SCA Market *Wave*

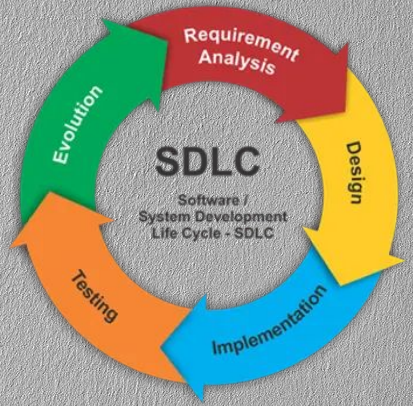
(Software Composition Analysis)

Kakao 오픈소스 기술파트 robin.hwang

kakao

어떤 오픈 소스 소프트웨어를 사용하고 있나요?

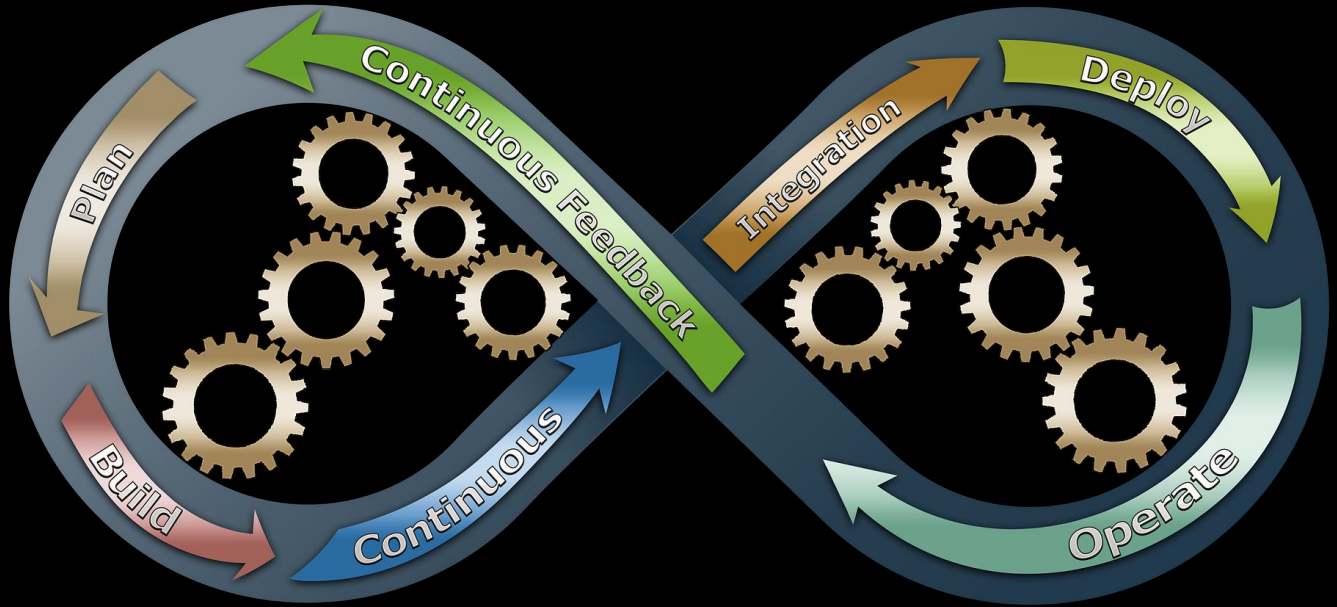
오픈소스 사용에 따른 의무사항 준수와 위험 요소 확인을 위해서는 SDLC 전체에서 지속적인 스캔 및 모니터링이 필요



kakao

SCA (Software Composition Analysis)

보안 및 라이선스 규정 준수를 발견하고 관리하기 위한 자동화 된 프로세스



kakao

image whitsource

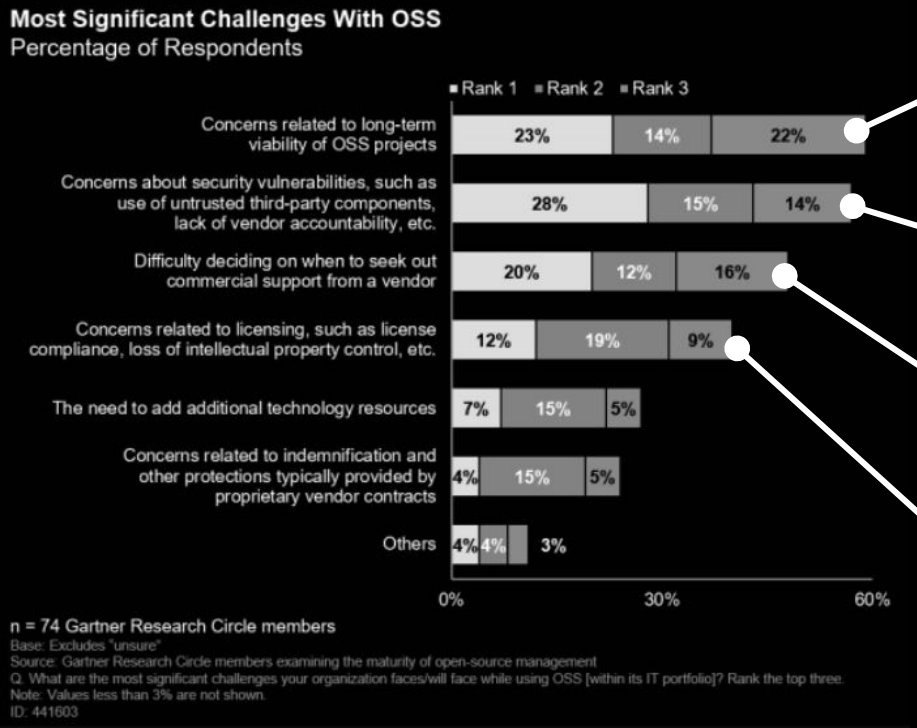
Gartner

Gartner: Technology Insight for Software Composition Analysis

Gartner Technology Insight for Software Composition Analysis (2019.11.01)

kakao

OSS 사용시 가장 중요한 과제는?



