SANS | GIAC CERTIFICATIONS

NEW TO CYBER FIELD MANUAL

The Ultimate Guide to Getting Into Cybersecurity
sansurl.com/newtocyber

One of the most asked questions we get is

“How Do I Get Started in Cybersecurity?”

Unfortunately, there isn’t a simple answer that works for everyone. This guide was created to help YOU figure out the best path to get into cybersecurity. Use it to help develop your skills and find a network of people to support you getting into the industry.

What to expect from this guide

This guide contains seven sections, each focusing on different ways to develop skills. If you focus efforts on each one of these, you will gain exposure to the industry and be able to define your specific pathway.

1. Take advantage of free content
2. Build your skills
3. Surround yourself with industry experts and mentors
4. Attend free and low-cost events
5. Engage with the community
6. Look for scholarship and community programs
7. Get training and certification

Twenty coolest careers in cybersecurity

Frequently asked questions

Why cybersecurity?

Now, more than ever, cybersecurity and InfoSec careers are in high demand. The industry is broad and needs a variety of skills. In addition, cybercrime never stops and technology changes rapidly, so this industry is never boring. Practically every industry out there needs cybersecurity professionals. Not only will you have plenty of work, you’ll also enjoy a sense of accomplishment, knowing you are part of a greater good.

1. Take advantage of free content

Take the time to watch webcasts and YouTube videos, read blogs, and start Googling when something piques your interest. Here are some we recommend you start with:

Webcasts

- The Foundation of Accelerating your Cybersecurity Career – James Lyne
- The 14 Absolute Truths of Security – Keith Palmgren
- Your 5-year path – John Strand, Black Hills InfoSec
- CAREERS IN CYBERSECURITY – Advice from Defcon 24

Blogs and Newsletters

- sans.org/blog – In particular, Top 5 Steps to Start in Cybersecurity
- Reading Room – The SANS Reading Room features over 3,010 original computer security white papers
- This Week in 4n6 – A weekly blog on all things Digital Forensics and Incident Response (DFIR)
- Newsbites – SANS NewsBites is a semiweekly high-level summary of the most important news articles on computer security during the last week
- Brian Krebs – His website will expose you to a whole new world
- HECFBlog – David Cowen dives deep into Digital Forensics

YouTube Channels

- SANS Institute
- Blue Team Operations
- Cloud Security
- Digital Forensics & Incident Response
- Industrial Control Systems
- Offensive Operations
- IT Career Questions

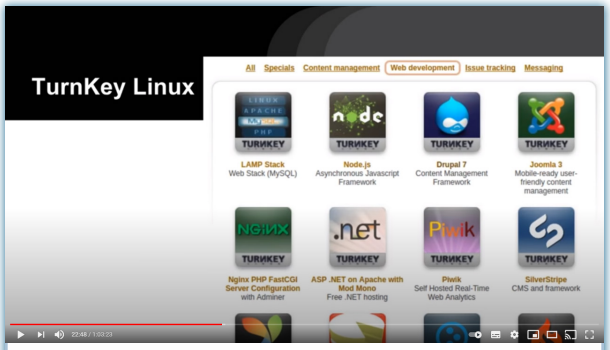
Podcasts

- Blueprint – Building the best in cyber defense
- Trust Me. I'm Certified – A podcast exploring how to conquer imposter syndrome, brought to you by GIAC Certifications
- Daily Stormcast from Internet Storm Center – Stormcasts are daily 5–10-minute information security threat updates
- Security Weekly – Connecting the security industry with the security community

Also check out sans.org/free. SANS instructors produce thousands of free content-rich resources for the information security community every year.

2. Build your skills

It's important to learn the core concepts and seek out hands-on opportunities to apply them. Familiarize yourself with Windows, Linux, Coding Languages, and Networking. How?



Build a Home Lab
Jeff McJunkin walks you through it in this webcast.

