

Jonathan Kayemb...: My name is Jonathan Kayembe. I am a cybersecurity assessment analyst. My job includes performing cybersecurity assessment, PCI compliance assessment, and including CMMC.

PCI stands for Payment Card Industry standards, a way of protecting [00:00:30] credit card information. So there's a standard regulation that companies have to follow in protecting credit card information.

CMMC stands for Cybersecurity Maturity Model Certification, a certification that got rolled out late in 2020 by the DOD.

For any contract working with the DOD, they have to be CMCC certified in order for them to receive an award letter and continue their operation.

[00:01:00] In the future I see myself expanding my technical skillset, going more on the defensive side of cybersecurity. I see myself ultimately becoming a security engineer.

The defensive side of cybersecurity includes being on the first [00:01:30] line of defense when it comes to security.

When you think of the army, the marines, they are the first line in combat. That's kind of like what we are, looking at incidents, triaging them and making sure everything is in a line. If there's any investigation that needs to happen, we're the first line of defense.

There's a lot of training that one can do to get to that next level, but ultimately [00:02:00] it's working in the industry. It's the best training one can get, working with people who are actually doing the job. I think that's the best route to go by.

Certification doesn't hurt to get, but ultimately working in the field will actually help you get that experience to get to the next level.

It started back in [00:02:30] the dorm rooms back in college. I changed my major relatively, probably three to four times.

The very first time I thought about it was when I was talking to my older brother. He's a software developer for a company down in Charlotte, North Carolina.

Just looking at what he did, programming, working in tech that caught my interest. Deciding a major to [00:03:00] major in in college was a very crucial moment in my life, but I never thought I would be in tech.

But looking at what my brother did and deciding what to do, that ultimately led to me deciding my major in computer information security.

The skills that I already had was, as I said, I'm a people person. Being able to carry a conversation with individual, [00:03:30] being a great listener is very important. Because if you don't have that, no matter how skillful you are in technology, you won't be able to understand what's at the core of any situation.

I would say start playing with computers. The first thing you would want to do is open up your own lab.

Everyone has [00:04:00] a router and a computer at home. Start manipulating with them and get to learn what is a router, what is a computer, what is a modem?

That's very basic, because everyone has the internet at home. I think that's a great starting point, starting to learn how computer communicate with each other.

I think starting the fundamental is to learn more about networking than ever, because that'll help you ultimately understand what at the core, what is [00:04:30] a TCP IP, how a computer communicated with each other. I think that's a great place to start.

The three main thing that I needed to do my job currently, I think integrity, having a humble spirit and have a passion for learning. It's very crucial.

For me, coming from where I come from, [00:05:00] integrity is very crucial. Going into the workforce with all these three combined, I think ultimately helped me to be first, a great employee, a great individual and be able to do my job well.

One technical skillset I use a lot requires a lot of the technical writing, analyzing information, control testing, I would say.

Being able [00:05:30] to write good deliverable, I think it's very crucial, especially in cyber assessments.

For me, success is not defined by how many accolades you get or what credentials is to your name. I think success for me is being able to recognize your [00:06:00] surroundings and be able to help another individual get to the same level as you are or greater. Helping people obtain their goals, for me, will ultimately give me a sense of gratitude.

Cyber governance and strategy is a lot of documentation, report writing. It doesn't really require a lot of technical aspect to it.

Being able to understand what someone who's not [00:06:30] technical, what words? Be careful with your words. What words can you use? But having that

skill to be able to communicate to a non-technical individual is very crucial, especially in my field.

If I knew someone who was about to start my job, one advice I would give them is to acquire these three skills. Be a great listener, have integrity [00:07:00] and be humble.

When you go into the workforce, working governance or any job, having these three skills will help you be successful at your job.

I think the main thing going into cybersecurity that everyone should be familiar with is, especially in my field, you have to understand the cybersecurity framework and how to utilize that framework, [00:07:30] understand people and what technologies utilize to actually protect these systems because we are the first line of defense.

As we are being able to understand how these systems work, what vulnerability are there in place, give you a headstart into knowing well how to defend what's at hand.

[00:08:00] One of my best memories was one time we traveled to Chicago for one of our clients. We got there to meet with higher executives, CFO, CEO, talk about how the environment is.

From there, we're able to understand what they do on a day-to-day basis, [00:08:30] what technology they have in place. That helps us gather that evidence to be able to test our controls. Being in a room full of CTO, CFO, you don't get that anywhere.

The best part about my job is working with great people, intelligent people [00:09:00] who encourage me every day to be a great individual. So, I guess every day could be my best day.