

CODE-RAY XG V 6.0 R2

Application Security Testing

SSR (주)에스에스알

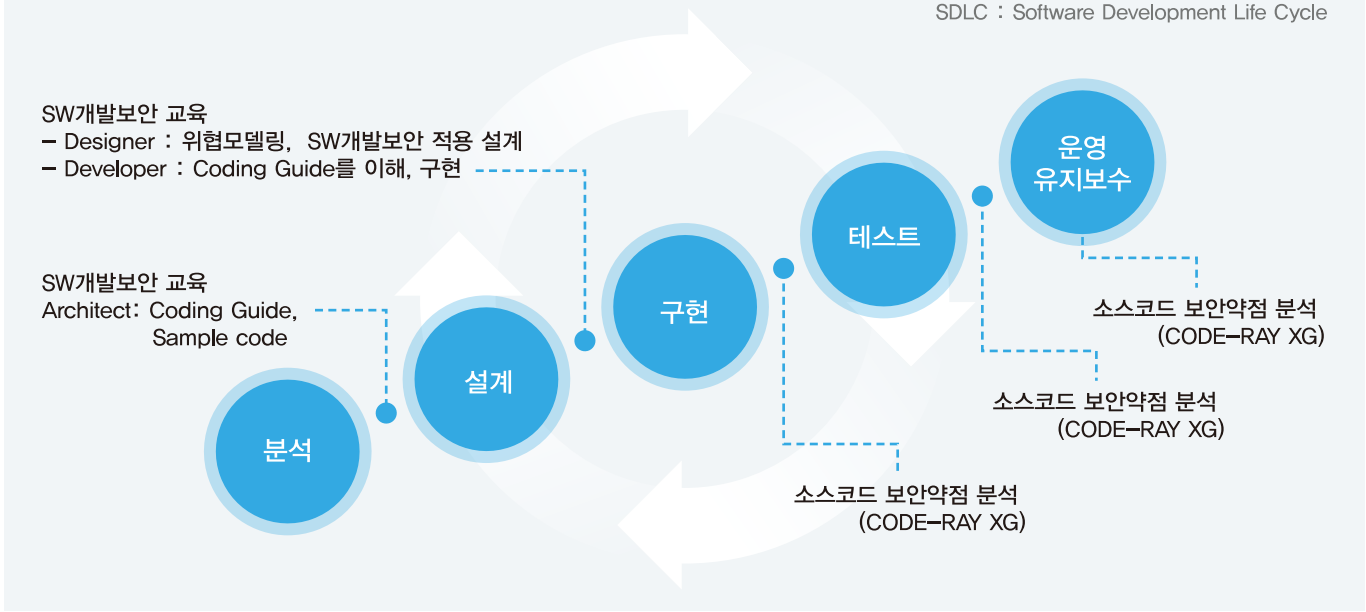
코드레이 엑스지 V 6.0 R2

Enterprise Secure-coding Guidance

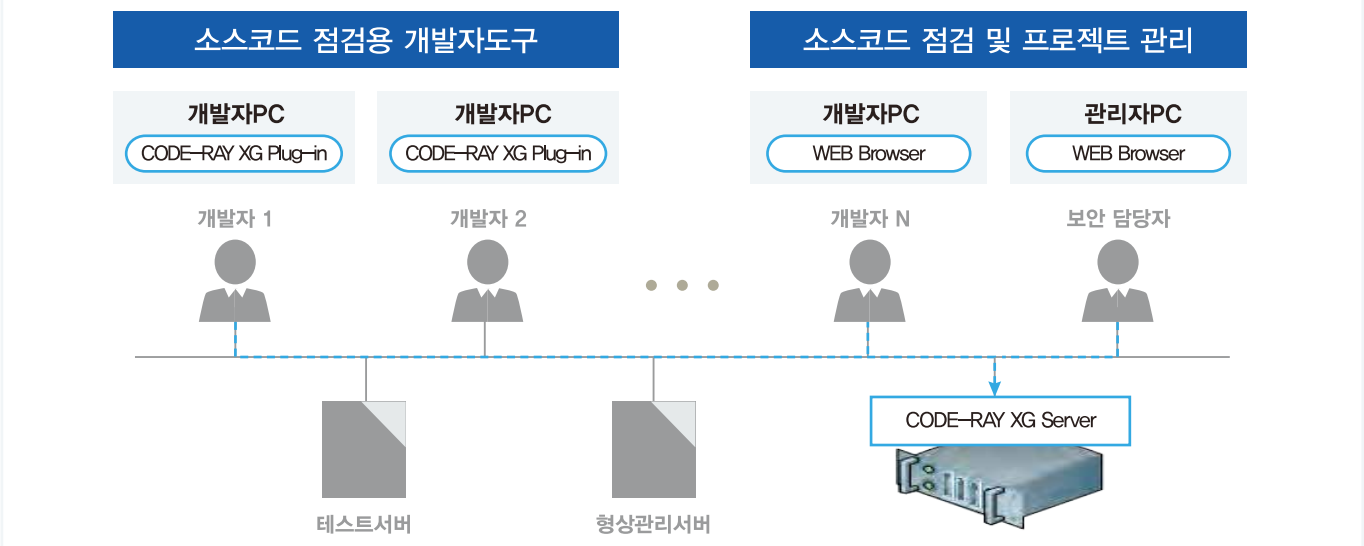
소스코드 개발보안 솔루션

- 소프트웨어의 개발공정(SDLC) 단계에서 발생할 수 있는 소스코드의 보안약점을 분석하고 관리하기 위해 다양한 점검 방법과 프로젝트에 대한 통합관리 기능을 제공합니다.
- 소프트웨어 개발보안 가이드 49개 항목(2021년 개정안), 국정원 웹 8대 취약점, 전자금융감독규정 8대 취약점, OWASP TOP 10, CWE/SANS TOP25, 소스코드 메트릭, 주요정보통신기반시설 기술적 취약점 항목(웹) 등 국내 · 외 다수의 점검 컴플라이언스를 지원합니다.
- Android, ASP, ASP.NET, C/C++, C#, Flutter(DART), HTML, IOS, JAVA, JAVASCRIPT, JSP, KOTLIN, TOBESOFT, PHP, PYTHON, SWIFT, TYPESCRIPT, VBSCRIPT, XML 등 다수의 개발언어를 지원합니다.

