check Point products and technologies. The exam deals with issues and problems related to commands, configuration of VPN tunnels, troubleshooting NAT, and other advanced topics. Candidates should know how to approach common deployment scenarios and apply common troubleshooting practices.

The CCSM 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 certification requires passing both the CCSA and CCSE exams, plus any two Infinity Specialist accreditations.
Prerequisites: Candidates who have earned the CCSA and the CCSE certifications plus two Infinity Specialist accreditations will automatically be awarded the CCSM certification.
Recommended experience: Check Point recommends candidates have extensive hands-on experience with Check Point products, advanced networking and server management skills, and a broad understanding of network security.

[CHECK POINT ADVANCED]

Check Point Certified Security Master Elite (CCSME)

The CCSM Elite certification is designed for experienced IT professionals who have reached the highest level of technical mastery. There is no specific exam for the CCSM Elite certification.

The CCSM Elite 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: There is no exam for the CCSME certification, however you must have passed the CCSA and CCSE exams in order to be eligible.
Prerequisites: Candidates who have earned the CCSM certification plus two subsequent Infinity Specialist accreditations will automatically be awarded the CCSM Elite certification.
Recommended experience: Check Point recommends candidates have extensive hands-on experience with Check Point products, advanced networking and server management skills, and a broad understanding of network security.

How Much Does It Cost to Get Check Point Certified?

Check Point certification costs vary by testing program, exam type, and region. You can find current prices on the Pearson Vue website by creating a Pearson VUE account, logging in and selecting the exam you are interested in under "Exam Catalog."

A search for U.S. prices during this guide's preparation found that the CCSA and the CCSE exams cost $250 each. Infinity Specialist accreditations vary by location and course.

Check Point Recertification and Renewal

Check Point certifications are only valid for two (2) years. Certifications, like security, must be kept current to be truly effective, so we strongly encourage you to constantly refresh and keep your certification current.

Because the exams are updated frequently, be prepared to retake exams when a new version comes out. It is up to the individual learner to monitor the changes and updates to the Check Point certification system.

Check Point Certification Salary and Career Information

According to Payscale, IT professionals with a Check Point CCSA certification can anticipate earning an average annual salary of around $89,000 (USD). A Check Point CCSE makes an average of $94,000 (USD) per year. Similar figures are unavailable for CCSM and CCSME, but one could anticipate entering the six figure earning realm.

CBT Nuggets considers the CCSA one of the more accessible certifications for those trying to break into the information security field. Additionally, the cost of the CCSA

certification is reasonable compared to other certifications. Considering the earnings potential for Check Point certified IT professionals, it's well worth the effort.

Check Point Certification Training

CBT Nuggets currently offers one Check Point video training course, with more on the way as of the time of this guide's writing. It is important to note that the exam associated with this course has been retired, however, it still retains value as a training resource.

- **Check Point Certified Security Administrator CCSA R80 (156-215.80)**

Check the CBT Nuggets website regularly for new Check Point training, as the library is constantly being updated.

CompTIA Certifications

CompTIA is a non-profit organization with membership comprising more than 200 leading IT companies, 2,000 member companies and 3,800 business partners spanning the IT industry.

As an IT industry trade organization, CompTIA aims to ensure there's 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 2.5 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. 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?**
- **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**

What is CompTIA Certification?

Unlike vendor certifications, CompTIA certifications are vendor-neutral, which means they validate the skills associated with a technology rather than a vendor product built on a technology. IT professionals who earn these certifications achieve a level of expertise that can be applied universally, regardless of vendor. For example, someone with CompTIA Network+ certification can apply their knowledge and skills to Cisco or Juniper networking technologies — at a basic level.

The CompTIA certification program encompasses certs in five categories:

- **Core**
- **Infrastructure**
- **Data & Analytics**
- **Cybersecurity**
- **Professional**

In their CompTIA Certification Roadmap, CompTIA sees the 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 8140/8570.01-M). This can provide certified professionals with job opportunities in the Federal government sector.

