EOSC
ETRI Open Source Center

오픈소스 컴플라이언스 도구의 평가 항목

– 라이선스 검증 도구 도입 검토 후기 –

2022.08.30.

ETRI 오픈소스센터
박정숙

발표 목적

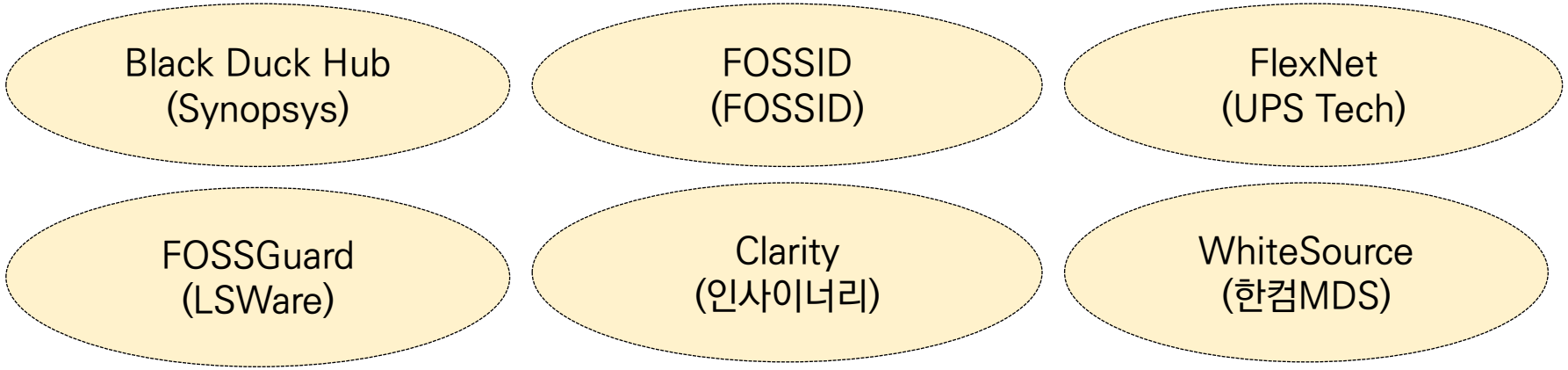
- 기관 차원의 도구 도입은 매우 중요
  - ❖많은 사용자가 고생할 수 있음
  - ❖적지 않은 예산
  - → 신중할 필요 있음
- ETRI의 경험 공유
  - ❖컴플라이언스 도구 평가 메트릭 소개

도구 검토 배경(‘19~ ‘20)

- ETRI는 라이선스 검증 도구로 블랙덕 Protex 도입 운영 중(‘08년~)
- 사용 중인 Protex의 라이선스 기한 만료(~ ‘20.4.) 예정
- 2018년 보안 전문업체 시놉시스가 블랙덕 인수 후 Protex 도구 제공 중단 선언
  - ❖그 후 Protex의 여전히 높은 시장 활용률로 인해 제공 중단을 철회한 상태
  - ❖Protex는 엔진 노화로 성능이 제한되는 등 구조적 단점 존재
    - ✓ 보안취약점 검사 기능 없음
    - ✓ KB 업데이트가 자주 이루어지지 않음 (1회/월)
    - ✓ 기능/성능 개선 없음: Spring 프레임워크, 매우 old한 방식
- 최근 동향
  - ❖최근 보안취약점의 중요성 증가로 보안취약점 검사 도구 수요 증가
  - ❖라이선스 검증 및 보안취약성 검증 기능이 같이 제공되는 형태로 툴들이 출시되고 있음