SDLC에서의 SW 개발보안 적용 방안



구성도



특장점

1. 통합 대시보드

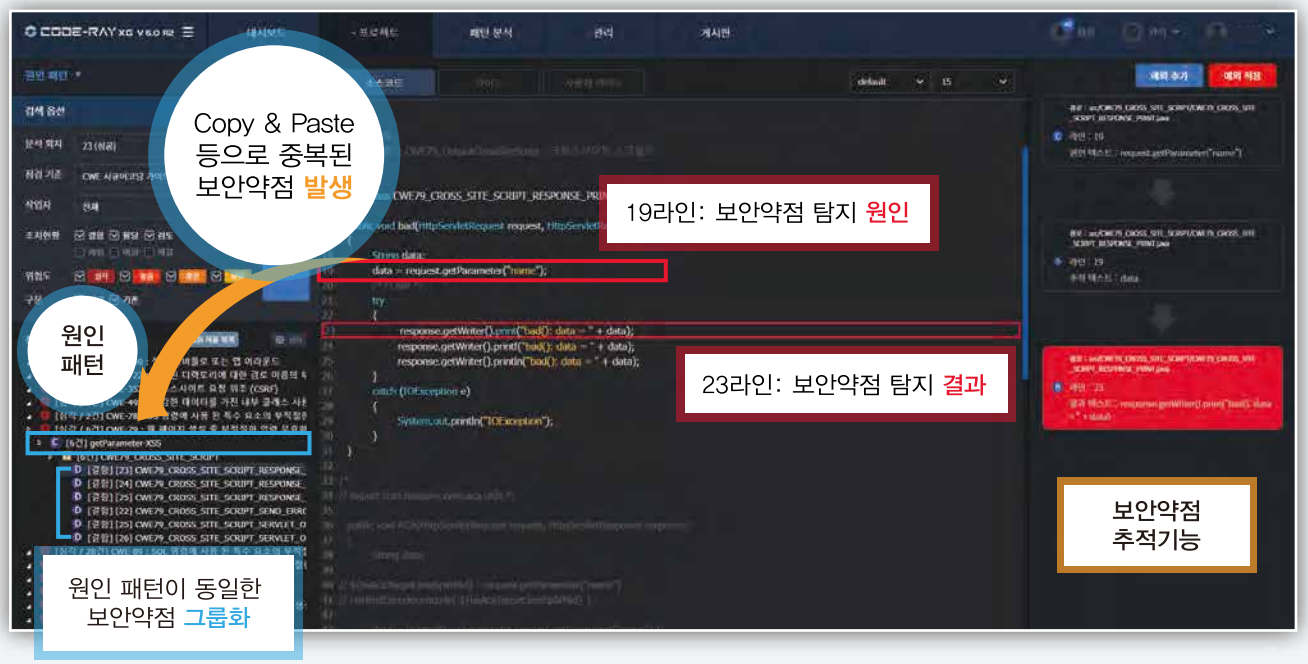
LOGIN SCREEN





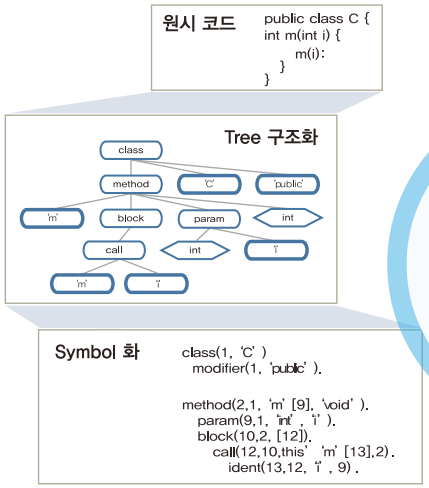
DASHBOARD

2. 보안약점 패턴 그룹 조회



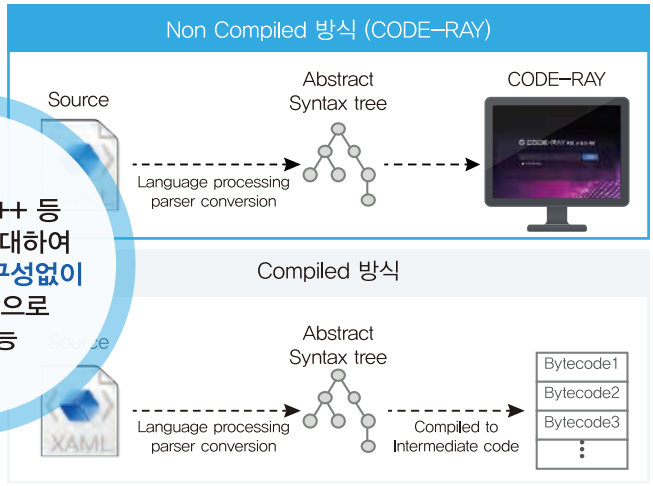
3. 강력한 분석엔진

가상컴파일을 통한 정적분석



