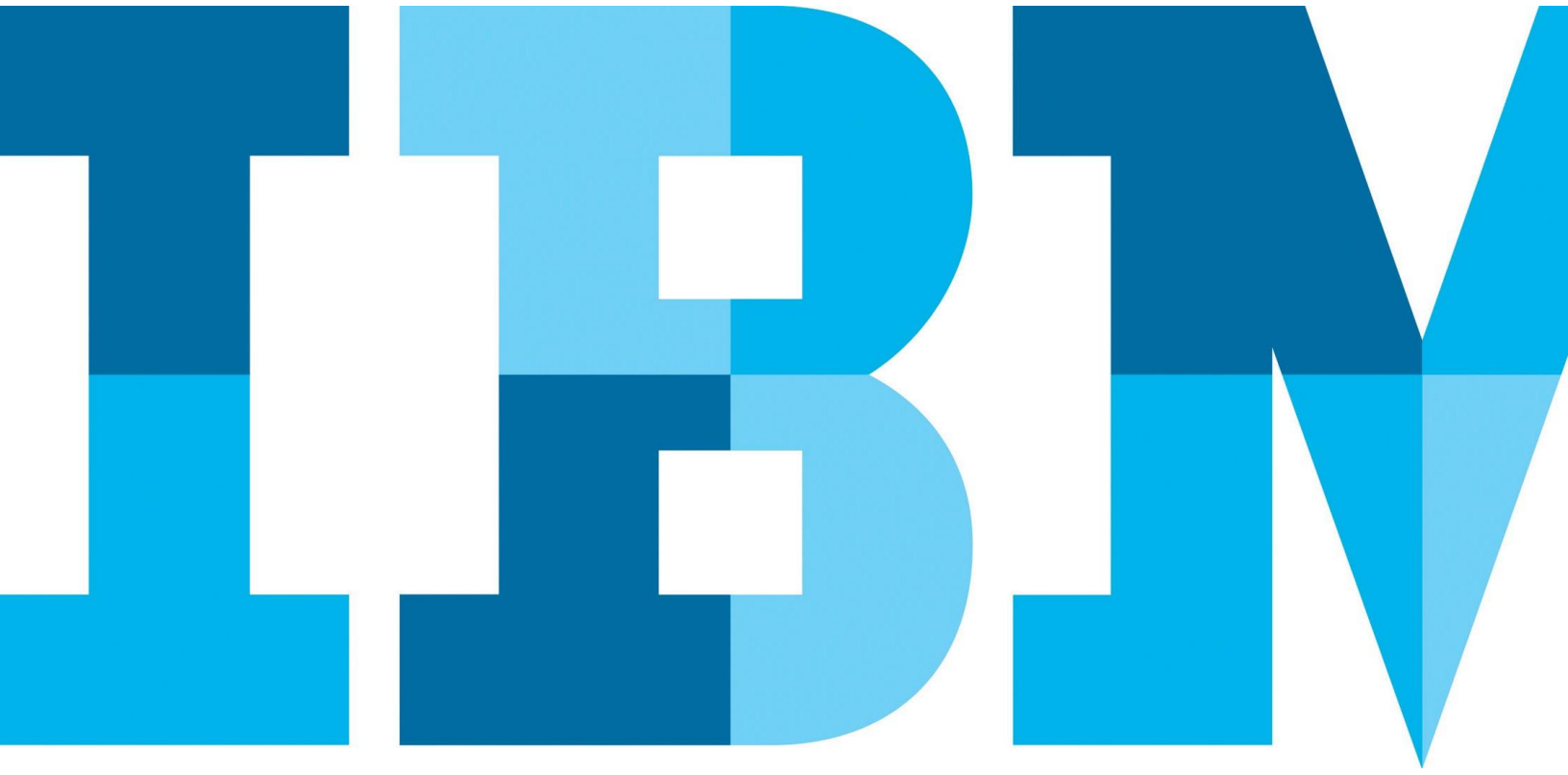
2016년 8월

기업의 중요 데이터 보호를 위한 애플리케이션 보안 위험 관리

IBM Security 애플리케이션 보안 관리 통합 솔루션은 취약점을 파악하고 애플리케이션 위험을 줄이도록 도와줍니다.



