TechTarget | SearchSecurity

E-guide

PRO+ Content

Your Guide to Security Certifications

Explore vendor-neutral and vendor-specific security certifications

In this e-guide

In this e-guide:

Close to 70% of hiring enterprises require a security certification for open cybersecurity positions, according to ISACA's State of Cyber Security 2017 report.

With that in mind, which vendor-neutral and vendor-specific security certifications will best suit your educational or career needs? We're here to help you decide.

In this guide, you'll find:

- **An alphabetized list of security certifications**
- **A brief description of each certification**
- **Pointers to further details**

We also provide some tips on choosing the right certification for you.

In this e-guide

Vendor-neutral certification guide for information security pros

Ed Tittel and Mary Kyle, Contributors

This article provides a brief analysis of the vendor-neutral landscape and suggested educational options for your information security career path that you can pursue at any point in your career.

(ISC)²'s Certified Information Systems Security Professional (CISSP), SANS Institute's Global Information Assurance Certification (GIAC) and the ISACA Certified Information Security Manager (CISM) are the best-known and most widely followed IT security certification programs. That said, the CompTIA Advanced Security Practitioner (CASP) is included in the U.S. Department of Defense Directive 8570.01-M, which means that credential is bound to be extremely popular with government employees and government contractors alike. The number of certified individuals in these programs varies; some have fewer than 10,000 certified members, while there are now more than 93,000 individuals worldwide who hold the CISSP designation. Broader programs, such as the Certified Information Systems Auditor (CISA) and the Certified Fraud Examiner (CFE), which both cover more than strictly information security topics, have populations that number 109,000 and nearly 45,000, respectively.

In this e-guide

CompTIA's Security+ still weighs heavily among the entry-level certs as it continues to attract strong interest and participation. Today, the number of Security+ certifications tops 284,000. IBM and Security University (SU) include Security+ in some of their own certification programs, and the U.S. Department of Defense accepts Security+ to meet its most basic information assurance (IA) certification requirements. Holders of Security+ can also substitute it for one year of job experience toward the CISM certification requirements. Security+ remains our leading selection as the best recognized and the best overall entry-level information security certification currently available. To earn Security+ certification, candidates must pass a single exam.

More broadly, the entry-level credentials with the most weight are CompTIA's Security+, SANS GIAC Information Security Fundamentals Certification (GISF) and the (ISC)²'s Systems Security Certified Practitioner (SSCP). Keep your eye on the Prometric Cyber Security Fundamentals credential, introduced in February 2013, which could eventually join this group. The CISSP, the CISM and the SANS GIAC intermediate and senior credentials remain the best bets for those seeking more than entry-level security credentials, while the Certified Ethical Hacker (CEH) is now a viable option for those interested in highlighting their current system penetration techniques and counter-hacking skills. The Certified Protection Professional (CPP), Professional Certified Investigator (PCI), Physical Security Professional (PSP) and the various CISSP concentrations are restricted to

In this e-guide

the most senior members of the security community, simply because they require five to nine years of work experience in the security field for candidates to even qualify for the exams.

There have been some interesting changes to the requirements for individuals who wish to work in information security for any arms of the U.S. government, branches of the U.S. military or contractors who supply workers and/or services into those markets. In this realm, IA means more or less the same as what computer scientists -- and your humble authors -- often refer to as information security. This is also a world where the word "qualification" means that individuals have obtained clearance and competence documents necessary to fill IA job roles, and have met certification and hands-on requirements to demonstrate their skills and abilities and real-world performance. Thus, when you see the word "qualified" in some infosec or IA certification names, you must understand that this speaks to a hands-on orientation and testing that includes performance-based methods in its scope and coverage.

Given this landscape, we recommend the following security certification ladder that individuals can start and climb at any point, depending on their current knowledge, skills and experience.

In this e-guide

Start your security certification journey with a broad, entry-level security cert. This could be one of the following credentials, any of which will provide an excellent and thorough background in computer security theory, operations, practices and policies:

CompTIA Security+

CompTIA's Security+ certification has become *the* entry-level information security certification of choice for IT professionals seeking to pursue further work and knowledge in this area. That's why it's our first choice and leading recommendation at this level.

