TRINITY SOFT

CODE-RAY XG V6.0

제품소개서

|주|트리니티소프트 | www.trinitysoft.co.kr

TRINITY SOFT

CONTENTS

I 제안 개요

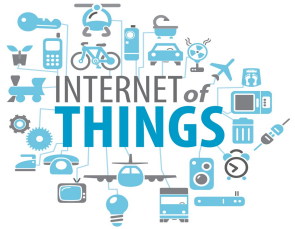
1. 시큐어코딩 필요성
2. 소프트웨어 개발보안
3. 시큐어코딩 관련 규정

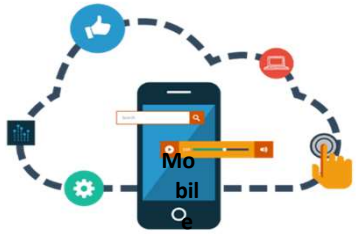
1. 시큐어코딩의 필요성

4차 산업의 핵심! SW

4차 산업이란 **모든 산업 분야에 정보통신 기술이 융합된 산업**으로 빅데이터, 인공지능, 로봇공학, 사물 인터넷 등이 있으며 4차 산업의 핵심기술은 **SW 기술**이며, SW의 핵심은 **코딩**입니다.

"소프트웨어가 중심이 되는 세상"



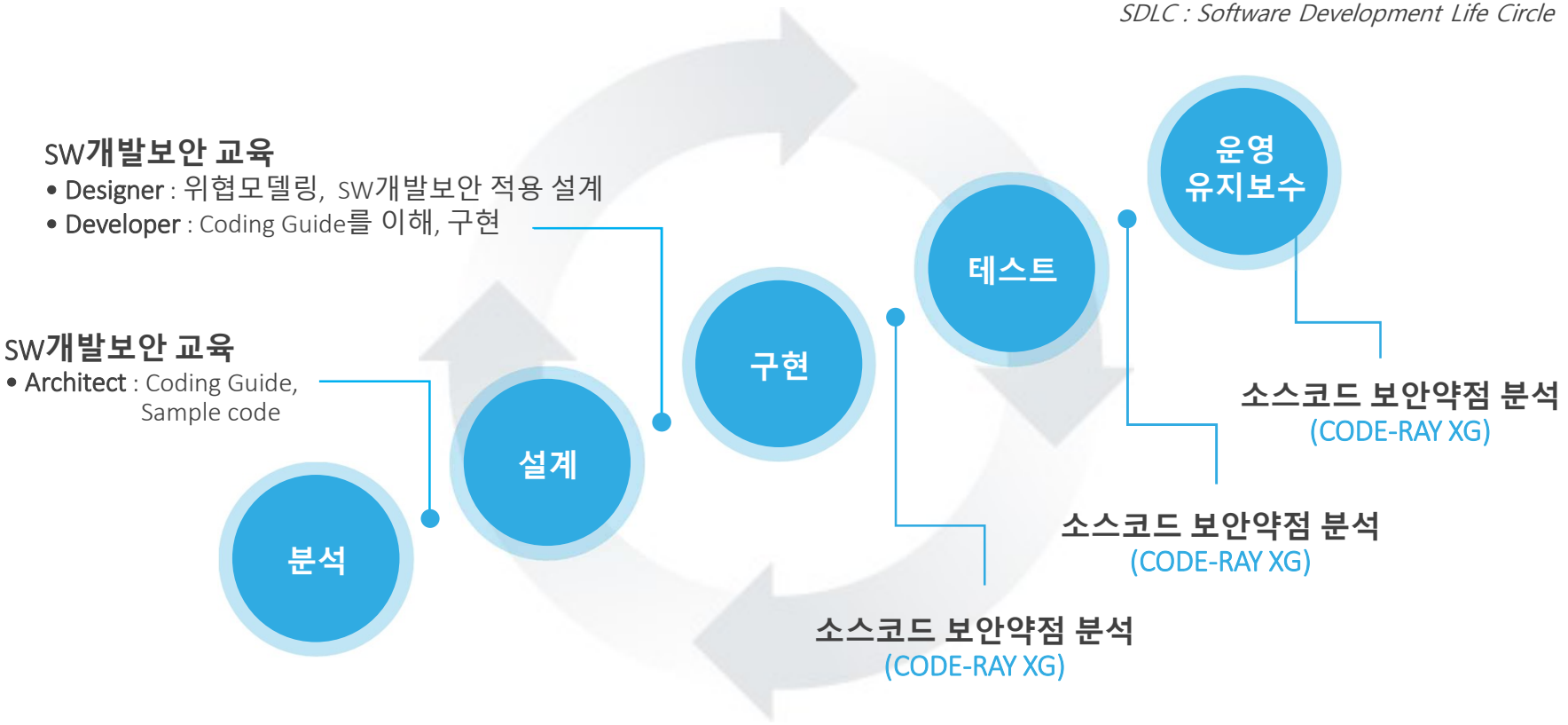


시큐어코딩 이란

SW 개발과정에서 개발자 실수, 논리적 오류 등으로 인해 **SW에 내재된 보안약점을 최소화**하는 한편, 해킹 등 보안위협에 대응 할 수 있는 **안전한 SW를 개발하기 위한 일련의 과정**을 의미합니다.

SDLC에서의 SW 개발보안 적용 방안

SDLC : Software Development Life Circle



3. 시큐어코딩 관련 규정

관련 규정

규정 1 행정안전부 고시

2021년1월19일 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 전자금융감독규정

- 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 SW산업진흥법

2020년12월10일 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 필수적**이므로 이를 명시

TRINITY SOFT

Ⅱ 제품 개요

1. 제품 개요
2. 제품 구성도
3. 환경 정보

1. 제품 개요

CODE-RAY XG V6.0

'소스코드 보안약점 분석도구' 로서 소프트웨어의 분석/설계, 구현, 테스트, 운영단계에서 발생 할 수 있는 소스코드의 보안약점을 관리하기 위해 **프로젝트 및 사용자 통합 관리, 프로젝트 보안약점 분석, 형상관리 연동** 등 소스코드 통합보안관리 기능을 제공합니다.

