

Open
Source
Solutions



EMPOWER
SMALL AND
MEDIUM
ENTERPRISES



Agenda

1. The OCCTET journey and goals
2. Open source tools for automated compliance and reporting
3. Self-assessing CRA compliance made simple
4. Standards in action
5. Q&A and Exchange



WHAT IS OCCTET?

**Open Source Compliance Comprehensive
tools and resources designed to simplify
and streamline the CRA compliance process
for SME, allowing them to tackle the
complexities of OSS compliance.**





FACTS SHEET

Project ID: 101190474

Funded by: ECCC

Call: DIGITAL-ECCC-2024-DEPLOY-CYBER-06

Duration: 24 months

Start date: November 2024

Total budget: 2,4M€

Partners: 7



**Co-funded by
the European Union**



Consortium Partners





Key Ambitions

- **Understanding the Cybersecurity Challenges Faced by SMEs**
 - High costs and limited resources
 - 61% struggle with cybersecurity due to insufficient skills and expertise
- **Empower SMEs**
 - Understand and apply effortless the CRA
 - Strengthening the cybersecurity posture
- **Automate Open Source Software Component handling**
 - Tooling / Global Embrace
- **Enhance Visibility and Impact**
 - Open Source tools for broad adoption
 - Federated Data Approach



Our Game Plan for Success

- Define and support compliance procedures
 - Helping SMEs understand and meet the requirements of the CRA.
 - Does this concern my product? What are my obligations? How do I meet them efficiently and reliably?



cra.occtet.eu - Self Assessment Web Application

- Automating Evaluation and Reporting with Open-Source Tools
 - Discovery: SBOM generation + Curation
 - Reference Data (FederateDB): Shared software metadata platform for packages
 - Triage, evaluation of security posture and remediation of vulnerabilities
 - Report: SBOM, VEX, Attestations

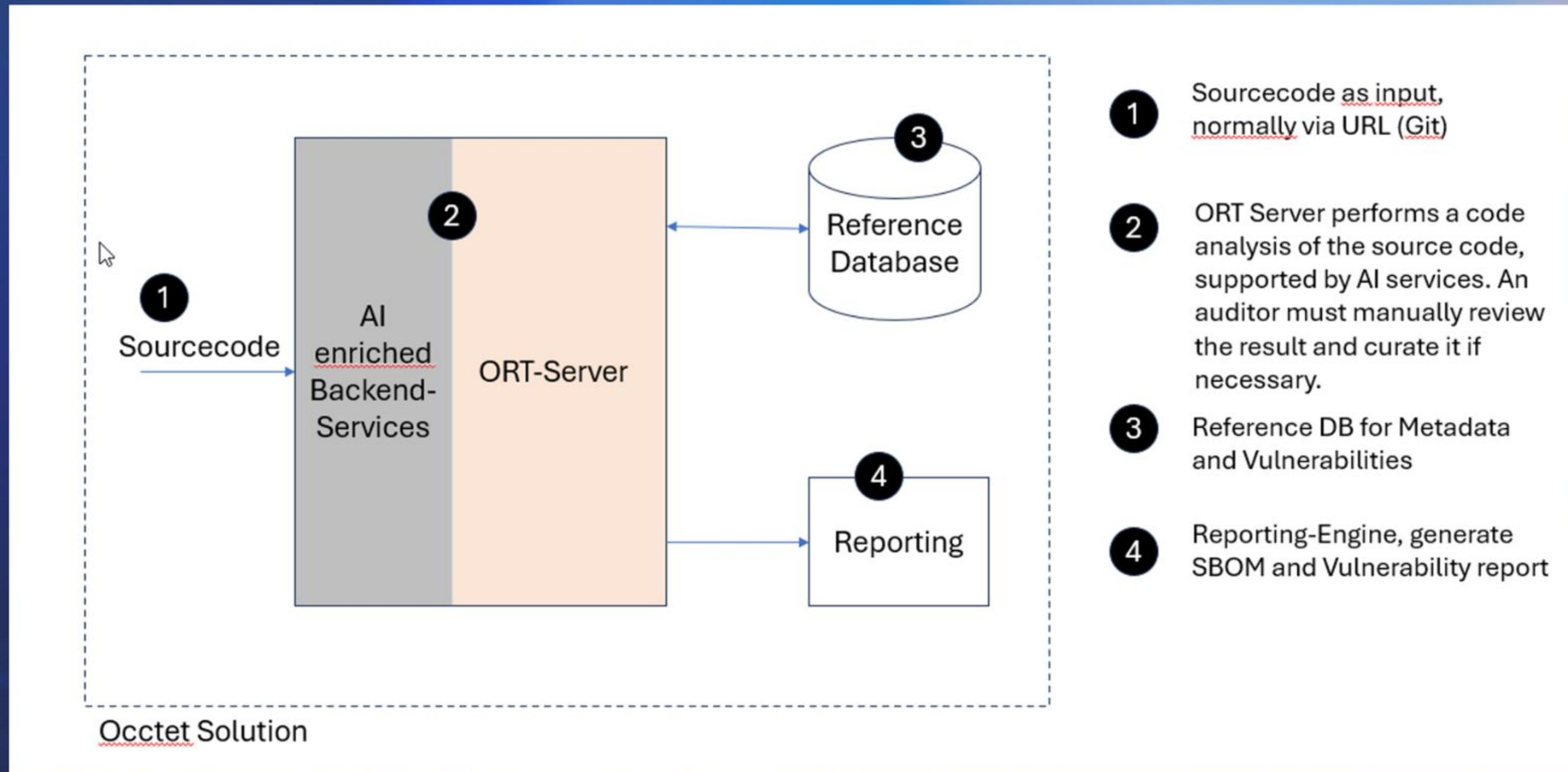


Agenda

- 1. The OCCTET journey and goals**
- 2. Open source tools for automated compliance and reporting**
- 3. Self-assessing CRA compliance made simple**
- 4. Standards in action**
- 5. Q&A and Exchange**



