OCCTET.eu

Open Source Solutions

EMPOWER SMALL AND MEDIUM ENTERPRISES

{code & compliance}

22-23 October 2025

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union

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

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union

Consortium Partners

{code & compliance}

22-23 October 2025

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union

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

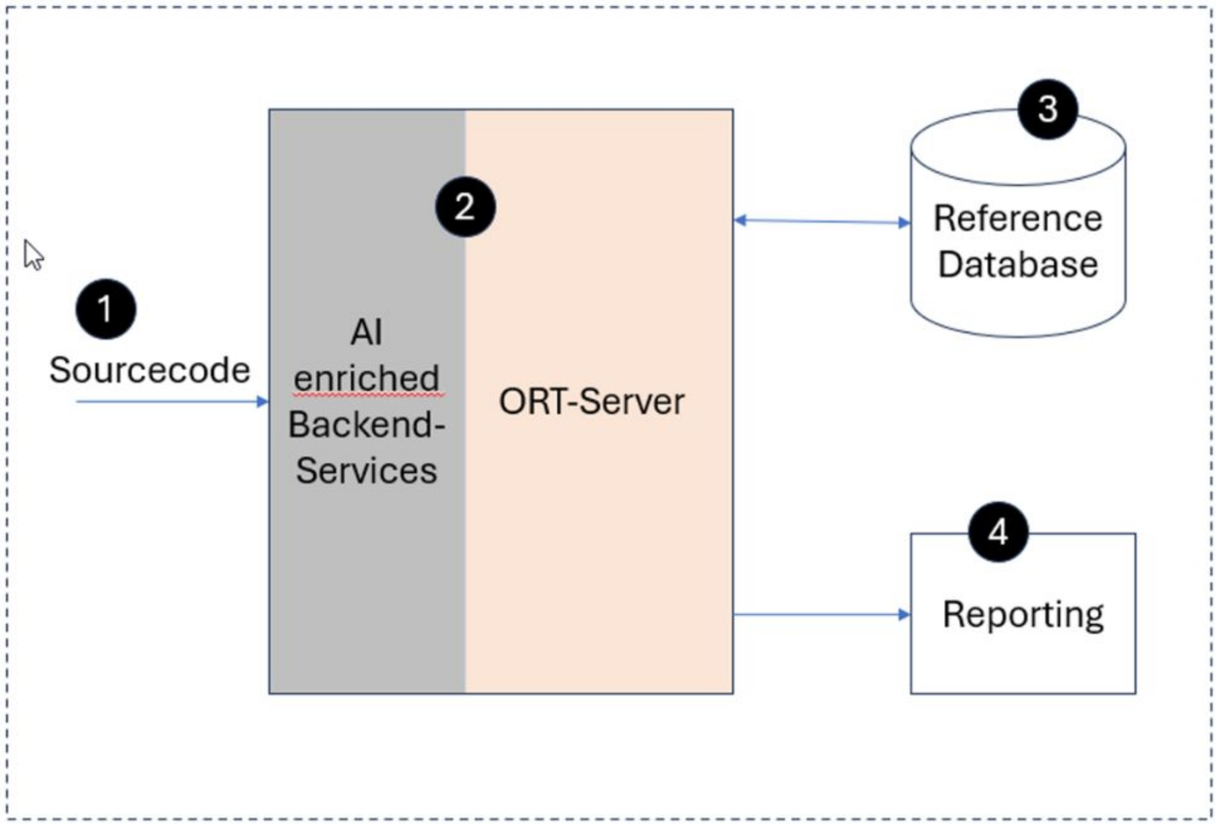
- Automating Evaluation and Reporting with Open-Source Tools
  - Discovery: SBOM generation + Curation
  - Reference Data (FederateDB): Shared software metadata platform for packages
  - Triage, evaluation of security posture and remediation of vulnerabilities
  - Report: SBOM, VEX, Attestations

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Co-funded by the European Union

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



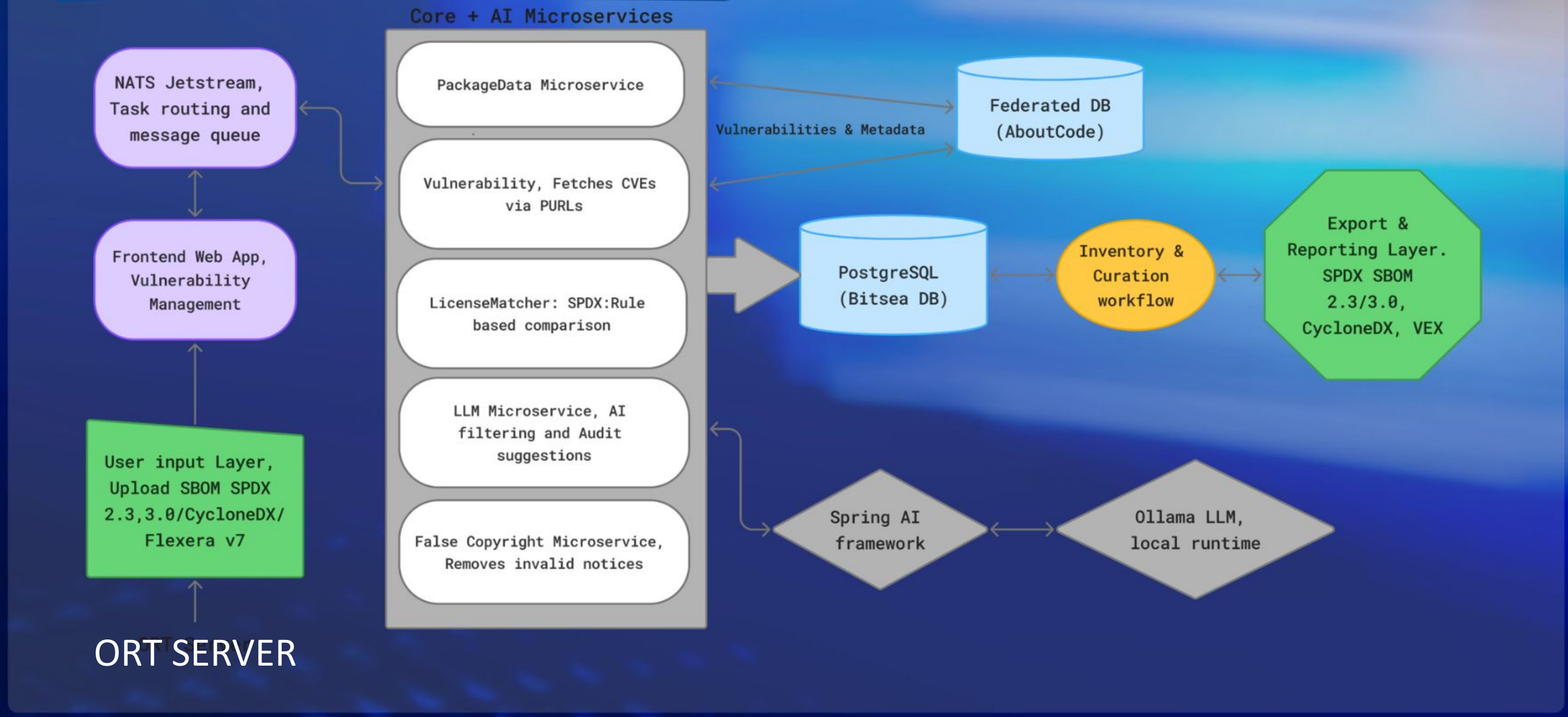
1. Sourcecode as input, normally via URL (Git)
2. ORT Server performs a code analysis of the source code, supported by AI services. An auditor must manually review the result and curate it if necessary.
3. Reference DB for Metadata and Vulnerabilities
4. Reporting-Engine, generate SBOM and Vulnerability report