설문 응답자의 2/3 이상이 오픈 소스 프로젝트의 장기적인 생존 가능성에 대해 우려하고 있다고 응답

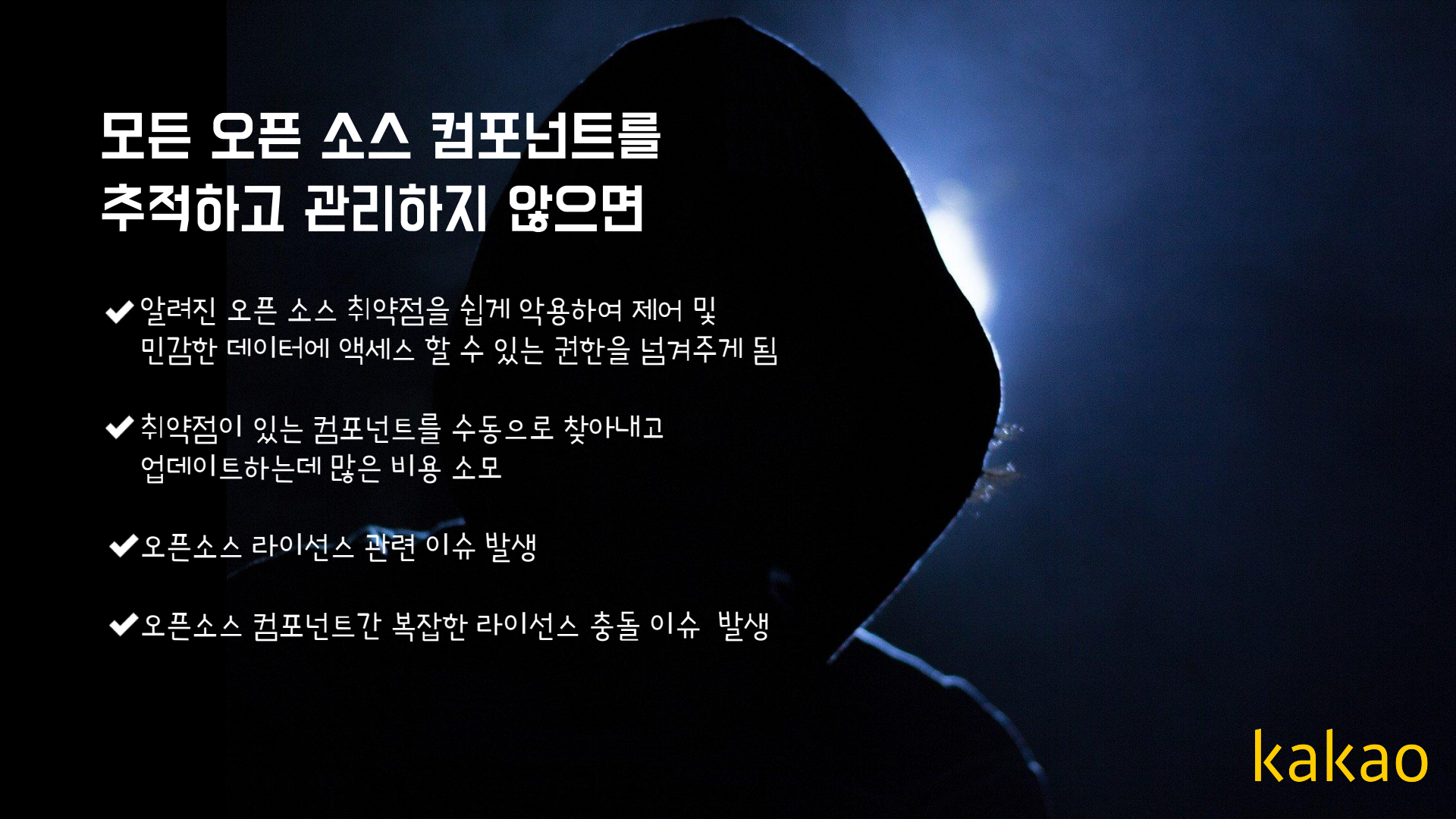
오픈 소스로 작업 할 때 보안 이슈가 큰 비중을 차지하며, 참여자의 57 %가 오픈 소스로 작업 할 때 취약점을 가장 우려

벤더로부터 상업적 지원을 받을 시기를 결정하는 데 어려움이 있음

라이선스 컴플라이언스, 지적 재산권 통제 상실 등 우려

kakao


대부분의 조직에서는
오픈 소스 소프트웨어를
잘 통제하지 못함
성숙하고 정교한 조직은 위험 평가를 위한 보다 주관적인 기준,
즉, 오픈 소스 프로젝트의 전반적인 건강과 신뢰성에 중점을 두고 있음
이러한 조직은 기고자 수, 업데이트 빈도, 취약성 해결 속도, 문제 및
수정 사항의 공개 여부와 같은 오픈 소스 프로젝트에 영향을 줄 수 있는
다양한 요소를 검토함
kakao



