BUILDING A CAREER IN CYBERSECURITY

THE STRATEGY AND SKILLS YOU NEED TO SUCCEED

YURI DIOGENES

Foreword by **MERAV BAHAT,** CEO and Co-Founder of Dazz

BUILDING A CAREER IN CYBERSECURITY

Certified in Cybersecurity (CC) by ISC2

This is a relatively new certification focused on cybersecurity fundamentals. The biggest advantage of this certification is the vendor—the International Information System Security Certification Consortium (ISC2). ISC2 is a reputable organization and very well respected across the entire cybersecurity industry.

The main ISC2 certification is CISSP, and that's the one many cybersecurity professionals know ISC2 for. However, ISC2 felt the market needed an entry-level cybersecurity certification, so they created the CC. This certification covers five domains:

- Security principals (26 percent of the exam)
- Network Security (24 percent of the exam)
- Access Controls Concepts (22 percent of the exam)
- Security Operations (18 percent of the exam)
- Business Continuity, Disaster Recovery, and Incident Response (10 percent of the exam)

Note

To learn more about this certification, visit *https://www.isc2.org/Certifications/CC*.

Cyber and IT Security Foundation by Exin

Exin was founded in 1984 and, over the years, has been recognized as one of the leading certification organizations, with more than 3 million certified professionals in different fields worldwide. The Cyber and IT Security Foundation certification is part of the Exin Foundation–level program. This certification covers the following topics (no percentage is assigned to each topic):

- TCP/IP networking
- Computer systems
- Applications and databases
- Cryptography
- Identity and access management
- Cloud computing
- Exploiting vulnerabilities

One of the things I really like about this certification is that it covers core TCP/IP networking concepts. In my opinion, this is a differentiator factor when it comes to foundational knowledge. I would even say this could be your first certification as you transition from a different field to cybersecurity. I've seen some students take this certification first, followed by the ISC2 CC. In other words, you can have two certifications to further solidify your foundational knowledge. As I always say, each person has a different need. Build your plan according to your needs.

Note

For more information about this certification, visit *https://www.exin.com/data-protection-security/exin-cyber-and-it-security/exin-cyber-and-it-security-foundation/*.

Security+ by CompTIA

The Computing Technology Industry Association (CompTIA) is a vendor-neutral, independent source of information on a wide range of technology topics.

CompTIA certifications are well recognized in the market, and Security+ certification is well-aligned with the National Initiative for Cybersecurity Education (NICE) framework. NICE is sponsored by the National Institute of Standards and Technology (NIST) in partnership with academia and the private sector. Security+ certification covers the following topics:

- Attacks, threats, and vulnerabilities (24 percent of the exam)
- Architecture and design (21 percent of the exam)
- Implementation (25 percent of the exam)
- Operations and incident response (16 percent of the exam)
- Governance, risk, and compliance (14 percent of the exam)

As I mentioned, Security+ was my first security certification, and I learned a lot from it. I also wrote an entire prep guidebook for the Security+ certification released in Portuguese (the first book about this certification ever to be released in Brazil) and trained hundreds of professionals over the years to help them pass the exam (during the 401 version of the exam). Because of this certification's impact on many careers, Security+ will always be one of the main certifications I recommend for beginners.

Note

For more information about this certification, see *https://www.comptia.org/certifications/security*.

Certified Security Specialist (ECSS) by EC-Council

EC-Council is a global information security education, training, and certification leader. The EC-Council's most well-known certification is the Certified Ethical Hacker (CEH), which is way more advanced. This certification covers the following topics:

- Information security and networking fundamentals (9 percent of the exam)
- Information security threats and attacks (21 percent of the exam)
- Information security controls (23 percent of the exam)
- Wireless network, VPN, and web application security (17 percent of the exam)
- Ethical hacking and pen testing (1 percent of the exam)
- Incident response and computer forensics fundamentals (6 percent of the exam)
- Digital evidence and file systems (4 percent of the exam)
- Windows and network forensics (10 percent of the exam)
- Logs and email crime forensics (6 percent of the exam)
- Investigation report (3 percent of the exam)

This is another example of a very granular body of content covering many aspects of cybersecurity, including areas not covered by any other exam, such as forensics and ethical hacking. The advantage of such broad exposure is that you may relate to some of these fields of expertise and pursue more specialized certifications.

