AppScan 的强大功能：点评 IBM Rational AppScan Standard Edition

调查结果摘要

经过对 IBM Rational AppScan Standard Edition (SE) 的审核，Enterprise Management Associates®(EMA™)小组发现，该产品以其易于实施和高度可配置性的特点，解决了诸多应用程序安全难题。长期以来，EMA 认为应用程序安全性评估解决方案必须包含自动化、培训，以及手动测试。包含这三方面功能的解决方案支持组织赋予员工通过自动扫描来执行全面、有效的应用程序安全评估的能力。除了此功能以外，AppScan SE 还使组织能够手动测试应用程序。这样一来，组织可以利用自动扫描技术发现任何可能忽略的漏洞，并通过手动测试减少误报结果。

结合 IBM Rational 的安全服务，IBM Rational AppScan SE 解决方案在这三个重要领域（自动化、培训、手动测试）有着强大的功能。旗舰产品 AppScan SE 是一个高度可配置的工具，获得了行业最优秀的渗透测试顾问的认可。此外，AppScan 通过修复报告培训用户，现在该报告中记载了操作指南，并强调了某些较为常见的安全性问题。这些功能让 AppScan SE 成为了开发团队、质量保证测试人员、渗透测试员、移动安全评估小组和顾问的最佳选择。

这些功能领域支撑着企业 IT 风险和遵从性管理战略。特别是，AppScan SE 准许组织对风险漏洞组件进行正确评估与修复。而这又使组织能够满足许多遵从性标准，比如 Payment Card Industry Data Security Standard (PCI DSS)、Control Objectives for Information and related Technology (COBIT)、Federal Information Security Management Act (FISMA)，以及 Gramm Leach Bliley Act (GLBA)。

从执行战略的角度来看，AppScan SE 让组织能够利用应用程序评估技术，将其作为文化变革的业务催化剂。这项将安全问题整合为日常活动的变革由经过培训的员工实施的协作流程实现。必要的业务活动，例如系统开发、维护和质量保证测试，将通过使用 AppScan SE 吸纳更多的安全意识。

AppScan SE 是专为支持安全性团队执行独立的 Web 应用安全评估而构建。为此，IBM Rational AppScan SE 继续运用业界领先的工具，由于在自动化、培训和手动测试方面的强大功能，该工具被安全团队认为是必不可少的。AppScan SE 是关注于单个评估人员的桌面解决方案。对于试图扩大与其他团队（比如应用开发人员、QA 和 IT 运营人员）协作的企业安全团队来说，Rational 应用安全解决方案产品组合包含功能更为广泛的产品，支持对当今企业应用安全来说较为关键的合作流程。

面对这些环境，IBM Rational 同时提供了两个解决方案，一个是在典型或软件即服务（SaaS）模型中交付的 AppScan Enterprise 解决方案，另一个是可实现更为强大的协作功能的报告解决方案 AppScan Reporting Console。虽然这些解决方案解决安全团队的问题，但它们本身并不处于评估范围之内。

作为独立的应用安全评估解决方案，EMA 认为 IBM Rational AppScan SE 是综合性黑盒产品中的一个行业领先者。除了在自动化、培训和手动测试方面的强大功能之外，IBM Rational 还会展示其他关注安全性的 IBM 业务部门中协作产品交付的未来走势。特别是，IBM 可以将 AppScan SE 与最近收购的 Internet Security Systems (ISS) 资产（例如 ISS Security Scanner 和 ISS RealSecure Intrusion Prevention System）相结合，创建一个适用于系统和应用程序评估和监控的单一解决方案。当然，这将在 AppScan SE 整合入 Rational 的行业领先软件开发平台的基础上进行。

企业战略启示

所有安全性投资的目标都只有一个，那就是应对组织的风险，让有限的风险管理资源得到最充分、最有效的利用。IBM Rational's AppScan SE 解决了风险漏洞组件中越来越重要的问题，这些问题也理所当然成为当今技术依赖型企业中 IT 风险管理的重中之重。

添加 AppScan SE 这样的解决方案到日常流程和应用程序开发和维护的规程中，是解决组织风险问题所必须的。如果没有合适的工具，在不经过漫长的测试的情况下，组织将不可能为应用程序风险确定一个基准。到头来将导致无法集中力量将安全性整合入软件开发生命周期早期。应用程序安全的早期整合有利用行政人员以经济有效的方式高度关注应用程序的质量保证和漏洞管理。这将使员工更加重视将安全性无缝整合到日常开发实践、质量保证和安全团队中。

这一整合是通过综合评估完成的，综合评估是实现生产应用程序的功能、安全性和质量三者之间平衡的催化剂。实现这一平衡以后，组织将更有能力交付不仅遵从 PCI-DSS、SOX、GLBA 和 FISMA 等法规标准、而且对于攻击更富有恢复力的高质应用程序。这些益处都是通过向应用程序安全评估解决方案的实现投入较少的工作量和资金实现的。

成功要素

选择 AppScan SE 最大的获益方可能是交付它的组织。Watchfire 是 IBM Rational 的一个分支，在应用程序安全方面有着透彻的理解力。这一理解力将引领 IBM Rational 开创一系列服务产品，这些产品将能够与收购 Watchfire 时所获得的旗舰应用程序安全产品相媲美。这些服务产品帮助组织执行高效率的应用程序评估，确定尽可能多的安全问题。

尤其是，IBM Rational 提供了一套完整的基于计算机的培训解决方案，可与 AppScan SE 一同购买。EMA 相信这一特别的解决方案目前比由其他行业领先企业提供的解决方案更加全面。员工轻松获得培训材料来正确执行应用程序安全评估的能力，对于刚开始构建应用程序评估能力、或者正在积累这方面经验的组织来说，是十分重要的。

执行正确、全面的应用程序评估意味着参与难度很高。没有正确的知识和工具支持有效的流程，应用程序安全评估将很难完成。AppScan SE 客户享有基于计算机的免费培训课程，可以根据自己的进度参加课程，同时可随时按需获取合适的培训材料。这些额外的功能让员工能够加速完成学习任务、提高效率并增强执行必要应用程序安全评估的能力。

除了基于计算机的培训和 AppScan SE 之外，IBM Rational 还提供了手动渗透测试服务。该服务让用户可以保证评估具有最大程度的覆盖面。今日的应用程序安全评估在更大意义上已经成为一门艺术，而不是科学，因为它完全依靠每一个应用程序的独特性质。Web 应用常常是自定义设计的，应用程序组件之间的关联可通过各种形式呈现。这些关联可能创建大量在无意中生成漏洞的功能。部署可应用于任何应用程序的工具，而无需真正理解一个具体应用程序的运作详情，这将频繁导致一定程度的不准确结果。为此，在没有手动测试的应用程序安全性评估中，将存在一定程度的误报和漏报结果。所以，除了 IBM Rational 的综合产品之外，IBM 还增加了季节性的渗透测试专业人员，从而构成了完整的应用程序安全评估三大相关领域：自动化、培训和手动测试。

组织匹配性

AppScan SE 与其他 IBM Rational 解决方案的结合，最适合开发团队、质量保证测试人员、渗透测试人员和顾问使用。

关于安全性最常见的抱怨是一种常常是错误的、但又十分普遍的观点：安全性经常与有效或高效的 IT 运营或其他的业务优先任务相冲突，尽管企业可能面临着由应用程序漏洞带来的重大业务风险。试图实现更有效的应用程序安全性的安全团队可能发现他们变成无效投诉的众矢之的，特别是当运营团队无法在给定的时间期限内达成修复目标的时候。这主要是由不同组织之间关系的性质决定的。为了遏制这些可能出现的问题，必须在不同的部门之间建立一个高度协作的关系。作为一个桌面解决方案，AppScan SE 对于培育这样一种跨组织关系爱莫能助。

这些团队将使用由 AppScan SE 生成的报告，但是他们之间的协作则很可能要求一个更具协作性的解决方案。试图将应用程序评估技术作为相关环境中的文化变革催化剂使用的安全团队，可以考虑 AppScan Enterprise 或 AppScan Reporting Console 等其他应用程序安全评估解决方案。

当然，这远不是开发团队、质量保证测试人员、渗透测试人员、移动安全评估团队和顾问的问题，这些人要么是更加独立地工作，要么有重点地使用 AppScan SE 自带的报告功能执行相应任务。

IBM Rational 应用程序安全性产品展望

今年年初，IBM 收购了 Watchfire，目的是获得 Watchfire 的服务产品及其旗舰产品 AppScan SE。对于行业分析师来说，这并不足为怪，因为应用程序安全市场已经变得很有发展前景——也可能蕴藏变化。IBM 不仅仅通过收购 Watchfire 给新兴的应用程序安全前景带来了稳定性，还通过将 Watchfire 部署到它的 Rational 软件分支中实现了这一点，使得 IBM 能够交付一个将安全性整合到 Rational 行业领先软件开发平台中的与众不同的解决方案

随着 Watchfire 越来越多地出现在 IBM 产品中，在 IBM Ratioanl 和 ISS 软件分支之间有望实现强强联合。Wathchfire 与 ISS 之间拥有许多共同兴趣和功能，一旦结合，将打造出在安全性领域中无与伦比的整合产品。特别是，Watchfire 和 ISS 可以利用双方各自业界领先的漏洞搜索团队，打造出一个用于系统级和应用程序级漏洞评估的整合解决方案。例如，一旦这两个领域结合在一起，可以预见，这个解决方案将超越安全评估的领域，成为一个更加智能的入侵防御系统。

IBM Rational 与 ISS 分支的协作自然是在 Watchfire 在 Rational 组织内部的协作基础上进行的。Rational 必然会继续整合 Watchfire 解决方案到 Rational 的 SDLC 解决方案中，以支持 Web 应用程序安全性测试在开发生命周期中的应用。

总之，未来几年内蓝色巨人（Big Blue）还会做出许多大事，让我们拭目以待。

Enterprise Management Associates 公司 1560.022008
5777 Central Avenue, Suite 105
Boulder, CO 80301
电话： 303.543.9500 传真：303.543.7687 网址： www.enterprisemanagement.com