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



SBOM Mgmt

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

id	aliases	weighte...	exploita...	risk score	sourceUrl	last upd...
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...

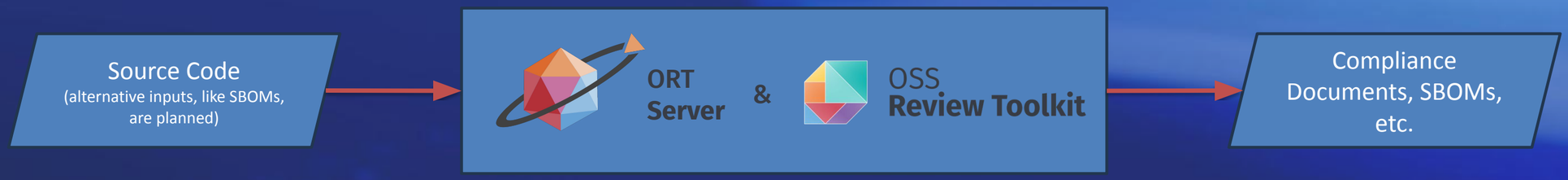
Update data

Expand all | Collapse all

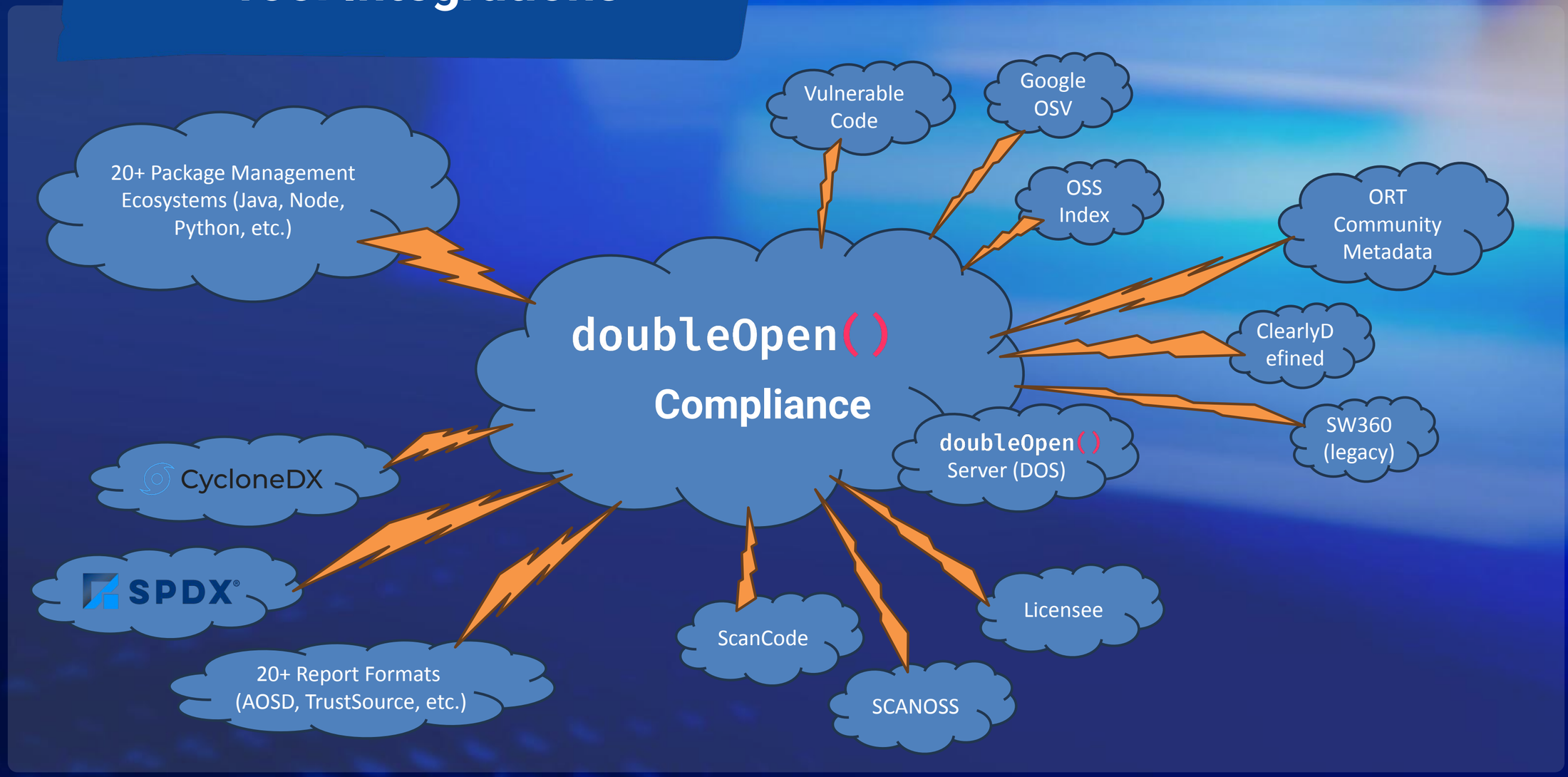
Item	Files #
org.apache.maven.wago...	0
org.apache.maven.wago...	0
org.apache.poi-poi-5.4.1...	3
org.apache.poi-poi-oox...	0
org.apache.poi-poi-oox...	18
org.apache.poi-poi-oox...	4
org.apache.servicemix.b...	0
org.apache.servicemix.b...	0
org.apache.servicemix.b...	0
org.apache.xmlbeans-xm...	480
org.apache.xmlbeans-xm...	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-awaitility-4....	0
org.awaitility-awaitility-4....	52
org.awaitility-awaitility-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...	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.



