ORBIT - Launchpad

Leveraging OpenSSF Tools and Frameworks for Manufacturer CRA Due Diligence

European Open Source Security Forum 2026

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Speakers

Christina Freeman, Principal Program Manager, Red Hat Product Security

- Highly skilled Information Security Governance and Compliance Professional with extensive expertise in industry standards, U.S. government requirements, and global regulations.
- Currently serves as the Principal Program Manager for Product Security at Red Hat, where she leads the Product Security governance program and ensures Product Security requirements are aligned with industry regulatory requirements.

Ryan Waite, Partner Group Manager, Azure Office of the CTO

- Leads Azure Open Source Incubations and Open Source Ecosystem teams, focused on how open source collaboration enables all of us to do more together than we can do alone.
- Led engineering teams focused on high performance computing, big data analytics, fraud detection, and mobile computing at Microsoft, Amazon Web Services, and Cray, the Supercomputing Company.

Legal Disclaimer

This is **NOT** legal advice and we are **NOT** lawyers.

ORBIT Launchpad builds upon existing OpenSSF tools and frameworks to help manufacturers demonstrate due diligence for their Cyber Resilience Act (CRA) obligations. Manufacturers are responsible for their own assessments and decisions regarding CRA compliance.

The Manufacturer Responsibility - Cyber Resilience Act

1

CRA Defines Security Requirement Obligations for Manufacturers and Stewards.

Manufacturer requirements are defined in Annex 1, as well as Articles 13, 14, 31, and 32, including open source due diligence. Steward requirements are primarily defined in Article 24. Some manufacturers are also stewards. There are no requirements for maintainers of open source.

2

CRA Regulation Guidance Is Evolving

The CRA lacks a clear definition of what "due diligence" means for open source consumption, single reporting platform has not yet been finalized although reporting requirements begin September 11, 2026. Many vertical and horizontal standards are in still in draft.

3

Most Existing Open Source Security Tools and Frameworks are for Maintainers

Most existing open source security tools and frameworks are designed for maintainers to demonstrate security fundamentals. There is a gap for manufacturers needing to demonstrate CRA due diligence.

4

Multiple Manufacturer Approaches To Solve CRA Requirements

As manufacturers look to fulfill CRA requirements, there is an opportunity to align and scale tooling efforts, across industries and foundations.

Opportunity for Manufacturers

Leveraging existing OpenSSF frameworks and extending them to help manufacturers demonstrate due diligence with the CRA.

OSPS Baseline

Defines 64 security requirements across 3 maturity levels, covering 8 security areas. It provides a minimum security checklist for open source projects which can streamline compliance efforts with global standards like the CRA and NIST SSDF.