(ISC)² Systems Security Certified Practitioner (SSCP)

The International Information Systems Security Certification Consortium is also home to the CISSP, the best-known senior-level security certification (senior-level certs are covered later in this article). If you're of a mind to go that route, the SSCP is a great way to prepare.

Those interested in pursuing the SSCP need to possess at least one year of experience in one or more of the seven SSCP Common Body of Knowledge domains. Candidates must also pass an exam to obtain the credential. Those who do not yet meet the experience requirement may choose to first obtain the Associate of (ISC)² certification, which is available to any candidate who passes the CAP, CCFP, CISSP, CSSLP, HCISPP or SSCP exam.

In this e-guide

SANS GIAC Information Security Fundamentals Certification (GISF)

The SANS Institute is long-standing and well-recognized powerhouse in the security industry. Likewise, its GIAC certifications continue to accrue visibility and acceptance. The GISF opens the door to other credentials in the respected SANS GIAC program. Since the GISF is an entry-level credential, there are no prerequisites; candidates need only pass a single exam to obtain the credential.

From here, practitioners can tackle a premium or senior-level security certification. Most such certifications require three or more years of relevant, on-the-job experience. Many also require submitting papers or research results in addition to passing exams, as well as taking specific classes. Of these, four are particularly worthy of mention, and pick up where the previous three leave off:

CompTIA Advanced Security Practitioner (CASP)

The CASP is intended as a follow-on to Security+ and is intended to recognize IT professionals with three or more years of direct, day-to-day information security experience, with skills and knowledge to match. The CASP requires continuing education for maintenance or a re-take of the exam every three years. It costs around $390, which is less than the CISSP, but it is ranked the same for a variety of Department of Defense-related IT positions, which will no doubt contribute to its future popularity. CompTIA announced an update to the CASP certification exam in February 2015 that

In this e-guide

includes new questions about contemporary threats as well as troubleshooting processes related to data, endpoint and network security.

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

The CISSP is arguably the best-known senior-level security certification in North America. It frequently shows up in top 10 certification wish and want lists, and it is often requested by name in job postings and classified ads. Those who are interested in extending their CISSP credentials should also look into its three concentrations -- Architecture (CISSP-ISSAP), Engineering (CISSP-ISSEP) and Management (CISSP-ISSMP). The CISSP exam costs $599 with an additional fee of $399 for each of the three specialty concentration areas.

Candidates without a college degree must possess at least five years of paid professional experience in two or more of the 8 domains to qualify for the credential; degreed individuals only need four years of paid experience. A waiver for one year of experience may be obtained (approval required) if the candidate possesses an (ISC)² credential from an approved (ISC)² list.

SANS GIAC Security Certifications

SANS Global Information Assurance Certification offers numerous topical specializations that extend the GISF and the GIAC Security Essentials Certification (GSEC), including firewalls, incident handling, intrusion analysis, Windows and Unix administration, information security officer and systems and network auditor certifications. This is a topical, timely and highly

technical program based on outstanding training online or at SANS conferences. For those willing to acquire four of these individual credentials (two of them "gold") and sit for a lengthy exam in two parts, moving on to the GIAC Security Engineer (GSE) certification probably makes sense.

Qualified Information Security Professional Certification

Security University's certification requires some of the best, most intense and hands-on information security training around. Highly popular with government and industry security heavies, this program is expensive, demanding and time-consuming, but it's worth the intensive investment it requires to complete.

Don't hesitate to let us know if our analysis of this landscape has missed anything. We can't claim to know, see or be able to find everything, so all feedback will be gratefully acknowledged. As always, feel free to email us with comments or questions.

Next article

In this e-guide

Vendor-specific information security certifications

Ed Tittel and Mary Kyle, Contributors

Introduction: Choosing vendor-specific security certifications

The process of choosing vendor-specific security certifications is much simpler than choosing vendor-neutral ones. In the vendor-neutral landscape, you must evaluate the pros and cons of various programs to select a viable option. On the vendor-specific side, it's only necessary to follow these three steps:

1. Inventory your organization's security infrastructure and identify which vendors' products or services are present
2. Check this guide (and vendor websites for items that don't appear here) to determine whether a certification applies to products or services in your organization.

