

텔레칩스의 오픈체인 인증과 남은 과제

2025.12.09

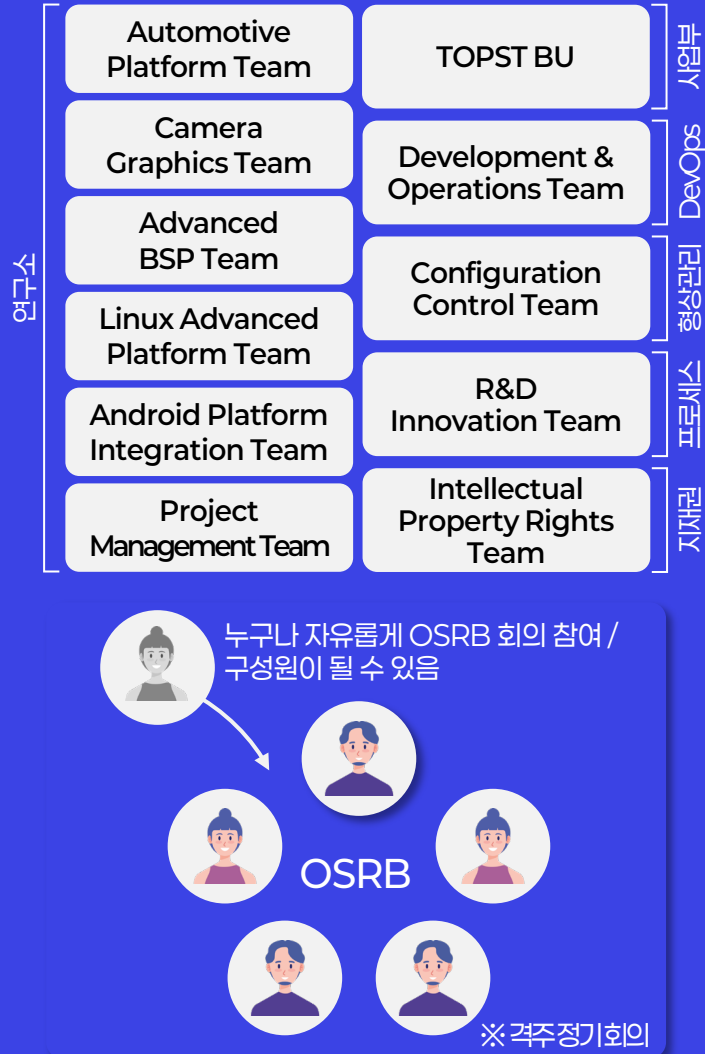
텔레칩스 지식재산권팀

연지영 매니저 (chloe.yeon@telechips.com)



1 오픈체인(ISO/IEC 5230:2020) 인증 취득

OSRB 구성원



구축 단계



OSS 점검 방안

가. 건 별 점검

- 개발 완료 건은 필요시 수동 점검 (소스코드 업로드, 저장소 연동 등)

나. 모듈 점검 – 개발단계

- 모듈(빌드리스 코드) 대상 점검
- Repository - dev branch에 Full Request 발생 시 점검

다. SDK 점검 – 릴리즈 단계

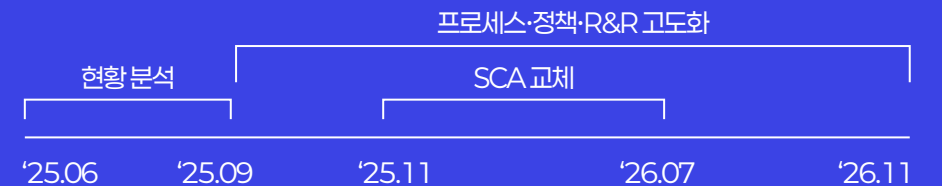
① Yocto

- Yocto 와 AOSP SDK를 구분하여 적합한 오픈소스 점검 방안 마련
- Yocto는 자체 SBOM 기능 활용
- ※ Yocto는 checksum 기능이 있지만 실제 소스코드와 checksum이 다를 수 있기 때문에 (휴먼에러) SCA 도구 점검 필요

② AOSP

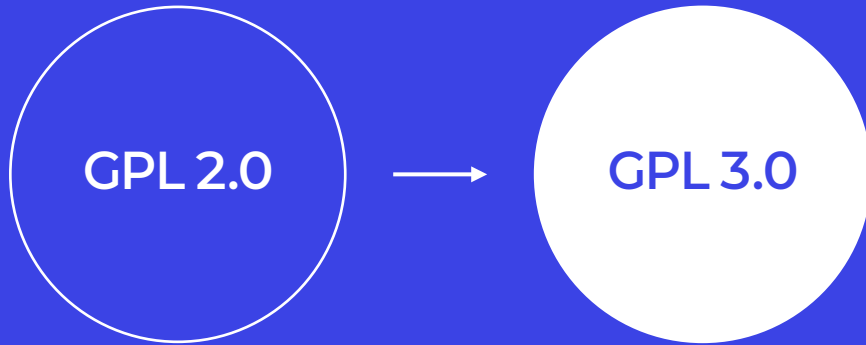
- Blackduck 1회 최대 점검 가능
- 사이즈 10GB 제한 이슈
- AOSP 중 텔레칩스가 오픈소스를 갖는 코드 점검

