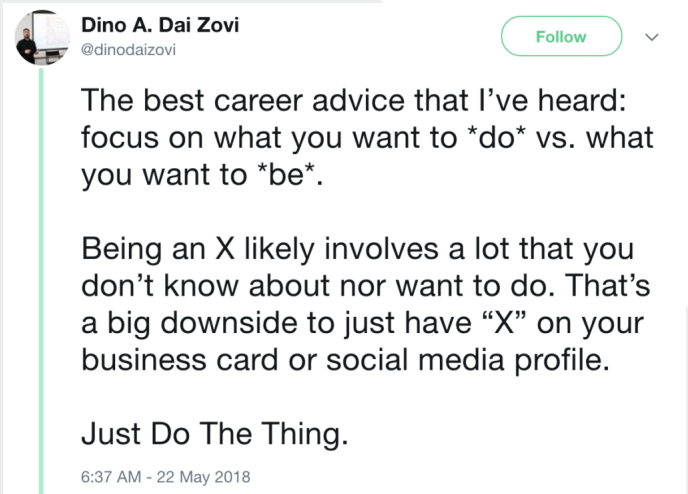
TLNT | 9 min read | May 31, 2018 | by Yanek Korff, Ben Brigida and Jon Hencinski

A beginner's guide to getting started in cybersecurity

It happens from time to time. Someone tweets something incendiary, it creates a hubbub and before long you've got yourself a veritable online brouhaha. One topic that seems to have piqued everyone's interest lately is this question: is there such a thing as an entry-level security job? It's a good one. And there seem to be two schools of thought:

1. Never start off in security. Start with IT infrastructure, helpdesk, or development.
2. Don't waste time, dive into security and fill in the technical gaps as you go.

Here at Expel, we agree with Dino's philosophy. First of all, start anywhere you damn well want to start. "Focus on what you want to *do*, versus what you want to *be*. Then, focus on finding the best place to do that and stay there."

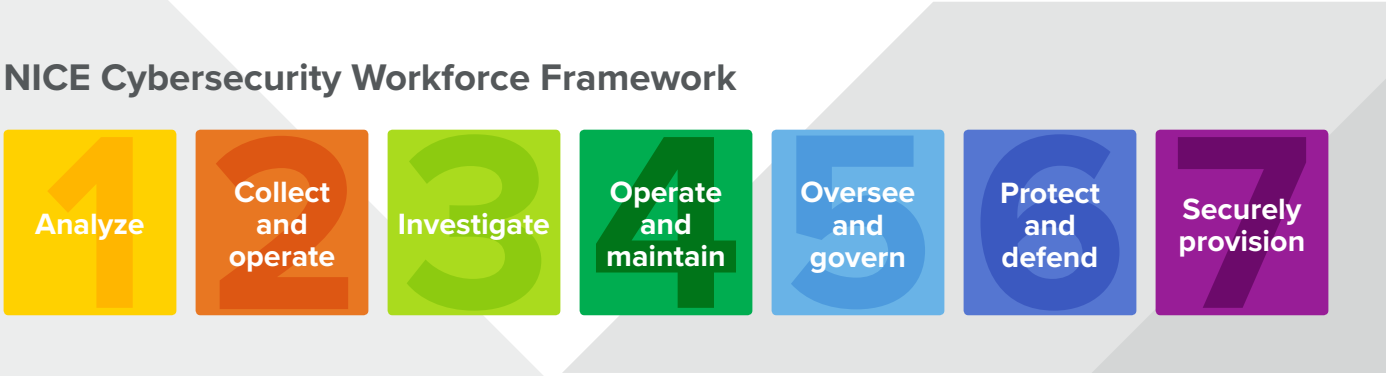


We've seen it first hand. We've hired several analysts straight out of college, and they're doing excellent work (If you're an employer and not plugged into the community at the Rochester Institute of Technology, and specifically working with their Computer Security program, you're definitely missing out). So we *know* there are degree programs out there that will prepare you for security jobs right off the bat.

