형상관리 저장소의 오픈소스 자동검증

2025-08-26

안랩 김강보

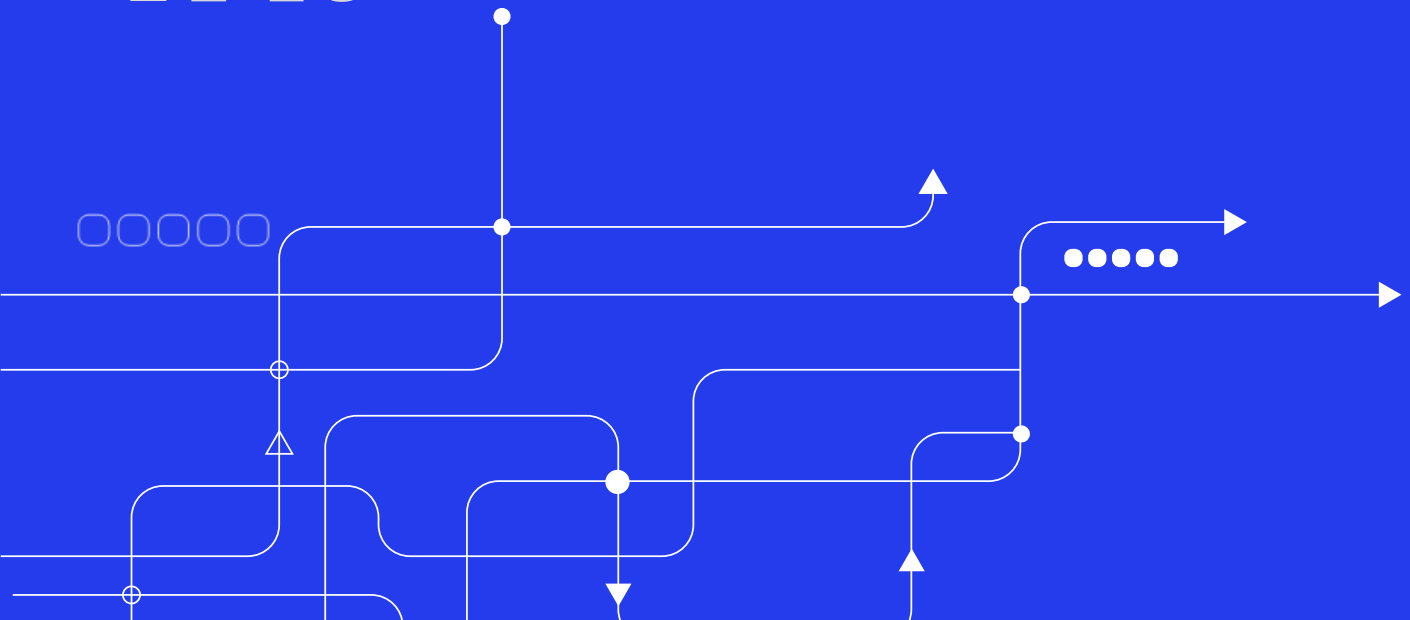
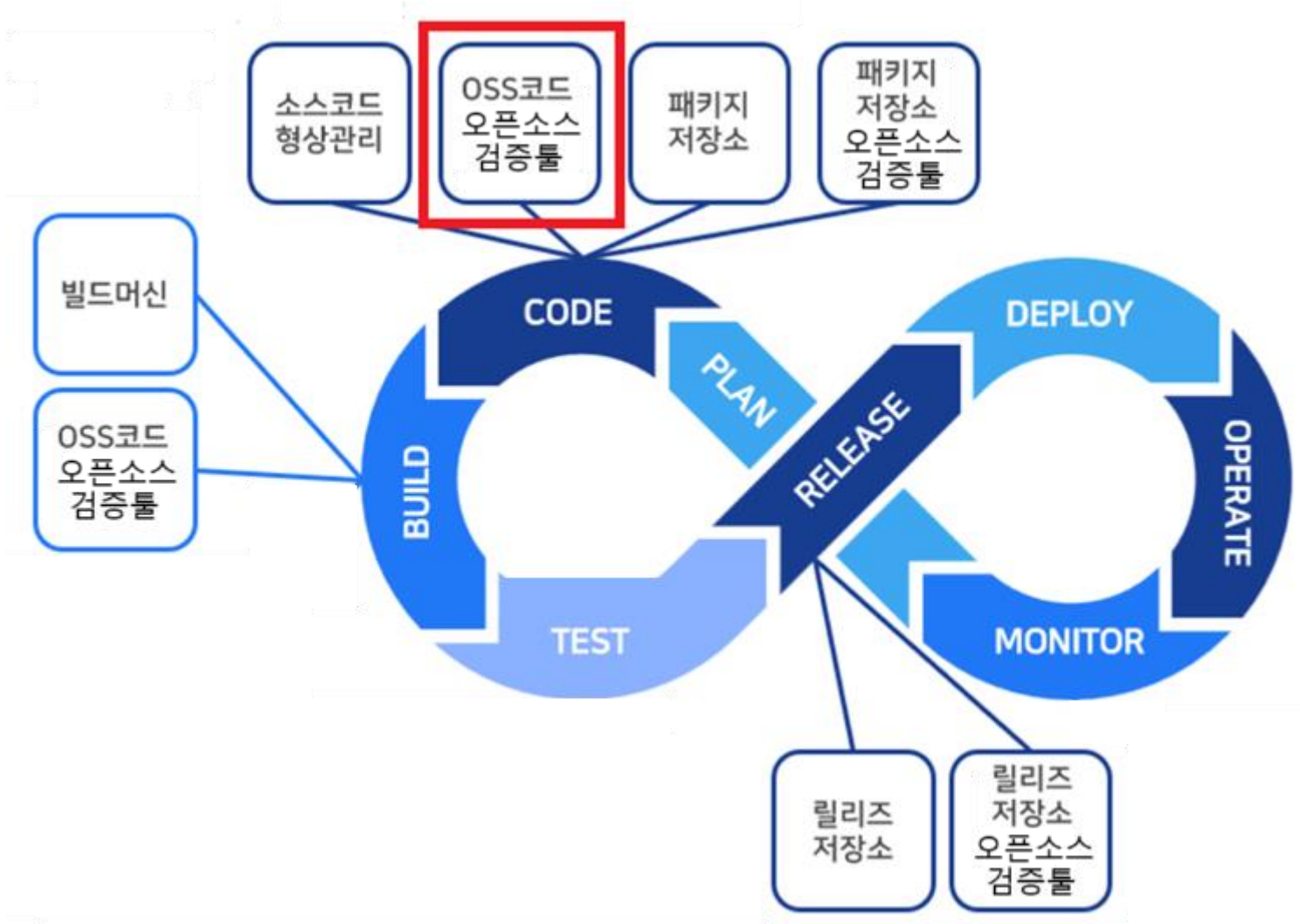