IBM

애플리케이션 보안의 당위성

많은 기업들이 중요 비즈니스 프로세스를 운영하고 공급업체와 거래를 하며 수준 높은 서비스를 고객에 제공하기 위해 소프트웨어 애플리케이션을 사용합니다. 하지만 기업들은 비즈니스 운영을 위해 애플리케이션에 의존하면서도 애플리케이션 보안에 투자를 거의 또는 전혀 하지 않고 있습니다. 이러한 기업들은 네트워킹이나 운영 같은 일상업무 그리고 접근제어 및 인증 같은 보안절차 관리를 위한 기존의 보안 기술에 대해서는 잘 알고 있지만 다수가 효과적인 애플리케이션 보안 프로그램의 구현, 관리, 유지보수에 어려움을 겪고 있습니다. 그러나 오늘날과 같이 점점 복잡해지는 환경에서 그러한 장애물은 사라져야 합니다. 애플리케이션이 기업 전체의 보안을 위태롭게 할 수 있기 때문에 애플리케이션 보안이 최우선 순위가 되어야 할 필요가 있습니다.

보안이 충분하지 않은 애플리케이션이 가져올 파급효과는 심각할 수 있습니다. 개발단계에서 의도치 않게 생겨난 취약점 때문에 해커들이 애플리케이션을 불안정하게 하고 회사 기밀정보나 개인 고객 데이터에 무제한으로 접근할 수 있게 됩니다. 이러한 유형의 데이터 손실은 브랜드 명성 훼손, 소비자 신뢰 하락, 비즈니스 운영 중단, 공급망 단절, 소송 위협, 규제 검열 등 궁극적으로 수익성에 영향을 미칠 수 있는 결과로 이어질 수 있습니다.

애플리케이션 보안 문제를 해결하는 것은 매우 어려운 일일 수 있습니다. 규모가 큰 기업들은 수 천 개의 애플리케이션을 관리하는데 이러한 애플리케이션의 보안은 대개 규모가 작고 업무량이 많은 팀에서 담당하게 됩니다. 이러한 결과가 발생하지 않게 하기 위해 기업은 위험 기반 애플리케이션 보안 관리를 구현해야 합니다. 즉, 인프라 전반에 걸쳐 명확한 가시성을 제공하고, 비즈니스에 미치는 영향에 따라 애플리케이션을 구별하고 우선순위를 매기며, 애플리케이션의 취약점을 평가하여 맥락에 따라 취약점의 위험수준을 결정하고, 필요한 코드 수정을 실행하거나 적절한 정책을 활용함으로써 위험을 완화할 수 있는 솔루션이 필요합니다. 애플리케이션 라이프사이클의 모든 단계에서 웹 기반 및 모바일 애플리케이션을 보호할 수 있는 보안 전략을 도입하는 것이 확실한 그 첫 번째 단계가 될 것입니다.

애플리케이션 보안 관리 전략의 도입

많은 기업들이 애플리케이션 보안을 우선순위에 두지 않아 기업의 환경 전체를 위험에 빠뜨립니다. Ponemon Institute에서 실시한 연구조사에 따르면 보안 전문가 32%가 기업의 가장 큰 잠재 위협으로 애플리케이션 계층 위협을 꼽은 반면 단 25%만이 네트워크 계층 위협을 가장 큰 잠재 위협으로 꼽았습니다. 그러나 응답자 기업에서는 총 IT 보안 예산의 평균 18%만 애플리케이션 보안에 지출한 것으로 보고하였습니다.[1] 그래서 문제는 과연 이렇게 진화하는 보안 위험에 상응하도록 충분한 보안 예산을 기업이 할당하고 있느냐 하는 것입니다.

효과적인 보안은 사실 위험 관리의 문제입니다. 기업은 기업의 가장 중요한 자산과 관련된 위험을 이해, 관리, 완화해야 합니다. 효과적인 애플리케이션 보안을 위해 기업이 해야 할 사항은 다음과 같습니다.

