Coverity

Global No.1 소스 코드 보안 취약점 및 코딩 가이드라인 검증 솔루션

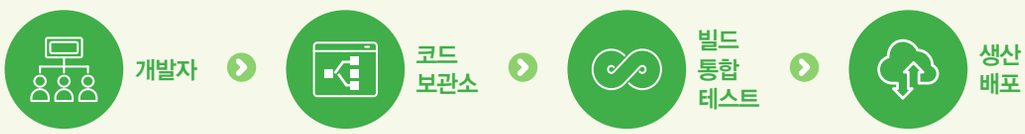
- SW의 품질 결함, 보안 취약점 분석, 코딩 규칙 분석 자동화 솔루션
- 임베디드 SW, 엔터프라이즈, 웹, 모바일 어플리케이션의 취약점 분석
- 국제 표준의 Certification 및 CWE Compatible 보유

특징 및 장점

- 정적 통합 분석 – 코딩 규칙, 메트릭, 결함 및 취약점 통합 분석
- CWE, OWASP, CERT C/C++/Java, MISRA, AUTOSAR 등 지원
- 다양한 개발 언어 분석 – C, C++, C#, Java, Python, Go, Android, iOS 등 20여개 이상
- 다양한 OS, 컴파일러 및 프레임워크 지원 (Windows, Linux, Mac, Solaris, AIX 등)
- 보안 정책 컴플라이언스 관리 지원 (ex〉 OWASP Top 10, CWE/SANS Top 25, PCI DSS 등)
- 결함 및 취약점 상세 설명, 심각도, CWE 정보, 결함 발생 위치, 수정 지침 및 데이터 플로우 추적
- 다양한 IDE, 소스 코드 관리, 이슈 트래커, CI 빌드 도구, ALM 솔루션과 통합
- 빌드 없는 분석을 통한 품질 및 보안팀의 효율성 높은 평가 지원

주요 검출 항목

- Buffer overflows
- Control flow issues
- Cross-site scripting (XSS)
- Hard-coded credentials
- Memory—corruptions
- Null pointer dereferences
- Race conditions
- Security best practices violations
- SQL injection
- Concurrent data access violations
- Cross-site request forgery (CSRF)
- Deadlocks
- Integer overflows
- Memory—illegal accesses
- Program hangs
- Resource leaks
- Security misconfigurations
- Uninitialized members



기대 효과

- SW 개발 단계에서 SW 결함과 취약점을 빠르고, 쉽고, 정확하게 수정
- 개발팀과 품질팀의 업무 협업 및 정량적인 품질 관리

적용분야 및 지원환경

- 임베디드, 모바일, Web, 시스템 등 다양한 소프트웨어 개발 환경
- 국방, 자동차, 산업용기기, 선박, 에너지, 의료, 항공, IT 등 다양한 산업시장