IBM Security AppScan Source

정적 애플리케이션 보안 테스트를 통한
애플리케이션 보호 및 보안 소프트웨어 구축

주요 특징

- 소스 코드의 취약점을 파악하고, 데이터 및 호출 흐름을 검토하며, 모든 애플리케이션의 위협 노출을 확인합니다
- 개발 주기에서 초기에 소스 코드를 스캔하여 개발팀의 보안 테스트 채택이 간소화됩니다
- 보안 테스트가 애플리케이션 개발 도구 및 IBM Rational® Collaborative Lifecycle Management 솔루션과 통합됩니다
- 일관된 정책을 수립하여 전사적으로 추진하고 시행할 수 있습니다

오늘날의 경제는 상호 연결된 지능형 시스템에 의존하고 있으며, 이 시스템은 맞춤형 소프트웨어와 웹 애플리케이션을 사용합니다. 이러한 제품과 애플리케이션은 방대한 양의 데이터를 생성하기도 하고, 데이터와 상호작용하기도 합니다. 기업들은 시장에서 기회를 선점하기 위해 똑똑한 제품과 애플리케이션을 더 신속하게 개발하고 있습니다. 하지만 시장을 선점하기 위한 경쟁에서 다수의 기업들은 애플리케이션 보안에 주의를 기울이지 않거나 우선순위를 높게 두지 않고 있습니다.

한 가지 분명한 점은 기업이 시스템, 애플리케이션, 기밀 데이터, 고객 정보를 보호하기 위한 적절한 조치를 취하지 않을 경우 자사의 수익과 브랜드에 엄청난 손실이 초래될 수 있다는 점입니다. 금전적인 손해와 매출 손실에서 고객의 신뢰를 떨어뜨리고 기업의 평판을 헤치는 시스템 가동 중단에 이르기까지, 손실의 범위는 다양합니다. 하지만, 다수의 기업은 이러한 위기를 극복할 역량을 갖추고 있지 않습니다. 여기서 포괄적인 애플리케이션 보안 전략의 중요성이 대두됩니다.

소스 코드의 취약점 파악

IBM Security AppScan® 포트폴리오의 애플리케이션 보안 테스트 및 위험 관리 솔루션은 다양한 애플리케이션 위험을 해결하도록 설계되어 있습니다. 이 포트폴리오의 핵심 구성요소 중의 하나인 IBM Security AppScan Source는 소스 코드의 취약점 파악, 데이터 및 호출 흐름의 검토, 애플리케이션의 위협 노출 확인에 유용한 정적(Static) 애플리케이션 보안 테스트 솔루션입니다.

소프트웨어 개발 수명주기 전반에 걸쳐 배치되는 IBM Security AppScan Source는 감사 및 컴플라이언스에 대비한 위협 노출의 파악을 한층 용이하게 합니다. 또한, 필요한 정보를 적시에 제공함으로써 개발 및 보안 팀 간의 협력 촉진에도 도움이 됩니다.

개발 수명주기의 초기 단계에 취약점 절감

IBM Security AppScan Source 소프트웨어는 소스 코드 분석에 대한 포괄적인 접근방식을 제공합니다. 시간 당 1백만 행 이상의 코드를 고속 스캔하도록 설계되어 있으므로, 복잡한 엔터프라이즈 애플리케이션도 스캔할 수 있습니다. 아울러, 취약 코드 행에 대해서도 우선순위가 부여된 유용한 정보를 제공합니다. 이는 취약 코드를 개발 주기의 조기에 발견하여 조치하고, 이미 사용중인 애플리케이션을 검토하며, 외주 개발 애플리케이션 또는 컴포넌트의 보안 및 품질을 확인하는 데 유용합니다. 일례로, 외주 계약에 대한 보안 요구사항을 규정할 수 있으며, IBM Security AppScan Source를 이용하여 수락 기준을 충족하는지도 확인할 수 있습니다.

즉시 사용할 수 있는 IBM Security AppScan Source는 보고 카드, 상세 메트릭과 애플리케이션의 취약점을 발견하여 제거하는 데 필요한 조치를 제시합니다. 그러나, 버퍼 오버플로우나 SQL(Structured Query Language) 인젝션을 파악하는 것만으로는 애플리케이션의 보안을 유지할 수 없습니다. 액세스 제어, 인증, 암호화 등의 보안 메커니즘을 부적절하게 구현할 경우, 기업에 큰 위험이 초래될 수 있습니다.

