The Power of AppScan: A Hands-On Review of IBM Rational AppScan Standard Edition

Summary of Findings

In a hands-on look at IBM Rational AppScan Standard Edition (SE), the ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) team finds in the product an easily implemented, highly configurable utility that addresses multiple application security pain points. EMA has long held that application security assessment solutions must include automation, education, and manual testing. Solutions that include these three areas allow organizations to empower their employees to perform comprehensive and efficient application security assessments through automated scans. In addition to this capability, AppScan SE gives organizations the ability to manually test applications. This allows organizations to discover any vulnerabilities that may go undetected by automated scanning technologies as well as reduce false positive findings through manual testing.

In combination with IBM Rational's security services, the IBM Rational AppScan SE solution has strong capabilities in these three essential areas (automation, education, manual testing). The flagship product, AppScan SE, is a highly configurable tool supported by some of the industry's best penetration testing consultants. In addition, AppScan educates users through fix advisories that now include recorded instruction and highlight some of the more common security issues. These capabilities make AppScan SE an excellent choice for development teams, quality assurance testers, penetration testers, mobile security assessment teams, and consultants.

These functional areas support enterprise IT risk and compliance management strategies. Specifically, AppScan SE empowers organizations to conduct proper assessment and remediation of the vulnerability component of risk. This in turn allows organizations to address compliance standards such as the Payment Card Industry Data Security Standard (PCI DSS), Control Objectives for Information and related Technology (COBIT), the Federal Information Security Management Act (FISMA), and the Gramm Leach Bliley Act (GLBA).

From an executive strategy perspective, AppScan SE allows organizations to leverage application assessment technologies in order to work as a business catalyst for cultural change. This change towards integration of security concerns into daily activities comes through a collaborative process implemented by educated employees. Necessary business activities such as system development, maintenance, and quality assurance testing will incorporate a greater consciousness of security through the use of AppScan SE.

AppScan SE is purpose-built to enable security teams to conduct a standalone assessment of the security of Web applications. For this purpose, IBM Rational AppScan SE continues to command a following as an industry leading tool that security teams will find necessary, due to its strong capabilities in automation, education, and manual testing. AppScan SE functions as a desktop solution focused on the individual evaluator. For enterprise security teams seeking to expand their opportunities for collaboration with other groups such as application developers, QA and IT operations, the Rational portfolio of application security solutions includes those that offer a broader range of functionality that supports this level of cooperative processes essential to securing today's enterprise

applications. For these environments IBM Rational offers both an AppScan Enterprise, a solution that can be delivered in a typical or Software as a Service (SaaS) model, and AppScan Reporting Console, a reporting solution geared toward more collaborative efforts. While these solutions address the concerns of security teams, they are not within the scope of this assessment.

As a standalone application security assessment solution, EMA believes IBM Rational AppScan SE is one of the industry's leaders among comprehensive blackbox offerings. In addition to their strong capabilities in automation, education, and manual testing, IBM Rational also boasts future possibilities for collaborative product delivery among IBM's other security-focused business units. In particular, IBM has the possibility of combining AppScan SE with recently acquired Internet Security Systems (ISS) assets such as ISS Security Scanner and ISS RealSecure Intrusion Prevention System to create a single solution for system and application assessment and monitoring capabilities. This of course is in addition to integrating AppScan SE into Rational's industry leading software development platform.

Business Strategy Implications

The goal of all security investments is to address the organization's risk and make the most effective use of limited risk management resources. IBM Rational's AppScan SE addresses what has become an increasingly significant aspect of the vulnerability component of risk, which of course is a key area of IT risk management critical to today's technology-dependent enterprise.

Adding a solution such as AppScan SE to the daily processes and procedures of application development and maintenance is a necessity for addressing organizational risk. Without the proper utilities, organizations will not be able to determine a baseline for risk in their applications without lengthy testing. The result is a lack of focus on integrating security into the early phases of the software development lifecycle. Early integration of application security allows executive staff to place higher emphasis on quality assurance and vulnerability management in their applications in a highly cost effective manner. This translates into a heavier focus on the seamless integration of security into the daily practices of development, quality assurance, and security teams.

This integration is accomplished through the efforts of comprehensive assessments that work as a catalyst for the balance between functionality, security, and quality of production applications. As a result of this balance, organizations will become more capable of delivering quality applications that are not only compliant to regulatory standards such as PCI-DSS, SOX, GLBA, and FISMA, but also far more resilient to attack. These benefits are accomplished through a minor amount of effort and investment into the implementation of application security assessment solution

Contributing Success Factors

Possibly the strongest benefit of selecting AppScan SE is the organization that delivers it. Watchfire, a division of IBM Rational, has a strong understanding of application security. This understanding has led IBM Rational to offer a number of service offerings in parallel to the flagship application security products acquired with Watchfire. These service offerings help organizations conduct highly efficient application assessments that determine as many security issues as possible.

