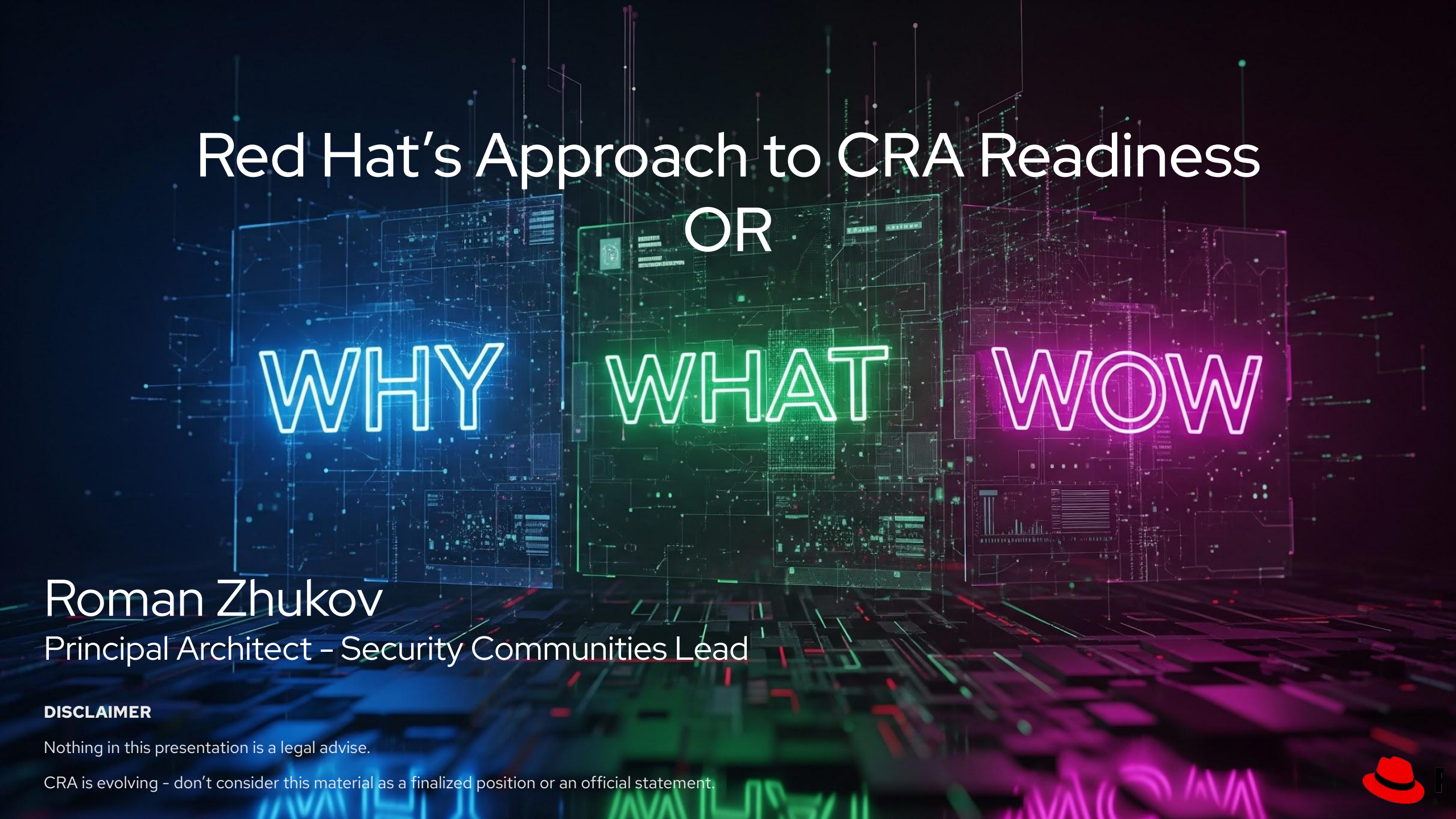
Red Hat's Approach to CRA Readiness
OR



Roman Zhukov
Principal Architect - Security Communities Lead

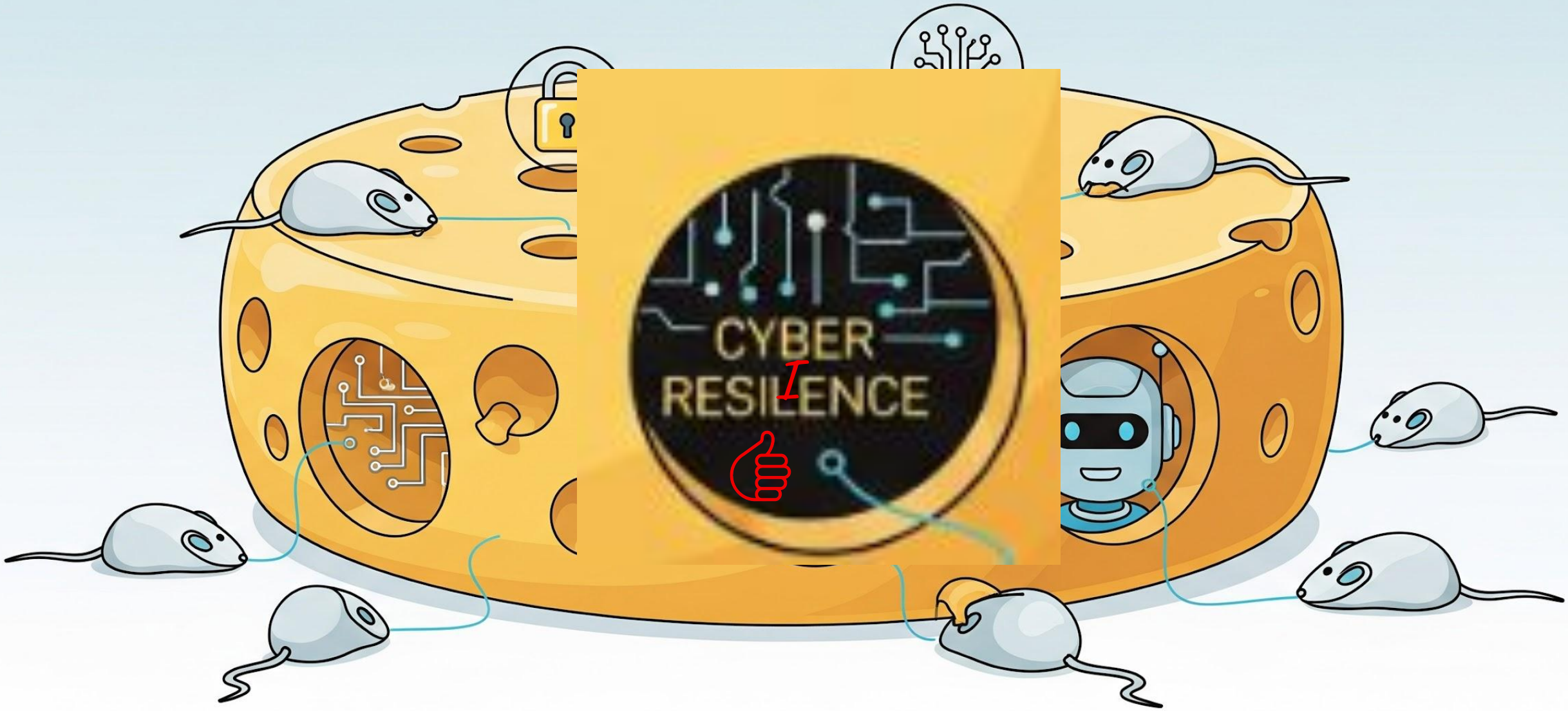
DISCLAIMER

Nothing in this presentation is a legal advise.

CRA is evolving - don't consider this material as a finalized position or an official statement.

THE “WHY”

I love this guy


CYBER
RESILENCE

Why CRA is Good

> CRA has a potential to make **more for supply-chain security** and OSS ecosystem health at scale **in just a few years** than
>
> we, as a minority of security experts in the engineering community, have been trying to make in decades.

OSS Security Community

public inbox for libc-alpha@sourceware.org

search help / color / mirror / Atom feed

* Cybersecurity Risk Assessment Request from [redacted] for libnsl
@ 2025-08-11 11:37 [redacted] [EMR/MSOL/PUNE]
2025-08-11 21:57 ` Mark Wielaard
0 siblings, 1 reply; 3+ messages in thread
From: [redacted] [EMR/MSOL/PUNE] @ 2025-08-11 11:37 UTC (permalink / raw)
To: bug-libc
Cc: [redacted]

[-- Attachment #1: Type: text/plain, Size: 2539 bytes --]

Hello,

I hope this message finds you well.

As part of our ongoing efforts to comply with the EU Cyber Resilience Act (CRA), we are currently c

To support this initiative, we kindly request your input on the following questions related to your

Additional Information:

* Purpose: This security assessment is part of our due diligence and regulatory compliance obli
* Confidentiality: All information shared will be treated as confidential and used solely for t
* Contact: Should you have any questions or need further clarification, please feel free to rea

We kindly request your response by Monday, August 25, 2025, to ensure timely completion of our assessment process. Thank you for your coopera

Queries to Vendor	
Response from Vendor (Yes/No)	
Additional Remarks from Vendor	
1	
Is Secure Software Development Lifecycle followed for developing this component?	
8	
Do you comply with EU-CRA requirements?	
9	
Do you provide proof of conformity regarding adherence to EU-CRA? If yes please mention details in Remark column	

Thanks for giving us exactly 2 week, bro =)

PDEs* are...

src: https://knowyourmeme.com/memes/x-x-everywhere

- Smart home
- **Operating Systems**
- Web browsers
- Password mgrs.