Holiday Hack Challenge – You can go through the past five years of challenges, just be careful of spoilers online.

Aman Hardikar's Mind Map – Check this out to practice InfoSec skills online.

CyberStart – Geared toward finding the next leaders in cybersecurity.

Learn Coding, Linux and Networking Basics – So many free resources, just start searching.

Participate in Cyber Ranges – NetWars runs free events throughout the year, HacktheBox is a large playground and Security Innovations has built a practice hacking range (3 days access free).

Download Free Tools – Play around with open-source tools like SIFT Workstation. The SANS faculty has created over 150 free tools. Find them **here**.

3. Surround Yourself With Industry Experts And Mentors

Following industry experts and mentors can open a world of tools, topics, and events that you would not otherwise be aware of.

SANS Instructors are very active on Twitter and worth following.
Here's a full list of SANS Instructors' Twitter handles.

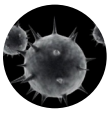
In addition to the full list, here are some of our most active:

James Lyne
@jameslyne

Johannes Ullrich
@johullrich

Heather Mahalik
@HeatherMahalik

John Hubbard
@SecHubb



Stephen Sims
@Steph3nSims

Frank Kim
@fykim

Lance Spitzner
@lspitzner

Lenny Zeltser
@lennyzeltser

And don't forget

SANS Institute's Twitter accounts:

twitter.com/SANSInstitute/lists

SANS | SANSCloud
SANSDefense | SANSDFIR
SANSICS | SANSLeadership
SANSOffensiveOps
SANSEMEA | SANSAPAC

Mentorships

There are a ton of mentorship opportunities available (found with a quick search). Here are a few of our favorites:

- Cybersecurity Mentoring Hub
- WiCyS (Women in Cybersecurity) Mentorship
- ICMCP (International Consortium of Minority Cybersecurity Professionals)

4. Attend free and low-cost events

There are so many great IT Security conferences, and many of them post their content online afterward.

SANS Summits – All are free in 2021

SANS Summits connect you with cybersecurity practitioners and experts who deliver applicable content based on real-world experience. Through in-depth presentations, panel discussions, interactive workshops, and sharing forums, you'll collaborate with fellow cybersecurity practitioners, learn about tools and generate solutions that will help you protect your organization from ever-evolving threats.

"I've managed to learn something I didn't know from nearly every session, and I've been made aware of additional tools or methodologies that will help." – Dallas Moore, PepsiCo

BSides – Countless dates and locations

BSides is a community-driven framework for building events for and by information security community members. The goal is to expand the spectrum of conversation beyond the traditional confines of space and time. BSides creates opportunities for individuals to both present and participate in an intimate atmosphere that encourages collaboration. These are intense events with discussions, demos, and interaction among participants. It is where conversations for the 'next big thing' are happening.

"BSides is a growing community of real security professionals who want to learn from each other and grow. Unlike most cons we see today, BSides cuts through the hype and allows you to have real conversations among your peers in an environment that's comfortable and welcoming."
– Michelle Schafer

RSA Conference – Much of their content is available free online

RSA Conferences are the best place to strengthen your resilience. From the first to the last day, you'll gain actionable insights from hundreds of traditional and immersive sessions, collaborate and share different perspectives with peers that will spark new approaches, and

5. Engage with the community

Get involved with groups, meetups, lists, forums, and LinkedIn communities:

SANS DFIR LinkedIn Community

Keep up with the latest of Digital Forensics & Incident Response topics, look for jobs and training, and more.

SANS Industrial Control Systems Community Forum

Participate in the SANS Industrial Control Systems (ICS) Community Forum, where ICS professionals discuss current security events, share tips, ask questions, and connect with others passionate about securing the critical infrastructure.

AFCEA Chapters

AFCEA provides a forum for military, government, and industry communities to collaborate so that technology and strategy align with the needs of those who serve.

ISACA Local Chapters

ISACA offers access to resources and a community of experts committed to lifetime learning and career progression to help you stay up to date.

