New approach to Software Composition Analysis

Stefan Just

Codescoop Oy

oscar
eclipse.org

Hello!

Stefan Just, heading the Europe Codescoop branch

Codescoop is a team of enthusiasts with strong roots in the Open Source ecosystem, that joined forces on a mission to ease working with Open Source (and Inner Source, that is…)

Agenda topics

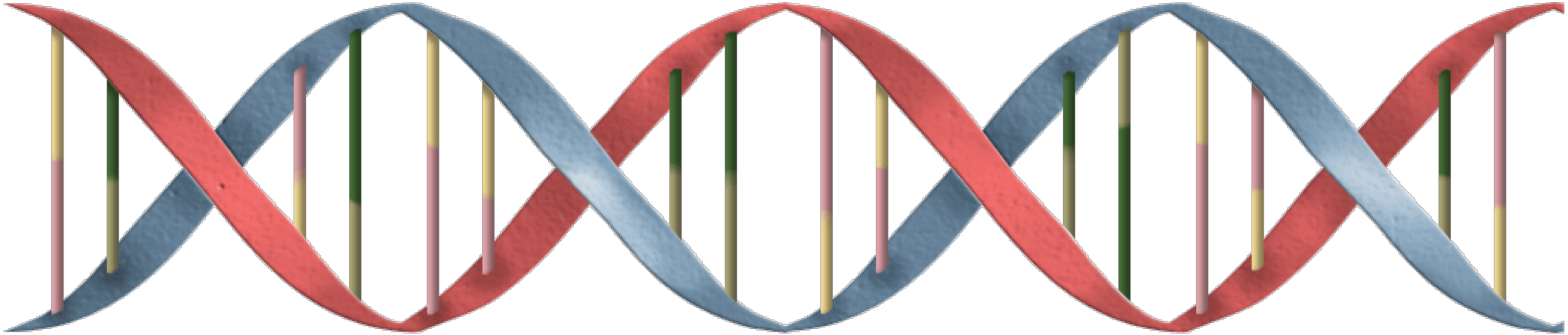
- What is SCA?
- Who asks questions around SCA? And why?
- What does exist ? What is missing ?
- OSCAR ? Anybody said OSCAR ?

What is SCA? Why does it matter?

- Software Composition Analysis
  - Tools around understanding what is in your stack
  - Mainly Open Source in your stacks, but not only
- Topic areas addressed by SCA
  - Compliance (can I use this ?)
  - Security (Will I be at risk ?)
  - Quality (Is this stuff better than alternatives ?)
  - Costs (of Review, Maintenance, Support, Mgmt, …)
  - …

Agreed common denominator

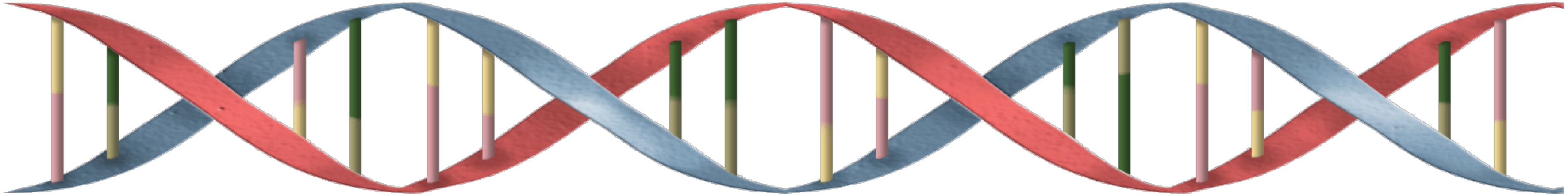
License Compliance



Security Management

But is that all that SCA is ?