Now that you know where we stand, we've got some tips on how to break into security. But there are lots of different jobs with the title "security" in them (and lots of jobs involving security that don't have "security" in the title) so it'll be important to make sure we know which ones we're talking about.

Which cybersecurity jobs are we talking about?

Wouldn't you know it, not only does NIST have a pretty great cybersecurity framework to help you manage risk, they've also got another nice framework that can help job seekers figure out what employers are looking for. A good first step towards finding the work you want to do is to identify the tasks that float your boat and map them to jobs that give you the opportunity to do just that.



Worried you don't have the technical depth for some of these roles? Entirely possible! If you drill into the framework a bit you'll see some jobs (like Cyber Defense Analysis, which we call a "SOC Analyst") have an *enormously* long list of knowledge areas you'll need to be proficient in. If that's the kind of job you want to do, it might make sense to start off with a less technically demanding role that has a lot of the same baseline prerequisites like an IT Program Auditor. You could use that as a stepping stone into other security roles as you develop a deeper understanding of the security space. And yes, you could certainly start with a role in Systems Administration or Network Operations to gain technical chops too.

"Wait a sec," you might be thinking to yourself, "isn't this just a cop out by defining non-security roles as security?" Yes, it absolutely is. You got us.

Frankly, as the NICE Framework makes clear, security is extraordinarily broad. While some argue it's "niche," it's really a compendium of niche knowledge across several vastly different work areas. That means if your mind (or your heart) is set on security, you can enter any of these domains and work your way into security. Or … you can start in security-specific domains and work your way into more technical roles over time.

Okay, so maybe you buy into the argument that the security domain is pretty diverse. Maybe you go one step farther and believe several of these roles include security responsibility even if they don't have "security" in their

title. After all, we've been saying that security needs to be built-in, not a bolt-on for years, right? Perhaps what's going on here is that the online brouhaha around "entry-level security jobs" is really focused on the security jobs where technical depth is essential. Maybe the argument is it's these jobs that require starting out in technical non-security roles first. Let's poke at that a bit. But first, there are a few things that'll apply no matter what direction you're coming from.

Let's try to agree on three things

Anyone can cook

Have you seen the movie Ratatouille? No? Yeah, that seems to be the most common answer. Ok, let's summarize [SPOILER ALERT].

There's this Chef, Auguste Gusteau, who authors "Anyone Can Cook." Throughout the movie, you're made to believe that the message of the book (and the movie) is that literally anyone can become a great chef. Even the protagonist, a rat, can do it because you can learn how to do it from a book. Yet, by the end of the movie, you realize the point is substantially more profound and realistic. Actually, no. Not *everyone* who picks up the book can become a great chef. But, in fact, a great chef could potentially come from anywhere.

There are so many paths to "success." There are exceptions to every rule. Anyone can cyber.

"Never" is rarely the right word

A few years ago one of us was walking up Main Street, USA at the Magic Kingdom. It was 8:30am and he refused to buy his younger daughter funnel cake first (oh, the humanity!) "You never buy me anything!" she exclaimed. He stopped. He looked around. He kept walking.

The notion that you should avoid absolutes isn't new. And in the tech space, it's particularly important. A great engineer and former colleague once said: "When the customer says it never happens, we need to build support for it to happen 5-10% of the time." So we're going to be cautious about these words when we're talking about career paths too.