제품명	▪ CODE-RAY XG V6.0
인증	▪ 2021년 3월 'CODE-RAY XG V6.0' 조달 등록 ▪ 2020년 11월 'CODE-RAY XG V6.0' CC인증, GS인증 획득 ▪ 2020년 10월 'CODE-RAY XG V6.0' 전자정부 프레임워크 호환성 인증 획득
주요기능	▪ 그룹 단위 프로젝트 별 룰셋, 사용자, 점검결과 통합관리 지원 ▪ 보안약점의 원인 및 패턴을 분석하여 그룹화 조회 및 관리 제공 ▪ SVN, GIT 등 외부 형상관리 연동 기본 지원 ▪ 보안약점이 발생된 원인을 추적하면서 확인 가능한 네비게이션 기능 제공 ▪ 보안약점 수정/관리를 위한 개발자 TASK 할당/관리 기능 지원 ▪ 원인 중심의 오탐 중복 방지 기법을 이용한 예외처리 지원

강력한 분석엔진

- 보다 빠르고 정확한 신규 엔진 탑재
- 빌드과정, 개발환경구축 없이 소스코드만으로 분석
- AST 구조 분석을 통하여 Data/Control Flow, 패턴분석, Configuration, semantic 등 다양한 분석 지원

WEB 기반 솔루션

- WEB기반의 SW타입으로 간편한 설치 지원
- 최신 UI/UX 적용 및 테마 기능 지원
- WEB 기반의 관리 및 점검도구 지원
- WEB기반으로 가상환경 지원 용이

다양한 컴플라이언스

- SW개발보안 가이드 49개 항목, 국가정보원 8대 취약점,, 전자금융감독규정, OWASP TOP 10, CWE/SANS TOP 25 등의 컴플라이언스 지원
- Java, JSP, Javascript, ASP, ASP.Net, PHP, HTML, C/C++, C#, Python, XML, Properties, Android, Objective-C, SWIFT 등의 점검언어 지원

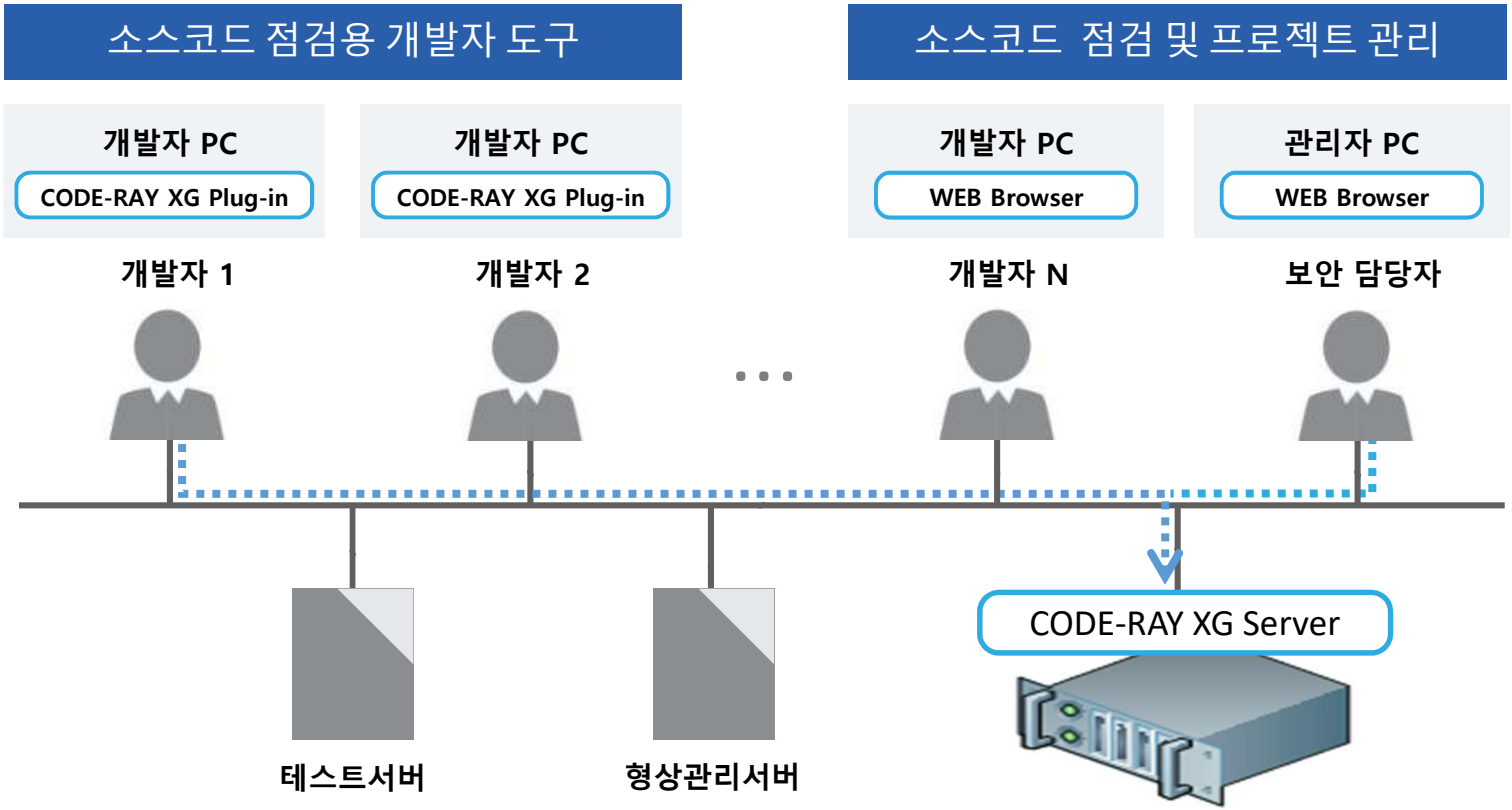
통합 관리 기능

- 그룹 단위 프로젝트 통합관리 지원
- 통합 대시보드를 통한 보안경보 레벨, 탐지/원인 건수 등 다양한 정보 제공
- 보안약점 상태관리 기능 지원

2. 제품 구성도

CODE-RAY XG V6.0

'소스코드 보안약점 분석도구'로서 Server, Client(WEB, IDE Plug-In, CLI)로 구성되어 있으며,
관리자는 WEB기반 관리도구를 통해서 프로젝트와 사용자에 대한 통합관리 및 소스코드 점검이 가능하며,
개발자는 WEB기반 점검도구, IDE Plug-In을 이용하여 소스코드 점검이 가능합니다.



3. 환경 정보

CODE-RAY XG V6.0

SW타입의 시큐어코딩 솔루션으로 H/W 및 S/W 요구사항을 만족하는 장비를 이용하여 다수의 개발자가 동시에 작업을 수행하는데 최적화 되어 있습니다.