License Compliance



Security Management

Export Restrictions

Supply Chain Management

Quality

Functional Analysis

Effort / Complexity

Architecture / Re-Use

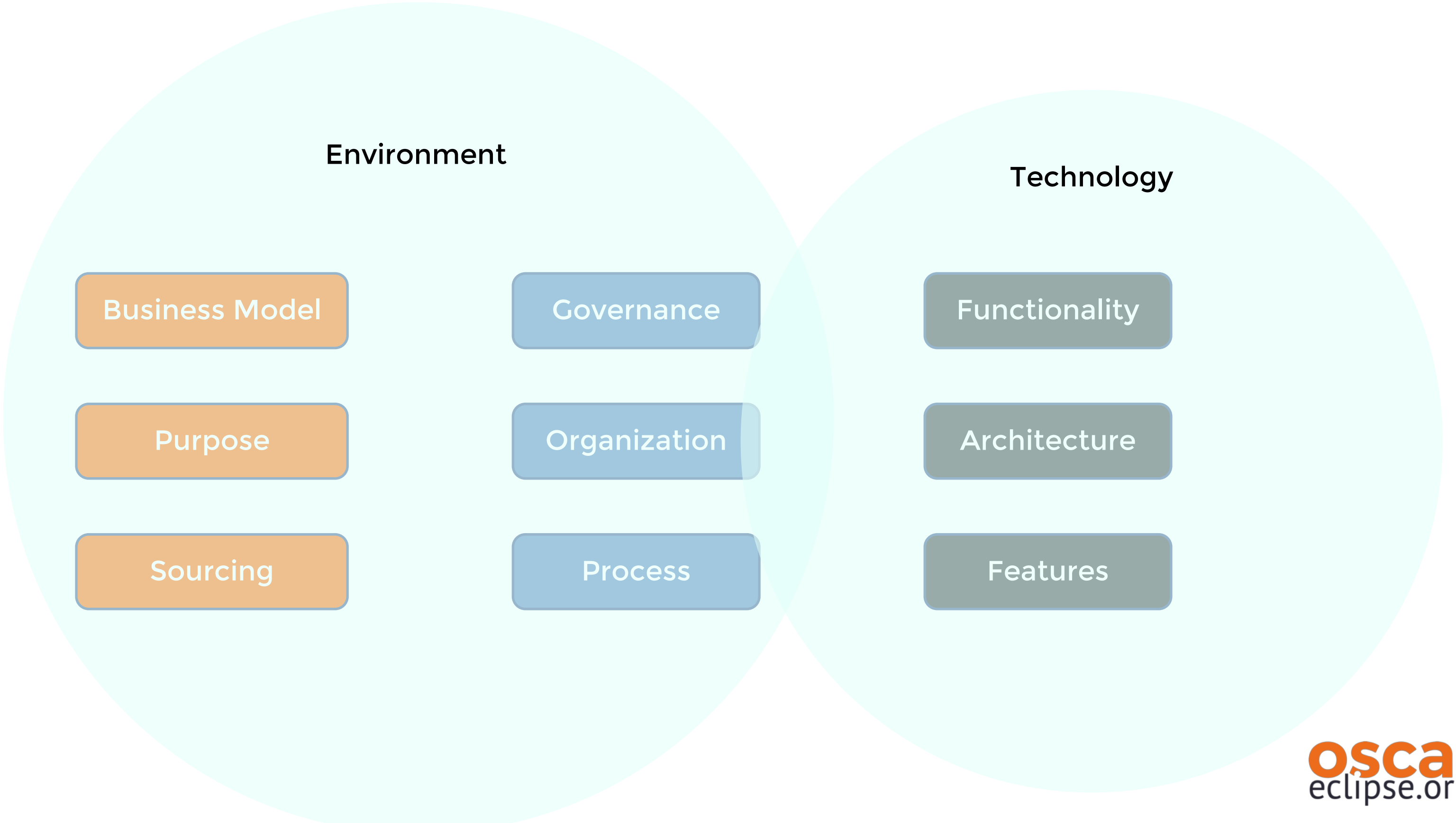
Obligations

Contribution/ Distribution

Support

oscar
eclipse.org

Holistic viewpoint



Environment

Business Model

Purpose

Sourcing

Governance

Organization

Process

Technology

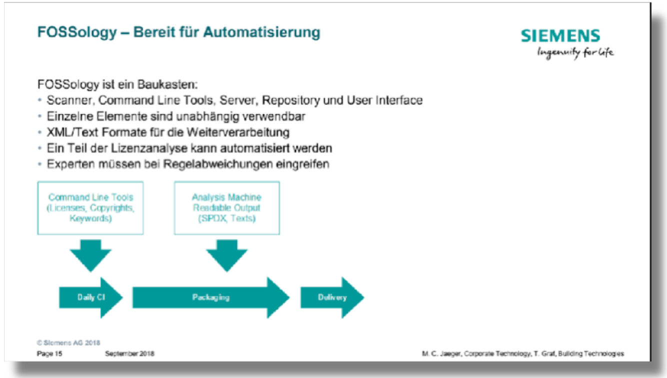
Functionality

Architecture

Features

oscar
eclipse.org

This is what companies do to manage their OSS utilization



FOSSology – Bereit für Automatisierung

SIEMENS
Ingenuity for life

FOSSology ist ein Baukasten:

- Scanner, Command Line Tools, Server, Repository und User Interface
- Einzelne Elemente sind unabhängig verwendbar
- XML/Text Formate für die Weiterverarbeitung
- Ein Teil der Lizenzanalyse kann automatisiert werden
- Experten müssen bei Regelabweichungen eingreifen

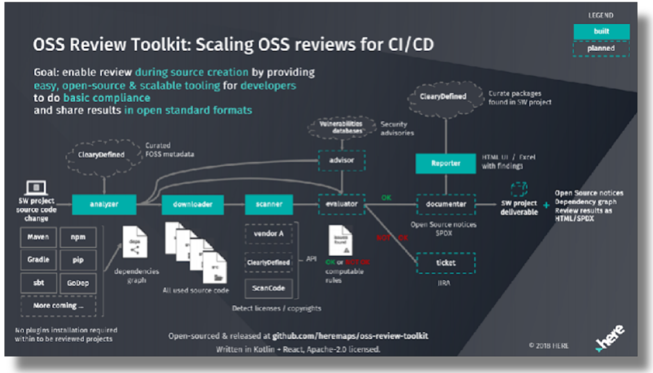
Command Line Tools (Licenses, Copyrights, Keywords)

Analysis Machine Readable Output (SPDX, Texts)

Daily CI → Packaging → Delivery

© Siemens AG 2018

Page 15 September 2018 M. C. Jaeger, Corporate Technology, T. Graf, Building Technologies



OSS Review Toolkit: Scaling OSS reviews for CI/CD

LEGEND
built
planned

Goal: enable review during source creation by providing
easy, open-source & scalable tooling for developers
to do basic compliance
and share results in open standard formats

SW project source code change → analyzer → downloader → scanner → evaluator → documenter → SW project deliverable

Maven, npm, Gradle, pip, sbt, GoDep, More coming ...

No plugins installation required within to be reviewed projects

ClearyDefined — Curated FOSS metadata

dependencies graph

All used source code

vendor A, ClearlyDefined, ScanCode — API

Detect licenses / copyrights

Vulnerabilities databases — Security advisories

advisor

OK or NOT OK computable rules

OK

NOT OK → ticket — JIRA

Open Source notices SPDX

ClearyDefined — Curate packages found in SW project

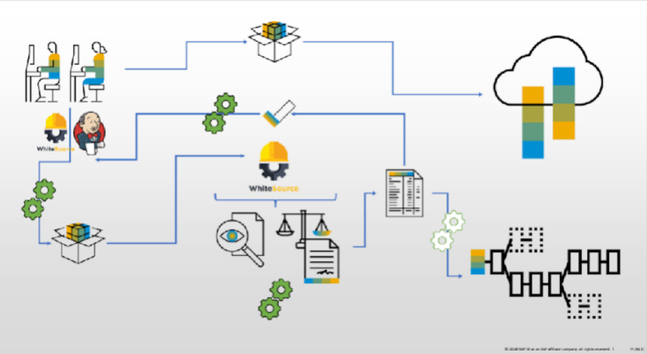
Reporter — HTML UI / Excel with findings

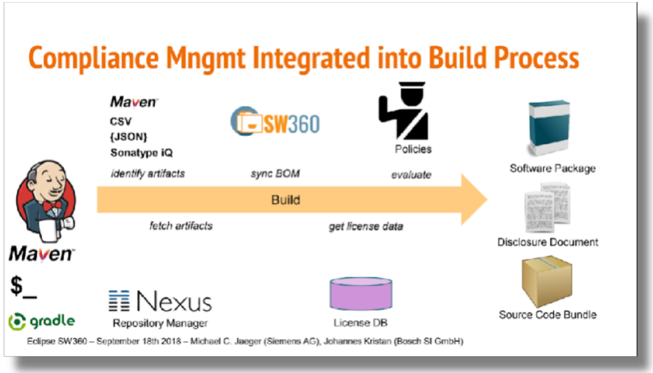
+ Open Source notices, Dependency graph, Review results as HTML/SPDX

Open-sourced & released at github.com/heremaps/oss-review-toolkit
Written in Kotlin + React, Apache-2.0 licensed.

