BLACKDUCK
BY SYNOPSYS

Black Duck Hub
소프트웨어 구성 분석

애플리케이션 라이프 사이클 전반의 오픈 소스 보안 및 라이선스 위험 관리 자동화

개요

Black Duck Hub는 보안 및 개발 팀이 애플리케이션 포트폴리오 전체에서 오픈 소스 관련 위험을 식별하고 완화할 수 있도록 도와줍니다.

Black Duck Hub를 이용하면 다음과 같은 이점이 있습니다.

- 사용 중인 특정 오픈 소스 및 종속성을 식별합니다.
- 알려진 취약점을 사용 중인 오픈 소스에 자동으로 매핑합니다.
- 보안 위험을 평가하고 취약점을 분류 합니다.
- 보안 및 라이선스 정책을 시행하여 위험 노출을 관리합니다.
- 문제 해결 일정을 계획하고 추적합니다.
- 오픈 소스 라이선스를 확인하고 Open HUB 커뮤니티 활동을 모니터링 합니다

다른 정적 분석 솔루션들도 코드 작성 시 개발자가 유발하는 코드 관련 취약점을 발견하는 데 중점을 두지만, 이러한 기술들은 보고된 취약점 중 소수만을 포착합니다. 개발자는 오픈 소스를 사용하여 개발 주기를 혁신적으로 개선하고 가속화하지만 Heartbleed, Shellshock, Poodle 및 Ghost 같은 취약점으로 인해 패치를 적용하지 않은 일반적인 오픈 소스 구성 요소에서 위험 수준은 더욱 두드러집니다. 게다가 널리 알려진 이러한 취약점은 매년 보고되는 4,000개 이상의 오픈 소스 취약점 중 극히 일부에 불과합니다.

Black Duck Hub는 보안 및 개발 팀이 애플리케이션 및 컨테이너의 오픈 소스 관련 위험을 식별하고 완화할 수 있도록 지원합니다.

주요 기능

Black Duck만이 제공하는 혜택

- 가장 많은 개발 언어와 개발 도구 통합 지원 개발 도구 통합
- 업계 최고의 완벽한 오픈 소스 소프트웨어 KnowledgeBase™
- 통합된 문제 해결 추적 및 관리 기능

보안은 가시성에서 시작합니다

오픈 소스 보안의 첫 번째 단계는 코드베이스에서 오픈 소스가 무엇인지에 대한 가시성을 확보하는 것입니다. 가시성이란 어떤 오픈 소스 라이브러리가 사용 중인지 뿐만 아니라 이 라이브러리가 어디서 어떻게 사용되는지를 파악하는 것을 의미합니다.

기존의 대다수 솔루션은 패키지 관리자 선언에 의존하여 개발 팀에서 사용하는 오픈 소스를 추적합니다. 이 방법은 선언되지 않은 상태에서 프로젝트에 들어가는 코드를 문서화하지 못하고, 이행 종속성(transitive dependencies)을 설명하지 못하며, 패키지 관리자를 사용하지 않는 C 및 C++ 같은 언어에는 적합하지 않습니다.

"우리가 Black Duck을 선택한 세 가지 이유를 꼽자면 평판, 사용 용이성, 결과에 대한 신뢰입니다. 또한, 내부적으로 관리할 필요가 없는 솔루션을 찾고 있기도 했고요."

– Copperleaf, Asset Investment Planning & Management Solution

업계에서 유일하게 Black Duck Hub만이 오픈 소스 검색에 다각적 접근 방식을 취하여 가장 완벽한 BoM(Bill of Material)을 생성합니다. Black Duck의 다각적 오픈 소스 검색 기술은 빌드 프로세스 모니터링, 파일 시스템 스캐닝, 선택적 스니펫 매칭 기술을 결합하여 빌드 중 식별된 종속성을 비롯해 사용 중인 모든 오픈 소스를 추적합니다. 이렇게 하면 일치 정확도를 높이고 오탐을 줄이기 위한 여러 가지 증거를 얻을 수 있습니다.

Black Duck Hub는 새로 도입된 오픈 소스에 대한 프로젝트를 지속적으로 스캔하고 문제가 되기 전에 보안 취약점을 관리합니다. 이 기능을 사용하면 취약성을 검토 및 우선 순위 지정, 교정 날짜 할당 및 밀착 추적을 수행할 수 있습니다.

Black Duck Hub는 애플리케이션 내에서 사용 중인 오픈 소스 라이브러리에 대해 나중에 보고되는 새로운 취약점을 자동으로 모니터링하므로, 새로 식별된 취약점에 신속하게 대응할 수 있도록 도와줍니다.