Security Badge Program

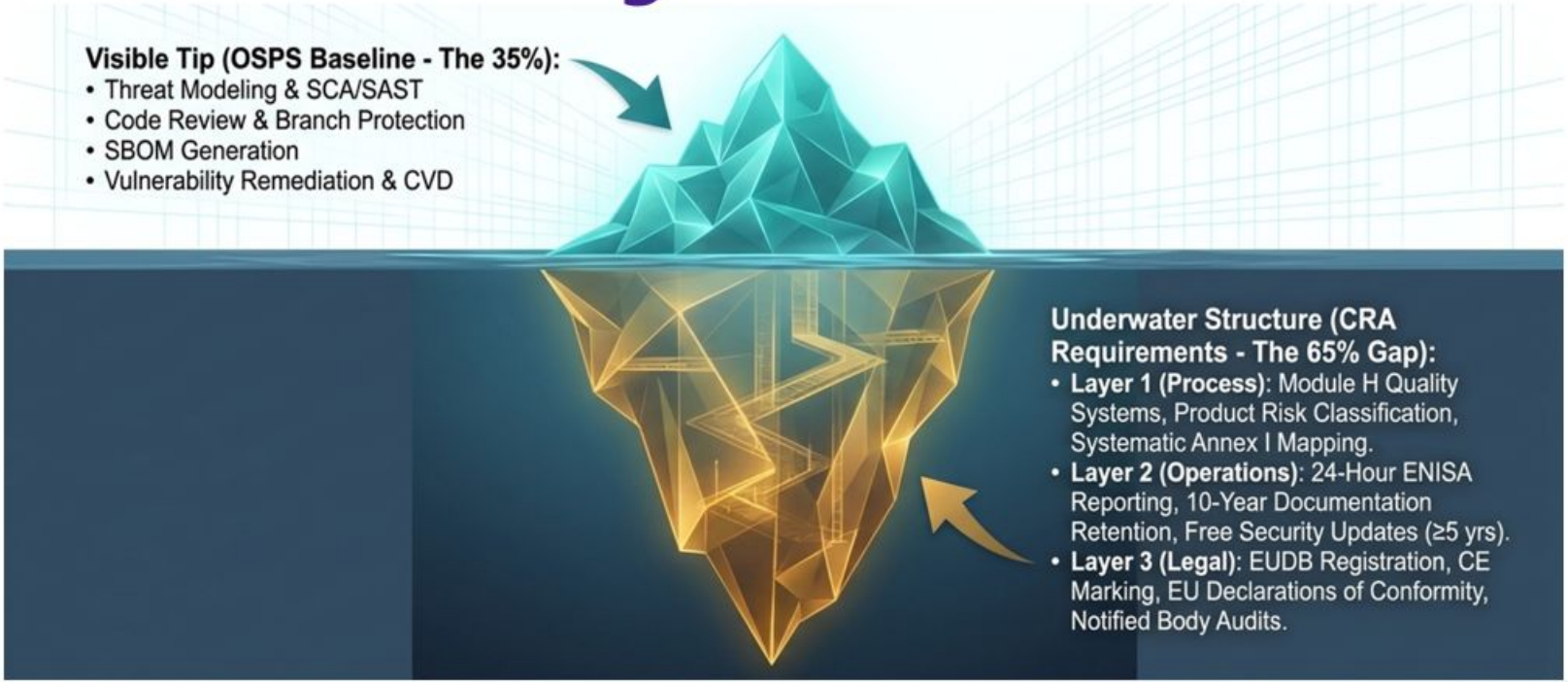
Enables OSS projects to voluntarily self-certify against best practice criteria at no cost, giving consumers transparent, verifiable evidence of upstream project security across passing, silver, and gold tiers.

S2C2F

A consumption-focused framework using a threat-based, risk-reduction approach with 8 practices and 4 maturity levels to secure how organizations consume open source software dependencies.

We are building upon these tools to create machine-readable outputs that help manufacturers demonstrate due diligence with the CRA.

OSPS Baseline Alignment with CRA



OSPS provides a world-class security engineering foundation, but development practices cannot substitute for legal compliance processes.

NotebookLM

ORBIT Working Group: Launchpad SIG

What It Is

- A space for manufacturers to review and discuss CRA obligations
- Contribute feedback, engineering resources, and tooling extensions to ORBIT projects
- Share best practices across manufacturers
- Partner with Global Cyber Policy