© 2018 HERE

here





Compliance Mngmt Integrated into Build Process

Maven
CSV
{JSON}
Sonatype iQ
identify artifacts

SW360
sync BOM

Policies
evaluate

Build

fetch artifacts

get license data

Maven
$_
gradle

Nexus Repository Manager

License DB

Software Package

Disclosure Document

Source Code Bundle

Eclipse SW360 – September 18th 2018 – Michael C. Jaeger (Siemens AG), Johannes Kristan (Bosch SI GmbH)

All slides taken from the material of the 2018 BITKOM OpenSource conference, © with their respective owners

Big spending, little re-use

Everyone we interviewed in last 9-12 months said....

- We use (often 2+) commercial SCA tools. “None fits all”
- Spend on **custom development** what we spend for tool license fees (or more)
- Have scanned available Open Source tools, and found good islands of fuctionality

Duplicated (or more) spend for commercial SCA tools and DIY.

What else did we hear ?

- “Tool vendors Consolidation comes with risk”
- “Data needs to be open and bi-directional”
- “SCA must exit the Ivory Tower”
- “OSS Management is more than license scan”
- “Existing OSS offers promising but small”
- “Tired of big $$/y invoices - feel like hostages”

Re-Thinking necessary...

OSCAR stands for Open SCA

- Re-Loaded
- Re-Invented
- Re-Thought

What is OSCAR today?

oscar
eclipse.org

Well, actually a bit more...

Capabilities heard from supporters

Container analysis (hierarchical BOM)

ID mapping (mapping results of various SCA tools)

Source access

Metadata interface

Messaging Plugins

Scan data interface

QA on compliance artifacts

Accuracy of scan returns

QA of supplementing docs

IDE integration

Analytics interface

CI integration

OSS Obligations

Curations

CLI Tools

Snippet scanner & data

Component vulnerability data

License risk policy

10 min for responses

Remediation automation

Public data service at scale

Binary identification

Repo accessibility

Policy driven automation

Continuous inbound to outbound review at scale

Dependency detection support over technologies

Tool integration (CI, Central Hub, data sources…)

External pre-scan data

Top 1M components

oscar
eclipse.org

What will OSCAR be?

1. *Open Source solution* for large-scale **continuous** software composition analysis starting with compliance and security
2. *An installable software **distribution***
   - For workstation, server or cloud
   - Assembled out of **existing and new** OSS building blocks
3. *An architecture* and application bus
   - Specification of interfaces between open source and vendor building blocks of SCA software
4. *An industry coordination forum* to define and drive the up-to-date SCA as open source
5. *A software production setup* organized as an open source project

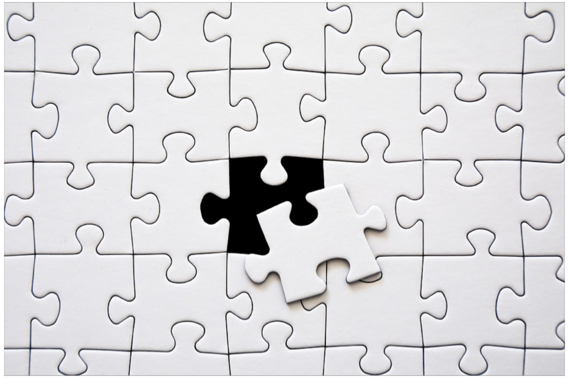
oscar
eclipse.org

OSCAR with existing OSS solutions

“Pieces of the puzzle” already supported partly by:

