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

During this course, I learned about secure coding principles. I also learned the importance of not leaving security till the end and how to deal with many code threats. I will use what I learned here to secure any code I write. I will also test the code repeatedly to ensure it is secured and has no errors or bugs. Using automated testing tools can be a good strategy for finding security vulnerabilities and errors. They will also ensure that security is not left till the end.

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

It is essential when I start building a new system or writing a code to asset the risks and the mitigation solutions. In my opinion, knowing the motive for hacking or attacking my system or my code can be the first step to securing it. Knowing the motive will guide me to what security I need in the place and what information I need secure. It will also help determine the cost of security and mitigation. Analyzing the risks and threats is my second step toward protecting my code or system. This step will help with creating the right security policies.

**Zero trust**

Zero trust is a cybersecurity strategy that means no one is trustable when it comes to security, and all steps need to be validated. For example, the IT team in an organization can’t have full access to everybody in the organization. They need to apply the least privilege principle. Applying zero trust means any suspicious behavior needs to be validated and checked. Using network segmentation and multi-factor authentication are examples of zero-trust strategies.

**Implementation and recommendations of security policies**

Before implementing security policies, I need to assess the risks and how to deal with them. I also need to document all security policies and schedule monthly training for employees in the organization. Next, we need to test the employees and check whether they understand the security policies. For example, sending a fake phishing email and seeing who will report it and who will open it. Finally, we need to update the policies regularly and learn from other organizations' mistakes.

Reference

What is a zero trust architecture. (n.d.). Palo Alto Networks. <https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>