Table of Contents

1. 전체 개발 Loop의 오픈소스 검증

1.1 전체 개발 Loop 중 "CODE"단계에서 형상관리 저장소에 저장된 OSS코드의 오픈소스 검증 필요



1. 전체 개발 Loop의 오픈소스 검증

1.2 개발 초기 단계에서의 문제 발견 및 해결

- CODE(형상관리 저장소)에 저장된 오픈소스는 BUILD 단계에서 오픈소스 검증
- 빌드 전 단계인 CODE에서 오픈소스 검증하여 판정 및 조치 시점을 앞당기는 것이 비용 효율적

    - **개발 초기 단계에서 문제 조기 발견**
        - 개발자가 코드를 커밋하거나 PR(Pull Request)을 생성할 때 오픈소스 검증 가 실행되면, **문제가 있는 라이브러리를 조기에 인지**가능
        - **오픈소스 Compliance 위배와 보안 취약점을 사전에 방지**하고, 나중에 수정하는 비용 감소
    - **개발자 피드백 루프 단축**
        - 빌드 서버에서 나중에 확인하는 것보다, **개발자가 직접 수정할 수 있는 시점에 알려주는 것이 효율적**
        - PR(Pull Request) 단계에서 오픈소스 검증 결과를 확인하면, Reviewer도 함께 검토할 수 있어 협업에 유리
    - **Shift Left 전략**
        - **오픈소스 Compliance 위배와 보안 취약점 발견을 개발 초기 단계로 이동(Shift Left)**