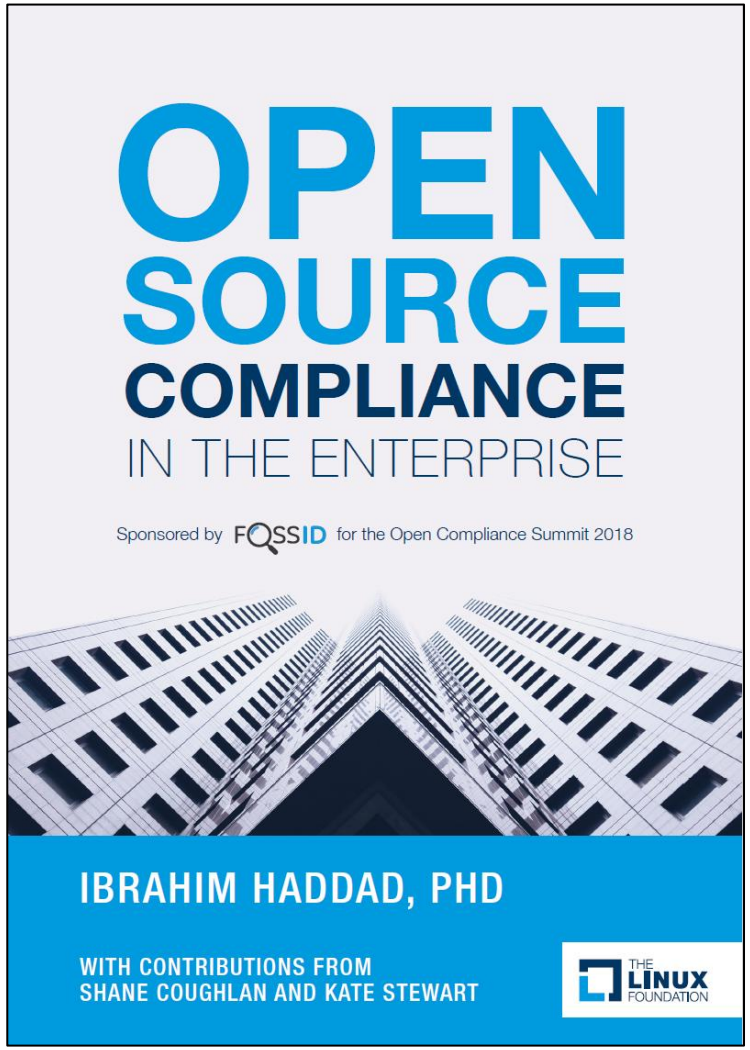
도구 대안들

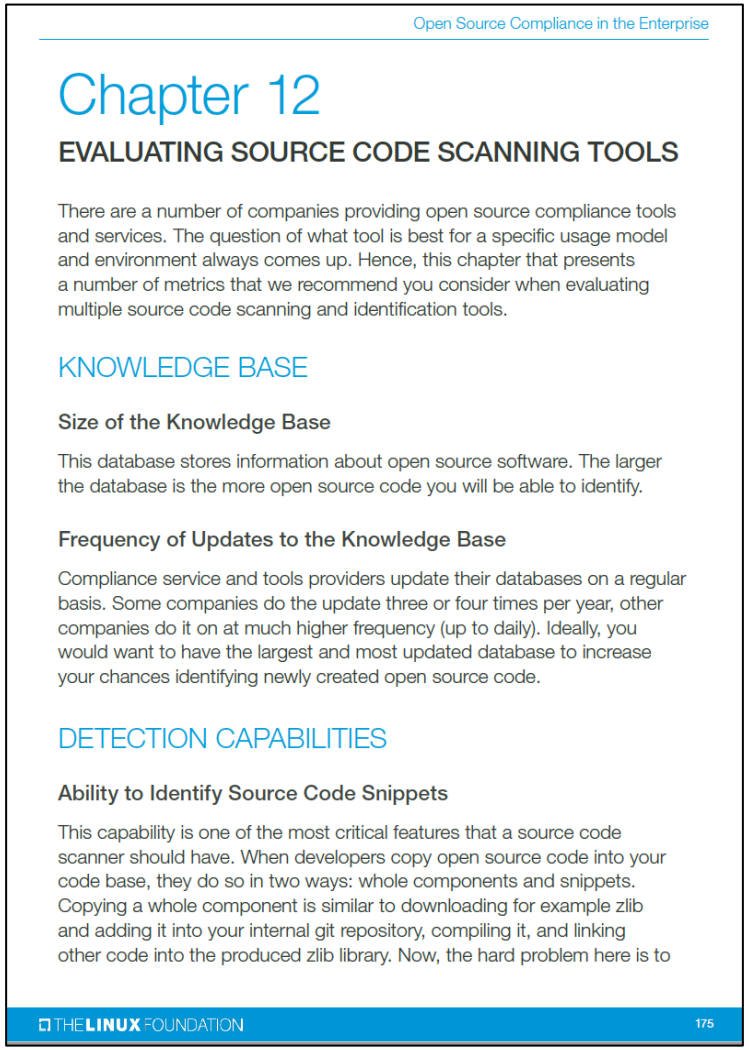
- 2018년 초부터 대안들 조사



제품	Protex	Black Duck Professional	FOSSID	WhiteSource	FlexNet	FOSSGuard	Clarity
검증대상	소스코드	소스코드	소스코드	소스코드	소스코드	소스코드	바이너리코드
검증방식	소스스캐닝	소스스캐닝	소스스캐닝	디지털시그니처	소스스캐닝	소스스캐닝	디지털시그니처

스캐닝 도구 평가 메트릭 참조





Open Source Compliance in the Enterprise

Chapter 12

EVALUATING SOURCE CODE SCANNING TOOLS

There are a number of companies providing open source compliance tools and services. The question of what tool is best for a specific usage model and environment always comes up. Hence, this chapter that presents a number of metrics that we recommend you consider when evaluating multiple source code scanning and identification tools.

KNOWLEDGE BASE

Size of the Knowledge Base

This database stores information about open source software. The larger the database is the more open source code you will be able to identify.

Frequency of Updates to the Knowledge Base

Compliance service and tools providers update their databases on a regular basis. Some companies do the update three or four times per year, other companies do it on at much higher frequency (up to daily). Ideally, you would want to have the largest and most updated database to increase your chances identifying newly created open source code.

DETECTION CAPABILITIES

Ability to Identify Source Code Snippets