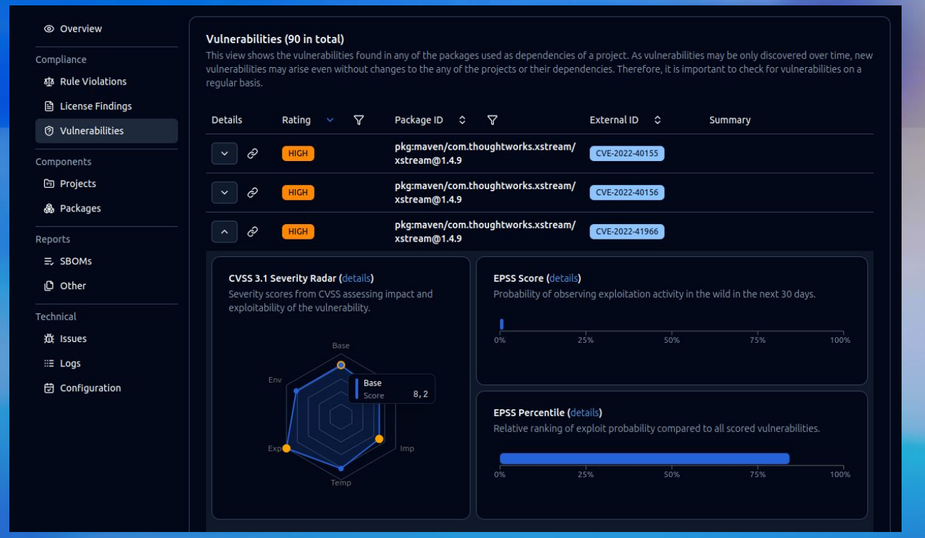
Tool Integrations

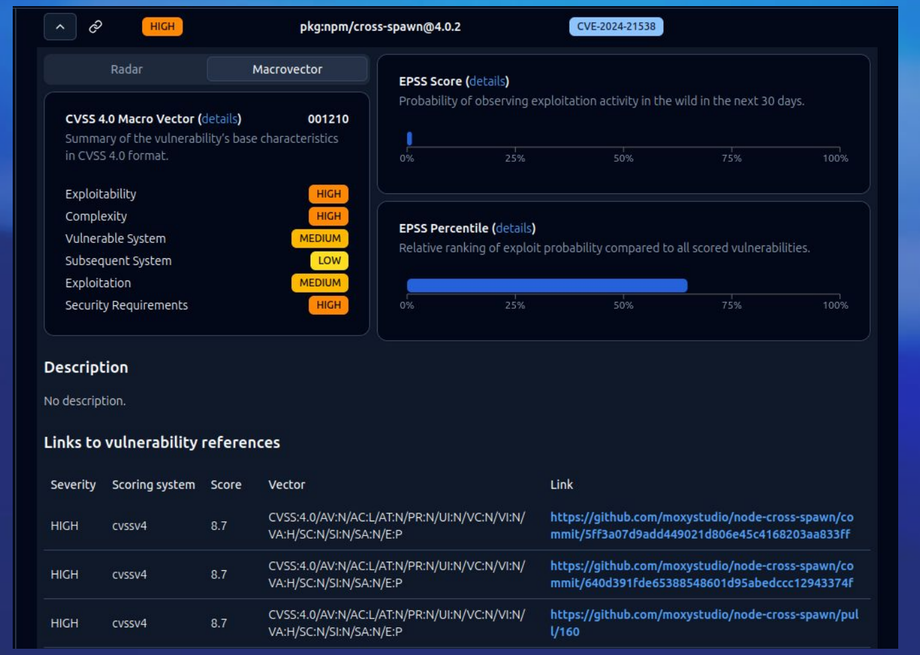


Vulnerability Management

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.