CompTIA Core Certifications

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

- **CompTIA IT Fundamentals+ (ITF+)**
- **CompTIA A+**
- **CompTIA Network+**
- **CompTIA Security+**
- **CompTIA Tech+**

CompTIA A+, CompTIA Network+, and CompTIA Security+ are all DoD 8140/8570.01-M approved certifications.

[COMPTIA CORE]

CompTIA IT Fundamentals+ (ITF+)

CompTIA IT Fundamentals+ (ITF+) 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:

- **IT Concepts and Terminology**
- **IT Infrastructure**
- **Applications and Software**
- **Software Development**
- **Database Fundamentals**
- **Security**

Required exam: Earning the CompTIA IT Fundamentals+ certification requires passing one exam — CompTIA IT Fundamentals+ (FC0-U61).
Prerequisites: None.
Recommended experience: No prior experience is necessary, however CompTIA recommends that candidates 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 knowledge and skills associated with these topics:

- **Mobile Devices**
- **Networking**
- **Hardware**
- **Virtualization and Cloud Computing**
- **Hardware and Network Troubleshooting**
- **Operating Systems**
- **Security**
- **Software Troubleshooting**
- **Operational Procedures**

Required exam: Earning the CompTIA A+ certification requires passing two exams — CompTIA A+ 220-1101 and CompTIA A+ 220-1102.
Prerequisites: None.
Recommended experience: CompTIA recommends that candidates have 9 to 12 months hands-on experience in the lab or field 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 for those looking 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 a candidate's knowledge and skills associated with these topics:

- **Networking Fundamentals**
- **Network Implementations**
- **Network Operations**
- **Network Security**
- **Network Troubleshooting**

Required exam: Earning the CompTIA Network+ certification requires passing one exam, but there are currently two versions available — CompTIA Network+ (N10-009) was launched in June 2024 to replace CompTIA Network+ (N10-008) which will retire in December 2024.

Prerequisites: None.

Recommended experience: CompTIA recommends that candidates have obtained CompTIA A+ certification and have at least 9 to 12 months of hands-on experience in an entry-level/junior networking experience.

[COMPTIA CORE]

CompTIA Security+

The CompTIA Security+ certification is designed to build a core foundation of skills that are essential to pave the way towards a fulfilling and successful career in cybersecurity. The Security+ certification validates a candidate's knowledge and skills associated with these topics:

- **General Security Concepts**
- **Threats, Vulnerabilities and Mitigations**
- **Security Architecture**
- **Security Operations**
- **Security Program Management and Oversight**

Required exam: Earning the CompTIA Security+ certification requires passing one exam — CompTIA Security+ (SY0-701).

Prerequisites: None.

Recommended experience: 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 certifications 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 Cloud+ is an approved certification for DoD 8140.03.

[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 sysadmin, network administrator, cloud engineer, systems or network engineer, and data center manager. The Cloud+ certification validates a candidate's knowledge and skills associated with these Cloud topics:

- **Cloud Architecture**
- **Deployment**
- **Operations**
- **Security**
- **DevOps Fundamentals**
- **Troubleshooting**

Required exam: Earning the CompTIA Cloud+ certification requires passing one exam, but there are currently two versions available — CompTIA Cloud+ (CV0-004) was launched in September 2024 to replace CompTIA Cloud+ (CV0-003) which will retire in early 2025.

Prerequisites: None.

Recommended experience: No prior experience is necessary, however CompTIA recommends that candidates have about 5 years total experience in the IT industry, including 2-3 years as a systems administrator or cloud engineer.

[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 a candidate's knowledge and skills associated with these Linux topics:

- **System Management**
- **Security**
- **Scripting, Containers and Automation**
- **Troubleshooting**

Required exam: Earning the CompTIA Linux+ certification requires passing one exam — CompTIA Linux+ (XK0-005).