This capability is one of the most critical features that a source code scanner should have. When developers copy open source code into your code base, they do so in two ways: whole components and snippets. Copying a whole component is similar to downloading for example zlib and adding it into your internal git repository, compiling it, and linking other code into the produced zlib library. Now, the hard problem here is to

THE LINUX FOUNDATION 175

소스코드 스캐닝 툴 평가 척도 표준

메트릭	세부 사항	의미
Knowledge Base	KB의 크기	KB 크기가 클수록 좋음
	KB의 업데이트 빈도	업데이트 간격이 짧을수록 좋음
탐지 능력	소스코드 스니핏 식별 능력	사용한 스니핏의 식별 최소 크기와 origin/license를 찾는 능력
	소스코드 자동 식별 능력(컴포넌트 및 스니펫)	False positive를 최소화할 수 있는 능력.(candidate 최소화)
사용 편의성	직관적이고 훈련 요구량이 최소인 것	쓰기 편해야 함
운영 능력	M&A 목적을 위한 사용	M&A 목적을 위해 사용가능한지 확인
	다른 audit 모델 지원	Traditional, blind, DIY 중 대부분은 traditional 사용
	프로그래밍 언어 agnostic	여러 프로그래밍 언어에 대해 잘 식별할 수 있는지 점검
	소스 코드 스캔 속도	소스 코드 스캔 속도가 빠를수록 좋음
통합 능력	API와 CLI 지원	기존의 개발 및 빌드 시스템과 통합에 필요
보안 취약점 DB	보안 취약점 DB의 크기	DB 크기가 클수록 좋음
	보안 취약점 DB의 업데이트 빈도	업데이트 주기가 짧을수록 좋음
	보안 취약점 정보의 소스들	보안 취약점 정보의 소스들 검토, 업데이트 메커니즘, 정보 수집에 사용된 소스들, 어떤 권고가 취약점 수정에 사용되는지에 대한 이해
	고급 보안 취약점 발견 지원	Traditional 방법, smart 방법. 스니펫 검사 기능이 있는 것이 좋음
비용	구축 비용	서버 구매, 유지보수, 업그레이드에 지불하는 비용
	운영 비용	툴이 제공하는 결과들을 관리하는 비용
	라이선스 비용	툴을 사용하는 라이선스 비용, SDK 액세스 비용
	통합 비용	툴을 워크플로우와 프로세스에 통합하는 비용
	Lock-in cost	전체 컴플라이언스 환경 구축에 필요한 비용
기타	고급 리포팅 능력	

