**AT: Aaron told me you work in security at ANZ. Could you give us a brief summary of what it is your job entails?**

TO: So, I work in threat intelligence, so the broad overview of the job is that we’re looking for information about what threat actors or hackers are doing around the world, particularly if they're interacting with banks or Australian targets. And figuring out how they do it and, if they're likely to target us, how they target us and helping investigate any incidents that happen.

**AT: I did some very light stalking and found your LinkedIn, but it’s very, very sparse**

TO: Yeah, that’s a mixture of me just being the sort of person who updated, but also, it's not actively discouraged or anything to keep it updated but if you don’t want to be targeted by hackers...

**AT: You listed that you had a Bachelor's degree in IT from RMIT. How much more training past that did you undertake to feel experienced enough to take on your job?**

TO: So, I’m in this job because I was working under the current boss of it and he basically thought I'd be good at it, so I went with him. I didn't have any other formal training before moving into this job but since moving into the job I've gone through some **SANS** courses and other training materials

**AT: Are there any specific modules that you might be able to highlight?**

TO: So one course I’ve done and completed is the reverse engineering of malware, a SANS course and I haven’t completed any formal assessments or done a formal qualifications, but I’ve gone through the material for CompTIA, some of *Certified Ethical Hacking,* and for those it was more just for my own benefit

**AT: So, a lot of it is just on the job training, rather than typical classes.**

TO: So, yeah a lot of what I’ve learnt for my job was just on the job, slash, as we were developing processes that we were going to use.

**AT: Do you happen to have any insight into what exactly makes your position different from other tech positions or even other cybersecurity positions.**

TO: So, threat intelligence as opposed to other security positions is a lot more open source intelligence focused, so we’re getting a lot of external intelligence and there is a lot of looking at internal logs and incidents, but I find other security jobs, from what I know of them, they're a lot more internally focused.

**AT: Do you have interactions with clients, vendors or like actual bank customers or is it just?**

TO: Only tool vendors, software vendors that of tools that we’re going to be using.

**AT: This is a very broad question. What exactly do you spend most of your time doing?**

TO: That, that changes depending on what’s going on. We put in a lot of effort into understanding the hackers, threat actors that will be relevant to ANZ. I think that’s probably one of the longer-term consistent activities.

**AT: What do you consider the most challenging tasks in your position to be?**

TO: Hard to say, it changes.

**AT:** Because I tried to do some level of background reading into this, but it was very, very vague because it seems people don’t like to talk about security based stuff

A**T: Changing tac slightly, do you find that, you're able to get a level of social life? That extends beyond your work, or do you find that you bring your work home?**

TO: I find it easy to separate, work and like personal life, and that's just always been me.  I can go from working on something to switching off in 5 minutes without an issue.

**AT: Is that the case throughout the field itself? Was that a personal thing?**

TO:  I think that's just a personal thing. I'm sure that the people would perhaps struggle more other people struggle less, but yeah, I've just always been able to split them.

**AT: For someone who was trying to get into your field. What sort of skills would you recommend they focus on whether that be not just technical skills, but like to some level, interpersonal skills and stuff like that.**

TO: I think being able to simply explain complicated topics is probably like the biggest one. but if, like you're just looking to get into the field, by far the most important thing, I found is just having like a genuine interest in the things that are going on like. Before I got into security, I was already just had an interest in it. I was able to like the things I have to know for work now. I already knew just because I'll be Googling, and I'll be talking to people online. Who were also interested in it.

**AT: This was more than just like a hobby that, because this was a passion that became a profession sort of thing, it wasn't just something that you pursued for the sake of money...**

TO: Yeah. So, I wasn't looking specifically for security when I ended up in it. But yeah, I just did have an interest and it worked out well, yeah.

**AT: We have run through all the questions quite quickly. I just had one more, one fun fact sort of thing. Do you happen to have a favorite cyber security event? That you pull out at a bar or something that people could talk about.**

TO: I've got a few. I, much to the dismay of some people, really, I mean, I’m really interested in, like, what hackers are doing, and I find it like, you know, other people like “oh no hack!”, and I'm like “that's a really cool way to hack.” and I could go and talk to them. So, there's been some like, really notable hacks over the years. The one I like to bring up is... It's a really old one, a malware called SQL Slammer. It was particularly widespread, it took over, like, so much critical infrastructure around the world, and then they just done nothing with it. It was like they just used it to prove a point. Like they could do it and then decided not to [use it].

**AT: Was this from like a rogue sort of group, was it?**

TO**:** No one knows. I don't know. This was, like, back in the day. The majority of the machines that basically required the Internet around the world and they just sat there.

**AT: I need to look into this one. I haven't heard this one. The one that I recently heard about was... there was one that I think the American government entered onto a USB and then and then somehow managed to get it into Iran and it's started playing with centrifuges and stuff.**

TO: Yep.

**AT: That's similar?**

TO: It's not similar to SQL Slammer, but also a really interesting one. Just because the delivery method was unique and it's obviously like, you know, super high stakes, high profile, that was a really good one.

**AT: Yeah. Adam, did you have anything else that you wanted to ask?**

**AL**: **Umm, probably just my one question is, where do you think the future of cybersecurity is heading, because you know how the world's changing, it's kind of like it's changed a lot from like say 20 years ago? And, where do you think it's going to be like in another 20 years?**

TO: 20 years. Yeah, like very hard to say because as you said, it's changing so much like no one 20 years ago could have predicted where technology and stuff was today. Um, I can say for sure that it's going to just keep getting more and more important. Umm, this stuff like, you know, the Australian government’s 5 fold increase the cyber security budget this year, so they're all about it. But yeah, hard to say where it will be, but it will be important.

**AT: You said five fold increase in the security budget?**

TO: I think, that's off the top of my head, but yeah, it used to be like nearly 2 billion. I think it's just over 10 billion now this year.

**AT: OK.**

**AL: You're probably happy with that.**

TO: Well, yeah. Except, I think that's going for specifically, like, jobs in government, which I'm not going after, but maybe one day if I do.

**AT: Do you think you'll stay in this field or...?**

TO: Yeah, I find it really interesting

**AT: Well, yeah, that that was about it. Thank you very much for your time.**

TO: No problem.