Toolchain



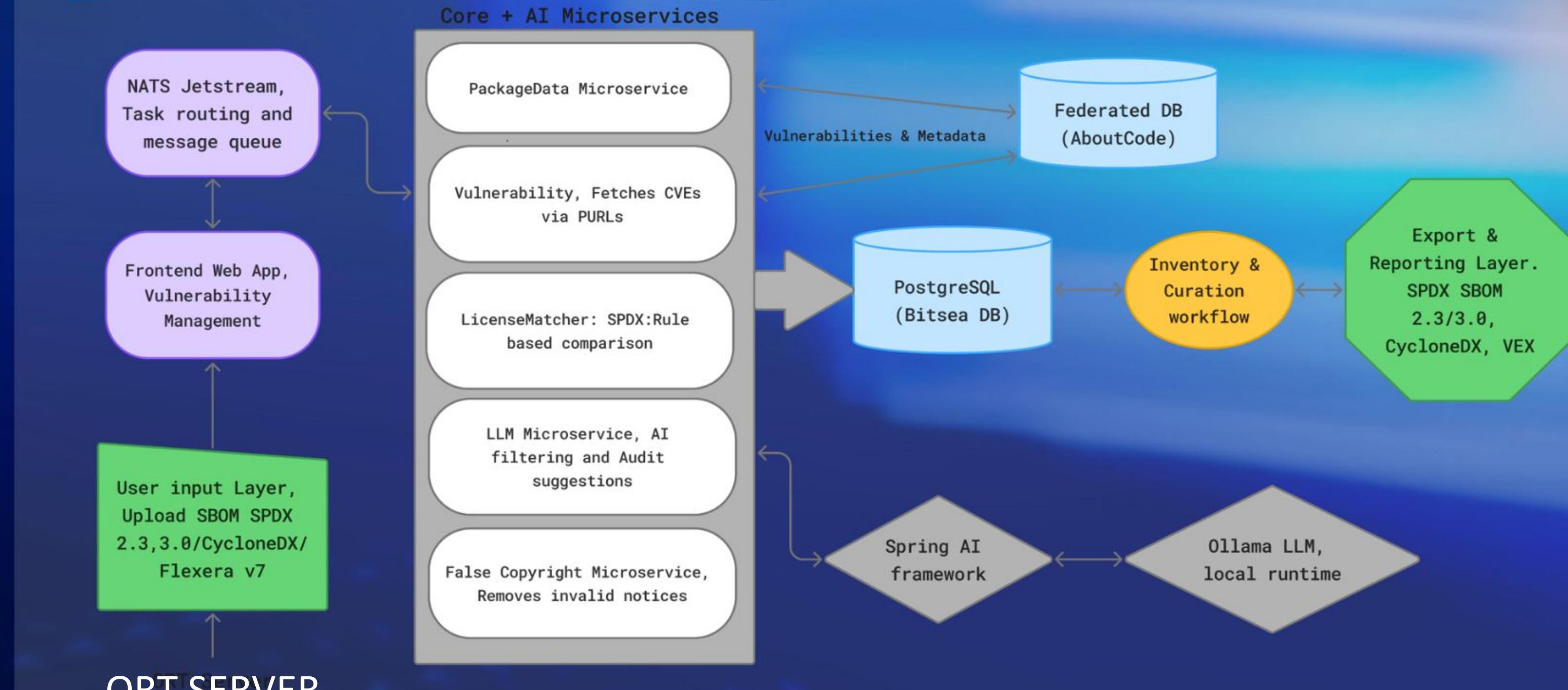


Occtet Curator

The Occtet-Curator is a web application with a messaging queue and integrated AI.

- Management of security vulnerabilities
- Generation of reports, SBOM and VEX
- Control of the SBOM through FOSS Management
- Support of the user through AI

Architecture Overview



Choose project

powsybl-core

[Expand all](#) [Collapse all](#)

File ▾

- > action-api
- > action-ial
- > ampl-converter
- > ampl-executor
- > cgmes
- > cim-anonymiser
- > commons
- > commons-test
- > computation
- > computation-local
- > computation-local-test
- > config-classic
- > config-test
- > contingency
- > distribution-core
- > docs
- > dsl
- > dynamic-security-ana...
- > dynamic-simulation
- > entsoe-util
- > ieee-cdf
- > iidm
- install.sh
- > itools-packager
- LICENSE.txt

Inventory Items Files

< cgmes-6.8.1 (MPL-2.0) ✕ com.powsybl-powsybl-core-6.8.1 ((MPL-2.0 AND CC-BY-4.0)) ✕ org.codehaus.plexus-plexus-archiver-2.2-source-artifact >

Inventory item	Vulnerabilities	Files	Audit notes	History	save
VCID-xzba...	CVE-2023-37460, GHSA-wh3p-fphp-9h2m	8.8	0.5	4.4	http://pub... 10/16/202...
VCID-xzba...	CVE-2023-37460, GHSA-wh3p-fphp-9h2m	8.8	0.5	4.4	http://pub... 10/16/202...
VCID-xzba...	CVE-2023-37460, GHSA-wh3p-fphp-9h2m	8.8	0.5	4.4	http://pub... 10/16/202... ⓘ
VCID-z6w...	CVE-2018-1002200, GHSA-hcxq-x77q-3469	8	0.5	4	http://pub... 10/16/202...
VCID-z6w...	CVE-2018-1002200, GHSA-hcxq-x77q-3469	8	0.5	4	http://pub... 10/16/202...
VCID-z6w...	CVE-2018-1002200, GHSA-hcxq-x77q-3469	8	0.5	4	http://pub... 10/16/202... ⓘ

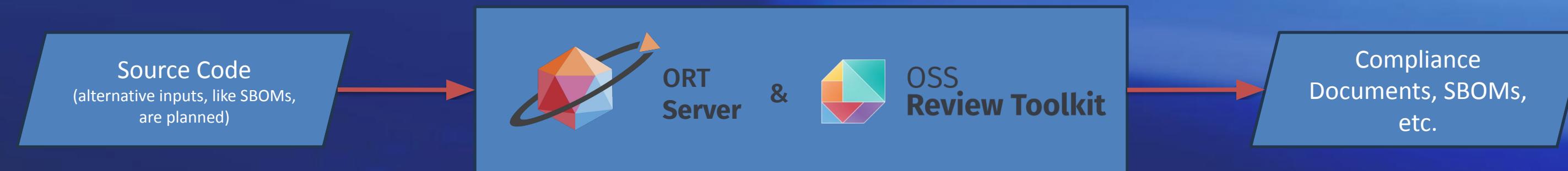
[⟳ Update data](#)

Item ▾	Files #
org.apache.maven.wago...	0
org.apache.maven.wago...	0
org.apache.poi-poi-5.4.1...	3
> org.apache.poi-poi-oox...	0
org.apache.poi-poi-oox...	18
org.apache.poi-poi-oox...	4
org.apache.servicemix.b...	0
org.apache.servicemix.b...	0
org.apache.xmlbeans-xm...	480
org.apache.xmlbeans-xm...	0
org.apfloat-apfloat-1.10....	208
org.apfloat-apfloat-1.10....	0
org.apiguardian-apiguar...	1
org.apiguardian-apiguar...	0
> org.assertj-assertj-core-3...	0
org.assertj-assertj-core-3...	0
org.assertj-assertj-core-3...	0
> org.awaitility-awaiterility-4....	0
org.awaitility-awaiterility-4....	52
org.awaitility-awaiterility-4....	0
org.codehaus.plexus-ple...	56
org.codehaus.plexus-ple...	0
org.codehaus.plexus-ple...	3
org.codehaus.plexus-ple...	0
org.codehaus.plexus-ple...	0
org.codehaus.plexus-ple...	36
org.codehaus.plexus-ple...	0
org.codehaus.plexus-ple...	3