1.3 공통 모듈에서의 오픈소스 조기 발견

- 공통 모듈처럼 **전체 제품에 영향을 미치는 코드에 오픈소스가 포함된 경우**, CODE 단계에서의 검출이 개발 전체 리소스에서 절감 효과가 큼

2. 기존 오픈소스 검증 툴 적용 시 문제점

2.1 기존 오픈소스 검증 툴의 형상관리 저장소 플러그인 미지원

- 많이 사용되는 오픈소스 검증 툴 (Black Duck, Protex, FossID 등)는 형상관리 저장소(예, BitBucket, GitHub)의 플러그인 미지원 (확인 필요)

2.2 타 오픈소스 검증 툴 도입 시, 문제점

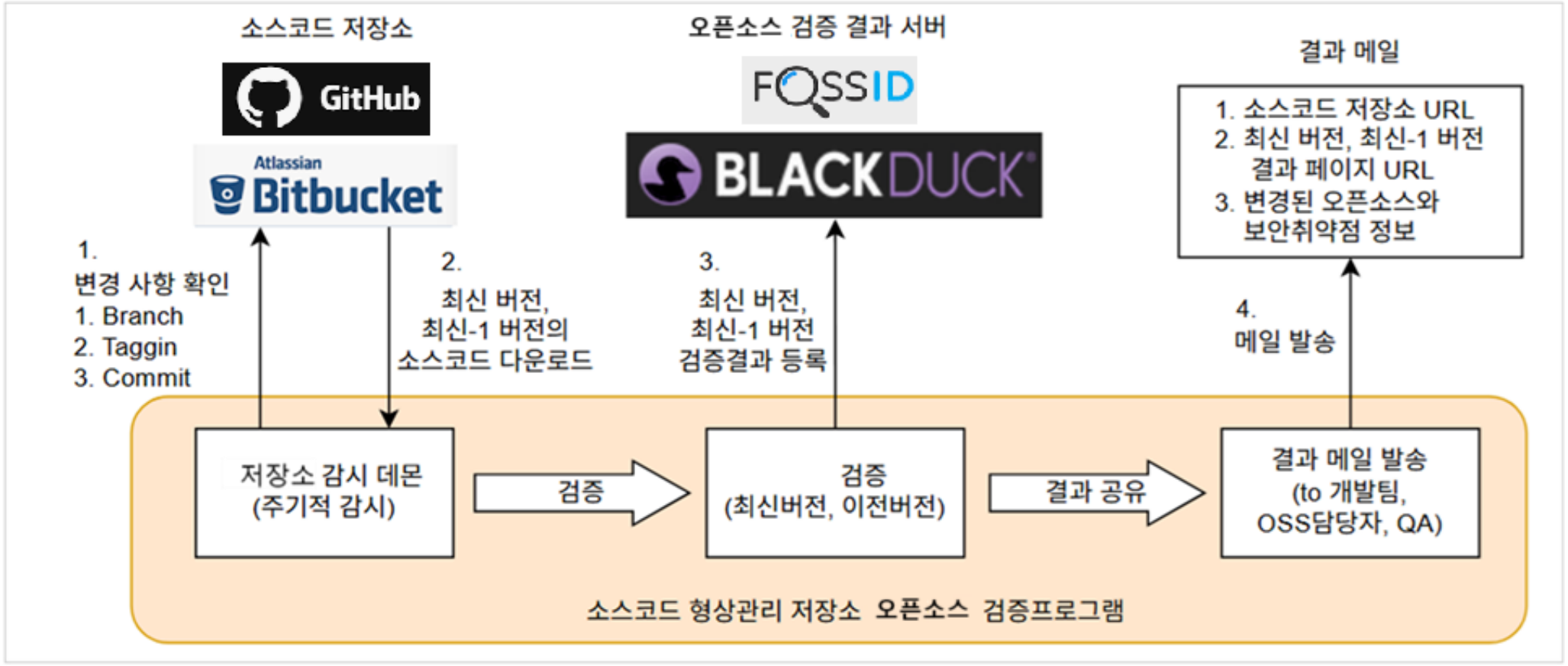
- 형상관리 저장소(예, BitBucket)의 플러그인 지원하는 오픈소스 검증 툴 구매 시, 추가비용 발생 (본체 가격 별도?)

