ISC2™

Behind the Scenes:

What Working in Cybersecurity is Really Like

Inside

A Career that Opens a World of Opportunities

Every industry needs skilled cybersecurity professionals to protect their networks, data and online transactions. It's not just government agencies, healthcare and financial institutions dealing with bad actors — even sectors that haven't traditionally focused resources on cybersecurity now find themselves under threat.

As a result, demand for cybersecurity talent is red-hot. Research shows the cybersecurity workforce needs an influx of 2.7 million professionals to meet global demand.[1]

This dynamic, rapidly evolving field offers the opportunity to model your career to match your interests. The National Initiative for Cybersecurity Careers and Studies identifies 52 distinct cybersecurity roles — the right one for you is out there.[2]

As you consider career paths, you'll discover cybersecurity is not a homogeneous field limited to a handful of roles. Instead, it covers a variety of functions and responsibilities, and is reliant on teams with diverse skills, experiences and ideas.

To help you explore your options, we asked cybersecurity experts at all stages of their careers about their experiences, background, day-to-day schedule and advice.

[1] 2021 Cybersecurity Workforce Study

[2] National Initiative for Cybersecurity Careers and Studies, Cyber Career Pathways Tool

Certified Cloud Professionals (CCSPs) in Action

Jonas Björk,
Security Presale Representative
at Telia Cygate

> *Cloud security is a sea of endless possibilities.*

What attracted you to cybersecurity?

At a security seminar I attended, the keynote speaker demonstrated a live hack. That's when I knew I wanted to work in cybersecurity. I was working in an IT admin role at the time. My first cybersecurity job was with a global company as part of its malware/threat hunting team. It was a fun time and a good start. I learned a lot and made great friends along the way.

What's the most satisfying part of your current role?

Part of it is the office environment. I worked from home for almost two years during the COVID lockdowns, and it took a toll on me. Then the opportunity to join Telia Cygate came up, and it's a good fit. It's extremely satisfying to be out, talking to customers and helping them, and working to make the world more secure. I like to help raise security awareness in a positive way. This field brings us constant challenges and constant changes — very seldom is it static.

What does a typical day look like for you?

It changes constantly. One day I'm sitting in meetings discussing NIST CSF, and the next day I'm recommending firewall options to a customer. Other days, I'm discussing the importance of IAM, MFA and vulnerability management. This job is as versatile as it gets and almost no day is the same. That's a big reason why I like working in cybersecurity.

What advice would you give to people considering a cloud security focus in their career?

There are endless possibilities in cloud security. It takes dedication, but it's incredibly rewarding. Within the field, there are new problems and new solutions emerging almost every day.
Be curious and follow through with it, and you will find the work totally satisfying.
Cloud security is a sea of endless possibilities.

Certified Cloud Professionals (CCSPs) in Action

Matt Lee,
Senior Director of Security and Compliance at Pax8

> *Go learn as much as you can about every part of cloud security. Go play, go test, go try, go read and go listen.*

What attracted you to cybersecurity?
When I was the director of technology and security at the managed service provider I founded, security kept creeping into everything we did. When you think about the enterprise security space, even with all its flaws, it's probably 15 years ahead of the server message block (SMB) market. Multi-factor authentication was just a normal part of life. It's been that way for a long time for most companies. However, for the SMB market, they have never heard the terms or fight it because it's inconvenient.

When you start to work with large numbers of customers, incidents start trickling up. You start asking yourself as a technology professional responsible for security, "What am I doing wrong? What's failing here?" At that point, you start realizing there's a large gap between what needs to exist and what currently exists, both from a service delivery perspective as well as from an actual tactical technical perspective.

What's one of the biggest challenges you've faced in your career?
The way I learned was through loss. That's probably common for most cybersecurity professionals. We learned because we were thrust into the perils of protecting an organization from cybercrime. Now, the challenge is the way organizations implement their cloud solutions, whether their environment is fully cloud-based or they're using a particular function as a service. Some of the biggest challenges for cloud today is the purer definition that's much more functional from how we deliver security. There are all kinds of technical concerns, but in the SMB world, it's a much higher level of security delivery than they could ever have achieved on their own.