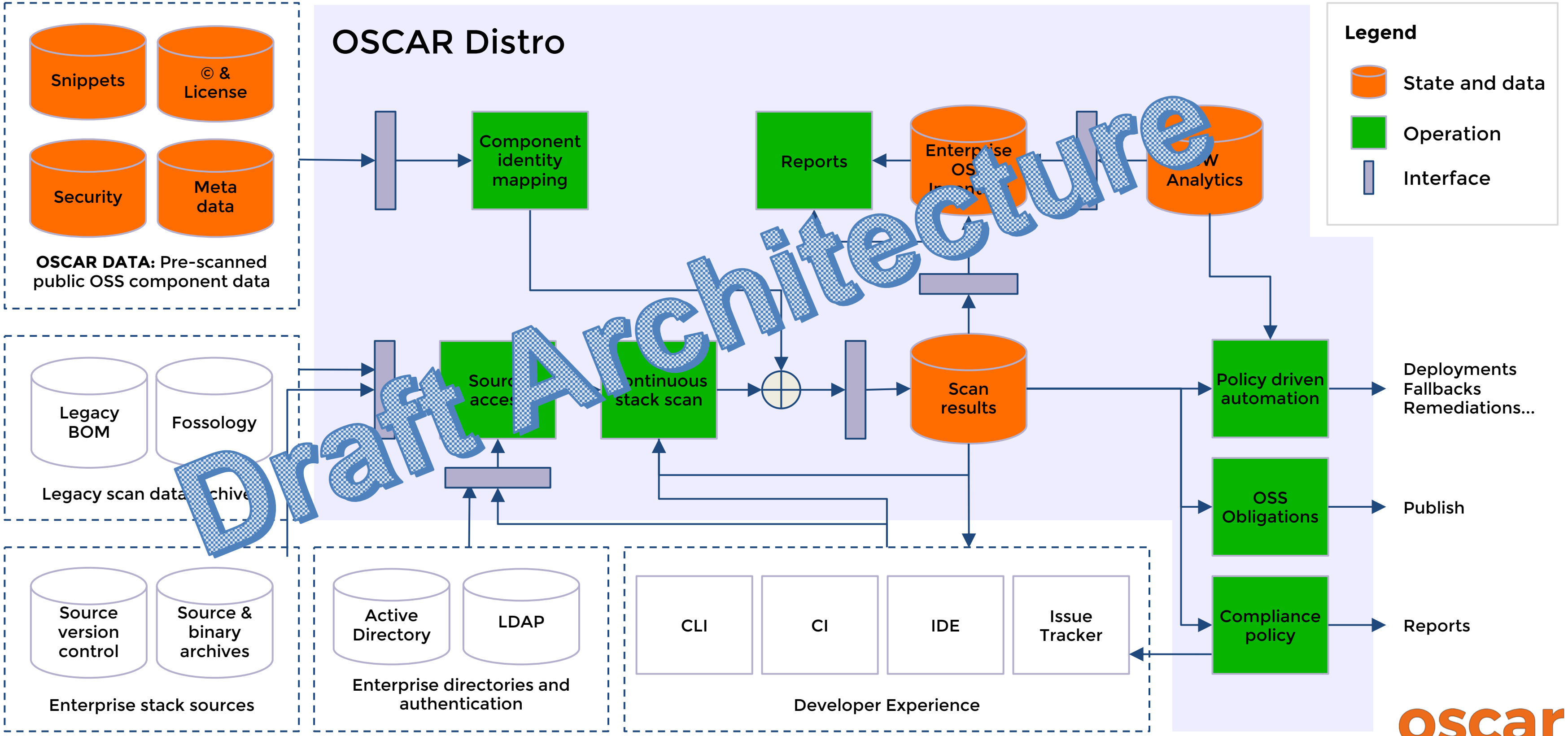
- Continuous scan engine
  - New 2017 ORT (**Here**)
  - New 2017 Grafeas (**Google**)
  - New 2018 Quartermaster (**Endocode**)
- Scanners
  - Fossology (**Siemens/HP**)
  - Scancode (**NexB**)
- Inventory: sw360 (**Siemens & Bosch**)
- Interfaces: SPDX (**Linux Foundation**)
- Data sources
  - New 2018 ClearlyDefined (**Microsoft, Qualcomm, Amazon**)
  - Coming 2018 ClearlySecured
  - Software Heritage
- New 2017 Analytics: CHAOSS (**Bitergia, Intel, RedHat**)

