Reflection Journal

Security in development used to be something left for the security team. It was also often only addressed after the application or systems were created and ready to be implemented. Now security is everyone’s concern. The DevOps stages have become the DecSecOps stages. This new structure incorporates security in every step and makes it everyone’s responsibility. This puts security in the for front of the designers, developers, testers, and implementers.

There is a cost to this strategy though. Obviously, some designs may take more time to figure out when taking security considerations in account. Building with automated testing will also take more time to set up, and more build time each time it runs. However the cost and effort of mitigating an issue would be so much more. Also as these practices become common place they will take less time.

The zero trust concept is one where no one is trusted and permission must be explicitly given for actions. This applies to people outside and inside the organization alike. Even authorized user must authencticate for different actions. This prevents someone from within the organization, exploiting a system, they had access to and they didn’t need.

Security policies set standards for many things, coding included. Coding standards set standards for how to code. Each item in the coding standard calls out the undesirable behavior and show examples of the desirable behavior. It also show the likely hood of this occurring, the risk, and the level of mitigation efforts. Each language a company uses, should have coding standards created. They should be introduced and implemented in the developer community. These standards should also be reinforced in the code reviews.