occtet.eu

EMPOWER SMALL & MEDIUM ENTERPRISES

OCCTET

Open CyberSecurity Compliance Toolkit

Sébastien Heurtematte — OCCTET Coordinator — Eclipse Foundation

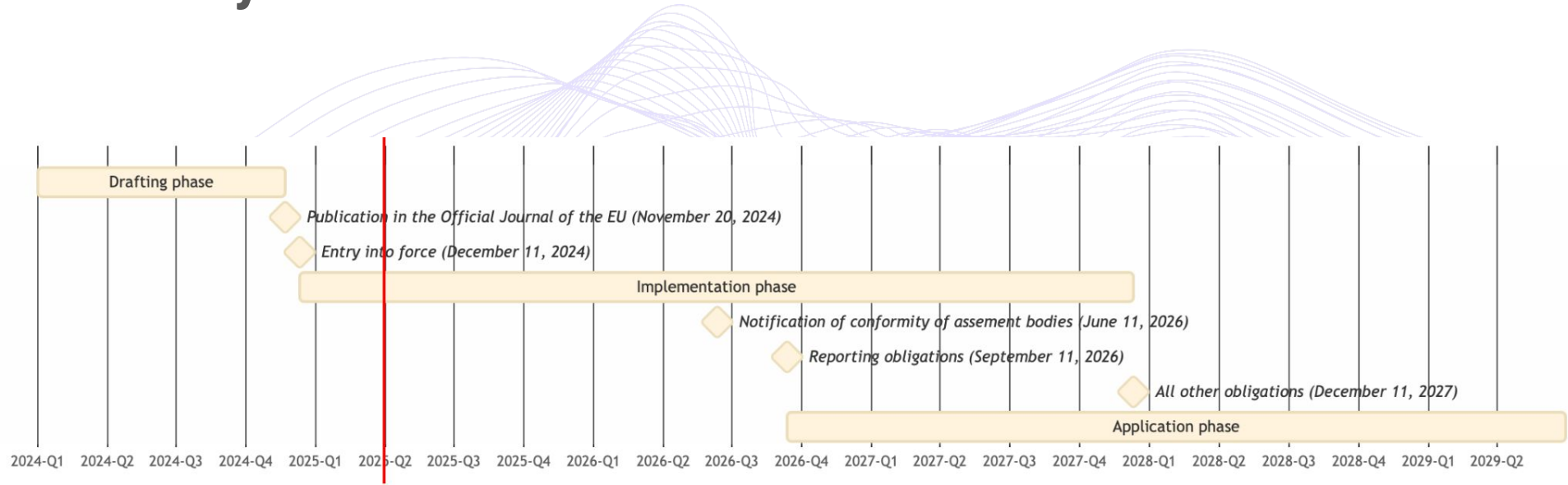
2025/04/14 — CRA Talks

The OCCTET project is funded by the European Union under Grant Agreement 101190574. The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Cyber Resilience Act, in a nutshell

- **Mandatory Cybersecurity Requirements** for Products with Digital Elements
  - From the design phase onwards.
- **Manufacturers**, **Importers** and **Distributors** are responsible for ensuring that products are and remain secure.

CRA Key Dates



CRA Requirements

- **Risk based approach**
- Products with digital elements shall be **designed, developed and produced** in such a way that they ensure an appropriate level of cybersecurity
- **Vulnerability Management** throughout product life cycles
  - Made available on the market **without known exploitable vulnerabilities**
  - **SBOMs** (Software Bill of Materials)
  - Exercise **due diligence** when integrating third parties components sourced, **including Open Source Software**
- Information and Instructions to the user