H/W 권장사항

구분	최소 사항
CPU	• Intel Quad Core 3.0Ghz 이상
MEMORY	• 권장 : 16GB 이상
HDD	• 권장 : 500GB 이상 • 대용량 분석 시 SSD 권장 • 분석 소스 코드 용량에 따라 변동
ETC	• 10/100/1000MB 이더넷 1개 포트
OS	• Oracle Linux 7.x 또는 8.x 64bit (8 권장) • RedHat Enterprise 7.x 또는 8.x 64bit (8 권장) • CentOS 7.x 또는 8.x 64bit (7 권장)

S/W 요구사항

구분	요구 사항
WAS	• Spring Boot 2.1.8
DBMS	• PostgreSQL V12.2
JAVA	• Openjdk-9.0.4
암호화 라이브러리	• Java Cryptography Extention (JCE)
WEB Browser	• Chrome 64bit (v84.0 이상) • Microsoft Edge 64bit (v84.0 이상)

CODE-RAY 설치 시 포함

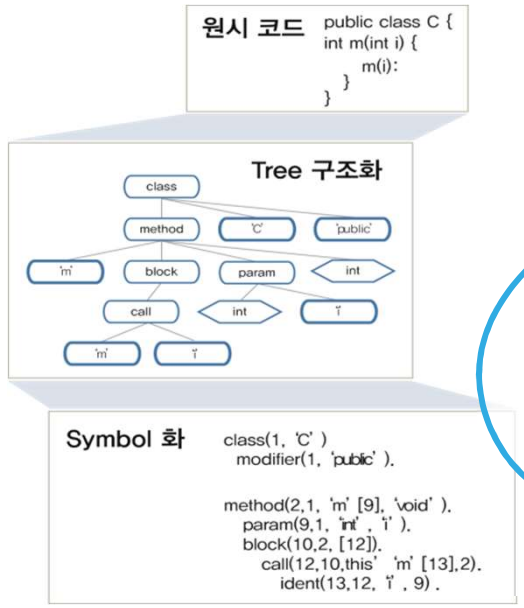
Ⅲ 주요 기능

1. 분석 매커니즘
2. 다양한 점검 언어 및 점검 기준
3. 다양한 점검 방법
4. 통합 대시보드
5. 보안약점 상세 조회
6. 다양한 리포트 제공

가상컴파일 / Non Compile

- 원시코드를 AST로 구조화한 후에 보안약점 식별 및 분석 가능한 가상 컴파일 방식 지원
- 형상관리 연동 시 체크아웃 후 컴파일 없이 바로 분석 가능

가상컴파일을 통한 정적분석

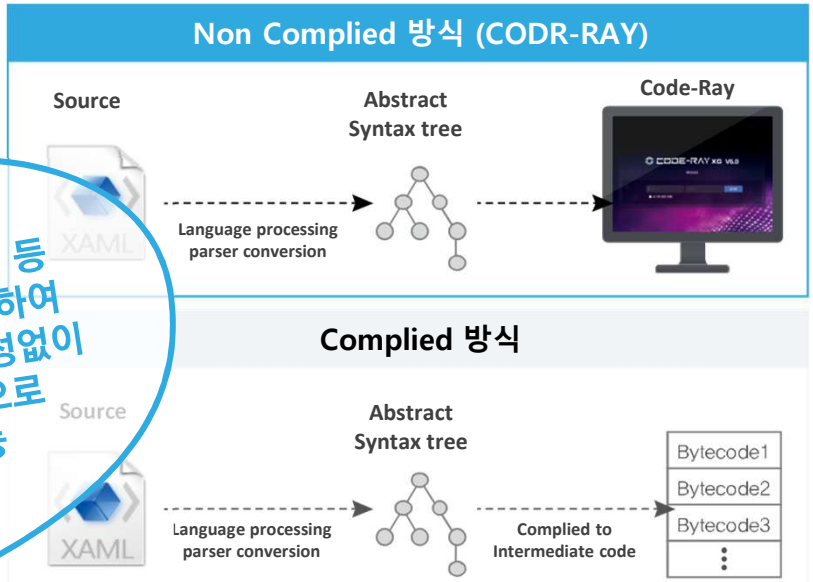


JAVA, C/C++ 등 지원 언어에 대하여 컴파일 환경 구성없이 소스코드만으로 분석 가능

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 분석



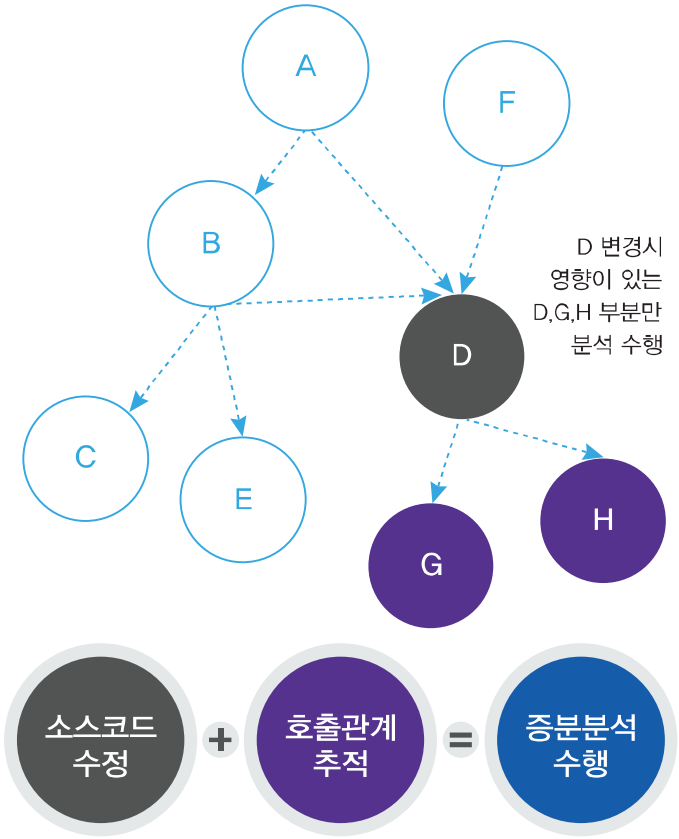
	Non Complied	Complied
분석 방식	가상컴파일을 통해 AST 구조를 생성함	실제 컴파일을 통해 AST 구조를 생성함
빌드 구성	빌드 환경 구성이 필요치 않음	빌드 환경 구성이 필요 취약점 분석 시간이 오래 걸림

연관관계 분석/증분 분석

- 다계층 개발환경의 여러 소스가 연계된 프로그램의 통합 연관 분석을 지원
- 추가/변경된 소스코드에 대하여 호출관계를 추적하여 증분 분석을 지원

다 계층 소스코드 간 연관관계 분석

증분 분석



2. 다양한 점검 언어 및 점검 기준

점검 언어 / 점검 기준

• 강력한 분석엔진을 이용하여 다양한 점검 언어와 점검 기준을 지원

다양한 점검 언어 지원

환경	지원 언어
개발 언어	JAVA, JSP, javascript, ASP, ASP.Net, PHP, HTML, VBScript, HTML5, C/C++, Visual C++, C#, Python, XML 등
모바일 언어	JAVA(안드로이드), Objective-C(IOS), SWIFT

다양한 점검 기준 지원

기준	Compliance 지원
국내 점검 기준	SW개발보안가이드 49개 항목, 모바일 기준 국가정보원 홈페이지 8대 취약점 전자금융감독규정
국외 점검 기준	CWE/SANS Top 25, CWE OWASP Top10, OWASP Mobile Top 10 PCI-DSS

3. 다양한 점검 방법

CODE-RAY XG V6.0

운영환경에 따라 소스코드 보안약점 분석에 대한 다양한 방식을 제공합니다.