…. growing by the month



oscar
eclipse.org

Potential OSCAR Architecture



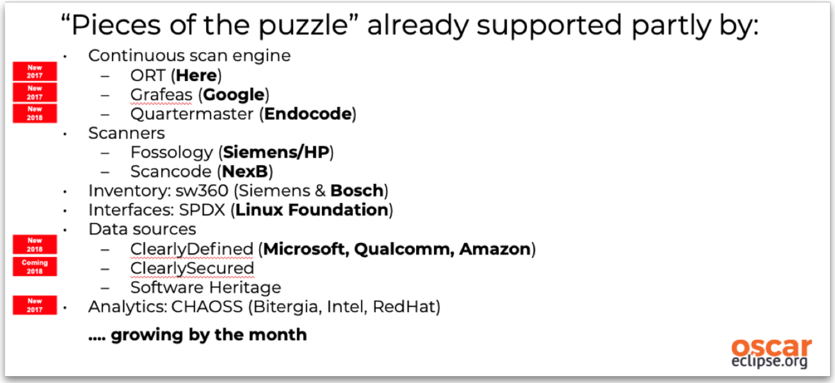
Draft Architecture

oscar
eclipse.org

Industry Backup & Support

- **Already existing** OSS Building Blocks supported by Here, HP, Siemens, Bosch, Google, Microsoft, Qualcomm, Amazon, Linux Foundation, ...
- **Industry Consortium** in the process of being built by SAP, Bosch, Siemens, Cisco, Here, Ericsson and Codescoop to fund and advance OSCAR
- Stakeholders will influence road map

No Green Field project

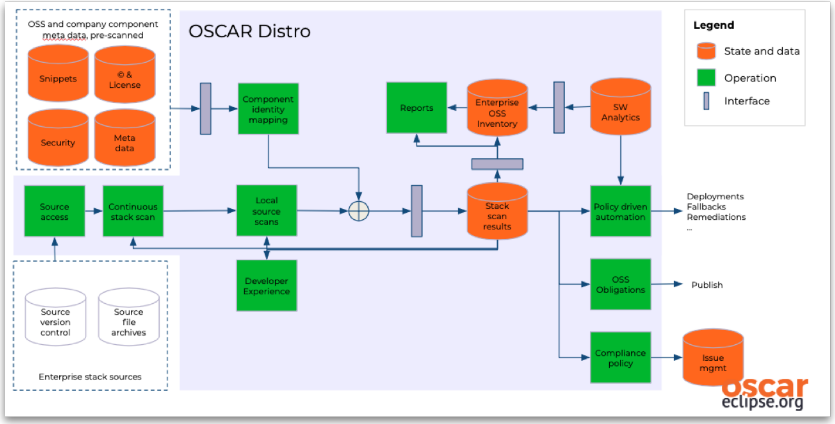


"Pieces of the puzzle" already supported partly by:

- Continuous scan engine
  - New 2017 – ORT (**Here**)
  - New 2017 – Grafeas (**Google**)
  - New 2018 – Quartermaster (**Endocode**)
- Scanners
  - Fossology (**Siemens/HP**)
  - Scancode (**NexB**)
- Inventory: sw360 (Siemens & **Bosch**)
- Interfaces: SPDX (**Linux Foundation**)
- Data sources
  - New 2018 – ClearlyDefined (**Microsoft, Qualcomm, Amazon**)
  - Coming 2018 – ClearlySecured
  - Software Heritage
- New 2017 – Analytics: CHAOSS (Bitergia, Intel, RedHat)

.... growing by the month

oscar eclipse.org



oscar eclipse.org

Eclipse OSCAR & OpenSCA

- OSCAR: **technical** project
  - Setup on Eclipse is complete
  - Anyone can contribute to OSCAR
  - Possibly embrace existing projects like ORT, sw360, …
- OpenSCA: Working Group to manage OSCAR
  - Finalizing of Charter in progress
  - Charter members vote functionality / priorities
  - Fees ensure tangible results / timelines

Where in the process is OSCAR

Think “Delivery Room”

- Announced OSCAR and OpenSCA @ EclipseCon in Oct.
- Initial industry consortium meeting end of Oct.
- Legal paperwork (and Charter) signed Nov. / Dec.
- Next: Kick Off meeting - 2H of January
  - List of work items/priorities
  - Chair & Committees set
  - Bi-weekly calls / slack / Google Docs / …
- Open for a few additional Companies - suggestions?

OSCAR release Map 0.1 ◆ 0.2 ◆ 1.0 ◆ 1.1 ◆ 1.2 ◆

Summary, why OSCAR

Answers to concerns and questions include

- Open SCA addresses vendor lock-in (and lagging behaviour)
- Open Source **and Data** creates transparency and “crowd QA”
- SCA starts where code is being produced - the developer
- Less need to build “custom patches” for dev shops
- Strengthen (small) SCA solutions within OSCAR context
  - more trust - because of larger supporter base
  - less risk - continuation within OSCAR “granted”
- Does not have to stop at compliance & security
- Free for consumers, alternative sourcing path for drivers

Join the Eclipse OSCAR project!

Help define the SCA technology you need & build the Organization that delivers

Thanks

oscar
eclipse.org