How It Operates

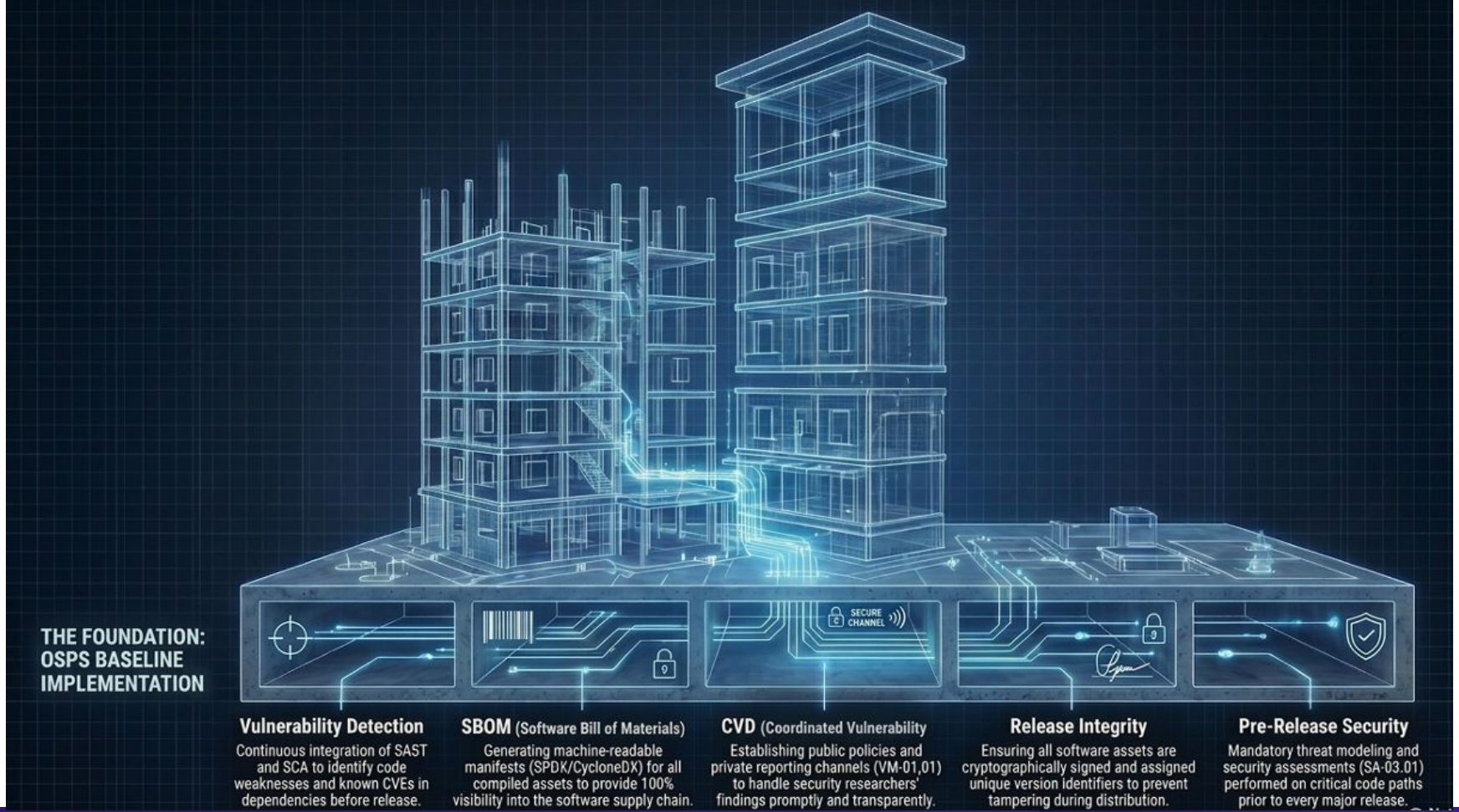
- Do no harm — no burden on maintainers
- Transparency, no duplication of efforts, progress over perfection
- Align compliance guidance with Global Cyber Policy WG
- Share lessons and provide feedback to ORBIT tooling maintainers
- Collaborate across foundations

