INSIDER PRO

FROM IDG

EXPERT INSIGHT INTO HOW TECHNOLOGY DRIVES BUSINESS

INSIDER EXCLUSIVE

GUIDE TO TOP SECURITY CERTIFICATIONS

Security professionals are in high demand and with the right certification, you're in even higher demand. To help you decide which certs are for you, **we've compiled a list of top security certifications.**

BY NEAL WEINBERG

POWERED BY CIO COMPUTERWORLD CSO InfoWorld NETWORKWORLD

IDGInsiderPro.com

Cyberattacks against enterprise networks are on the rise, and the bad guys, from solo actors all the way up to nation states, show no signs of easing up anytime soon. As the cost of a data breach keeps increasing, companies are spending more money on security, resulting in tons of unfilled security positions.

So, what are you waiting for? It's time to put on that white hat, get certified and make the move into a high-paying security position. According to CyberSeek, an interactive online tool created by CompTIA through a federal grant from NIST, common feeder roles that lead into a career in security include networking, software development, systems engineer and financial and risk analysis.

Security breach statistics are staggering. In 2018 alone, A Marriott breach affected 500 million guests, at UnderArmor it was 150 million records, Quora exposed 100 million records, the genealogy site MyHeritage exposed 92 million records and the list goes on and on. There were a total of 1,232 breaches that we know of in 2018 and the number of compromised records was up 133 percent compared to 2017.

The price tag of a security breach is also rising. The average cost of a data breach worldwide was $3.86 million in 2018, up 6.4 percent over the previous year, according to the Ponemon Institute. In the U.S., the average cost was far higher, at $7.9 million, which includes $4.2 million in lost business. It turns out that U.S. consumers take a particularly dim view of companies that fail to protect their data.

Shortage of security practitioners is getting worse

There is no question that security professionals are in demand. And there is also no question that we're facing a severe shortage of security practitioners. ISACA, a non-profit information security advocacy group, says there is a shortfall of 2 million security professionals worldwide.

To comment on this story, visit Insider Pro's Twitter page.

According to the ISACA's State of Cybersecurity 2019 report, 69 percent of enterprise respondents say their cybersecurity teams are understaffed. "While the number of high-profile cyberattacks are on the ascent on one side, so are the number of cybersecurity vacancies going unfilled," says Renju Varghese, Fellow & Chief Architect, CyberSecurity & GRC at HCL Technologies, which partnered with ISACA on the report.

Frank Downs, director of cybersecurity practices at ISACA, puts it this way: "The most prized hire within a cybersecurity organization is a skilled professional who not only understands the business operation and how cybersecurity fits into the greater needs of the organization, but also knows how to communicate well." In the survey, 58 percent of respondents said their organizations have unfilled cybersecurity positions. And the survey results show a 6 percent increase, from 26 percent in 2017 to 32 percent in 2018, in organizations that took at least six months to fill open cybersecurity positions.

CyberSeek puts the total number of cybersecurity job openings in the U.S. at more than 300,000, with around 770,000 cybersecurity professionals employed in today's workforce. And the projections are that the number of openings could hit 500,000 in the U.S. and 3 million worldwide by 2021.

GETTY IMAGES

Certifications lead to high-salary positions

The way CyberSeek describes the security career ladder, employees start at entry level roles like security specialist or technician, security analyst or investigator, incident response analyst or IT auditor. Then they move into mid-level positions like security analyst, security consultant or penetration tester/vulnerability analyst. Advanced level positions include security manager/administrator, security engineer and security architect.

Compensation for these highly sought-after security positions follows the basic law of supply and demand, so the pay is excellent and there's plenty of opportunity for advancement at your current place of employment or somewhere else. In fact, ISACA says that retention is major problem for most companies. "An overwhelming 82 percent indicate that most individuals leave their companies for another because of financial and career incentives such as higher salaries, bonuses and promotions," according to the report.

In the Robert Half Technology Salary Guide 2019, positions like systems security administrator and network security administrator command salaries of between $93,000 up to $160,000; data security analysts can earn from $105,000 to $178,000 and security managers can expect a salary range from $116,000 to $200,000, depending on experience level and size of the company.

The hottest security-related certifications are certified ethical hacker (CEH), certified information systems security professional (CISSP) and global information assurance certification (GIAC), according to the Robert Half report.