모든 오픈 소스 컴포넌트를 추적하고 관리하지 않으면

- ✔ 알려진 오픈 소스 취약점을 쉽게 악용하여 제어 및 민감한 데이터에 액세스 할 수 있는 권한을 넘겨주게 됨
- ✔ 취약점이 있는 컴포넌트를 수동으로 찾아내고 업데이트하는데 많은 비용 소모
- ✔ 오픈소스 라이선스 관련 이슈 발생
- ✔ 오픈소스 컴포넌트간 복잡한 라이선스 충돌 이슈 발생

kakao

SCA 도구 선택 기준 (Gartner)

취약성 데이터베이스

대부분 SCA 에서는 NVD 만을 기반으로 오픈소스 취약점 데이터베이스를 제공함
커뮤니티의 이슈 트래킹의 경우 NVD 에 포함되지 않음

개발자 지원

IDE 및 Repository 연동
코드 추가전 오픈소스 평가기능
추천 업데이트 기능

오픈소스 라이선스 준수

모든 라이선스를 추적하고 보고하는 기능이 있는가
라이선스 정책을 자동으로 설정할 수 있는가

응답 시간 단축

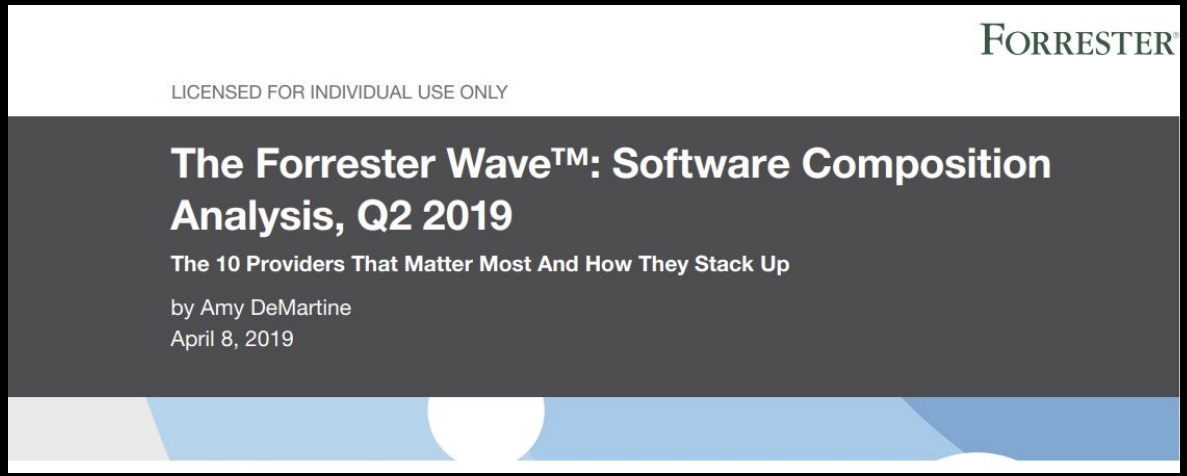
취약성을 빠르게 감지
취약점의 우선순위 결정

보고서 기능

라이선스, 저작권, 버전관리 등
관련정보를 포함한 보고서 발급

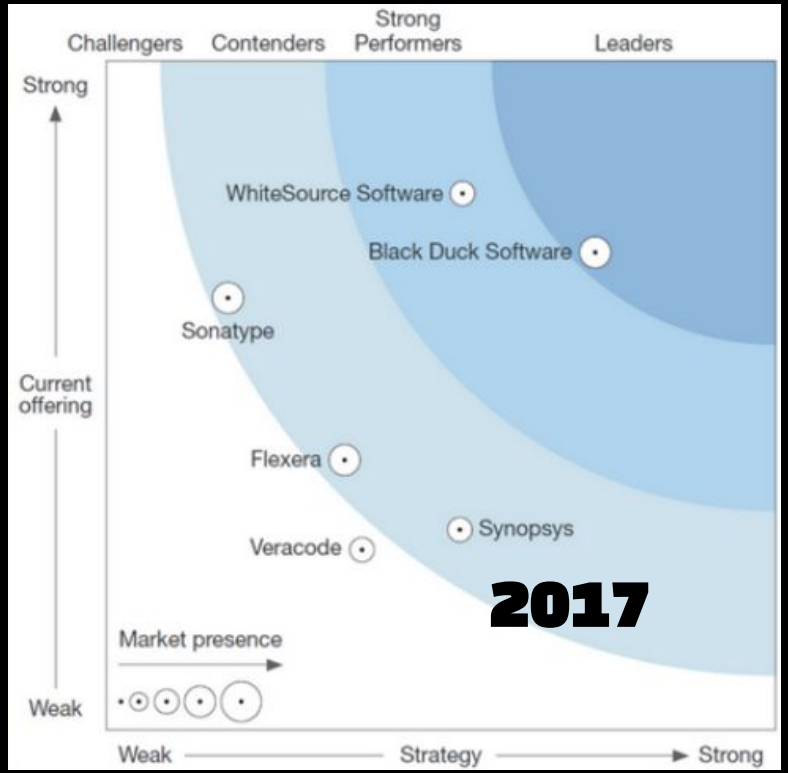
kakao

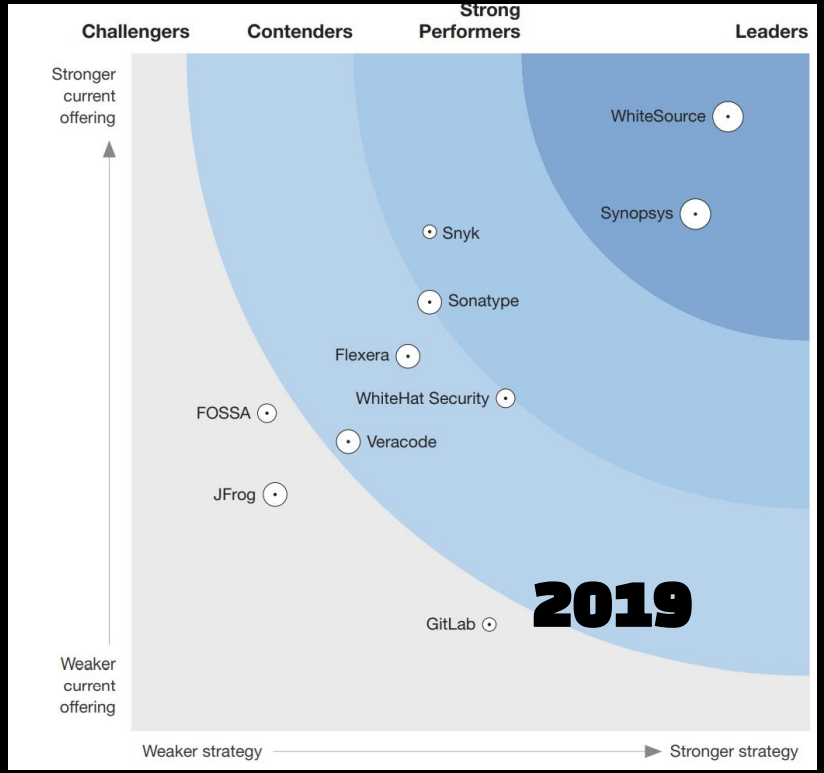
THE FORRESTER WAVE (2019 2Q)



