Cybersecurity Certifications - are they valuable?

Taz Wake | Halkyn Consulting Ltd | Originally published 2025-03-27

A super common discussion in cybersecurity is about certifications and if they are "worth it." While this has been going on since the dawn of time (or at least 25 years, which is basically the same thing in IT), I wanted to take this chance to add some of my thoughts about it.

Disclaimer: I want to make a few things clear from the start. First, this is absolutely my opinion and not the opinions of any organisation or company. Second, I teach classes for SANS that include associated GIAC certificates. But to be clear, I do not "work" for SANS, and I teach for them *because* I believe it is the best training and the most valuable certificates, not the other way around. If I didn't believe this, I wouldn't teach for SANS. Lastly, I am not going to get involved in any discussions about is Cert X "better" than Cert Y. That is way too subjective.

Are certifications valuable for cybersecurity professionals?

This is a deceptively simple question, because the answer is "it depends." Like most things in life, the answer is complex, and we should avoid going with simple answers just because they are the easy option.

So we need to dig deeper.

What types of certifications are there?

Even the term can mean different things, so for the purposes of this discussion, I've tried to classify them into groups. This is pretty arbitrary, but my thinking is:

1. Training-based. By this type, I mean a certification you gain by sitting an exam or other form of test at the end of a training period. The idea is that you study something new, then sit an exam to prove/demonstrate what you have learned. Examples here include GIAC certs, EC-Council certs, possibly OSCP, etc.
2. Prior knowledge-based. By this, I mean exams that are generally "stand alone" and used to test if the person has acquired the required level of knowledge through a variety of means. This includes things like the CCSK and possibly things like CISSP (even though bootcamp classes exist).
3. Formal educational qualifications. Lots of people dont include this in the "certification" discussion, but I think it makes sense to include degrees, master's, etc., and other training from formal, traditional educational institutes. Often this requires 3+ years of study and involves producing at least a dissertation to show understanding of a subject.

4. Vendor qualifications. Most cybersecurity vendors have long since realised that offering a training course and certification in their product is a money spinner, and improves customer retention (or "lock-in"...), so I want to treat them differently from the others, as they have (IMHO) different impacts.

This is all so confusing...

What do certifications do?

Ultimately, all certifications are designed to show that the holder has met the criteria pre-defined by the body responsible for the certification.

Try not to read too much into this.

If someone holds the Expert Ninja Pentester certification from ImaginaryCorp, it simply means they've passed ImaginaryCorp's test. It doesn't mean they know everything. It doesn't even mean they know everything about ImaginaryCorp's body of knowledge. It just means they passed the test.

However, that is not attempting to belittle it. Passing tests requires knowledge. People who think a certification is easy or hard are simply talking about their own knowledge, not other people's. Often, people who say "that cert is too easy" are simply trying to show off their own knowledge. Any exam is easy if you know the answers and hard if you don't.

Experts do not need to know everything and almost certainly don't. Don't fall into the Dunning-Kruger problem of thinking this. Experts are often painfully aware of how much

there is to know on a topic and it is generally inexperienced people who think "you can know it all."

All exams have a passing "score" of some type. That means some people will scrape a pass and some will ace the test. Both have passed, and both hold the cert/qualification. Lots of certs dont record the score, so it is rarely something worth worrying about. Also, the score is often a reflection of other factors such as "easier to understand questions" or "not enough sleep last night", rather than a true reflection of knowledge.

Wait, that seems relevant.

You might have picked up on that last statement, because it is true that some people will fail an exam even if they have the correct level of knowledge, just because they are having a bad day. Others will pass just because the stars align. If we accept that circumstances other than knowledge can have a 10% variation on your score (and I think it is more, but...), then an exam with a pass mark of 70% will lead to some people who *should have got* 60% getting getting 70% and passing and some people who should have got 79% getting 69% and failing.

But this is the nature of any type of test. A world-class tennis player can have a bad day and get eliminated in an early round by a much worse player.

The number of truly undeserving who pass is actually pretty low, and the deserving who fail need to pick themselves up and just do it again. Perfection is not an achievable thing here.

(Plus "should have got 60%" is truly arbitrary and often just used to belittle people we dont like. If they really were bad, it is unlikely they could have been that much better than normal.)

Is this progress?

How are certifications used?

For me, this is the meat which allows us to decide if a certification is valuable. The answer is still it depends, but it gives us a framework to think about it.

While it is totally up to you how you use your certification, there are some common themes.

