

- + Application Code Review
- + Threat Modeling Service
- + SDL Integration Service
- + Training Services

➤ APPLICATION_SECURITY_SERVICES

IOActive

COMPREHENSIVE COMPUTER SECURITY SERVICES

WWW.IOACTIVE.COM

SECURITY

WHY APPLICATION SECURITY SERVICES?

Secure software is a subset of quality software and reliable software. At IOActive we are committed to helping our clients produce better quality software through our holistic approach of enabling competitive and efficient business through the adoption of secure software programming practices. IOActive was chosen by Microsoft as one of three firms in the world to perform source code security review for the Vista operating system.

While it is impossible to prevent every attack, it is estimated that nearly half of all application security vulnerabilities are completely preventable—if security is considered as a normal part of the development process. Whether you are an IT manager, developer, program manager, CIO, CISO, or CTO, your organization, users, and customers depend on you to protect the privacy and integrity of their information, and to ensure system availability.

Engaging IOActive provides you access to industry-leading software security expertise and an experienced, mature firm that is committed to the success of your project and organization.

8 out of 10 internet security attacks are using port 80/HTTP to compromise system security. (Source - Information Security)

Case History

In response to the largest known compromise of financial data to date, CardSystems Solutions has agreed to settle Federal Trade Commission charges that CardSystems' failure to take appropriate security measures to protect the sensitive information of tens of millions of consumers was an unfair practice that violated federal law. According to the FTC, the security breach resulted in millions of dollars in fraudulent purchases. The settlement will require CardSystems to implement an in-depth information security program and obtain audits by an independent third-party every other year for the next 20 years. Additionally, VISA and American Express notified CardSystems that they will no longer do business with them.

Software Analysis tools are useful but they are no replacement for human beings performing manual code reviews. No tool will replace humans.
Michael Howard / David LeBlanc Writing Secure Code 2nd Edition

Methodology

IOActive delivers customized application security services based on our clients' development process and deployment or product-ship requirements. We believe that through a Security Development Lifecycle (SDL), security considerations and protective measures should be incorporated into all phases of a project, from design review through development, testing, and into deployment. By embedding security measures into the overall development process in this way, organizations can help ensure that software vulnerabilities are detected and addressed before they result in lasting damage. To assist our clients in this process, IOActive offers the following services:

Application Code Review

IOActive manually audits client source code to identify vulnerabilities. We then document the location and nature of each problem we find, and advise developers on how to address the immediate problem, and avoid similar problems in the future. Because software development is evolutionary and iterative, IOActive recommends that the code audit function reflects the structure of the development process and includes audit checkpoints for each of the major product stages: alpha, beta, and release-candidate. In addition to source code review, IOActive examines vulnerable points in design (such as legacy interoperability) for design flaws that may result in a security compromise. IOActive works with client development teams to help them ensure that their products are demonstrably hardened against attack; designed and built based on relevant analysis of risks, threats, and exposures; and appropriately tested to meet their defined security criteria and functionality requirements.

IOActive consultants have years of code auditing experience, and routinely assist organizations with highly complex and advanced application security challenges.

- + Application Code Review
{C/C++, .NET, JEE, Delphi, ASM, Perl}
- + Web Application Code Review
{ASP.NET, C#, JEE, PHP}
- + Black Box Application Pen-Test
- + Product Evaluation and Recommendation {white/black}
- + Reverse Engineering Software and Protocols
- + DRM Testing
- + Fuzz Testing // Application and Protocol
- + M&A due diligence

Threat Modeling Service

IOActive's threat modeling service is designed to occur early in the project lifecycle and can be used to find security design issues before a single line of code is written. Organizations leveraging this service have found that it often leads to significant project cost savings because issues are resolved early in the development lifecycle.

Security Development Lifecycle Integration

IOActive's SDL integration service is designed to help organizations integrate security into all phases of the software development process. Our consultants work alongside an organization's project managers, security architects, and coders to identify efficient methods for integrating security into the overall development process. Covering the complete lifecycle of software development, from conception to deployment, IOActive reviews practices and tasks, providing strategic recommendations for the implementation of a security-focused development lifecycle, and identifying opportunities to increase the effectiveness of risk management for the enterprise.

Training Services

IOActive believes that education is critical to delivering secure software. Our training helps developers understand how to design, build, test, and deploy secure systems. With years of real-world experience, IOActive's instructors craft customized curricula presented in an engaging classroom environment to maximize learning potential.

- + Advanced Asp.Net Exploits and Countermeasures
- + Writing Secure Code: .NET and Java
- + Rapid Application Threat Modeling
- + The Security Development Lifecycle

Statistics

Security investments made in creating secure coding practices will return 12-21% of overall project costs. Security investment made during design phase will yield organizations a 21% ROI. If security is not incorporated until the implementation phase, organizations will benefit from a 15% ROI. If organizations have phased security into their test cycle, 12% ROI of total project costs. - Study conducted by Kevin Soo Hoo MIT, Andrew W. Sudbury, Andrew Jaquith

For more information about our services please contact:

SECURE@IOACTIVE.COM
TOLL FREE (866) 760-0222

About IOActive

Established in 1998, IOActive is a professional services consulting firm specializing in information risk management and application security analysis for global organizations and software development companies.

Unlike commoditized network security services and off-the-shelf code scanning tools, IOActive performs gap analysis on information security policies and protocols, and conducts in-depth analysis of information systems, software architecture and source code by using leading information risk management security frameworks and carefully-focused threat models.

As a home for highly skilled and experienced computer security professionals, IOActive has attracted the likes of Dan Kaminsky, Jason Larsen, Darek Milewski, Ward Spangenberg, and Ted Ipsen; key advisors like Steve Wozniak; and a crew of unequivocally talented "white-hat" hackers who, before being asked to host the infamous Capture the Flag at Def Con, owned the competition three years in a row.

Another data-point reflecting the talent of our consultants is the fact that IOActive is one of only three firms in the world that were tasked by Microsoft with the security code review of the Vista client operating system.

Application Security Services

- + Threat Modeling
- + Application Code Review
{C/C++, .NET, C#, Java, Delphi, ASM, Perl}
- + Web Application Code Review
{ASP.NET, C#, Java, PHP}
- + Black Box Application Pen-Test
- + Product Evaluation {white box/black box}

Infrastructure Audit Services

- + Vulnerability Testing
- + Penetration Testing

Incident Response Services

- + On Call Contracts
- + Network Flow Data Analysis
- + Disk Level Analysis
- + DDoS Mitigation

Advisory & Risk Management Services

- + ERM Development and Implementation
- + ISO 27001 / 17799 Implementation
- + Security, Privacy & IT Audit Co-Sourcing
- + Compliance Assessments
- + PCI Data Security Standard
- + Third-party Due Diligence Reviews

Training Services

- + Advanced Asp.Net Exploits and Countermeasures
- + Writing Secure Code: .NET and Java
- + Rapid Application Threat Modeling
- + The Security Development Lifecycle
- + How to Respond to a Security Breach
- + Security Incident Response Seminar

APPLICATION