kakao

THE FORRESTER WAVE





kakao

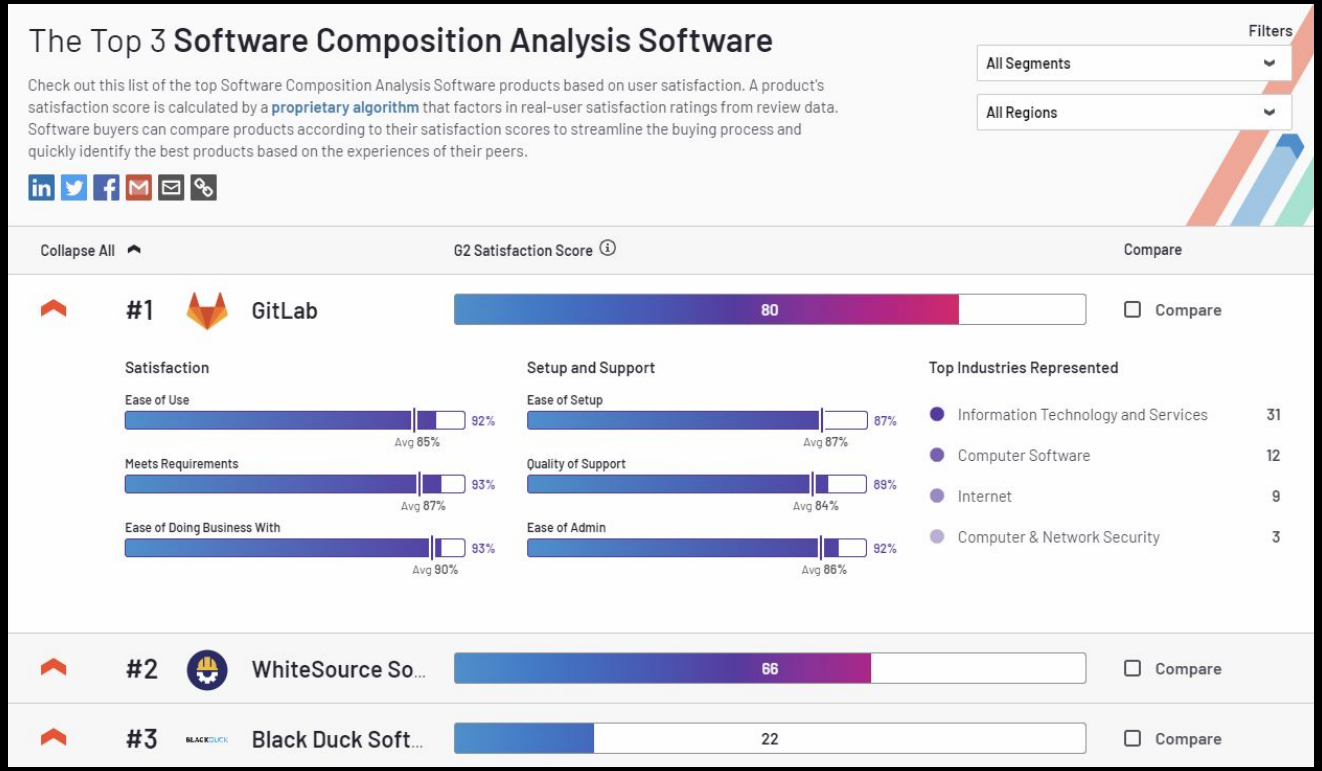
THE FORRESTER WAVE

New service

Existing service

kakao

SCA 서비스들 https://www.g2.com/categories/software-composition-analysis



kakao

SCA 서비스들

GitLab

단일 애플리케이션으로 제공되는
오픈 소스 DevOps 플랫폼

WhiteSource

