SYNOPSYS®

KMS Technology

Coverity

정적 분석

코딩 중 중대한 보안 및 품질 이슈를 신속히 발견하여 해결

이점

- **향상된 보안 위험 가시성 제공.** 교차 제품 보고 기능은 동급 최고의 AppSec 도구를 이용하여 프로젝트의 위험에 대한 종합적이고 완전한 가시성을 제공합니다
- **배포 유연성.** 온프레미스 또는 클라우드 중 AppSec 테스트를 실행할 프로젝트 집합을 선택할 수 있습니다.
- **초기부터 보안 테스트 적용.** 개발자들은 코딩 단계부터 몇 초 만에 높은 신뢰도의 분석 결과를 얻을 수 있어 빌드 테스트 전에 미리 이슈를 해결할 수 있습니다.
- **개발자 지원.** 이슈 해결 방법을 찾기 위해 필요한 모든 컨텍스트, 상세 정보 및 조언을 개발팀에 제공하여 소프트웨어 결함을 신속하고 쉽고 정확하게 해결합니다.
- **상황별 eLenaring** (eLearning 고객 대상) 개발자의 자체 코드에서 확인된 CWE에 특정한 상황별 eLearning(eLearning 고객 대상)은 필요할 때 즉각적인 보안 교육을 제공합니다. 따라서 개발자가 굳이 보안 전문가가 될 필요가 없습니다.

개요

Coverity®는 고품질의 안전한 애플리케이션 개발에 필요한 속도, 편의성, 정확성, 산업 표준 준수 및 확장성을 제공합니다. Coverity는 비용이 가장 적게 들고 수정이 가장 쉬운 개발 프로세스 초기에, 작성된 코드에서 중요한 소프트웨어 품질 결함과 보안 취약점을 식별합니다. 정확하고 실용적인 취약점 해결 정보와 상황별 eLearning을 통해 보안 전문가가 아니더라도 우선순위에 따라 신속하게 문제를 해결할 수 있습니다. Coverity는 자동화된 보안 테스트 기능을 사용자의 CI/CD 파이프라인에 원활하게 통합하고, 기존의 개발 도구 및 워크플로를 지원합니다. 온프레미스에서 개발을 진행할 수도 있고, 높은 확장성을 제공하는 클라우드 기반 애플리케이션 보안 플랫폼인 Polaris Software Integrity Platform™ (SaaS)을 통해 클라우드에서 개발을 진행할 수도 있습니다. Coverity는 22개 언어와 70개 이상의 프레임워크 및 템플릿을 지원합니다.

Coverity에 포함된 Rapid Scan은 웹 및 모바일 애플리케이션, 마이크로서비스 및 IaC(Infrastructure-as-code) 구성을 스캔하는 빠르고 가벼운 정적 분석 엔진입니다. Rapid Scan은 추가 구성 없이 Coverity 스캔이 실행될 때마다 자동으로 실행되며 기존 스캔 완료 시간으로 전체 CI 빌드의 일부로도 실행이 가능합니다. Rapid Scan은 Code Sight™의 독립형 스캔 엔진으로 배포될 수 있고, 명령 줄 인터페이스(CLI)를 통해 배포될 수도 있습니다. 또한, 자동화된 빌드 파이프라인에 배포할 수도 있습니다. 대부분의 프로젝트에서 Rapid Scan은 몇 초 만에 유용한 결과를 제공합니다. 별도의 설정 없이 디렉토리 또는 Git 리포지토리만 선택하면 되므로 사용하기 편리합니다. 다양한 플랫폼과 파일 형식을 지원하므로 IaC 구성 파일을 손쉽게 스캔할 수 있습니다. API 및 구성 검사기를 이용하면 API 오용 및 설정 파일 내 취약한 구성을 탐지할 수 있습니다. 이 기능은 코딩 중에, 또는 모든 코드 커밋에서 즉각적인 분석 피드백을 원하는 개발자들에게 적합합니다. 다양한 분석 출력 형식(SARIF, JSON 및 콘솔)과 GitHub Actions 및 GitLab CI 지원을 통해 파이프라인 스캔 자동화 및 이슈 관리를 지원합니다. 또한, Rapid Scan은 이슈를 정책 파일에 할당하여 빌드를 자동으로 중단할 수 있습니다.

