Zack: Incident response and the value of playbooks

My name is Zack. I'm a Software Engineer on the security team in Google Workspace. I have non-traditional background. When I graduated college, I originally thought that I would pursue law, but I was accepted and I decided not to go. Instead, I joined Google in recruiting. Through that work, I did a little bit of strategy work where I taught myself web scraping and I really liked it, so I took one of Google's internal training courses that helped me move from recruiting to software engineering. Processes and playbooks are documentation that software engineers and other people at Google use to determine how we can respond to things that happen. Whether that's a security or privacy incident, whether that's an active attack, we have sets of guidelines or algorithms that we use to determine the best course of action to make sure that we manage people's data and security well. I'm relatively new to cybersecurity. I've been a software engineer here for about two years, and I don't have enough knowledge to be able to respond to every single thing that could possibly come my way when I'm on call or when I'm helping resolve a vulnerability. The playbooks are super important to people like me and other folks who are joining the industry new because they allow you to solve the problem with the experience of a much more experienced person, basically decades of experience in your own resolution because you can rely on this playbook and other people's advice. The kind of things that we use playbooks for our open attacks, privacy incidents, data leaks, denial of service attacks, service alerts, and others. When I first started out at Google, my first task on the security team was to fix an externally reported vulnerability. That means some security researcher out in the wild was playing with our app and found something that could potentially leak our user's data. When I received that, it was my first task on the team. Looking back on it, it's a relatively easy thing to solve, but it felt really overwhelming at the time. But when we receive a vulnerability report, it comes with remediation guidance. There were steps in the bug that was sent toe saying this is the things that we think that you should do. The things that I would say to somebody who's interested in starting out in cybersecurity is talk to as many people in the industry as you can. You'll learn about what the job is like. You'll learn about the skills that you need to get yourself there. If that's something that you're interested in, you'll learn about open jobs and roles, what it's like to work at different companies. I wish people had told me when I graduated college that what these jobs are really like. I thought that coding would be heads down, typing away at a computer and a dark office for 12 hours a day. But it's not like that at all. 50% is communicating with other people and reviewing designs and talking about ideas. That's really compelling and I think if somebody had said that to me at the beginning of my career would have been totally different. Some teams come in and out of fashion, but security is ever-present. It's really important now it's only getting more important. There's a certain amount of security that comes with being in a security team. Definitely, a good place to be.

Revision #1
Created 2023-06-15 12:49:19 UTC by naruzkurai
Updated 2023-06-15 12:49:58 UTC by naruzkurai