참고: "Open Source Compliance in the Enterprise", Ibrahim Haddad

EOSC
ETRI Open Source Center

ETRI 스캐닝 툴 평가 메트릭 선정 및 검증 방법

메트릭	세부 사항	ETRI 확인 방법	업체로부터 구할 정보
지식베이스	KB의 크기	-	크기, 수집 구조/방법
	KB의 업데이트 빈도	-	업데이트 주기, 수집량
탐지 능력	소스코드 스니펫 식별 능력	스니펫 추가 후 식별 가능한지 확인	-
	소스코드 자동 식별 능력	False positive 최소화 기능 확인	-
사용 편의성	직관적이고 훈련 요구량 최소	사용 경험에 의해 판단	-
운영 능력	다른 audit 모델 지원		어떤 Audit 모델 사용하는지 확인
	프로그래밍 언어 agnostic	언어별 시험(C++, Java, C, Go) 비교	어떤 특정 언어들을 지원하는지
	소스 코드 스캔 속도	타이머를 이용한 스캔 소요 시간 측정	DB 구성 방식 문의
통합 능력	API와 CLI 지원	-	업체에 문의
보안 취약점 DB	보안 취약점 DB의 크기	-	크기, 수집 구조/방법
	보안 취약점 DB의 업데이트 빈도	-	업데이트 주기, 수집량
	보안 취약점 정보의 소스들	시험 확인	-
	고급 보안 취약점 발견 지원	시험 확인	-
비용	구축 비용	-	견적서
	운영 비용	-	견적서
	라이선스 구매 비용	-	견적서
	통합 비용	-	견적서
기타	고급 리포팅 능력	- 리포팅 양식, 리포트 출력 포맷 확인	ETRI 요구에 tailoring 해 줄 수 있는지 확인

분석 및 평가 결과 표현(예)

