

Black Duck[®] SCA

소프트웨어 구성 분석

소프트웨어 공급망 위험의 식별 및 관리

가시성 확보

- 코드, 바이너리, 컨테이너, 아티팩트에서 오픈소스를 탐지합니다.
- SBOM으로 3자 컴포넌트를 확인합니다.
- DevOps 통합으로 스캔을 자동화합니다.

위험 관리

- 종속성을 알려진 취약점 및 상태 문제에 매핑합니다.
- 악성 구성요소 및 민감한 정보를 스캔합니다.
- 라이선스 위험 및 충돌을 식별합니다.
- 심각도에 따라 문제 해결의 우선순위를 결정합니다.

신뢰 구축

- 위험 허용 범위와 고객의 요구사항을 바탕으로 정책을 정의
- 오픈소스 및 사용자 정의 종속성을 포괄하는 SBOM 생성
- 애플리케이션 배포 전에 공급망 위협 해결

개요

Black Duck[®] SCA는 애플리케이션, 컨테이너 및 기타 소프트웨어 아티팩트, 라이브러리에서 발생하는 보안, 라이선스 준수 및 코드 품질 위험을 관리하는 포괄적 솔루션입니다.

Forrester가 소프트웨어 구성 분석(SCA) 리더로 선정한 Black Duck은 3자 종속성에 대한 높은 가시성을 제공하며, 고객이 소프트웨어 공급망에서 비롯되는 위험을 관리할 수 있도록 지원합니다.

소프트웨어 공급망 가시성 확보

상용 애플리케이션을 구성하는 코드의 대부분은 3자 코드이며, 최종 애플리케이션을 배포 및 사용하는 회사는 그러한 코드의 작성을 통제하거나 모니터링할 수 없습니다. Black Duck은 다양한 종속성 탐지 기술을 결합하여 애플리케이션 구성에 대한 높은 가시성을 제공하며, 효과적인 위험 분석과 관리를 지원합니다.

- **종속성 분석:** 패키지 관리자가 선언한 직간접적 종속성을 식별
- **바이너리 분석:** 펌웨어, 컨테이너 이미지 등 소스 코드에 대한 접근 권한이 없는 사후 구축형 아티팩트의 종속성 탐지
- **코드 조각 분석:** AI 코딩 도구 등에 포함된 코드 조각을 오리지널 오픈소스 프로젝트와 매칭
- **CodePrint 분석:** 패키지 관리자의 선언 없이도 소스 파일 및 디렉터리에서 종속성 식별
- **컨테이너 스캔:** 바이너리 분석과 CodePrint 분석을 결합하여 컨테이너 이미지에서 레이어별로 오픈소스 종속성을 식별
- **C/C++ 스캔:** 패키지 관리자 없이도 C/C++ 애플리케이션의 오픈소스 종속성 및 라이브러리를 정확히 식별

위험 식별 및 관리

식별한 모든 종속성에 대하여 관련 위험을 평가하고, 우선순위 결정과 문제 해결을 지원합니다.

보안 취약점

Black Duck KnowledgeBase를 기반으로 한 Black Duck Security Advisories(BDSA)가 기존의 오픈소스 취약점과 새로운 취약점에 대한 알리를 적재적소에 제공합니다. BDSA 알림의 내용은 다음과 같습니다.

- 중요한 위험 지표, 취약점별 기술 정보 및 악용 정보
- CVSS 점수 및 CWE 분류 데이터
- 고객의 위험 프로파일을 기반으로 한 취약점 위험 점수
- 구성요소 업그레이드 및 개선 지침, 위험 요인 완화, 그리고 보정 제어

BDSA는 사람과 AI의 능력을 결합하여 고객에게 피해를 줄 가능성이 높은 취약점을 발견, 분석, 보고합니다. BDSA는 취약점 공개 몇 시간 만에 그 어떤 업체보다도 정확한 분석을 제공합니다.