Prerequisites: None.

Recommended experience: No prior experience is necessary, however CompTIA recommends that candidates have CompTIA A+, Network+ and Server+ certifications, as well as 12 months of experience working with Linux servers.

[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 a candidate's knowledge and skills associated with these Server topics:

- **Server Hardware Installation and Management**
- **Server Administration**
- **Security and Disaster Recovery**
- **Troubleshooting**

Required exam: Earning the CompTIA Server+ certification requires passing one exam — CompTIA Server+ (SK0-005).

Prerequisites: None.

Recommended experience: No prior experience is necessary, however CompTIA recommends that candidates have obtained the CompTIA A+ certification (or equivalent knowledge), as well as 2 years of experience working in a server environment.

CompTIA Data & Analytics Certifications

CompTIA Data and Analytics certifications are a new addition to CompTIA's technical certification path. As the importance for data analytics grows, more job roles are required to set context and better communicate vital business intelligence. Collecting, analyzing, and reporting on data can drive priorities and lead business decision-making. There are currently three certifications available for Data and Analytics:

- **CompTIA Data+**
- **CompTIA DataSys+**
- **CompTIA DataX**

[COMPTIA DATA & ANALYTICS]

CompTIA Data+

The CompTIA Data+ certification is designed for early-career data analytics professionals tasked with developing and promoting data-driven business decision-making. The Data+ certification validates a candidate's knowledge and skills associated with these topics:

- **Data Concepts and Environments**
- **Data Mining**
- **Data Analysis**
- **Visualization**
- **Data Governance, Quality & Controls**

Required exam: Earning the CompTIA Data+ certification requires passing one exam — CompTIA Data+ (DA0-001).

Prerequisites: None.

Recommended experience: CompTIA recommends candidates have 18–24 months of experience in a report/business analyst job role, exposure to databases and analytical tools, a basic understanding of statistics, and data visualization experience.

[COMPTIA DATA & ANALYTICS]

CompTIA DataSys+

The CompTIA DataSys+ certification is a foundational level data management certification that focuses on the logistics of data administration and security. It is the only vendor-neutral database certification on the market, allowing candidates to develop database administrator skills regardless of vendor. The DataSys+ certification validates a candidate's knowledge and skills associated with these topics:

- **Database Fundamentals**
- **Database Deployment**
- **Database Management and Maintenance**
- **Data and Database Security**
- **Business Continuity**

Required exam: Earning the CompTIA DataSys+ certification requires passing one exam — CompTIA DataSys+ (DS0-001).

Prerequisites: None.

Recommended experience: CompTIA recommends candidates have 2-3 years of experience in a database administrator role.

[COMPTIA DATA & ANALYTICS]

CompTIA DataX

The CompTIA DataX certification is an advanced skills development program designed for highly experienced data scientists to solidify a comprehensive understanding of critical data tools and concepts. Although only

released in mid-2024, it is already highly regarded as a vendor neutral data science certification. The DataX certification validates a candidate's knowledge and skills associated with these topics:

- **Mathematics and Statistics**
- **Modeling, Analysis and Outcomes**
- **Machine Learning**
- **Operations and Processes**
- **Specialized Applications of Data Science**

Required exam: Earning the CompTIA DataX certification requires passing one exam — CompTIA DataX (DY0-001).
Prerequisites: None.
Recommended experience: CompTIA recommends candidates have 5+ years of experience in data science or a similar role.

CompTIA Cybersecurity Certifications

CompTIA Cybersecurity certifications make up the fourth step of the CompTIA technical certification path. These certifications are for advanced and expert-level professionals. There are three certs at this tier which are all DoD Directive 8140.03M approved:

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

[COMPTIA CYBERSECURITY]

CompTIA Cybersecurity Analyst (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 a candidate's knowledge and skills associated with these topics:

- **Security Operations**
- **Vulnerability Management**
- **Incident Response and Management**
- **Reporting and Communication**

Required exam: Earning the CompTIA CySA+ certification requires passing one exam — CompTIA CySA+ (CS0-003).
Prerequisites: None.
Recommended experience: CompTIA recommends candidates have CompTIA Network+ or Security+ certification, or the equivalent knowledge, and at least four years of hands-on information security or related experience.

