Module Eight Journal

Zachary DeRepentigny

Cybersecurity is a vast and complex field that grows and evolves which each passing day. Secure coding is among the most important ways in which companies can improve their security but establishing good standards that address security needs throughout the development process. The learning accomplished throughout the course established that the best practice is to continuously test and improve the security performance of code through a variety of means such as unit testing. By following this process, developers can ensure that, not only are individual components of a program secure, but also that the overall compatibility of components within the program are also secure from attackers.

In a perfect world, companies could implement an infinite number of security measures and policies to ensure the maximum possible safety of their products. Unfortunately, resources are inherently finite due to the cost of implementing these security elements. Because of this, companies need to be able to properly evaluate and assess the risks and costs of mitigation strategies to find what best works for them. There is no one size that fits all of this and each company will come up with different solutions to their security needs based off of the value of their individual assets.

One such example of best practices that may be implemented is Zero Trust. Zero Trust is a series of practices designed to enhance the overall security of assets by improving how vulnerable systems are handled. Implementing security policies can be challenging, as more secure policies often have the downside of higher costs and greater impact on the staffs’ work processes. An example of this may be implementing multiple-factor authentications systems whenever staff log in to applications or systems they use for work. In addition, a policy may also be to limit what applications staff are able to access only to those absolutely required for their role. This may limit their ability to improve their work processes, but otherwise prevents the potential use of compromised applications that would impact assets.