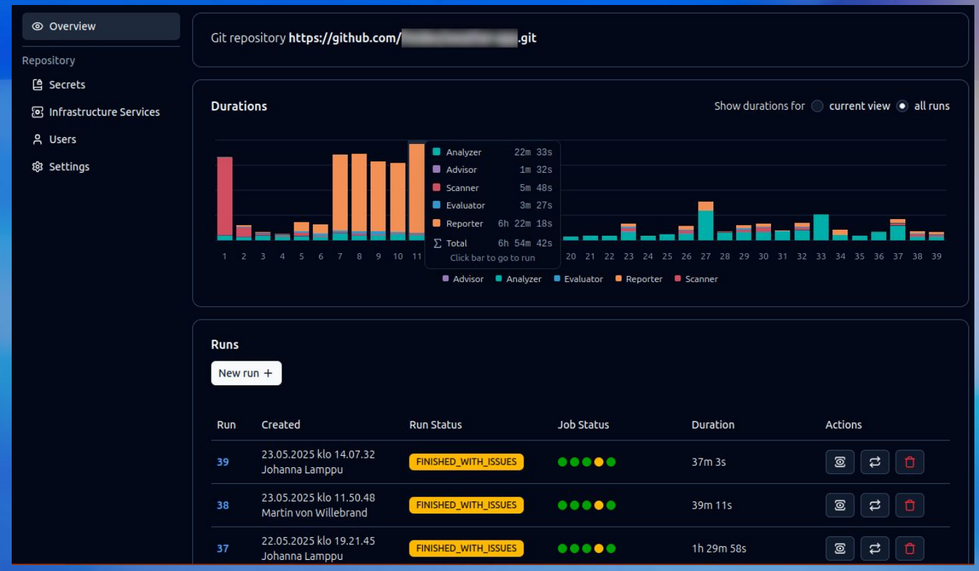


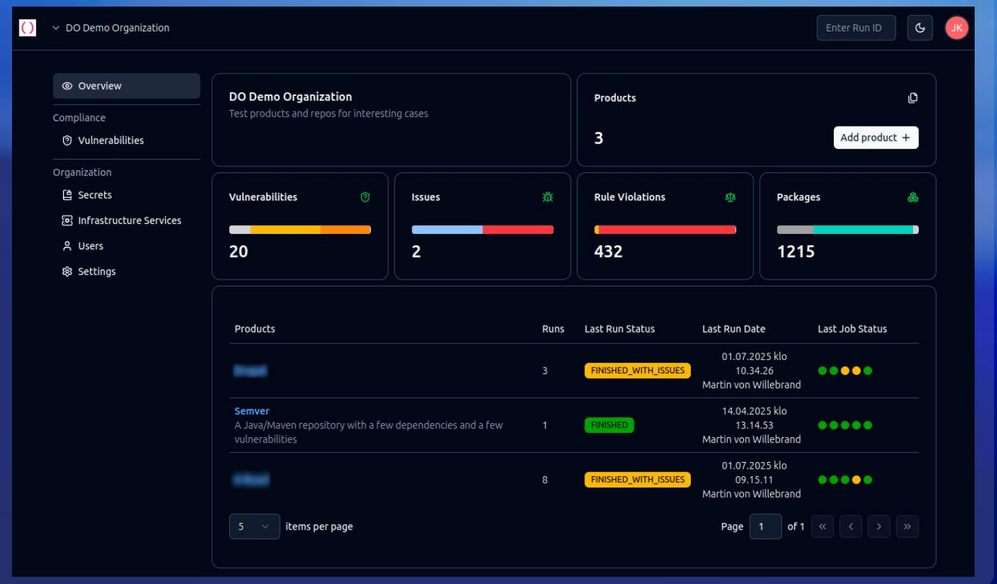


Statistics Dashboards

The Double Open Compliance solution provides

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





{code & compliance} | 22-23 October 2025

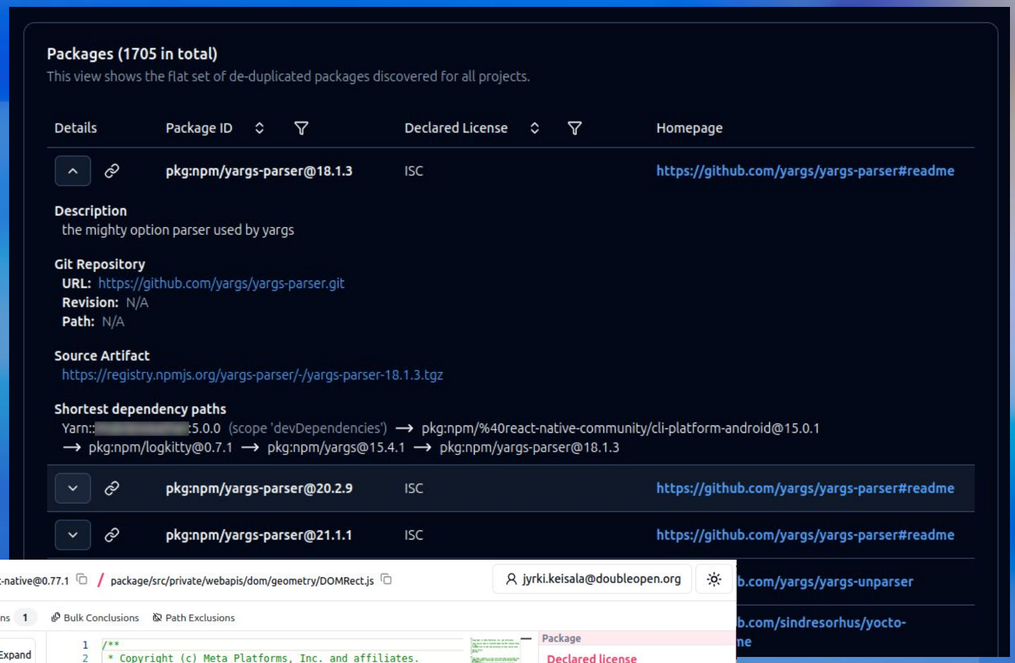
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

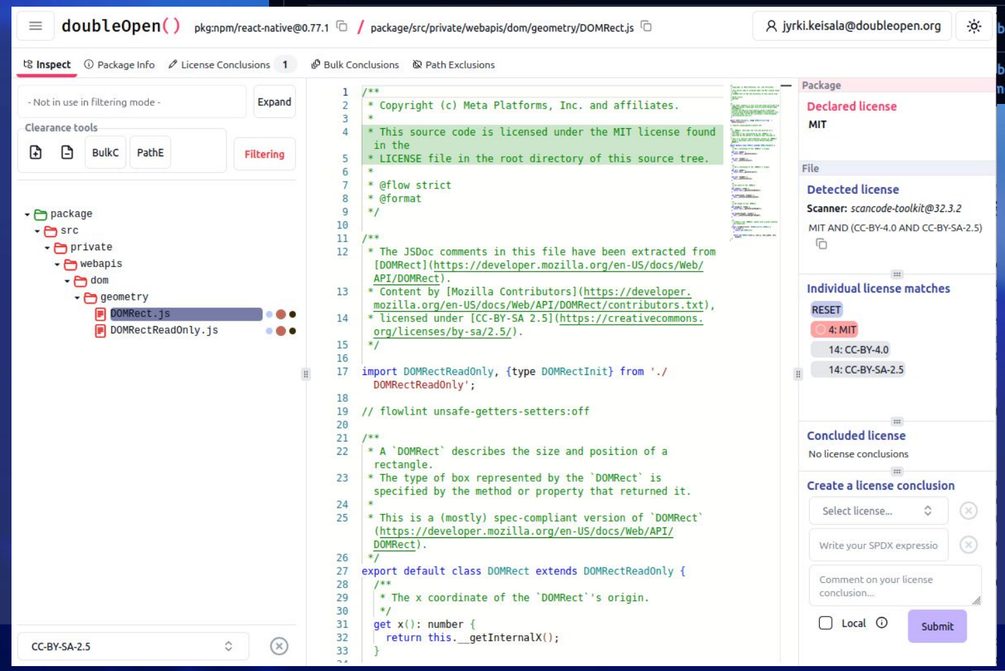
Co-funded by the European Union

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.





