Maya Ellison

6/19/2023

Portfolio Reflection

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

Implementing secure coding standards is following a set of rules and guidelines used to prevent and detect security vulnerabilities. “Don’t leave security until the end” means incorporating and testing security features and vulnerabilities throughout the entire SDLC. Security is most thought of during the production phase, but it is equally as important to include security in the pre-production phase. Examples include testing code early and often and defense in depth (DiD).

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

Benefits of incorporating security now include cost effectiveness, a positive reputation and strong security. Risks of waiting to incorporate security into our software include being susceptible to vulnerabilities and breaches, increased cost and effort, and could lead to a negative reputation if our software is not in compliance with laws and regulations set in place to protect user data. Examples of where security automation can be integrated into our SDLC include use of security architecture in the asses and plan phase, input validation and session management in the design and build phases, continuous testing and white/black box testing in the verify and test phase, automated defect remediation such as StackStorm in the respond phase, use of log scanners in the monitor and detect phase and configuration management in the transition and health check phase.

**Zero trust**

I think of zero trust as a security system that relies heavily on authorization and authentication. Since nowadays people can access companies' networks from almost anywhere in the world, it is important to enforce continuous verification to prove that the user is who they say they are and that they have permission to access the data they are trying to retrieve. Even if a system remembers a user or device, authentication must be used before every new session.

**Implementation and recommendations of security policies**

To implement a security policy awareness and compliance of the policy should be enforced, and any staff member found in violation of said policy will be subject to disciplinary action. The risk management committee or RMC should review the company reports monthly. As a part of the distribution process, employees should certify acceptance and awareness of the policy annually.

**References:**

Raza, M. (2023, March 3). *The 7 devsecops concepts & principles to ace for true devsecops*. Splunk. <https://www.splunk.com/en_us/blog/learn/devsecops-concepts-principles.html>