오픈체인 준비 기간(1년 5개월)



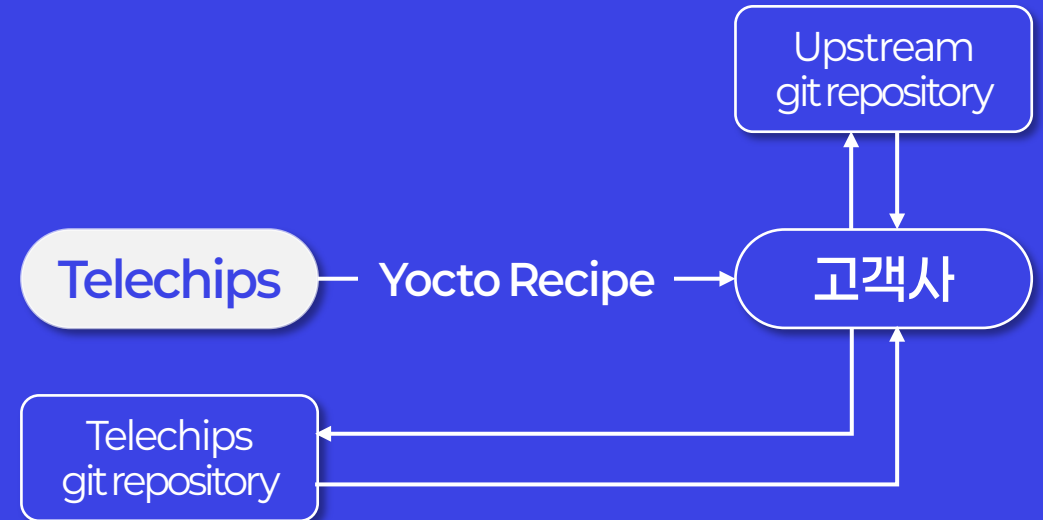
2 남은 과제 > Yocto와 GPL 3.0 이슈

Yocto Project의 라이선스 변경 이슈



- Yocto Project의 GNU OSS 중 GPL 3.0으로 라이선스가 변경되는 사례 등장
- GPL 2.0으로 다운그레이드 → 기술 간극으로 호환 이슈 발생 가능
- 다른 오픈소스로 대체 ? → 기능적 불완전성, 빌드 실패 가능성
 - gperf, gettext를 제거하려면 모든 종속 패키지 패치 필요
 - 제거 시 Yocto 자체를 사용 못할 수 있음

Yocto Recipe의 라이선스 준수



- Yocto Recipe에 대한 라이선스 의무 (소스코드 다운 + 빌드 스크립트)
- Yocto Recipe가 빌드하는 오픈소스
- 우리가 빌드하지 않고, 우리 repo에서 배포된 것이 아니지만 고객사가 활성 처리할 수 있는 오픈소스

2 남은 과제 > Android SDK 점검 고도화

Android SDK 점검 문제점

- Android SDK는 수많은 오픈소스 라이브러리와 도구를 포함
- 수많은 구성 요소와 복잡한 의존성으로 정확한 점검이 어려움
- Android 13+에는 SBOM Generator 기능이
추가되었지만 Linux yocto의 SBOM 생성 기능에 비해
정확도가 많이 떨어짐
- 여러 개발 부서가 작업하는 특성상 Android SDK 점검
결과에서 검출된 이슈의 담당자를 식별하기 어려움

검토 고려 중인 방법

1. 블랙덕 점검 방법 변경

Origin AOSP를 점검 후 프로젝트를 Clone하여
텔레칩스가 Ownership 갖는 버전 점검

2. AOSP 점검을 위한 새로운 도구 검토

- FOSSLight
- Android SBOM Generator
- 기타

3. 기타

2 남은 과제 > 보안취약점

보안취약점 대응 범위와 대상 판단

오픈소스 EOL

<

반도체 칩의 EOL

최소 10년 이상 ▲

Longterm release kernels

Version	Maintainer	Released	Projected EOL
6.12	Greg Kroah-Hartman & Sasha Levin	2024-11-17	Dec, 2026
6.6	Greg Kroah-Hartman & Sasha Levin	2023-10-29	Dec, 2026
6.1	Greg Kroah-Hartman & Sasha Levin	2022-12-11	Dec, 2027
5.15	Greg Kroah-Hartman & Sasha Levin	2021-10-31	Dec, 2026
5.10	Greg Kroah-Hartman & Sasha Levin	2020-12-13	Dec, 2026
5.4	Greg Kroah-Hartman & Sasha Levin	2019-11-24	Dec, 2025

- EOL 이후 발생한 CVE는 깃로그를 서칭 필요
 - 담당자는 있지만, 규모의 팀이 구성되어 있지 않아 어려움이 있음
- CVE에 즉각적으로 대응해야 하는가?

Vendor

Tier 1

OEM

사이버시큐리티 충족을 위해
밴더사는 무엇을 어떻게 해야 하는가?

감사합니다.