오픈 소스 보안 및 라이선스 규정
준수 관리 솔루션

Snyk

오픈소스 보안유지를 위한 개발자
우선 보안 솔루션. 도커이미지 분석

Synopsys | Black Duck

오픈소스 소프트웨어 보안 취약성,
규정준수 및 운영 관리

Fossa

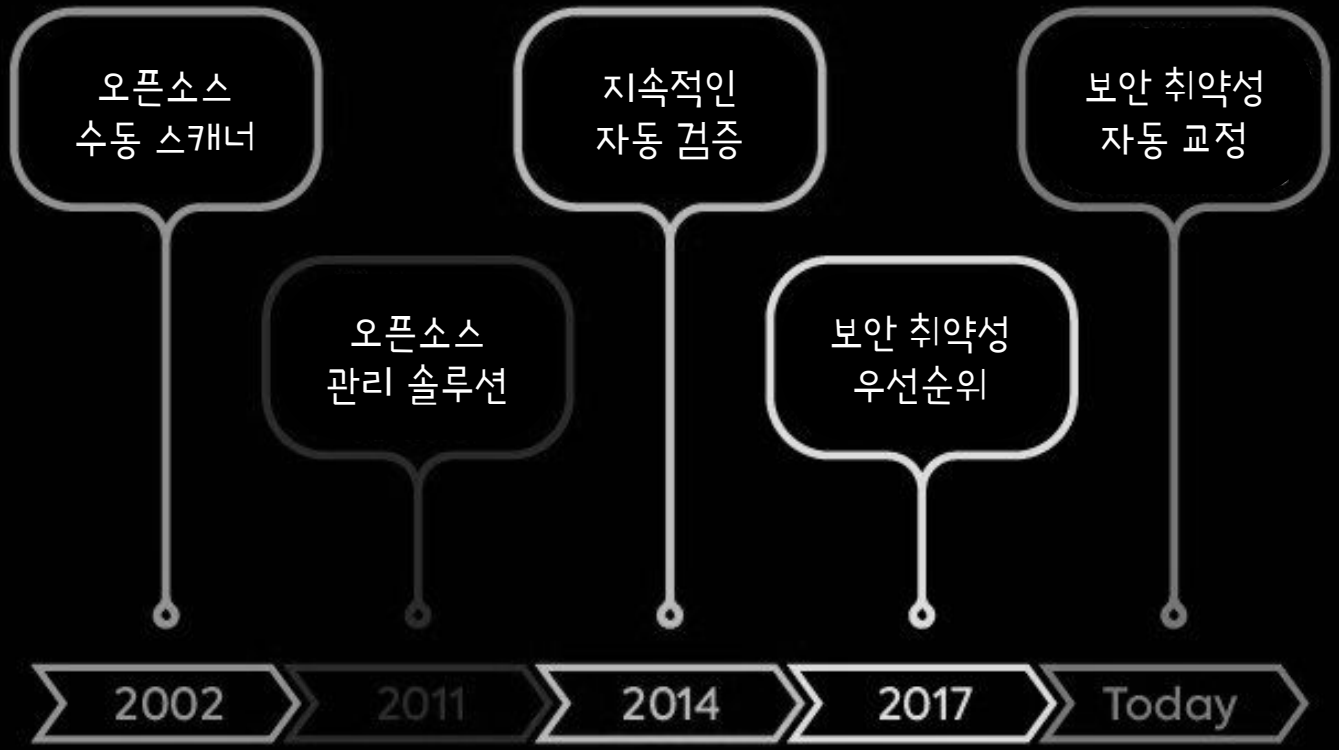
오픈소스 컴포넌트 관리 및
라이선스 준수와 고지문 발급

Flexera | Revenera

오픈 소스 취약성 및 오픈소스 감사
솔루션

kakao

SCA 서비스의 진화 (WhiteSource사례)