GETTY IMAGES

Certifications that pay off big-time

For prospective security practitioners looking to optimize their certification dollars, CyberSeek has put together a listing of the most commonly held certifications and the number of job listings requesting that specific certification. The data shows that 173,000 people currently hold the entry-level CompTIA Security+ certification, but there are only 36,000 openings requesting that specific certification. On the other hand, there are 54,000 people that currently hold Global Information Assurance Certification (GIAC) and there are 36,000 job openings, which makes the odds more favorable.

The most sought-after certification is CISSP. There are 77,000 openings requesting CISSP certification and only 76,000 people currently hold the certification, which means your chances of landing a job are pretty high. And your job prospects are even better if you have a Certified Information Systems Auditor (CISA) certification, because there are only 33,000 people with the certification and there are 45,000 job listings seeking people with CISA certification.

Neal Weinberg *is an award-winning technology journalist and a regular contributor to Insider Pro. You can contact him at neal@misterwrite.net*

INSIDER EXCLUSIVE

TOP SECURITY CERTIFICATIONS

Here's a list of the **top security certifications, broken down by entry-level, intermediate and advanced certifications.**

ENTRY-LEVEL Security Certifications

1. CompTIA Security+

Description: This is the place to start your journey into security certifications. CompTIA's Security+ is a popular, well-respected, vendor-neutral security certification. Security+ credential holders are recognized as possessing superior technical skills, broad knowledge and expertise in multiple security-related disciplines. The certification combines hands-on trouble shooting with practical problem-solving skills to ensure those who pass the certification can both identify and address security incidents. It covers network security, compliance and operation security, threats and vulnerabilities, as well as application, data and host security.

Requirements: At least two years of experience working in network security. Candidates should also consider first obtaining CompTIA's Network+ certification. The CompTIA Security+ credential is approved by the U.S. Department of Defense and complies with the standards for ISO 17024.

Details: Exam is 90 questions in 90 minutes and costs $339.

2. GSEC: SANS GIAC Security Essentials

Description: Another popular entry-level credential is the GIAC Security Essentials (GSEC), designed for professionals seeking to demonstrate that they not only understand information security terminology and concepts but also possess skills and technical expertise necessary to occupy "hands-on" security roles. GSEC holders have knowledge and technical skills in areas such as identifying and preventing common and wireless attacks, access controls, authentication, password management, DNS, cryptography fundamentals, ICMP, IPv6, public key infrastructure, Linux, network mapping and network protocols.

Requirements: There are no specific requirements, but a training course is recommended.

Details: Priced at $769 for applicants who take the training course, or $1,899 for those who don't. The proctored exam is 180 questions over five hours.

3. Cisco CCNA Cyber Ops

Description: The associate-level Cisco CCNA Cyber Ops certification is designed for people

GETTY IMAGES

Data security analysts can earn from **$105,000 to $178,000** and **security managers** can expect a salary range from **$116,000 to $200,000**

who work as analysts in security operations centers (SOCs) in large companies and organizations. The Cisco CCNA Cyber Ops certification program provides practical, relevant, and job-ready certification curricula aligned closely with specific, real-world tasks needed as an associate-level SOC professional. Candidates will be prepared to help determine through various types of event monitoring whether an intrusion or security-related event is currently occurring or has occurred. Candidates will gain skills to support the front lines of an active security defense, including monitoring systems, responding to alerts and alarms, analyzing activity logs, and blocking live attacks as they happen. The Cisco Security curriculum is specific to the best practices of network security administrators, engineers, and experts using the latest Cisco equipment, devices, appliances, and popular security analysis tools.

Requirements: There are no specific requirements, but candidates must pass two separate exams: Understanding Cisco Cybersecurity Fundamentals and Implementing Cisco Cybersecurity Operations.

The exams test a candidate's knowledge and skill needed to successfully handle the tasks, duties and responsibilities of an associate-level security analyst.

Details: Passing scores are set by using statistical analysis and are subject to change. The Cybersecurity Fundamentals test is 55-60 questions in 90 minutes. The SECOPS exam is 60-70 questions in 90 minutes. The tests cost $300.

4. (NCSF) NIST Cybersecurity Framework/Foundation

Description: The NIST CSF Foundation training course outlines the challenges surrounding critical infrastructure sector security and explains how implementing a security program based on the NIST Cybersecurity Framework can help organizations mitigate these issues. The Foundation certification program is designed to teach IT, business and cybersecurity professionals the fundamentals of Digital Transformation, Cybersecurity Risk Management and the NIST Cybersecurity Framework.