What does a typical day look like for you?
My day is comprised of 20 or more different categories of things. Every day, I try to consume one to two hours of cyber news or research to keep up with what's going on in different environments. I do one to three external live webinars with partners each day, either speaking to their clients or directly to our partners from an educational perspective. There's a lot of travel to events. I also participate in external thought leadership like CSA's Zero Trust group.

What advice would you give to people considering a cloud security focus in their career?
Go learn as much as you can about every part of cloud security. Go play, go test, go try, go read and go listen. Find content you enjoy and resources that inspire you to love what you're doing. There are so many cool things in cloud security. Go find the vein in cloud security you want to be involved in and stay passionate about it.

Certified Cloud Professionals (CCSPs) in Action

Panagiotis Soulos,
Global Information Security
Manager at Intrum

> *There is no typical day in cybersecurity. There's always a new challenge to face — and that's the exciting part!*

What attracted you to cybersecurity?
I become interested in cybersecurity while I was finishing my bachelor's degree in 2004. I was motivated by another student who was about to earn a master's degree in network security at Royal Holloway, University of London. I was also looking to earn a master's degree, and cybersecurity sounded interesting. I wanted to be involved in protecting information and learn more about cyberattacks, as well as how to ethically bypass controls and gain access to systems.

What's the most satisfying part of your current role?
From the administrative side, the compliance part of cybersecurity and information security is extremely satisfying. The core of it is knowing how to audit or assess a control. You have to know what options are available and what you should do to ensure a threat or risk is mitigated correctly.

What does a typical day look like for you?
There is no typical day in cybersecurity. There's always a new challenge to face — and that's the exciting part! There's always something happening: a new critical vulnerability, a new product that mitigates threats, an attack happening in your infrastructure or an internal user acting negligently, resulting in a security incident that needs to be mitigated. My day usually involves discussions with my team members on how to assign tasks, set goals on deliverables and plan the team's schedule. Since mine is a second-line-of-defense role, I'm not directly involved with managing daily incidents or vulnerabilities but I do have to monitor them.

What advice would you give to people considering a cloud security focus in their career?
You should certainly cloud security it because it's the way to move forward. Cloud is the present and the future — it's here to stay. Everyone will use it. Cloud security skills are an asset for your career. You must be able to understand how the cloud works and the roles and deployment models. Most importantly, you must understand the shared responsibility model. Cybersecurity is everyone's responsibility, especially in the cloud. When using services from vendors, depending on the model, an amount of responsibility is with them.

Certified Information Systems Security Professionals (CISSPs) in Action

Jerome Leach,
Defensive Cyber Operations Lead
- Cyber National Mission Force
at U.S. Cyber Command

> *Being a cybersecurity professional goes deeper than just the job — you will be the beacon.*

Why did you first decide to get into cybersecurity?

After I completed my undergraduate degree, I wanted to attend a medical program. I had about a year of prerequisites to complete, and I knew once I finished those courses, I'd need to wait another year to start the program. Then I discovered the military would provide me with an additional skillset along with more options as I worked through my ambitions, so I enrolled. I was presented with a medical position in the Air Force, only to have my recruiter call back the next day and say that option was off the table. He went on to say he had a cybersecurity position available. I took it.

What was your first cybersecurity job?

I enlisted as a 3D0X3 (Cyber Surety). Our primary roles were computer security (policy, regulations, IG inspections), communication security (crypto issuance and management) and emission security/ TEMPEST (preventing emanations, data leakage from classified systems). At times, you may have found us focusing on combat crew communications or working as a local registration authority for classified public key infrastructure issuance.

What does a typical day look like for you?

