

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

California SB 1386 mandates the disclosure of computer breaches which confidential information is disclosed to a former resident. The law covers enterprises, public or private, with California residents. If a breach has occurred, could cause damages, or face class action.

- + Application Security Services
- + Advisory & Risk Management Services
- + Infrastructure Audit Services
- + Incident Response Services
- + Training Services

SECURITY_SERVICES_OVERVIEW
public class Command_private



SECURITY_SERVICES_OVERVIEW

IOActive
COMPREHENSIVE COMPUTER SECURITY SERVICES

WHO WE ARE

IOActive is a talented and experienced group of self-motivated individuals with the desire to advise and support clients in protecting information assets and mission-critical systems by efficiently and effectively mitigating security risks in today's complex and interconnected business environments.

HOW WE CAN HELP

Enterprise security has never been more complicated. The proliferation of legislation designed to protect consumers and organizations places unprecedented pressure on companies to secure their systems and data. However, few companies have the internal expertise or available resources to effectively and consistently manage information risk. Without expert insight, the task of assessing and addressing risk can strain company budgets and staff, and the patience of executives and investors.

IOActive can help organizations manage their risks by:

- + Identifying and inventorying information assets
- + Assessing risks and gaps in compliance requirements
- + Aligning solutions with business processes and objectives
- + Building secure systems
- + Testing controls
- + Drafting policies, standards, and procedures
- + Training people
- + Implementing security technology and repeatable processes
- + Monitoring and measuring the ongoing effectiveness of controls

Are You Compliant?

The legislative landscape relevant to information security continues to rapidly evolve, and poses a challenge for organizations to ensure that their policies, procedures, and standards support compliance. Failure to comply can result in substantial criminal and civil penalties.

Payment Card Industry (PCI)

The Health Insurance Portability and Accountability Act (HIPAA)

Gramm-Leach-Bliley Act (GLBA)

Sarbanes-Oxley Act of 2002 (SOX)

Data Breach Laws

European Union Data Protection Directive (US SafeHarbor)

Federal Trade Commission Act (FTCA)

Canada's Personal Information Protection and Electronic Documents Act

NERC Cyber Security Standards

USAPATRIOT Act of 2001

The Children's Online Privacy Protection Act (COPPA)

The Family Education Rights and Privacy Act (FERPA)

The Federal Information Security Act of 2002 (FISMA)

Notification of Risk to Personal Data Act (NORPDA)

Our Services

IOActive offers a comprehensive suite of information security, assessment, and training services coupled with risk management consultancy services. Together, they give IOActive clients proactive, strategic approaches to managing information and security risks by addressing people, process, and technology across the enterprise.

Application Security

IOActive delivers customized application and code audit services based on each client's software development process. We believe that security awareness and focus should be incorporated in the overall development life-cycle, as a security thread that runs through design, development, testing, and deployment. Embedding security considerations throughout the software development life-cycle creates proactive, methodical, and repeatable processes to detect and address risks and potential vulnerabilities before they become a problem, thereby improving the overall effective and reliable operation of the application. The efficiency of development will also be enhanced since fewer patches and fixes will need to be written after deployment.

- + Threat Modeling
- + Fuzz Testing // Applications, Protocols
- + Application Code Review // C/C++, .NET, C#, Java, ASM
- + Web Application Code Review // ASP.NET, C#, Java, PHP
- + Black Box Application Penetration Tests
- + Product Evaluation {white/black}

Infrastructure Audit

IOActive offers a suite of infrastructure audit services designed to provide an in-depth technical review of an organization's network and technical infrastructure, identifying and evaluating significant risk, and providing recommendations for addressing specific exposures as well as improving overall security.

- + SCADA Testing
- + Network Vulnerability Testing
- + Penetration Testing
- + Wireless Auditing
- + Phone Sweeps
- + VOIP Auditing

Training Services

IOActive brings both customized and general security training to organizations, through instructor-led, hands-on courses that lead students step-by-step through the process of threat modeling, risk and vulnerability assessment, and security implementation.

For more information, please request a training curriculum package.

- + 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

Advisory & Risk Management Services

IOActive's experienced Advisory and Risk Management (ARM) team is passionate about helping organizations implement a control framework with measurable processes and aligning information security with business strategy. By utilizing and recommending proven practices, involving and educating the right people, and understanding and working with appropriate technologies, we are ready to help your organization with offerings such as:

Advisory Services

- + Coaching and Advisement for Executives and the CISO/CSO/CPO
- + Enhancement of the Enterprise Security Program
 - + Alignment of Security and Data Privacy Practices with Business Strategy
 - + Analysis and Remediation of Enterprise-wide Defense in Depth Gaps
 - + Drafting of Policies, Procedures, Standards, and Guidelines
 - + Preparation of a Corporate Information Security Staffing Model
 - + Development of an ISMS

- + Development and Operation of Security Solutions
 - + Selection and Implementation of Technology and Control Processes
 - + IT Security Project Management

Risk Management Services

- + Compliance Assessments
 - + PCI Data Security Standard & Application Best Practices
 - + M&A and Vendor Due Diligence
 - + Regulatory (HIPAA, GLBA, NERC, SOX)
 - + European Union Data Protection Directive
 - + ISO 27001 / 17799
- + Third-Party Assessments (e.g., SAS 70 support)

Incident Response Services

IOActive's Incident Response team supports organizations in the wake of an identified or suspected instance of system compromise, computer misuse, or other information security attack. Through collaborative analysis with our clients, we work to identify the type and source of attack, depth of penetration, length of compromise, and, where appropriate, provide support for criminal prosecution or civil redress.

Reality

In 2006, more than 48 million personal records were exposed according to the Data Loss Archive and Database maintained by attrition.org. Information published by Ponemon states that data breaches have increased by 31% this year and the average cost incurred to disclosing companies is 182 dollars per compromised record. This equates to \$8.7 billion dollars in financial losses for 2006.

For more information about our services please contact:

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

SECURITY_SERVICES