Aaron Shipley

CS 405: Project Reflection

Southern New Hampshire University

Wasim Alim

10/22/2022

Throughout the project, I kept in mind principles that would affect the way I would create my new DevSecOps policy. One of the principles I kept in mind was not to leave security until the end. By keeping security in mind throughout the creation process, I was able to gauge my understanding of security and rank standards according to their remediation cost, prevalence, and probability, while ensuring that I implemented a plan with takeaways based on security throughout for all members.

In terms of the ranking of standards portion of the revised security policy, mitigation and cost were major factors in how standards were ranked. The ranking consisted of their mitigation and remediation cost, prevalence, and probability of encountering the particular standard. One can easily break down the 10 standards listed and see their rankings with these factors in mind. One standard may have a higher prevalence, remediation cost, or probability of encounter, but it does not mean it will be ranked higher than other standards. One must look into the overall scope of the standard and apply all filters to gain proper insight into the ranking of the standard.

As far as the rankings are concerned, I used these factors to build my ranking system. Once the initial top 5 rankings were compiled, ranking the remaining five standards became a little harder. The reason for this is the factors being used were similar or identical in their outcome, so I had to research more in-depth and use judgment to complete the rankings. Pure statistics can aid in the process of creating a new policy, but one must still use experience and judgment as well to create a well-rounded security policy.

The process of zero trust was implemented throughout the new policy. Zero trust takes the walls of security from the traditional location of everything within the company being protected from the outside and moves them to everything outside of the data being untrusted. This policy is applied within the new DevSecOps policy through the use of AAA principles and the principles of encryption. By protecting data from all parties, including employees or others within the organization, the policy will protect the user data stored or transferred at the highest degree. Heavy encryption, such as AES 256 encryption, will be implemented to apply top tier encryption security.