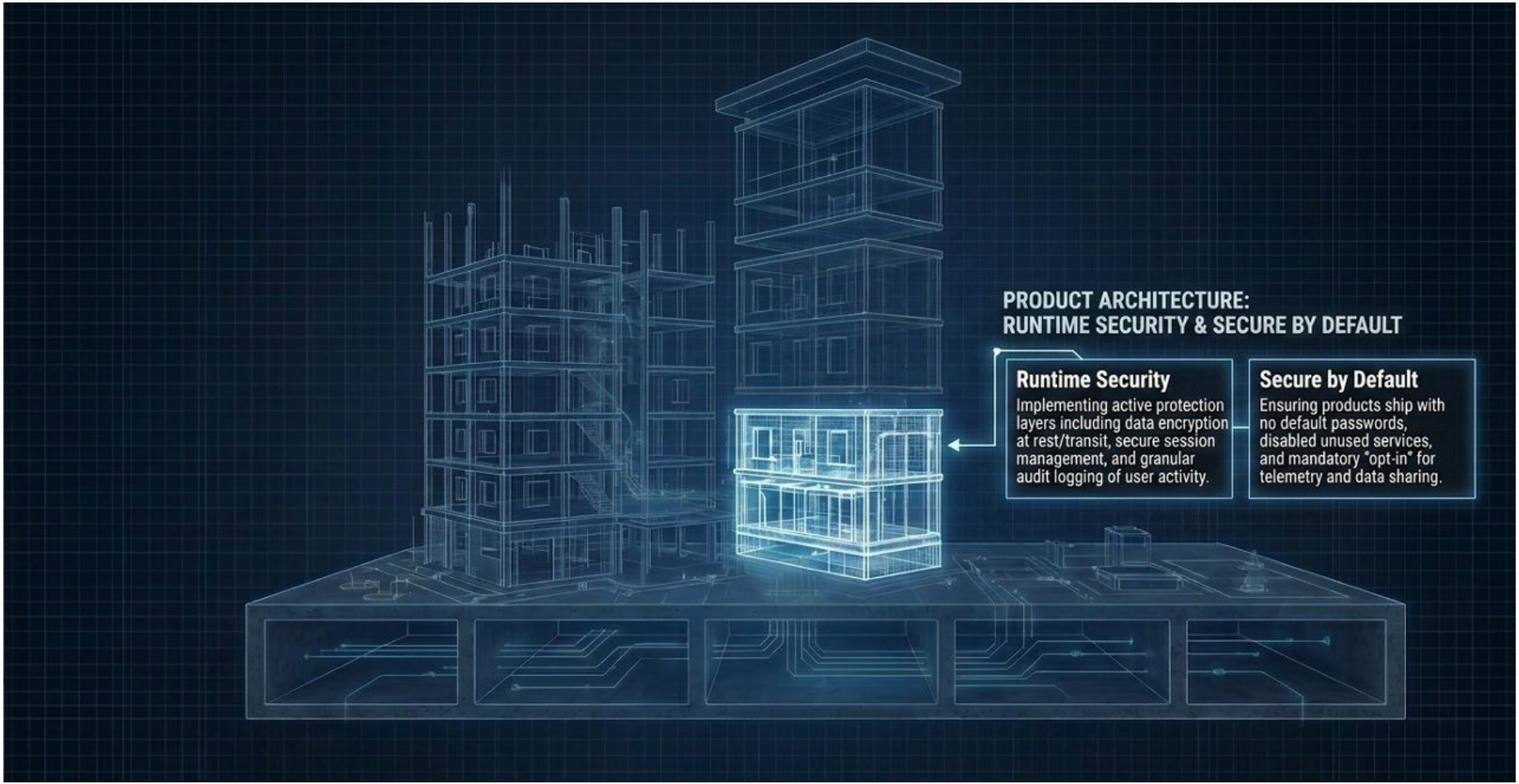
2026 Focus Areas

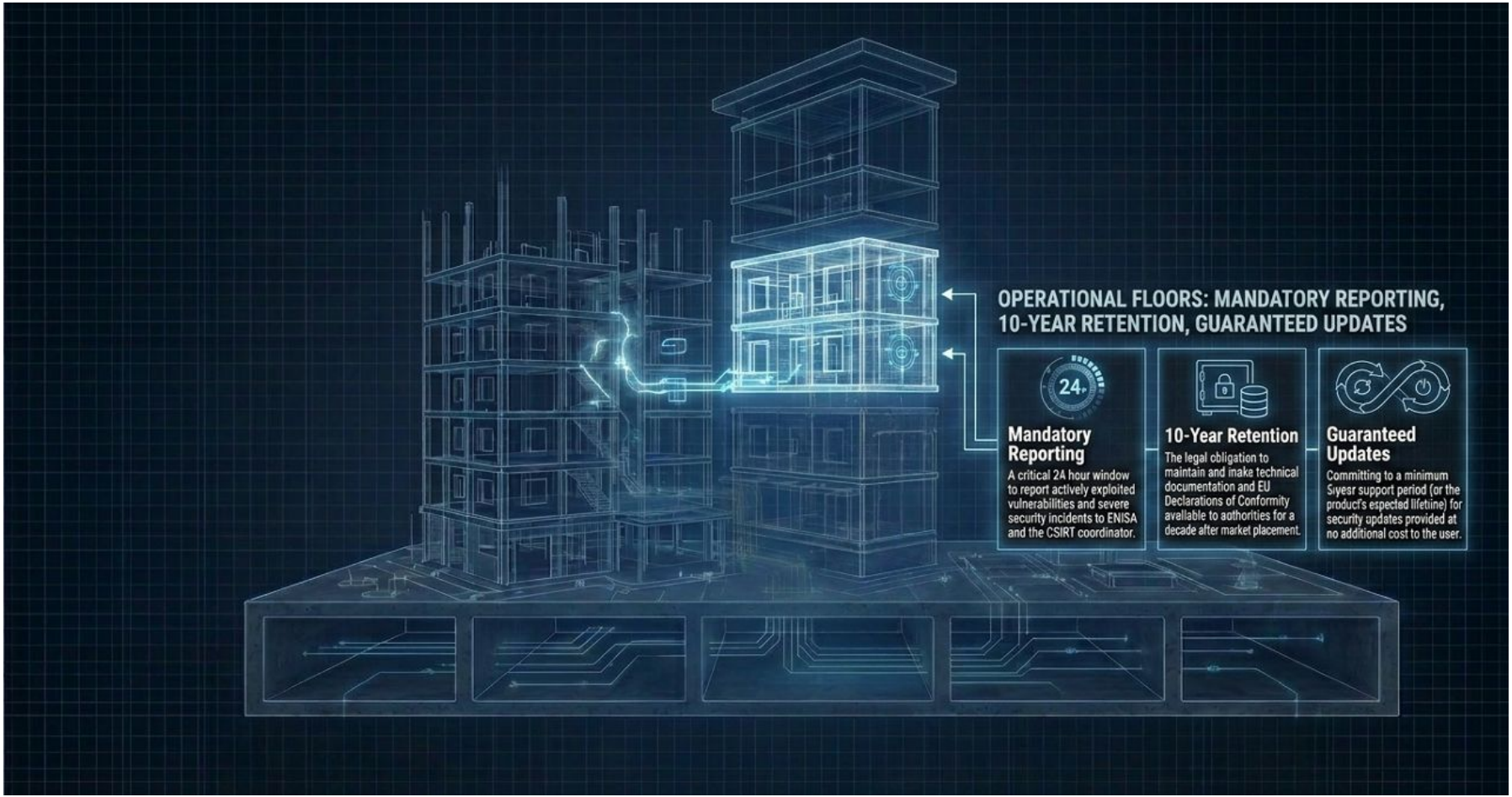
- Drive community alignment for Open Source Due Diligence Requirements for Manufacturers
- Align CRA Manufacturer Requirements
- Investigate OpenSSF Tooling, Industry Best Practices