ISSA Chapter Directory

ISSA is the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk, and protecting critical information and infrastructure.

OWASP Chapters Program

The OWASP Foundation works to improve the security of software through its community-led, open-source software projects, hundreds of chapters worldwide, tens of thousands of members, and the hosting of local and global conferences.

SANS OSINT Community

This is a place for people who are OSINTers, looking to become an OSINTer, and who are members of the global OSINT community!

Advancing Women in CyberSecurity

WiCyS is where the recruitment, retention and advancement of women in cybersecurity happens.

Search Discord Servers

Here's a list of discord servers tagged with cybersecurity **https://disboard.org/servers/tag/cyber-security**

SANS Blue Team Ops

https://discord.gg/hD2A2Egy

6. SANS Cyber Academies

https://www.sans.org/about/academies/

To help fill the cybersecurity skills gap, the SANS Institute created the CyberTalent Immersion Academy, an intensive, accelerated training program that provides world class training and GIAC certifications to quickly and effectively launch careers in cybersecurity.

More than 600 scholarships have been awarded so far and 90% of our graduates are employed within six months of graduation. Find out if you could be one of the next to participate and launch a new career in cyber!

Department of Defense STEM

DoD STEM offers opportunities for potential students, educators, and the current workforce.

Scholarships.com and Unigo

A list of cybersecurity college scholarships.

https://www.scholarships.com/financial-aid/college-scholarships/scholarship-directory/academic-major/cybersecurity

https://www.unigo.com/scholarships/by-major/cybersecurity-scholarships

7. Get Training and Certification

SANS offers an accredited college certificate – the **Undergraduate Certificate in Applied Cybersecurity** from the SANS Technology Institute – that guides you through a sequence of four courses. The program includes an introductory course plus three SANS courses leading to GIAC certifications that provide the foundational knowledge and hands-on skills needed to launch a cybersecurity career. The program also serves as a pathway to the SANS.edu master's degree program and job-specific graduate certificate programs. A 100% online option is available. Applications are accepted monthly.

"I was having a hard time getting a job in information security due to my lack of hands-on experience. SANS gave me extraordinary training and the opportunity to rise to the top of the résumé pile."
– AJ Langlois, BB&T

SANS Security Essentials courses are designed to provide a range of topics to help you grasp foundations quickly and fill critical knowledge gaps. The certifications associated with the courses provide assurance to employers that their prospective hires can actually do the job. Below is a list of SANS foundational courses and certifications, with supporting resources that can help you get started, and that might give you an idea of the path that interests you the most:

SANS Foundations

SANS Foundations is the best single course available to learn the core knowledge and develop practical skills in computers, technology, and security fundamentals that are needed to kickstart a career in cybersecurity. The course features a comprehensive variety of innovative, hands-on labs and practical exercises that go far beyond what is offered in any other foundational course in cybersecurity. These labs are developed by leading subject-matter experts, drawing on the latest technology, techniques, and concepts in cybersecurity.

The course provides students with the practical learning and key skills to empower future cybersecurity learning and professional development.

"I think the biggest value add for SANS Foundations was simply how comprehensive it was. It covered a lot of topics, but each was covered in enough depth for a better handle on the basics without being overwhelming." – U.S. government federal law enforcement professional

SEC301: Introduction to Cyber Security teaches you real-world cybersecurity fundamentals to serve as the foundation for your career skills and knowledge for years to come.

Course Demo | GIAC Information Security Fundamentals (GISF)

"Coming from a non-cybersecurity background, this course was perfect for setting my cyber foundation." – Marco Godinez, Discover Financial

"The best parts of this class are the real-world examples and historical events, which illustrate how these course topics are applicable and why they are important to learn/understand." – Gia M.

SEC401: Security Essentials Bootcamp Style teaches you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems.

