David Hendershot

Ben Battle

CS-405

10/25/2024

**8-2 Journal Portfolio Reflection**

Security needs to be incorporated into development from the beginning because it cannot be added as an afterthought. The implementation of secure coding standards at the beginning of development prevents developers from creating buffer overflows and bad input validation and injection attacks. The implementation of SEI CERT and OWASP standards enables developers to maintain code consistency which simplifies problem resolution before product release.

The process of risk assessment taught me to determine the value of security measures against their implementation costs. All organizations should dedicate their resources to prevent major security breaches because they represent the most critical threats. The additional time required for authentication and encryption and validation implementation leads to better protection that exceeds the implementation expenses.

The zero trust model introduced a new perspective about how organizations should handle access control. The system requires all incoming requests and user authentication because it operates under the assumption that internal resources need verification for safety. The system achieves better security through restricted access when system failures occur.

The development of security policies which teams must follow helps all members understand their data protection responsibilities and incident response duties. The combination of secure coding standards with risk evaluation and zero trust and clear policies creates an entire framework for developing secure and dependable software.