

Application Security



PROTECT
SERVICE

Improve corporate risk reduction with strategic security and privacy services.

Is the Application Security Service right for your company?

- Do you know that more than 80% of information security attacks occur at the application level?
- What are you doing to ensure the security of your applications?
- Is security integral to your development process, or “added in” at the end of development?

Overview

Business applications are becoming more complex; the required functionality is increasing as users and partners expect to be able to access information and complete online transactions. Commercial applications are being used in unexpected ways as people push them to keep pace with customer requirements. At the same time, pressure is being put on development staff to promote internally developed applications to production as quickly as possible.

How do you secure these applications in the existing threat environment?

Application security is the result of addressing underlying vulnerabilities during the Software Development Lifecycle (SDLC) - design, development, deployment, maintenance and termination of an application.

DigitalDefence’s application security service, based on the SDLC, aligns the technical aspects of application security to client business requirements, ensuring delivery of cost-effective and meaningful solution.

Benefits of an Application Security Program

- Lowers costs and security risks by addressing potential vulnerabilities earlier in the software development lifecycle
- Prevents application downtime, improves productivity
- Standards-based assessment methodology helps to achieve and maintain compliance with Federal and industry regulations
- Improves user confidence in applications and data security
- Assure key clients, auditors, and management as to your organization’s commitment to security

Application Threats

- Input validation (buffer overflows, SQL injection)
- Authentication / password attacks
- Authorization (elevation of privilege, data tampering)
- Configuration management (insecure admin interfaces)
- Sensitive data
- Session management (interception of data)
- Cryptography (poor security of the cryptokey)
- Parameter manipulation (cookie theft)
- Exception management (information disclosure, denial of service attacks)
- Auditing and logging (attacker destroys audit logs)

Does your development team know how to identify, and mediate, these vulnerabilities?

About Digital Defence

Digital Defence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss

Service Description

Digital Defence's Application Security service is built around the secure development lifecycle (SDLC) model, and includes:

- Review of client policies and procedures
- Architecture and Design review with development staff, management, and business owners to clarify business and security objectives, architecture, and design assumptions
- Management and controls review to ensure that the most effective security practices are integrated into the security lifecycle development process
- Threat modeling, a structured process to identify and document security threats to the application
- Static source code analysis using automated tools and manual inspection
- Penetration testing of the application, the server hosting it, and its interactions with other network and data resources
- Specific assessments for applications such as databases
- Fuzzing analysis, an automated input test designed to push an application beyond designed boundaries to determine if it fails to an unsecured state
- Reverse engineering, or "taking apart" applications to understand their functionality (if required)

Digital Defence also provides developer-focused training in secure software development to ensure developers are aware of common attacks and vulnerabilities, and how to code to reduce corporate risks.

For more information please visit www.digitaldefence.ca



Digital Defence Inc

Toll-Free 866-677-1337 | Tel 905-681-3310
302 - 3310 South Service Road,
Burlington, Ontario L7N 3M6

Disclaimer

© 2010 Digital Defence. All rights reserved.
This document is for informational purposes only.
Digital Defence makes no warranties, express or implied, in this document.