Madeline Sides: My name's Madeline Sides. I'm a SOC analyst for Ally Financial. Working in the security operations center, pretty much the day-to-day task is triage, investigate and escalate. We kind of work as the first responders of the whole company.

When there's a SOC event, we triage it, which means we just assess it, look at it, and we investigate it to the best of my ability. [00:00:30] Then from there, I escalate it up if I can't make a determination on if the event's malicious, non-malicious or if it's a security concern. Then from there, it might go all the way up to the CSIRT, which is the incident response team, and it'll be handled accordingly from there.

Cybersecurity careers that seem exciting to me would be part of the pen testing side or the red team, because it's the [00:01:00] offensive side and you get to actively hack the company or search for vulnerabilities. It's kind of different than the role I'm in now, whereas I'm defensive, so I think it would just be really cool to see that field.

Mainly what I liked to do before I went into cyber with computers was just creating fun videos with my friends or just the basic schoolwork using Microsoft PowerPoint, [00:01:30] Excel. Really my knowledge of computers compared to other people, it wasn't as broad I would say, it was just pretty limited to the basic usage. I knew how to operate the computer and I could probably troubleshoot a problem, but outside of that, there wasn't much else that was occurring.

I think it was easy to transition into cybersecurity with not have a big computer background, just because when you learn cybersecurity, it starts you from the ground. You don't just dive in, [00:02:00] this is what a vulnerability is, this is all the different types of malware, these are all the different types of tools. It really started you from the ground, like this is first, this is the computer, this is how computer operates. So, really just starting from the basics and then building your way into it. The more and more you wanted to learn on your own too, so you found yourself in your free time just kind of studying and researching stuff on your own.

So, [00:02:30] I would say what prepared me for going into cyber outside of school was being involved, so getting involved doing internships and studying for certifications. I think the certifications really showed me that I knew the knowledge, it made me more confident as a person in the field of cybersecurity, because while I could read the textbooks and go to class, the certifications really proved that I knew what I was doing. I think everybody's kind of nervous on their first day of work, and so for me it was just calming and reassuring that everybody [00:03:00] starts somewhere.

Obtaining the professional experience required through internships was a big help, because not only did you get to learn how a business operated, but you learned what roles you may like in cybersecurity, what roles you may not like, and so it kind of helped navigate to where I wanted to go after I graduated.

To help me get through incidents, especially when I first started, I really just relied on my teammates and having the skill set that they [00:03:30] provided, because I think anytime you start a job, you're scared that you're not going to be able to perform the role, which is totally the opposite. They're there to help you learn and train you along the way, so I really relied on my teammates the most for their help and guidance, and some of them have become my mentors throughout my career so far.

Teamwork in the SOC I would say is really built around communication. You want to make sure that you're communicating the right things to the right teams and that you're responding accordingly to the event that's happening.

[00:04:00] If I had a friend who was about to go to school for cybersecurity, I would just tell them that you really just got to start reading. You got to find the current news, stay up-to-date, you just got to find what interests you, what you want to learn about more, but really just starting to read, learn more about what cybersecurity is.

Some skills that I think my friends would need to have if they were going to go into this field is communication, because you got to [00:04:30] be able to respond on time and appropriately, but also just having leadership skills. People like to see you take lead sometimes, especially when it's a call. Normally the SOC is in charge of leading it until it's escalated to the CSIRT level, so really just leadership and communication, being a good teammate overall as well.

One way that I measured my success in my career is reflection. [00:05:00] Reflecting over the past year that I've been in this role, I can see where I started and how shy I was and now how vocal I am in this role. Now I speak up more, to the point where I train the new hires, which is cool to see, 'cause I couldn't have done it without my teammates guiding me along the way. So, really help from others.

Another thing that helps measure my success is the positive feedback that I receive from my teammates. They're always encouraging and let me know ways that I can correct myself [00:05:30] if I do make a mistake, but always in a positive way.

One way to help me grow in cybersecurity was through a mentorship. So I have somebody who mentors me and they help guide me along the right track, always asking me questions, making sure I'm still putting myself in challenging positions, going outside the box and really just challenging my overall knowledge. I think one good quality that somebody has to have in the cybersecurity field is just [00:06:00] their integrity.

A day in the life of a SOC analyst is you make sure that whenever the person coming in to take over knows exactly what they're doing, and if there's meetings that need to take place, you're normally the first one to hop on. Other things that I would say I tackle on a daily basis is phishing is a big term. Going through a bunch of phishing [00:06:30] emails, assessing, making sure that they're legit, and if they're not, explaining what they are.

One of the things I do is monitor and scan our endpoint detection tools, making sure that our IDS hasn't picked up anything, and if it has, then I assess it, just taking over from what the night crew had passed on. We monitor our dashboards for various type of alerts. Alerts come through our endpoint detection systems on an IDS, which is an intrusion detection system [00:07:00] that we have in place, then we'll go and assess it. Sometimes that may start up bigger calls depending on the severity or the criticality rating of the alert, so you're always constantly investigating things in the SOC.

I think cybersecurity can be for anybody who has a passion for computers or just wanting to learn more about cybersecurity. For anyone who's considering cybersecurity, [00:07:30] I would just say go for it, because you're not going to get bored, it's something new every day. You're always going to be challenged, you're always going to be thriving in whatever role that you're placed in, and really it's just a lot of fun.