1. **자산목록 작성**: 기업의 자산은 무엇이며 어떠한 자산이 가장 중요한 것인지 이해합니다. 지금 당장 모든 애플리케이션에 보안 조치를 실시하는 대신 가장 중요한 자산에 먼저 집중하는 것이 중요합니다.
2. **비즈니스 영향 평가**: 기업의 애플리케이션 자산에 우선순위를 매긴 후 취약성 분석을 수행합니다. 비즈니스 영향 및 취약도에 따라 애플리케이션 각각의 위험을 평가합니다.
3. **취약점 우선순위 부여**: 각 애플리케이션의 위험 순위 평가가 끝난 후 위험이 가장 큰 애플리케이션에 집중하고 가장 심각한 취약점을 먼저 해결합니다.
4. **치료 계획**: 위험 완화는 코딩 에러 해결, 웹 애플리케이션 방화벽을 통한 가상 패치 생성, 일부의 경우 애플리케이션의 임시 오프라인화를 포함할 수 있습니다.
5. **투자수익률 측정**: 다양한 지표를 활용하여 기업의 애플리케이션 보안 상태를 모니터링하고 현재 진행 중인 애플리케이션 보안 프로그램의 효과성을 측정할 수 있습니다.

애플리케이션 보안 여정

애플리케이션 보안 관리를 위한 위험 기반 접근법에는 5가지 핵심 고려사항이 있습니다.

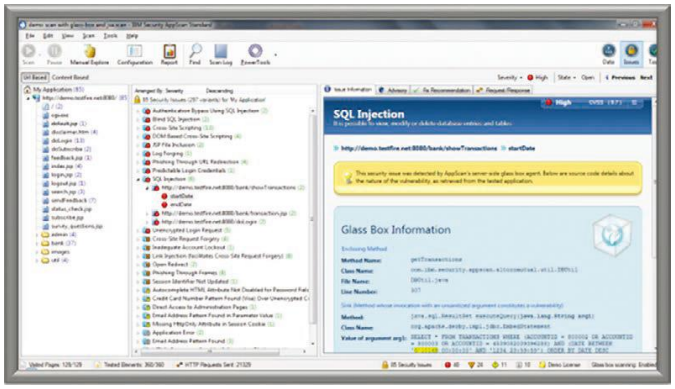
IBM 통합 애플리케이션 보안 관리 소개

규모가 큰 기업에서 애플리케이션 보안 이니셔티브를 운용하는 것이 매우 어려울 수 있습니다. 종종 규모가 작은 보안팀이 여러 개발팀이 구축한 수 천 개의 애플리케이션 보안을 담당합니다. IBM은 보안팀이 매일매일 씨름하는 취약점을 해결할 수 있도록 애플리케이션 보안 관리를 위한 통합 기능을 제공합니다. 이 포트폴리오는 IBM 비즈니스 파트너의 솔루션뿐만 아니라 온프레미스 및 클라우드 기반 옵션을 포함합니다.

온프레미스 솔루션

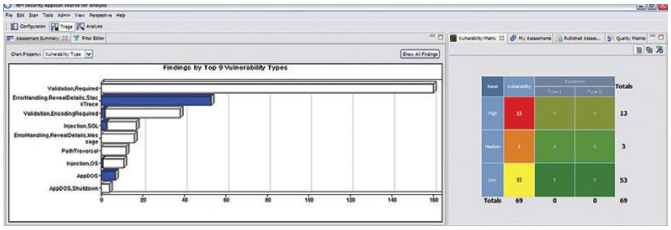
IBM® Security AppScan® 솔루션은 규모와 상관없이 모든 기업의 애플리케이션 보안 관리자 및 개발팀을 위해 특별히 설계된 컴포넌트를 제공합니다. 온프레미스 오퍼링은 다음을 포함합니다.

- **IBM Security AppScan Standard:** 애플리케이션 보안 취약성 테스트 자동화 및 고급 DAST 기능을 활용함으로써 애플리케이션 공격 및 데이터 침입 위험을 줄여줍니다.



AppScan Standard 소프트웨어는 추가 취약점 확인, 스캔 구성 단순화, 추가 실행가능 결과 제공을 위한 런타임 분석과 유리상자 테스트(Glass-box Test)를 포함합니다.