I'm currently a Defensive Cyber Operations Lead at USCYBERCOM/Cyber National Mission Force. A typical day is comprised of briefings and working groups. Since it's a joint venture, we tend to collaborate with component military services, DoD agencies and foreign partner countries. I look at policy with regard to our DCO missions to understand how to leverage it, and clarify the intent of it as needed. My biggest focus is on our National Cyber Protection Teams, posturing them for deployment and hunt-forward operations. This typically takes months of planning and fostering meetings with host nations and key leadership in the command.

What do you think people considering a career in cybersecurity should know?

Cybersecurity takes time and repetition. The more you see something, the easier it becomes, and the more time you allocate, the more impressive you become. Being a cybersecurity professional goes deeper than just the job — you will be the beacon. My charge to you is to continually strive to be the best version of yourself. You will be expected to operate ethically; your actions will define all of us.

Certified Information Systems Security Professionals (CISSPs) in Action

Adesoji Ogunjobi,
Head of IT Audit at Wema Bank

> *A cybersecurity career is a journey. Continuing education is very important.*

Why did you first decide to get into cybersecurity?

I had achieved Microsoft, CompTIA and Cisco certifications, and it dawned on me that you really can't derive value from your IT infrastructure without thinking about security. So I went for the CISSP credential.

What was your first cybersecurity job?

My first cybersecurity role was IT security manager. I worked for a person who formerly consulted for a global IT company. He left that job and became the head of information technology in the company where I was employed. Since then, continual skill improvement is responsible for my progress in cybersecurity.

What does a typical day look like for you?

As the Head of IS Audit at Wema Bank in Nigeria, I handle cybersecurity audits in addition to core information system audits. I guide a team of IS auditors on how to spot control gaps. During a cybersecurity audit, I leverage the principles covered in the CISSP. Over the years, I've observed that most breaches result from the violation of fundamental cybersecurity principles covered in the CISSP Common Body of Knowledge. In addition, I review audit reports to ensure they're adequate and cover the areas that need assessment.

What do you think people considering a career in cybersecurity should know?

A cybersecurity career is a journey. Continuing education is very important. I continue to learn and contribute to the community by participating in training, volunteer opportunities, personal study, webinars and wherever I can gain more knowledge.

Certified Information Systems Security Professionals (CISSPs) in Action

Laurie Mack,
Director Security and Certifications at
Thales Digital Identity and Security

> *“The traditional fields of cybersecurity – network, physical, software, etc. – are really interesting and a great start for a career.”*

Why did you first decide to get into cybersecurity?

Early in my career as a military officer, I became an advocate for the security and protection of sensitive information. But more than that, I embraced the notion that security could be an enabler for organizations. Reliable security measures facilitated building the infrastructure and capabilities we use today, and I wanted to be part of that process.

What was your first cybersecurity job?

My first focus in cybersecurity was with the Canadian government’s Communications Security Establishment, working in an area that focused on supporting federal government departments to better understand their risk and to guide them in applying good security measures. It was exciting and challenging work, and it gave me the opportunity to address challenges, both nationally and internationally.

What does a typical day look like for you?

My day usually starts early since my team and I work in various time zones. As an example, for one of our many security certification projects, we’re working with a French lab, a UK product owner and engineering teams in United States and India. We hold a team “scrum” in the morning where each of us outlines the tasks for the day and to determine if help or priority adjustment is needed to the weekly plan. In addition to my management activities, I typically participate in at least three meetings with my team members each day. We cover a variety of topics, including security design or certification requirements or status; security vulnerabilities management; security standards development; site security, access control and business continuity; and contract manufacturing security to name a few.

What do you think people considering a career in cybersecurity should know?

The traditional fields of cybersecurity – network, physical, software, etc. – are really interesting and a great start for a career. I think the world is moving to a cloud environment. DevSecOps is also where an exciting future in the field lies. I wholeheartedly recommend obtaining the CISSP professional certification.