주요 특징

빠르고 정확한 분석

- Code Sight™ 통합 개발 환경(IDE) 플러그인을 통해 개발자는 코딩 중 IDE에서 몇 초 만에 정확한 분석을 수행할 수 있습니다. Coverity는 설명, 카테고리, 심각도, CWE 데이터, 결함 위치, 상세 해결 가이드, 데이터 흐름 추적 등 이슈 해결에 필요한 모든 정보 뿐만 아니라, IDE 내 이슈 분류 및 관리 기능까지 제공합니다.
- Coverity의 Point & Scan 데스크톱 애플리케이션은 소스 코드만 선택하면 손쉽게 애플리케이션을 온보딩(IaC 빌드 캡처 기능 포함) 할 수 있도록 지원합니다. 개발팀이 명령 줄 인터페이스를 선호하는 경우에는 Coverity CLI 기능이 유용합니다.

종합 보고 및 규정 준수 가시성

Coverity on Polaris는 소프트웨어 개발 수명주기(SDLC)의 각 단계에서 조직의 애플리케이션의 위험 상태에 대한 통합적인 가시성을 제공합니다.

- 보안팀은 전체 애플리케이션 포트폴리오에 대한 통합된 위험 프로필을 얻을 수 있습니다. 또한, API를 통해 결과를 다른 위험 보고 도구로 가져올 수도 있습니다.
- 카테고리별로 취약점을 필터링하고 추세 보고서를 확인하며 중요도에 따라 취약점 해결의 우선순위를 설정하고 팀과 프로젝트 전반에 걸쳐 보안 정책 준수 (OWASP Top 10, CWE Top 25 및 PCI DSS 등)를 관리할 수 있습니다.
- "기간별 이슈" 보고서는 기간별로 이슈 심각도를 보여주고 프로젝트의 보안 태세에 관한 즉각적인 정보를 제공합니다. PDF 보고서 다운로드는 감사 담당자가 상세한 규정 준수 기록을 유지할 수 있도록 합니다.

또한, Coverity는 C/C++에 대한 동급 최고의 코드 품질 이슈 탐지 기능을 제공하며, 다양한 안전, 보안, 신뢰성 표준(예: MISRA®, CERT C/C++, CERT Java, DISA STIG, ISO 26262, ISO/IEC TS 17961, AUTOSAR®) 및 NVIDIA의 CUDA C++ 가이드라인에 포함된 품질 이슈들을 탐지해 냅니다. Coverity Qualification Kit (Q-Kit)을 통해 안전성이 중요한 프로젝트들이 업계 안전 표준을 만족할 수 있도록 Coverity의 구성을 확인할 수 있습니다.

엔터프라이즈급 확장성 및 민첩성

- Coverity on Polaris를 사용하는 조직들은 고가의 온프레미스 장비를 설치하고 유지할 필요가 없으며, 비즈니스 요구 사항에 따라 탄력적으로 애플리케이션 보안 테스트 규모를 확장할 수 있습니다.
- Polaris 설치는 매우 간단합니다. URL에 로그인한 후 명령 줄 인터페이스(CLI)를 다운로드해서 설치하거나, CI 워크플로를 통해 실행하여 소스 코드 분석을 시작할 수 있습니다.
- Coverity 분석 엔진은 가용성이 높은 클라우드 플랫폼에서 실행됩니다. 따라서 Coverity on Polaris는 수천 명의 개발자와 프로젝트를 수용하고, 높은 성능 및 가동 시간을 바탕으로 수 백 만 건의 이슈를 처리할 수 있도록 확장할 수 있습니다.