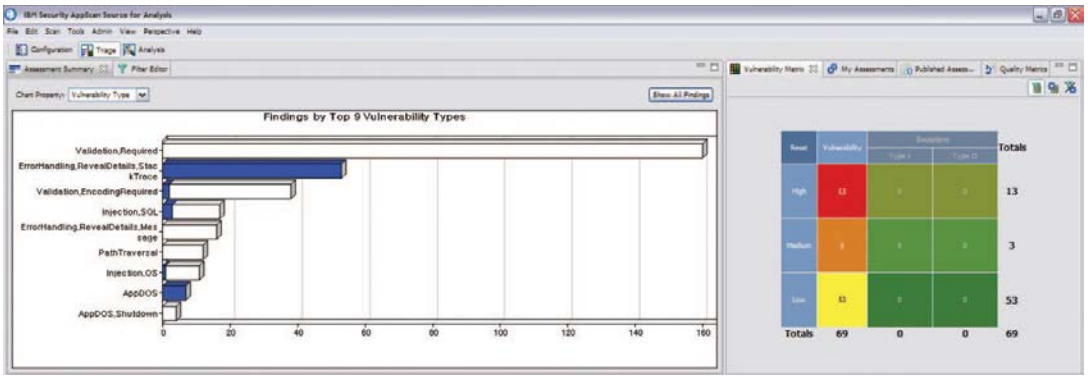

그림 1: IBM Security AppScan Source 소프트웨어는 애플리케이션 위험을 자세히 설명한 평가 요약을 제공하며 애플리케이션에 영향을 미치는 취약점에 대한 통찰력을 제공합니다.

IBM Security AppScan Source를 Rational Collaborative Lifecycle Management 솔루션과 통합하면 대부분의 치명적인 취약점에 조치를 할 수 있으며, 다음이 가능해집니다.

- 테스트 계획 및 실행에 대한 동적 프로세스 및 활동 기반 워크플로우를 이용하여 비즈니스, 개발, 테스트 팀 간의 협업이 이루어질 수 있습니다
- 노동 집약적인 보안 테스트 및 감사를 자동화하여 조기에 보안 문제를 파악하고, 출시시간을 단축하며, 프로젝트 비용을 절감하고 비즈니스 위험을 완화할 수 있습니다
- 개발자 및 품질 전문가와 같은 비보안 전문가들이 보안 테스트를 실시하고, 취약점을 파악하여 코드를 수정할 수 있습니다
- 개개인과 팀에 적합하게 우선순위가 부여된 메트릭을 보고하여 가시성 제고를 촉진하며 의사결정권자들이 소신 있는 결정을 내리고 컴플라이언스를 문서화할 수 있습니다
- 성공적인 배치 패턴을 운영 핵심성과지표(KPI)에 연계시켜 예측 가능성을 제고할 수 있습니다

자동화된 보안 테스트의 사용으로 효율 향상

소프트웨어 애플리케이션의 수동 테스트는 릴리스 지연이나 일관성 없는 테스트 결과를 유발할 수 있습니다. 자동화된 솔루션은 더 철저하고 신속한 소프트웨어 테스트에 도움이 될 뿐만 아니라, 테스트 담당자들이 가치 창출 업무에 더 많은 시간을 할애할 수 있는 여유를 제공합니다. 또한, IBM Security AppScan Source는 데이터를 위험에 처하게 할 수 있는 코드 오류와 설계 결함의 제거에 우선순위를 부여합니다. 애플리케이션의 설치 및 구성이 용이하므로, 신속하게 구축하여 기존 프로세스의 중단 없이 워크플로우를 자동화할 수 있습니다.

IBM Security AppScan Source는 취약점의 발견과 우선순위 부여를 용이하게 합니다. Application Discovery Assistant와 같은 특수 기능은 오랜 시간이 소요되는 구성 단계를 자동화하면서 더 정확하고 철저한 종속성 분석을 제공합니다. 보안 전문가들은 애플리케이션의 구성이 아니라, 애플리케이션의 보안에 더 많은 시간을 할애할 수 있습니다. 유연하며 사용자 정의할 수 있는 스캔 구성은 분석 시간 단축에 도움이 되며, 기업이 자사에 가장 중요한 업무에 주력할 수 있게 합니다.

집중화된 정책, 프로세스, 보고를 통한 일관성 촉진

IBM Security AppScan Source는 전사적으로 적용할 수 있는 일관된 정책을 수립, 추진하고 시행하는 데 도움이 됩니다. 보안 분석가들은 IBM Security AppScan Source for Analysis 클라이언트를 이용하여 모든 정적 테스트를 관리하고, 고급 소스 코드 스캔을 실행하며, 빌드 시스템에서나 개발자들이 자신의 통합 개발 환경(IDE)에서 시행 가능한 테스트 정책을 수립할 수 있으며, 이는 전세계적으로 공유될 수 있습니다. IBM Security AppScan Source for Automation 소프트웨어는 IBM Rational Build Forge® 소프트웨어, CruiseControl, Apache Continuum and Maven, Microsoft MSBuild 소프트웨어와 같은 다양한 빌드 애플리케이션과 연동하며, 빌드 시스템에 대하여 신규 코드를 검사할 때 소스 코드 스캔을 자동으로 트리거합니다.