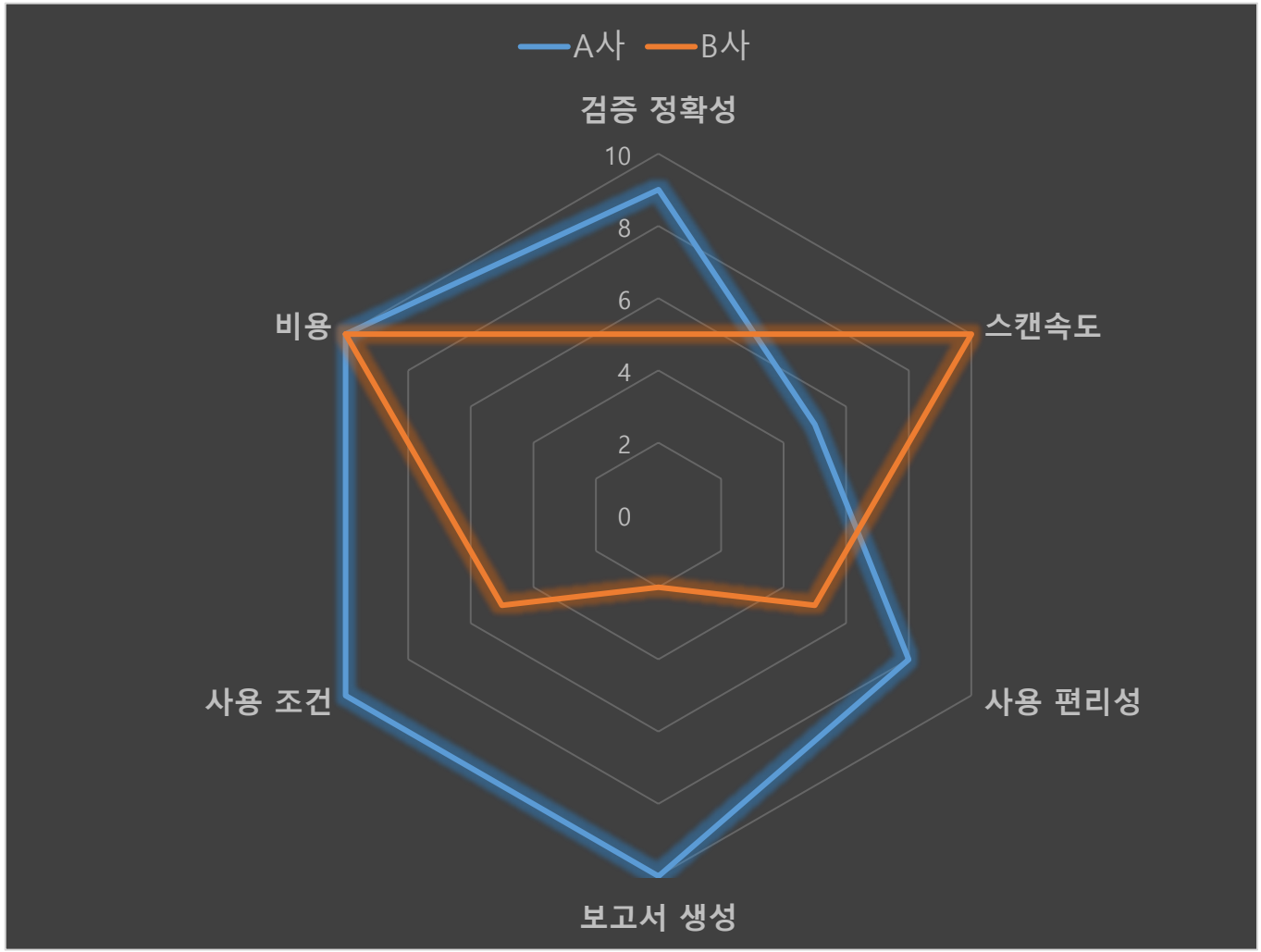
❑ 특성 분석

비교 항목	Protex(기존)	A사	B사
거래처			
소스 검사 기능	○		
Snippet 검사 기능	○		
의존성 검사 기능	×		
보안취약점 검사 기능	×		
스캔 속도	보통		
도구 정확성	우수		
전문가 검증 능력	우수		
보고서	우수		
플랫폼 연동 API	○		
사용 친숙도	좋음(익숙함)		
클라이언트 설치	필요		
도구 사용 조건	제한(인원수)		
비용			

❑ 장단점 비교

비교 항목	Protex(기존)	A사	B사
장점	·가장 오래된 검증 도구로 시장 활용률 높음 ·가독성 높은 보고서 생성 ·가장 익숙함		
단점	·클라이언트 설치 필요 ·사용자 계정 제한적 ·기능 업데이트 없음		

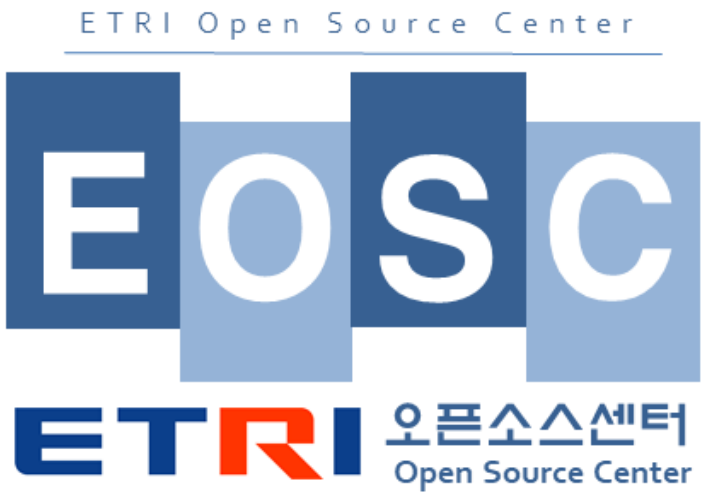
분석 및 평가 결과 표현(예)



결론

- 분석/비교한 결과, 절대적으로 우수한 스캐닝 도구는 선정하기 힘들었음
- 기관별 도입 목적 고려, 평가지표 간 가중치 부여 필요
- 평가 지표는 근거 증빙 자료로 활용성이 높음
- 컴플라이언스 도구들에 대한 공통 평가지표 수립 필요


EOSC
ETRI Open Source Center


ETRI Open Source Center
EOSC
ETRI
오픈소스센터
Open Source Center