- **IBM Security AppScan Source:** 웹과 모바일 애플리케이션의 소프트웨어 취약점을 개발 라이프사이클 초기에 찾아내어 개발 전에 제거함으로써 비용을 낮추고 위험 노출을 줄여줍니다.

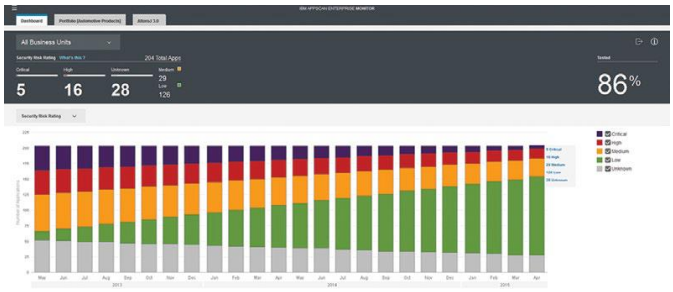


AppScan Source 소프트웨어는 애플리케이션 위험과 맵핑한 평가 요약을 제공하며 기업의 애플리케이션에 영향을 주는 취약점에 관한 인사이트를 제공합니다.

- **IBM Security AppScan Enterprise:** 기업들이 애플리케이션 보안 위험을 완화하고 규제를 준수하도록 합니다. 또한 보안 및 개발팀이 애플리케이션 목록을 구축하고, 비즈니스 영향에 따라 애플리케이션을 분류하며 취약점에 우선순위를 매기고, 애플리케이션 라이프사이클 전반에 걸쳐 취약점을 치료하도록 합니다.

클라우드 기반 솔루션

IBM Application Security on Cloud는 기업의 애플리케이션 포트폴리오의 보안 위험을 쉽게 관리하고 클라우드에서 웹 및 모바일 애플리케이션 보안 테스트를 수행하도록 합니다. 이 솔루션은 정적 애플리케이션 보안 테스트(SAST) 및 동적 애플리케이션 보안 테스트 (DAST) 분석을 포괄적인 올인원 오퍼링에서 지원합니다.



AppScan 애플리케이션 보안 관리 기능은 보안팀이 매일매일 씨름하는 취약점을 해결할 수 있게 합니다.

IBM 비즈니스 파트너 솔루션

IBM 비즈니스 파트너도 다음과 같은 다양한 애플리케이션 보안 테스트 솔루션을 제공합니다.

- **Arxan Application Protection for IBM Solutions**: 모바일 애플리케이션 하드닝, 암호화 키 보호, 런타임 보호까지 취약성 분석 기능을 확장합니다.
- **Cigital Application Security Testing Managed Services**: 기업의 변화하는 애플리케이션 포트폴리오를 맵핑하는 서비스 모델로서 유연한 애플리케이션 보안 테스트를 제공합니다. 이 오퍼링은 애플리케이션 포트폴리오 전반에 걸쳐 실행 가능한 취약성 인사이트, 침투 테스트, 선두 애플리케이션 보안 파트너인 Cigital이 제공하는 전문 치료를 통해 보안 위험을 크게 완화하도록 설계됩니다.

솔루션 기능

IBM의 애플리케이션 보안 테스트 솔루션은 기업들이 애플리케이션 라이프사이클 전반에 걸쳐 보안을 관리하도록 합니다. 핵심 기능은 다음과 같습니다.

- **확장가능 애플리케이션 보안 테스트**—AppScan으로 기업에 적합한 솔루션을 선택할 수 있으며 애플리케이션 보안 프로그램이 성숙해감에 따라 맞춤화가 가능하도록 컴포넌트를 추가할 수 있습니다.
- **고수준 가시성**— AppScan은 애플리케이션-위험 대시보드를 통해 기업 전반의 보안 상태, 애플리케이션 및 프로세스의 준수 위험에 대한 엔터프라이즈 수준의 가시성을 제공합니다.
- **규제요건 관리**—웹 애플리케이션 관련 주요 준수 요구에 직면한 많은 기업의 요구사항을 충족하기 위해 AppScan은 사용자가 40개 이상의 사전 정의된 보고서에서 선택하고 스캔 결과를 주요 산업 및 규제 준수 기준에 맵핑할 수 있게 합니다.
- **보안 테스트 거버넌스**—AppScan을 통해 기업 전반에 적용할 수 있는 일관된 보안 정책을 수립, 추진, 실행할 수 있도록 테스트 정책 및 스캐닝 템플리트가 제공됩니다.
- **이슈 치료**—AppScan은 각 스캔에서 발견된 취약점 모두에 대해 순위 리스트를 생성하고 최우선순위의 문제를 먼저 해결하도록 합니다.
- **보안 인텔리전스**—AppScan은 다른 IBM 보안 오퍼링과 통합하여 위협 평가 및 보안 이슈 우선순위 부여를 더욱 향상시킵니다.