Certified Information Systems Security Professionals (CISSPs) in Action

Mari Aoba,
Security Analyst at Japan Security Operation Center

> *I was fascinated by the rarity that forensics isn't a job just anyone can do.*

Why did you first decide to get into cybersecurity?

During my job hunt, when I learned about the forensics business, it seemed interesting. I was fascinated by the rarity that it's not a job just anyone can do. I got into cybersecurity without really realizing there was such a field.

What was your first cybersecurity job?

My first cybersecurity job was investigating the unauthorized removal of sensitive information using computer forensics tools. I was responsible for the collection of evidence, investigation and report writing.

What does a typical day look like for you?

I start working from home around 9 a.m. I used to have to come to work, but I've been working remotely for the last three years so I don't have to commute. I spend my day working on projects related to planning and launching cybersecurity services, as well as planning and executing operational innovations. I finish work around 5:30 p.m. I am currently attending graduate school while working, so I spend my time after work taking classes.

What do you think people considering a career in cybersecurity should know?

It is necessary for those who are in this industry to keep gathering information daily. We have to improve our knowledge and skills so we can keep up with the remarkable progress of IT technology and cybersecurity.

Certified Information Systems Security Professionals (CISSPs) in Action

Javvad Malik,
Lead Security Awareness
Advocate at KnowBe4

> *Whatever background you have or whatever skillset you have, you can bring it to cybersecurity and make a positive difference.*

Why did you first decide to get into cybersecurity?
My university degree had a one-year work placement option. I applied for a number of roles and got a placement within the IT security team at a bank. I had no idea what IT security did or what to expect, but I found the work incredibly interesting. The bank seemed to like me, too, and it offered me a permanent job once I finished my degree.

What was your first cybersecurity job?
My first job was as a security administrator in the IT security team of a large global bank.

What does a typical day look like for you?
There are many moving parts, and as my role has developed and grown over the years, my day looks very different. The morning is the quietest period of the day for me as far as external distractions go. Being in the U.K., I have the jump on the U.S., so it's the time when I take a peek at the trending news stories. Then I tackle any deep research I need to do.

From 11 a.m. – 2 p.m., it's lunch and chat time. I try to schedule most of my meetings during this time. Particularly since the pandemic, there's been an uptick in video calls and meetings, and they do end up taking a chunk of time. While it's not always the most convenient, I do believe it's important to have regular and ongoing communication with peers, colleagues and team members.

From 2 p.m. – 5 p.m., it's The Wild West. It's pretty much a free-for-all at this point, responding to emails and looking into important issues. It's also the time I usually set aside to deliver webinars and record podcasts or do my admin tasks, such as submitting my expense reports.

What do you think people considering a career in cybersecurity should know?
Cybersecurity is a vast field that extends far beyond pen testing or coding. Whatever background you have or whatever skillset you have, you can bring it to cybersecurity and make a positive difference.

Christine Izuakor,
Founder and CEO at Cyber Pop-up

> *Get creative and do whatever you need to do to gain the experience.*

Why did you first decide to get into cybersecurity?

I absolutely fell in love with cybersecurity when I took a class on it. There was an encryption assignment and it just felt like a game. The assignment was to decipher an encrypted message. I had so much fun in that class, I decided to start studying security management. I followed that path all the way from my undergrad to my master's to my Ph.D.

What was your first cybersecurity job?

I made sure while I was in school that I was getting experience. I ended up working full time through my master's and Ph.D. I got a two-month internship with Continental Airlines in Houston, and they kept extending it until I was there for a year. At the end of my internship, there were different openings because the cybersecurity team was growing there. I recall at least three offers to choose from, which was a really nice position to be in, so I accepted one and never looked back.

What does a typical day look like for you?

I've transitioned from being a cybersecurity leader in very specific technical and management domains to being the CEO of a cybersecurity company. As a result, my day-to-day has shifted quite a bit. I deal with all ends of the business, from contributing to the design of cybersecurity projects to overseeing key financial, legal and strategic business decisions. My day often includes meeting with members of my team to understand challenges and help remove roadblocks, making key decisions based on data and connecting the entire company to new and exciting growth opportunities.

