oniro

Eclipse Oniro Compliance Toolchain

Continuous Compliance
the Open Source Way

ARRAY

TECHPARK SÜDTIROL/ALTO ADIGE

ECLIPSE ONIRO COMPLIANCE TOOLCHAIN

Who

ARRAY

TECHPARK SÜDTIROL/ALTO ADIGE

What

oniro

other EF projects?

Standards

OPENCHAIN

SPDX

REUSE SOFTWARE

Tools & "Friends"

fossology

ScanCode

yocto PROJECT

debian

more to come...

Welcome us :)

WHAT IS THE PROJECT ABOUT?

Sustainability

release fast, release often vs. testing, compliance, security:continuous *pain*?

- decouple CC from development process (through repo mirrors)
- **parallel processes**, meeting only when needed
- reduce pain for developers to a minimum

Data Aggregation

multi-arch multi-kernel OS
(~ multiple IoT projects with a common core):
copyright & license
metadata aggregation
is key

CONTINUOUS COMPLIANCE

(the Open Source Way)

Data Representation

present data in a comprehensive and meaningful way

Seeking help from friends

too many aliens at your party: friends or troublemakers?
Ask a friend who can vouch for them:
Debian

Giving back to the community

- fully open and transparent process
- upstream first, also in compliance
  - to Debian and Yocto
  - to upstream component projects

LAST 12 MONTHS ACHIEVEMENTS

Audit Work:

(with the help of "friends")

- ~3.7M source files audited
- ~1.2K source components/variants
- 98% coverage of current project snapshots
- ~80 IP issues managed
- several issues raised and fixed upstream (zephyr, intel-media), others pending
- OpenChain (ongoing)

Metadata Collection:

(TinfoilHat)

- Support multiple Yocto fetchers
- Yocto layers and layer overrides
- CVE metadata
- 1st Database API POC
- 1st POC to track upstream source files to binary files in Yocto
- 1st POC of BANG integration for deps scanning

Metadata Analysis:

(Aliens4Friends)

- many incremental improvements based on Audit Team suggestions
- better import of findings from Scancode and Debian in Fossology
- component variants management
- session management (for pipelines)