kakao

SCA vs SAST

Software
Composition
Analysis

- ✔ 알려진 오픈소스의 취약점을 파악
- ✔ 오픈소스 라이선스 준수사항 관리
- ✔ 발견된 새로운 취약점 모니터링

Static
Analysis
Security
Testing

- ✔ 독점 코드의 결함 파악
- ✔ SDLC 초기에 약점 분석
- ✔ 코드 생산전에 취약점 탐지

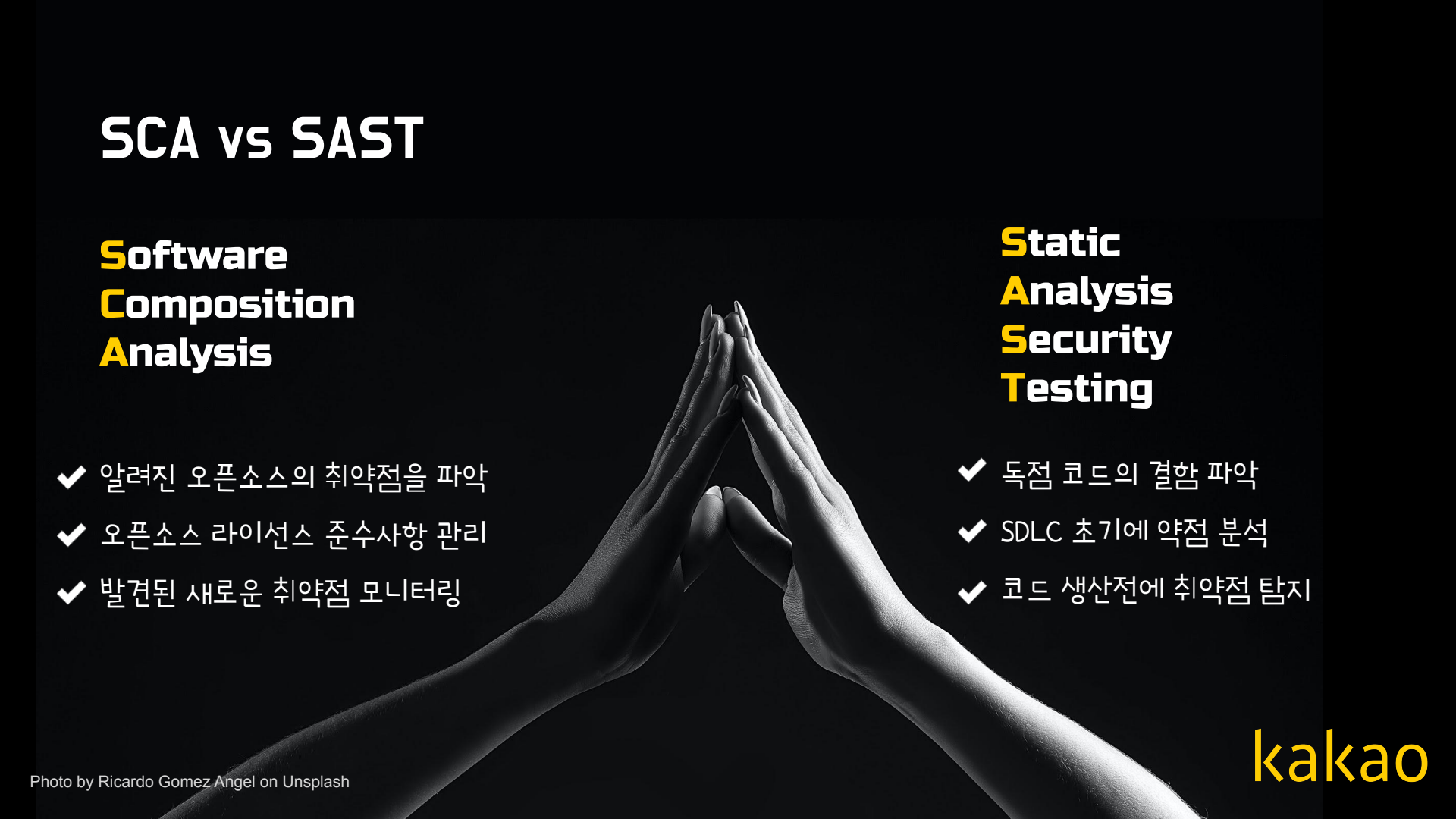


Photo by Ricardo Gomez Angel on Unsplash

kakao

FOSSA

2018년 4명으로 시작
라이선스 준수 관리

+

오픈소스 취약성 관리
2020.10~

2300만달러 Series B

Developer-Friendly

Most comprehensive ecosystem coverage of 20+ languages, with 100% native SPDX support

Native integration into all CI/CD pipelines with an easy-to-use CLI ensures continuous compliance

Code review and pull request integrations prevent bad code from landing into master

Local OSS scan or repo scan, plus compliance violation alerts delivered via Slack, JIRA, or email

Integrations

We support multiple languages and tools, such as JavaScript, Ruby, Clojure, Debian, Golang, Haskell, Java, RPM, Scala, PHP, iOS, Python, .NET, Rust, Perl, C, C++, and many more.

Javascript Slack Python GitHub NPM Gitlab Ruby

완벽한 오픈소스 인벤토리
풍부한 오픈소스 메타 데이터
정교한 정책 거버넌스
리스크 보고서 및 BoM 생성
CI/CD 통합

개발자 친화적
Twitter, Uber, Zendesk 등
JS Foundation 제휴
Linux Foundation 제휴
NPM 제휴
tl;dr 라이선스 관리 서비스

kakao

Snyk

2015년 설립
오픈소스 취약성 관리

+

라이선스 준수 관리
2020.04~

2억달러 Series D

IDE 통합
Pull Request 스캔
CI/CD Security Gate
Docker Container
Production Monitoring

종속성 Tree Viewer
우선 순위 선별 시스템
런타임 모니터링
전담 보안 연구팀이 리뷰
Docker 공식 독점 보안 파트너
IBM Cloud DevOps 통합
Red Hat, OpenShift, Kubernetes

kakao

White Source

2011년 설립
라이선스 준수 관리
오픈소스 취약성 관리
오픈소스 감사
Inventory/BoM

Merge Confidence
2020.11 ~

방대한 데이터 베이스
110억개 이상의 소스코드 파일
200개 이상의 언어 지원
1억개 이상의 라이브러리

취약성 데이터베이스
보안 권고, 이슈 트래킹, NVD 기반

컨테이너 및 서버리스 모든 환경
커밋 수행시 자동 식별
취약성 우선순위 배정
이슈 자동 교정 시스템

Microsoft Azure DevOps 서비스
Gitlab Ultimate 지원
Github Package 지원

kakao

블로그 및 다양한 정보 제공을 통해 커뮤니티 활성화

6 days ago

Microservices Architecture: Security Strategies and Best Practices

Why is microservices security important? Key principles and best practices to ensure your microservices architecture is secure.

