



KEY FEATURES:

- Simulate real-world attacks to identify vulnerabilities and threats to applications and products
- Deliver an action plan including prioritized recommendations for mitigating risks to applications
- Provide best practices for relevant security architecture components
- Identify specific areas of security strengths and weaknesses in an application's security architecture
- Inform organizations of where in the application to focus security efforts and development resources to avoid attacks on, or failures within, an application
- Provide in-depth knowledge transfer illustrating specific vulnerabilities identified and best practices for remediation

Now, Evaluate the Security of an Organization's WebSphere Applications Interconnectivity Products!

Evans Resource Group's WebSphere Interconnectivity Penetration Tests evaluate the security of an organization's Software Oriented Architecture (SOA) applications against security best practice criteria. By simulating real-world, message queue and enterprise service bus (ESB) application-level attacks, the tests provide insight into the ability of an organization's application to resist attacks from unauthorized users and to help prevent misuse by valid users.

Evans Resource Group (ERG) has proven methodologies to provide WebSphere interconnectivity application penetration tests to address specific business needs including, but not limited to; testing an organization's existing Web-based applications, payment gateways, and business-to-business application security before the release of new software or a major software upgrade, and testing the security of third-party commercial applications. As part of the testing, ERG application security consultants gather and review available information about the customer's software design, the interaction of the application's components, and security architecture. These tests can be used to validate the effective implementation of role-based access controls; confirm that external users, such as partners and affiliations, are secure; help satisfy the requirements of an organization's formal operational risk management program; and allow organizations to demonstrate due diligence through independent validation.

Testing can be performed onsite, or remotely, via the Internet, depending on the desired approach. Consultants assess a variety of attack vectors including data validation, session management, access controls, use of cryptography, and use of third-party components, among others. After identifying and testing existing security controls, ERG security consultants deliver a written report that provides prioritized remediation guidance for application security vulnerabilities that they have identified and validated as well in-depth knowledge transfer to assist customers in understanding their application security strengths and weaknesses as well as best practices for remediation. The report serves as a roadmap to prioritize application security issues that require immediate and longer-term strategic attention.



KEY BENEFITS:

- Reduce patching efforts by identifying vulnerabilities in applications and products prior to deployment
- Reduce the security risks associated with applications and help demonstrate due diligence
- Incorporated with a suite of services that provide organizations with a programmatic approach to significantly improve their ability to design, develop, test, and maintain the security of applications

About Evans Resource Group

Evans Resource Group is the global leader in WebSphere interconnectivity information security providing a broad range of software, appliances, and services designed to help small- and mid-sized businesses, and large enterprises, secure and manage their WebSphere IT infrastructure. Our MQSentry brand of products is the worldwide leader in WebSphere interconnectivity security and problem-solving solutions. Headquartered in New York, N.Y., Evans Resource Group has operations in more than 10 countries.

For additional information, please visit:

www.evansresourcegroup.com

or, to speak with an Evans Resource Group Security Consulting Services Specialist in the US call toll-free
1 - 888 MSECURE

Types of Penetration Tests

ERG offers various types of Application Penetration Tests, based on business needs, including:

- **WebSphere Web Application Server (WAS) -** Evaluates an organization's application built with web-based server technologies, including frameworks such as J2EE (for example, assessing the organization's e-Store through its web site or its internal human resources systems).
- **WebSphere Message Broker Enterprise Service Bus -** Tests the security of the Message Broker product included as the interconnectivity enterprise service bus embedded in an application or appliance that the organization utilizes to process, transmit or transform card data. The test can be conducted in an informed ("white box") or blind ("black box") scenario. In an informed test, the customer provides Evans Resource Group with access to developers, product documentation, and other resources as necessary, which facilitates greater depth of analysis. Examples of commercial products tested by Evans Resource Group include: mobile phones, wireless handheld devices, networking and security devices, printers, cable boxes, voting applications, mainframe operating systems, wireless cards, online gaming systems, cryptographic accelerators, databases, application servers, and business intelligence and reporting applications.
- **WebSphere Message Queue (WMQ) Client/Server-** Provides an internal test of a client/server message queue application that resides on the organization's network or is shared between the organization and one or more business partners.



Evans Resource Group and the Evans Resource Group logo are U.S. registered trademarks of Evans Resource Group Corporation. Other brands and products are trademarks of their respective holders. Copyright © 2009 Evans Resource Group Corporation. All rights reserved. Printed in the U.S.A. All product information is subject to change without notice.