Note

For more information about this certification, see https://www.eccouncil.org/programs/certified-security-specialist-ecss/.

TIP

All these certifications have network infrastructure and operating system components in some way covered in the exam, hence the criticality that you have these skills as mentioned in Chapter 1.

Cybersecurity Analyst and Security Practitioners Certifications

Many professional certifications are designed for the cybersecurity analyst role and security practitioners. However, regardless of which one you pursue next, remember that you can't skip the foundational certifications unless you already have all the knowledge covered by them.

The following list has some of the main Cybersecurity Analyst certifications in the market. Keep in mind the intention here is not to give you the ultimate list of certifications. Instead, I am providing a list of certifications that I believe, based on my experience, can make a difference in your career. For example, these certifications could add critical knowledge for a particular role and give you the advantage of having an industry certification tailored for it.

Cybersecurity Analyst (CySA+) by CompTIA

One of the biggest advantages of this certification is that the exam includes hands-on questions. As you study for this certification, you will gain both a theoretical understanding of the technologies and hands-on knowledge of how to do some of the tasks.

If you are new to Cybersecurity and just finished the foundational track, you can start with this certification to gain hands-on practice in different scenarios based on real-world situations. This certification covers the following topics:

- Threat and vulnerability management (22 percent of the exam)
- Software and systems security (18 percent of the exam)
- Security operations and monitoring (25 percent of the exam)
- Incident response (22 percent of the exam)
- Compliance and assessment (13 percent of the exam)

Note

I became CySA+ certified during the beta phase of this exam, and I truly enjoyed the experience. I also released a dedicated CySA+ Exam prep book (at that time, it was called CSA+) in Portuguese. To obtain more information about this certification, visit *https://www.comptia.org/certifications/cybersecurity-analyst*.

Systems Security Certified Practitioner (SSCP) by ISC2

This is another great certification from ISC2, and it meets U.S. Department of Defense (DoD) Directive 8570.1. This certification is also good for IT professionals migrating to cybersecurity after acquiring the foundational skills. This certification covers the following topics:

- Access controls (15 percent of the exam)
- Security operations and administrator (16 percent of the exam)
- Risk identification, monitoring, and analysis (15 percent of the exam)
- Incident response and recovery (14 percent of the exam)
- Cryptography (9 percent of the exam)
- Network and communication security (16 percent of the exam)
- Systems and application security (15 percent of the exam)

Note

Read more about U.S. Department of Defense (DoD) Directive 8570.1 at *https://www.isc2.org/Training/US-Government*.

TIP

As you can see, this certification has a more granular approach regarding the distribution of topics covered on the exam. To learn more about this certification, visit *https://www.isc2.org/Certifications/SSCP*.

Certified Cybersecurity Technician (CICT) by EC-Council

This certification focuses on hands-on skills and requires you to learn how to read logs to identify malicious activity, which you can only do if you have hands-on practice.

This type of certification is a great alternative for professionals working in a job that doesn't expose them to these technologies and scenarios. In other words, you will learn things you won't be able to learn in your current job because you don't work in cybersecurity yet. The page for this certification doesn't specify the percentage of the topics covered in the exam, but it provides the topics covered by the course.

Note

For more information, visit *https://www.eccouncil.org/programs/certified-cybersecurity-technician-certification*.

Specializations

You can easily go off the rails regarding cybersecurity certifications. Covering every certification in detail would require a dedicated chapter for each vendor, which is unnecessary since all the information is available on the vendor's website. Instead, this section lists the main specialized certifications from the primary industry vendors.

Table 2.2 maps the main certifications according to the professional field of specialization.

Table 2.2 Specializations

Field	Certification	Vendor
Professionals who work on the red team (pen testers and related jobs)	Pentest+	CompTIA
	GIAC Penetration Tester (GPEN)	GIAC
	CIPENT	EC-Council
	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	GIAC
	GIAC Certified Incident Handler (GCIH)	GIAC
	OSCP	Offensive Security
	EICIH	EC-Council
	EICEH	EC-Council
Professionals who work with cloud security	CICSE	EC-Council
	GIAC Cloud Security Essentials (GCLD)	GIAC
	GIAC Cloud Threat Detection (GCTD)	GIAC
	CCSP	ISC2