1. **To get a job**. Possibly the most common use is to secure, or at least help secure, a new job.
2. **To show we've learned new things**. Also very common. We study something new and then want to be able to show that we paid attention in class. Often, this is linked to "getting better pay" if not getting a brand new job as well. Just to be clear, I dont see getting a cert as simply "to learn new things," because you can do most classes without deciding to take any final exam.
3. **Personal pride**. Sometimes it's cool to just do stuff because it makes you feel good about yourself. Even if you never intend to shout it out to the world, you can be happy knowing that you passed $TEST. This isn't the most common motivation, but it absolutely exists.
4. **Social pressure**. This is probably more about Degrees and other forms of tertiary education, where people feel the need to do it because everyone assumes you do it. It is definitely less common for more focused cybersecurity courses, but it is growing. An example of this is how most Western societies assume everyone will leave high school and go to college or university before entering the workforce. This leads to a lot of confusion about "value" all by itself.

I think that the main reason people have heated debates about certifications is because we argue from our own ideas of how it should be used and assume that applies to the other person. If it doesn't, their idea of value will **always** be different to ours.

Just to reiterate one important point from above, though: Getting a certification is **NOT** about learning new things. The training for the certification does that. The exam is a **TEST** of knowledge, not a way to provide it.

Some common misconceptions and negative points

- A lack of certification does NOT mean a lack of knowledge. You can absolutely be an expert in a subject and have no formal qualifications. No one should doubt that.
- No certification is truly bad. Yes, we all have ones we look down on for a variety of reasons, but ultimately, every certification will have people who have studied, put effort in, and struggled to pass it. Just like a lack of certification doesn't equal a lack of knowledge, holding a cert you think is bad doesn't equal bad knowledge.
- Try not to get too hung up on the difference between practical skills, and theoretical skills in cybersecurity. This is not bricklaying. Yes, it helps if some cybersecurity practitioners know how to type the right commands, or click the right buttons in a tool, but we are, fundamentally, a knowledge-based industry. If someone KNOWS the right answer, that should be the benchmark. Most of the tools we use have help files,

search engines exist, finding the way to do something is almost trivial, but knowing what the right way is can be harder.

- Likewise, some certifications are memory tests, others are open book. Again, try not to get too hung up on the differences. I believe open book is better, although some people see it as "cheating." If the exam is designed to be open book, it isn't. That should mean the questions force the student to think deeper, rather than just regurgitate from memory. Ultimately, what is more important: someone who can memorise the switches for nmap or someone who understands the advantages and disadvantages of the different approaches, so can look up what they need in the man pages? However, this is just my view. The world can allow both solutions to exist, and maybe they should.

Finally, we are getting to the point!

Enough of this, do cybersecurity certifications have value?

Ok, we've established some ground rules, so I can try to give you my answer here.

But that is still simplistic. Really, it is up to you, but it's best to make a rational decision.

How can we decide if certifications have value then?

It really is down to a few questions.

Is the certification free? If the answer is yes, then it absolutely has value. I know your time costs, but look at it as a hobby. If it costs you an hour of your life, then it is probably worth it, because you'd spend the same amount of time sitting in traffic on the way to

work and not think anything of it. Or longer doomscrolling social media. At this point, it's just another thing you do to pass time, so the fact you get "something" out of it means there is some value. If the cost is free and the value is non-zero, then it is worth it...

If not, is it something you are just doing because you think it would be cool to do? If the answer here is yes, then it probably does have value, simply because you want it. You'd need to think if you want it enough to justify the price.

If not, why do you want it? Now we get the complexity. So let's dig deeper and talk about the motivations.

Do you need certifications for jobs in cybersecurity?

> *Strictly speaking, no. By this, I mean most, if not all, cybersecurity jobs require knowledge rather than a bit of paper, and we dont really have a "Cybersecurity profession" that controls who can and cant work in the industry.*

This might change (like medicine did), but today, even in regulated industries, the requirements are loose, with a lot of confusion about what is relevant for given roles anyway.

However, and this is the important bit, in practice it is **very** different.

For all the talk on social media about how $PERSON got $JOB with no qualifications (often claiming "*self-taught*" as well, which is a bit misleading, as it normally means "*I learned from others for free*"), this isn't as common as they make out.

If you are in a minority group or even just young, then certifications are often a deal breaker. Don't be tricked by the small number of people who, through fame or other advantages, have bypassed this requirement. Unless you are famous enough for hiring managers to have heard of you, you probably need certs. If you are famous, they are reaching out to ask you to work for them, not the other way round...

The guidance I had in school was along the lines of "if you match 70% apply," but that really does not apply to every group of people. You should still apply, but if they are looking for reasons to cut applicants, failing to match with certs has given them an easy excuse.