Black Duck Hub의 주요 기능	
안전한 DevOps를 위한 통합	Hub Detect 오픈 소스 검색 클라이언트를 사용하면 Black Duck Hub를 기존 개발 도구 및 프로세스에 쉽게 통합할 수 있습니다. 자동으로 어떤 언어와 패키지 관리자가 사용되고 있는지 확인하고 검색을 위한 적절한 통합을 구성하며 코드를 분석하는 가장 효과적인 방법을 찾습니다. 오픈 소스 보안 인사이트가 필요한 곳에 그 어느 때보다 빠르게 이를 전달합니다.
사용자 지정 BoM (리소스 명세서: Bill of Material)	자동화된 스캐닝 결과, 빌드 도구 및 패키지 관리자 매니페스트, 수동 입력을 결합하여, 편집 가능한 오픈 소스 BoM(리소스 명세서: Bill of Material)으로 코드 가시성을 유지합니다.
자동 취약점 매핑 및 경고	애플리케이션의 오픈 소스와 관련된 알려진 취약점을 파악하고 새로 보고된 취약점이 영향을 미칠 때 경고를 받습니다.
향상된 취약점 데이터 제공	Black Duck Hub는 KnowledgeBase™의 위험 등급 심각도 메트릭 및 향상된 취약점 데이터를 사용하여 애플리케이션 보안 위험 상황에 대한 상세한 통찰력을 제공합니다: • 취약점에 대한 자세한 기술 설명 • 영향을 받는 프로젝트 및 구성 요소의 색인 • CVSS 2 및 CVSS 3 메트릭 • CWE 데이터 • 활용의 일반적인 결과 • 구성 요소 수준 업그레이드 및 문제 해결 지침
취약점 개선 방법 추적	개별 프로젝트 내에서 일정대로 시행되거나 실제로 이루어지는 취약점 개선 진행 상황을 추적합니다. Black Duck의 양방향 Jira 통합을 활용하거나 문제 해결 보고서를 CSV 내보내기 기능을 통해 타사 도구로 쉽게 내보낼 수 있습니다.
정책 관리	오픈 소스 프로젝트, 라이선스 유형 및 취약점 허용에 대한 정책을 설정합니다. 정책 위반을 빠르게 식별하고 프로젝트 및 구성 요소별로 예외 사항을 관리합니다.
스니펫 매칭	라이선스 준수 위험에 대한 더 자세한 통찰력을 얻기 위해 74개 언어, 149가지 파일 유형에 대해 스니펫 스캔을 수행합니다.
위험 대시 보드 및 보고서	이해하기 쉬운 보안, 라이선스, 커뮤니티 활동 위험, 문제 해결 진행 대시보드 및 보고서를 통해 프로젝트 내외의 위험을 분석합니다.

BLACKDUCK BY SYNOPSYS

Black Duck Hub 지원 기술

Languages

- C
- C++
- C#
- Erlang
- Golang
- Java
- JavaScript
- Node.js
- Objective-C
- Swift
- Perl
- Python
- PHP
- R
- Ruby
- Scala
- .NET

Package managers

- NuGet
- Hex
- Vndr
- Godep
- Dep
- Maven
- Gradle
- Npm
- CocoaPods
- Cpanm
- Conda
- Pear
- Composer
- Pip
- Packrat
- RubyGems
- SBT

DevOps tools

IDEs

- Eclipse
- Visual Studio IDE

Continuous integration

- Jenkins
- TeamCity
- Bamboo
- Team Foundation Server
- Travis CI
- CircleCI
- GitLab CI
- Visual Studio Team Services
- Concourse CI
- AWS CodeBuild
- Codeship

Bug and issue trackers

- Jira

Binary and source repositories

- Artifactory
- Nexus
- GitHub

Application security suites

- IBM AppScan
- Micro Focus Fortify
- SonarQube
- ThreadFix

Cloud technologies

Cloud platforms

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

Container platforms

- Docker
- OpenShift
- Pivotal Cloud Foundry
- Kubernetes

Databases

- PostgreSQL

BLACKDUCK
BY SYNOPSYS

Synopsys의 차별점

Synopsys는 개발 팀이 안전하고 우수한 소프트웨어를 구축하고 위험을 최소화하면서 속도와 생산성을 극대화할 수 있도록 지원합니다. 정적 분석, 소프트웨어 구성 분석 및 애플리케이션 보안 테스트 분야의 공인된 선두업체인 Synopsys는 독점 코드, 오픈 소스 및 런타임 환경 전반에서 모범 사례를 적용할 수 있는 독보적인 입지를 갖추고 있습니다. 업계를 선도하는 도구와 서비스, 전문 기술을 결합하여 조직이 소프트웨어 개발 라이프 사이클 전반에 걸쳐 DevSecOps의 보안 및 품질을 극대화할 수 있도록 돕고 있는 곳은 Synopsys밖에 없습니다.

보다 자세한 정보를 원하시면 www.synopsys.com/software 를 참조하십시오.

엔시큐어㈜

서울특별시 용산구 한강대로71길 4
한진중공업빌딩 7층 (우)04322

Trust & Communications
eNsecure
엔시큐어㈜

제품문의 : 070-7826-6807 | mktg@ensecure.co.kr | www.ensecure.co.kr