

Certifications: Where's the Beef?

By Philip Cox and Brad Johnson

Phil.cox@systemexperts.com

Brad.johnson@systemexperts.com

Introduction

This article is about certifications that are currently “hot” or the most desirable (from the authors’ point of view) in the computer industry. That being said, it needs to be stated up front that while “training” is applicable and useful to anyone and everyone (i.e., there is no one who knows it all), “certifications” need to be viewed with a bit different slant.

Certifications are, for the most part, used as an indicator of a level of knowledge. However, certifications do not indicate practical experience. Also, the lack of a certification does not automatically translate to a lack of knowledge. To put this in more concrete form, technical certifications held by junior- and intermediate-level staff CAN be a good indicator of their knowledge and ability, but certifications are usually NOT a leading indicator of knowledge and ability in senior staff. For senior staff, practical experience and accomplishments are much more important than any certification they hold.

The remainder of this article will focus on giving junior and intermediate staff some thoughts and information to “chew on” when it comes to the seeking of certifications.

Sorting It Out

At this point and time in the industry, consumers are confused and practitioners don’t know which certifications to pursue. Certifications work when there is a clear body of knowledge, standard of conduct, and recognized governance structure to define what the certification means and the process to obtain it. Currently, both consumers and practitioners are looking for certifications that have this, but the industry is just not there. For example, there is a well-known understanding of what certain higher-education certifications (degrees) mean. When you see Associate, Bachelor, Master, MD, or PhD, it is (to some level) quantifiable and useful as an indicator of an individual’s knowledge in a particular area. This is not the case currently with security-related certifications. Take it into consideration as you seek out the certifications that will be of most use to you.

What’s Out There?

As a point of reference, we did a quick search of security-related certifications and training and came up with over 100. An exhaustive search is sure to yield numbers in the thousands. Some of the certifications offer an “overall” scope, like the Certified Information

Systems Security Professional (CISSP) and Systems Security Certified Professional (SSCP) from (ISC)². Others are more specific, like the SANS Global Information Assurance Certification (GIAC) Certified UNIX Security Administrator. Still others are product-specific, like the SAINT certification for the SAINT vulnerability scanner.

Needless to say, there is a certification for just about anything you can think of, but the question you have to ask yourself is *are they really helpful?*

What is HOT!

Arguably one of the hottest sectors in training involves security testing. It seems that every week there is another company offering classes on how to compromise systems or applications.

Testing correctly is critical, so certifications in this area are helpful for those who have limited practical experience (i.e., junior- and intermediate-level staff) or limited time. Most hackers don't have certifications, but many of them have extensive knowledge gained through years of hacking. The problem is that most of us do not have the unlimited time to pursue that path. Certifications can offer a jump-start in this area.

Network and host vulnerability testing

This certification teaches you how to compromise networks and the hosts residing on them. It focuses on attacking at the operating system and general services layer. The classes leading up to the certification tend to focus on teaching the practitioner how to use a specific tool, or how to actually code an attack, or even both.

It is our belief that you should focus on learning the tools and understanding the exploits, and not the details of writing exploits, unless that is your job. Detailed exploit writing classes are of limited value unless you plan on pursuing that as a career. For example, spending time to understand the machine language needed to code buffer overflows for all the different operating systems and platforms will be of limited value if you are not going to write buffer overflows.

Application vulnerability testing

Application testing is a different beast altogether. You need to look for a class that teaches you how to think correctly, or more appropriately, "how to look for holes." Application testing, which is synonymous with Web-based applications, can be viewed as more of a mental exercise (i.e., thinking about where holes might be and trying them), than a purely technical one. For application testing, find a class that teaches you to think like an attacker.

As an aside, network and host vulnerability testing is being quickly taken over by automated tools, whereas application testing requires logic and observation, and the tools to do this are nowhere near complete or sufficiently sophisticated enough at this point in time.

So What Should You Do?

When you are thinking about getting a certification, you need to determine your primary purpose for the certification. To do this you should ask yourself two specific questions:

- ▲ What area of knowledge do I want my certification to show I am proficient in?
- ▲ Do I want my certification to show specific technical expertise or a broad range of knowledge?

After you have the answers to the above questions, you should determine a coherent plan of attack that will help you obtain your desired goal. This will assist you in plotting a well thought out professional growth and development path, as opposed to getting an incoherent jumble of unrelated certifications. To assist in developing this path, you could do the following:

- ▲ First, seek vendor-specific certifications to develop the requisite skills needed to be a true expert in the field you are pursuing. There are few things worse than a global "know it all" who has had little experience in actually applying technical knowledge.
- ▲ Second, pursue industry-recognized breadth-level certifications. This allows you to achieve a more overarching view of how you can utilize your specific expertise within the bigger picture. This will also help you successfully gravitate to the next level, in terms of being able to apply your knowledge. Instead of the old adage "when you have a hammer, every problem looks like a nail," you can go beyond your detailed expertise to finding the problem and then applying or finding the proper solution.

Where to Go?

After you determine the path you want to take, you should find providers. While it may seem obvious where to go for "vendor" training, you may have more options than you first think. You should research providers, and then go with the leaders, the providers who have a proven

track record. Probably the best place to determine where to go is by word of mouth. Seek out others who have the certification you desire, and ask for recommendations. Just as the reputation of your college is used as a shortcut (often unfairly) to assess intelligence and aptitude, certifications from second- or third-tier organizations carry little weight and are often not worth the expense or effort. So go with reputable training organizations.