{code & compliance} | 22-23 October 2025

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union

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

```
MIT License

Copyright (c) 2022 Syphynx0

Permission is hereby not granted, free of charge, to any person ob
of this software and associated documentation files (the "Softwar
in the Software without restriction, including without limitation
to use, copy, modify, merge, publish, distribute, sublicense, and
copies of the Software, and to permit persons to whom the Softwar
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be 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

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Co-funded by the European Union

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

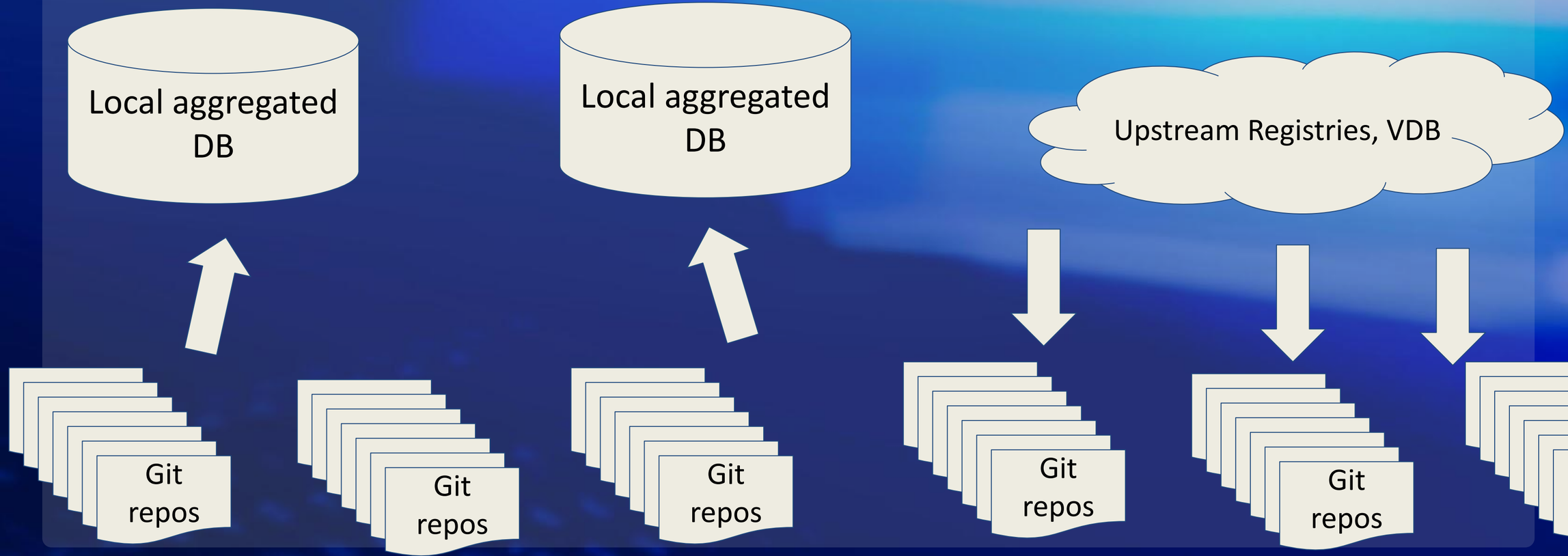
keshav-space Add maven package vulnerabilities from VulnerableCode

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



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).

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Co-funded by the European Union

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.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Co-funded by the European Union

The OCCTET CRA Self-Assessment Platform

cra.occtet.eu

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

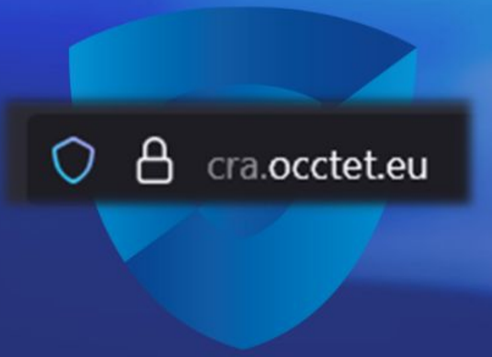