Requirements: There are no course prerequisites.

Details: The 60-minute exam consists of 40 questions and costs $995.

> * The **average cost of a data breach** worldwide was **$3.86 million** in 2018, **up 6.4 percent** over the previous year.
>
> **– SOURCE: PONEMON INSTITUTE**

GETTY IMAGES

INTERMEDIATE-LEVEL Security Certifications

1. CEH: Certified Ethical Hacker (EC-Council)

Description: The Certified Ethical Hacker (CEH) is an intermediate-level credential offered by the International Council of E-Commerce Consultants (EC-Council). It's a must-have for IT professionals pursuing careers in ethical hacking. CEH credential holders possess skills and knowledge of a wide range of hacking practices. According to the EC-Council, an ethical hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system. The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

Requirements: Candidates should take the comprehensive, five-day CEH training course prior to taking the exam. Candidates may self-study, but must submit documentation of at least two years of work experience in information security with employer verification. Self-study candidates must also pay an additional $100 application fee. Education may be substituted for experience, but this is evaluated on a case-by-case basis.

Details: The four-hour exam consists of 125 multiple-choice questions and costs $950.

2. CompTIA Cybersecurity Analyst (CySA+)

Description: The CompTIA Cybersecurity Analyst (CySA+) is a vendor-neutral certification designed for professionals with three to four years of security and behavioral analytics experience. The behavioral analytics skills covered by CySA+ identify and combat malware and advanced persistent threats, resulting in enhanced threat visibility across a broad attack surface. CySA+ is for IT pros looking to perform data analysis, configure and use threat-detection tools and secure and protect applications and systems within an organization.

Requirements: A minimum of 3-4 years of hands-on information security or related experience. While there is no required prerequisite, CySA+ is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus.

Details: The exam, which consists of 85 questions over 165 minutes, costs $349.

3. NIST Cybersecurity Framework/Practitioner

Description: The NIST Practitioner certification program is designed to teach Engineering, Operations and Business Risk professionals how to design, implement, operate and continually improve a NIST Cybersecurity Framework program that will enable enterprises to identify protect, detect, respond and recover from cyberattacks.

Requirements: Candidates must hold a valid NIST Cybersecurity Foundation Certification or have equivalent knowledge.

Details: The exam, which costs $995, consists of 65 multiple choice questions in 120 minutes.

300,000+

total number of cybersecurity job openings in the U.S

– SOURCE: CYBERSEEK

4. CFR: CyberSec First Responder

Description: If you find incident response and investigation intriguing, check out the Logical Operations CyberSec First Responder (CFR) certification. This ANSI-accredited and U.S. DoDD-8570 compliant credential recognizes security professionals who can design secure IT environments, perform threat analysis, and respond appropriately and effectively to cyberattacks.

Requirements: Ideal for people with 2+ years of experience in IT or information security. Training program is 5 days (35 hours).

Details: The two-hour,100-question exam costs $300.

GETTY IMAGES

ADVANCED-LEVEL Security Certifications

1. CEH (Practical): Certified Ethical Hacker (Practical) (EC-Council)

Description: Once a candidate obtains the CEH designation, a logical progression on the EC-Council certification ladder is the Certified Ethical Hacker (Practical) credential. A recent addition to the EC-Council certification portfolio, the CEH (Practical) designation targets the application of CEH skills to real-world security audit challenges and related scenarios.

Requirements: The preparatory course for this certification is the Certified Ethical Hacker course. While there is no additional course or training required, the EC-Council strongly recommends that candidates attempt the C|EH (Practical) exam only if they have attended the current C|EH course/ equivalent.

Details: To obtain the credential, candidates must pass a rigorous six-hour practical examination. Conducted on live virtual machines, candidates are presented 20 scenarios with questions designed to validate a candidate's ability to perform tasks such as vulnerability analysis, identification of threat vectors, web app and system hacking, OS detection, or network scanning, packet sniffing, steganography, virus identification, and more. Exam costs $550.