보안약점 분석

업로드

압축파일
업로드 점검

로컬 점검

로컬 파일시스템의
경로 점검

형상관리 연동

SVN, GIT 등 형상관리
서버와의 연동 점검

IDE 개발도구

Eclipse, IntelliJ,
Android Studio 등
개발도구 점검

CLI (Command Line Interface)

명령어를 이용한
프로젝트 점검

4. 통합 대시보드

전체 대시보드

전체 프로젝트에 대한 현황정보를 확인 할 수 있는 통합 대시보드를 제공합니다.

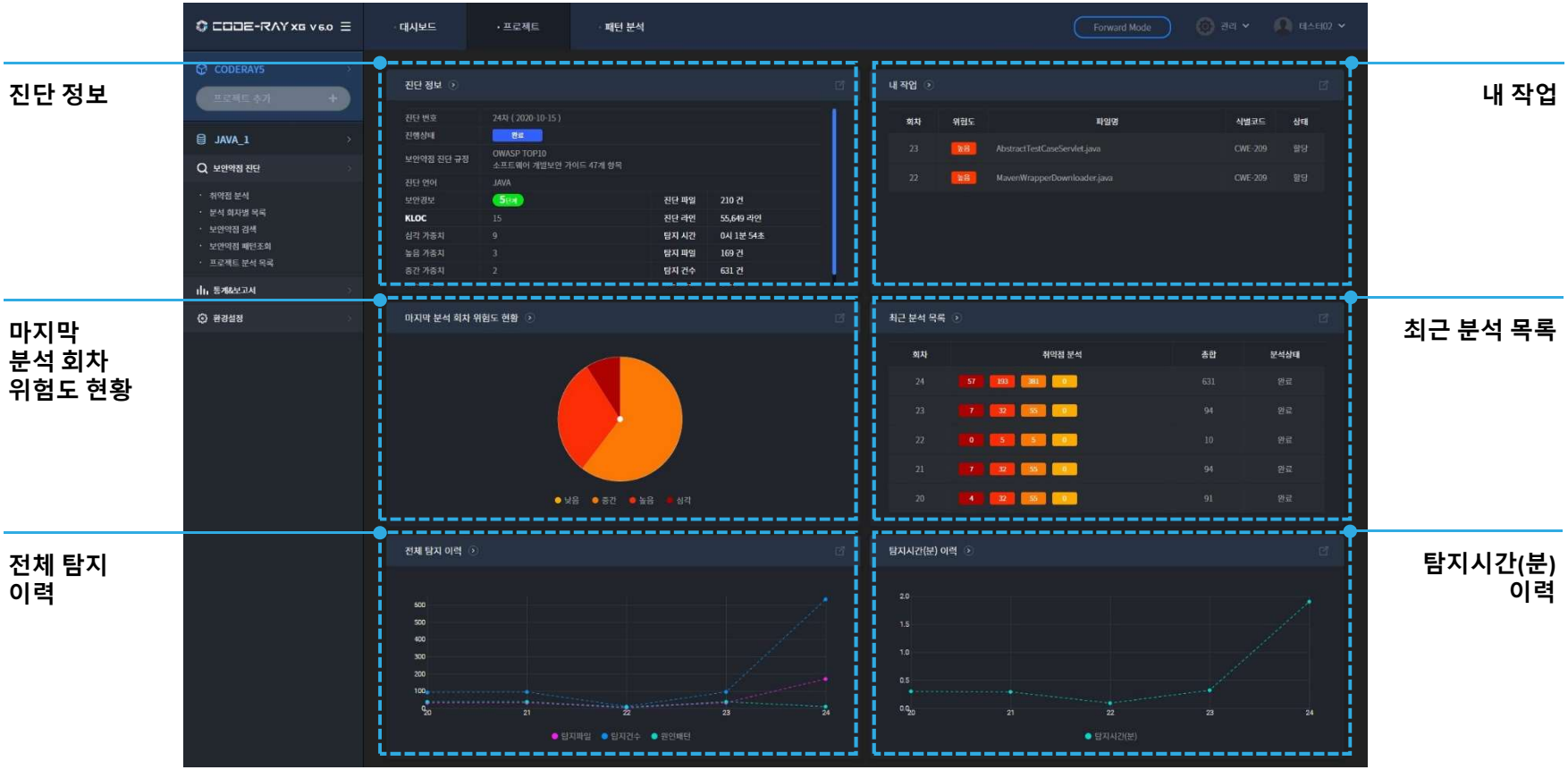
통합 대시보드

4. 통합 대시보드

프로젝트 대시보드

그룹 별 프로젝트에 대한 현황정보를 확인 할 수 있는 프로젝트 대시보드를 제공합니다.