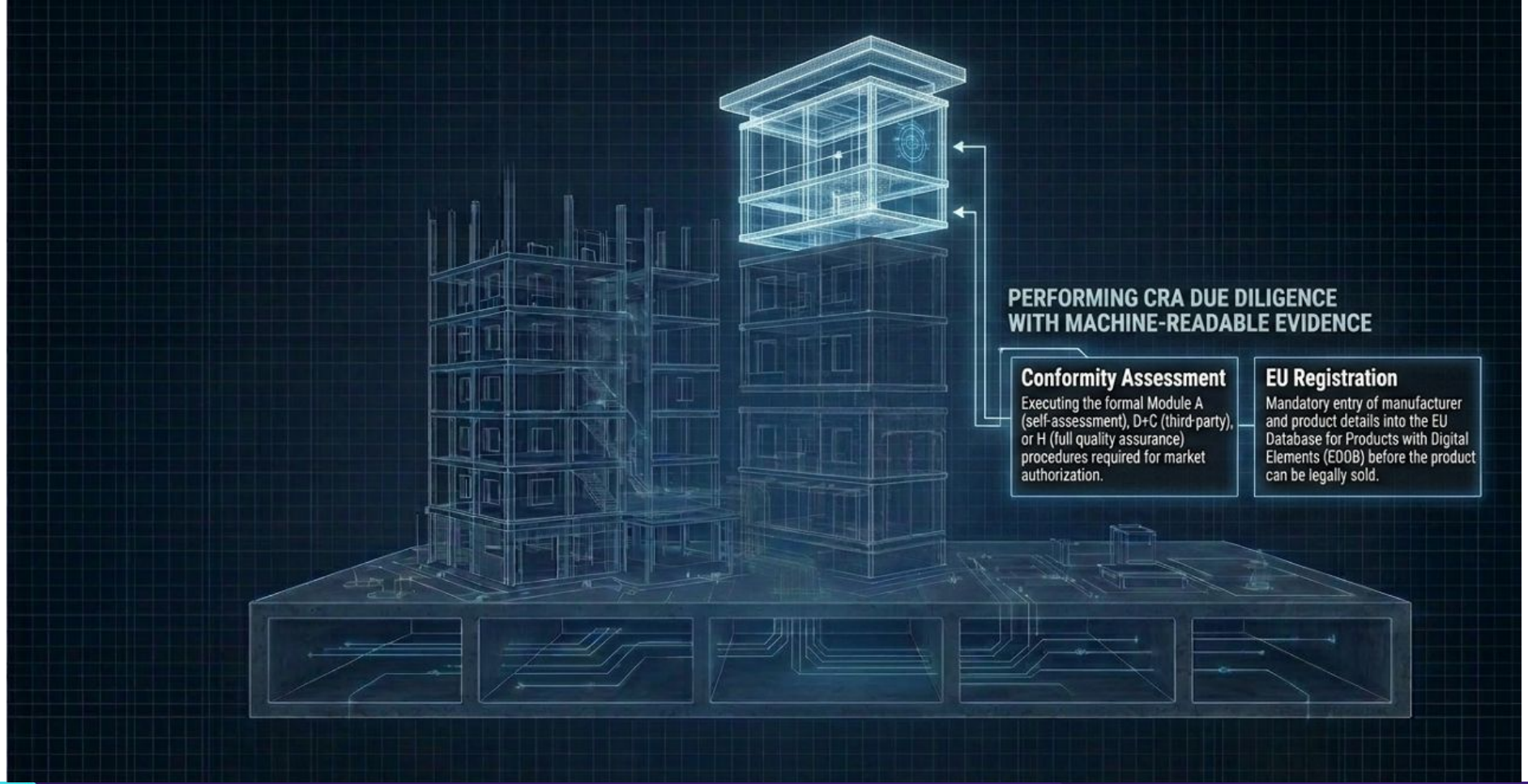
Key Outcomes

- Shared best practices and community guidance
- Tooling improvements and gap identification to help manufacturers demonstrate due diligence with the CRA

