SYNOPSYS®

KMS Technology

Black Duck
소프트웨어 구성 분석

소프트웨어 공급망 전반에서 이루어지는 오픈 소스 보안 및 관리

개요

Black Duck은 애플리케이션 및 컨테이너에서 오픈 소스 사용으로 인해 발생하는 보안, 라이선스 컴플라이언스 및 코드 품질 위험을 관리하는 포괄적인 솔루션입니다. Forrester에서 소프트웨어 구성 분석(SCA) 분야의 리더로 선정된 Black Duck은 서드파티 코드에 대한 뛰어난 가시성을 제공하여 소프트웨어 공급망과 애플리케이션 수명 주기 전반에 걸쳐 코드를 관리할 수 있도록 지원합니다.

소스 및 바이너리를 위한 통합 솔루션

Black Duck은 업계 최고의 SCA 솔루션으로, 다양한 오픈 소스 리스크 관리 기능에 세밀한 바이너리 검사를 적용하여 오픈 소스 및 서드파티 소프트웨어와 관련된 위험을 최소화합니다. 최근 오픈 소스가 평균 코드베이스의 70%를 구성하게 됨에 따라, Black Duck은 다음과 같이 개발과 운영, 조달, 보안 팀을 지원하고 있습니다.

- **보안 취약점 탐지 및 수정** - SDLC의 각 단계에서 보안 취약점을 탐지하고 수정할 수 있도록 취약점 별로 수정에 관한 세부 지침 및 기술적 통찰을 제공합니다.
- **오픈 소스 라이선스 컴플라이언스 위반 점검** - 업계 최대 규모의 오픈소스 Knowledge Base에 2,750개 라이선스를 리스트업하여 사용자 애플리케이션의 오픈 소스와 관련된 라이선스를 식별하고(더 큰 구성요소의 코드 조각을 포함) 오픈 소스 라이선스 컴플라이언스 위반을 예방하며 지적 재산을 보호합니다.
- **개발 비용 초과 및 코드 붕괴 방지** - 오픈 소스 코드의 품질 저하와 관련된 운용 리스크 측정 지표를 적용합니다.
- **모든 소프트웨어, 펌웨어 및 소스 코드를 스캔** - 전반적으로 모든 소프트웨어, 펌웨어 및 소스 코드를 스캔하여 내부 구성요소에 대한 포괄적인 BOM(Bill of Materials, 소프트웨어 재료 명세서)을 제공합니다.
- **새로운 취약점에 대한 자동 모니터링** - BOM에 영향을 미치는 새로운 취약점을 자동으로 모니터링하고, 사용자 지정 정책 및 워크플로우 트리거로 개선 속도를 가속화해 리스크가 발생할 수 있는 상황을 줄여 줍니다.

탐색

- **식별** - 코드, 바이너리 및 컨테이너에서 오픈 소스를 식별합니다
- **탐지** - 구성요소의 일부분 및 수정된 구성요소를 탐지합니다.
- **자동화** - DevOps 통합으로 스캔을 자동화합니다.

보호

- **매핑** - 구성요소를 알려진 취약점에 매핑합니다.
- **식별** - 라이선스 및 구성요소 품질 리스크를 식별합니다.
- **모니터링** - 개발 및 생산 과정에 나타나는 새로운 취약점을 모니터링합니다.

관리

- **정책 설정 및 시행** - 오픈 소스 사용 및 보안 정책을 설정하고 시행합니다.
- **자동화** - DevOps 통합으로 정책 시행을 자동화합니다.
- **우선순위 지정 및 추적** - 수정 활동의 우선순위를 지정하고 추적합니다.

주요 이점

보다 심층적이고 간소화된 분석

Black Duck은 완전한 BOM을 생성하고 검증하기 위해 고유한 멀티펙터 탐지 기술을 사용하여 명시된 컴포넌트와 고유한 파일 해시 시그니처, 빌드 과정에서 해결된 의존성과 오픈소스 코드 조각을 추적하여 더 많은 오픈소스를 보다 정확하게 탐지합니다. Black Duck은 이러한 스캐닝 방법을 효율적으로 적용하여 SDLC의 전반에서 철저한 보안과 규정 준수가 이루어지게 합니다. 여기에는 IDE의 Rapid Scan이 포함되며, CI/CD 및 바이너리 레파지토리 도구와 통합하여 빌드 및 빌드 이후 단계에서 심층 분석을 하게 됩니다.