In this e-guide

3. Decide if spending the time and money to obtain such credentials (or to fund them for your employees) is worth the resulting benefits.

In an environment where numerous jobs exist for every qualified IT security professional, the benefits of individual training and certifications can be hard to appraise. Many employers pay the costs involved in achieving certification in an effort to develop and retain their employees, as well as to boost the organization's in-house expertise. Most see this as a win-win for employers and employees alike. On the flip side, however, employers often require full or partial reimbursement for related costs they incur if employees decide to leave their jobs sooner than some specified payback period after cert completion.

Now, we're ready to dive into a big heaping bowl of alphabet soup to explore the vendor-specific security-related certification programs that occupy this landscape.

Basic certifications

CCNA Security -- Cisco Certified Network Associate (CCNA) Security
Prerequisites: A valid Cisco CCNA Routing and Switching, Cisco Certified Entry Networking Technician (CCENT) or Cisco Certified Internetwork Expert (CCIE) certification

In this e-guide

This credential recognizes associate-level professionals who can install, troubleshoot and monitor Cisco routed and switched network devices for the purpose of protecting both the devices and networked data. A person with a CCNA Security certification knows how to plan and implement a security infrastructure, can identify threats and vulnerabilities to networks, and can mitigate security threats. CCNA credential holders also possess the technical skills and expertise necessary to maintain access control lists, virtual LANs and routing protocols including IP, Ethernet and gateway. The successful completion of one exam is required to obtain this credential.
Source: Cisco

CCSA R77 -- Check Point Certified Security Administrator
Prerequisites: While there are no prerequisites, CCSA R77 training and six months to one year of experience with Check Point products are recommended.

Check Point's foundation-level credential prepares individuals to manage basic installations of Check Point security systems products and technologies, such as: Security Gateway, firewall, SmartConsole, remote access VPN, IPSEC VPN, user directory, antispam/virus/mail, URL filtering and identity awareness. Credential holders also possess the skills necessary to configure such systems and manage day-to-day operations of Check Point Security Gateway and Management Software Blades systems on GaiA operating systems. Topics covered include securing Internet

communications, backing up and restoring networks, upgrading products, troubleshooting network connections, configuring security policies, protecting email, protecting message content, defending networks from intrusions and other threats, analyzing attacks, managing user access in a corporate LAN environment, and configuring tunnels for remote access to corporate resources. Candidates must pass a single exam to obtain this credential.
Source: Check Point Software Technologies Ltd.

CMSS -- Certified McAfee Security Specialist
Prerequisites: None, although completion of an associated training course is highly recommended.

CMSS certification holders possess the knowledge and technical skills necessary to install, configure, manage and troubleshoot specific McAfee products or, in some cases, a suite of products. Candidates should possess one to three years of direct experience with one of the specific product areas.

The current products targeted by this credential include:

- CMSS -- DLPe, focused on McAfee Data Loss Prevention Endpoint products

In this e-guide

- CMSS -- ePO, focused on McAfee ePolicy Orchestrator and VirusScan products
- CMSS -- HIPs, focused on McAfee Host Intrusion Prevention system
- CMSS – NGFW, focused on McAfee Next Generation Firewall
- CMSS -- NSP, focused on McAfee Network Security Platform

All credentials require passing one exam. The new SIEM credential mentioned in the introduction covers the Security Information and Event Management products from McAfee.
Source: McAfee, Inc.

FCESP -- Fortinet Certified Email Security Professional
Prerequisites: None, although the training course, "221-FortiMail Email Filtering" is highly recommended.

This credential recognizes individuals who configure, manage, monitor and administer FortiMate devices, and work with SMTPS, SMTP over TLS, and S/MIME to regulate use of company resources and protect against spam, malware and message-borne threats. Candidates must possess an understanding of FortiMail administration and configuration functions as well as email security threats and how to protect against them. To obtain the FCESP, candidates must pass a single exam.
Source: Fortinet Inc.

In this e-guide

FCNSA -- Fortinet Certified Network Security Administrator
Prerequisites: None, although the training course, "201-FortiGate Multi-Threat Security Systems I" is highly recommended.

This credential recognizes individuals who configure, manage, monitor and administer FortiGate devices, and work with VPNs and firewall policies. Candidates must possess an understanding of the Fortinet line of products, hardware and services. To obtain the FCNSA, candidates must pass a single exam.
Source: Fortinet Inc.