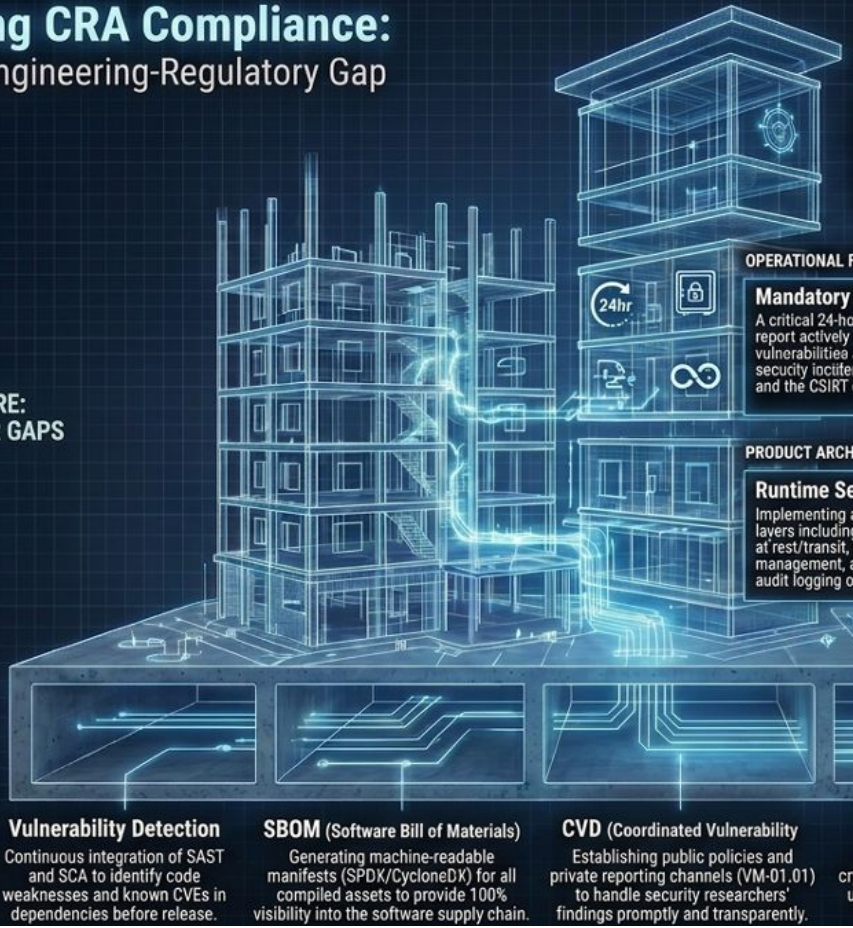

THE FOUNDATION:
OSPS BASELINE
IMPLEMENTATION
SECURE CHANNEL
Vulnerability Detection
Continuous integration of SAST and SCA to identify code weaknesses and known CVEs in dependencies before release.
SBOM (Software Bill of Materials)
Generating machine-readable manifests (SPDX/CycloneDX) for all compiled assets to provide 100% visibility into the software supply chain.
CVD (Coordinated Vulnerability
Establishing public policies and private reporting channels (VM-01,01) to handle security researchers' findings promptly and transparently.
Release Integrity
Ensuring all software assets are cryptographically signed and assigned unique version identifiers to prevent tampering during distribution.
Pre-Release Security
Mandatory threat modeling and security assessments (SA-03.01) performed on critical code paths prior to every major release.


PRODUCT ARCHITECTURE:
RUNTIME SECURITY & SECURE BY DEFAULT
Runtime Security
Implementing active protection layers including data encryption at rest/transit, secure session management, and granular audit logging of user activity.
Secure by Default
Ensuring products ship with no default passwords, disabled unused services, and mandatory "opt-in" for telemetry and data sharing.


OPERATIONAL FLOORS: MANDATORY REPORTING, 10-YEAR RETENTION, GUARANTEED UPDATES
24
Mandatory Reporting
A critical 24 hour window to report actively exploited vulnerabilities and severe security incidents to ENISA and the CSIRT coordinator.
10-Year Retention
The legal obligation to maintain and make technical documentation and EU Declarations of Conformity available to authorities for a decade after market placement.
Guaranteed Updates
Committing to a minimum 5-year support period (or the product's expected lifetime) for security updates provided at no additional cost to the user.