소프트웨어 개발 수명주기 통합

- Code Sight 플러그인은 별도의 설정이 필요 없으며 Visual Studio, Visual Studio Code, Eclipse, IntelliJ, WebStorm, PyCharm, PhpStorm, RubyMine의 마켓플레이스 웹사이트에서 다운로드할 수 있습니다.
- Coverity는 또한 IDE(예: Visual Studio, Eclipse, IntelliJ, RubyMine, Wind River Workbench, Android Studio), 소스 코드 관리(SCM) 솔루션, 이슈 트래커(예: Jira, Bugzilla), CI 빌드 도구(예: Jenkins, Azure DevOps), 애플리케이션 수명주기 관리(ALM) 솔루션에 대한 레거시 기본 통합을 지원합니다.
- REST API를 통해 다른 빌드 자동화 솔루션을 지원하고 분석 결과를 다른 엔터프라이즈 또는 사용자 정의 도구로 가져오는 기능도 지원합니다.
- Coverity on Polaris는 개발 및 배포 전 단계 중 자동화된 클라우드 기반 보안 테스트를 위한 추가적인 플러그인 및 통합을 지원합니다.
- REST API를 통해 분석 결과를 보안 및 위험 보고 도구로 가져올 수 있습니다. 자세한 설명은 Polaris 데이터시트를 참조해 주십시오.

종합 이슈 관리 대시보드

- 개발 관리자는 전반적인 보안 위험 및 산업 표준(예: OWASP Top 10, CWE Top 25)에 대한 준수, 그리고 개별 개발자 또는 전체 프로젝트팀이 우선 순위에 따라 이슈들을 어떻게 해결하고 있는지를 보여주는 "기간별 이슈" 추세선 차트를 생성할 수 있습니다.
- 업계 우선순위 목록(Industry Recognized Priority Lists), Top 5 이슈 유형(Top 5 Issues Types) 및 기술적 리스크 지표(Technical Risk Indicators) 등의 보고 대시보드를 손쉽게 확인함으로써 조직에 가장 중요한 이슈들에 집중하고 이들의 우선순위를 결정할 수 있습니다.
- 사전 정의된 필터들을 통해 CWE, 표준 분류 체계, 우선순위 목록, 위험 지표, 경로 및 개별 개발 책임자를 기준으로 이슈들을 필터링하고 그룹화 할 수 있습니다.

확장된 표준 준수 및 취약점 탐지

Coverity Extend는 개발자가 고유한 결함 유형을 탐지할 수 있게 해주는 사용하기 쉬운 소프트웨어 개발 키트(SDK)입니다. 이 SDK는 사용자 지정 또는 도메인별 결함을 탐지하는 프로그램 분석기 또는 검사기를 작성하기 위한 프레임워크입니다. Coverity CodeXM은 개발자들이 자신만의 맞춤형 검사기를 손쉽게 개발할 수 있도록 지원하는 도메인별 함수형 프로그래밍 언어입니다. 이 맞춤형 검사기들은 기업 보안 요구사항과 산업 표준 또는 지침에 대한 준수를 지원합니다.

Coverity 정적 분석 | 기술 사양

지원 언어 및 플랫폼

- Apex
- C/C++*
- C#*
- CUDA
- Java*#
- JavaScript*#
- PHP*#
- Python*
- .NET Core
- ASP.NET
- Objective-C
- Go
- JSP
- Ruby*
- Swift*#
- Fortran
- Scala
- VB.NET
- iOS
- Android
- TypeScript#
- Kotlin

* 이 언어들은 현재 Coverity의 Point and Scan 데스크톱 애플리케이션과 Coverity CLI 기능을 통해 지원됩니다.
# 이 언어들은 소스 코드 내 보안 취약점 스캔을 위해 Rapid Scan을 통해 지원됩니다.

지원 IaC 플랫폼 및 파일 포멧

Platforms

- Terraform
- AWS CloudFormation
- Kubernetes
- Helm
- ELK

File formats

- JSON
- YAML
- HCL (Terraform)
- HTML
- XML
- plist
- TOML
- Properties
- Vue template
- JSX
- TSX

클라우드 배포 지원

- Coverity Connect는 AWS, Azure 및 GCP 공용 클라우드의 컨테이너에서 실행 가능합니다.
- 클라우드 네이티브 기술 지원: Docker 및 Kubernetes

지원 프레임워크

Coverity는 Java, JavaScript, C# 및 기타 언어에 대한 70개 이상의 프레임워크를 지원합니다. Coverity는 또한 AWS 서비스(EC2, S3, DynamoDB, IAM) 및 Google Cloud Storage APIs (GCP)와 상호작용하는 클라우드 네이티브 JavaScript 앱을 위한 주요 클라우드 제공자 API 프레임워크의 보안 모델링을 지원합니다.