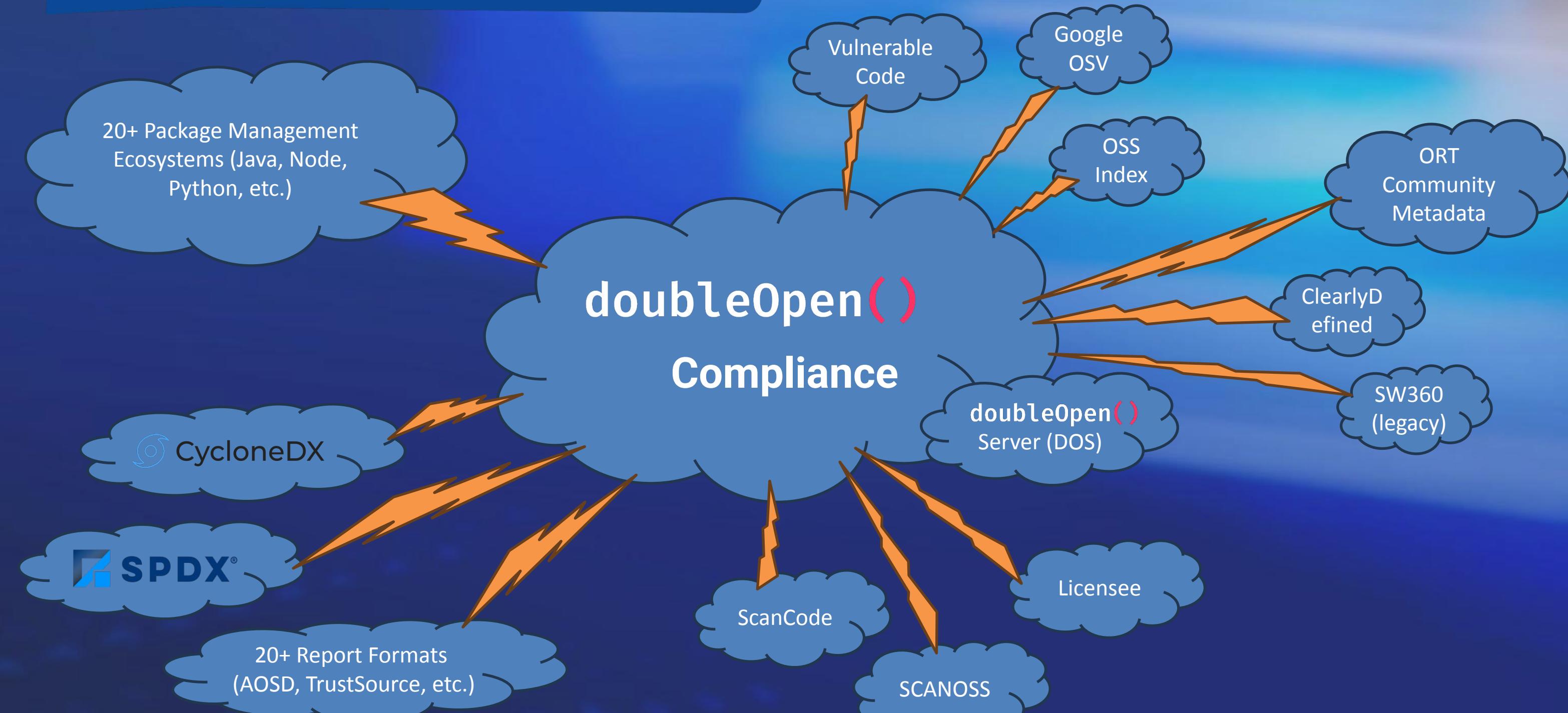


doubleOpen() Compliance

Double Open Compliance (DOC) is a SaaS-based solution to highly automate security and license compliance processes based on the [OSS Review Toolkit \(ORT\) ecosystem](#).



Tool Integrations





Vulnerability Management

The Double Open Compliance solution provides

- detailed vulnerability information for security experts,
- high-level risk view for product owners or managers,
- means to compare results from different vulnerability advisors.

This screenshot shows a dashboard for vulnerability management. On the left, a sidebar lists various categories: Overview, Compliance, Rule Violations, License Findings, Vulnerabilities (which is selected), Components, Projects, Packages, Reports, SBOMs, Other, Technical, Issues, Logs, and Configuration. The main area displays a table of vulnerabilities. The first three rows are shown, each with a package name, version, rating (HIGH), package ID, external ID, and summary. Below the table are two cards: 'CVSS 3.1 Severity Radar' and 'EPSS Score'.