PERFORMING CRA DUE DILIGENCE
WITH MACHINE-READABLE EVIDENCE
Conformity Assessment
Executing the formal Module A (self-assessment), D+C (third-party), or H (full quality assurance) procedures required for market authorization.
EU Registration
Mandatory entry of manufacturer and product details into the EU Database for Products with Digital Elements (EDDB) before the product can be legally sold.

Architecting CRA Compliance:
Bridging the Engineering-Regulatory Gap



PERFORMING CRA DUE DILIGENCE WITH MACHINE-READABLE EVIDENCE

Conformity Assessment
Executing the formal Module A (self-assessment), D+C (third-party), or H (full quality assurance) procedures required for market authorization.

EU Registration
Mandatory entry of manufacturer and product details into the EU Database for Products with Digital Elements (EOOB) before the product can be legally sold.

THE SUPERSTRUCTURE: CRA MANUFACTURER GAPS

OPERATIONAL FLOORS: MANDATORY REPORTING, 10-YEAR RETENTION, GUARANTEED UPDATES

Mandatory Reporting
A critical 24-hour window to report actively exploited vulnerabilities and severe security incidents to ENISA and the CSIRT coordinator.

10-Year Retention
The legal obligation to maintain and make technical documentation and EU Declarations of Conformity available to authorities for a decade after market placement.

Guaranteed Updates
Committing to a minimum 5-year support period for the product's expected lifetime) for security updates provided at no additional cost to the user.

PRODUCT ARCHITECTURE: RUNTIME SECURITY & SECURE BY DEFAULT

Runtime Security
Implementing active protection layers including data encryption at rest/transit, secure session management, and granular audit logging of user activity.

Secure by Default
Ensuring products ship with no default passwords, disabled unused services, and mandatory "opt-in" for telemetry and data sharing.

THE FOUNDATION: OSPS BASELINE IMPLEMENTATION

Vulnerability Detection
Continuous integration of SAST and SCA to identify code weaknesses and known CVEs in dependencies before release.

SBOM (Software Bill of Materials)
Generating machine-readable manifests (SPDX/CycloneDX) for all compiled assets to provide 100% visibility into the software supply chain.

CVD (Coordinated Vulnerability
Establishing public policies and private reporting channels (VM-01.01) to handle security researchers' findings promptly and transparently.

Release Integrity
Ensuring all software assets are cryptographically signed and assigned unique version identifiers to prevent tampering during distribution.

Pre-Release Security
Mandatory threat modeling and security assessments (SA-03.01) performed on critical code paths prior to every major release

CRA Catalogs for Manufacturers – Machine Readable & Scalable

Catalogs pull in existing OSPS Baseline Level Security Control Statements and amend with new security control statements. Catalogs will produce machine readable and scalable evidence for manufacturers.

CRAB-FOMA: CRA Baseline for Manufacturers

Security controls catalog mapped to CRA manufacturer requirements
(Annex 1, Articles 13, 14, 31, 32)

includes

CRAB-FOSC: CRA Baseline for Open Source Consumption

Subset of CRAB-FOMA addressing Article 13 para 5: manufacturer due diligence for open source consumption
For manufacturers who only need the open source consumption piece

Get Involved with ORBIT Launchpad

SIG Meetings

Every other Friday, 11:00 AM EST

Next meeting: June 12

Comms & Code

Slack: https://openssf.slack.com/archives/C0ADW8Q20BS

GitHub: https://github.com/ossf/orbit-launchpad

Review

CRAB-FOSC

CRA Baseline For Open Source Components

https://docs.google.com/spreadsheets/d/1_Ym2f1VumXN5y6sQUzXZbmyIZ8ySuYYmSEaEoh8hQ5U/edit?gid=1542948066#gid=1542948066

Review

CRAB-FOMA

CRA Baseline For Manufacturers

https://docs.google.com/spreadsheets/d/1k4C4wxQZRubHHa-4vXIzvTFvNyRRKEfJZ7EPZClAmiY/edit?gid=1602912614#gid=1602912614