Java

- Android SDK
- Apache Shiro
- Axis
- DWR
- Enterprise Java Beans (EJBs)
- GWT
- Hibernate
- iBatis
- Java Frameworks
- Java Persistence API (JPA)
- Javax.websocket
- JAX RS
- JAX WS
- JEE
- JSF/Facelets
- JSP and JSP Standard Tag Library (JSTL)
- ReactiveX (RxJava, Reactor)
- Restlet
- Spring Boot
- Spring Framework
- Struts
- Terasoluna
- Tiles
- Vert.x
- WS XML-RPC

C#

- ASP.NET Core MVC/ASP.NET MVC
- ASP.NET Core Web API
- ASP.NET ASMX Web Services
- ASP.NET Web Forms
- Identity Server
- MassTransit
- Razor templates
- WCF Services

JavaScript/TypeScript

Client-side

- Angular
- Angular JS
- Apache Cordova
- Backbone
- Bootstrap
- Ember
- HTML5 DOM APIs/Ajax
- jQuery
- Mithril
- React/ Preact
- Socket.IO
- Swig
- Vue

Server-side
- Angular server-side rendering (Express and Hapi engines)
- Express
- Fastify
- Hapi
- Koa
- Mean.io
- Node
- Passport
- React server-side rendering (Next.js)
- Restify
- SAP XS Classic and Advanced
- Socket.IO
- Vue server-side rendering

Template engines
- Consolidate
- doT.js
- EJS
- Handlebars
- Hogan
- Jade
- koa-views
- Lodash (templating)
- Marko
- Mustache
- Nunjucks
- Pug
- Swig
- Twig
- Underscore (templating)
- Vision

Major libraries
- Axios
- Google Cloud APIs (Storage)
- Mongoose / MongoDB
- Request
- Sequelize
- Sqlx
- Swashbuckle
- Underscore / Lodash

GO
- Echo

PHP
- Symfony

Python
- Flask
- Django

Ruby
- Ruby on Rails

Rapid Scan IaC 프레임워크
- Android
- Apache Cordova
- Apache Kafka
- Apache Struts
- Apache Zookeeper
- Apollo GraphQL
- AWS Cloudformation
- Consul
- Express
- Grails® framework
- GraphQL
- Istio
- Jakarta Server Faces
- Java/Jakarta EE
- Kubernetes
- mybatis
- NodeJS
- OpenAPI
- Postman
- RabbitMQ
- React
- Socket.IO
- Spring
- Terraform
- Vue.js

지원 플랫폼
- Windows
- Linux
- Mac OS X
- Solaris
- AIX
- NetBSD
- FreeBSD

SDLC 네이티브 통합

SCM
- AccuRev
- Apache Subversion (SVN)
- CVS
- Git
- Mercurial (Hg)
- Perforce Helix
- Team Foundation Server SCM

Legacy IDEs
- IBM Rational Team Concert
- QNX Momentics
- Wind River Workbench

CI build servers
- Azure DevOps Server
- Bazel
- Jenkins

Code Sight supported IDEs*
- Visual Studio for VB.NET, C#, C/C++, JavaScript, PHP, Python, Ruby, TypeScript
- Visual Studio Code for C# (.NET Core), C/C++, Java, JavaScript, PHP, Python, Ruby, TypeScript
- Visual Studio Code (Rapid Scan) for Java, JavaScript, and TypeScript
- Eclipse for Java, JavaScript, C/C++, PHP, Python, Ruby, TypeScript
- IntelliJ for Java, JavaScript, PHP, Python, Ruby, TypeScript
- WebStorm for JavaScript, TypeScript
- PyCharm for Python
- PhpStorm for PHP
- RubyMine for Ruby