[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 a candidate's knowledge and skills associated with these topics:

- **Planning and Scoping**
- **Information Gathering and Vulnerability Scanning**
- **Attacks and Exploits**
- **Reporting and Communication**
- **Tools and Code Analysis**

Required exam: Earning the CompTIA PenTest+ certification requires passing one exam — CompTIA PenTest+ (PT0-002).
Prerequisites: While there is no required prerequisite, PenTest+ is intended to follow CompTIA Security+ and has a technical, hands-on focus.

Recommended experience: CompTIA recommends candidates have CompTIA Network+ or Security+ certification, or the equivalent knowledge, and at least 3-4 years of hands-on information security or related experience.

[COMPTIA CYBERSECURITY]

CompTIA Advanced Security Practitioner (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 a candidate's knowledge and skills associated with these topics:

- **Security Architecture**
- **Security Operations**
- **Governance, Risk and Compliance**
- **Security Engineering and Cryptography**

Required exam: Earning the CompTIA CASP+ certification requires passing one exam — CompTIA CASP+ (CAS-004).
Prerequisites: None.
Recommended experience: CompTIA recommends candidates have at least ten years of general hands-on IT experience, with at least five years of that experience focused on security.

CompTIA Professional Certifications

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

- **CompTIA Project+**
- **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 a candidate's knowledge and skills associated with these topics:

- **Project Basics**
- **Project Constraints**
- **Communication and Change Management**
- **Project Tools and Documentation**

Required exam: Earning the CompTIA Project+ certification requires passing one exam — CompTIA Project+ (PK0-005).
Prerequisites: None.
Recommended experience: CompTIA recommends candidates have the equivalent of at least 6-12 months of project management experience in an IT environment.

[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+ certification validates a candidate's knowledge and skills associated with these topics:

- **Cloud Concepts**
- **Business Principles of Cloud Environments**
- **Management and Technical Operations**
- **Governance, Risk, Compliance and Security for the Cloud**

Required exam: Earning the CompTIA Cloud Essentials+ certification requires passing one exam — CompTIA Cloud Essentials+ (CLO-002).

Prerequisites: None.

Recommended experience: CompTIA recommends candidates have the equivalent of at least 6-12 months experience in an IT environment with some 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

CompTIA 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+ exams.

[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 pass both CompTIA A+ and Linux+ exams.

[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 pass both CompTIA Network+ and Cloud+ exams.

[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+ exams.

[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 CNIP stackable certification, you must pass both CompTIA Network+ and Linux+ exams.

CompTIA Stackable Cybersecurity Certifications

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 Security Analytics Expert (CSAE)**
- **CompTIA Security Infrastructure Expert (CSIE)**

[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 pass the CompTIA A+, Network+ and Security+ exams.

[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 the Security+ and Cloud+ exams.

[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 pass the Security+ and CySA+ exams.

[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 pass the Security+ and PenTest+ exams.

[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 the Security+, PenTest+ and CySA+ exams.

[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 pass the Security+, CySA+ and CASP+ exams.

[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 pass the Security+, CySA+, PenTest+ and CASP+ exams.

Getting Your CompTIA Stackable Certifications

When you complete the set of CompTIA certifications that represent a particular CompTIA Stackable Certification, you will automatically be 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 $138 and $509, depending on the exam. For CompTIA A+, you must pass two exams for a total cost of $506. For CompTIA Security+, the single CompTIA certification exam costs $404. The cost for the CompTIA Network+ exam is $369.

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.