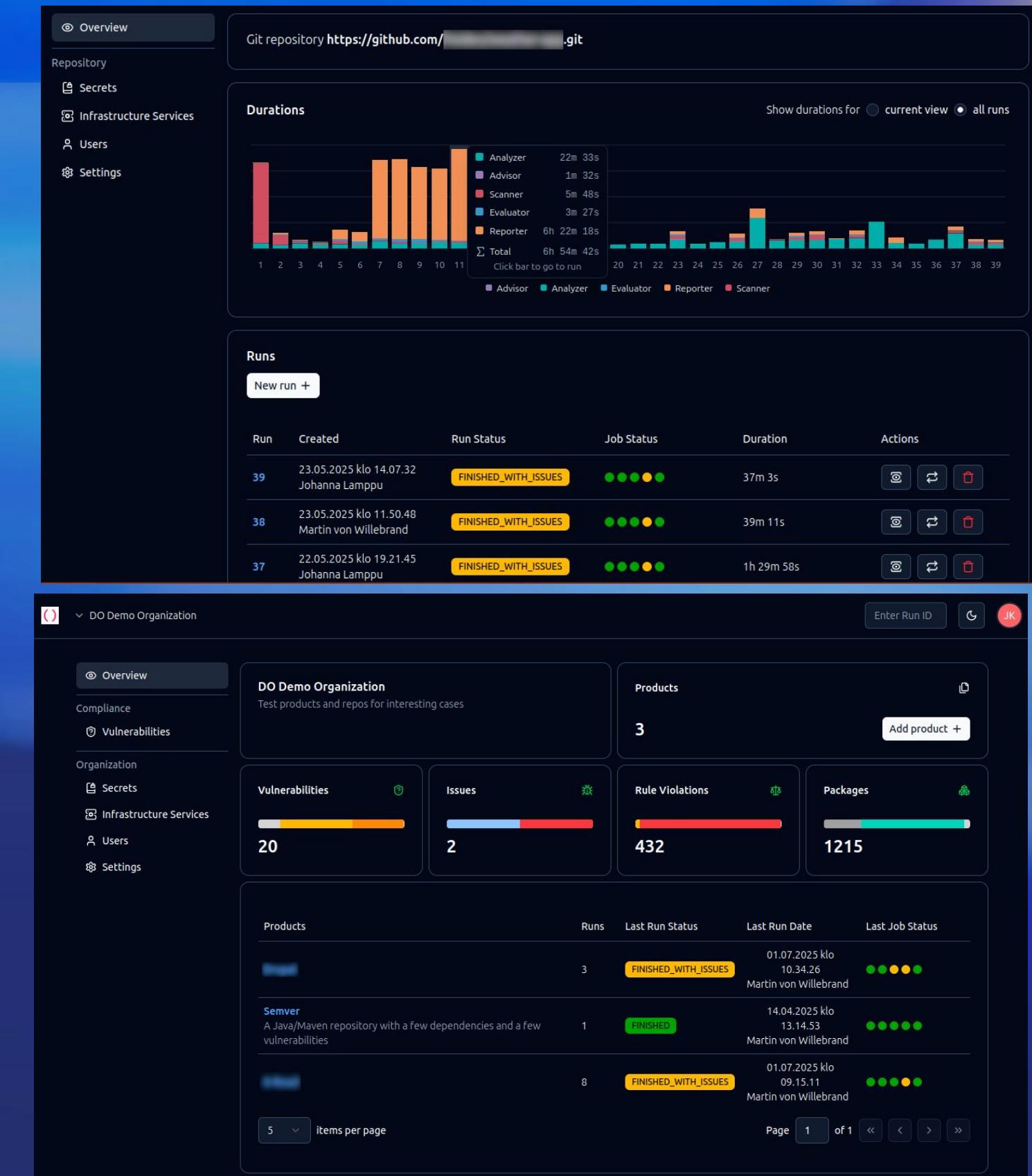
This screenshot shows a detailed view of a specific vulnerability. At the top, it shows the package name 'pkg:npm/cross-spawn@4.0.2' and its CVE ID 'CVE-2024-21538'. It includes tabs for 'Radar' (selected) and 'Macrovector'. The 'Radar' section shows a CVSS 4.0 Macro Vector with a score of 001210. The 'Macrovector' section lists exploitability, complexity, vulnerable system, subsequent system, exploitation, and security requirements, each with a color-coded rating (e.g., HIGH, MEDIUM). Below these are sections for 'Description' (No description) and 'Links to vulnerability references', which lists three entries with severity, scoring system, score, vector, and link.



Statistics Dashboards

The Double Open Compliance solution provides

- an overview of runtimes and performance metrics,
- general organization- and product-level dashboards.





Package Metadata

The Double Open Compliance solution provides

- deep insights into metadata of packages / software components,
- capabilities to inspect package source code for license findings.

The screenshot displays the doubleOpen application interface. At the top, a navigation bar includes 'doubleOpen()' and 'pkg:npm/react-native@0.77.1'. Below this, tabs for 'Inspect' (selected), 'Package Info', 'License Conclusions', and 'Bulk Conclusions' are visible. The main area shows a file tree under 'package' with 'src' expanded, containing 'private', 'webapis', 'dom', and 'geometry' subfolders. A file named 'DOMRect.js' is selected. To the right of the file tree is a large text area showing the source code of 'DOMRect.js'. The code includes JSDoc comments and imports from 'DOMRectReadOnly'. On the far right, a sidebar provides detailed information about the package:

- Package**: Declared license MIT
- File**: Detected license Scanner: scancode-toolkit@32.3.2 MIT AND (CC-BY-4.0 AND CC-BY-SA-2.5)
- Individual license matches**: 4: MIT, 14: CC-BY-4.0, 14: CC-BY-SA-2.5
- Concluded license**: No license conclusions
- Create a license conclusion**: Fields for Select license..., Write your SPDX expression, and Comment on your license conclusion... (with a Local checkbox and Submit button).



Reference Data for code origin, dependencies and vulnerabilities

*Good processes, and good tools
are harmless without good data!*

- Code origin, license and dependencies
- Known vulnerabilities, with actionable reachability
 - and remediations, fix commits, patches, upgrades
- Project health



1 MIT License

2

3 Copyright (c) 2022 Syphtnx0

4

5 Permission is hereby granted, free of charge, to any person obtaining
6 a copy of this software and associated documentation files (the "Software")
7 in the Software without restriction, including without limitation
8 to use, copy, modify, merge, publish, distribute, sublicense, and/or
9 sell copies of the Software, and to permit persons to whom the Software
10 furnished to do so, subject to the following conditions:

11

12 The above copyright notice and this permission notice shall be included in



Share all the scans 🎁

We SHOULD NOT redo the work

- We are all rescanning the same open source packages
- This is wasteful and ruining the planet
- Instead: **scan once, and only once**, in the open, and share freely all the scans
- Work together to refine, review and curate these only once
- Federated, decentralized Data



main ▾

vulnerablecode-data / aboutcode-packages-maven-3e / maven
/ purls.yml



keshav-space

Add maven package vulnerabilities from VulnerableCode



Code

Blame

- 1 - pkg:maven/org.apache.logging.log4j/log4j-core@1.0.4
- 2 - pkg:maven/org.apache.logging.log4j/log4j-core@1.2
- 3 - pkg:maven/org.apache.logging.log4j/log4j-core@2.0
- 4 - pkg:maven/org.apache.logging.log4j/log4j-core@2.0.0
- 5 - pkg:maven/org.apache.logging.log4j/log4j-core@2.0.1
- 6 - pkg:maven/org.apache.logging.log4j/log4j-core@2.0.2
- 7 - pkg:maven/org.apache.logging.log4j/log4j-core@2.0-alpha1
- 8 - pkg:maven/org.apache.logging.log4j/log4j-core@2.0-alpha2
- 9 - pkg:maven/org.apache.logging.log4j/log4j-core@2.0-beta1
- 10 - pkg:maven/org.apache.logging.log4j/log4j-core@2.0-beta2
- 11 - pkg:maven/org.apache.logging.log4j/log4j-core@2.0-beta3



main ▾

vulnerablecode-data / aboutcode-packages-maven-3e / maven
/ **vulnerabilities.yml**



