Name: Gerardo Gonzalez

Date: 2024/02/11

SNHU: CS-405

**8-2 Journal: Portfolio Reflection.**

Reflecting on this course I have learned that adopting a secure coding standard is essential for a developer, this is because having a secure coding standard helps stay up to date, and prepares one for real-world situations where threats come from all places.

Evaluating these threats and assessing the levels of risks and costs they can have on assets, systems, and data not to mention a company's reputation is necessary for an organization to stay protected. Finding out what are the risks and costs is the first step to creating a mitigation strategy such as using DiD to prevent and lower the levels of risk and cost attacks if a malicious user gets past certain defense barriers.

One way to identify malicious users is by having a zero-trust framework where everyone both internal and external, is not trusted. This proactively creates a situation where the potential weak points are removed and amplifies the DiD concept. One way this is done is by having the users go through a “Triple A” framework where each user will need to be Authenticated, Authorized, and all Activities monitored.

My recommendation on what to implement is to use more heavily layered DiD while also keeping the system performance balanced. Then using the zero trust framework along with the triple A framework to address all users as an attack only comes from malicious users. Finally adopting an SSDLC rather than a traditional SDLC is also recommended because it addresses issues and vulnerabilities that are typically missed, such as handling end-of-life products and their data, assets, and systems.