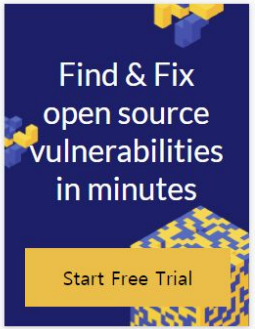
Read Article

13 days ago

Software Composition Analysis Explained

In this article we explain what Software Composition Analysis tool is and why it should be part of

Read Article



20 days ago

White Box Testing Guide

Learn all about white box testing: how it's done, its techniques, types, and

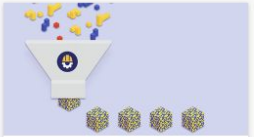
Read Article

27 days ago

Achieving Application Security in Today's Complex Digital World

All about application security - why is the application layer the weakest

Read Article



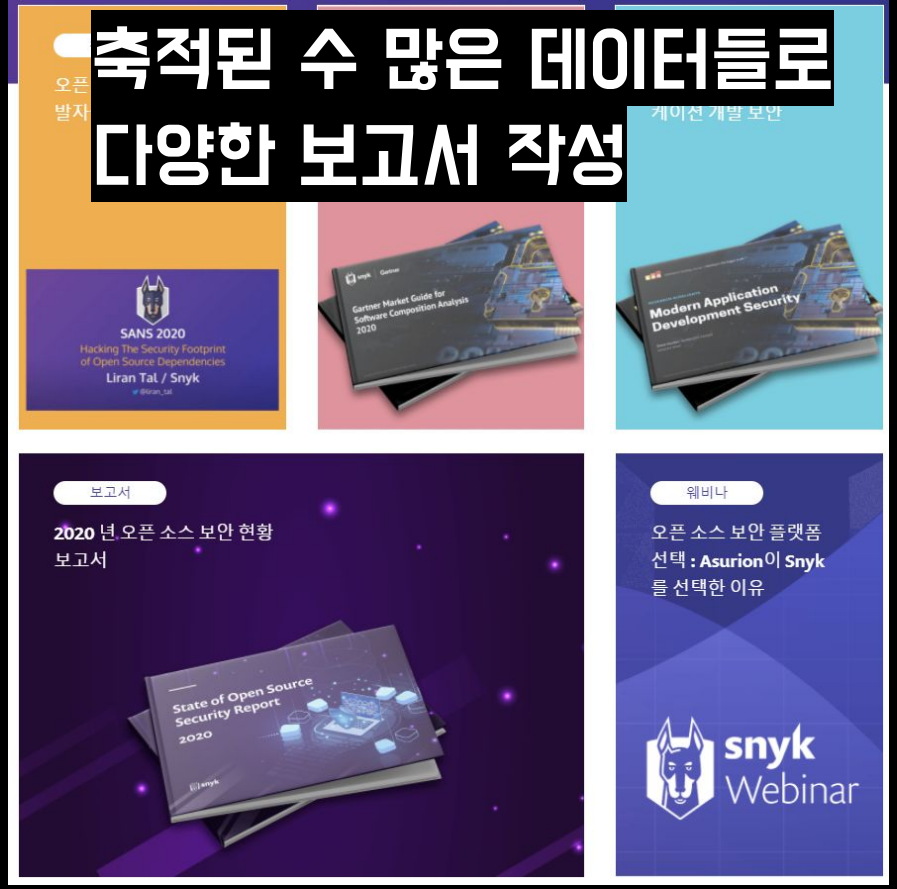
about a month ago

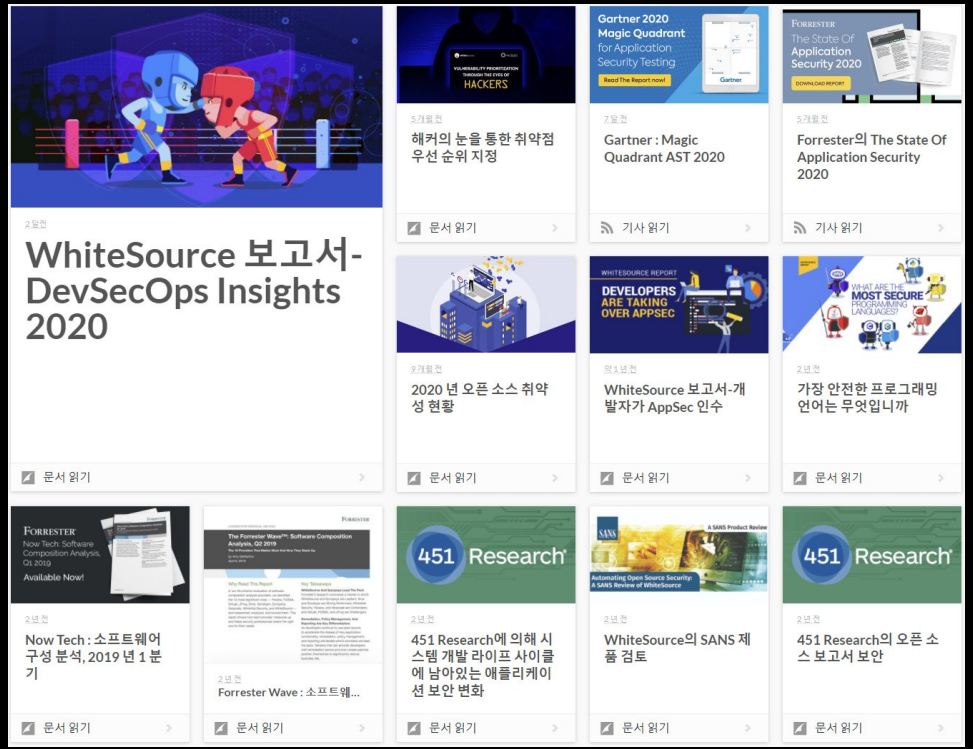
Top Tips for Getting Started With a Software Composition Analysis Solution