Course Demo | GIAC Security Essentials (GSEC)

"SEC401 took what I thought I knew and truly explained everything to me. Now, I also UNDERSTAND the security essentials fundamentals and how/why we apply them. Loved the training, cannot wait to come back for more." – Nicholas Blanton, ManTech International

"SEC401 provides an excellent overview of security fundamentals delivered by experienced industry professionals." – Jathan Watso, Department of Finance

Brand New Course!

FOR308: Digital Forensics Essentials will teach you the fundamentals of Digital Forensics & Incident Response, including what digital data is, how to find it, acquire it, preserve it, and most importantly, how to understand it and explain findings.

Course Demo

"FOR308 was valuable as it filled in many gaps in my experience and it set a good foundation of the basics to which I can build upon, I enjoyed the acquisition, and validation section."
– Carla Dawn, FOR308 student

"FOR308 is packed with technical information and covers aspects necessary for those taking their first steps in the digital forensics as well as those who think about leading teams in the field. An overall good balance of theory to practice, delivered in a very professional manner."
– Wiktor Kardacki, 6point5

20 Coolest Careers in Cybersecurity

Here's the list of Top 20 Coolest Careers in cybersecurity. Challenge your skills, take the next step in your career, and become an invaluable asset to employers.

1. **Threat Hunter**
2. **Red Teamer**
3. **Digital Forensic Analyst**
4. **Purple Teamer**
5. **Malware Analyst**
6. **Chief Information Security Officer (CISO)**
7. **Blue Teamer – All-Around Defender**
8. **Security Architect & Engineer**
9. **Incident Response Team Member**
10. **Cyber Security Analyst/Engineer**
11. **OSINT Investigator/Analyst**
12. **Technical Director**
13. **Cloud Analyst**
14. **Intrusion Detection / (SOC) Analyst**
15. **Security Awareness Officer**
16. **Vulnerability Researcher & Exploit Developer**
17. **Application Pen Tester**
18. **ICS/OT Security Assessment Consultant**
19. **DevSecOps Engineer**
20. **Media Exploitation Analyst**

Frequently Asked Questions

We asked numerous SANS Instructors how they would respond to the FAQs and organized the responses below.

Q. What are the best ways to get started in Cybersecurity?

A. Start by playing around to figure out what specialty interests you the most. There's a lot to choose from: forensics, defense, penetration testing, cloud, security awareness, policy, auditing, malware reverse engineering, blue team, defense, forensics, and compliance, just to name a few. By reading up, listening to webinars, and asking people in the field about their specialty, you can start to build a foundation and learn the basic IT and critical thinking skills you'll need to pursue whichever specialty you choose.

Make sure you have a basic understanding of the main Internet protocols like TCP, UDP, HTTP, and FTP, and seek out information on certain vulnerabilities and how they work. How do you do this? Try to join communities like OWASP, SANS, and other security communities, or take some free courses on sites like cybrary.it, udemy, or coursera. Play around with some tools on your computer or a virtual machine to get to know certain parts of the systems, and maybe try out a Capture-the-Flag event playing on a team or on your own. In other words, just practice and see what you like in the cybersecurity realm. Above all, love technology and understanding how technology works.

Q. How can I get into cybersecurity with no experience?

A. College degrees and certifications can provide a good baseline, but individual exploration can be equally valuable. Employers will appreciate seeing applicants who have made Github contributions, written blog posts, or given talks at local meetups. Even if you've just talked about basic information that exists elsewhere on the Internet, it shows a genuine interest in the field. For those who qualify, service in the military can be a fantastic option, even part-time in the National Guard or Reserves. You'll certainly get some experience and training there (often including SANS courses). For those with professional experience outside of cybersecurity, join a cybersecurity company doing what you do best, whether it's marketing, project management, graphic design, customer service, or any other specialty. Then, make a plan with your manager and technical teams about how to transition into cyber. If you have no experience, be able to show a potential employer that you are serious about cybersecurity, even if it's just things you read and that show your interest in the field. Take part in Capture-the-Flag events, online courses, and practical hands-on labs, many of which are freely available.

