DevSecOps Checklist

A set of common opportunities where best practices can be applied to mitigate risks and vulnerabilities

Checklist Developed by Guardian Project, June 2024

Implement Secure Deployment Practices

Ensure secure deployment practices, such as using encrypted connections, restricting access to sensitive data, and implementing strong authentication mechanisms.

Prioritize Traffic Protection

Implement robust security measures to protect against traffic manipulation and eavesdropping, such as Transport Layer Security (TLS) encryption and intrusion detection systems.

Develop Comprehensive Test Plans

Create comprehensive test plans that cover various scenarios and use automated testing tools to thoroughly evaluate the system's functionality and performance.

Eliminate Hard-Coded Credentials

Implement secure credential management practices, such as using secrets management tools and rotating credentials regularly.

Protect Against Supply Chain Attacks

Implement measures to protect against supply chain attacks, such as verifying the integrity of software updates and using a trusted software repository.

Secure Database Access and Authentication

Implement secure database access controls, such as role-based access control and input validation, and ensure strong authentication mechanisms for authentication services.

Improve Exception Logging

Implement robust exception logging to capture and analyze errors, facilitating proactive problem resolution and enhancing system reliability.

Prioritize Input Sanitization

Implement rigorous input sanitization techniques to prevent malicious inputs from exploiting vulnerabilities and ensure the integrity of the system.

To learn more visit www.holisticaudits.org