고급 애플리케이션 테스트

애플리케이션 보안에 대한 접근법이 다양하게 존재하기 때문에 AppScan 소프트웨어는 애플리케이션 라이프사이클의 모든 단계에서 애플리케이션 심층 분석이 가능한 광범위한 테스트 기술을 활용합니다.

IBM의 애플리케이션 보안 테스트 솔루션은 유리상자 테스트 및 런타임 분석 같은 혁신적인 기술뿐만 아니라 동적 및 정적 애플리케이션 보안 테스트도 제공합니다. 이 기술들은 사용자들이 가장 최신의 위협에 선제적으로 대응하고 정밀하고 실행 가능한 결과를 도출하도록 합니다. AppScan 테스트 기법은 다음과 같습니다.

- **정적 분석**은 잠재적 취약점의 소스 코드를 검사하여 취약점을 개발사이클 초기에 발견할 수 있도록 촉진합니다.
- **동적 분석**은 실행 중인 애플리케이션을 잠재적 해커와 유사한 방식으로 검사함으로써 개발사이클 후기 단계에서 애플리케이션을 테스트합니다. 이를 통해 기업은 더 쉽게 취약점과 잠재적 악용과의 관계를 밝힐 수 있습니다.

- **대화식 분석**은 테스트가 진행되는 동안 런타임 에이전트를 애플리케이션 머신 상에 두고 애플리케이션을 분석합니다. 런타임 시 동적 및 정적 분석 측면을 결합하여 더 정확하게 더 많은 취약점을 찾아낼 수 있습니다.
- **하이브리드 분석**은 동적 및 정적 분석을 결합하여 결과간의 상관 관계를 밝히거나 검증을 수행합니다. 이 분석은 동적 분석을 통해 밝혀진 이슈에 대해 문제가 되는 코드 라인까지 추적하며 정적 분석에서 밝혀진 이슈는 외부 테스트로 검증합니다.
- **JavaScript 클라이언트측 분석**은 클라이언트에 다운로드된 코드의 분석을 도와줍니다. 기업이 더 많은 기능을 클라이언트측에서 수행하면 할수록 클라이언트측 취약점과 악용의 잠재성은 더 커집니다.

IBM 애플리케이션 보안 테스트 솔루션의 주요 수혜자

IBM 애플리케이션 보안 테스트 솔루션은 다음과 같은 세 가지 주요 그룹에 혜택을 주도록 설계되었습니다.

- 현업 소유자 또는 최고정보보안책임자(CISO): 애플리케이션 보안 및 불충분한 보호의 결과에 대해 궁극적으로 책임이 있는 사람들이 기업의 보안 위험 및 전반적인 준수 상태를 더 잘 이해하게 됨으로써 혜택을 볼 수 있습니다.
- 애플리케이션 보안팀: 기업 내에서 애플리케이션 보안 관리 및 완화를 담당하고 있는 팀이 기업의 보유 자산, 자산의 중요도 순위, 보안 수준, 가장 중요한 취약점을 정확히 이해함으로써 혜택을 볼 수 있습니다.
- 애플리케이션 개발팀: 애플리케이션을 개발하는 팀이 가장 먼저 해결해야 할 중요한 취약점이 어떤 것인지 또 해결 방법은 무엇인지 이해함으로써 혜택을 볼 수 있습니다.