2. CISM: Certified Information Security Manager (ISACA)

Description: The Certified Information Security Manager (CISM) is an advanced credential for IT professionals responsible for managing, developing and overseeing information security systems in enterprise-level applications, or for developing organizational security practices. ISACA's organizational goals are specifically geared toward IT professionals interested in the highest quality standards with respect to audit, control and security of information systems. The CISM credential targets the needs of IT security professionals with enterprise-level security management responsibilities. Credential holders possess advanced and proven skills in security risk management, program development and management, governance, and incident management and response. Holders of the CISM credential, which is designed for experienced security professionals, must agree to ISACA's Code of Professional Ethics, pass a comprehensive examination, possess at least five years of security experience, comply with the organization's continuing education policy and submit a written application. Some combinations of education and experience may be substituted for the experience requirement.

Requirements: A minimum of five years of information security work experience, including at least three years in information security management or in areas such as risk management, incident management, governance or program development and management.

Details: Candidates must pass the exam and agree to the ISACA code of ethics. Exam fees are $575 for members; $760 for nonmembers. The exam consists of 150 questions over four hours.

3. CISSP: Certified Information Systems Security Professional (ISC)2

Description: Certified Information Systems Security Professional (CISSP) is an advanced-level certification for IT pros offered by the International Information Systems Security Certification Consortium, known as (ISC)2. This vendor-neutral credential is recognized worldwide for its standards of excellence. CISSP credential holders are decision-makers who possess expert knowledge and technical skills necessary to develop, guide and then manage security standards, policies and procedures within their organizations. The CISSP continues to be highly sought after by IT professionals and is well recognized by IT organizations. It is a regular fixture on most-wanted and must-have security certification surveys.

Requirements: A minimum of five years of experience in at least two of (ISC)2's eight knowledge domains, or four years of experience in at least two domains and a college degree or an approved credential. The domains are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communications and Network Security, Identity and Access Management (IAM), Security Assessment and Testing, Security Operations, and Software Development Security. There are also optional concentrations that enable candidates to achieve certifications in CISSP Ar-

The **hottest security-related certifications** are certified ethical hacker (CEH), certified information systems security professional (CISSP) and global information assurance certification (GIAC).

chitecture, CISSP Engineering and CISSP Management.

Details: The basic CISSP exam costs $699; and each CISSP concentration is $599. Exam is 100-150 questions in three hours.

4. CCNP: Cisco Certified Network Professional Security

Description: This certification is aligned to the job role of the Cisco Network Security Engineer responsible for security in routers, switches, networking devices and appliances, as well as choosing, deploying, supporting and troubleshooting firewalls, VPNs, and IDS/IPS solutions for their networking environments.

Requirements: CCNA Security or any CCIE certification can act as a prerequisite. This certification requires passing four separate tests covering the knowledge of a network security engineer to configure and implement security on Cisco network perimeter edge devices, the technologies used to strengthen security of a network perimeter, advanced firewall architecture and configuration with the Cisco next-generation firewall, utilizing access and identity policies, secure access solutions, and overall network threat mitigation and endpoint control solutions. It also includes the fundamental concepts of bring your own device (BYOD), secure mobility and VPN solutions.

Details: Each exam is 90 minutes (65 - 75 questions) and costs $300.

5. CISA: Certified Information Systems Auditor (ISACA)

Description: The CISA certification is seen as a world-renowned standard of achievement for any security professional who has to audit, control and monitor information technology and business systems. Being CISA-certified showcases your audit experience, skills and knowledge, and demonstrates you are capable to assess vulnerabilities, report on compliance and institute controls within the enterprise.

Requirements: Candidates must have five years of work experience in the field performing duties that are specifically related to information systems auditing, control, assurance or security.

Details: Exam is 200 questions over four hours. Cost is $575 for ISACA members and $760 for non-ISACA members.

6. CSSP: Certified Cloud Security Professional (ISC)²

Description: The CCSP demonstrates that candidates have the advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud, using best practices, policies and procedures established by the cybersecurity experts at (ISC)². This certification helps candidates demonstrate proficiency in cloud data security, cloud architecture and design, as well as day-to-day operations, application security considerations and more. Anyone who is looking to take a role in a cloud-based environment will be well served with a CCSP certification.

Requirements: Candidates must have a minimum of five years of full-time experience in IT, of which three years must be in information security. They must also have one year of experience in at least one of the six areas of the CCSP's Common Body of Knowledge (CBK).

Details: The exam costs $549, contains 125 questions and is four hours long. ◆

GETTY IMAGES