라이선스 위험

Black Duck은 명시적으로 선언된 라이선스, 2차 라이선스, 탑재형 라이선스 등 애플리케이션 종속성의 라이선스를 정확히 파악합니다. 각 라이선스의 요구사항과 제한사항을 간단히 요약하여 라이선스 문서 및 저작권 정보와 함께 제공합니다. 고객은 거의 모든 오픈소스 라이선스에 동반되는 알림 파일을 자동으로 생성할 수 있습니다.

구성요소 상태

보안 위험에 대한 적극적 예방을 지원하기 위해 Black Duck은 오픈소스 프로젝트의 상태, 이력, 커뮤니티 지원, 출처, 평판 등을 평가하기 위한 다양한 지표를 제공합니다.

멀웨어

Black Duck은 고객이 위험 평가 범위를 확장하여 알려진 취약점 외에도 다양한 위험 요소를 평가할 수 있도록 지원합니다. Black Duck은 소프트웨어 아티팩트의 빌드 후 구축 분석을 통해 의심스러운 파일, 예상치 못한 피해를 줄 수 있는 애플리케이션, 프로테스트웨어(Protestware), 의심스러운 파일 구조 등을 탐지합니다.

구성요소 위험 정보

Black Duck은 알려진 취약점에 대한 위험 평가뿐만 아니라, 멀웨어, 디지털 서명, 보안 대응 조치, 민감한 정보 등 기타 다양한 구성요소 위험 정보에 대한 사후 구축 분석까지 지원합니다.

오픈소스 정책 관리 자동화

라이선스 유형, 취약점 심각도, 오픈소스 구성요소 버전 등 여러 기준에 따라 오픈소스 보안 및 사용 정책을 구성합니다. 자동 워크플로 트리거, 알림, 양방향 Jira 및 Azure 통합을 바탕으로 정책을 적용하여 개선 조치와 보고를 신속히 처리합니다. 개발팀이 위험한 구성요소를 사용하지 못하도록 통제하고, 해당 구성요소가 릴리스 단계에 유입되지 않도록 빌드를 차단합니다.

SBOM을 애플리케이션 라이프사이클에 통합

Black Duck의 서비스를 통해 고객은

- 3차 소프트웨어 SBOM을 가져와 알려진 구성요소에 종속성을 자동으로 매핑하고, 사용자 정의 종속성 및 상용 종속성에 따른 구성요소를 새로 만들 수 있습니다.
- 오픈소스 종속성, 사용자 정의 종속성, 상용 종속성을 포괄하는 SBOM을 SPDX 또는 CycloneDX 형식으로 추출하여 고객, 산업, 또는 규제 요건을 충족할 수 있습니다. 미리 준비된 템플릿을 활용하여 고객이 정의한 적절한 수준의 공유 세부 사항을 충족합니다.
- SDLC 도구에 통합하여 SBOM 생성을 자동화하고, 기존 위험이나 새로 발견한 위험의 SBOM 종속성을 지속적으로 모니터링할 수 있습니다.

Black Duck이 지원하는 언어, 패키지 관리자, 통합 시스템에 관한 정보는 홈페이지에서 확인해 주시기 바랍니다.

Black Duck 소개

Black Duck®은 업계에서 가장 포괄적이고 강력하며 신뢰할 수 있는 애플리케이션 보안 솔루션 포트폴리오를 제공합니다. 전 세계 기업이 소프트웨어를 신속하게 보호하고, 개발 환경에 보안을 효율적으로 통합하며, 새로운 기술을 통해 안전하게 혁신할 수 있도록 지원하는 탁월한 실적을 보유하고 있습니다. 소프트웨어 보안 분야에서 인정받는 리더, 전문가, 혁신적인 기업인 Black Duck은 소프트웨어에 대한 신뢰를 구축하는 데 필요한 모든 것을 갖추고 있습니다.

자세한 내용은 www.blackduck.com 에서 알아보십시오.