You can also verify your certifications using a Digital Badge. Clicking on a Digital Badge allows you and anyone you share it with to access your current and validated certification status. Once you earn a CompTIA certification, you'll receive an email letting you know that you can claim your digital badge via the Credly website.

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. (CE fees are required for this option)

- **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 the majority of 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. There are currently four CompTIA certifications that are GFL:

- **CompTIA IT Fundamentals+ (ITF+)**
- **CompTIA Cloud Essentials+**
- **CompTIA Server+**
- **CompTIA Project+**

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+:** $73,000
- **CompTIA Server+**: $71,000
- **CompTIA Network+:** $77,000
- **CompTIA Project+:** $81,000
- **CompTIA Linux+:** $88,000
- **CompTIA Security+:** $85,000
- **CompTIA CTT+:** $85,000
- **CompTIA Cloud+:** $80,000
- **CompTIA CASP+:** $99,000

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 such as experience, location and job sector.

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 Security+ (SY0-701)
  - CompTIA Network+ (N10-008)*
  - CompTIA A+ (220-1101)
  - CompTIA A+ (220-1102)
  - CompTIA ITF+ (FC0-U61)

- **Infrastructure Series**
  - CompTIA Cloud+ (CV0-003)*
  - CompTIA Linux + (XK0-005)
  - CompTIA Server+ (SK0-005)

- **Cybersecurity Series**
  - CompTIA CySA+ (CS0-003)
  - CompTIA PenTest+ (PT0-002)
  - CompTIA CASP+ (CAS-004)

- **Data Analytics Series**
  - CompTIA Data+ (DA0-001)

- **Additional Professional Series**
  - CompTIA Project+ (PK0-005)
  - CompTIA Cloud Essentials+ (CLO-002)

**CompTIA has released new exams for these certifications (N10-009 and CV0-004), however these trainings are still relevant and valuable resources. As of the time of this guide's writing, an updated Network+ exam training will be released in 2024. Be sure to check CBT Nuggets CompTIA training for new and updated training relevant to your personal CompTIA certification goals.*

Cisco Certifications

Many cybersecurity threats may be in the application layer, but defense starts at the network layer. Network administrators or engineers working in a Cisco shop will find a good match between these Cisco security certifications and their existing networking skills.

Cisco Network Security Certifications

With Cisco certifications, everything starts with networking. These Cisco security certifications validate a candidate's skills and knowledge in securing and protecting on-premise and cloud network infrastructures that organizations rely upon. These certifications then are at the professional and expert levels, which provide a good path forward for anyone who wants to progress in their career securing networks.

- **Cisco Certified Network Professional - Security (CCNP Security)**
- **Cisco Certified Internetwork Expert - Security (CCIE Security)**

[CISCO PROFESSIONAL]

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:

- **Security Concepts**
- **Network Security**
- **Securing the Cloud**
- **Content Security**

- **Cisco Security Products**

Required exam: The core exam for the CCNP Security certification is Implementing and Operating Cisco Security Core Technologies (350-701 SCOR v1.1). Candidates must also choose one of seven concentration exams to earn the CCNP Security certification:

- Securing Networks with Cisco Firewalls (300-710 SNCF v1.1)
- Implementing and Configuring Cisco Identity Services Engine (300-715 SISE v1.1)
- Securing Email with Cisco Secure Email Gateway (300-720 SESA v1.1)
- Securing the Web with Cisco Secure Web Appliance (300-725 SWSA v1.0)
- Implementing Secure Solutions with Virtual Private Networks (300-730 SVPN v1.1)
- Automating and Programming Cisco Security Solutions (300-735 SAUTO v1.0)
- Designing and Implementing Secure Cloud Access for Users and Endpoints (300-740 SCAZT v1.0)

Prerequisites: None.

Recommended experience: Cisco recommends that candidate's have three to five years of experience implementing security solutions.