프로젝트 대시보드

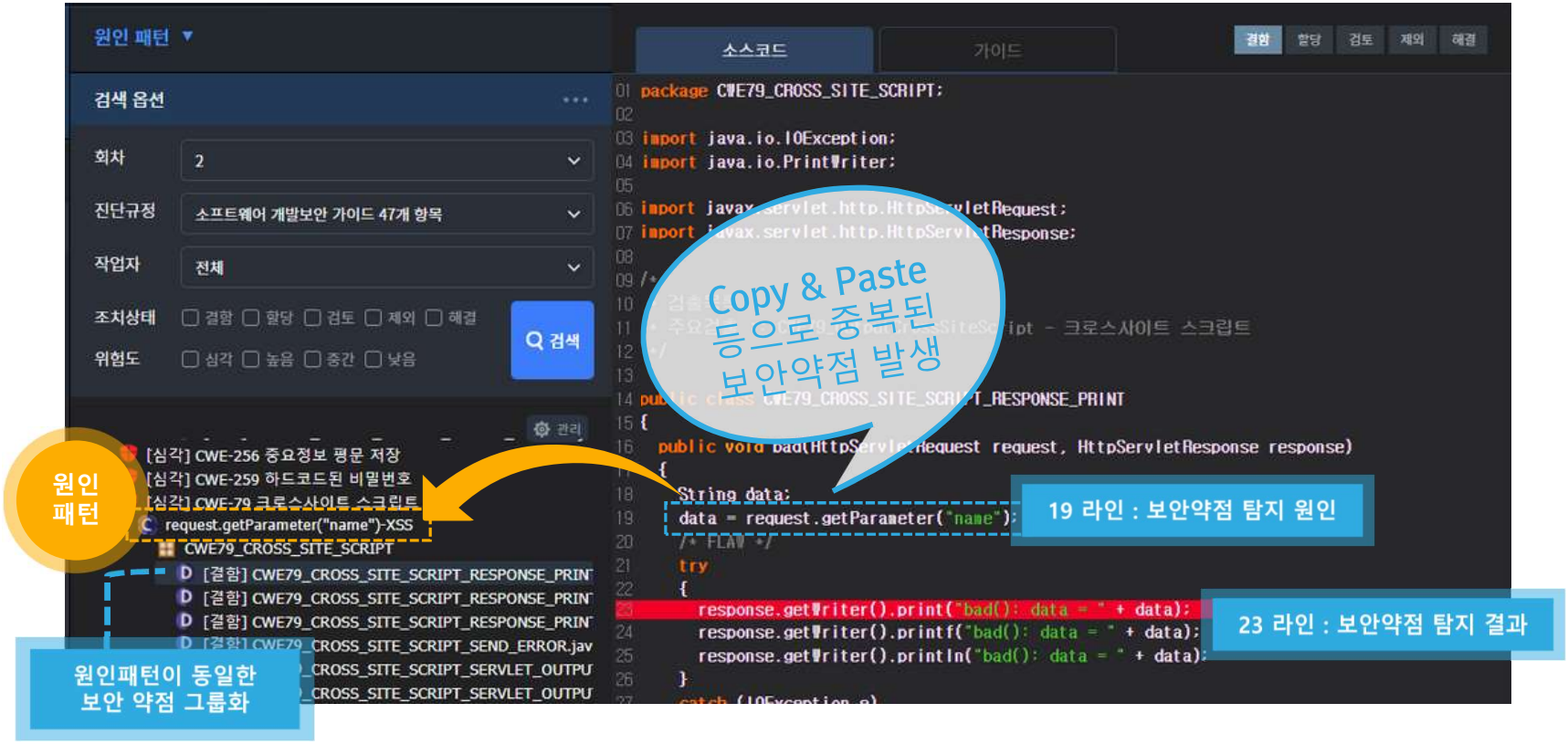


5. 보안약점 상세 조회

Intelligent Pattern Search

탐지된 보안약점의 원인 및 패턴을 분석하여 그룹화 조회를 제공하며, 유사한 보안약점들을 보다 빠르게 확인하고 공통 원인패턴을 수정 함으로 시큐어코딩 적용 시간을 단축할 수 있습니다.

지능형 패턴 조회



5. 보안약점 상세 조회

Intelligent Pattern Search

탐지된 보안약점에 대하여 정/오탐 판단이 용이한 보안약점 추적 네비게이션 기능을 제공 합니다.

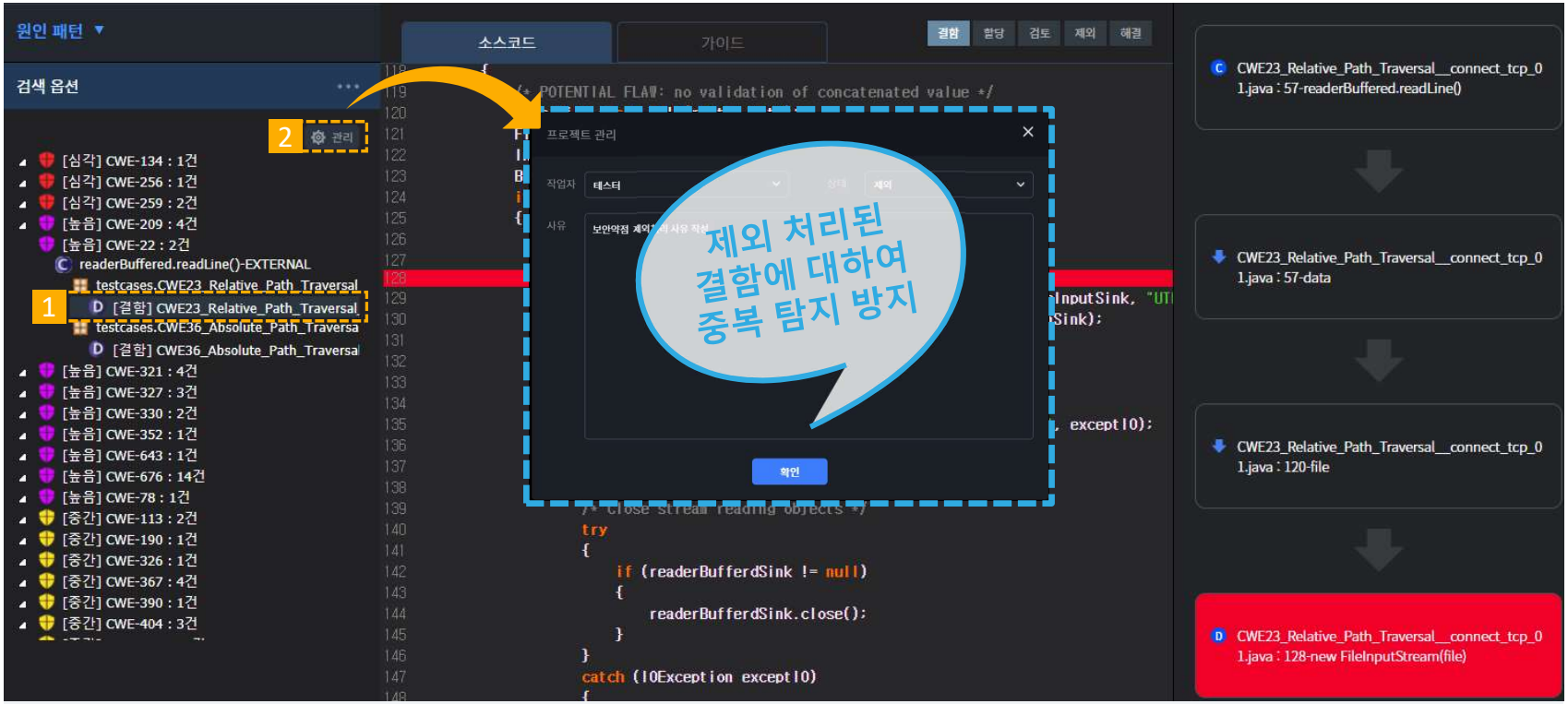
보안약점 추적 네비게이션

5. 보안약점 상세 조회

Intelligent Pattern Management

탐지된 보안약점에 대하여 결함, 할당, 검토, 제외 등의 상태관리 기능을 제공하며,
식별이 불필요한 결과에 대하여 제외처리를 지원 합니다.

지능형 패턴 관리 (제외처리)



개발자가 검토 요청한 결함에 대하여 관리자가 알람 확인 후 제외처리 적용

6. 다양한 리포트 제공

보안약점 분석 보고서

분석된 결과에 대하여 점검기준 별 요약, 상세, 이행, 로우데이터 보고서 등 다양한 포맷 (PDF, DOCX, HWP, EXCEL)의 형태로 제공합니다.