Broad-scale discouragement is a Bad Thing™

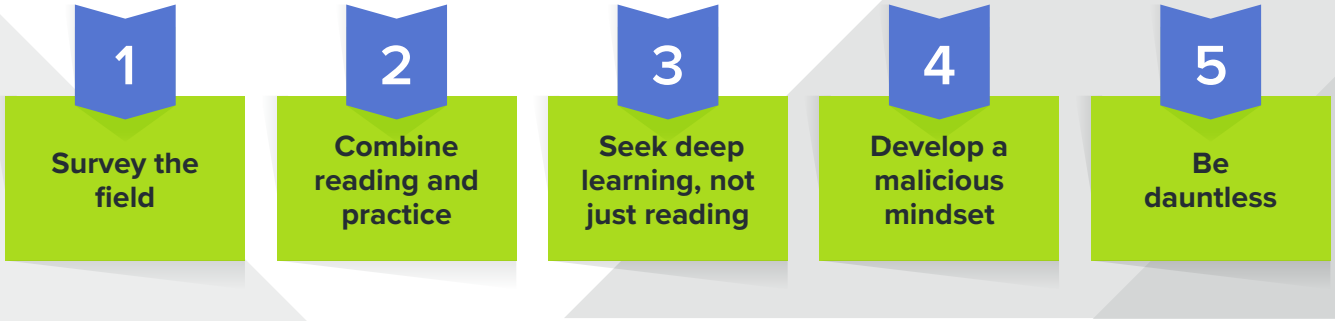
When you engage in an argument or even a mild discussion, there's a decent chance your conversation partner is already coming to the table with an opinion. If it's a strongly-held opinion, your counter-argument may actually galvanize their original belief. In that case, your discouragement is going to fall on deaf ears … so why bother?

In other cases, people may have a more flexible mindset. Think about a scout versus a soldier mindset. To a soldier, everything is black and white. Good and evil. Kill or be killed. Compare that to a scout, who's in information gathering mode all the time. Drawing conclusions are some general's job. Discouragement, in this case, could actually be effective! So good job, you've managed to discourage a portion of the population who could actually have been amazing contributors in the field. What harm is there on succeeding or failing on one's own merit? Why encourage people to punt on first?

Five habits that are helpful for (entry-level) security jobs

If you don't agree with the three items above, well … it might be a good idea to stop reading now because we're about to do some hardcore *encouragement*, and that might make you grumpy. After all, the next great information security practitioner could be reading this blog right now.

Also, we promised in the title to explain how to get into cybersecurity. So here are a few practical next steps. There are all sorts of resources out there that'll help you on the path towards becoming a super-nerdy cyber superhero. Here's our list of five things you can do to take the first steps to an entry-level technical cybersecurity career.



1. Survey the field

Follow influential cybersecurity evangelists on Twitter. The most successful ones probably aren't calling themselves cybersecurity evangelists. They're just constantly dropping knowledge bombs, tips and tricks that can help your career. Here's a short list to get you going:

@bammv, @cyb3rops, @InfoSecSherpa, @InfoSystir, @JohnLaTwC, @armitagehacker, @danielhbohannon, @_devonkerr_, @enigma0x3, @gentilkiwi, @hacks4pancakes, @hasherezade, @indi303, @jackcr, @jenrweedon, @jepayneMSFT, @jessysaurusrex, @k8em0, @lnxdork, @mattifestation, @mubix, @pwnallthethings, @pyrrhl, @RobertMLee, @ryankaz42, @_sn0ww, @sroberts, @spacerog, @subtee, @taosecurity

2. Combine reading and practice

This may shock you, but there's this security company called Expel that has a bunch of great content (full disclosure: we're biased). Self-serving comments aside, there are several companies that produce high-value security content on a pretty regular basis. High on our list are CrowdStrike, Endgame, FireEye, Kaspersky, Palo Alto's Unit 42, and TrendLabs. As you read, try to figure out how you'd go about detecting the activity they describe. Then, how would you investigate it?

Are you looking to grow your technical foundation for something like an analyst role? The breadth of what you need to know can be daunting. Perhaps the most foundational knowledge to pick up is around the TCP/IP protocol suite. Be prepared to answer the "what happens when" question confidently.