개발자는 IBM Security AppScan Source를 이용하여 코드를 스캔하고, 취약점을 수정하며, 자신의 IDE에 할당된 작업 항목을 해결할 수 있습니다. 자신의 코드를 스캔하는 개발자들을 위해, IBM은 IBM Security AppScan Source for Development 소프트웨어를 IDE 모듈 또는 플러그인으로 제공하고 있습니다. 빌드 시스템에서 실행된 스캔 결과를 간단히 분석하여 보안 분석가가 할당한 문제를 해결하려는 개발자들을 위해, IBM Security AppScan Source for Remediation 소프트웨어는 스캐닝 기능이 없는 IDE 모듈을 제공합니다. 두 IDE 옵션 모두 결함에 관한 상세한 설명과 권장 코드 수정 방안을 제시하여 취약점을 해결해 줍니다.

모든 테스트 결과는 IBM Security AppScan Enterprise Server에서 집중식으로 관리됩니다. 이 서버는 애플리케이션 보안 테스트 및 위험 관리를 위한 중앙 플랫폼을 제공합니다. IBM Security AppScan Enterprise Server는 다음을 구현합니다.

- 동적 테스트와 정적 테스트를 결합합니다
- 하이브리드 분석을 위해 결과를 연계합니다
- KPI를 포함한 경영진 레벨의 대시보드를 제공합니다
- Rational Collaborative Lifecycle Management 스위트를 통합합니다
- PCI DSS(Payment Card Industry Data Security Standard), HIPAA(Health Insurance Portability and Accountability Act), EU 데이터 보호 지침, Security Control Standard(ISO 27001) 등의 규제에 대한 40여 가지의 컴플라이언스 보고서를 바로 사용할 수 있습니다
- IBM Security Network Intrusion Prevention System, IBM Proventia® Management SiteProtector™, IBM Security Server Protection 솔루션과 통합하여, IBM Security AppScan 소프트웨어가 확인한 취약점을 노린 공격을 차단할 수 있습니다

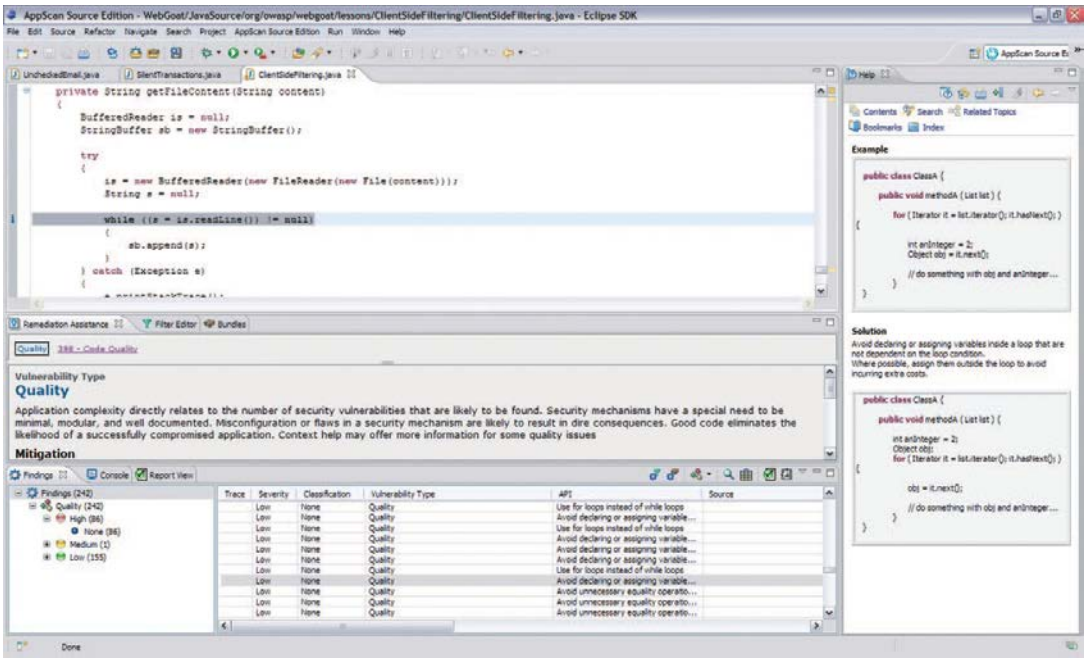

그림 2. IBM Security AppScan Source 소프트웨어에는 IDE를 스캔하거나 결함에 대한 상세내역, 위험에 관한 설명, 결함 수정 방법에 관한 권고를 이용하여 IDE의 결과를 간단히 평가하는 다양한 옵션이 포함되어 있습니다.