Important Class I (19)

- Firewalls
- Tamper-resistant CPUs
- **Hypervisors**

Important Class II (4)

- HW Devices w/Security Boxes
- Smart meter gateways
- Smart Cards

Critical (3)

- Consumer devices and everything else
- **All other SW****

Default Category

The rest 90%

* PDE - Product with Digital Elements

** SW that is PDE as defined in the CRA.

Red Hat role in CRA

Red Hat as a Manufacturer

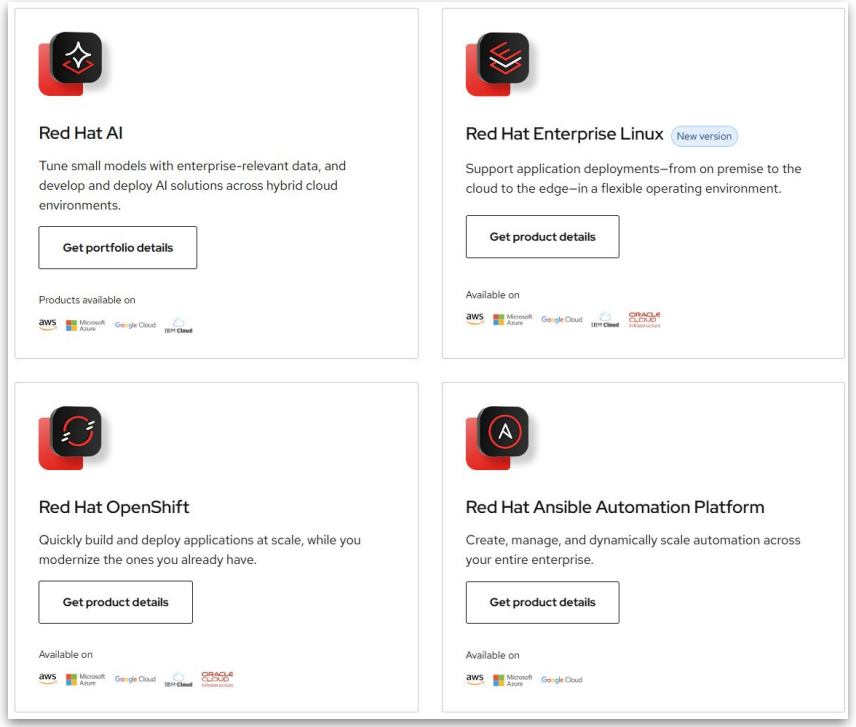
- Provider of enterprise open-source software solutions for the global market, including the EU.

Red Hat as a potential Open Source Software Steward

- Red Hat's relationship with open source software is foundational. The company actively supports Fedora and countless others projects.

Red Hatters are Contributors and Maintainers

- Thousands of Red Hatters contribute to open source projects everyday.



fedora

KONFLUX

ramalama

We're leading CRA efforts in Open Source Communities and EU Official Standardization bodies to make sure the open-source ecosystem is CRA-compliant and healthy.

THE LINUX FOUNDATION

ECLIPSE FOUNDATION

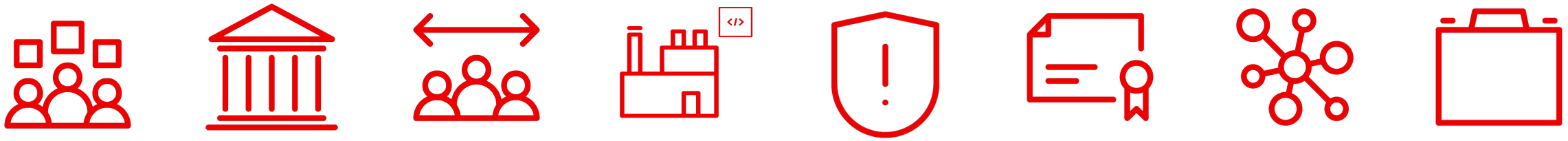
CEN CENELEC

THE “WHAT”

Red Hat CRA Program

Red Hat CRA Program Structure - 8 Workstreams

Awareness & Communications	Participation in EU Standards Development	Upstream Engagement & Contributions	Manufacturer & Steward Obligations	Vuln Mgmt / Incident Response Obligations	Conformity & Certification	Data Collection	Legal
Prepare internal and external CRA comms and training	Coordinate interactions with standardization bodies to provide Red Hat's expertise and advocate for open source	Coordinate interactions with foundations and upstream communities regarding CRA	Align the CRA with Red Hat's SDLC practices to ensure all requirements are understood	Ensure VM/IR policies and processes met CRA requirements and reporting obligations	Define the processes for Red Hat software to attest it has met the CRA requirements	Gather metrics to evaluate resourcing & investments for CRA	Support for other workstreams, develop internal CRA guidance, review deliverables



