New approach to Software Composition Analysis

Stefan Just
Codescoop Oy
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
Holistic viewpoint

Environment
- Business Model
- Purpose
- Sourcing
- Governance
- Organization
- Process

Technology
- Functionality
- Architecture
- Features
This is what companies do to manage their OSS utilization.
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?
Well, actually a bit more...
Capabilities heard from supporters

- IDE integration
- Source access
- CLI Tools
- Messaging Plugins
- Component vulnerability data
- Scan data interface
- Analytics interface
- OSS Obligations
- Snippet scanner & data
- Metadata interface
- CI integration
- CI integration
- Component vulnerability data
- Messaging Plugins
- Accuracy of scan returns
- OSS Obligations
- Snippet scanner & data
- License risk policy
- 10 min for responses
- Remediation automation
- Public data service at scale
- QA on compliance artifacts
- QA of supplementing docs
- Curations
- CLI Tools
- Component vulnerability data
- Repo accessibility
- Policy driven automation
- Continuous inbound to outbound review at scale
- Binary identification
- External pre-scan data
- Top 1M components
- Dependency detection support over technologies
- Tool integration (CI, Central Hub, data sources...)
- Accuracy of scan returns
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 with existing OSS solutions

“Pieces of the puzzle” already supported partly by:

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

…. growing by the month
Potential OSCAR Architecture

OSCAR Distro

Legend
- State and data
- Operation
- Interface

OSCAR DATA: Pre-scanned public OSS component data

Snippets
© & License
Security
Metadata

Legacy BOM
Fossology
Legacy scan data archives

Source version control
Source & binary archives
Enterprise stack sources

Active Directory
LDAP
Enterprise directories and authentication

Component identity mapping

Scan results

Reports

Enterprise OSS Inventory

Potential OSCAR Architecture

Security
Continuous stack scan
Scan results

Enterprise directories and authentication

CLI
CI
IDE
Issue Tracker

Developer Experience

Policy driven automation
OSS Obligations

Compliance policy

Deployments Fallbacks Remediations...

Publish

Reports

Oscar eclipse.org

Draft Architecture
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 Codescoo 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
  - ORT (Here)
  - Grafeas (Google)
  - Quartermaster (Endocode)
- Scanners
  - Fossology (Siemens/HP)
  - Scancode (NexB)
  - Inventory: sw360 (Siemens & Bosch)
- Interfaces: SPDX (Linux Foundation)
- Data sources
  - ClearlyDefined (Microsoft, Qualcomm, Amazon)
  - ClearlySecured
  - Software Heritage
- Analytics: CHA OSS (Bitergia, Intel, RedHat)
  ... growing by the month
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 ◆

oscariclipse.org
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