[CISCO EXPERT]

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 their ability to plan, design, deploy, operate, and optimize dual stack solutions (IPv4 and IPv6) for complex enterprise networks in hands-on lab exam. The CCIE - Security core exam validates a candidate's understanding of security topics, including:

- **Contextual Policy Enforcement**
- **Centralized Policy Orchestration**
- **Cloud Adoption**
- **Automation and Programmability**
- **Cisco Security Products**

Required exam: The written exam for the CCIE Security certification is Implementing and Operating Cisco Security Core Technologies (350-701 SCOR v1.1). CCIE candidates must then travel to a Cisco facility to take the CCIE Security Lab Exam v6.1.

Prerequisites: None.

Recommended experience: Cisco recommends that candidate's have five to seven years of experience with designing, deploying, operating, and/or optimizing security technologies and solutions.

Cisco Cybersecurity Certifications

Cisco's cybersecurity certifications equip IT professionals with the necessary skills to secure today's complex digital environments. These certifications focus on both the foundational and advanced aspects of cybersecurity and cover all the bases for learners to thrive in one of IT's most in-demand fields. Cisco's offerings range from associate-level certifications to advanced professional and expert tracks, providing a clear career progression path for those aiming to specialize in cybersecurity.

- **Cisco Certified Support Technician (CCST) Cybersecurity**
- **Cisco Certified CyberOps Associate**
- **Cisco Certified CyberOps Professional**

[CISCO ENTRY-LEVEL]

Cisco Certified Support Technician (CCST) Cybersecurity

This Cisco Certified Support Technician (CCST) Cybersecurity certification prepares entry-level cybersecurity professionals to operate, maintain, troubleshoot, and configure the Cisco devices and software that keep devices and networks secure. The CCST cybersecurity certification validates a candidate's understanding of security topics, including:

- **Security Principles**
- **Network and Endpoint Security**
- **Vulnerability Assessment**

- **Risk Management**
- **Incident Response and Handling**

Required exam: Earning the CCST cybersecurity certification requires passing one core exam - 100-160 CCST Cybersecurity.

Prerequisites: None.

Recommended experience: None.

[CISCO ENTRY-LEVEL]

Cisco Certified CyberOps Associate

The Cisco Certified CyberOp Associate certification is one of the most comprehensive ways of getting a thorough understanding of network security policies and procedures on a Cisco network. This certification is designed for new or aspiring IT professionals looking to specialize in cybersecurity as well as experienced IT professionals looking to prove their skills with Cisco and related cybersecurity technologies. The CyberOps Associate certification validates a candidate's understanding of cybersecurity topics, including:

- **Security Concepts**
- **Security Monitoring**
- **Host-Based Analysis**
- **Network Intrusion Analysis**

Required exam: Earning the CyberOps Associate certification requires passing one core exam - Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS v1.1).

Prerequisites: None.

Recommended experience: None.

[CISCO PROFESSIONAL]

Cisco Certified CyberOps Professional

The Cisco Certified CyberOp Professional certification proves you have the ability and reliability that companies need to perform active defense security roles. It is designed to develop advanced knowledge and

skills and enhance the career of IT professionals already in the cybersecurity industry. The CyberOps Professional certification validates a candidate's understanding of cybersecurity topics, including:

- **Security Fundamentals**
- **Security Techniques**
- **Security Processes**
- **Security Automation**

Required exam: Earning the CyberOps Professional certification requires passing one core exam - Performing CyberOps Using Cisco Security Technologies (350-201 CBRCOR v1.1) - as well as passing one concentration exam:

- Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (300-215 CBRFIR v1.1)
- Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (300-220 CBRTHD v1.0)

Prerequisites: None.

Recommended experience: Cisco recommends that candidate's have have three to five years of experience in IT security and implementing enterprise networking solutions.

Cisco Specialist Certifications

Cisco's Specialist certifications are designed to allow learners to customize their specializations towards a particular career focus. Specialist certifications can be earned on the path to professional and expert certification and they can also be earned independently to advance skills and knowledge in specific areas.

