

Gerald Auger: My name's Gerald Auger, Vulnerability Analyst. And that job basically is responsible for making sure that the systems and the processes and even the people at the organization, any vulnerabilities that they have are at least known about, and that there's some either acceptance of those vulnerabilities or that there's a remediation plan in place to remediate them and make them not vulnerable. [00:00:30] I really feel like in the industry there's kind of two traditional paths. You either go super deep on one specific technical element, you're the best pen tester, you're the best SOC analyst, or you go more of the analyst management role. And for me, that's the choice. And becoming a chief information security officer for a good size organization is really where I'd like to go, specifically because I'm able to apply all of the lessons I've learned across my career to really put it all together [00:01:00] and I guess own that entire responsibility.

So there are a lot of different on-ramps to cybersecurity. One of the really sexy, interesting, fun things about the industry is that everybody kind of has a different story. Me personally, I went more of the traditional computer science undergraduate degree. I got out thinking that you could only be a software [00:01:30] engineer with that degree. So that's what I went on and did. And early on in my career, maybe a year and a half into being a software engineer, I had my code audited, but only from a cybersecurity perspective, which was a totally new concept for me. Cyber, I went through undergrad in the late '90s and cybersecurity wasn't really a thing at that time. So when I got audited and did horrible, quite frankly for cybersecurity components in my software, [00:02:00] I was kind of taken back and wanted to know more about why did I fail, what was up with this?

And then as I began to understand, I realized this is very cool. This is, oh, super cutting edge. There's an element of cat and mouse to it as you're dealing with criminal actors and really not just understanding how IT works, but understanding how you can secure IT and if you're coming at it from the other angle, how you can abuse or hack IT in order to do things that it [00:02:30] wasn't necessarily designed for. So once I found out about that entire element of the industry, the IT industry, if you want to say it that way, I was hooked and immediately pivoted and never looked back frankly.

I'll say this about skills. There's kind of, again, two buckets that I would say. One is your core hard technical skills, things that [00:03:00] you can just learn. A perfect example is programming and with a computer science background, networking and operating systems also. So I regularly tell people, "If you want to work in cybersecurity, you really need to understand networking and you need to understand operating system, and you really don't need to understand programming, you don't." But because I was a software engineer, I do understand programming and that skill gave me a huge leg up because I was able to read other people's software, you download some [00:03:30] open source tool, you can quickly analyze it, assess it, tweak it if you want to. So I found having that skill gave me a huge advantage early on in my career. Now,

from a non-technical skill perspective, I'm naturally inquisitive. I have a thirst for knowledge and I take a lot of initiative and proactivity, I'm self-driven I guess is the way to put it. And in the world of cybersecurity, that's equally important.

[00:04:00] So if I was going to talk to a high school senior, really anyone who was looking to pivot into the industry, regardless of where they are in their career and regardless of what level of experience they might have, what I would definitely tell them is there are so many free resources out there. So definitely, definitely take advantage of those and just Google's your friend or search engines are your friend, however you want to say it [00:04:30] and learn basic, basic computer networking. Professional networking is important as well, but understanding how a network works. When a computer talks to another computer on the internet, how that happens is important because when you understand how it's supposed to happen, then you can begin to understand and see how you could break it from working the way it's intended or abuse it to work for some way that you want. And by seeing how you can break it, that is the vulnerabilities. [00:05:00] That's what you're identifying is how is this vulnerable to attack?

Looking and thinking, it's almost the mindset. So you can use tools and techniques and we'll talk about that in a second, but understanding the mindset of what you're looking for when you're thinking vulnerabilities will go far further for you than just memorizing a checklist of five things that you need to do. Again, the technical piece is you do need to understand [00:05:30] some of it, so you can have frame of reference when you're actually doing vulnerability assessment and analysis, but you need to have the mindset of you're looking for things that can compromise, again, confidentiality, integrity, and availability of these systems. Now, by the way, you can also think of this as two different ways.

I don't want you to pigeonhole into there's just the guy or the woman at the desk analyzing a report that this tool pops out that I mentioned earlier. You can think of vulnerability analysis [00:06:00] from both a defensive perspective and an offensive perspective. What I mean by that is the defender who is protecting the organization, and this is more of the role that I currently play. I'm defending the organization, so I'm constantly aware of where are the vulnerabilities on my network.

In an enterprise environment, so if you're doing this for a company or corporation, you'll come in. Typically, [00:06:30] if you have a lot of endpoints we call them, or devices on your network that need to be scanned, you may not be able to scan them every day or every week. You'll have these, they're called scanner appliances deployed tactically through your environment, and these appliances will be scanning across your network range, your IP range of your endpoints. As they're scanning them, and by the way, they scan them and then start over and start scanning them again because everything changes so quickly and [00:07:00] the vulnerabilities get dropped every day, you need to scan it

again. There's never a sit on your laurels. So you'll go in, you'll look at the most recent output of vulnerability scan reports, see if there's been any major changes in your environment.

Maybe some devices showed up in your environment that you weren't expecting, maybe some went away that you didn't know about, fully understanding that then it's less of a actual day in the life of and maybe more of a month in the life [00:07:30] of because you'll start putting together your reports of, okay, here are all the vulnerabilities that we have. It looks like we've got these critical ones. You'll want to group your vulnerabilities in level of, I guess, how bad they are, frankly. So you can have some really obscure vulnerability that has a very low likelihood of ever being exploited, and even if it was, it's on the coffee machine and while I start my morning with coffee, if it goes down, I can just go to the coffee [00:08:00] shop and get a coffee. So there's really no impact of that coffee machine getting compromised.

So you don't even worry about that. But if it's our main manufacturing machine that prints the money and that's got a massive vulnerability on it and it's facing the internet, you can believe that that becomes a red-hot priority and you might not even do your regular kind of like, here's a bunch of things that we need to fix and here's like the plan on how to fix them. You may pull that out and escalate that immediately. [00:08:30] Again, speaking to the business, we've got this real serious issue right here. We've got this vulnerability. If it gets exploited, the entire system could go down and this is why you get paid. Ultimately, making recommendations in helping business decision makers make a decision for a way forward that would have you in a better cybersecurity posture.

For anyone who wants to work in the field, one thing that I can't [00:09:00] emphasize enough is that nobody should feel like this field and this job specifically is out of reach of them because they're not technical. You can accumulate the knowledge that you need to do this job regardless of what you're into or what your background is or what your walk of life is. It's a very, very accessible and inclusive job role. I will say that in my opinion, there's something for everybody in cybersecurity. So if vulnerability analyst isn't your bag, [00:09:30] then definitely continue to look at the other roles because the field has given me incredible satisfaction and it's given me a great career and I'm looking forward to continuing to work in the field.