What do you think people considering a career in cybersecurity should know?

Experience is king. It's much better to realize that you need experience on the front end and start working toward it. Get creative and do whatever you need to do to gain the experience. In my case, I was working full-time but also did pro bono projects for nonprofits and small companies to get whatever experience I could.

The Essential Skills You Need

How can you know if cybersecurity is right for you? Cybersecurity professionals say roles at all levels require this core set of essential skills.

Leadership and communication. You should demonstrate credibility, responsiveness and ethics. Strong communication skills can help you earn trust from senior management and your peers.

Passion for learning. You'll be expected to continuously learn the latest cybersecurity trends, technologies and security challenges facing organizations. You must be passionate about learning and professional growth to be successful.

Determination. You must be persistent in the ever-changing threat landscape. You'll be expected to see a solution through to completion and never stop until the challenge is solved.

Collaboration. Cybersecurity is a shared responsibility across the organization. Professionals must be collaborative and work at all levels to instill a culture that ensures security policies are not only in place but followed. It is also critical to gain buy-in throughout the organization for security initiatives.

Analytical and critical thinking. You'll be expected to be analytical regarding how incidents occur, the attack surfaces prone to exploitation and how to minimize cyber-attacks. An analytical and insightful security professional anticipates how hackers will exploit the network and its applications.

How to Get Your Foot in the Door

What's the best way to break into cybersecurity? It depends where you are in your career, what you want to do and where you see your future. If you thrive on solving problems, are driven to help people and are stoked at the prospect of working in a constantly evolving field, you already have a lot in common with today's cybersecurity workforce.

You don't need an IT degree to work in cybersecurity. In fact, more than half of cybersecurity professionals got their start outside of IT, transitioning from unrelated careers, getting their start with cybersecurity education and exploring cybersecurity concepts on their own.

Here are some fundamentals to consider, whether you're a student or a professional.

Advice for Students

Know the technical basics. Not everyone in cybersecurity comes from a deep technical background, but it's important to know the basics. Some industry experts advise starting on a more general technical path and then focusing on security later, once the basics are mastered. Whatever path you choose, you will need a general understanding of systems, coding, networking, and how applications are run and maintained.

Get certified. Certifications can help you get your foot in the door. Working professionals say they're the most important way for career pursuers to enter the field.[5]

Consider training in general IT. Finding an internship, apprenticeship or entry-level job in IT is a great launch pad. Consider data entry, help desk or any other ground-level technical position to learn IT fundamentals. You'll get a hands-on sense of technical processes and real-world business scenarios that will serve you well in cybersecurity.

Focus your area of interest. What does your ideal cybersecurity career look like? Your path in the short term will springboard your future. Roles that pave the way include systems administrator, web administrator, web developer, network administrator, IT technician, network engineer and software engineer.

Learn independently. There are many ways to learn the technical skills used in cybersecurity, including books, self-directed learning (teaching yourself how to code, for example), online courses and guided training. Whichever you choose, these fundamentals will be essential as you get deeper into security work.

[5] 2021 Cybersecurity Career Pursuers Study

Advice for Career-Changers

For incoming professionals just starting in cybersecurity, persistence is key. Don't give up if your first few attempts to get in front of a hiring manager fall flat. Keep in mind, many recruiters are focused on processing applications and candidates across an entire organization. Your goal is to reach the hiring manager. Here are some ways to connect with people in the field to get there.[6]

- **Online Communities** - There are many active forums on social media, including Reddit, LinkedIn and more, where you can connect, research your questions and learn from other cybersecurity professionals' experiences and opinions.
- **Cybersecurity Chapters** - Local chapters around the world focus on creating in-person and online networking opportunities for cybersecurity professionals. Many first-timers find professionals who are willing and eager to share their experiences and advice.
- **Industry Events** - Cybersecurity conferences provide networking opportunities to get in front of the right people, including recruiters, hiring managers and cybersecurity team members who can help open doors into their organizations.