- Designed to guide users' step by step through the CRA compliance journey.

- 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

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

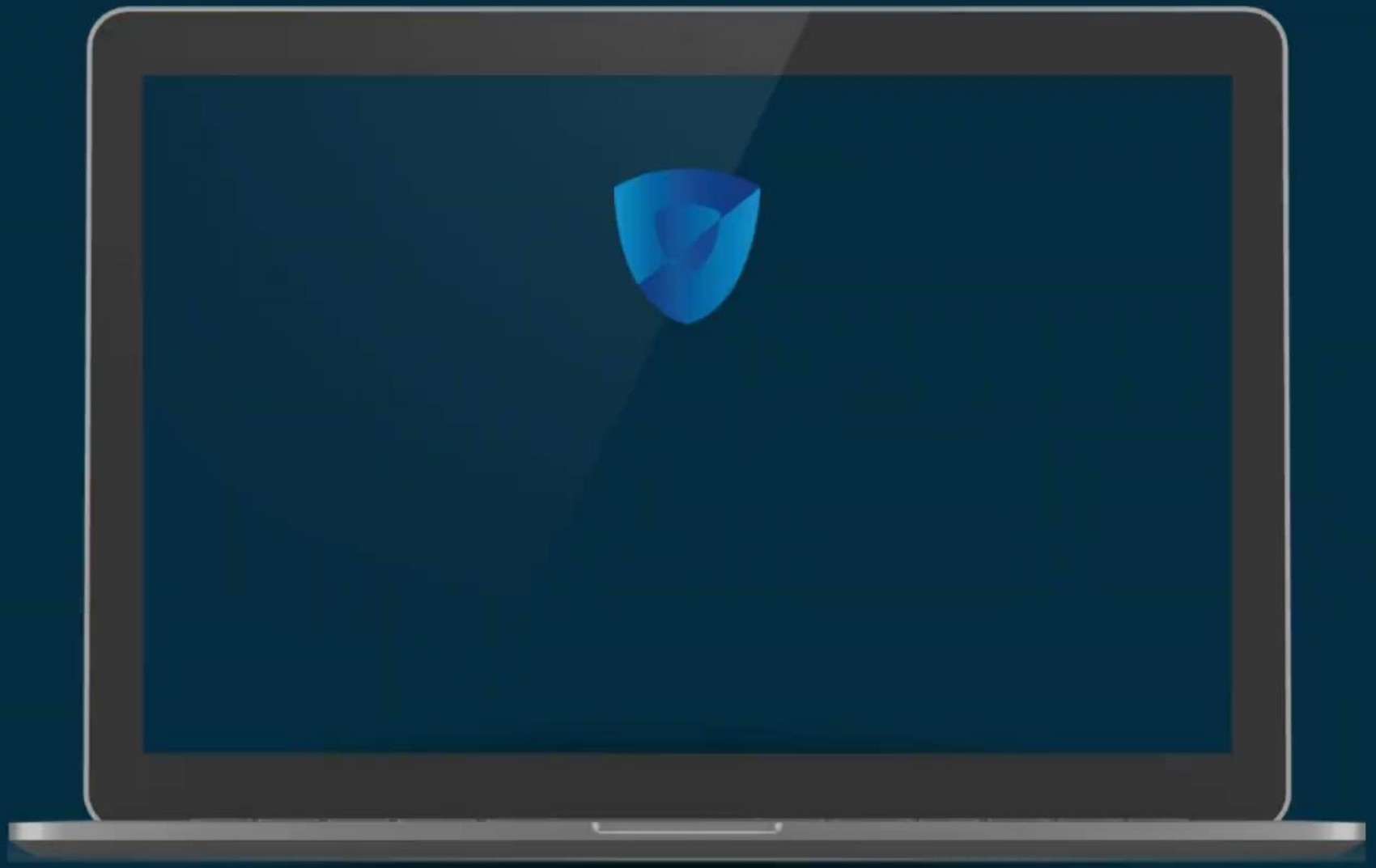
Readiness & Maturity Checklist
"How prepared am I?"

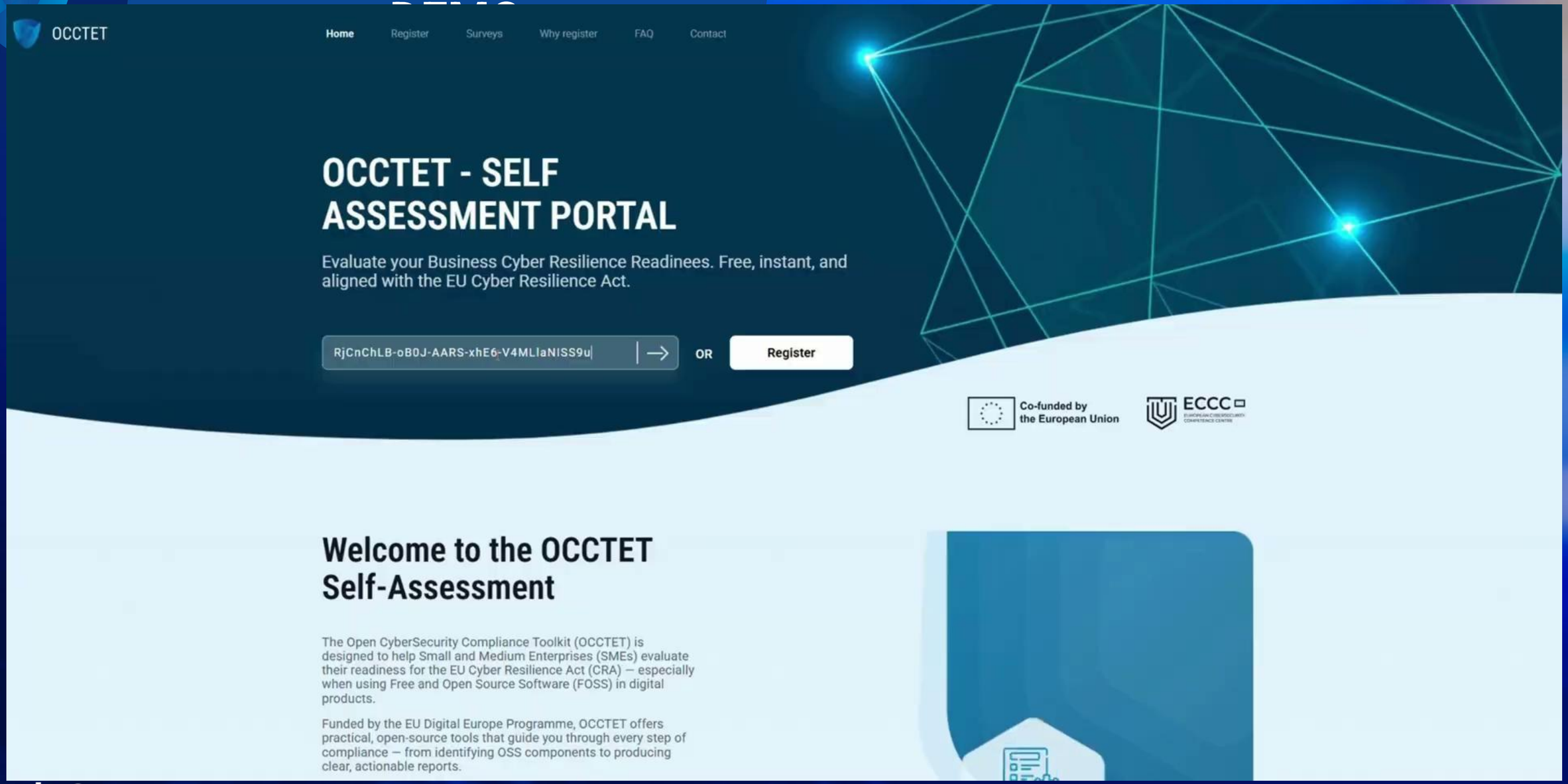
- Translate CRA Annex I security requirements into actionable controls
- Evaluate current practices: Basic / Intermediate / Advanced
- Generate tailored improvement recommendations

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.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Co-funded by the European Union

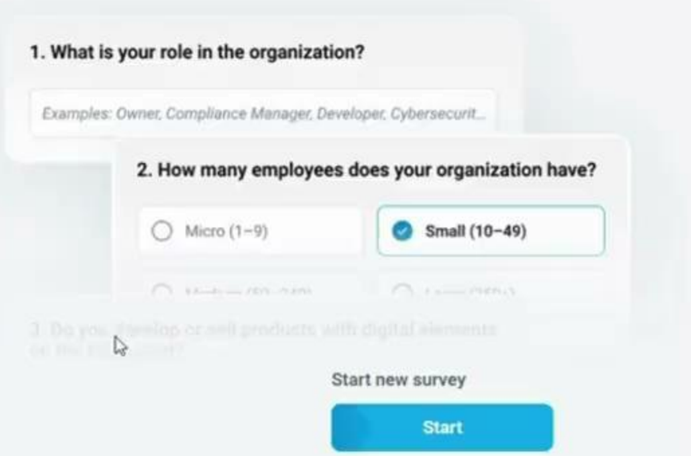


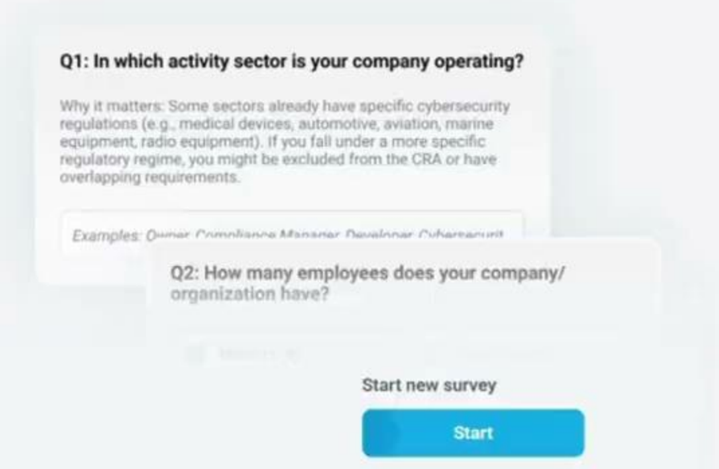

OCCTET
Home
Register
Surveys
Why register
FAQ
Contact
OCCTET - SELF ASSESSMENT PORTAL
Evaluate your Business Cyber Resilience Readinees. Free, instant, and aligned with the EU Cyber Resilience Act.
RjCnChLB-oB0J-AARS-xhE6-V4MLlaNISS9u
OR
Register
Co-funded by the European Union
ECCC
Welcome to the OCCTET 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.

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.





STEP 1 STEP 2 STEP 3

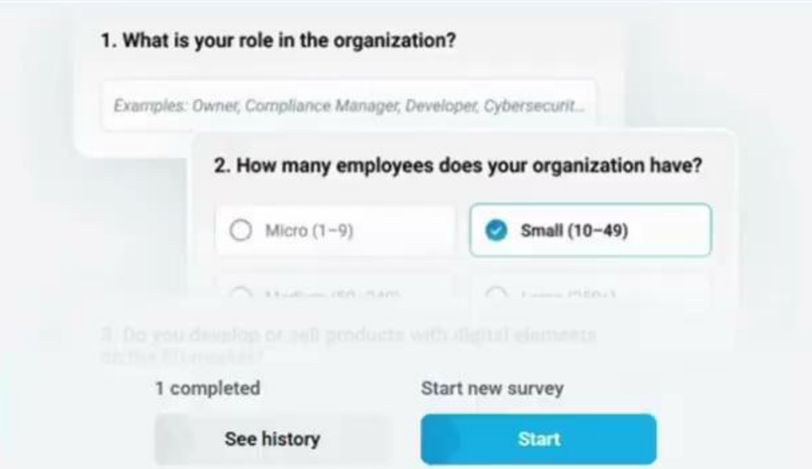
Self-Qualification Questionnaire

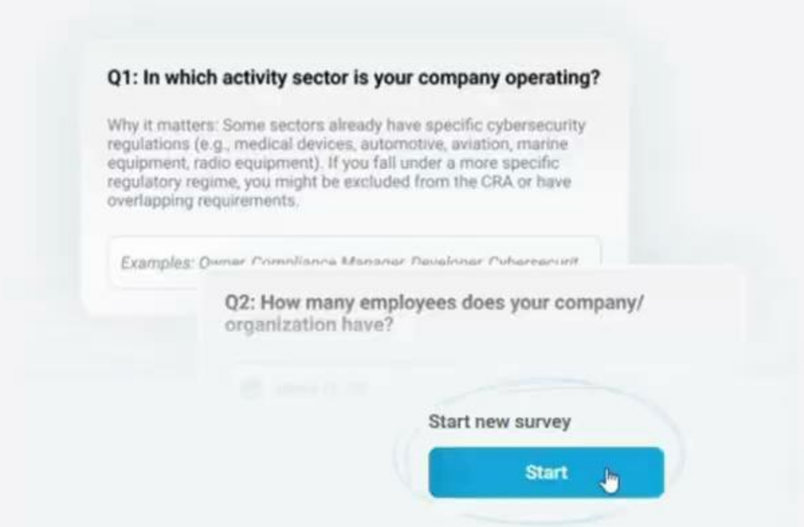