MTA -- Microsoft Technology Associate
This credential started as an academic-only credential for students, but it was made available to the general public in 2012, which is why it is included here. There are 11 different MTA credentials across three tracks (IT Infrastructure with four certs, Database with one and Development with six). Nearly all of these credentials include a security component or topic area.

To earn each MTA certification, candidates must pass the corresponding exam.
Source: Microsoft

SCS -- Symantec Certified Specialist
This security certification program focuses on data protection, high availability and security skills involving Symantec products. To become an

In this e-guide

SCS, candidates must select an area of focus and pass an exam. All exams cover core elements, such as installation, configuration, product administration, day-to-day operation and troubleshooting for the selected focus area.

As of this writing, the following exams are available:

- Exam 250-254: Administration of Symantec Cluster Server 6.1 for Unix
- Exam 250-255: Administration of Symantec Storage Foundation 6.1 for Unix
- Exam 250-271: Administration of Symantec NetBackup 7.5 for Unix
- Exam 250-310: Administration of Symantec Enterprise Vault 10.0 for Exchange
- Exam 250-315: Administration of Symantec Endpoint Protection 12.1
- Exam 250-316: Administration of Symantec Backup Exec 2012
- Exam 250-352: Administration of Veritas Storage Foundation and High Availability Solutions 6.0 for Windows
- Exam 250-371: Administration of Symantec NetBackup 7.5 for Windows
- Exam 250-403: Administration of Symantec Management Platform 7.1

In this e-guide

- Exam 250-407: Administration of Symantec Client Management Suite 7.1 / 7.x
- Exam 250-409: Administration of Symantec Clearwell eDiscovery Platform 7.1
- Exam 250-410: Administration of Symantec Control Compliance Suite 11.x
- Exam 250-505: Administration of Symantec Data Center Security: Server Advanced 6.0
- Exam 250-513: Administration of Symantec Data Loss Prevention 12
- Exam 250-530: Administration of Symantec Network Access Control 12.1

In addition to exams for current product offerings, Symantec maintains a number of exams on legacy product versions. Current available legacy exam topics include administration of Veritas cluster servers, storage foundation for Unix, Symantec NetBackup and data loss prevention. IT professionals working on legacy products should consult Symantec to determine if a particular credential is still available.
Source: Symantec Corp.

In this e-guide

Intermediate certifications

CCNP Security -- Cisco Certified Network Professional (CCNP) Security
Prerequisites: CCNA Security or any CCIE certification.

This Cisco credential recognizes professionals who are responsible for router, switch, networking device and appliance security. Candidates must also know how to select, deploy, support and troubleshoot firewalls, VPNs and IDS/IPS products in a networking environment. Successful completion of four exams is required.
Source: Cisco Systems

CCSE R77 -- Check Point Certified Security Expert
Prerequisite: CCSA certification R70 or later

This is an intermediate-level credential aimed at VPN implementations, advanced user management and firewall concepts, policies, data loss prevention, strategies and advanced troubleshooting for Check Point Software Blades. The CCSE focuses on Check Point's VPN, Security Gateway and Management Server systems. To acquire this credential, candidates must pass one exam.
Source: Check Point Software Technologies Ltd.

In this e-guide

Cisco Cybersecurity Specialist
Prerequisites: None; however, CCNA Security certification and an understanding of TCP/IP are recommended.

This Cisco credential targets IT security professionals who possess expert-level technical skills and knowledge in the field of threat detection and mitigation. The certification focuses on areas such as event monitoring, event analysis (traffic, alarm, security events) and incident response. One exam is required.
Source: Cisco

CSSA -- Certified SonicWall Security Administrator (CSSA)
The CSSA now comes from Dell Inc. thanks to its 2012 acquisition of SonicWall. The exam covers basic administration of SonicWall appliances and the network and system security behind such appliances. Classroom training is available but not required to earn CSSA; candidates must pass one exam to become certified.
Source: Dell Inc.

EnCE -- EnCase Certified Examiner
Prerequisites: Candidates must attend 64 hours of authorized training or have 12 months of computer forensic experience. Completion of a formal application process is also required.