OCCTET 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

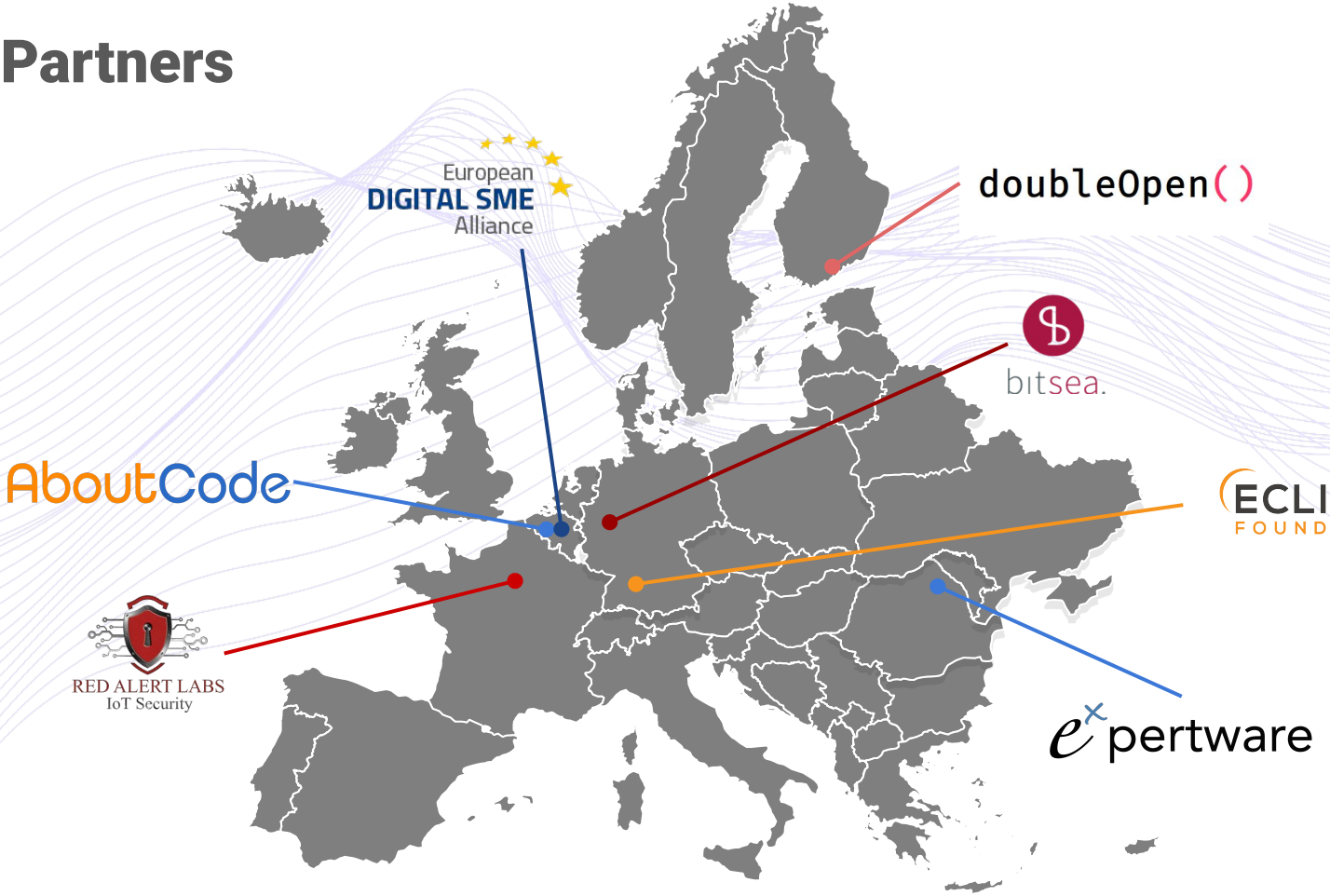
Keywords:

- Cybersecurity
- CRA Compliance
- SMEs/FOSS Communities

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.

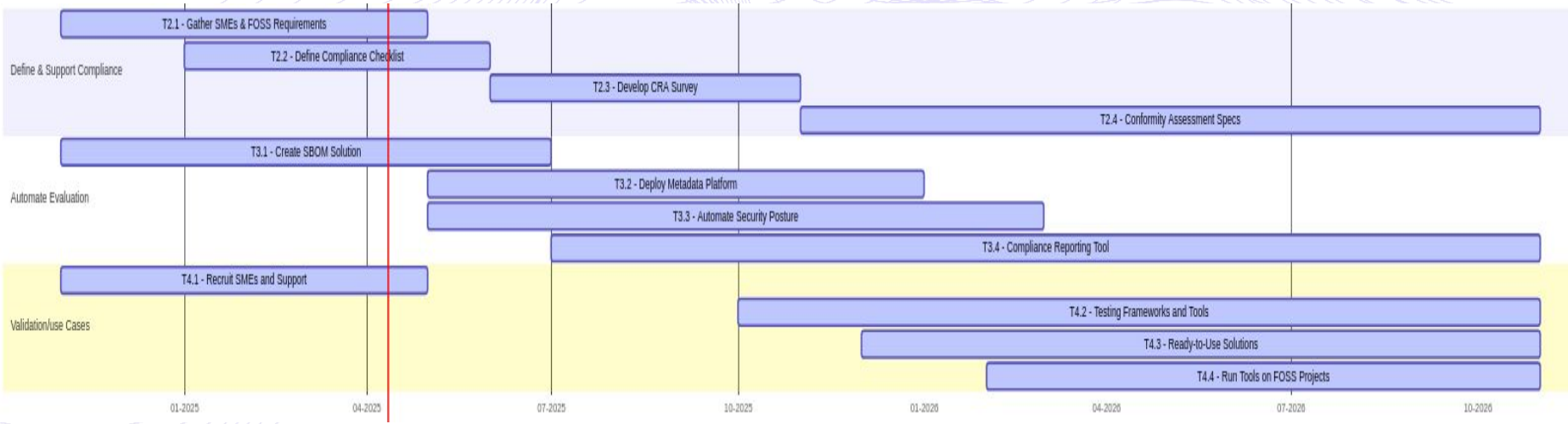
OCCTET Partners



OCCTET Objectives

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

OCCTET Timeline



OCCTET Define and Support Compliance

- **Define and support compliance procedures focuses on 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?
- **Deliverables**:
  - Gather SME and FOSS requirements
  - Define the compliance checklist (related to requirements results and with interviews)
  - Develop the CRA Self-assessment survey and questionnaire => web application