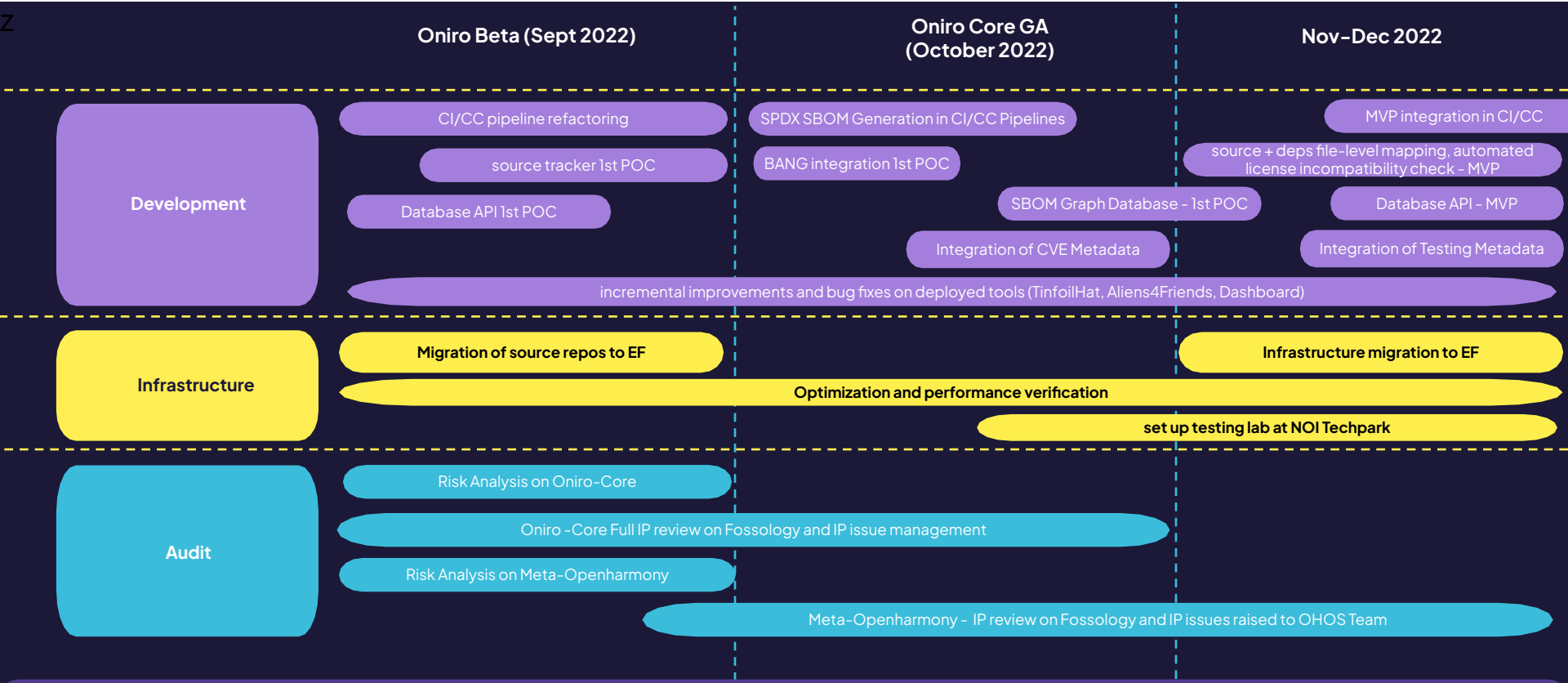
CI/CC Pipelines:

- complete refactoring
- build matrix included in pipeline definition
- infrastructure optimization
- automatic generation of SPDX SBOM, filtered by released images

Dashboard:

- optimization
- better filtering with more filter options
- better handling of component variants and tags
- integration with Gitlab pipelines via url param.
- CVE metadata integration

ROADMAP


Oniro Beta (Sept 2022)
Oniro Core GA (October 2022)
Nov-Dec 2022
Development
CI/CC pipeline refactoring
SPDX SBOM Generation in CI/CC Pipelines
MVP integration in CI/CC
source tracker 1st POC
BANG integration 1st POC
source + deps file-level mapping, automated license incompatibility check - MVP
Database API 1st POC
SBOM Graph Database - 1st POC
Database API - MVP
Integration of CVE Metadata
Integration of Testing Metadata
incremental improvements and bug fixes on deployed tools (TinfoilHat, Aliens4Friends, Dashboard)
Infrastructure
Migration of source repos to EF
Infrastructure migration to EF
Optimization and performance verification
set up testing lab at NOI Techpark
Audit
Risk Analysis on Oniro-Core
Oniro -Core Full IP review on Fossology and IP issue management
Risk Analysis on Meta-Openharmony
Meta-Openharmony - IP review on Fossology and IP issues raised to OHOS Team

CHALLENGES: HELP WANTED

Graph Database

- mapping upstream sources to binaries at file level
- mapping runtime dependencies in languages other than C/C++
- set inbound and outbound license incompatibility rules
- check license incompatibilities via graph queries

Testers wanted!

- we are willing to test our compliance toolchain on other projects, to ensure compatibility with all versions of Yocto
- good candidates could be other Yocto-based projects, or application projects that can be deployed on Yocto
- explore also other environments, different from Yocto

Share Audit Work – Public API Design

- we would like to share reviewed copyright and license metadata so that they can be reused in other projects
- we need feedback and ideas on what we should offer via public API and how

Thank you!

Communication channels

- mailing list: oniro-compliancetoolchain-dev@eclipse.org
- project repos: https://gitlab.eclipse.org/eclipse/oniro-compliancetoolchain