In this e-guide

Aimed at both private- and public-sector computer forensic specialists, this certification permits individuals to become certified in the use of Guidance Software's EnCase computer forensics tools and software.

Individuals gain certification by passing a two-phase exam: a computer-based component and a practical component.
Source: Guidance Software Inc.

EnCEP -- EnCase Certified eDiscovery Practitioner
Prerequisites: Candidates must attend one of two authorized training options and have three months of experience in eDiscovery collection, processing and/or project management. A formal application process is also required.

Aimed at both private- and public-sector computer forensic specialists, this certification permits individuals to become certified in the use of Guidance Software Inc.'s EnCase eDiscovery software, and recognizes their proficiency in eDiscovery planning, project management and best practices from legal hold to file creation. EnCEP professionals possess technical skills necessary to manage e-discovery, including search, collection, preservation and processing of electronically stored information (ESI), in accordance with the Federal Rules of Civil Procedure.

In this e-guide

Individuals gain certification by passing a two-phase exam: a computer-based component and a scenario component.
Source: Guidance Software Inc.

FCNSP -- Fortinet Certified Network Security Professional
Prerequisite: Fortinet Certified Network Security Administrator (FCNSA)

The FCNSP credential recognizes individuals who install, configure and troubleshoot all FortiGate product features and functionality. Candidates should also have a good working knowledge of FortiAnalyzer, in addition to a basic understanding of the entire Fortinet line of products and services. FCNSP candidates possess skills necessary to take advantage of features for large-scale environments such as HA and redundant VPNs to configure multiple FortiGate devices.

Candidates must pass the FCNSP exam, and have already passed the FCNSA exam.
Source: Fortinet Inc.

Oracle Certified Expert, Oracle Solaris 10 Certified Security Administrator
Prerequisite: Oracle Certified Professional, Oracle Solaris 10 System Administrator

This credential aims to identify experienced Solaris 10 administrators with security interest and experience. It's a mid-range credential that focuses on general security principles and features, installing systems securely, application and network security, principles of least privilege, cryptographic features, auditing and zone security. A single exam -- geared toward the Solaris 10 operating system or the OpenSolaris environment -- is required to obtain this credential.
Source: Oracle

RSA Archer CA -- RSA Archer Certified Administrator (CA)
Prerequisites: None, although EMC² highly recommends RSA training and two years of product experience as preparation for RSA certification exams.

EMC² offers this certification, which is designed for security professionals who manage, administer, maintain and troubleshoot the RSA Archer eGRC platform. Candidates must pass one exam (code 050-v5x-CAARCHER01), which focuses on integration and configuration management, security administration, and data presentation and communication features of the RSA Archer eGRC product.
Source: EMC Corporation

RSA SecurID CA -- RSA SecurID Certified Administrator (RSA Authentication Manager 8.0)
Prerequisites: None, although EMC² highly recommends RSA training and two years of product experience as preparation for RSA certification exams.

EMC² offers this certification, which is designed for security professionals who manage, maintain and administer enterprise security systems based on RSA SecurID system products and RSA Authentication Manager 8.0. RSA SecurID CAs can operate and maintain RSA SecurID components within the context of their operational systems and environments, troubleshoot security and implementation problems, and work with updates, patches and fixes. They can also perform administration functions and populate and manage users, set up and use software authenticators, and understand the configuration required for RSA Authentication Manager 8.0 system operations.
Source: EMC Corporation

RSA Security Analytics CA -- RSA Security Analytics Certified Administrator (CA)
Prerequisites: None, although EMC² highly recommends RSA training and two years of product experience as preparation for RSA certification exams.

This EMC² certification is aimed at security professionals who configure, manage, administer and troubleshoot the RSA Security Analytics product. Knowledge of the product's features, as well using the product to identify security concerns, is key.

Candidates must pass one exam (code 050-103-CARSASA01), which focuses on knowledge of RSA Security Analytics functions and capabilities,

configuration, management, monitoring and troubleshooting.
Source: EMC Corporation

SAINT certification
Prerequisites: None.

SAINT certification requires attending a training course geared toward information security professionals and system administrators. SAINT offers online and Jumpstart training in addition to classroom training. A full-course agenda is required to become certified.