JAVA, C/C++ 등
모든 언어에 대하여
컴파일 환경 구성없이
소스코드만으로
분석 가능

Non Compiled 분석



다양한 방식의 정적분석 기법 제공

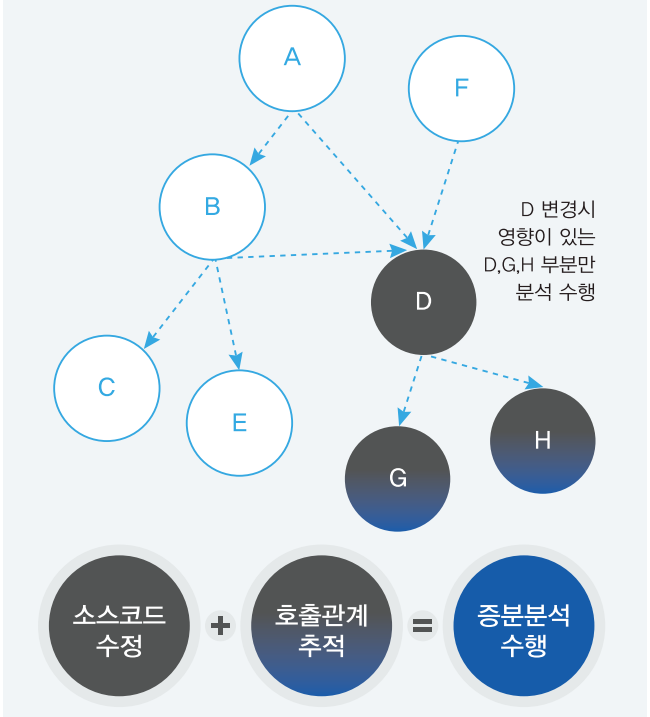
패턴분석 탐지기법 특정 키워드에 대한 정규 표현식 탐지	Configuration 탐지기법 Properties 등 설정 정보 탐지
DataFlow 및 Semantic 탐지기법 변수/함수 추적 등을 통한 흐름추적	