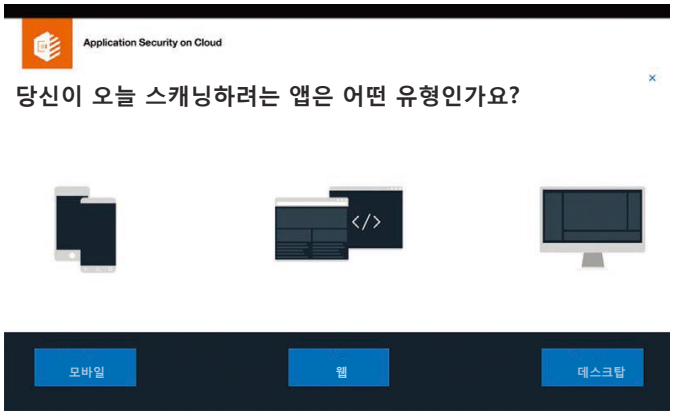
엔드-투-엔드 보안 솔루션 생성

애플리케이션 보안은 스캔을 수행하고 취약점을 찾는 것뿐만 아니라 위험 관리에 관한 것이기도 합니다. 애플리케이션 보안을 위해 통합형 자동화 솔루션을 설치하면 더 간소화되고 비용효율적이며 신뢰성 있는 결과를 제공할 수 있습니다. 통합은 모든 애플리케이션을 즉시 보호할 수 없는 현실에서 기업이 이를 대처하도록 돕는 위험기반 접근법을 구현합니다. 예를 들어 보안 인텔리전스는 애플리케이션의 우선순위를 부여하고 가장 먼저 해결해야 할 애플리케이션이 무엇인지 또 그 해결 시점과 방법을 결정하기 위해 필요합니다.

이것이 바로 애플리케이션 보안 테스트 솔루션 및 보완적인 IBM Security 제품이 설계된 이유입니다. 이 솔루션들은 기업에 애플리케이션 보안뿐만 아니라 현존하는 위험에 따라 위협과 취약점을 더 잘 평가할 수 있는 역량을 제공합니다. 여기에 포함되는 제품은 다음과 같습니다.

- **IBM QRadar® Security Intelligence Platform**은 보안 정보 및 이벤트 관리(SIEM), 로그 관리, 이상 탐지, 인시던트 포렌식(incident forensics), 구성 및 취약성 관리를 통합하기 위한 단일 아키텍처를 제공합니다.
- **IBM Security QRadar Vulnerability Manager**는 네트워크 기기 및 애플리케이션 보안의 취약점을 사전에 발견하고 상황을 고려하여 치료, 완화 활동의 우선순위를 매기도록 돕습니다.
- **IBM Security Network Intrusion Prevention System**은 계속 진화해가는 위협이 비즈니스에 영향을 미치기 전에 그 위협을 막기 위해 설계되었습니다.

- **IBM Security Guardium®**은 민감한 데이터의 발견 및 분류에서부터 민감한 데이터를 보호하기 위한 데이터와 파일 활동의 취약성 평가, 모니터링, 마스킹, 암호화, 차단, 경고, 격리에 이르기까지 광범위한 기능을 갖춘 통합적인 데이터-보안 플랫폼을 제공합니다.
- **IBM mobile security solutions**는 IBM Application Security on Cloud 모바일 애플리케이션 보안 테스트 기능과 통합하여 모바일 애플리케이션의 잠재적 보안 취약점을 선제적으로 해결하고 운영 효율성을 개선하도록 지원합니다.
- **IBM cloud security solutions**는 애플리케이션에서부터 데이터센터에 이르기까지 모든 온디맨드 컴퓨팅 자원을 인터넷을 통해 종량제로 제공합니다.



IBM Application Security on Cloud로 모바일, 웹, 데스크탑 애플리케이션 스캐닝이 매우 쉬워집니다. 사용자들은 스캔하고 싶은 애플리케이션 유형만 선택하면 됩니다.

요약

애플리케이션 보안의 중요성은 명확하고, 해결해야 할 과제는 복잡합니다. 필요한 인프라의 가시성과 적합한 보안 솔루션이 없다면 기업을 보호하는 것이 감당하기 힘든 일처럼 보일 수 있습니다. IBM은 애플리케이션 보안을 위한 명확한 로드맵을 보여주면서 효과적이고 성공적인 애플리케이션 보안 테스트 프로그램을 생성하기 위해 기업이 취할 수 있는 중요한 단계가 무엇인지 제시해 왔습니다.