The course focuses on TCP/IP and security fundamentals as well as installing, configuring and using SAINT and SAINTwriter, configuring scan range, performing vulnerability assessments with SAINTscanner, penetration testing with SAINTexploit, and vulnerability management using SAINTmanager. SAINT credential holders possess the technical skills necessary to resolve complex security issues using SAINT technologies.

There is no exam to achieve certification; however, candidates must be attend two days of training.
Source: SAINT Corp.

In this e-guide

Advanced certifications

CCIE Security -- Cisco Certified Internetwork Expert (CCIE) Security
Prerequisites: None; however, three to five years of professional working experience recommended.

Arguably one of the most coveted certifications around, the CCIE is in a league of its own. Having been around since 2002, the CCIE Security track is nonpareil for those interested in dealing with information security topics, tools and technologies in networks built using or around Cisco products and platforms. CCIE candidates possess expert technical skills and knowledge of security and VPN products, understanding of Windows, Unix, Linux, HTTP, SMTP, FTP and DNS, in-depth understanding of Layer 2 and 3 network infrastructures, and ability to configure end-to-end secure networks, as well as troubleshooting and threat mitigation.

To achieve certification, candidates must pass both a written and lab exam. The lab exam must be passed within 18 months of successful completion of the written exam.
Source: Cisco Systems Inc.

CCSM -- Check Point Security Master
Prerequisites: CCSE R70 or later, and experience with Windows Server, UNIX, TCP/IP and networking and Internet technologies.

In this e-guide

The CCSM is the most advanced Check Point certification available. This credential is aimed at security professionals who implement, manage and troubleshoot multifaceted Check Point security products. Candidates must be experts in perimeter, internal, Web and endpoint security systems. To acquire this credential, candidates must pass a written exam.
Source: Check Point Software Technologies Ltd.

CSSP -- Certified SonicWall Security Professional
Prerequisites: Associated CSSA certification.

Those who achieve this certification have attained a high level of mastery of Dell SonicWall products. In addition, credential holders can deploy, optimize and troubleshoot all associated product features. Earning a CSSP requires specific experience, taking an "Advanced Administration" course that focuses on either network security or secure mobile access, taking an e-learning course (Network Security track only) and passing the associated certification exam.
Source: Dell Inc.

IBM Certified Administrator – Tivoli Monitoring V6.3
Prerequisites: Security-related requirements include basic knowledge of SSL, data encryption and system user accounts.

Those who attain this certification can plan, install, configure, upgrade and customize workspaces, policies and more. In addition, credential holders can

In this e-guide

troubleshoot, administer and maintain an IBM Tivoli Monitoring V6.3 environment. Candidates must successfully pass one exam.
Source: IBM

IBM Certified Advanced Deployment Professional -- IBM Service Management Security and Compliance V4
This certification recognizes individuals who demonstrate a high level of implementation knowledge and skills in IBM Tivoli Security, risk and compliance products. Three exams are required to obtain this certification; the two required exams cover Tivoli Identity Manager V5.1 Implementation and Tivoli Access Manager for e-business V6.1.1 Implementation. Candidates may select the third exam from IBM Security Access Manager for Enterprise Single Sign-on V8.2 Implementation, or substitute with the CompTIA Security+, (ISC)² SSCP or (ISC)² CISSP. (Candidates should review the website for the current list of exams which qualify to fulfill the third exam requirement.)
Source: IBM

IBM Certified Advanced Deployment Professional -- IBM Service Management Security Intrusion Protection V1
Those who hold this certification must demonstrate they possess in-depth knowledge and technical skills in the area of IBM Tivoli Security Intrusion Protection products. To gain the credential, candidates must pass two IBM-specific exams (IBM Security SiteProtector Systems V2.0 SP8.1 and IBM

In this e-guide

Security Network Intrusion Prevention System V4.3 Implementation) and pass one of the following exams: (ISC)² SSCP, (ISC)² CISSP or SNIA Storage Networking Management & Administration. (Candidates should review the website for the current list of exams which qualify to fulfill the third exam requirement.)
Source: IBM

IBM Certified Deployment Professional -- Tivoli Federated Identity Manager V6.2.2
Prerequisites: None; however, there is an extended list of recommended knowledge and technical skills including knowledge of related products, HTTP, HTML and Web services, and data center methodologies.