Read Article

kakao

축적된 수 많은 데이터들로 다양한 보고서 작성





kakao

Process Automation

Vulnerability Alerts

Navigation for vulnerability remediation

Language Support

Seamless Integration

Programmatic Policy Governance

kakao

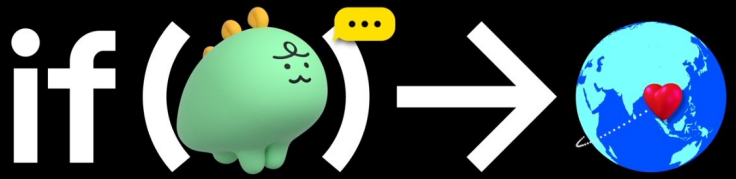
Photo by russn_fckr on Unsplash


Compliance
Security
SCA Market Wave
kakao

if(kakao)2020

OLIVE

카카오에서 제공하는 오픈소스 관리 서비스

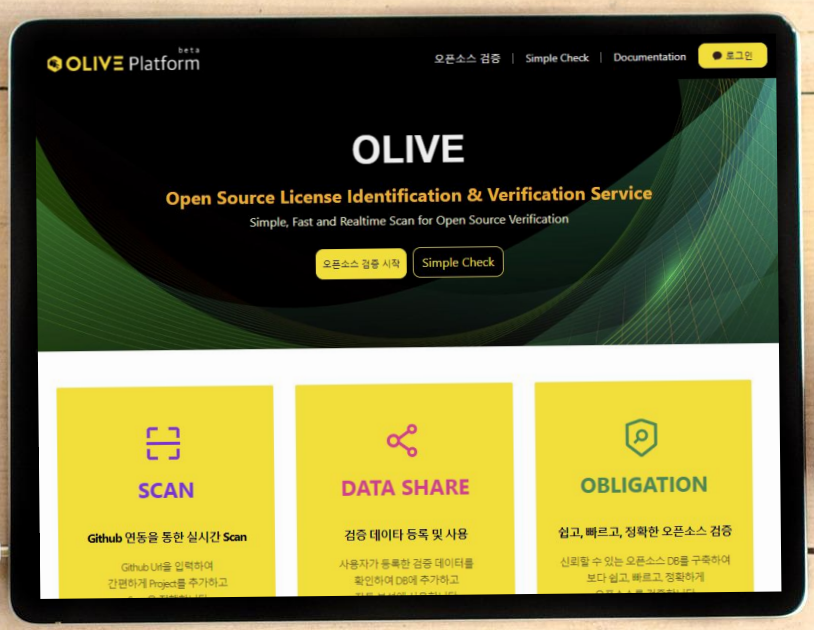


https://if.kakao.com/session/104

황은경 Violet, 김영환 Sean
카카오

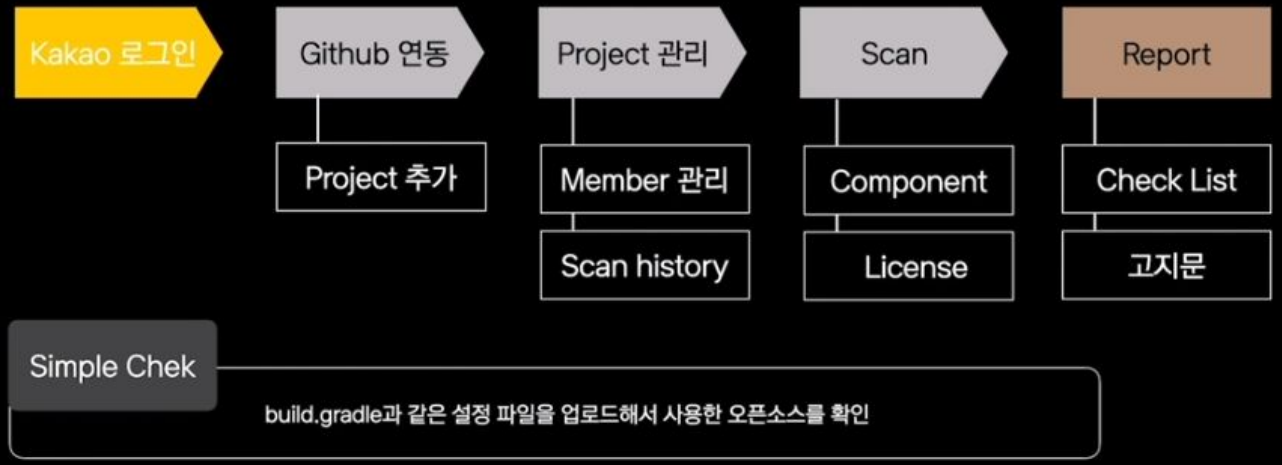
kakao

https://olive.kakao.com



kakao

OLIVE Process



kakao

OLIVE Roadmap

kakao


OLIVE 를 사용하세요!
설문조사 https://forms.gle/KUHNCmPm3ezXEz2V8
kakao