툴 이름	통합 방식	가격 (10명 기준)
Snyk	BitBucket 앱 + UI 리포트	$3,000/year
FOSSA	BitBucket 앱 + UI 리포트	$2,500/year
GitGuardian	BitBucket 앱 + UI 리포트	별도 견적 필요
Debricked	BitBucket 앱 + UI 리포트	$960/year
Xygeni	BitBucket 앱 + UI 리포트	$4,500~$8,100/year
Backslash Security	BitBucket 앱 + UI 리포트	커스텀 견적 필요

- 타 오픈소스 검증 툴의 오픈소스 정보가 기존 오픈소스 검증 툴과 일치하지 않아 오픈소스 정보 컨버터 추가 개발 필요

3. 해결 아이디어

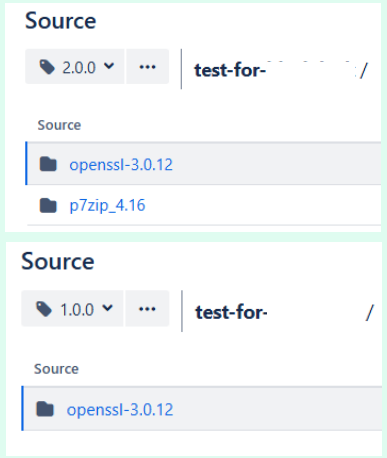
- 기존에 구매 및 적용 중인 오픈소스 검증 툴(예, Black Duck, Protex, FossID 등)을 활용
- 형상관리 시스템(BitBucket, GitHub 등)과 최소한의 네트워크 통신으로 부하를 최소화
- 형상관리 시스템과 별도로 제품 소스코드 저장소의 변경사항을 감시, 오픈소스 검증 시스템을 운영하여 형상관리 시스템과의 관계를 최소화
- 제품 소스코드 저장소에 오픈소스 변경사항이 발생될 경우 개발팀, OSS 담당자에게 결과 알림 메일 발송



4. 테스트 결과

- 개발팀: 소스코드 저장소에 제품 버전별 소스코드 저장
- 소스코드 저장소 오픈소스 검증 시스템(OSS담당자): 소스코드 저장소의 최신 제품 버전별 소스코드 검증 및 메일 발송
- 개발팀: 추가 및 삭제된 오픈소스의 정보 확인 및 조치

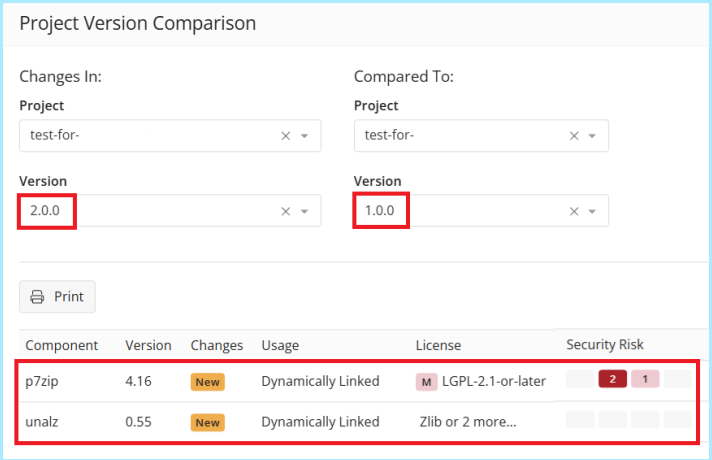
소스코드 저장소



개발팀

- 1.0.0과 2.0.0 버전 소스코드를 소스코드 저장소에 등록

오픈소스 검증 툴 대시보드



소스코드 저장소 오픈소스 검증 시스템

- 최신 2개 소스코드 버전의 오픈소스 자동 검증
- 추가 혹은 삭제된 오픈소스 구별

결과 메일

개발팀

- 추가 삭제된 오픈소스 정보 확인 및 조치

5. 향후 계획

5.1 형상관리 저장소의 변경 사항 감지 옵션 확대

- 버전 Branch
- 버전 Tagging
- 특정 Branch의 Commit 리비전

5.2 형상관리 저장소에 바이너리 파일 존재 시, 바이너리 파일 오픈소스 검증 진행 (바이너리 파일 오픈소스 검증 툴 필요)

- 바이너리 파일 구분
- 바이너리 파일의 오픈소스 검증 진행

감사합니다.