다양한 종류 및 포맷의 리포트

요약 보고서

: 탐지된 보안약점에 대한 요약 정보 제공

상세 보고서

: 탐지된 보안약점에 대한 요약, 상세 정보 제공

이행 보고서

: 탐지된 보안약점에 대한 회차별 히스토리 정보 제공

로우데이터 보고서

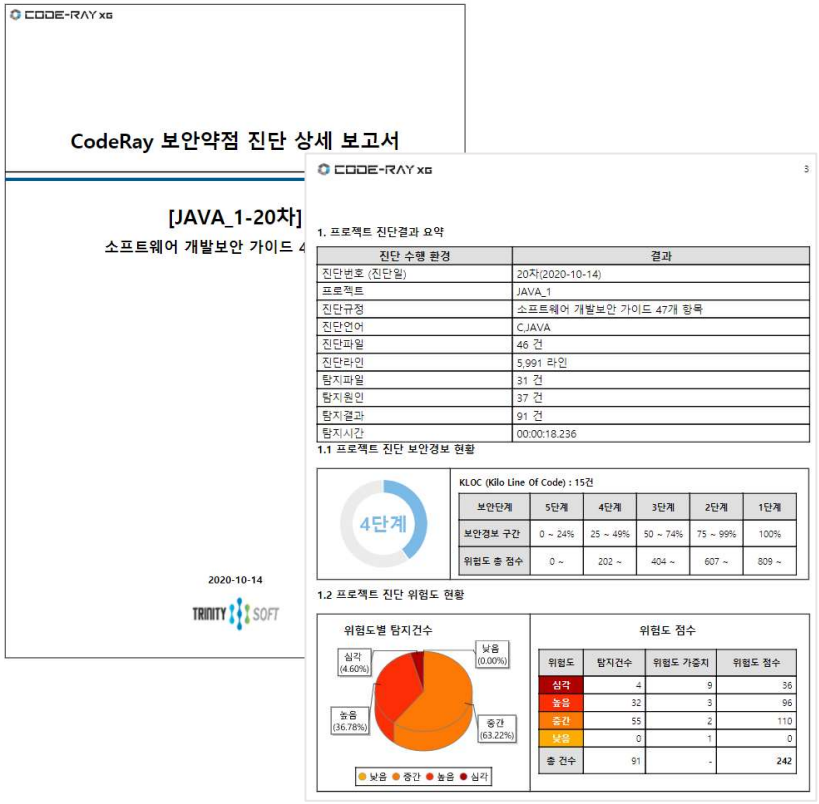
: 탐지된 보안약점에 대한 로우데이터 정보 제공

다양한 점검 기준 별 보고서

: 행안부 47개 항목, 국정원8대 취약점, 전자금융감독규정 등 제공

지원 포맷

: PDF, DOCX, HWP, EXCEL 등 지원



CODE-RAY xG

CodeRay 보안약점 진단 상세 보고서

[JAVA_1-20차]

소프트웨어 개발보안 가이드 4

2020-10-14

TRINITY SOFT

CODE-RAY xG

1. 프로젝트 진단결과 요약

진단 수행 환경	결과
진단번호 (진단일)	20차(2020-10-14)
프로젝트	JAVA_1
진단규정	소프트웨어 개발보안 가이드 47개 항목
진단언어	C,JAVA
진단파일	46 건
진단라인	5,991 라인
탐지파일	31 건
탐지원인	37 건
탐지결과	91 건
탐지시간	00:00:18.236

1.1 프로젝트 진단 보안경보 현황

4단계

KLOC (Kilo Line Of Code) : 15건

보안단계	5단계	4단계	3단계	2단계	1단계
보안경보 구간	0 ~ 24%	25 ~ 49%	50 ~ 74%	75 ~ 99%	100%
위험도 총 점수	0 ~	202 ~	404 ~	607 ~	809 ~

1.2 프로젝트 진단 위험도 현황

위험도별 탐지건수

심각 (4.60%)
낮음 (0.00%)
높음 (36.78%)
중간 (63.22%)
낮음 중간 높음 심각

위험도 점수

위험도	탐지건수	위험도 가중치	위험도 점수
심각	4	9	36
높음	32	3	96
중간	55	2	110
낮음	0	1	0
총 건수	91	-	242

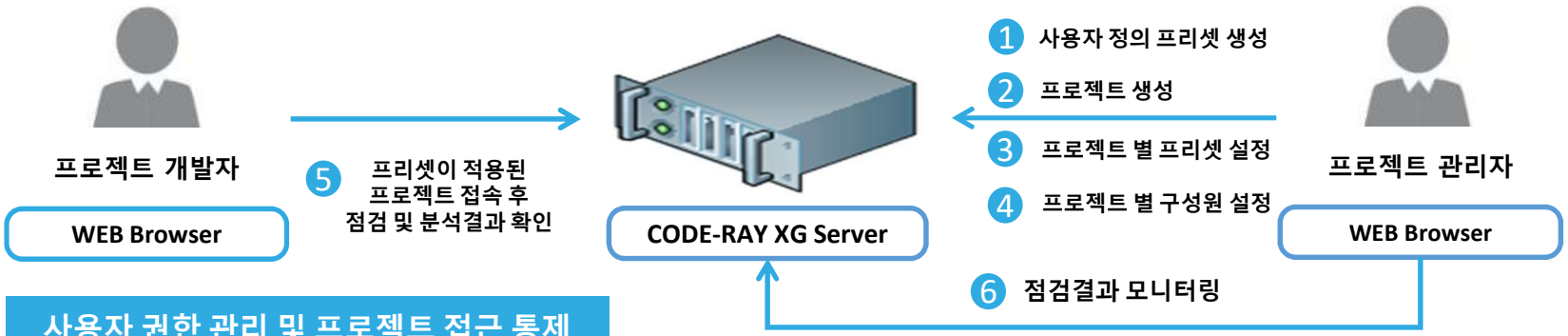
IV 운영방안

1. 통합관리 방안
2. 다양한 점검 방안

프로젝트 통합관리

관리자가 중앙에서 프로젝트 생성 후 점검정책 및 구성원 설정을 통하여
개발자들이 소스코드 점검이 가능하며, 분석된 결과는 중앙에서 통합관리 가능합니다.