포괄적인 확장성 테스트 기능을 제공합니다

IBM Security AppScan Source는 다양한 언어를 사용하며 규모가 크고 복잡한, 포괄적인 애플리케이션 포트폴리오를 수용할 수 있는 특허 설계에 기반을 두고 있습니다. 아울러, 광범위한 보안 취약점을 파악하여 데이터 및 운영을 위험에 처하게 하는 코드 결함과 설계 오류를 정확하게 찾아냅니다. 심층 분석 기능은 확인된 취약점을 가장 치명적인 보안 결함으로 분류하여 즉시 격리시킬 수 있습니다. 물론 보안 결함을 파악하기 위해서는, 분석 소프트웨어가 다양한 언어 및 애플리케이션 프레임워크에 대한 테스트를 수행할 수 있어야 합니다. IBM Security AppScan Source 소프트웨어 고유의 확장 가능한 웹 애플리케이션 프레임워크는 상용, 오픈 소스 및 사내 개발, 주문 개발 웹 애플리케이션 프레임워크의 데이터 플로우 분석에 대한 가시성을 제고합니다.

분석, 보고, 워크플로우를 사용자 정의할 수 있습니다

IBM Security AppScan Source를 이용하면, 고객이 자사의 정책과 중요한 보안 문제에 적합하도록 분석을 정의할 수 있습니다. 기존 취약점의 심각도를 조정하고 가장 치명적인 취약점에 대한 우선순위를 조정할 수 있는 유연성을 갖추게 됩니다. IBM Security AppScan Source는 정보를 선정하여, 그룹화하고 조치방안, 컴플라이언스, 위험 관리 보고를 제시하는 방법을 사용자가 결정할 수 있는 사용자 정의 보고를 제공합니다. 또한, 고객이 자사에 가장 적합한 워크플로우를 이용하여 보안 팀과 개발 팀 간의 정보 흐름을 자동화할 수 있도록, 유연한 선별 및 수정 구성을 제공합니다.

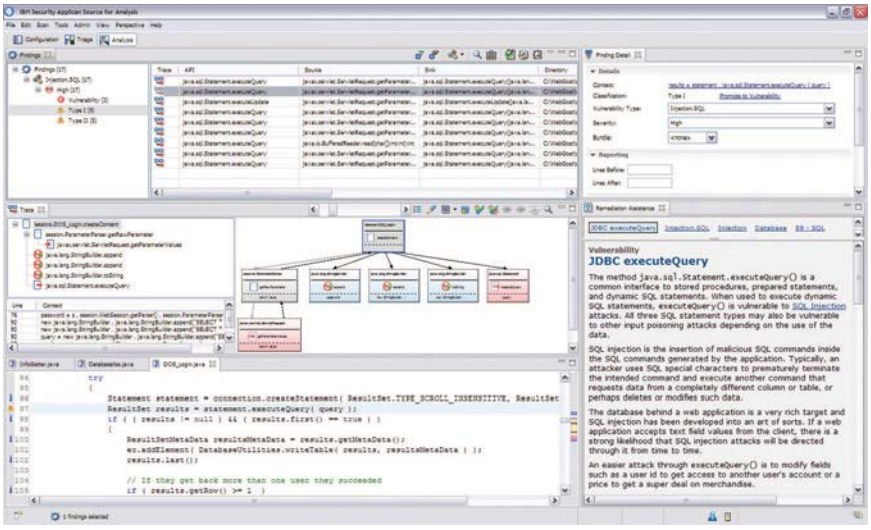

그림 3. IBM Security AppScan Source는 보안 위험에 해당하는 코드 행의 격리를 포함하여, 모든 취약점에 대한 수정 지원을 제공합니다.

IBM Security AppScan Source는 고객의 현 우선순위 및 심각도 용어와 기존 워크플로우를 이용하여 기존의 프로세스와 결부된 IBM Security AppScan Source 소프트웨어 문제를 디스패치할 수 있는 프레임워크를 갖춘 결함 추적 시스템(DTS)을 통합합니다.

모바일 애플리케이션의 보안

기업들은 모바일 애플리케이션을 제공해야 합니다. 이러한 요구는 내부 및 외부의 사용자들에 의해 발생되고 있으며, 많은 BYOD(Bring-Your-Own-Device) 사용자들은 내부 애플리케이션을 모바일 디바이스에 개방하도록 IT 조직에 압력을 가하고 있습니다. LOB 그룹은 고객을 위한 새로운 모바일 애플리케이션 요구사항을 확대하고 있습니다. 하지만, 모바일 애플리케이션에서 비롯되는 보안 위험 및 노출은 자동화된 솔루션이 없이는 관리가 불가능합니다.