Incoming professionals should also absorb as much information as possible about the roles and responsibilities associated with the job titles that intrigue them most. That way, once you get in front of a recruiter or hiring manager, you're ready to:

- Ask questions and share opinions that demonstrate knowledge of the profession, as well as the current threat landscape.
- Emphasize an understanding of the skills required to mitigate risk, such as problem solving, communication and critical thinking.
- Show a willingness to learn as much as possible about cybersecurity through training, mentoring, on-the-job learning, webinars and self-guided online courses.

[6] How to Get a Cybersecurity Job

How Certification Factors In

Cybersecurity professionals say the most important way to enter the field successfully is through certification.[6] They point to certification as an achievement and a proof point to their employers, peers and themselves that validates their skills.

Certified in Cybersecurity from ISC2 — the new entry-level certification from world's leading cybersecurity professional organization known for the CISSP® — gives you the knowledge and skills you need to begin your first role ready for what's next.

No Experience Required

No work experience in cybersecurity or formal educational diploma/degree is required to take the exam. If you're a problem-solver with an analytical mindset, Certified in Cybersecurity (CC) is right for you.

When you successfully complete the exam, you'll gain immediate access to valuable ISC2 membership benefits, including thought leadership, exclusive networking and more.

More Benefits of Certification

- **Respect** - Validate your knowledge and build credibility.
- **Job offer and advancement** - Gain the solid foundation of cybersecurity knowledge employers are looking for, from an association they trust.
- **Growth and learning** - Develop new skills you can apply in day-to-day work.
- Pathway to cybersecurity careers and advanced certifications - Build a strong foundation for an infosec career and become familiar with exam formats for advanced ISC2 certifications like CISSP.
- **Community of professionals** - Access a network of peers and CPE/learning opportunities.
- **Higher salaries** - ISC2 members report 35% higher salaries than non-members.