In particular, IBM Rational offers a full computer based training solution that can be purchased in addition to AppScan SE. EMA believes that this particular solution is currently more comprehensive than those offered by other industry leaders. The ability for employees to easily access training material in order to properly conduct application security assessments is a necessity for organizations who are just embarking on, or still building expertise in, their application assessment capabilities.

Conducting proper, comprehensive application assessments represent difficult engagements. Without the proper knowledge and utilities to enable effective processes, application security assessments can be very difficult to complete. By offering free computer based training courses, AppScan SE customers are able to take classes at their own pace as well as access the proper training materials whenever necessary. These additional capabilities allow employees to progress up the learning curve at an expedited pace, creating better efficiency and greater ability to perform necessary application security assessments.

In addition to computer based training and AppScan SE, IBM Rational also offers manual penetration testing services. These services allow customers to ensure the highest level of assessment coverage. Application security assessment today is more an art than a science because it is entirely dependent on the unique characteristics of each individual application. Web applications are often custom designed, and relationships between application components can take on any form. These relationships create an untold number of possible functions that inadvertently create vulnerabilities. Deploying a tool that can be applied generally to *any* application without a true understanding of the intricacies of a *specific* application will frequently produce some level of inaccurate results. For these reasons, there will be a certain level of false positives as well as false negatives in any application security assessment that does not include manual testing. The addition of seasoned penetration testing professionals to IBM Rational's comrehensive offering thus completes the relevant areas of application security assessment: automation, education, and manual testing.

Organizational Fit

The combination of AppScan SE and other IBM Rational solutions is best suited for development teams, quality assurance testers, penetration testers, and consultants.

One of the most frequent complaints about security is the perception—often erroneous, but just as often common—that security tends to interfere with effective or efficient IT operations or other business priorities, in spite of the significant business risk enterprises may face from application vulnerabilities. Security teams attempting to implement more effective security into applications may find themselves as targets for claims of inefficiency, particularly if operational teams are unable to meet remediation goals within a given period of time. This is primarily due to the nature of the relationship between these differing organizations. In order to curb these possible issues, a highly collaborative relationship must be struck between these differing departments. As a desktop solution, AppScan SE does little to cultivate this level of relationship across organizational groups.

These teams will utilize the reports generated by AppScan SE, but their cooperative efforts for remediation will likely require a more collaborative solution. Security teams attempting to leverage application assessment technology as a catalyst for cultural changes within their respective environments may want to consider other application security assessment options such as AppScan Enterprise or AppScan Reporting Console. This of

course is far less of an issue for development teams, quality assurance testers, penetration testers, mobile security assessment teams, and consultants, who are operating either more independently or on a focused engagement where self-contained reporting capabilities of AppScan SE are adequate.

Outlook for IBM Rational's Application Security Offerings

Earlier this year, IBM acquired Watchfire in order to gain Watchfire's service offerings as well as its flagship product, AppScan SE. This came as no surprise to industry analysts as the application security market had become highly promising—and potentially just as volatile. By acquiring Watchfire, IBM not only helps bring stability to the emerging application security landscape, it does so by positioning Watchfire in its Rational division, enabling IBM to deliver a solution for the distinctive integration of security into Rational's industry leading software development platform.

As Watchfire becomes more visible across IBM, one should expect significant collaboration between IBM's Rational and ISS divisions. There are a number of common interests and functions between Wathchfire and ISS that, once combined, could result in an integrated offering currently unrivaled in the security arena. In particular, Watchfire and ISS could leverage both of their industry leading vulnerability research teams to create an integrated solution for system-level and application level vulnerability assessment. For example, once these two areas are combined, this solution could conceivably extend beyond the assessment aspect of security into a more intelligent intrusion prevention system.

This collaboration between the Rational and ISS divisions of IBM is of course in addition to the collaboration that Watchfire will do internally within the Rational organization. Rational will certainly continue to integrate Watchfire solutions into Rational's SDLC solutions to support the adoption of Web application security testing in the development lifecycle.

Put simply, expect big things from Big Blue in these areas in the coming years.

Enterprise Management Associates, Inc.
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: 303.543.9500, Fax: 303.543.7687, Web: www.enterprisemanagement.com

1560.022008