keshav-space Add maven package vulnerabilities from VulnerableCode

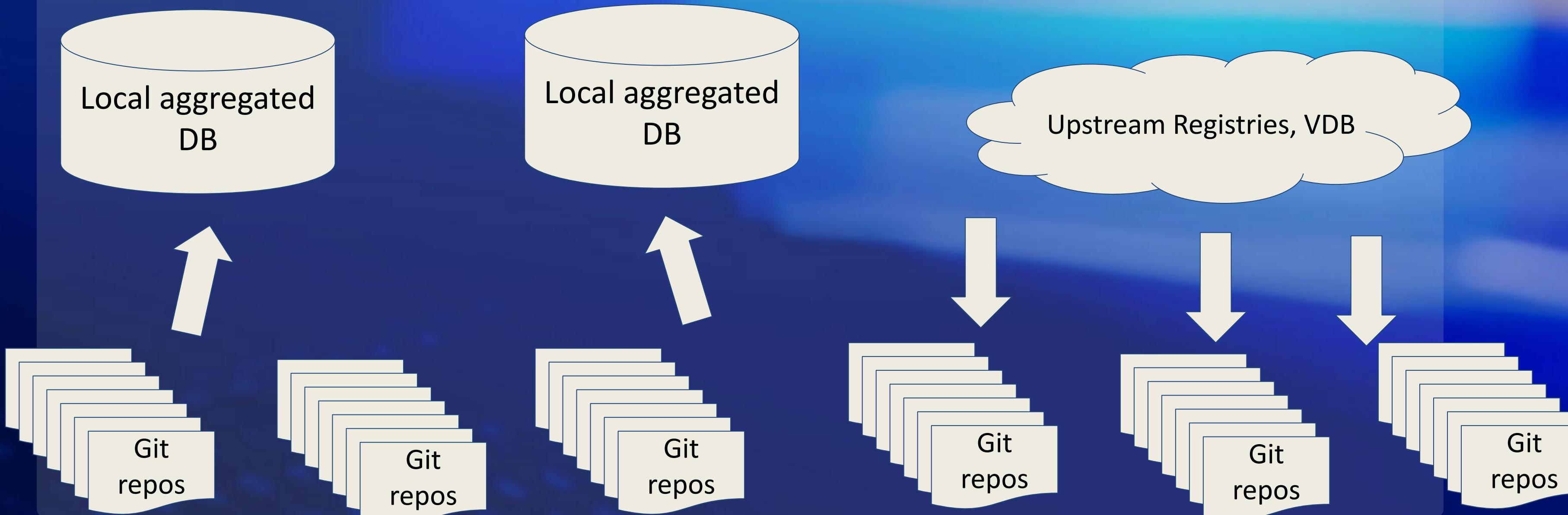
Code Blame

```
1      - purl: pkg:maven/org.apache.logging.log4j/log4j-core@1.0.4
2        affected_by_vulnerabilities:
3          - VCID-qzs5-6t9p-aaac
4        fixing_vulnerabilities: []
5      - purl: pkg:maven/org.apache.logging.log4j/log4j-core@1.2
6        affected_by_vulnerabilities:
7          - VCID-mmty-783v-aaaf
8        fixing_vulnerabilities: []
9      - purl: pkg:maven/org.apache.logging.log4j/log4j-core@2.0
10        affected_by_vulnerabilities:
11          - VCID-3ra8-evd3-aaaa
```



Share and curate all the SBOMs,
all the Scans, all the advisories

OCCTET, and your apps and systems





What's in YOUR SBOM???????????

And SBOM clarity is ... WIP

2024 SCA for Containers Report:

- Compared SCA tools for container scanning using SBOM accuracy as proxy
- The results were not great...
- Some invented Package IDs and invalid PURLs, lots of "creativity"
- Download report:
<https://nexb.com/sca-containers>
- Watch talk from OSS Summit EU 2024:
<https://sched.co/1ej58>

2025 CMU SEI's SBOM Plugfest Report:

- Compared SCA tools using SBOM accuracy as a proxy
- The results were not great ... again.
- Inconsistencies on the format and content across many tools
- Download report:
<https://www.sei.cmu.edu/news/study-finds-key-causes-of-divergence-in-software-bills-of-materials/>



Curate all the data 🎁

Curate, together, upstream!!!

- ClearlyDefined, curate all the licenses
- Software Heritage and Code Commons: scan all the files
- T-Rust: Curate all the crates
- Nix Clarity: Curate all the nixpkgs
- Maven Heaven: at last, fix the lingering Log4shell, with Log4J MAINTAINERS



Agenda

1. The OCCTET journey and goals
2. Open source tools for automated compliance and reporting
3. Self-assessing CRA compliance made simple
4. Standards in action
5. Q&A and Exchange



Building Secure by Design: The CRA Revolution

CRA is a cornerstone EU regulation to make all digital products secure by design and by default.

Every unpatched product, every weak update process – from now on, those aren't just cybersecurity issues; they're compliance violations.



The goal:
protect consumers,
improve resilience,
and create a
consistent security
baseline across
Europe.

It strengthens trust in the digital single market by ensuring manufacturers and developers address cybersecurity risks from the start.

CRA establishes clear responsibilities for product security throughout the lifecycle.



CRA at a Glance



CRA

- Cyber Resilience Act (CRA) is a regulation introduced by the European Union that aims to strengthen cybersecurity for products with digital elements across the EU.



CRA applies to:

- Manufacturers, importers, distributors of digital products.
- Software developers and integrators, including open-source components.



CRA Scope Exemptions

- Medical devices (EU 2017/745, 2017/746)
- Motor vehicles (EU 2019/2144)
- Civil aviation (EU 2018/1139)
- Marine equipment (EU 2014/90)



CRA Timeline

The dates are fixed in the regulation text itself (Art. 71 and related provisions).

10 October 2024
Adopted by Council



20 November 2024
Publication in Official
Journal of the EU



10 December 2024
CRA enters into force
(becomes law)



11 June 2026
Notification of
Conformity Assessment
Bodies



11 September 2026
Reporting obligations start
(vulnerabilities & incidents)



11 December 2027
Full application / most
obligations apply





CRA Business Implications

Financial Impact



Substantial Fines

Non-compliance can result in fines up to **15 million EUR or 2.5% of global turnover**, whichever is higher.



Product Recall Risk

Authorities can order withdrawal or recall of non-compliant products, leading to significant financial losses and operational disruptions.



Operational Requirements



Implement Continuous Monitoring

Establish systems to monitor products for security issues and threats throughout their lifecycle.



Vulnerability Management Process

Create clear channels for receiving vulnerability reports and establish protocols for addressing them.



Timely Reporting

Report actively exploited vulnerabilities within 24 hours to relevant authorities and users.



Proactive Security Updates

Develop processes to deliver timely security updates and patches to mitigate risks.



The OCCTET CRA Self-Assessment Platform

Your gateway to OCCTET's resources and compliance solutions



- A free and intuitive web tool to help organizations understand, assess, and improve their CRA readiness



- Designed to guide users' step by step through the CRA compliance journey.



- Includes built-in explanations, examples, and recommendations.



