

IOACTIVE SECURITY TRAINING SERVICES

Outsourcing network security services to a reputable consulting firm is only one of many steps an organization can do to protect its information assets. Although many organizations rely on their IT staffs to stay abreast of security threats, it is unrealistic to expect internal IT staffs to be experts across all areas of information security. Most IT organizations are resource challenged, creating an environment of reactive problem solving and crisis response, rather than one that proactively manages and addresses risk by providing appropriate tools and skills to IT staff.

IT staffs trained by IOActive are better equipped to address security issues in a timely and knowledgeable manner.

IOActive offers training across a broad spectrum of security topics that is designed to increase the ability of organizations to proactively assess and manage threats and exposures.

IOActive's industry-recognized consultants can deliver training to our clients onsite or at our training facilities. Our clients should expect a dynamic classroom environment with a hands-on approach to maximize learning opportunities and turn security theory into practical skills that improve employee effectiveness.

You cannot build a secure system until you understand your threats. It's as simple as that. Mike Howard, David LeBlanc
coauthors of Writing Secure Code

Our Approach

Training is an integral part of effectively implementing and supporting organizational security policies, processes, and standards. IOActive brings real-world experience and security expertise to the classroom, offering practical, unbiased, and relevant training services that provide students with an in-depth understanding of complex issues related to security strategy, design, and implementation. Our courses can be tailored to meet the technical sophistication or specific needs of organizations to maximize the relevance and value of training. Our training consists of lectures, workshops, hands-on lab exercises, and technical demonstrations, all designed to provide a solid foundation of knowledge as well as applied skills that are immediately transferable to the workplace.

Advanced ASP.Net Exploits and Countermeasures

In this two-day course, students will push the limits of ASP.NET, and will learn how ASP.NET applications and environments are exploited by skilled attackers. Advanced exploitation techniques will be presented together with low-level technical analysis of the .NET framework. Students will also learn advanced defense techniques such as building an ASP.NET security protection layer (also called a web application firewall), and real-time patching of vulnerabilities in the target application, the .NET framework, or the CLR.

Writing Secure Code: .NET and Java

Security isn't nearly as effective when it is tacked on at the end of a project; it must be part of the development life-cycle from the beginning. These two-day courses focus on Java and .NET developers and are designed to better prepare developers to make security an integral part of their development. Written by industry-leading security researchers, these classes cover security issues and tools specific to the Java and the .NET framework, and better prepare students to do it right the first time. This class has been delivered at BlackHat Vegas.

Advanced Network Pen-Testing

Our Advanced Penetration Testing class is designed to equip students with all the tools and knowledge they need to better run and manage enterprise security testing. This two-day class is delivered by IOActive's industry-leading security professionals and covers everything from understanding an attacker's mindset to exploring the latest tools being used in the underground.

Rapid Application Threat Modeling

Threat modeling is quickly becoming a required process for software development. Threat modeling is a process designed to systematically identify systemic threats to an application architecture. Increasingly, organizations are recognizing the usefulness of effectively modeling the threats to their applications before they are deployed. This two-day class is targeted at software developers and project managers, introducing them to the concepts and methodologies of threat modeling.

Security Incident Response Seminar

This interactive workshop is designed for network managers and security personnel. IOActive's incident response consultants will coach participants through a simulated security incident, guiding them through the development of an effective incident response plan. This class covers legal considerations and requirements for criminal prosecution and civil redress, and the phases of incident response from identification through analysis and notification, containment, eradication, recovery, and reporting.

PCI Compliance Workshop

Any organization dealing with cardholder data must meet the Payment Card Industry Data Security Standards, which govern the secure storage and transmission of cardholder information. In addition to IOActive's PCI Compliance auditing services, we also offer a class covering the detailed requirements and common pitfalls related to achieving PCI compliance. This one-day class is designed for compliance professionals, internal auditors, security managers, and others who are tasked with meeting the PCI standards.

Reality

It is imperative that the people responsible for the prudent custodial stewardship of personally identifiable information and other sensitive data understand their duties relative to privacy, and know how to appropriately use technology and process to help them carry out their duty of protection. From C-level executives to engineering staff, data privacy and information protection are cross-organizational issues that are best understood through training led by instructors with deep industry experience.

For more information about our services please contact:

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

Perspective

"Education is critical to delivering secure systems. Do not expect people to understand how to design, build, test document, and deploy secure systems; they may know how security features work, but that really doesn't help. Security is one area where 'What I don't know won't hurt me' does not apply; what you don't know can have awful consequences" -
Michael Howard /
David LeBlanc

TRAINING SERVICES