중앙에서 점검정책 관리 및 배포



사용자 권한 관리 및 프로젝트 접근 통제

계정 역할	권한
슈퍼 관리자	모든 관리 기능 (최초 생성 계정, 추가 x)
시스템 관리자	모든 관리 기능 - 프로젝트/그룹 관리 - 사용자/그룹 관리 - 점검 기준 관리 (프리셋) - 체커 관리
시스템 파워유저	프로젝트 관리 (할당 프로젝트 조회, 수정) - 그룹/프로젝트 생성 - 체커 관리
시스템 일반유저	관리 기능 미제공

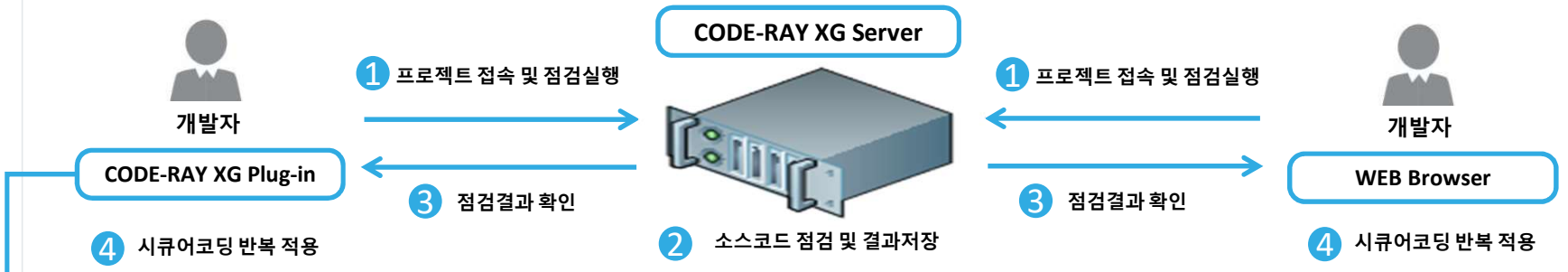
프로젝트 구성원	권한
프로젝트 관리자	보안약점 분석/결과 조회 보안약점 상태 관리 - 결함, 할당, 검토, 제외, 해결
프로젝트 개발자	보안약점 분석/결과 조회 보안약점 검토 요청

2. 다양한 점검 방안

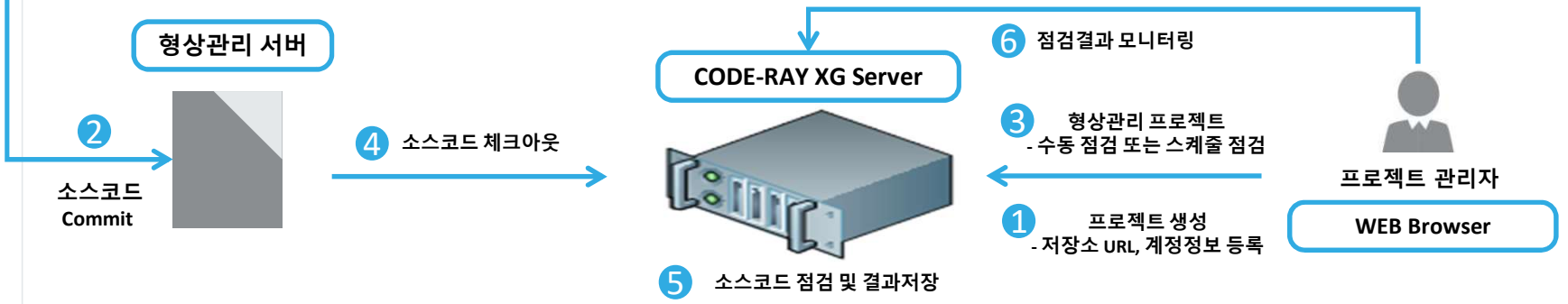
소스코드 점검 방안

WEB 기반 점검과 IDE Plug-In 점검을 지원하며, 저장소 URL과 저장소 계정정보 등록만으로 형상관리에 대한 손쉬운 점검을 지원합니다.

WEB / Plug-In 점검 (자가 점검)



SVN/GIT 형상관리 연동 점검 (전수 점검/스케줄 점검)



TRINITY SOFT

V 특장점 및 기대효과

1. 특장점
2. 기대효과

1. CODE-RAY XG V6.0 특장점

강력한 신규 엔진 탑재

- 보다 빠르고 정확한 신규 엔진 탑재
- 속도 개선 및 실행 흐름 추적 강화
- 보다 편리한 탐지규칙 관리 기능 지원
- 에러처리 등 안전성 강화

가상컴파일/ Non-Compile 방식

- 모든 지원 언어에 대하여 소스코드만으로 점검 지원
- 컴파일러에 의한 빌드환경 설정 불필요
- 형상관리 연동 시 체크아웃 후 컴파일 과정 없이 바로 분석 가능
- 소스코드 간의 연관 분석 및 증분 분석

다양한 연동 지원 (DevSecOps)

- SVN, GIT 형상관리 점검 기본 지원
- 보안경보레벨 - 시큐어코딩 만족도 체크
- ViewTable 을 통한 통계 정보 제공
- CLI 를 통한 점검 지원
- AD 연동 지원

Intelligent Pattern DashBoard (지능형 패턴 대시보드)

- 탐지된 보안약점의 패턴을 시각화 및 추적하여 검색 제공
- 프로젝트의 전체 결함, 보안약점 별 패턴 별 결함 건수 제공

Intelligent Pattern Search (지능형 패턴 조회)

- 탐지된 보안약점의 원인 및 패턴을 분석 하여 그룹화된 결함 제공
- 공통 원인패턴을 수정 함으로 시큐어코딩 적용 시간을 단축
- 유사한 보안약점들을 보다 빠르게 조회

Intelligent Pattern Management (지능형 패턴 관리)

- 탐지된 보안약점의 결함, 할당, 검토, 제외 등의 상태 관리 기능 제공
- 탐지된 보안약점의 원인 및 패턴을 분석 하여 그룹화된 결함의 상태 일괄 처리 제공
- 탐지된 보안약점에 대하여 점검기준, CWE번호, 등으로 검색 후 일괄 상태 처리 제공

2. CODE-RAY XG V6.0 기대효과

기대효과

CODE-RAY XG를 도입하여 지속적인 취약점 점검 체계를 마련하여
해킹 등의 악의적인 보안 위협으로부터 안정적인 서비스를 제공할 수 있습니다.

S/W 보안취약점 사전제거

취약점 사전 진단 및 자산 보호

- S/W 취약점에 대한 사전 예방
- 개발 보안에 대한 방향 제시 및 품질 향상
- 어플리케이션 소스코드 개발 단계에서 보안약점의 사전 점검 및 제거
- 기 배포/운영 중인 소스코드 보안약점의 일괄 점검

지속적인 취약점 점검 체계 구축

시큐어코딩 시스템 구축

- 개발 및 유지보수 과정에서 보안약점을 점검할 수 있는 체계확보
- 개발자의 프로그램 작성 및 기법 등에 대한 명확한 기준 정립
- 어플리케이션 소스코드 배포, Check-In시 보안약점 점검 및 배포 통제 방안 확보
- 향후 신규 추가되는 어플리케이션 취약점의 신속한 점검 및 대응 방안 확보

컴플라이언스 이슈 준수

다양한 점검 기준 제공

- 초기 개발단계부터 체계적인 소스코드 관리 및 분석 (정보화 업무의 행정안전부 고시 2017-7호)
- 정적 분석 솔루션 구축으로 시큐어코딩 관련 가이드 준수
- 다양한 점검기준 (OWASP TOP 10, Mobile Top 10, 행안부 47개, PCI-DSS, CWE/SANS, 전자금융감독규정 등)