OCCTET Build Open Source Tools to Automate Evaluation

- **Discovery**
  - Identify and classified software components within digital assets => Generation of SBOM
  - Accurate inventory: correctness processes for actionable SBOM
- **Reference Data: FederatedDB**
  - Shared software metadata platform for packages: SBOM, code origin and vulnerability
  - Collect/aggregate/combine/correlated Metadata of FOSS Packages
  - Vulnerabilities aggregate from: NVD, GitHub, GitLab… and upstream Open Data Sources, upstream project advisories
  - Collaboration with vulnerability reporting, peer reviewing, remediation actions

OCCTET Build Open Source Tools to Automate Evaluation

- **Automate triage, evaluation of security posture and remediation of vulnerabilities**
  - Produce an enriched SBOM with known vulnerable software packages
  - Assess if a vulnerability applies and the risks associated with the vulnerability
- **Report**
  - CRA compliance reporting tool
  - Generate outbound SBOMs, VEX(Vulnerability Exploitability eXchange) CyclonDX, and attestations
  - Communicate with upstream FOSS projects, downstream users, customers, government, regulatories agencies

OCCTET KPI

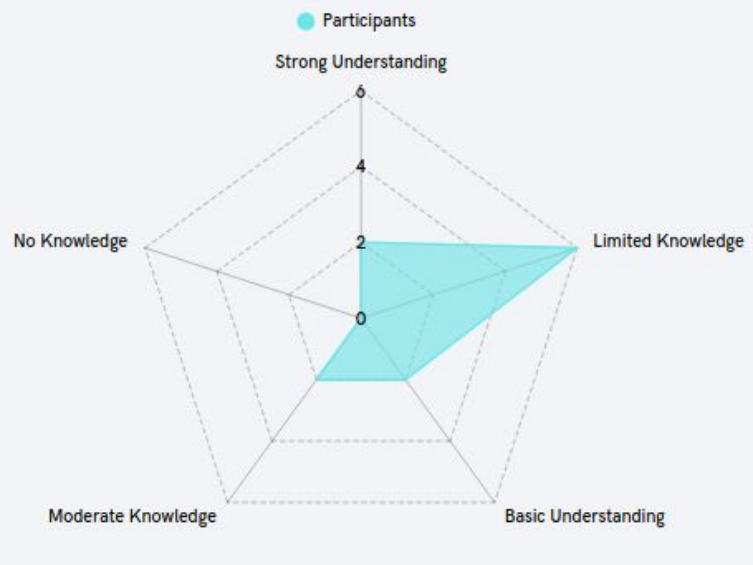
- **Number of CRA essential requirements fully covered by tools**
  - Cover 100% of the essential requirements (18/22 total requirements)
- **Number of CRA essential requirements partially covered by tools**
  - 4 remaining requirements will be partially covered
  - Requires manual and ongoing efforts by SMEs (lifecycle product)
- **Number of tools developed for CRA compliance**
  - Between 10 to 15 tools: document generator, federated data platform, automatic dependency analysis tools, etc.

OCCTET KPI

- **Workshops, trainings, and events for SMEs**
  - Webinar, events, workshops
  - Target: 200+ SMEs
- **Use cases and best practices**
  - 60+ use cases (20 OSS, 40 SME) testing the tools

OCCTET First Deliverables

- **CRA SME requirements and self-assessment checklist**
- **Need Analysis Workshop**
  - Download the report on the website



and contributo

EU Projects - Cross initiative

- Cyberstand, OCCTET, CRA-AI, STAN4CR, STAN4CR2
- Dissemination
  - Cross Promotion Effort
  - Newsletters, webinars, events
- Find opportunities!

Going beyond with OCCTET

- Stay Informed About OCCTET
  - Website: https://occtet.eu
  - Social Media: linkedin, bluesky, youtube
  - Newsletter: soon available!
- Want to participate in OCCTET?
  - Send us an email: occtet-eu@eclipse.org
  - Surveys
    - Shaping CRA Compliance for the FOSS Ecosystem
    - Shaping CRA compliance for SMEs with OCCTET project

occtet.eu

EMPOWER SMALL & MEDIUM ENTERPRISES

The OCCTET project is funded by the European Union under Grant Agreement 101190574. The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

occtet.eu

EMPOWER SMALL
& MEDIUM
ENTERPRISES

Questions?