IBM Security AppScan Source는 서버 기반의 모바일 애플리케이션 컴포넌트에 대한 보안을 제공해왔으며, 이제는 원시 모바일 애플리케이션 코드도 제공할 수 있습니다. IBM Security AppScan Source는 현재 안드로이드 모바일 애플리케이션의 정적 분석을 지원하고 있습니다. 방대한 안드로이드 보안 연구를 활용하여 정보 유출과 같은 공통적인 모바일 보안 위험을 검출하여 시정할 수 있으며, 기업들은 모바일 디바이스 상의 안드로이드 보안 위험을 사전에 처리할 수 있습니다.

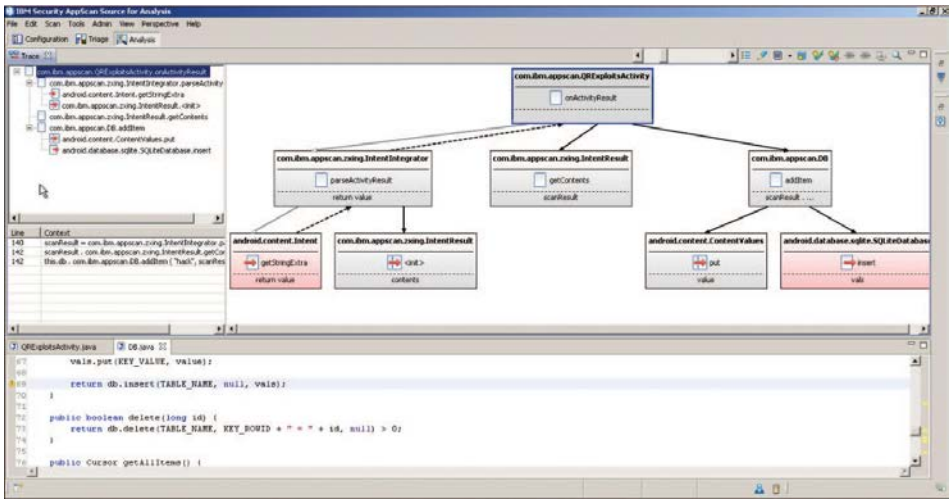

그림 4. 포괄적인 호출 및 데이터 플로우 분석은 모바일 애플리케이션 보안 위험의 격리에 유용합니다.

엔터프라이즈 현대화에 따른 위험을 관리합니다

레거시 애플리케이션의 엔터프라이즈 현대화 또한 애플리케이션 위험의 근원이 될 수 있습니다. COBOL은 여전히 전세계의 코드 사용률에서 약 80%를 차지하고 있으며,[1] 이러한 레거시 애플리케이션을 위한 웹 인터페이스는 코드가 작성되었던 20 ~ 40년 전에는 없었던 위협에 코드를 노출하고 있습니다.

IBM Security AppScan 소프트웨어 포트폴리오는 엔터프라이즈 현대화를 위한 전체 범위의 보안을 제공하여 웹 인터페이스의 보안을 확보하고 레거시 코드를 분석하여 보안 취약점을 파악합니다. Java, .NET, C/C++, PHP, SAP ABAP, COBOL을 포함한 다양한 언어와 더불어, Rational Application Developer, Eclipse, Microsoft Visual Studio와 같은 IDE와의 통합을 지원하는 IBM Security AppScan Source는 사전에 애플리케이션 보안을 확보함으로써 레거시 자산의 보호와 보안 위험의 관리에 도움을 줍니다. 주요 이점은 다음과 같습니다.

- 애플리케이션 취약성의 사전 수정으로 위험을 비용 효과적으로 관리
- 애플리케이션 수명주기 초기에 애플리케이션 보안을 확보하여 레거시 자산을 보호
- Java, ServerSide JavaScript, JSP, ColdFusion, C, C++, .NET(C#, ASP.NET, and VB.NET), Classic ASP,(JavaScript/VBScript), PHP, Perl, VisualBasic 6, PL/SQL, T-SQL, SAP ABAP, COBOL 등의 여러 언어와 관련된 취약점과 위험을 파악

코드 품질을 포함하도록 정적 테스트를 확장합니다

대다수 일류 기업들은 보안을 품질관리 요소로 간주하여 보안을 자사 소프트웨어 개발 프로세스에 통합하고 있습니다. 보안과 품질이 하나로 통합됨에 따라, IBM Security AppScan Source의 정적 코드 분석 기능이 확장되었으며, 이제 품질 결함의 파악이 분석에 포함되었습니다. IBM Security AppScan Source에는 또한 IBM Rational Software Analyzer가 제공하는 다음과 같은 기능도 포함되어 있습니다.