VI 레퍼런스

1. 정부중앙행정기관
2. 지방자치단체, 교육기관
3. 금융기관, 일반기업, 기타
4. 소스코드 보안약점 진단 컨설팅

레퍼런스

감리/인증 업체 활용

정보시스템감리협회 전략적 협력 관계 체결

전자신문 Conference allshowTV ETEdu English

통신&방송 SW&게임&성장기업 소재&부품 전자&자동차&유통 경제&금융 산업&과학&정책 전국

트리니티소프트, 정보시스템감리협회와 '시큐어코딩' 솔루션 협력

발행일 : 2021.03.09

[올쇼TV] 다이나트레이스, 디지털 트랜스포메이션 전략 소개 (3/11 생방송)

<(왼쪽부터) 하재진 트리니티소프트 영업팀장, 이충호 정보시스템감리협회 감사, 김진수 트리니티소프트 대표, 정현수 정보시스템감리협회 수석부회장이 전략적 협력 계약을 체결했다. 트리니티소프트 제공>

트리니티소프트가 정보시스템감리협회와 시큐어코딩 솔루션 '코드레이 엑스지'에 대한 전략적 협력 계약을 체결했다.

트리니티소프트는 이번 계약을 통해 정보시스템감리협회 회원사를 대상으로 시큐어코딩 진단 도

70개 이상 감리업체 CODE-RAY XG 감리 활용

< 출처 : 전자신문 >

CC인증 기관 및 보안 업체 지속적 도입 및 운영

<코드레이 엑스지 V6.0. 트리니티소프트 제공>

트리니티소프트가 한국기계전기전자시험연구원(KTC)에 소프트웨어(SW) 개발보안 솔루션 '코드레이 엑스지 V6.0'을 공급했다.

이번 공급으로 회사 측은 한국시스템보증(KOSYAS), 한국아이티평가원(KSEL), 한국정보[illegible](KOIST)까지 총 4개 공통평가기준(CC) 인증 평가기관을 레퍼런스로 확보하게 됐다.

'코드레이 엑스지 V6.0'은 시큐어코딩 솔루션이다. SW 개발 공정에서 발생 가능한 소스코드 보안 약점을 분석·관리하기 위해 다양한 점검 방법과 프로젝트 통합 관리 기능을 제공한다. CC인증과 GS인증을 동시에 획득했다.

안랩, 윈스, 소만사 등 국내 주요 보안 업체[illegible] V6.0'을 이미 도입한 상태다. 트리니티소프트는 [illegible]

김진수 트리니티소프트 대표는 "이번 수주는 [illegible] 인증 평가기관으로부터 발주여서 의미가 크다"고 [illegible]

오다인기자 ohdain@etnews.com

KTC, KOSYAS, KSEL, KOIST 등 CC인증 기관 CODE-RAY XG 도입

< 출처 : 전자신문 >

1. 정부중앙행정기관, 공사, 공단, 산하기관

- 국가정보원
- 대검찰청
- 경찰청
- 산림청
- 식품의약품안전처
- 한국철도공사
- 한국도로공사
- 한국석유공사
- 대한석탄공사
- 한국가스기술공사
- 서울도시철도공사
- 한국관광공사
- 한국지역난방공사
- 교통안전공단
- 한국환경공단
- 한국원자력환경공단
- 공무원연금공단
- 한국환경산업기술원
- 한국지역정보개발원
- 한국건설기술연구원
- 한국농수산물식품공사
- 한국정책방송원
- 한국임업진흥원
- 축산물품질평가원
- 국군기무사령부
- 국가기술표준원
- 기초과학연구원
- 전략물자관리원
- 한국법제연구원
- 한국행정연구원
- 한국영상자료원
- 한국인터넷진흥원
- 한국형사정책연구원
- 한국국제협력단
- 한국노인인력개발원
- 우정사업본부
- 질병관리본부
- 산업통상자원부
- 교육부
- 국립중앙도서관
- 세외수입 정보화사업단
- 위택스(지방세 인터넷 납부시스템)
- 사회보장정보원
- 온실가스종합정보센터
- 대한체육회
- 한국문화예술위원회
- 게임물관리위원회
- 정부청사관리본부

2. 지방자치단체, 교육기관

- 서울특별시청
- 서울특별시 마포구청
- 경기도 수원시청
- 경기도 안양시청
- 경기도 광주시청
- 경기도 과천시청
- 경기도 부천시청
- 경기도 파주시청
- 경기도 용인시청
- 경기도 안성시청
- 경기도 의왕시청
- 경기도 의정부시청
- 경기도 연천군청
- 대구광역시청
- 대구광역시 남구청
- 대구광역시 북구청
- 경북 포항시청
- 경북 안동시청
- 경북 영주시청
- 경북 영천시청
- 경북 상주시청
- 경북 영양군청
- 경북 구미시청
- 경남 창원시청
- 경남 하동군청
- 제주특별자치도 서귀포시청
- 서울소방재난본부
- 서울 서대문 경찰청
- 인천교통공사
- 경기도인재개발원
- 대구디지털산업진흥원
- 창원경륜공단
- 인천U시티
- 서울특별시교육청
- 경기도파주교육청
- 광주광역시교육청
- 제주도교육청
- 경북대학교
- 공주대학교
- 충청대학교
- 한남대학교
- 부천대학교
- 우석대학교
- 호남대학교
- 한국폴리텍대학교(강서)
- 원광대학교
- 대림대학교
- 협성대학교
- 성결대학교
- 호서대학교

3. 금융기관, 일반기업, 기타

- 삼성전자
- SK증권
- SK엔카
- 안랩
- 삼성창원병원
- 하나금융티아이
- 애큐온저축은행
- 사학연금
- 메트라이프생명
- 한국마사회
- 한국지방재정공제회
- 포항산업과학연구원
- 중소기업중앙회
- 전문건설공제조합
- 전국렌터카공제조합
- 웨이버스
- 메디오피아테크
- 이지팜

- 삼성물산
- SK C&C
- SK 인포섹
- LG CNS
- LG엔시스
- LG유플러스
- 인천국제공항
- 제주국제자유도시개발센터
- 대한적십자사
- 한국국제교류재단
- 한국정보기술단
- 타임게이트
- 시공미디어
- 에이앤디신용정보
- 코어스넷
- 에이텍아이엔에스
- 소만사
- 케이에스솔루션

- 현대카드
- 한화S&C
- 한화호텔&리조트
- 한화자산운용
- GS리테일
- 현대홈쇼핑
- 웅진홀딩스
- 네이버시스템
- BMW파이낸셜
- 웨어밸리
- 한국ICT융합협동조합
- 어빌리티시스템즈
- 아이퀘스트
- 지니언스
- E1
- 이나인페이
- 나이스페이먼츠
- 윈스

4. 소스코드 보안약점 진단 컨설팅 (공공기관, 산하기관)

4. 소스코드 보안약점 진단 컨설팅 (지방자치, 교육기관, 일반기업)

TRINITY SOFT

Thank you