IBM Security AppScan 솔루션은 고급 보안 테스트 및 애플리케이션 위험 관리 플랫폼을 통해 기업들이 더 쉽게 최신 보안 전략을 시작하고 관리할 수 있도록 설계되었습니다. 이 솔루션은 보안 취약점을 식별하는 것뿐만 아니라 전반적 애플리케이션 위험을 줄이는 데 필요한 보안 전문지식 및 핵심 통합을 애플리케이션 라이프사이클 관리와 함께 제공합니다.

앞으로 기업의 애플리케이션 보안 성숙도가 진화하게 되면 기업에서는 기업의 특정 요구사항에 가장 적합한 컴포넌트를 이용해 IBM 애플리케이션 보안 테스트 솔루션을 맞춤화할 수 있습니다.

지금 무료로 IBM Security AppScan을 체험하고 싶으시면 아래 IBM Security AppScan 웹페이지를 방문하십시오.

IBM Application Security on Cloud의 무료 체험 계획에 액세스하려면 IBM Application Security Analyzer 웹페이지를 방문하십시오.
https://www.ibm.com/marketplace/cloud/application-security-on-cloud/us/en-us

자세히 알아보기

IBM 애플리케이션 보안 테스트 솔루션에 대한 자세한 내용은 IBM 영업 대표 또는 IBM 비즈니스 파트너에 문의하시거나, 다음 웹사이트를 참조하십시오. **ibm.com**/applicationsecurity

보완적인 IBM Security 오퍼링에 대한 자세한 내용은 다음 웹사이트를 참조하십시오. **ibm.com**/security

각 애플리케이션 보안 테스트 솔루션의 상세한 시스템 요건을 보시려면 아래 링크를 클릭하십시오.

- IBM Security AppScan Standard
- IBM Security AppScan Source
- IBM Security AppScan Enterprise
- IBM Application Security on Cloud
- Arxan Application Protection for IBM Solutions
- Cigital Application Security Testing Managed Services

© Copyright IBM Corporation 2016

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
2016년 8월

IBM, IBM 로고, ibm.com, AppScan, QRadar 및 Guardium은 전세계 여러 국가에 등록된 International Business Machines Corp.의 상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다. 현재 IBM 상표 목록은 웹 "저작권 및 상표 정보" (**ibm.com**/legal/copytrade.shtml)에 있습니다.

이 문서는 최초 발행일을 기준으로 하며, 통지 없이 언제든지 변경될 수 있습니다. IBM이 영업하는 모든 국가에서 모든 오퍼링이 제공되는 것은 아닙니다.

이 문서의 정보는 상품성, 특정 목적에의 적합성에 대한 보증 및 타인의 권리 비침해에 대한 보증이나 조건을 포함하여(단, 이에 한하지 않음) 명시적이든 묵시적이든 일체의 보증 없이 "현상태대로" 제공됩니다. IBM 제품에 대한 보증은 제품의 준거 계약 조항에 의거하여 제공됩니다.

법률과 규정을 준수하는지 확인해야 할 책임은 고객에게 있습니다. IBM은 법률 자문을 제공하지 않으며 IBM의 서비스나 제품을 통해 관련 법률이나 규정에 대한 고객의 준수 여부가 확인된다고 진술하거나 보증하지 않습니다.

우수 보안 관리제도에 대한 설명: 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 합법적이며 종합적인 보안 접근방법의 일부로서 고안되며, 이러한 접근방법은 필연적으로 추가적인 실행절차를 수반하며 가장 효과적이기 위해서는 다른 시스템, 제품 또는 서비스가 필요할 수도 있습니다. IBM은 시스템과 제품이 임의의 당사자의 악의적 또는 불법적 행위로부터 영향을 받지 않는다는 것을 보장하지는 않습니다.

[1] "IBM Survey on Application Security Risk Management," Research study by the Ponemon Institute, Sponsored by IBM Corp., .

재활용하십시오.

WGB03009-KRKO-02