Q. Do you need to learn programming to get into Cybersecurity? If so, what's the best language?

A. You don't need to know how to program to get into the field, but you should at least be familiar with the concepts. Some areas in cybersecurity may need more programming skills and understanding than others. Certain knowledge on scripting languages like Bash or Python is helpful to quickly go through some data and automate small tasks, but it's not a requirement to start with. A good place to start is by getting familiar with a language such as Python, and just move from there. A site that gives interactive tutorials on programming is codecademy.com, and if you have some money to learn secure programming you can try securecodewarrior.com. Another recommended site to learn coding is checkio.org.

Beyond that, it depends on which direction you want to go. For example, if you go into pentesting web applications, it would be good to at least understand ASP.net, PHP, and .NET web development frameworks with C#.

Q. What are the best websites to learn how to hack?

A. Try online cybersecurity training platforms such as Hack the Box, The Cyber Mentor, or Try Hack Me. Some other recommended sites are overthewire.org/wargames, hacking-lab.com/index.html, ctf.hacker101.com, and hackthissite.org.

And don't forget SANS Institute's own annual Holiday Hack Challenge: here's a link to the 2020 version: holidayhackchallenge.com/2020. It's OK to use winning answers as walkthroughs!

Q. How do I get an introductory job in cybersecurity?

A. Many people start as a junior analyst in a Cyber Security Operations Center (CSOC) examining alerts and trying to analyze them. You learn a lot doing this and from there you can go in other directions. One SANS instructor started as a security engineer looking at how to implement security applications within a particular environment, which involved a lot of troubleshooting on the network that helped the instructor get a better understanding of network security and protocols.

You can also look for internships. Here's a sampling of helpful sites: seap.asee.org, nreip.asee.org, vsfs.state.gov, and blog.collegevine.com/14-awesome-internships-for-high-school-students. For those in college, make sure to use the career services office and other resources available to you on your campus.

Q. When just getting started, which is better, a degree or certification?

A. There are some fields in cybersecurity for which a degree is certainly an advantage, but then there are others for which certifications are best suited because they demonstrate competency in a specific area. So if you want to start broad and don't know yet what your focus will be, a degree is best to get a good job down the line. But if you are really focused on a specific field, like web application pentesting or SIEMs, then a certification can be a great start for that specific job.

Q. What should I do if I don't know which path I want to take?

A. What is exciting for you? What gives you the drive and determination to dig in and want to learn more? Figure that out, then figure out a path that also achieves your career goals that align and you'll be well on your way to success. If you're not sure yet, try a little bit of everything. It's not necessarily best for everyone to try to specialize too early. Having a good general background is a big advantage and allows you to actually get a sense of what you enjoy.

Q. What advice do you like to give to those just starting out?

A. There are a lot of answers to that question, but they can all help you. For starters, read, practice, and don't be afraid to make mistakes. Set up your own lab, log things from those servers, then try to execute attacks you learned on the Internet or from books and see what happens. In other words, just play around a bit and find out what you like and are good at. Networking also matters, in fact it's golden in the cybersecurity field. Join and volunteer at local meetups (ISACA, Security BSides, (ISC)2, Defcon, OWASP, WiCyS). Many post their meetings on meetup.com or their parent websites. Go to conferences and try to meet as many people as possible.

Final Advice from Lance Spitzner

"If you've always been curious about getting started in cybersecurity, don't let your education or background determine your career path or limit your options. No matter what your background is, you bring something unique and special to this field, which we desperately need. As long as you have passion, and desire to learn, you're on the right track. Never lose that desire to learn. Once you start to develop your skills and you begin to develop a network of people, trust me, the opportunities will come".

Read full blog on **Getting Started in Cybersecurity with a Non-Technical Background**

sansurl.com/newtocyber