Toni: My path to cybersecurity

Hi, I'm Toni, I'm a Security Engineering Manager. Our teams protect Google and its users from serious threats. Usually government-backed attackers, coordinated influence operations and serious cybercrime threat actors. I grew up as an army brat. My dad was in the military and we moved around a lot. I've always had an interest in security sort of generally. I got really hooked on international relations when I was in high school. I did a lot of Model United Nations. And that really sort of brought these two things together for me, the way that security works in the world. I come from a big family. I knew I was going to need financial assistance to go to college. And the Department of Defense provides a lot of educational opportunities that are tied to service. So this was a natural fit for me. I knew I was interested in this area and this was going to provide a career path into something I was passionate about. I started as an intelligence analyst, but not focused on cybersecurity. I worked counterinsurgency for a number of years and geopolitical intelligence issues. Eventually, as I looked and saw that the way that cybersecurity was starting to have an impact both in our daily lives and in that world of international relations, I got more and more drawn to it. Transitioning into cybersecurity was a huge shift for me. I came in without a solid technical background, had to learn a lot of that on the job and through self-paced learning in different types of courses, I needed to learn programming languages like Python and SQL, two of the things that we cover in this certificate, I needed to learn a whole new language about the vocabulary of threats and the different components and how those manifest technically. One of the things that I had to figure out very early in this journey is what kind of learner I was. I work best with a structured learning style. So turning to a lot of these online courses and resources that took this material and structured it sort of from first principles through application resonated very well for me. A lot of this was also learned on the job by co-workers who were willing to share and invest time in helping me understand this. I asked a lot of questions and I still do. Most of cybersecurity work is going to be learned on the job in the specific environment that you're protecting. So you have to work well with your teammates in order to be able to build that knowledge base. My advice would be to stay curious and keep learning, especially focusing on your technical skills and growing those throughout your career. It's really easy to get imposter syndrome in cybersecurity because it's so broad and mastery of all these different areas is a lifetime's work. And sometimes that imposter syndrome can shut us down and make it feel like, why bother trying to keep growing. I'm never going to be able to master this instead of motivating us. So keep learning, push through that fear. The efforts always going to be rewarded.

Revision #1
Created 30 May 2023 13:00:23 by naruzkurai
Updated 30 May 2023 13:00:33 by naruzkurai