Best Information Security Certifications For 2017

By Ed Tittel DECEMBER 13, 2016 5:28 AM

InfoSec professionals who want to set themselves apart as leaders in IT security should seriously consider one of these top five information security certifications for 2017.

When it comes to information security, you need only read the headlines to observe that those with malicious intent constantly find new and scary ways to access and misuse privileged information for criminal, unscrupulous or questionable purposes. As a result, IT professionals skilled in information security remain in very high demand. In 2016, there were more than 200,000 security positions available in the U.S., with forecasts pointing to 1.5 million open positions globally by 2019.

When evaluating prospective InfoSec candidates, employers frequently look to certification as one measure of excellence and commitment to quality. In this article, we take a look at five InfoSec certifications we consider to be leaders in the field of information security today:

1. CompTIA Security+
2. CEH: Certified Ethical Hacker
3. GSEC: SANS GIAC Security Essentials
4. CISSP: Certified Information Systems Security Professional
5. CISM: Certified Information Security Manager

This year's list includes entry-level credentials, like Security+ and GIAC Security Essentials, as well as more advanced certs, such as the CEH, CISSP and CISM. We also offer some additional certification options in the last section, as the field of information security is both wide and varied.

Security-related job roles cover a lot of ground, such as information security specialist, security analyst, network security administrator, system administrator (with security as a responsibility) and security engineer, as well as specialized roles such as malware engineer, intrusion analyst and penetration tester. Average salaries for information security specialists and security engineers – two of the most common job roles – vary widely depending on the source. For example, SimplyHired reports $120,000 for specialist positions, whereas Glassdoor's national average is just under $75,000. For security engineers, SimplyHired reports $93,000, with Glassdoor's average at $83,000.

If you're serious about advancing your career in the IT field and are interested in specializing in security, certification is a great choice. It's an effective way to validate your skills and show a current or prospective employer that you're qualified and properly trained.

Before examining the details of the top five InfoSec certs, take a look at the results of our informal job board survey. The data indicates the number of job posts nationwide in which our featured certifications were mentioned on a given day. The data should give you an idea of the relative popularity of each certification.

Job Board Search Results

Certification	SimplyHired	Indeed	LinkedIn Jobs	TechCareers	Total
CEH	1,977	2,184	1,427	257	5,845
CISM	3,286	3,585	2,337	10,629	19,837
CISSP	10,526	11,617	7,632	15,212	44,987
GSEC	1,317	1,477	954	128	3,876
Security+	3,038	3,396	1,275	1,431	9,140

Now let's take a closer look at the top five information security certifications for 2017, in no particular order.

1. CompTIA Security+

CompTIA's Security+ is a 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.

While Security+ is an entry-level certification, successful candidates should possess at least two years of experience working in the area of network security and should consider first obtaining the Network+ certification. IT pros who obtain the cert possess expertise in areas such as threat management, cryptography, identity management, security systems, security risk identification and mitigation, network access control, and security infrastructure. The CompTIA Security+ credential is also approved by the U.S. Department of Defense to meet Directive 8570.01-M requirements.

The Security+ credential requires a single exam, currently priced at $311 (discounts may apply to those who work for CompTIA member companies, and to full-time students). Training is available but not required. If you're thinking about taking the Security+ exam sometime in 2017, be aware that CompTIA released the current version – SY0-401 – in May 2014. Because the organization typically releases exams every three years, a new exam should be available in late spring or summer 2017.

IT professionals who earned the Security+ cert prior to Jan. 1, 2011 remain certified for life. Those who certify after that date must renew the certification every three years to stay current. To renew, candidates are required to pass the most current Security+ exam, pass a higher-level CompTIA exam or complete 50 continuing education units (CEUs) prior to the expiration of the three-year period. CEUs can be obtained by engaging in a variety of activities, such as teaching, blogging, publishing articles or white papers, and participating in professional conferences and similar activities.

CompTIA Security+ Facts & Figures

Certification Name	CompTIA Security+
Prerequisites & Required Courses	None. CompTIA recommends at least two years of experience in IT administration (with a security focus) and the Network+ credential before taking the Security+ exam.
Number of Exams	One: SYO-401
Cost of Exam	$311 (discounts may apply)
URL	https://certification.comptia.org/certifications/security
Self-Study Materials	Exam objectives, sample exam questions, the CertMaster online training tool, training kits, computer-based training and a comprehensive study guide are available at CompTIA.org.