Issue tracking
- Jira
- Bugzilla

지원 컴파일러
- Analog Devices Blackfin
- Analog Devices SHARC
- Analog Devices TigerSHARC
- ARM C/C++
- Borland C++
- CEVA BXx
- CEVA XC16
- CEVA-X2
- CEVA-XC4500
- Clang
- Cosmic C
- Freescale CodeWarrior
- GNU GCC/G++
- GHS PowerPC on Windows
- Green Hills C/C++/EC++
- HI-TECH PICC
- IAR C/C++
- IBM AIX
- IBM XLC
- Intel C++ for Windows
- JDK for Mac OS X
- Keil compilers
- Marvell MSA
- MPLAB XC8
- Nvidia CUDA Compiler (NVCC)
- OpenJDK

- QNX C/C++
- Renesas C/C++
- SNC C/C++
- SNC GNU C/C++
- SONY PS4 SDK
- STMicroelectronics GNU C/C++
- STMicroelectronics ST Micro C/C++
- Sun (Oracle) CC
- Sun/Oracle JDK
- Synopsys MetaWare C and C++
- Tasking for ARM Cortex and TriCore
- TI Code Composer
- Visual Studio
- Wind River C/C++

(This list is not exclusive)

중요 검사항목

- API usage errors
- Best practice coding errors
- Buffer overflows
- Build system issues
- Class hierarchy inconsistencies
- Code maintainability issues
- Concurrent data access violations
- Control flow issues
- Cross-site request forgery (CSRF)
- Cross-site scripting (XSS)
- Deadlocks
- Error handling issues
- Hard-coded credentials
- Incorrect expression
- Insecure data handling
- Integer handling issues
- Integer overflows
- Memory—corruptions
- Memory—illegal accesses
- Null pointer dereferences
- Path manipulation
- Performance inefficiencies
- Program hangs
- Race conditions
- Resource leaks
- Rule violations
- Security best practices violations
- Security misconfigurations
- SQL injection
- Uninitialized members

·최신 CodeSight 및 지원되는 IDE 버전에 대해서는 https://dev.sig-docs.synopsys.com/codesight/topics/support_matrix/r_code_sight_support_matrix.html를 참조해 주십시오.

Rapid Scan 분석 엔진에 관한 최신 발표 및 릴리즈 업데이트(단독형 유스케이스)에 관해서는 여기를 참조해 주십시오.

이 데이터시트는 Coverity 2022.12.0 이상에만 적용됩니다.

Synopsys Partner

제품문의는 시높시스 공식 파트너 KMS 테크놀로지로 문의주시기 바랍니다.

KMS Technology

주 소 | 서울시 강남구 언주로 337(역삼동) 동영문화센터 6층
홈페이지 | www.kmstech.co.kr
전화번호 | 02-6925-0803
이 메 일 | info@kmstech.co.kr

SYNOPSYS®

Synopsys의 차별성

Synopsys는 위험을 최소화하고 속도와 생산성은 극대화하여 개발팀이 안전한 고품질 소프트웨어를 개발할 수 있도록 지원합니다. 애플리케이션 보안 분야의 리더로서 Synopsys는 정적 분석, 소프트웨어 구성 분석, 동적 분석 솔루션을 제공합니다. 개발팀은 이를 활용하여 자사코드, 오픈소스 컴포넌트, 애플리케이션 동작의 취약점과 결함을 빠르게 발견하고 보완할 수 있습니다. 업계 최고 수준의 도구, 서비스, 전문성을 겸비한 Synopsys와 함께라면 DevSecOps 및 소프트웨어 개발 주기 전체에서 보안과 품질을 최적할 수 있습니다.

자세한 사항은 www.synopsys.com/software를 참조해 주십시오.

Synopsys, Inc.
경기도 성남시 분당구 판교역로 235
에이치 스퀘어 N동 5층 (우)13494
시높시스코리아

연락처:
대표 번호: (82) 2-3404-2700
Email: sig-info@synopsys.com