CS-405 Module 8: Journal Reflection

Sarah Brady

12/16/2022

**Adoption of a secure coding standard, and not leaving security to the end**

The adoption of a secure coding standard and not leaving security to the end leads to an efficient and more secure system. Writing code with the mindset of security allows you to also work to create a more secure system that will protect data. Eliminate any possibility of vulnerabilities that could be taken advantage of. If leaving this to the end, there is a much higher chance of errors which will lead to huge security risks. Never leave security to the end.

**Evaluation and assessment of risk and cost benefit of mitigation**

Developing while following the pipeline of DevSecOps ensures that secure code will be free of vulnerabilities. Planning and developing code as well as testing, scanning, releasing, logging, penetrative testing, monitoring, responding and recovering will produce a stronger system. Thought the cost may be higher, in the end the reward is greater.

**Zero trust**

Zero trust is a framework that measures and protects users’ information. This include the triple-A framework that consists of authentication, authorization, and accounting.

**Implementation and recommendations of security policies**

Here are my recommendations: Continuing to keep up with current security trends to maintain the proper level of security. Following security standards. Automating. Proper code testing to maintain the line of defense.