MORE: CompTIA Certs & Career Paths

CompTIA Security+ Training

You'll find a number of companies offering online training, instructor-led and self-study courses, practice exams, and books to help you prepare for and pass the Security+ exam.

Pluralsight offers a series of Security+ video training courses as part of its monthly subscription plan for the latest SY0-401 exam. Split up into six sections, the training series is just more than 18 hours long and covers network security, compliance and operational security, threats and vulnerabilities, application, data and host security, access control and identity management, and cryptography.

360training.com offers a similar training lineup for the Security+ cert that is available for a one-time fee. At more than 16 hours, the video training is divided into 10 lessons that cover the SY0-401 exam objectives. The training includes hands-on demonstrations along with a student workbook to help you prepare for the exam.

If you want to test your security knowledge before attempting the real exam, Transcender offers a Security+ practice exam with more than 400 mock questions and nearly 500 study flashcards. The practice exam can be a good additional resource to online training and books, helping you gain confidence in your understanding of the exam objectives and knowledge of security essentials.

2. CEH: Certified Ethical Hacker

Hackers are innovators and constantly find new ways to attack information systems and exploit system vulnerabilities. Savvy businesses proactively protect their information systems by engaging the services and expertise of IT professionals skilled in beating hackers at their own game (often called "white hat hackers" or simply "white hats"). Such professionals use the same skills and techniques hackers use to identify system vulnerabilities and access points for penetration, and to prevent unwanted access to network and information systems.

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 on hacking practices in areas such as footprinting and reconnaissance, scanning networks, enumeration, system hacking, Trojans, worms and viruses, sniffers, denial-of-service attacks, social engineering, session hijacking, hacking web servers, wireless networks and web applications, SQL injection, cryptography, penetration testing, evading IDS, firewalls, and honeypots.

To obtain the CEH certification, candidates must pass one exam. A comprehensive five-day CEH training course is recommended, with the exam presented at the end of training. Candidates may self-study for the exam but must submit documentation of at least two years of work experience in information security with employer verification. Self-study candidates are also required to pay an additional $100 application fee. Education may be substituted for experience, but this is approved on a case-by-case basis.

Because technology in the field of hacking changes almost daily, CEH credential holders are required to obtain 120 continuing education credits for each three-year cycle.

CEH Facts & Figures

Certification Name	Certified Ethical Hacker (CEH)
Prerequisites & Required Courses	Training is highly recommended. Without formal training, candidates must have at least two years of information security-related experience and an educational background in information security, pay a nonrefundable eligibility application fee of $100, and submit an Exam Eligibility Application prior to purchasing an exam voucher.
Number of Exams	One: 312-50 (125 multiple-choice questions, four hours)
Cost of Exam	$500 EC-Council test center; $600 Pearson VUE test center
URL	https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
Self-Study Materials	EC-Council instructor-led courses, computer-based training, online courses and more are available at ECCouncil.org. A CEH skills assessment is also available for credential seekers.

MORE: EC Council Certs & Career Paths

Certified Ethical Hacker (CEH) Training

While EC-Council offers both instructor-led and online training for its CEH certification (as listed in the table above), IT professionals have plenty of other choices of self-study materials, including video-based training, practice exams and books.

Pluralsight currently offers several ethical hacking courses geared toward the 312-50 exam. With a monthly subscription, you get access to all of these courses plus everything else in Pluralsight's training library. Through Pluralsight's ethical hacking courses, IT professionals learn about session hijacking, reconnaissance and footprinting, SQL injection, enumeration, social engineering, and how to hack web servers, applications and mobile platforms.

360training.com offers a few training courses covering the Certified Ethical Hacking exam 312-50. Through an interactive environment, IT professionals get access to a lab where they can learn how to scan, test, hack and secure various systems. Topics covered include DDoS attacks, intrusion detection and virus creation.

Finally, Transcender offers a practice exam for the CEH 312-50 certification that includes 235 questions. Backed by its "pass the first time" guarantee, Transcender is so confident that this practice exam will help you prepare for the CEH exam that you can get a full refund if you don't pass the CEH exam.

3. GSEC: SANS GIAC Security Essentials

Another fine 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 the skills and technical expertise necessary for "hands-on" security roles. GSEC credential holders demonstrate 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.

Currently priced at $1,249, the GIAC Security Essentials exam is quite a bit more expensive than the Security+ exam. While a training program is not required, credential seekers may take a SANS course that includes the cost of the exam.

GSEC certifications must be renewed every four years. To renew, candidates must accumulate 36 continuing professional experience credits (CPEs). GIAC offers several ways to meet the CPE requirement. Some options are passing the current certification exam (worth 36 CPEs), attending or teaching approved courses, and publishing books, articles or research papers. In addition, credential holders must pay a certification maintenance fee of $399 every four years.

GSEC Facts & Figures

Certification Name	GIAC Security Essentials (GSEC)
Prerequisites & Required Courses	None, but training is recommended.
Number of Exams	One proctored exam (180 questions, five hours) Exam administered by Pearson VUE. Registration with GIAC required to schedule an exam.
Cost of Exam	$689, if part of training/bootcamp $1,249 (no training – referred to as a "certification challenge" or "certification attempt")
URL	http://www.giac.org/certification/security-essentials-gsec
Self-Study Materials	Training available from numerous sources, including SANS. Ric Messier's *GSEC GIAC Security Essentials Certification All-in-One Exam Guide* is also available from Amazon.

The SANS GIAC Program

In addition to the GSEC credential, SANS GIAC currently offers a full range of certifications (30 individual credentials, in fact) from entry to advanced levels for IT professionals seeking careers in the fields of security administration, forensics, legal, audit, management and software security. GIAC certifications are designed to stand alone; however, GIAC recommends that credential seekers obtain entry-level certifications and use them as skill builders for more advanced credentials.

4. CISSP: Certified Information Systems Security Professional

The Certified Information Systems Security Professional (CISSP) is an advanced-level certification for IT pros serious about careers in information security. Offered by the International Information Systems Security Certification Consortium, known as (ISC)2 and pronounced "ISC squared," 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 well recognized by IT organizations. It is a regular fixture on most-wanted and must-have security certification surveys.

CISSP is designed for experienced security professionals. A minimum of five years of experience in at least two of (ISC)2's eight Common Body of Knowledge (CBK) domains, or four years of experience in at least two of (ISC)2's CBK domains and a college degree, is required for this certification. CBK domains include Security and Risk Management, Asset Security, Security

Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

(ISC)2 also offers three CISSP concentrations targeting specific areas of interest in IT security:

- Architecture (CISSP-ISSAP)
- Engineering (CISSP-ISSEP)
- Management (CISSP-ISSMP)

CISSP concentration exams are $399 each, and credential seekers must currently possess a valid CISSP.

An annual fee of $85 is required to maintain the CISSP credential. Recertification is required every three years. To recertify, candidates must earn 40 continuing professional education (CPE) credits each year for a total of 120 CPEs within the three-year cycle.

CISSP Facts & Figures

Certification Name	Certified Information Systems Security Professional (CISSP) Optional CISSP concentrations: • CISSP Architecture (CISSP-ISSAP) • CISSP Engineering (CISSP-ISSEP) • CISSP Management (CISSP-ISSMP)
Prerequisites & Required Courses	At least five years of paid, full-time experience in at least two of the eight (ISC)^{2} domains or four years of paid, full-time experience in at least two of the eight (ISC)^{2} domains and a college degree.
Number of Exams	One for CISSP (250 multiple-choice and advanced innovative questions, six hours) One for each concentration area
Cost of Exam	CISSP is $599; each CISSP concentration is $399
URL	https://www.isc2.org/CISSP/Default.aspx
Self-Study Materials	See the CISSP Exam Preparation web page. A variety of training materials are available, including instructor-led, live online, on-demand and private training. An exam outline is available for candidate review, as well as study guides, a study app, interactive flashcards and practice tests.

MORE: (ISC)^{2} Certs & Career Paths

Certified Information Systems Security Professional (CISSP) Training

With the popularity of the CISSP certification, there is no shortage of available training options, including classroom-based training offered by (ISC)2 as well as online video courses, practice exams and books from third-party companies.

Pluralsight's CISSP series of courses cover the security concepts required for the certification exam. Current courses include security engineering, asset security, software development security and physical (or environmental) security. There are several courses still in development that will cover the topics of security and risk management, communications and network security, identity and access management, and more. Available for a low monthly fee, the CISSP is part of a subscription plan that gives IT professionals access to Pluralsight's complete library of video training courses.

360training.com also offers an online training course for the CISSP. The course, available for a one-time fee, features video lectures and hands-on demos, along with a student workbook to help you follow along. Topics include risk management, access control, application security, cryptography, security architecture and design, law, and investigation and ethics.

When you're ready to test your security knowledge, you can take a simulated exam that mimics the format and content of the real CISSP exam. Transcender offers a CISSP practice exam that includes over 900 practice questions and almost as many flashcards to help you prepare for this challenging exam. The practice exam covers all of the CISSP exam objectives and helps you identify your weak areas so that you're confident in your understanding of all of the CISSP content.

6. CISM: Certified Information Security Manager

The Certified Information Security Manager (CISM) is a top credential for IT professionals responsible for managing, developing and overseeing information security systems in enterprise-level applications, or for developing best organizational security practices. The CISM credential was introduced to security professionals in 2003 by the Information Systems Audit and Control Association (ISACA).

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.

Designed for experienced security professionals, CISM credential holders must agree to ISACA's Code of Professional Ethics, pass a comprehensive examination, possess at least five years of security experience, comply with the Continuing Education Policy and submit a written application. Some combinations of education and experience may be substituted to meet the experience requirement.

ISACA members who register early pay $450 for the exam; nonmembers pay $635 for early registration. Regular registration fee for members is $500 and $685 for nonmembers. The CISM credential is valid for three years, and credential holders must pay an annual maintenance fee of $45 (ISACA members) or $85 (nonmembers). Credential holders are also required to obtain a minimum of 120 continuing professional education (CPE) credits over the three-year term to maintain the credential. At least 20 CPEs must be earned every year.

CISM Facts & Figures

Certification Name	Certified Information Security Manager (CISM)
Prerequisites & Required Courses	To obtain the CISM credential, candidates must do the following: 1. Pass the CISM exam. 2. Agree to the ISACA Code of Professional Ethics. 3. Possess a minimum of five years of information security work experience, including at least three years of work experience in information security management in three or more of the job practice analysis areas. Experience must be verifiable and obtained in the preceding 10-year period prior to the application date or within five years after passing the exam. There are some exceptions to this requirement depending on current credentials held. 4. Submit an application for CISM certification (processing fee is $50). Credential must be obtained within five years of passing the exam. 5. Agree to the CISM Continuing Education Policy.
Number of Exams	One (only offered in June, September and December; candidates are encouraged to register early)
Cost of Exam	Online early registration: member $450, nonmember $63 Mailed/faxed early registration fee: member $525, nonmember $710 Online final registration deadline fee: member $500, nonmember $685 Mailed/faxed final registration deadline fee: member $575, nonmember $760

URL	http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx
Self-Study Materials	Training and study materials in various languages, information on Job Practice Areas, primary references, publications, articles, the *ISACA Journal*, review courses, exam prep community, terminology lists, a glossary and more are available at ISACA.org.

ISACA Certification Program

In addition to the CISM, ISACA offers numerous certifications for those interested in information security and best practices. Other credentials worth considering include the following:

- Certified Information Systems Auditor (CISA)
- Certified in the Governance of Enterprise IT (CGEIT)
- Certified in Risk and Information Systems Control (CRISC)

The CISA designation was created for professionals working with information systems auditing, control or security. The CGEIT credential targets IT professionals working in enterprise IT management, governance, strategic alignment, value delivery and risk, and resource and performance management. IT professionals seeking careers in all aspects of risk management will find the CRISC credential nicely meets their needs.

MORE: ISACA Certs & Career Paths

Certified Information Security Manager (CISM) Training

360training.com offers an online course covering the CISM exam that's just over 14 hours long. The course features video lessons, hands-on demonstrations and a student workbook, and it covers all of the CISM exam domains. Topics include information security governance, concepts and technologies, how to create and implement an information security strategy, and risk and incident management.

Beyond the Top 5: More InfoSec Certs

In addition to these must-have InfoSec credentials, there are many certifications available to fit the career needs of any IT professional interested in information security.

For those who find incident response and investigation intriguing, check out the Logical Operations CyberSec First Responder (CFR) certification. This ANSI-accredited credential recognizes security professionals who can design secure IT environments, perform threat analysis, and respond appropriately and effectively to cyberattacks. Logical Operations offers a few other certifications as well, including the Master Mobile Application Developer (MMAD) and the Certified Virtualization Professional (CVP).

Two new certifications to explore or keep your eye on are the Cisco CCNA Cyber Ops and the CompTIA Cybersecurity Analyst (CSA+). The associate-level Cisco CCNA Cyber Ops certification aims at people who work as analysts in security operations centers (SOCs) in large companies and organizations. Candidates who qualify through the Cisco Global Scholarship Program may receive free training, mentoring and testing to help them achieve the CCNA Cyber Ops certification. The CompTIA Cybersecurity Analyst (CSA+), scheduled to launch in February 2017, is a vendor-neutral certification designed for professionals with three to four years of security and behavioral analytics experience.