Examples

Experience indicates that if you want to learn a specific technology, then a vendor-specific course is obviously the best place to start, such as Cisco certifications for Cisco products.

If you are primarily in the Microsoft universe, then obtaining an applicable Microsoft Certified System Engineer (MCSE) certification and utilizing the TechEd Conference and Professional Development Conference (PDC) of Microsoft is the best avenue to pursue.

If you desire to be a security "tester," then two classes tend to stand out: The Certified Ethical Hacker by the EC-Council, and the INFOSEC Assessment Methodology (IAM) by the National Security Agency (NSA).

If you want training and not necessarily a certification that will increase your feel for the industry and allow you to network with your peers, then look for a general conference such as ISSA SecureWorld Expo or Network+Interop.

Keeping the Certification Current

Don't forget that there is a huge hidden cost of certification programs. Most require well-documented officially sanctioned continuing professional education programs, payment of annual fees, as well as periodic recertification. Let's look at the Information Systems Assurance and Control Association's (ISACA) Certified Information Security Manager (CISM) certification requirements as an example:

- ▲ Attain and report an annual minimum of 20 CPE hours
- ▲ Submit annual CPE maintenance fees to ISACA in full
- ▲ Attain and report a minimum of 120 CPE hours for a three-year reporting period
- ▲ Submit required documentation of CPE activities if selected for the annual audit (you have to document as you go)
- ▲ Comply with ISACA's Code of Professional Ethics

In this example, CPEs are basically formal training and learning.

Plan to Use It

All this being said, it's important that the information security professional understand that none of these certifications by themselves are sufficient. You must have a plan to utilize the training after you have received it. If there is little or no use of the specific knowledge obtained, it will basically be forgotten within three months. It is strongly recommended that people new to the security field focus on basic principles, practices and procedures to establish a solid base to build upon.

Specific Certifications

Of the myriad of certifications that are out there, the following are some of the more useful, relevant, and ultimately the most profitable to obtain:

- ▲ Certified Information Security Manager (CISM) by ISACA
- ▲ Security+ by CompTIA
- ▲ GIAC Security Essentials Certification (GSEC) by SANS
- ▲ Systems Security Certified Professional (SSCP) by (ISC)²
- ▲ ICSA Computer Security Associate (TICSA) by TruSecure
- ▲ Security Certified Network Architect (SCNA) by Security Certified Program
- ▲ Microsoft Certified Systems Administrator: Security (MCSA: Security) by Microsoft
- ▲ Certified Information Systems Security Professional (CISSP) by (ISC)²
- ▲ Cisco Certified Security Professional CCSP by Cisco
- ▲ Check Point Certified Security Expert (CCSE) by CheckPoint
- ▲ Cisco Certified Internet Expert (CCIE) by Cisco
- ▲ INFOSEC Assessment Methodology (IAM) by NSA
- ▲ Certified Ethical Hacker (CEH) by EC-Council

What's Missing?

The Internet community needs to have security certifications that are meaningful. Right now, there are a hodgepodge of organizations that offer certifications in a wide variety of areas.

Most of these certifications are for entry-level skills or are product-specific. The industry certainly needs certifications that demonstrate that someone is competent for the same reason that we hire licensed plumbers or electricians.

What is missing is a uniform EXPERT-level certification akin to the MD for physicians. And just like in medicine, there should be specialist security certifications to designate significant knowledge beyond the baseline MD-equivalent (i.e., orthopedic specialist).

Resources

A few resource pointers to help you in your research are provided below:

- ▲ CramSession (www.cramsession.com): Covers all of the major certifications, so any in-depth search should start here
- ▲ *Certification* magazine (www.certmag.com): A good site for finding vendors who provide certification

It is interesting to note that in the area of law, the possession of certifications for senior/expert-level staff does indeed make a difference. While in all practicality, an individual with 20 years of practical experience in computer security would likely be more of an expert than someone with 5 years. If the person with 5 years has a certification, they MAY be viewed as having more knowledge. So, if you desire to use your knowledge in the legal realm, seeking certifications as a senior-level staff is probably worth your while.

Final Word


As someone looking to hire people holding certifications, remember that certifications are only one indicator of aptitude; you need to look beyond the certification. Certifications are helpful as a screening tool; the certifications most accurately characterize an applicant's general experience level (junior, intermediate, expert). However, the certifications don't address the most important intangibles, such as intelligence, judgment, and work ethic. Be sure to understand your genuine requirements for seeking candidates with particular certifications versus letting the certification play a leading role in defining an individual's value.

As a seeker of certifications, be clear about what you are trying to accomplish. What do you want the certifications to say about you? Recognize that certifications have become defensive and stick to the premium brands. Plan a coherent progression, and emphasize quality over quantity. Figure out where do you want (or need) to specialize:

- ▲ The operating system level
- ▲ Networking
- ▲ Middleware and infrastructure
- ▲ Application-level
- ▲ Other areas such as specialized security disciplines or product expertise (e.g. forensics, risk assessment, incident response, or data classification)

Because of ongoing costs, it is easy to quickly reach diminishing returns.

Spread the Word

In the security industry right now, there is no way to determine if you're working with a real expert or not. So the burden is on all of us to spread the word when we find them. If somebody has successfully executed a task for you as an "expert," you should recommend that person to your friends. For the time being, however, we have to deal with the fact that there is no uniform or accepted method of rating the various certification processes and titles, and no label to distinguish true experts. 

Phil Cox, MCSE, ISACA/CISM, is a Consultant at SystemExperts.

Brad Johnson, ISACA/CISM, NSA/IAM, is the Vice President of Consulting at SystemExperts.