Why We Built It – How It Helps

CRA is complex – SMEs need clarity, not legal text

Obtain a readiness checklist showing what to improve to meet CRA's essential requirements

Classify products – whether they are “default”, “important”, or “critical”, and identify what kind of conformity assessment is required – self-assessment or third-party;

Guides users to understand their role, product class, and required actions

shield icon lock icon cra.occtet.eu



The Three Questionnaires

1

Applicability & Role *"Does CRA apply to me?"*

- Identify company role: manufacturer / importer / distributor
- Check product type and market presence
- Exclude products already covered by sectoral legislation (medical, automotive, etc.)
- Clarify if open-source or non-commercial → out of CRA scope

2

Classification & Conformity Route *"What level of assurance do I need?"*

- Apply CRA classification logic: Default / Important I / Important II / Critical
- Determine corresponding conformity assessment procedure
→ Self-assessment, third-party assessment, or certification

3

Readiness & Maturity Checklist *"How prepared am I?"*

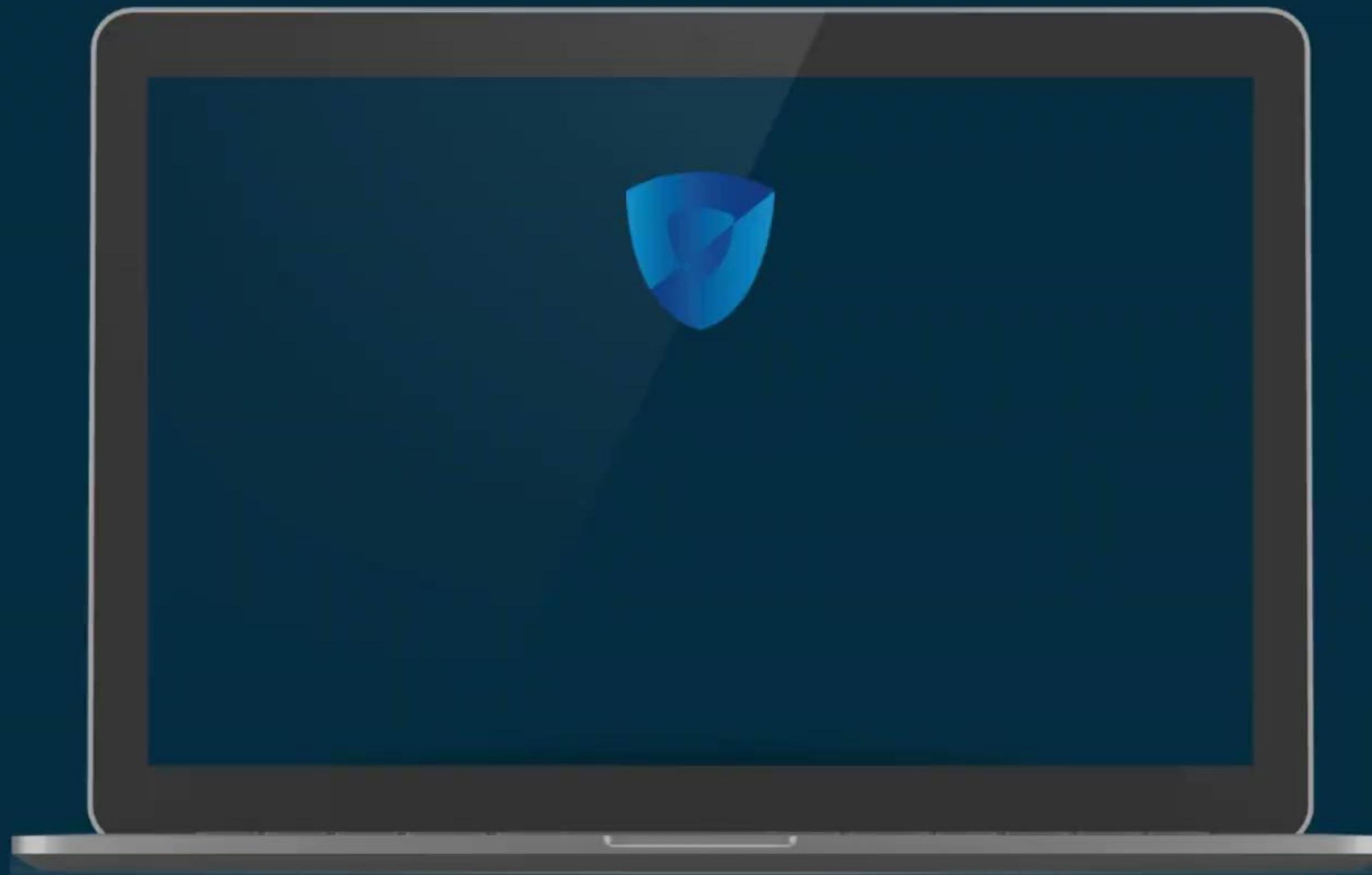
- Translate CRA Annex I security requirements into actionable controls
- Evaluate current practices: Basic / Intermediate / Advanced
- Generate tailored improvement recommendations



CRA Readiness Scoring – Turning Answers into Insight

- Each answer contributes to maturity (Basic / Intermediate / Advanced).
- Four areas: Secure Design, Vulnerability Handling, Updates, Transparency.
- Generates a visual readiness score highlighting improvement priorities.
- Directly linked to CRA Annex I requirements.







OCCTET

Home Register Surveys Why register FAQ Contact

OCCTET - SELF ASSESSMENT PORTAL

Evaluate your Business Cyber Resilience Readiness. Free, instant, and aligned with the EU Cyber Resilience Act.

RjCnChLB-oB0J-AARS-xhE6-V4MLiaNISS9u| →

OR

Register



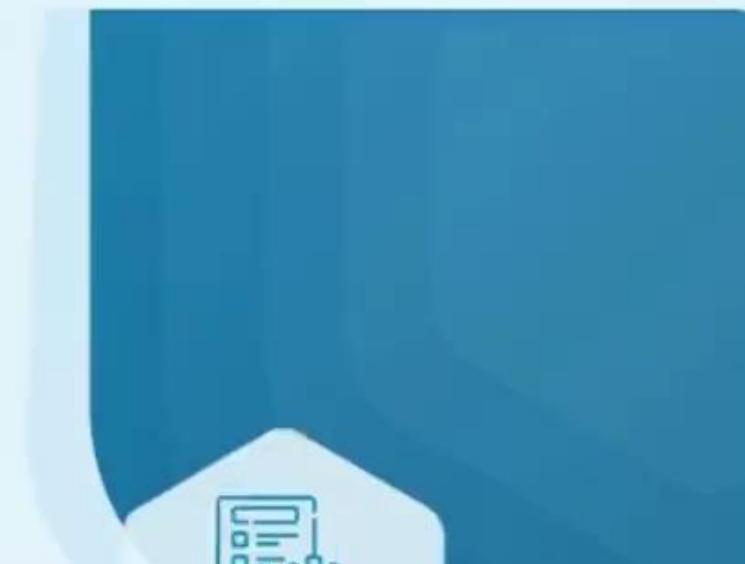
Co-funded by
the European Union



Welcome to the OCCTET Self-Assessment

The Open CyberSecurity Compliance Toolkit (OCCTET) is designed to help Small and Medium Enterprises (SMEs) evaluate their readiness for the EU Cyber Resilience Act (CRA) – especially when using Free and Open Source Software (FOSS) in digital products.