Requirements for Manufacturers at Glance

- Security by design and by default
- Risk management
- Data and communication protection
- Clear documentation, incl. security
- Vulnerability management
- Exploited/severe incident reporting (in 24h)
- Due Diligence for 3rd parties and SBOMs
- Disseminate security updates without delay
- Conformity and CE marking

- Risk management standards (ISO 27005 & ETSI TS 102 165-1), GRC
- SDLC frameworks (e.g., OWASP SAMM, NIST SSDF, C2C2F)
- Incident Response (IRP) and Coordinated Vulnerability Disclosure (CVD), ISO 30111 and 29147
- Access control, encryption, validation
- Secure defaults configs and user guidance on secure usage
- Generate and store SBOMs

free

5 Years - Support and Handle Vulnerabilities
10 Years - Documentation and Updates available

Not entirely new, but will lead to process and documentation adjustment.

Red Hat Stewardship Approach

- There is no “opt-in” or “opt-out” from being Steward
  - Looking forward for the Commission’s FOSS guidance to be published
- We developed a framework based on Steward definition criteria
  - Is the FOSS project a PDE?
  - Why this FOSS project is important for Red Hat?
  - How we support the project’s development and collaboration platforms?
  - How FOSS governance is structured?
  - Is there a better potential Steward?
- Selected projects* classified by Basic and Champion Stewardship categories

Red Hat’s key principle: understand community practices and governance rules for each project, offer targeted help where needed.

* The list is still under evaluation.

Requirements for Stewards at Glance

Basic

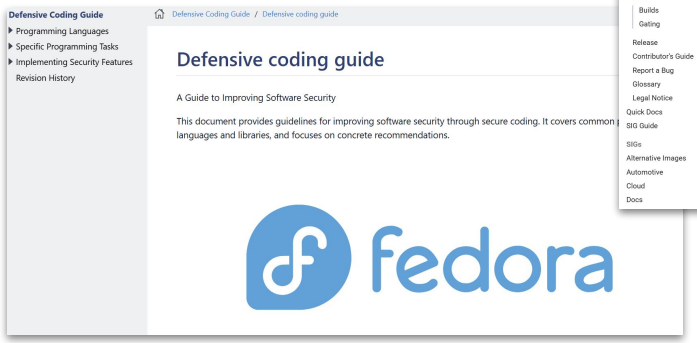
- Security Policy
- Vulnerability Management (CVD)
  - Actively Exploited
- Incident Response (IRP)
  - Severe Incidents
- Secure Development Practices
  - Dependency management, security scans, MFA, code reviews, etc.

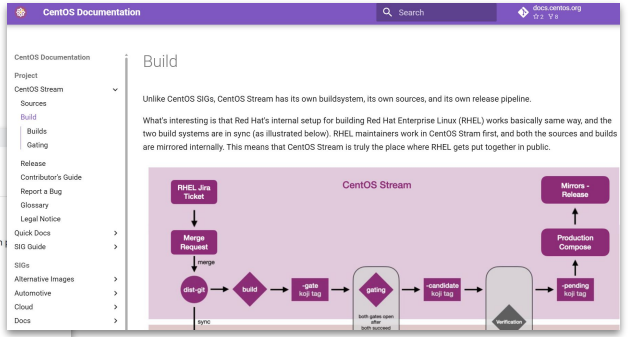
Champion

- SBOMs - generate and store
- Security Self-Assessment - in repo
- OpenSSF Baseline (OSPS) - L1
- OpenSSF Best Practices - Passing
- SLSA - L1

Cooperate with Market Surveillance Authorities, with CSIRTs and ENISA.

>70% are met*





* Preliminary quick analysis.

THE “WOW”

Challenges and Lessons Learned

Ambiguity – “commercial activity”, “actively exploited vulnerabilities”.

Unknowns – standards and implementing documents are work in progress.

41 standards (!) – just to maintain awareness is challenging.

Timeline – no gap between standards are completed and enforcement.

Alignment – affects all stakeholders, incl. Prod. Management, Procurement

How to Make CRA Even Better

> This goes **far beyond just CRA compliance**; it's a call for the entire open source ecosystem to unite, take action, and support one another. Regardless of your role as a **steward**, **manufacturer**, or **maintainer**, we invite you to join us!
>
> ...recognizing a collective responsibility [...] to evolve yesterday's often afterthought **security to default expectations**.
>
> Red Hat CRA Blog, 2025

https://www.redhat.com/en/blog/eu-cyber-resilience-acts-impact-open-source-security

BUILDING SECURE FUTURE. OPEN SOURCE WAY. FOR ALL.

LINKEDIN.COM/IN/ROZHUKOV

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat