



Rational software

IBM Rational AppScan Source Edition

특장점

- 소스 코드 내의 취약성을 파악하고 데이터 흐름을 검토하여 각 애플리케이션의 위험 노출을 파악할 수 있습니다.
- 정적 코드(static code)를 개발 주기의 초기에 스캔할 수 있어 이미 사용 중인 애플리케이션을 검토하거나 아웃소싱한 애플리케이션이나 컴포넌트의 품질 검사를 수행할 수 있습니다.
- 이미 사용하고 있는 애플리케이션 개발 및 보안 애플리케이션들을 통합하여 기존의 자산을 활용할 수 있습니다.
- 전사적으로 적용할 수 있는 일관된 정책을 수립하고 채택하여 시행할 수 있습니다.

상호연결, 기능화, 지능화된 제품들이 시장에 넘쳐나고 있습니다. 기계 및 전자 부품과 함께 임베디드 소프트웨어로 이루어진 이 똑똑한 제품들은 상당 수의 데이터를 생성해내고 있습니다. 그 결과, 이러한 제품들을 작동시키고 그 정보를 처리하는 소프트웨어에 대한 의존성이 높아지게 되었습니다.

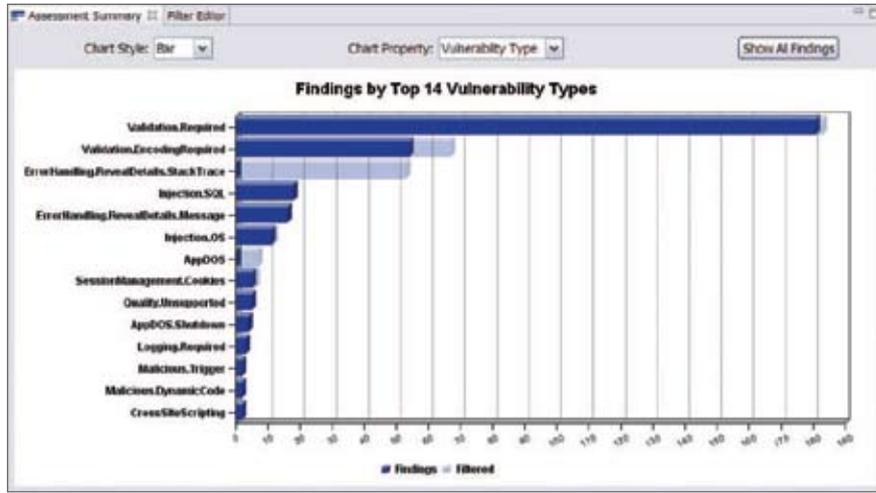
시장에서 기회를 포착하길 바라면서, 기업들은 점점 더 빠른 속도로 이러한 똑똑한 제품들을 개발하고 있습니다. 그러나 선두를 차지하기 위한 경쟁에서 다수 기업들이 애플리케이션 보안과 그 우선순위에는 많은 주의를 기울이지 않고 있습니다.

유감스럽게도, 이런 사안들은 기업이 자사의 시스템, 애플리케이션, 개인 정보 데이터와 고객 정보에 적절한 조치를 취하지 않는다면 회사의 손익과 브랜드에 치명적인 결과를 가져올 수 있다는 한 가지 사실을 명확하게 보여주고 있습니다.

그 결과는 막대한 과징금 부과와 수익 손실에서 시스템 가동 중지에도 이르면, 고객 신뢰를 잃게되고 회사의 평판을 해치게 됩니다. 그러한 위험을 무릅쓸 수 있는 기업이 있을까요? 대부분이 그렇지 않을 것입니다. 완벽한 보안 전략을 갖추는 것이 매우 중요한 이유가 바로 그 때문입니다.

소스 코드 내의 취약성 파악

IBM Rational® AppScan® Source Edition 소프트웨어*는 소스 코드 내의 취약성을 파악하고, 데이터 흐름을 검토하여 각 애플리케이션의 위험 노출을 파악할 수 있는 정적 분석 보안 테스트 애플리케이션입니다. Rational AppScan Source Edition 소프트웨어를 개발 단계에 사용하면 감사 및 규제준수를 위하여 소프트웨어 개발 수명주기(SDLC) 전반에 걸쳐 실행 수준에서 위험 노출을 한층 쉽게 파악할 수 있습니다. 또한 Rational AppScan Source Edition 소프트웨어는 필요할 때 필요로 하는 정보를 개발팀과 보안 팀에 제공함으로써, 두 팀 간의 협력을 촉진할 수 있습니다.



Rational AppScan Source Edition 소프트웨어는 애플리케이션에 영향을 미치는 취약성에 대한 통찰력을 부여하는 평가 요약を提供합니다.

SDLC의 초기에 취약성을 저감

Rational AppScan Source Edition 소프트웨어는 소스 코드 분석에 대한 포괄적인 접근법을 제공하고 시간 당 1백 만 행 이상에 달하는 고속 코드 스캔을 제공하여 가장 복잡한 엔터프라이즈 애플리케이션도 스캔할 수 있습니다. 또한, 취약 코드 행에 이르기까지 조치 가능하며 우선순위가 부여된 정보를 제공합니다.

이로써, 애플리케이션을 이용하여 개발 주기의 초기에 취약 코드를 발견하여 조치하고 이미 사용하고 있는 애플리케이션을 검토하거나 개발을 위해 아웃소싱한 애플리케이션이나 컴포넌트에 대한 품질 검사를 수행할 수 있습니다. 일례로, 아웃소싱 계약에 보안 요구사항을 포함시키고 Rational AppScan Source Edition 소프트웨어를 이용하여 허용 기준을 만족하는지를 확인할 수 있습니다.

Rational AppScan Source Edition 소프트웨어는 애플리케이션의 취약성을 발견하여 제거하는데 필요한 보고 카드(report card), 상세한 매트릭스와 교정 방법에 대한 조언을 제공합니다. 단지 버퍼 오버플로우나 SQL(Structured Query Language) Injection (주입) 문제만을 파악하는 것만으로는 애플리케이션의 보안을 확보할 수 없으며 액세스 제어, 인증 및 암호화와 같은 여타 보안 메커니즘을 부적절하게 실행하면 조직에 더욱 더 큰 위험을 초래할 수 있습니다.

첨단 소스 코드 분석 기술을 이용하여 가장 치명적인 취약성에 대한 조치를 취하세요.

Rational AppScan Source Edition의 소스 코드 테스트 기능을 Rational AppScan 포트폴리오의 여타 솔루션 (제공물)이 제공하는 웹 애플리케이션 보안 스캐닝 영역과 결합시키면 애플리케이션의 취약성을 다루기 위한 가장 포괄적인 커버리지를 확보 할 수 있습니다.(하는데 유용합니다.) 또한, IBM Rational AppScan Reporting Console 이나 IBM Rational AppScan Enterprise Edition 소프트웨어로 정적 및 동적 분석 결과의 통합 보고서를 얻을 수 있습니다.

기존 투자 보호

Rational AppScan Source Edition 소프트웨어는 공개된 아키텍처 상에 구축되어 있으므로 늘 하던 방식대로 작업을 계속할 수 있습니다. 이미 보유하고 있는 애플리케이션과 쉽게 통합하여 기존 엔터프라이즈 SDLC 도구와 보안 인프라스트럭처의 투자를 보호할 수 있습니다. 소프트웨어는 다음과 통합할 수 있습니다:

- **DTS (Defect tracking system)**

Rational AppScan Source Edition 소프트웨어는 DTS 통합 프레임워크를 제공하여, 그 결과물을 기존 DTS와 원활하게 통합할 수 있습니다. 이 프레임워크는 기존 우선순위 및 심각도 목록과 기존 워크플로를 이용하여, 기존 프로세스와 관련된 Rational AppScan Source Edition 이슈를 처리할 수 있도록 합니다.

- **소프트웨어 형상관리 (SCM:Software configuration management) 및 빌드(build) 관리 도구**

Rational AppScan Source Edition for Automation 서버는 IBM Rational Build Forge® CruiseControl, Apache Continuum 및 Microsoft® MSBuild 소프트웨어를 포함한 광범위한 빌드 애플리케이션을 다룰 수 있습니다.

- **동적 분석 도구와 웹 애플리케이션 방화벽**

Rational AppScan Source Edition 소프트웨어에는 평가 데이터베이스에 대한 공개 API가 포함되어 있어 다른 보안 시스템과의 통합을 위해 데이터를 가공(조작 처리)할 수 있습니다. 침투 테스트의 결과를 상관시켜 문제가 생긴 코드를 집어낼 수 있으며 (코드 행의 문제를 정확하게 파악하기 위한 침투 테스트의 데이터를 상관시켜) 악용될 소지가 있는(익스플로잇(exploit)의) 소스를 파악할 수 있습니다. Rational AppScan Source Edition 스캔 결과를 이용하면 취약성 보안 작업을 하면서 자산을 보호할 방화벽을 보다 잘 동조시킬 수 있습니다.

자동화를 이용한 효율성 개선

소프트웨어 애플리케이션을 수동으로 테스트하면 배포가 지연되거나 모순된 테스트 결과를 낼 수 있습니다. 자동화 솔루션은 소프트웨어를 보다 철저하고 신속하게 테스트하면서, 테스터들이 보다 고부가가치를 창출할 수 있는 작업에 더 많은 시간을 할애할 수 있도록 합니다.

또한, Rational AppScan Source Edition 소프트웨어는 데이터를 위태롭게 하는 설계 결함과 코딩 오류를 제거해야 할 결과에 우선순위를 부여합니다. 애플리케이션을 간편하게 설치하고 구성할 수 있으므로 신속하게 실행하여 기존 프로세스에 최소한의 영향으로 워크플로우를 자동화할 수 있습니다.

통합형 정책, 프로세스 및 보고로 일관성을 촉진

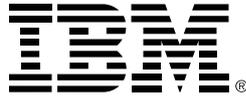
Rational AppScan Source Edition 소프트웨어는 전사적으로 적용할 수 있는 일관된 정책을 수립하고 채택하여 시행할 수 있도록 합니다. 또한, 통합형 정책 및 평가 데이터베이스로 전사적인 매트릭스와 보고를 제공합니다. 한 세트의 정책과 한 세트의 데이터를 이용함으로써, 보다 일관성 있고 효율적이며 효과적인 엔터프라이즈 테스트 플랫폼을 구현할 수 있습니다. 평가 결과는 보고서(복사) 및 교정 정보와 함께 통합 저장되므로, 팀들은 대시보드를 통해 접근할 (이용할) 수 있습니다. 이해관계자들도 Rational AppScan Source Edition 온라인 포트폴리오를 통하여 프로젝트 진척도를 모니터링 할 수 있습니다. 맞춤형 규제 준수 결과와 교정 목록을 공지하여 파트너와 공급업체를 포함하는 외부 팀들에게도 진행상황을 알려줄 수 있습니다.

포괄적이며 확장 가능한 테스트 기능을 제공

Rational AppScan Source Edition 소프트웨어는 광범위한 언어에 대하여 최대 규모의 가장 복잡한 애플리케이션들의 포괄적인 포트폴리오를 수용할 수 있는 특허 설계에 기반하고 있습니다. 또한, 광범위한 보안 취약성을 파악하여 데이터를 위태롭게 하는 코딩 결함과 설계 오류를 정확하게 찾아낼 수 있습니다. 그 심층적인 모듈간(cross-modular) 분석은 가장 치명적인 보안 결함을 바로 겨냥하는 취약성을 잡아낼 수 있습니다.

분석, 보고 및 워크플로우의 커스터마이징

Rational AppScan Source Edition 소프트웨어를 이용하면 보안 정책과 치명적인 보안 문제에 적합하도록 분석을 구성하여 커스터마이징 할 수 있습니다. 조직 특유의 취약성을 추가하고 기존 취약성의 심각도를 조정하여 가장 치명적인 것들의 우선순위를 조정할 수 있습니다. Rational AppScan Source Edition 소프트웨어는 유연한 맞춤형 보고를 제공하여 교정, 규제 준수 및 리스크 관리를 위해 정보를 선택하고 그룹화하며 기술하는 방법을 결정할 수 있습니다. 또한 이 애플리케이션은 유연한 분류체계(triage)와 교정 구성을 제공하므로 조직에 가장 적합한 워크플로우를 이용하여 보안팀과 개발팀 간의 정보 흐름을 자동화할 수 있습니다.



© Copyright IBM Corporation 2010

제작자: 대한민국

2010년 3월

All Rights Reserved

IBM, IBM 로고, ibm.com Rational 및 AppScan은 미국 및/또는 다른 국가에서 IBM Corporation의 상표 또는 등록 상표입니다. 상기 및 기타 IBM 상표로 등록된 용어가 본 문서에 처음 나올 때 상표 기호(® 또는 TM)와 함께 표시되었을 경우, 이러한 기호는 본 문서가 출판된 시점에 IBM이 소유한 미국 등록 상표이거나 관습법에 의해 인정되는 상표임을 나타냅니다. 해당 상표는 미국 외의 다른 국가에서도 등록 상표이거나 관습법적인 상표일 수 있습니다. IBM의 최신 상표 목록은 ibm.com/legal/copytrade.shtml 웹 페이지의 "저작권 및 상표 정보" 부분에서 확인할 수 있습니다.

Microsoft는 미국 및/또는 다른 국가에서 Microsoft Corporation의 상표입니다.

기타 국가, 제품 또는 서비스 이름은 다른 기업의 상표 또는 서비스 마크일 수 있습니다.

이 문서에 IBM 제품 또는 서비스가 언급되어 있는 경우에도 IBM이 비즈니스를 진행하고 있는 모든 국가에서 사용할 수 있음을 의도한 것은 아닙니다.

본 문서에 수록된 내용은 정보 용도로만 제공됩니다. 본 문서에 수록된 정보가 완전하고 정확한 지를 확인하기 위해 많은 노력이 기울여졌지만, 수록된 정보는 어떠한 명시적이거나 암묵적인 보장 없이 "있는 그대로" 제공됩니다. 또한, 이러한 내용은 IBM의 현재 제품 계획 및 전략에 기초한 것으로 사전 예고 없이 변경될 수 있습니다. IBM은 본 문서 또는 기타 문서의 사용에 기인하거나 그와 관련하여 발생하는 어떠한 피해에 대해서도 책임을 지지 않습니다. 본 문서 또는 기타 문서에 수록된 어떠한 내용도 IBM(또는 IBM의 공급업체 및 공식 협력업체)의 보증 또는 약속을 발생시키거나 IBM 소프트웨어 사용에 적용되는 해당 라이선스 계약의 조건 및 규정을 변경할 의도로 작성되지 않았으며, 그러한 효력을 가질 수 없습니다.

IBM 고객은 법적인 요구 사항을 준수할 책임이 있습니다. 고객의 비즈니스에 영향을 미칠 수 있는 관련 법규 및 규제 사항 그리고 해당 법규나 규제 사항을 준수하기 위해서 고객이 취해야 하는 행위에 대한 식별과 해석에 대해서 능력 있는 법조인의 조언을 구하는 것은 전적으로 고객의 책임입니다. IBM은 법적 자문을 제공하지 않으며, IBM의 서비스 또는 제품을 통해 고객이 해당 법률을 준수할 수 있다는 보증이나 표현을 일체 하지 않습니다.

* Ounce Labs의 이전 Ounce 6 소프트웨어.

조직 대부분의 모든 팀에게 혜택을 제공

Rational AppScan Source Edition 소프트웨어는 다음을 포함하여 조직 내의 모든 보안 이해관계자들을 지원하는 컴포넌트와 함께 뛰어난 혜택을 제공하도록 고안되어 있습니다:

- *Rational AppScan Source Edition for Core*-보안 지식 기반 및 다중 애플리케이션 평가 데이터베이스
- *Rational AppScan Source Edition for Security*-보안 정책을 관리하고 우선순위 취약성을 구성하며 스캔하여 조치를 취할 수 있는 워크벤치
- *Rational AppScan Source Edition for Automation*-스캐닝, 퍼블리싱 및 보고를 빌드 환경에 원활하게 통합시키는 서버 컴포넌트
- *Rational AppScan Source Edition for Developer*-소스 코드를 스캔하여 코드 행의 치명적인 취약성을 파악하여 조치할 수 있는 IDE(integrated development environment) 모듈
- *Rational AppScan Source Edition for Remediation*-코드 행의 치명적인 취약성을 처리하고 조치할 수 있는 IDE 모듈

추가 정보

IBM Rational AppScan Source Edition 소프트웨어에 대하여 자세히 알아보시려면, 해당 IBM 대리점 또는 IBM Business Partner에게 연락 하시거나, 다음 웹사이트를 방문하세요:

ibm.com/software/rational/products/appscan/source