Portfolio Reflection

Most of these are relatively common sense however if you don’t know the things then they can’t really get to a point where they become something that seems simple and obvious. Keeping your program secure and adopting security policies like 0 trust is very important. Attacks can come from everywhere, even from within your organization itself. Technically I’ve signed an NDA but what I can talk about is that I work at a data center for a very big FAANG company, and 0 trust is something they 100% percent practice and as a software dev I tend to analyze the programs I use a bit. The idea behind it is pretty cool, as we learned in our readings both the machine and the data are both authenticated through a proxy so unless someone has both my credentials, my UB key and is on a laptop connected to the private network at work, you won’t be able to access any data. However, this system must be properly implemented, just the idea alone isn’t secure. Every employee must be given a UB key, a laptop, and the network requires constant maintenance as new vulnerabilities could be discovered and every system is not 100% secure.

When breaches or bugs do happen, it’s important to perform a cost-benefit analysis of how big the breach/bug is and the damage that will be caused. This is pretty essential as it will allow you to see how a problem will affect everything and whether its worth to fix it or just leave it till another day and concern yourself with the more important aspects of security.