- 코딩 시에 코드 레벨 품질 결함을 확인하므로, 시간 및 비용 절감에 도움이 됩니다
- 잠재적 코딩 오류를 파악하여 해결함으로써 전반적인 코드 품질 및 예측 가능성을 개선합니다
- 개발자가 우수 사례를 습득하는 데 유용한 KPI를 제공합니다
- 즉시 사용할 수 있고 사용자 정의가 가능한 보고를 이용하여 프로젝트 가시성을 향상시키고 거버넌스 및 컴플라이언스를 더 효과적으로 관리합니다
- 집중식 소프트웨어 코드 스캔 솔루션을 위한 빌드 프로세스의 일부로 코드 품질 분석을 자동화합니다

IBM Security AppScan Source 소프트웨어는 IBM Security AppScan Source for Developer 소프트웨어 및 IBM Security AppScan Source for Remediation 소프트웨어를 포함한 IDE에서 또는 IBM Security AppScan Source for Automation 소프트웨어를 탑재한 빌드 시스템에서 품질 테스트를 실행할 수 있는 옵션을 제공합니다. 정적 분석을 확장하여 품질 테스트를 포함시킴으로써, IBM Security AppScan Source는 고객이 지속적으로 코드 품질 우수 사례를 향상시켜 출시 시간을 단축하고 고객 만족도를 제고하는 데 도움을 줍니다.

IBM을 선택해야 하는 이유

고급 보안 테스트 및 애플리케이션 위험을 관리하는 플랫폼을 갖춘 IBM Security AppScan 포트폴리오는 취약점을 파악하여 전반적인 애플리케이션 위험을 낮출 수 있도록 애플리케이션 수명주기 관리에 대한 통합과 보안 전문지식을 제공합니다. IBM은 고급 정적 분석 및 동적 분석과 더불어, 최신 위협에 대처하면서 정확하고 유용한 결과를 도출하는 혁신적인 기술을 이 포트폴리오에 포함시켰습니다.

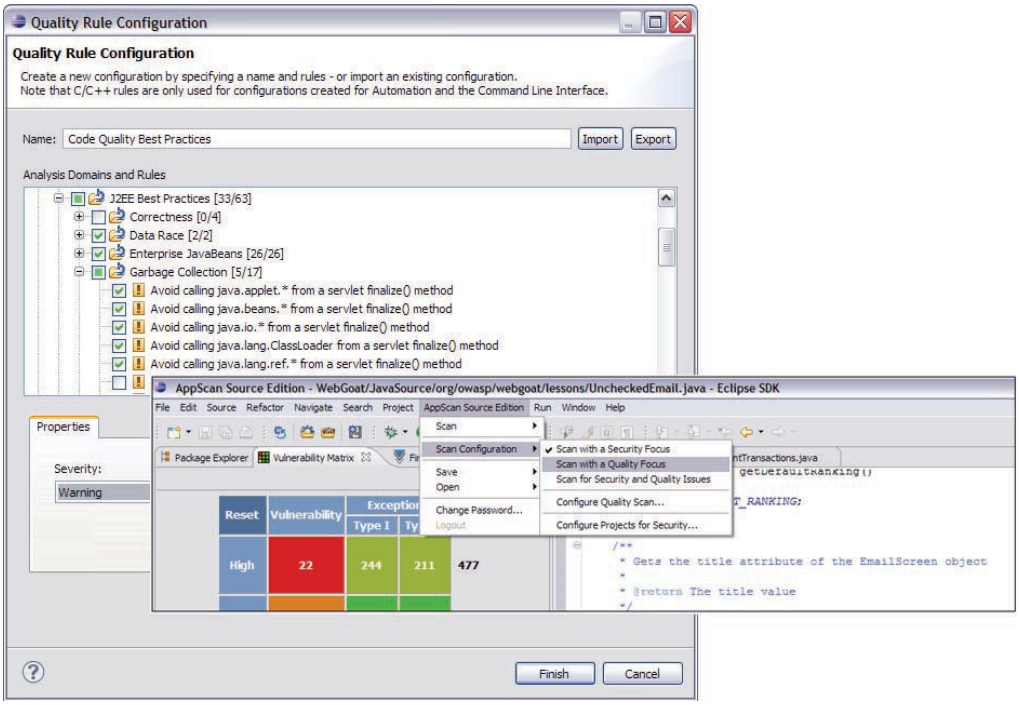

그림 5. IBM Security AppScan Source에는 IDE에서 또는 보안 테스트와 마찬가지로 빌드 시스템에서 실행할 수 있는 코드 품질 분석이 포함되어 있습니다.