[6] 2021 Cybersecurity Career Pursuers Study

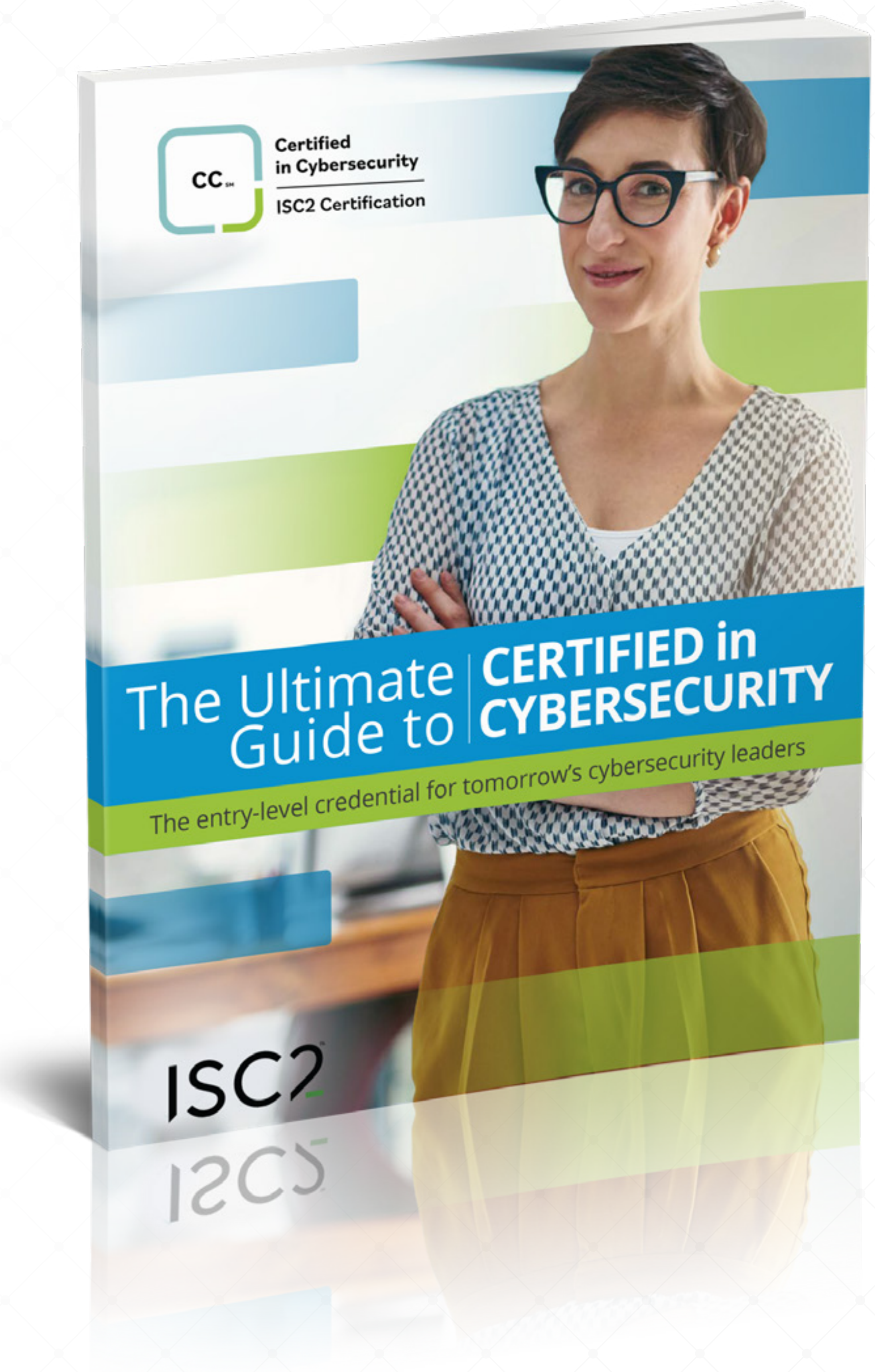
Next Step: The Ultimate Guide to Certified in Cybersecurity

Take the next step toward a career in cybersecurity with The Ultimate Guide to Certified in Cybersecurity: The Entry-Level Credential for Tomorrow's Cybersecurity Leaders. It covers everything you need to know about the credential. Find out how Certified in Cybersecurity and ISC2 can help you discover your certification path, create your plan and acquire the knowledge and skills for a successful career in cybersecurity.

Inside: Your Questions Answered!

- What's Covered in the Exam?
- What are the Exam Prep Options?
- What are the Benefits of Certification?
- Plus, Real-World Testimonials

Get Your Guide


CC
Certified in Cybersecurity
ISC2 Certification
The Ultimate Guide to CERTIFIED in CYBERSECURITY
The entry-level credential for tomorrow's cybersecurity leaders
ISC2

From the World's Leading Cybersecurity Professional Organization

ISC2 cybersecurity certifications, including CISSP and CCSP, are recognized globally as the gold standards for excellence.

Elite Cybersecurity Professionals

ISC2 members represent an elite global network of information security professionals. They are top experts in their fields, dedicated to the highest ethical standards and best practices. Our members work for governments and highly respected companies around the world. Through ISC2 certifications, they show superior competency.

Members Around the World

ISC2 is the world's leading cybersecurity professional organization, 500,000+ associates, candidates and members strong. Our members work in high-level cybersecurity, information, software and infrastructure positions all around world.

Far-Reaching Impact

The professionals who make up the ISC2 community play a vital role. They not only protect the organizations they serve, they help keep society safe and secure. And they're in high demand, as organizations place more importance on information security.

Learn more at isc2.org or follow us on X or connect
with us on Facebook, LinkedIn and YouTube.