	Non Compiled	Compiled
분석 방식	가상컴파일을 통해 AST 구조를 생성함	실제 컴파일을 통해 AST 구조를 생성함
빌드 구성	빌드 환경 구성이 필요치 않음	빌드 환경 구성이 필요 취약점 분석 시간이 오래 걸림

다 계층 소스코드 간 연관관계 분석



증분 분석



관련 규정

규정 1 행정안전부 고시

2021.01.19 개정안 고시

행정안전부 고시 제2021-3호(2021. 1. 19)
- SW보안약점 기준 개정 : 6개 항목 신설, 8개 항목 4개 통합

행정안전부 고시 제2019-69호(2019. 8. 23)
- 행정기관 및 공공기관 정보시스템 구축 · 운영 지침
- 신규개발 : 설계단계 산출물 및 소스코드 전체
- 유지보수 : 변경된 설계단계 산출물 및 소스코드 전체
- 국가보안기술연구소장이 인증한 보안약점진단도구 사용 (국정원 EAL2 CC인증)

규정 2 전자금융감독 규정

금융위원회고시 제2018-36호, 2018. 12. 21., 일부 개정

제20조

(정보처리시스템 구축 및 전자금융거래 관련 사업 추진)

4. 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 분석 · 설계 단계부터 보안대책을 강구할 것

규정 3 ISMS-P

1. 관리체계 수립 및 운영(16개)
2. 보호대책 요구 사항(64개)

2.8 정보시스템 도입 및 개발보안

인증기준 : 정보시스템의 도입 · 개발 또는 변경 시 정보보호 및 개인정보보호 관련 법적 요구사항, 최신 보안취약점, 안전한 코딩방법 등 보안 요구사항을 정의하고 적용하여야 한다.

규정 4 SW진흥법

2020.12.10 개정안 시행

제29조(소프트웨어개발보안 진흥)

과학기술정보통신부장관은 소프트웨어개발보안을 진흥하기 위하여 다음 각 호의 사업을 추진

제30조(소프트웨어안전 확보)

정부는 소프트웨어안전 확보를 위한 시책을 마련

과학기술정보통신부장관은 소프트웨어안전 확보를 위한 지침을 정하여 고시

제27조 6호(소프트웨어개발보안 진흥 등)

개발보안 적용여부 확인을 위한 이행점검이 필수적이므로 이를 명시

H/W 및 S/W 사양

H/W 권장사항

구분	최소 사양
CPU	· Intel XEON 3.0Ghz Quad Core 이상
MEMORY	· 권장: 32GB 이상
HDD	· 최소: 500GB 이상 · 권장: 1TB 이상 (분석 소스 코드 용량에 따라 변동)
NIC	· 10/100/1000MB 이더넷 1개 포트
ETC	· 대용량 분석 시 SSD 권장

S/W 요구사항

구분	요구 사양
OS	· RedHat 8.x or 9.x 64bit · Oracle Linux 8.10 64bit (Redhat 8.x 계열)
WAS	· Spring Boot 2.6.6
DBMS	· PostgreSQL V16
JAVA	· Openjdk-17.0.0.1
암호화 라이브러리	· Java Cryptography Extension (JCE)

주요 고객사

공공	한국도로공사, 한국지역난방공사, KLID 한국지역정보개발원, 금융보안원, 국세청, 법무부, 교육부, 한국원자력안전기술원, 공무원연금공단	외 다수
금융/일반	애큐온저축은행, 유안타증권, DB저축은행, 하나금융TI, 한화자산운용, IBK신용정보, 인하대병원, 삼성창원병원, SK 주식회사, 삼성물산	외 다수
지자체/교육	용인시, 대구광역시, 영주시, 광주시, 의왕시, 인천대학교, 호서대학교, 동국대학교, 성결대학교, 원광대학교	외 다수
컨설팅	해뜨는 서산, BPA 부산항만공사, KISA 한국인터넷진흥원, 한국정책방송원 KTV 국민방송, (주)씨에이에스, (주)한국정보기술단, KERIS 한국교육학술정보원, 경찰청, NIA 한국지능정보사회진흥원, 강원특별자치도	외 다수





서울시 구로구 디지털로26길 111, JNK디지털타워 1606호
TEL 02-6240-6000 FAX 02-6959-0130

SSR (주)에스에스알