솔루션 컴포넌트	특징 및 이점
IBM Security AppScan Enterprise Server(필요)	• 수많은 애플리케이션에 대해 애플리케이션 보안 테스트를 실시하고 위험을 관리할 수 있는 중앙 플랫폼을 제공합니다 • 보안 팀, 개발 및 테스트 팀 간의 협업을 촉진하며, 취약점을 수정하고 위험을 줄입니다 • 즉시 이용할 수 있는 40여 가지의 컴플라이언스, 추적, KPI 평가용 보고서 템플릿으로 애플리케이션 보안 및 컴플라이언스 위험에 대한 전사적인 시각을 제공합니다 • 동적 및 정적 스캔의 보안 테스트 결과를 연계하고 분류합니다 • IBM Security Network Intrusion Prevention System, IBM Proventia Management Site Protector, IBM Security Server Protection 소프트웨어와 통합하여, IBM Security AppScan 소프트웨어가 확인한 취약점을 겨냥한 공격을 차단합니다 • QRadar SIEM과 통합하여 애플리케이션 취약점 데이터를 제공하며, QRadar는 이 데이터를 이용하여 모든 이벤트를 비즈니스 영향에 따라 우선순위가 부여된 소수의 조치 가능한 공격으로 줄입니다
IBM Security AppScan Source for Analysis(정적 분석에 필요)	• 워크벤치를 이용하여 정적 애플리케이션 보안 테스트 정책(구성 및 스캔)을 관리합니다 • 정적 테스트의 결과를 분류하여 취약점을 수정하기 위한 조치를 취합니다 • IBM Rational ClearQuest®, HP Quality Center, Rational Team Concert™, Microsoft Team Foundation Server와 같은 결함 추적 시스템에 대한 통합을 제공합니다
IBM Security AppScan Source for Automation(선택)	• 정적 애플리케이션 보안 테스트, 공개, 보고를 빌드 환경으로 완벽하게 통합합니다 • 빌드 프로세스의 일부로 코드 품질 분석을 자동화합니다
IBM Security AppScan Source for Development(선택)	• 소스 코드를 스캔하고 코드 행의 치명적인 취약점을 파악하여 처리할 수 있는 IDE 모듈을 제공합니다 • 결함에 대한 상세한 설명과 소스 코드 수정 권고를 이용하여 IDE의 보안 취약점을 수정할 수 있습니다 • 비보안 소프트웨어 코드 레벨의 품질 결함을 파악하여 수정할 수 있습니다
IBM Security AppScan Source for Remediation(선택)	• 코드 행의 치명적인 취약점을 처리하고 해결할 수 있는 IDE 모듈을 제공합니다 • 결함에 대한 상세한 설명과 소스 코드 수정 권고를 이용하여 IDE의 보안 취약점을 수정할 수 있습니다 • 비보안 소프트웨어 코드 레벨의 품질 결함을 파악하여 수정할 수 있습니다
IBM Security AppScan Enterprise Dynamic Analysis Scanner(선택)	• 고급 동적 애플리케이션 보안 테스트가 추가되어 있습니다
IBM Security AppScan Enterprise Reporting Console(선택)	• 웹 기반 사용자가 테스트 결과를 선별하고, 개발 팀과 협력하며, 보고서를 생성하고 애플리케이션 위험 관리를 확대할 수 있는 기능을 제공합니다
Virtual Forge CodeProfiler for IBM Security AppScan Source(선택)	• 정적 코드 분석을 SAP ABAP 애플리케이션으로 확대하고, 보안 취약점 및 성능 문제를 파악하여 수정합니다

IBM Security AppScan Source 요약

시스템 요구사항:

- 디스크 공간: 약 1.5GB의 가용 하드 디스크 공간(설치할 경우 2GB 필요)
- 미디어 드라이브: CD-ROM 또는 DVD-ROM 드라이브
- 메모리: 2GB 이상의 RAM 권장
- NIC 네트워크 드라이버: TCP/IP로 구성된 네트워크 통신용 1NIC(10Mbps) (100Mbps 권장)
- 프로세서: 3.0GHz Intel Pentium IV 호환 프로세서(고속 프로세서 또는 다중 프로세서 권장)

운영 체제:

- Microsoft Windows 7 Professional, Enterprise 및 Ultimate 32/64 비트(32비트 모드로 실행)
- Microsoft Windows XP Professional(SP2 이상)
- Microsoft Windows Vista Business, Enterprise, Ultimate(SP1 이상) 32/64 비트(32비트 모드로 실행)
- Microsoft Windows Server 2003 Enterprise 및 Standard(SP2) (32비트 x86)
- Microsoft Windows Server 2003 R2 Enterprise 및 Standard(SP2) (32비트 x86)
- Microsoft Windows Server 2008 Enterprise 및 Standard(SP1 및 SP2) (32비트 x86)
- Microsoft Windows Server 2008 R2 Enterprise 및 Standard 64 비트(32비트 모드로 실행)