- **Cisco Certified Specialist – CyberOps Core**
  Exam: Performing CyberOps Using Cisco Security Technologies (350-201 CBRCOR v1.1)
- **Cisco Certified Specialist – CyberOps Forensic Analysis and Incident Response**
  Exam: Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (300-215 CBRFIR v1.1)

- **Cisco Certified Specialist – Threat Hunting and Defending**

  Exam: Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps (300-220 CBRTHD v1.0)
- **Cisco Certified Specialist - Security Core**

  Exam: Implementing and Operating Cisco Security Core Technologies (350-701 SCOR v1.1)
- **Cisco Certified Specialist - Network Security Firepower**

  Exam: Securing Networks with Cisco Firewalls (300-710 SNCF v1.1)
- **Cisco Certified Specialist - Security Identity Management Implementation**

  Exam: Implementing and Configuring Cisco Identity Services Engine (300-715 SISE v1.1)
- **Cisco Certified Specialist - Email Content Security**

  Exam: Securing Email with Cisco Secure Email Gateway (300-720 SESA v1.1)
- **Cisco Certified Specialist - Web Content Security**

  Exam: Securing the Web with Cisco Secure Web Appliance (300-725 SWSA v1.0)
- **Cisco Certified Specialist - Network Security VPN Implementation**

  Exam: Implementing Secure Solutions with Virtual Private Networks (300-730 SVPN v1.1)
- **Cisco Certified DevNet Specialist - Security Automation and Programmability**

  Exam: Automating and Programming Cisco Security Solutions (300-735 SAUTO v1.0)
- **Cisco Certified Specialist – Secure Cloud Access**

  Exam: Designing and Implementing Secure Cloud Access for Users and Endpoints (300-740 SCAZT v1.0)

How Much Does It Cost to Get Cisco Certified?

Cisco security certification costs vary by the level of certification and exam type. Pearson VUE administers all Cisco exams except CCIE lab exams. Exams range in price from $125 USD for an entry-level certification to $1,900 USD for a CCIE Cisco Kit Mobile Lab Exam.

Cisco Recertification and Renewal

Most Cisco certifications are valid for three (3) years from the date you earn the certification. The Cisco Certified Support Technician (CCST) entry-level certifications never expire.

You can recertify Cisco certification at any time during the active three year period by re-taking the exam for your existing certification, advancing to the next level of certifications, earning Continuing Education credits, or a combination of both.

If you do not meet all recertification requirements by your certification expiration date, you must complete the full exam process again to earn active status.

Cisco Certification Salary and Career Information

According to Payscale, IT professionals with a Cisco CCNP security certification can anticipate earning an average annual salary of around $106,000 (USD), with the average salary increasing to $139,000 (USD) with the CCIE certification. Salaries are influenced by several factors, including professional experience, geography, and industry, but it can quite safely be said that earning a Cisco security certification can put you ahead of the game in terms of career progression and earning potential.

A Cisco certification can be beneficial to someone at any stage of their career with their well designed career certification pathway. From entry all the way to expert level, a Cisco security certification is the gold standard for validating IT security skills and knowledge. IT professionals who specialize in networking security and cybersecurity will more than likely work in a Cisco environment at some point.

Cisco Certification Training

CBT Nuggets offers a variety of Cisco security training courses tailored to all levels of learners. There are courses that map to the following Cisco security certification exams;

- Cisco Certified Network Professional - Security (CCNP Security)
    - Core Exam
    - Securing Networks with Cisco Firewalls (300-710 SNCF)
- Cisco Certified Support Technician (CCST) Cybersecurity
- Cisco Certified CyberOps Associate

As well as courses which focus on the skills needed to implement and manage popular Cisco security solutions and help learners build foundations towards more advanced certifications.

In addition to quality, engaging video training from expert-level trainers, CBT Nuggets provides everything a learner needs to study for Cisco security certifications and skills, including virtual labs, supplemental files, practice exams, and access to a robust Learner Community.