Funded by the EU Digital Europe Programme, OCCTET offers practical, open-source tools that guide you through every step of compliance – from identifying OSS components to producing clear, actionable reports.



{code & compliance} |

22-23 October

2025

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Co-funded by
the European Union



OCCTET

Company details

Co-funded by
the European Union

STEP 1 STEP 2 STEP 3

Survey for SMEs on CRA Compliance

This survey is intended for SMEs and FOSS contributors to help determine whether their products or activities fall within the scope of the EU Cyber Resilience Act (CRA). By completing it, you'll gain insight into your responsibilities and contribute to identifying areas where further guidance or tools are needed.

Q1: In which activity sector is your company operating?

Why it matters: Some sectors already have specific cybersecurity regulations (e.g., medical devices, automotive, aviation, marine equipment, radio equipment). If you fall under a more specific regulatory regime, you might be excluded from the CRA or have overlapping requirements.

Examples: Owner, Compliance Manager, Developer, Cybersecurity...

Q2: How many employees does your company/organization have?

Start new survey

Start

1. What is your role in the organization?

Examples: Owner, Compliance Manager, Developer, Cybersecurity...

2. How many employees does your organization have?

Micro (1-9)

Small (10-49)

3. Do you develop or sell products with digital elements
on the market?

Start new survey

Start

STEP 1 STEP 2 STEP 3

Self-Qualification Questionnaire

The purpose of this questionnaire is to assist SMEs in establishing the applicability of the CRA, assessing the criticality of their products or services, and accessing structured guidance on compliance and maturity assessment processes.



OCCTET

Company details



STEP 1 STEP 2 STEP 3

Survey for SMEs on CRA Compliance

This survey is intended for SMEs and FOSS contributors to help determine whether their products or activities fall within the scope of the EU Cyber Resilience Act (CRA). By completing it, you'll gain insight into your responsibilities and contribute to identifying areas where further guidance or tools are needed.

Q1: In which activity sector is your company operating?

Why it matters: Some sectors already have specific cybersecurity regulations (e.g., medical devices, automotive, aviation, marine equipment, radio equipment). If you fall under a more specific regulatory regime, you might be excluded from the CRA or have overlapping requirements.

Examples: Owner, Compliance Manager, Developer, Cybersecurity...

Q2: How many employees does your company/organization have?

Start new survey

Start

1. What is your role in the organization?

Examples: Owner, Compliance Manager, Developer, Cybersecurity...

2. How many employees does your organization have?

Micro (1–9)

Small (10–49)

3. Do you develop or sell products with digital elements
within your organization?

1 completed

Start new survey

See history

Start

STEP 1 STEP 2 STEP 3

Self-Qualification Questionnaire

The purpose of this questionnaire is to assist SMEs in establishing the applicability of the CRA, assessing the criticality of their products or services, and accessing structured guidance on compliance and maturity assessment processes.

Q1: In which activity sector is your company operating?

Why it matters: Some sectors already have specific cybersecurity regulations (e.g., medical devices, automotive, aviation, marine equipment, radio equipment). If you fall under a more specific regulatory regime, you might be excluded from the CRA or have overlapping requirements.

Examples: *Digital Communications Manager, Datacenter Administrator*

Q2: How many employees does your company/
organization have?

1 completed

Start new survey

See history

Start

STEP 1

STEP 2

STEP 3

Self-Qualification Questionnaire

The purpose of this questionnaire is to assist SMEs in establishing the applicability of the CRA, assessing the criticality of their products or services, and accessing structured guidance on compliance and maturity assessment processes.

STEP 1 STEP 2 **STEP 3**

SMEs CRA Maturity Assessment

This maturity assessment helps SMEs evaluate their technical readiness in relation to the Cyber Resilience Act (CRA). It identifies strengths and weaknesses in current practices, highlights areas that require improvement, and provides tailored guidance to support continuous development toward compliance.