Credential holders possess the technical skills necessary to install, configure, administer and maintain an IBM Tivoli Federated Identity Manager V6.2.2. A single exam is required to obtain the credential.
Source: IBM

Master CSSA -- Master Certified SonicWALL Security Administrator
The Master CSSA is an intermediate between the base-level CSSA credential (itself an intermediate certification) and the CSSP. To qualify for Master CSSA, candidates must pass three (or more) CSSA exams and then email training@sonicwall.com to request the designation. There are no other charges or requirements involved.
Source: Dell Inc.

In this e-guide

Conclusion

Remember, when it comes to selecting vendor-specific security certifications, you or your organization's existing or planned security product purchases should dictate your options. If your security infrastructure includes products from vendors not mentioned here, be sure to check with them to determine if training or certifications on such products are available.

Next article

In this e-guide

Which are the best cybersecurity certifications for beginners?

Mike Villegas, Vice President - K3DES LLC

I'm in college studying IT, and I'd like to pursue a career in security. Which are the best cybersecurity certifications for beginners?

Cybersecurity is a laudable and exciting profession. As the number of cybersecurity incidents continues to escalate, the demand for skilled cybersecurity professionals will only increase over the years.

The State of Cybersecurity Survey: Implications for 2016 conducted by ISACA in January 2016 reported that nearly 65% of the 461 cybersecurity managers and practitioners stated all entry-level cybersecurity applicants lacked the requisite skills to perform the tasks related to the jobs they were seeking. It further reports that 86% of those polled use on-the-job training as the means to develop needed technical skills. Only 16% would engage 2-year technical/trade schools and 4-year college/university applicants. It also stated that 38% of hiring is based on skills-based training and cybersecurity certifications.

In this e-guide

Cybersecurity certifications for beginners: Are they worth it?

A separate 2016 Cybersecurity Survey polling of nearly 3,000 IT and cybersecurity professionals reported that when hiring new graduates for entry-level cybersecurity positions, 63% of hiring managers stated that "it is difficult to identify who has an adequate level of skills and knowledge." It further reports that 81% are more likely to hire a cybersecurity applicant who holds a performance-based certification. These would include cybersecurity certifications that require demonstrable hands-on cyber skills as opposed to skills-based certifications.

For example, skills-based cybersecurity certifications include Certified Information Systems Auditor, CISSP, Certified Information Security Manager, Certified in Risk and Information Systems Control, Certified Secure Computer User, EC-Council Certified Security Specialist, Security+ and the GIAC cybersecurity essentials certification. Performance-based certifications include the Certified Ethical Hacker, Offensive Security Certified Professional, Offensive Security Web Expert, GIAC Web Application Defender, GIAC Certified Forensic Analyst, and CSX Practitioner. This is not a complete list, but it does include the mostly widely achieved cybersecurity certifications for beginners.

In this e-guide

Millennials are our future and the opportunities in cybersecurity abound. The cybersecurity and CIS degrees are a plus and prove the applicant has a good foundation and aptitude for information security. However, the best advice is to start with skills-based cybersecurity certifications, most of which require three to five years of experience. However, if an entry-level candidate has taken the exam and successfully passed it, it sends the employer a clear signal of the candidate's serious intention to grow into the position. You can attempt to take a performance-based certification examination but most entry-level candidates may find it more of a challenge.

But don't stop there. Get involved in professional organizations such as ISACA, ISSA and OWASP. Volunteer in local chapter events, such as conferences, seminars, chapter meetings and research projects. Network with member professionals and make an impression. Let them see your interest in cybersecurity and your passion to learn. Participate in collegiate cyberdefense competitions and above all, read, study and find your niche that you want to develop expertise in. When an opportunity arises, you will undoubtedly come to mind. We all look forward to you joining us fight the fight.

Next article

In this e-guide

About SearchSecurity

IT security pros turn to SearchSecurity.com for the information they require to keep their corporate data, systems and assets secure.

We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security certification training resources, security standard compliance, webcasts, white papers, podcasts, Security Schools, a selection of highly focused security newsletters and more -- all at no cost.

For further reading, visit us at http://SearchSecurity.com/

Images; Fotalia