For learning about endpoint forensics, you probably can't get a better foundation than Incident Response and Computer Forensics 3rd Edition. The chapter on Windows forensics is gold. Dive into Powershell, associated

attack frameworks, and learn how to increase visibility into PowerShell activity with logging. Pair this knowledge with some of the best free training out there at Cobalt Strike. Watch the (most excellent) videos and apply the concepts you've learned as part of Cobalt Strike's 21-day trial. Not enough time? Consider making the investment. The Blue Team Field Manual and Red Team Field Manual round out our recommendations on this front. In parallel, set up a lab with Windows 7 (or later) workstations joined to a domain. Compromise the workstation using some of the easier techniques, then explore post exploitation activity. Your goal is to get a feel for both the attack and defense sides of the aisle here.

On the network side, consider The Practice of Network Security Monitoring, Practical Packet Analysis, and Applied Network Security Monitoring. When it comes time to take some of this book learning and make it real, resources like the malware traffic analysis blog and browsing PacketTotal where you can get a sense for what's "normal" versus what's not. Your goal here should be to understand sources of data (network evidence) that can be used to detect and explain the activity. To refine your investigative processes on the network, consider Security Onion. Set up some network sensors, monitor traffic and create some Snort/Suricata signatures to alert on offending traffic. Your goal is to establish a basic investigative process and like on the endpoint side, understand both the attack and defense sides of the equation.

3. Seek deep learning, not just reading

Have you ever taken a class and then months later tried to use the knowledge you allegedly learned only to discover you've forgotten all the important stuff? Yeah, if you disconnect learning from using the knowledge, you're going to be in a hard spot. This might be one of the biggest challenges in diving into a more technical security role up front.

To help offset this, in addition to combining reading with practice, consider the Feynman technique. Never heard of it? Well, it's easy to skim over bits and pieces you don't understand … but if you can distill it down into simple language such that others could understand it, then *you'll* have understood it better in the process. Nothing helps you learn quite like teaching.

4. Develop a malicious mindset

Years ago, a security practitioner was explaining how you can become a better defender by thinking like an adversary. The story came with some awkward (and humorous) interchanges. He walked into a hotel room with his family while on vacation, saw the unsecured dispenser installed into the shower wall and said out loud, "Wow, it would be so easy to replace the shampoo with Nair!" His family was horrified.

To be clear: we're not advocating that you replace shampoo with Nair, or similarly nefarious anti-hair products. And the concept of thinking like an attacker is not new. Eight years ago when Lance Cottrell was asked what makes a good cybersecurity professional, he said they put "themselves in the shoes of the attacker and look at the network as the enemy would look at the network and then think about how to protect it."

The best way to do that these days is by wrapping your head around the MITRE ATT&CK framework. It's quickly becoming the go-to model for wrapping some structure around developing an investigative process and understanding where (and how) you can apply detection and investigation. You might want to familiarize yourself with it prior to doing extensive reading and then come back to it from time to time as needed.

5. Be dauntless

Don't let your lack of knowledge stop you. There are organizations out there willing to invest in people with the right traits and a desire to learn. Apply for the job, even if you don't think you're qualified. Maybe you get a no. So what? Try again at a different company. Or try again at that same company later. Reading will only get you so far … applying your knowledge will get you to the next level. And guess what, remember that Feynman technique? Yeah, teaching that knowledge you've acquired to others will get you one level farther.

Good luck, happy hunting!

Finally … to those who say "an IT background and deep technical skills will help you get a job in security," we say: "We agree!"

And …

To those you say "security roles can be broad and you can use them to develop technical expertise over time," we say: "We also agree!"

What we don't believe in is telling people we don't know that they can't do something without understanding their unique situation. There may be paths that are generally easier, or generally harder. But assuming you can't do something is headwind you don't need. Hopefully you've found some guidance here that gives you the push you need to consider an entry-level (or later) security job and you'll apply. To that end, we say … best of luck!

Visit the EXE blog for more articles like this.

Expel provides transparent managed security. It's the antidote for companies trapped in failed relationships with their managed security service provider (MSSP) and those looking to avoid the frustration of working with one in the first place. To learn more, check us out at www.expel.io