빠른 취약점 탐지 및 수정

Black Duck은 공개된 출처의 선별된 데이터(예: NVD)와 Synopsys Cybersecurity Research Center(CyRC)의 상세한 자체 분석 데이터를 결합하여 오픈 소스 보안 위험에 대한 통찰을 제공합니다. 또 새로운 취약점이 NVD에 게시되기 바로 몇 주 전에 미리 알림을 받을 수 있는(위험 노출 시간을 줄임) 기능과 다음과 같이 Synopsys만의 독점적인 취약점 데이터 및 BDSA(Black Duck Security Advisories)의 혜택을 제공합니다.

- 중요 위험 지표, 취약점 별 기술적 통찰, 세부 악용 정보 및 영향도 분석
- CVSS 2와 CVSS 3 점수 및 CWE 분류 데이터
- 일반적인 공격 패턴 목록 및 등급(CAPEC)
- NVD에서 제공하지 않는 시간 점수(Temporal score)
- 구성요소 업그레이드 및 개선 지침, 요인 완화, 그리고 보정 제어
- 취약한 코드가 애플리케이션에 의해 호출되고 있는지 파악하는 취약점 영향도 분석
- 위험 프로필에 따른 맞춤 취약점 위험 스코어 적용
- 심각도, 솔루션 가용성, 악용 가능성, CWE 및 도달 가능성 등, 여러 중요 데이터 점수에 따라 취약점 해결의 우선순위 지정 가이드

자동으로 보안 설정 및 정책 사용

라이선스 유형, 취약점 심각도, 오픈 소스 구성요소 버전 등을 포함하며, 여러 기준에 따라 오픈 소스 보안을 구성하고 정책을 사용하도록 지원합니다. 신속한 개선 조치 시작 및 리포트를 위한 자동 워크플로우 트리거, 알림, 양방향 Jira 통합을 통해 정책을 시행합니다.

소스 코드 없이도 오픈 소스 식별

사용자 툴킷에 Black Duck을 통합하면 소스 코드에 액세스하지 않고도 벤더에서 공급받은 바이너리를 빠르고 쉽게 분석하여 소프트웨어 공급망의 취약점을 탐지할 수 있습니다. 상세하고 실행 가능한 위험 지표를 통해 위험에 노출되기 전 기술을 사용하고 조달 시 정확한 정보에 기반한 의사결정을 내림으로써 위험에 사전 대비할 수 있습니다(해당 기술의 사용 및 조달에 관한 위험에 대비하기 위해 심층적이고 실행 가능한 위험 지표를 확보하십시오.). Black Duck의 지능형 스캔 클라이언트는 대상 소프트웨어에 대해 소스 또는 컴파일된 바이너리 여부를 자동으로 파악한 후 사용자의 애플리케이션에 영향을 미칠 수 있는 모든 서드파티 소프트웨어 구성요소, 관련 라이선스 및 알려진 취약점을 식별하고 분류합니다.

Black Duck | 소스 및 패키지 관리자 스캐닝

■ Black Duck에만 해당
✖ BDBA에만 해당

스캐닝

언어

- C
- C++
- C#
- Clojure
- Erlang ■
- Golang
- Groovy
- Java
- JavaScript ■
- Kotlin
- Node.js ■
- Objective-C
- Perl ■
- Python ■
- PHP ■
- R ■
- Ruby
- Scala
- Swift ■
- .NET 클라우드 기술

패키지 관리자

- NuGet ■
- Hex ■
- Vndr ■
- Godep ■
- Dep ■
- Maven ■
- Gradle ■
- Npm ■
- CocoaPods ■
- Cpanm ■
- Conda ■
- Pear ■
- Composer ■
- Pip ■
- Packrat ■
- RubyGems ■
- SBT ■
- Bazel
- Cargo
- C/C++ (Clang)
- GoLang
- Erlang/Hex
- Rebar
- Python
- Yarn
- Yocto

BDBA 패키지 관리자 지원

- 배포판 패키지 관리자: Linux 배포 패키지 관리자 데이터베이스의 정보를 활용하여 구성요소의 정보를 추출합니다.
- 다음 네 가지 방법은 Java 바이트 코드에만 적용할 수 있습니다.
  - pom: JAR 파일의 pom.xml 또는 pom.properties 파일에서 Java 패키지, 그룹 이름 및 버전을 추출합니다.
  - manifest: JAR 파일의 MANIFEST.MF 파일 항목에서 Java 패키지 이름 및 버전을 추출합니다.
  - jar-filename: jar-filename에서 Java 패키지 이름 및 버전을 추출합니다.
  - hashsum: JAR 파일의 sha1 체크섬을 사용하여 알려진 Maven Central에 등록된 Java 프로젝트에서 검색합니다.

