Raquese Harris: Hi, how you doing? I'm Raquese Harris. I am an incident responder. So what an incident responder is, is someone who is very investigative, loves to correlate different events together and be able to respond to malicious activity.

So some examples of malicious activity could be like a phishing attempt, [00:00:30] so this could be someone that is sending an email to maybe your coworker and it's disguised as you yourself, but it's not actually you. That's one example of a malicious activity.

I actually started in the criminal justice field at first in the intelligence field and the way that I pivoted into cyber is that [00:01:00] I just really liked the criminal aspect of cyber. And when I started learning the backend of how a threat actor behavior was, my dream goal was like, okay, I think that I want to be that person that is defending our governments and our networks and moving up through the ranks of probably in the C-suite of CISO or CIO. The biggest thing that [00:01:30] I would say that is really going to get me there is adopting mentors. And currently I have about three mentors that sit in those seats right now. As a CISO, I would be able to be over the whole cybersecurity infrastructure or the whole network.

I think the biggest thing that happened to me was just seeing cyber crime. [00:02:00] I used to work in an intelligence agency and I would see a lot of cyber events from a fraud perspective, like actors from Russia or other different countries committing these actual cyber crimes and there's no trace, we don't know how to trace it or anything like that. And that's sort of really got me interested in how do I take the necessary steps to be a part of the other side of the house of trying to defend [00:02:30] our nation and everyone from these type of malicious acts.

The biggest skills that I think I definitely had was being investigative, being more of learning how to triangulate different events and using open source things. And when I say open source, I'm talking about a Google or any type of open source search engine. The beauty [00:03:00] about the industry is that everything's not going to be just in one place and there's a lot of other sources that you're able to grab from to be able to really correlate a type of event that you see. And so those type of ideal characteristics are very valuable in the industry of just being a self-starter and being able to triangulate different events together to come up with one [00:03:30] actual conclusion.

When I first started cyber, I had zero technical experience at all. Like I said, I was coming from more of a law enforcement intelligence background and military background. I used a lot of training academies and what those platforms provided me was a roadmap as well to get to where I wanted to be. So I was able to set [00:04:00] up different labs and environments at my own home and use those events and scenarios to use it as a relevant experience. So when I would interview with recruiters, anything like that, they would say, "Okay, what is your experience?" And I can tell them, Hey, I don't have professional experience, but this is what I've done in my own home. And most of those courses are literally called security analysts or incident [00:04:30] responder or SOC analysts, and it would be really simulating the job that you would have. So when you're speaking to the scenarios that you're doing at home, it's literally what the recruiters are looking for and they would be more happy to hire someone like that versus someone that's just interested in the industry.

You pick a role that you want to do in the industry, so if you want to be a security analyst in the SOC, YouTube should be your best friend. There's so [00:05:00] much out there that you can see and people are talking about a day in the life of what they do, and so you want to do your due diligence on the actual role, whichever company that you're interviewing for, you want to do your due diligence about the company itself. You want to show the recruiters and everyone that you are a self-starter and that you have a technical acumen, but you're also highly motivated because those are what [00:05:30] we're looking for in the industry is someone that's motivated and not wanting to be on autopilot.

What makes you a great cyber security professional is thinking outside of the box. Cybersecurity, you're never going to know everything. You have to know that it's okay to not know everything. It's an environment that has to be collaborative. You can't have this without that. [00:06:00] And that's like the beauty of the industry itself. So I would say if you have leadership characteristics, being able to have good continuity skills and communication skills, you'll thrive in the industry for sure.

You would know that you're being very successful when you go home at night after you log off and there's an event that has bothered you that you couldn't get to the end of it and you want to go home and you want to work on it after hours. I think that's when I really felt like [00:06:30] this is really my career.

Something about the job that most people wouldn't know about coming into it is that you don't always have to know how to code. And I think that when someone thinks about cybersecurity, they think that you're behind a desk, the average hacker or something like that, but there's so much opportunity in cybersecurity right now that [00:07:00] people just don't know. I think I looked it up not too long ago that it was over 500,000 job openings and it's projected to grow by 350% with over the next eight years. And that's not all surrounded by coding and stuff like that. There's a compliance side of the house, there's an incident handling side of the house and other realms of cybersecurity. So I think that knowing that [00:07:30] it's not just a technical industry, there's non-technical roles in the industry as well.

You're going to come in, usually you're working 12-hour shifts, and so the guys that just came in, they're going to do a handover. They're going to tell you, "Hey," if you're working nights, I actually did have the fortunate to work overnight, so I will work a 7:00 PM to 7:00 AM and so [00:08:00] at 7:00 AM we would do a turnover to our day shift, tell them anything that has happened in the environment over our shift and kind of tell them if upper management has told us that we need to do something of those sorts.

And then coming in, you're going to sit down, you'll open up all your tools, so that probably be your networking tool, your SEM tool, which is a security incident management tool. So from there you're going to see those [00:08:30] anomalies that I was talking about and should you see something like that, now you're looking into another database to kind of see if there was any historic events prior to this. And if there was, you can kind of see how the previous analyst or the previous team handled this event and then you can take that and be able to remediate this event or notice that, oh, if this ended in a false positive that you know that this event is actually a false positive. From there, you'll [00:09:00] be able to write up a report for your customer and you can say, "Hey, this event took place at this day, at this time. These are the steps that I took, me and my team. Here's the artifacts that are associated with this event, and now we're going to go ahead and close this out."

I would definitely say that do not sell yourself short, that you are smart enough, you can do it. There's so [00:09:30] many opportunities in the field whether you're technical or non-technical, and is absolutely needed and it's going to be needed for a long time.