1. Threat Modeling and Risk Assessment

0 - no formal process

1 - existing process,
coverage <25%

2 - e
COVE

4 - e

1. Secure Software Development Lifecycle

2/4

2. Protection from unauthorized access

3/4

3. Confidentiality

4/4

4. Vulnerability Management and Disclosure

2/4

5. Risk Management and Governance

2/4

6. Incident Response

2/4

7. Business Continuity

2/4

8. Stakeholder Engagement

2/4

9. Legal and Regulatory Compliance

2/4

10. Risk Management and Governance

2/4

11. Business Continuity

2/4

12. Stakeholder Engagement

2/4

13. Legal and Regulatory Compliance

2/4

14. Risk Management and Governance

2/4

15. Business Continuity

2/4

16. Stakeholder Engagement

2/4

17. Legal and Regulatory Compliance

2/4

18. Risk Management and Governance

2/4

19. Business Continuity

2/4

20. Stakeholder Engagement

2/4

21. Legal and Regulatory Compliance

2/4

22. Risk Management and Governance

2/4

23. Business Continuity

2/4

24. Stakeholder Engagement

2/4

25. Legal and Regulatory Compliance

2/4

26. Risk Management and Governance

2/4

27. Business Continuity

2/4

28. Stakeholder Engagement

2/4

29. Legal and Regulatory Compliance

2/4

30. Risk Management and Governance

2/4

31. Business Continuity

2/4

32. Stakeholder Engagement

2/4

33. Legal and Regulatory Compliance

2/4

34. Risk Management and Governance

2/4

35. Business Continuity

2/4

36. Stakeholder Engagement

2/4

37. Legal and Regulatory Compliance

2/4

38. Risk Management and Governance

2/4

39. Business Continuity

2/4

40. Stakeholder Engagement

2/4

41. Legal and Regulatory Compliance

2/4

42. Risk Management and Governance

2/4

43. Business Continuity

2/4

44. Stakeholder Engagement

2/4

45. Legal and Regulatory Compliance

2/4

46. Risk Management and Governance

2/4

47. Business Continuity

2/4

48. Stakeholder Engagement

2/4

49. Legal and Regulatory Compliance

2/4

50. Risk Management and Governance

2/4

51. Business Continuity

2/4

52. Stakeholder Engagement

2/4

53. Legal and Regulatory Compliance

2/4

54. Risk Management and Governance

2/4

55. Business Continuity

2/4

56. Stakeholder Engagement

2/4

57. Legal and Regulatory Compliance

2/4

58. Risk Management and Governance

2/4

59. Business Continuity

2/4

60. Stakeholder Engagement

2/4

61. Legal and Regulatory Compliance

2/4

62. Risk Management and Governance

2/4

63. Business Continuity

2/4

64. Stakeholder Engagement

2/4

65. Legal and Regulatory Compliance

2/4

66. Risk Management and Governance

2/4

67. Business Continuity

2/4

68. Stakeholder Engagement

2/4

69. Legal and Regulatory Compliance

2/4

70. Risk Management and Governance

2/4

71. Business Continuity

2/4

72. Stakeholder Engagement

2/4

73. Legal and Regulatory Compliance

2/4

74. Risk Management and Governance

2/4

75. Business Continuity

2/4

76. Stakeholder Engagement

2/4

77. Legal and Regulatory Compliance

2/4

78. Risk Management and Governance

2/4

79. Business Continuity

2/4

80. Stakeholder Engagement

2/4

81. Legal and Regulatory Compliance

2/4

82. Risk Management and Governance

2/4

83. Business Continuity

2/4

84. Stakeholder Engagement

2/4



OCCTET

Company details

Home / Surveys / CRA maturity assessment Surveys

Start

Started date	Updated date	Status	Result



OCCTET - SELF ASSESSMENT PORTAL

Evaluate your Business Cyber Resilience Readiness. Free, instant, and aligned with the EU Cyber Resilience Act.



OR

[Register](#)

Welcome to the OCCTET Self-Assessment

The Open CyberSecurity Compliance Toolkit (OCCTET) is designed to help Small and Medium Enterprises (SMEs) evaluate their readiness for the EU Cyber Resilience Act (CRA) – especially when using Free and Open Source Software (FOSS) in digital products.



Co-funded by
the European Union



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Demo



OCCTET

Home

Register

Surveys

Why register

FAQ

Contact

Thank you!



**Scan to begin your
assessment**



Agenda

- 1. The OCCTET journey and goals**
- 2. Open source tools for automated compliance and reporting**
- 3. Self-assessing CRA compliance made simple**
- 4. Standards in action**
- 5. Q&A and Exchange**



Standards for Software Supply Chain(s)

Good data is unactionable without standards

- Identifiers
 - Package-URL (PURL) for packages
 - SPDX License expressions for licenses
- SBOMs and VEX
 - CycloneDX and SPDX for SBOMs
 - CSAF and CycloneDX for VEX/VDR



What is PURL?

PURL is the standard for package identification across ecosystems

- Package-URL (PURL) is the glue between all your software supply chain tools, data, and standards
 - Adopted in all SBOM and VEX specs
 - Most SCA tools
 - Many vulnerability databases
- Across Dev to Ops to Sec (to DevSecOps)
- Ecma standardization at TC54
- Simple, obvious, expressive syntax:
 - pkg:npm/file@1.9.1
 - pkg:deb/ubuntu/7zip@21.07+dfsg-4
 - pkg:pypi/django@1.11.1



Better PURLs enable standardized SBOM format interoperability

Share better inventories

- Consistent identification across formats
 - Reference the same package using identical PURL identifiers



[https://cyclonedx.org/docs/1.6/json/
#components_items_purl](https://cyclonedx.org/docs/1.6/json/#components_items_purl)



[https://spdx.github.io/spdx-spec/v3.0.1/mod
el/](https://spdx.github.io/spdx-spec/v3.0.1/model/)
[SoftwareProperties/packageUrl/](https://spdx.github.io/spdx-spec/v3.0.1/SoftwareProperties/packageUrl/)



Better PURLs enable standardized
VEX formats interoperability

Disclose better vulnerabilities

- Precise vulnerability to package matching with unambiguous package identification



<https://github.com/openvex/spec/blob/main/OPENVEX-SPEC.md?plain=1#L249>

{code & compliance}

22-23 October

2025



CycloneDX

[https://cyclonedx.org/docs/1.6/json/
#components_items_purl](https://cyclonedx.org/docs/1.6/json/#components_items_purl)



[https://docs.oasis-open.org/csaf/csaf/v2.0/os/
csaf-v2.0-os.html#31334-full-product-name-type
---product-identification-helper---purl](https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html#31334-full-product-name-type---product-identification-helper---purl)



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Co-funded by
the European Union

Better PURLs improve reference data quality

Accurate data, keyed by PURL

ClearlyDefined

ClearlyDefined supports converting PURLs to "Coordinates" format in its data model.

<https://docs.clearlydefined.io/docs/resources/coordinates#purl-type-mapping>

Sonatype OSS Index

OSS Index can consistently map components to their corresponding vulnerability data using PURL.

<https://ossindex.sonatype.org/doc/coordinates>

AboutCode PurIDB

Continuously updated reference data for open source packages' origin, information and licensing, utilizing PURL.

<https://github.com/aboutcode-org/purldb>

ecosyste.ms

Lookup information about a PURL in both text and JSON formats.

<https://github.com/andrew/purl>

deps.dev

PURLs serve as unique identifiers for allows for precise tracking and analysis of dependencies within the deps.dev system.

<https://docs.deps.dev/api/v3alpha/#purllookup>

OSV

OSV uses PURLs to identify packages within its database and API queries.

<https://ossf.github.io/osv-schema/#affectedpackage-field>



PURL adoption

PURL is adopted industry- and community-wide

**All open source SCA and SBOM tools
use PURL, including:**

- Linux Foundation's OSS Review Toolkit, and Fossology
- OpenSSF OSV and GUAC
- OWASP Dependency-Track, Dependency-Check, and cdxgen
- All OWASP CycloneDX libraries
- GitHub's Dependency Graph
- Microsoft's OSS Gadget, SBOM tool
- Anchore's Syft and Grype
- Aquasec's Trivy
- LG's FOSSLight
- SCANOSS
- Snyk's Parlay

**Most proprietary SCA, SBOM, and
code host tools use PURL, including:**

- GitHub
- GitLab
- Snyk
- Mend
- BlackDuck
- Sonatype

**Vulnerability databases use PURL,
including:**

- Google's OSV
- Sonatype's OSS Index
- CVE specification v5.1
- VulnerableCode

**PURL facilitates better compliance
processes for end users, including:**

- Most free and open source software foundations
- Five of the Big Tech companies, with three building their entire SCA compliance operations on PURL
- A leading database company
- A leading Linux company
- European and US government agencies
- All major European car manufacturers and most of their vendors
- Major US chip and microprocessor providers
- Four leading European industrial companies
- A leading European medical devices company



Standards for Software Supply Chain(s)

In OCCTET

- Tool-to-tool exchanges based on standard SBOMs and VEXs
- And all keyed by Package-URL (PURL)
- Data provisioned from FederatedCode



Agenda

1. The OCCTET journey and goals
2. Self-assessing CRA compliance made simple
3. Standards in action
4. Open source tools for automated compliance and reporting
5. Q&A and Exchange



Get in touch with us!



occtet.eu



www.occtet.eu

OUR SELF-ASSESSMENT PLATFORM IS AVAILABLE! NOW!

<https://cra.occtet.eu>



Scan the QR code for easy
access to our Survey and
Wishlist!