> *Certifications almost never get you the job, but they do open the door.*

When it comes to hiring candidates, remember some key points:

- Most recruiters do automated/keyword searches on job seeker profiles to decide if they fit a role. Having certs increases the chances you will match on the keyword and be selected.
- Most hiring managers are looking for easy ways to make their job simpler. If they have ten candidates but only want to interview four, certifications become a trivial way to eliminate people.
- Most organisations use HR (or an outsourced 3rd party) to hire candidates. That means the hiring manager has to go through a painful process of writing job

descriptions and explaining what would make a good candidate. The path of least resistance is to sprinkle in some certs because it keeps HR happy. This then goes from being a "nice to have" or "conversation piece" to being a hard rule at HR, and anyone without them gets rejected.

- Almost none (*I suspect it is none, but I am sure I'd be proven wrong*) hiring managers will reject a candidate **because** they have a certification. There are definitely cases where the certification might seem over the top (CISSP for L1 SOC analyst, for example), but I've never seen this lead to a rejection.
- Some regulators adopt a "*suitably qualified and experienced professional*" requirement, which mandates a "certification" for specific roles. Hilariously often, the choice of certification isn't specified, so any cert counts. No regulator says "they must not hold certifications."

Really, in this view, it seems crazy not to have a certification. At least for part of your career. Once you've been in the industry for 30 years, it definitely becomes less important, but doesn't always go away. I still have contracts with strange, yet non-negotiable, requirements such as "the lead consultant on the IR engagement must hold CISSP" but it does become less frequent.

Summary?

> *Having a certification gives you a better chance of getting a job than not having one.*

Please, please, keep in mind though, there are no guarantees. Any training or certification provider that sells you a bootcamp with a "guaranteed job" afterwards is probably scamming you. Training, knowledge and certifications can get you into the interview, but after that, it is still down to you. Hiring managers hire (or dont hire) for a huge range of reasons, sometimes they are even illegal reasons. Focus on the things you can control, not the things other people control.

Is that *really* everything?

Elephants in the room

There are some other things I should talk about here. They can be significant but also can be contentious, so please bear with me.

Job requirements are often nonsensical. I don't know why this happens so much; it could be laziness, or it could be misunderstandings, etc. I have no idea. Often, this manifests as jobs asking for very different certifications as if they were equal, for example, a role requiring "CISA or OSCP" when they have almost no overlap of content. This is annoying and is a strong indicator that the certifications are irrelevant for the role, but someone in the process wanted to include them.

The general advice here is to ignore the requirement and apply anyway. I agree with this, but it carries two risks. The first is that some hiring managers or HR teams will stick to the requirement and dismiss you (you lose nothing though, you just dont get an interview), or it could be a sign that the hiring manager is clueless and if you get the job, the job will suck.

Some recruiters are totally arbitrary. I am sure good ones exist, but most of the recruiters you encounter looking for work will misunderstand your profile, fixate on keywords and push you in random directions. I have "Magnet Axiom" on my CV, and almost every day, recruiters across the world reach out to see if I am interested in an Axiom Developer role. Same with the fact that I have experience investigating iOS

devices. I am not an iOS developer by any stretch of the imagination, but the keyword hit gets me almost daily emails.

It is hard to predict how recruiters and HR will react to a CV. The golden rule is that if you have the right words on your CV/Resume/Profile, you will get the recruiter's attention. Most won't read the profile until after they've mailed you about the role, you've replied and expressed an interest, and they need to get names in front of the client. Then they'll often ask you to write a new one anyway and tell you how they want it tailored.

Lots of advertised jobs dont exist. You cant do anything about this, so try not to worry about it. Companies and recruiters advertise jobs for lots of reasons, having a genuinely open vacancy isn't the only one. Also, funding for roles can be pulled, so you might apply and it vanishes. You have no control over this, so try not to worry about it. The Job Ad gives an idea of what people think a good role might look like, so it's worth trying to match as much as possible.

What about the price? For lots of reasons, I am not going to talk about this too much. It is true that the price of a certification directly impacts its value. A 10 (unit of currency irrelevant) unit certification can be valuable by delivering less than a 10,000 unit certification. But, as is often the case, it is more complex than that. Realistically, only you can decide if the value of the certification justifies the price.

When you consider this, however, keep in mind the real values. For example, if you are getting a certification which you hope will lead to a 150,000 job, then hesitating because it costs 10,000 would be strange. It would, arguably, be a better investment than (say) a 3-year degree costing 50,000 getting you a 75,000 job; however, social pressure makes us think that is normal today. There is no escaping the fact that upfront cost is a gamble, but so is not getting one. No one can make this decision for you.

Final note - should you train your staff?

This is the most emphatic yes I can ever muster.