프로젝트 파일:

- Visual Studio 2005, Visual Studio 2008 및 Visual Studio 2010 / Eclipse 3.3, 3.4, 3.5, 3.6, 3.7 / IBM Rational Application Developer V7.0, V7.5, V7.5.0.3, V8.0, V8.0.1, V8.0.2, V8.0.3, V8.5

컴파일러:

- GCC(GNU Compiler Collection), Visual Studio 2005(V8) for Windows, Visual Studio 2008, Visual Studio 2010, Linux 및 Solaris용 Sun Studio C 및 C++ 컴파일러

IBM Security AppScan Source 요약

보안 지원 언어:

- Java, ServerSide JavaScript, JSP, ColdFusion, C, C++, .NET(C#, ASP.NET, VB.NET), Classic ASP(JavaScript/VBScript), PHP, Perl, VisualBasic 6, PL/SQL, T-SQL, COBOL

코드 품질 스캐닝 지원:

- Java, C/C++(CLI만 해당)

IDE 플러그인 지원:

- Eclipse 3.3, 3.4, 3.5, 3.6, 3.7 / IBM Rational Application Developer V7.0, V7.5, V7.5.0.3, V8.0, V8.0.1, V8.0.2, V8.0.3, V8.5 / Visual Studio 2005, Visual Studio 2008, Visual Studio 2010
- Rational Application Developer 및 Eclipse는 Java 지원 / Visual Studio는 C#, ASP.NET, VB.NET 지원

결함 추적 시스템 지원:

- IBM Rational ClearQuest V7.0, V7.1.1, 7.1.2, 8.0 / HP Quality Center 9.2, 10.0, 11.0 / Rational Team Concert 2.0.0.2, 3.0, 3.0.1, 4.0 / Microsoft Team Foundation Server 2008 및 2010

외부 데이터베이스 지원:

- Oracle Database 10g 및 11g

라이센스 요구사항:

- 라이센스 서버: Rational License Server 8.1.1 및 8.1.2(플로팅 라이센스로 활성화할 경우)

추가 정보

IBM Security AppScan Source가 소스 코드의 취약점 및 위협 노출의 파악에 얼마나 유용한지 자세히 알고 싶으시면, 담당 IBM 대표 또는 IBM 비즈니스 파트너에게 문의하거나, 다음 사이트를 방문하시기 바랍니다.
ibm.com/software/awdtools/appscan

또한 IBM Global Financing은 가장 비용 효과적이며 전략적인 방법으로 여러분의 비즈니스 요구사항에 부응하는 IT 솔루션을 확보할 수 있도록 도와 드립니다. IBM은 신뢰도 높은 고객들과 협력하여 귀사의 비즈니스 목표에 부합하는 IT Financing 솔루션을 맞춤화하고, 효과적으로 현금을 관리하며, 총소유비용을 향상해 드립니다.
IBM Global Financing은 중요한 IT 투자 자금을 확보하고 비즈니스를 가속화할 수 있는 가장 현명한 방법입니다. IBM Global Financing에 대한 자세한 정보는 www.ibm.com/financing에서 확인하실 수 있습니다.

IT 시스템 보안은 귀사 내/외부로부터의 부적절한 접근을 방지, 감지, 대응함으로써 시스템과 정보를 보호하는 일을 포함합니다. 부적절한 접근은 정보의 변경, 파괴 또는 유용을 초래하거나, 타 시스템에 대한 공격을 포함한 귀사 시스템에 대한 피해나 오용을 초래할 수 있습니다. 어떠한 IT 시스템이나 제품도 완벽하게 안전할 수 없으며, 단 하나의 제품이나 보안 조치만으로는 부적절한 접근을 완벽하게 방지하는 데 효과적이지 않을 수 있습니다. IBM 시스템과 제품은 종합적인 보안 접근방법의 일부로서 고안되며, 이러한 접근방법은 필연적으로 추가적인 실행절차를 수반하며 다른 시스템, 제품 또는 서비스가 가장 효과적일 필요가 있을 수도 있습니다. IBM은 시스템과 제품이 임의의 악의적 또는 불법적 행위로부터 영향을 받지 않는다는 것을 보장하지는 않습니다.

1 "TechBrief: Cobol – still doing the business," Nick Bray, January 2010. http://www.bankingtech.com/bankingtech/article.do?articleid=20000168221

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
July 2012

RAD14105-USEN-03