The purpose of this questionnaire is to assist SMEs in establishing the applicability of the CRA, assessing the criticality of their products or services, and accessing structured guidance on compliance and maturity assessment processes.

STEP 1 STEP 2 STEP 3

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.

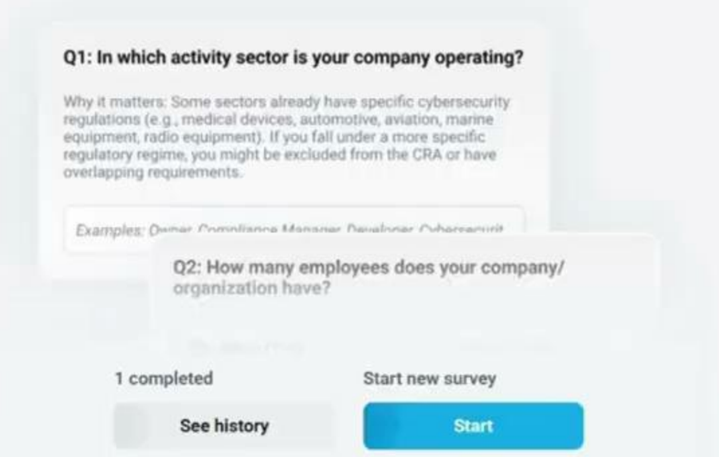




STEP 1 STEP 2 STEP 3

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

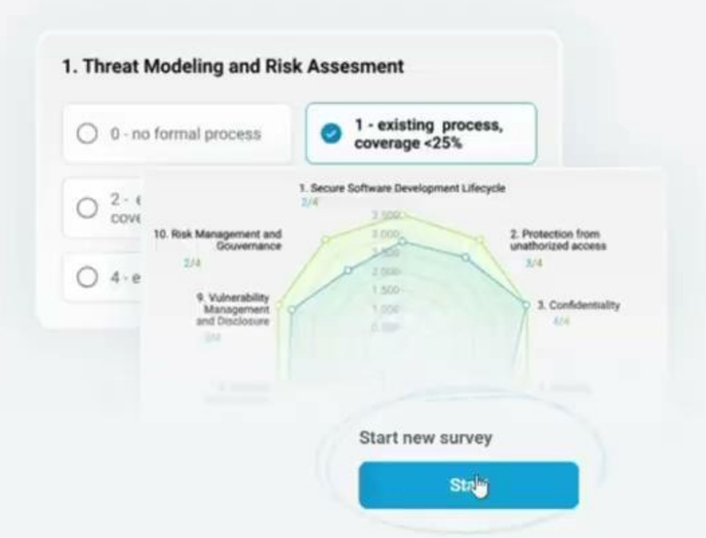
Self-Qualification Questionnaire

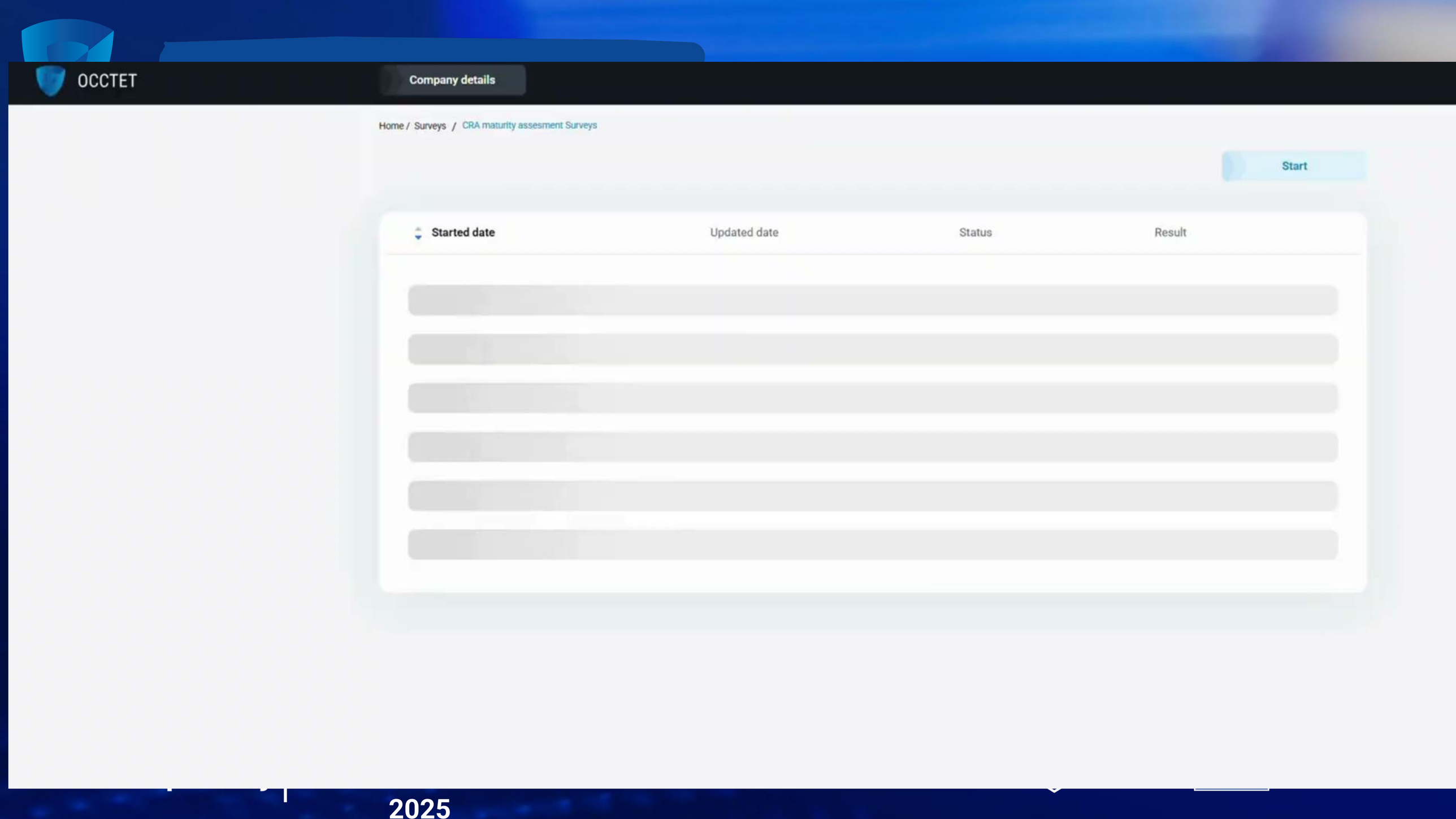
The purpose of this questionnaire is to assist SMEs in establishing the applicability of the CRA, assessing the criticality of their products or services, and accessing structured guidance on compliance and maturity assessment processes.

STEP 1 STEP 2 **STEP 3**

SMEs CRA Maturity Assesment

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.




OCCTET
Company details
Home / Surveys / CRA maturity assesment Surveys
Start
Started date
Updated date
Status
Result

2025

OCCTET

Home Register Surveys Why register FAQ Contact

OCCTET - SELF ASSESSMENT PORTAL

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

Enter your code → OR Register

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

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.

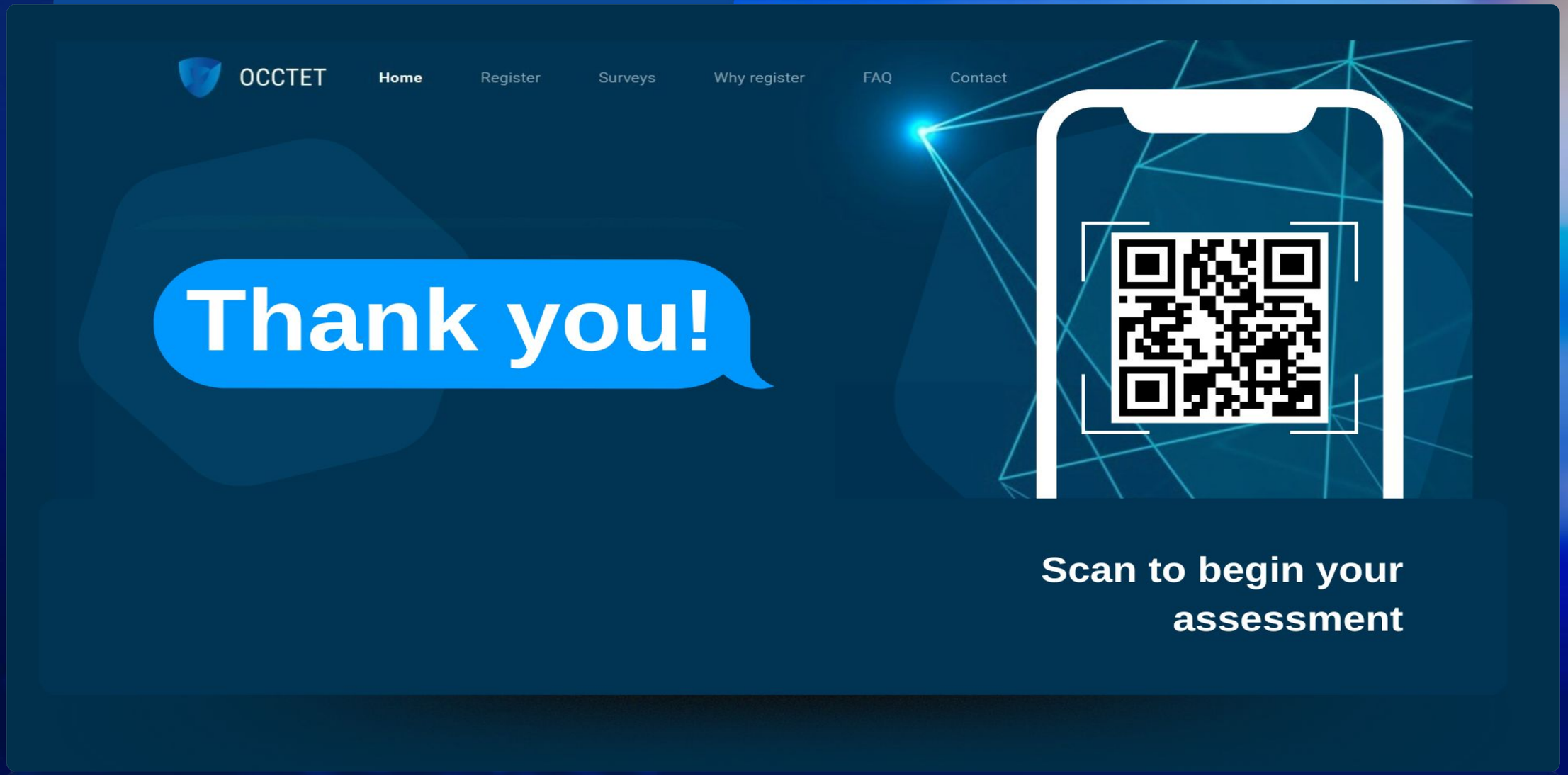
compliance}

22-23 October 2025

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

the European Union

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

Share better inventories

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

CycloneDX

https://cyclonedx.org/docs/1.6/json/#components_items_purl

SPDX®

https:/spdx.github.io/spdx-spec/v3.0.1/model/Software/Properties/packageUrl/

Better PURLs enable standardized VEX formats interoperability

Disclose better vulnerabilities

- Precise vulnerability to package matching with unambiguous package identification

CycloneDX

https://cyclonedx.org/docs/1.6/json/#components_items_purl

OpenVEX

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

CSAF

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

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

AboutCode PurlDB

Continuously updated reference data for open source packages' origin, information and licensing, utilizing PURL.
https://github.com/aboutcode-org/purldb

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

Sonatype OSS Index

OSS Index can consistently map components to their corresponding vulnerability data using PURL.
https://ossindex.sonatype.org/doc/coordinates

ecosyste.ms

Lookup information about a PURL in both text and JSON formats.
https://github.com/andrew/purl

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

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Co-funded by the European Union

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!