If you have staff and you refuse to provide training, you don't value your staff. I can only assume you are planning, in the short to medium term even, to eliminate the staff and outsource the work (or sell the company and make everyone redundant).

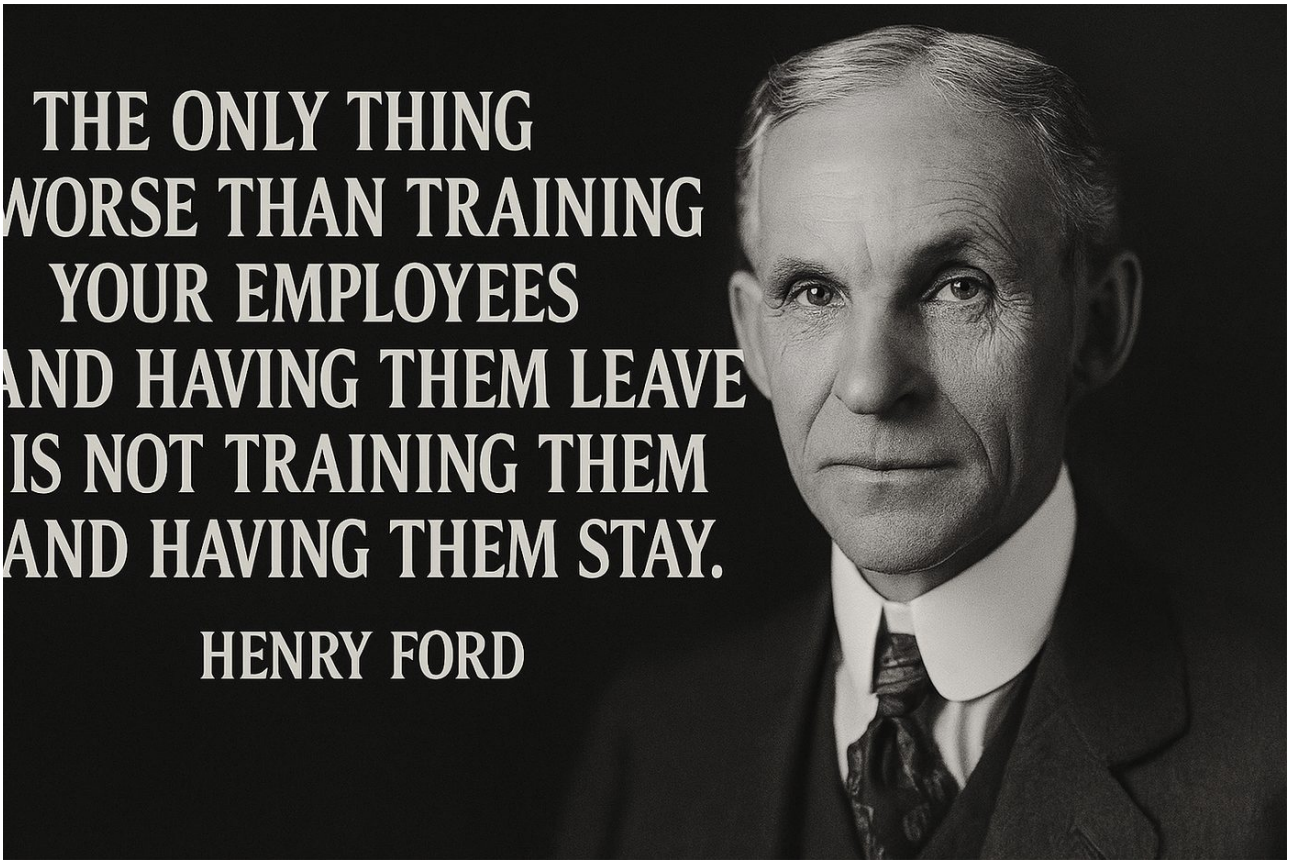
It is a big red flag.

If you are worried about your staff getting certifications and leaving, you are a bad employer, and your staff are going to leave anyway. You should look to be better, give better reasons to remain and, honestly, thinking you need to trap your staff is also a big red flag. If you promise your cybersecurity staff annual training, they'll almost never leave you.

If you will train your staff, but you have a limited training budget, that is not a red flag, unless your limits are punitive or badly thought out. Every organisation has budget issues, so think about where the money should be spent. If you spend 2 million units on security tools and 50 units on staff training (literally one organisation I did some work

with), then you really are wasting your 2 million units. If you invest in your staff, they are better staff, happier staff, harder working staff.

This has been known for centuries. Be a good manager, develop great staff and get great performance.



"The only thing worse than training your employees and having them leave is not training them and having them stay" - Henry Ford.

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858