Hannah Hendrix

12/21/2024

CS-405

8-2 Journal Reflection

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

* This course has provided me with a deeper understanding of security principles, emphasizing the importance of adopting a secure coding standard from the start. This involves practices like input validation, error handling, and secure API design, ensuring vulnerabilities are addressed during development, reducing risks and minimizing rework.

Evaluation and assessment of risk and cost benefit mitigation

* The evaluation and assessment of risk, combined with a cost-benefit analysis of mitigation strategies, has taught me how to prioritize security measures effectively. For example, identifying high-impact vulnerabilities allows for targeted resource allocation to reduce risk without overburdening the project budget. This balance between security and practicality is vital for sustainable development.

Zero trust

* The Zero Trust model, based on the principle of "never trust, always verify," revolutionizes network security by assuming both internal and external systems can be compromised. It emphasizes continuous authentication, granular access control, and segmentation to limit breaches, aligning with secure coding practices.

Implementation and recommendations of security policies

* Implementing and recommending security policies is crucial for aligning technical measures with organizational goals. Regular audits, incident response plans, and ongoing security training ensure security remains a dynamic part of the organization's culture, reducing risks and fostering team collaboration.