바이너리 형식

- 네이티브 바이너리
- Java 바이너리
- .NET 바이너리
- Go 바이너리

압축 형식

- Gzip(.gz)
- bzip2(.bz2)
- LZMA(.lz)
- LZ4(.lz4) ✖
- Compress(.Z)
- XZ(.xz)
- Pack200(.jar)
- UPX(.exe)
- Snappy
- DEFLATE
- zStandard(.zst) ✖

아카이브 형식

- ZIP(.zip, .jar, .apk, 및 기타 파생파일)
- XAR(.xar) ✖
- 7-Zip(.7z)
- ARJ(.arj)
- TAR(.tar)
- VM TAR(.tar) ✖
- cpio(.cpio)
- RAR(.rar)
- LZH(.lzh) ✖
- 전자 아카이브(.asar) ✖
- DUMP

설치 형식

- Red Hat RPM(.rpm)
- Debian 패키지(.deb)
- Mac 설치 프로그램(.dmg, .pkg)
- Unix 쉘 파일 설치 프로그램(.sh, .bin)
- Windows 설치 프로그램(.exe, .msi, .cab)
- vSphere 설치 번들(.vib) ✖
- Bitrock 설치 프로그램 ✖
- 지원되는 설치 프로그램 생성기 형식:
  - 7z, zip, rar 자동 압축 풀기 .exe ✖
  - MSI 설치 프로그램 ✖
  - CAB 설치 프로그램 ✖
  - InstallAnywhere ✖
  - Install4J ✖
  - InstallShield ✖
  - InnoSetup ✖
  - Wise 설치 프로그램 ✖
  - Nullsoft 스크립팅 가능 설치 시스템 (NSIS) ✖
  - WiX 설치 프로그램 ✖

펌웨어 형식

- Intel HEX ✖
- SREC ✖
- U-Boot ✖
- Arris 펌웨어 ✖
- Juniper 펌웨어 ✖
- Kosmos 펌웨어 ✖
- Android sparse 파일 시스템 ✖
- Cisco 펌웨어 ✖

파일 시스템 / 디스크 이미지

- ISO 9660 / UDF (.iso) ✖
- Windows 이미징 ✖
- ext2/3/4 ✖
- JFFS2 ✖
- UBIFS ✖
- RomFS ✖
- Microsoft 디스크 이미지 ✖
- Macintosh HFS ✖
- VMware VMDK(.vmdk, .ova) ✖
- QEMU Copy-On-Write (.qcow2) ✖
- VirtualBox VDI(.vdi) ✖
- QNX—EFS, IFS ✖
- NetBoot 이미지(.nbi) ✖
- FreeBSD UFS ✖

컨테이너 형식

- Docker

Black Duck | 통합

클라우드 기술

클라우드 플랫폼
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Pivotal Cloud Foundry

컨테이너 플랫폼
- Docker
- OpenShift
- Pivotal Cloud Foundry
- Kubernetes Package managers

데이터베이스
- PostgreSQL

DevOps 도구

IDEs
- Eclipse
- Visual Studio IDE
- IntelliJ IDEA
- WebStorm
- PyCharm
- RubyMine
- PhpStorm
- VS Code
- Android Studio

지속적인 통합
- Jenkins
- TeamCity
- Bamboo
- Team Foundation Server
- Travis CI
- CircleCI
- GitLab CI
- Visual Studio Team Services
- Concourse CI
- AWS CodeBuild
- Codeship
- Azure DevOps
- GitHub Actions
- OpenShift

워크플로우 및 알림
- Jira
- Slack
- Email
- SPDX
- Azure Boards
- Microsoft Teams

바이너리 및 소스 레파지토리
- Artifactory
- Nexus

애플리케이션 보안 제품군
- IBM AppScan
- Micro Focus Fortify
- SonarQube
- ThreadFix
- Cybric
- Code Dx
- Fortify
- ZeroNorth

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 만의 차별성

Synopsys는 위험을 최소화하고 속도와 생산성은 극대화하여 개발팀이 안전한 고품질 소프트웨어를 개발할 수 있도록 지원합니다. 애플리케이션 보안 분야의 세계적 리더인 Synopsys는 정적 분석, 소프트웨어 구성 분석 및 동적 분석 솔루션을 제공합니다. 개발팀은 이를 활용하여 자사 코드, 오픈 소스 구성요소, 애플리케이션 동작의 취약점과 결함을 빠르게 발견하고 보완할 수 있습니다.

자세한 정보는 www.synopsys.com/software에서 확인할 수 있습니다.

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

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