8-2 Journal

The zero-trust policy helps to ensure a network is at its most secure. This is obtained by not just assumingly trusting anyone in and/or outside of your organization. On top of making your code the most secure that it can be, it is best to ensure that whoever has access to your product is the correct person. The first way this is done is by validating every user to ensure that you have the correct user accessing the correct files. The second way is validating the devices that the user is accessing the files through. Providing limited access on a need-to-know basis is also a great way to implement the zero-trust policy. The best way to operate with a zero-trust policy is to conduct yourself as if it is going to be a breach soon. This will keep you alert to always implement this policy. Another way to implement the zero-trust policy is to ensure that you are taking note of who is logging in and at what times.

The zero-trust policy changes the way that I think about security by making me want to make my code as secure as possible, while also being un-hackable. This policy causes me to want to be very careful as I double check my code prior to submitting it. This will impact my user by ensuring to them that they are using a secure network that is un-hackable. I will persuade developers who oppose the zero trust policy, by showing them how much of an easier, un-hackable, trustworthy, and more efficient it is to use the zero trust policy.