THE LINUX FOUNDATION OPEN SOURCE SUMMIT JAPAN

AI_dev Open Source GenAI & ML Summit

AUTOMOTIVE LINUX SUMMIT

Cherry Blossom and Compliance

A Intro to the EU CRA

Mike Bursell &
Chris “CRob” Robinson

“Cherry Blossom and Crayfish”

“Cherry Blossom and Crayfish”

With apologies to:

- Katsushika Hokusai

- Lovers of art
- Lovers of poetry

CRAfish swims
Deep in the CRA, yay!
Cyber-bliss for all

Agenda

- What is the CRA?
- What products are covered by the CRA?
- What responsibilities do I have under the CRA?
- When does the CRA start to apply?
- What types of compliance are there?
- How is open source special under the CRA?

Disclaimer / Weasel Words

Neither Mike nor CRob is a lawyer.

Mike and CRob are certainly not YOUR lawyers.

These are thoughts, feelings, and insights from Mike’s and CRob’s careers; consult YOUR attorney to understand what YOU and YOUR Org need to be doing.

Created by Neon Banana with the prompt “create a square image of a weasel who is a lawyer in the style of a 19th century Japanese woodcut”

What is the CRA?

The Cyber Resilience Act ("CRA")

- Effective Dec 2024; duties apply Dec 2027
- Covers "Products with digital elements" (PDE)
- CE marking now includes cybersecurity assurance
- Secure-by-design, vulnerability handling, and post-market duties

Created by Neon Banana with the prompt "create a square image of a worried looking goose facing a samurai with the words "EU Cyber Resilience Act" on his chest, all in the style of a 19th century Japanese woodcut"

The CRA - a positive thing

As cyber-security professionals and practitioners,

this is what we’ve been requesting for decades!

Secure-by-Design

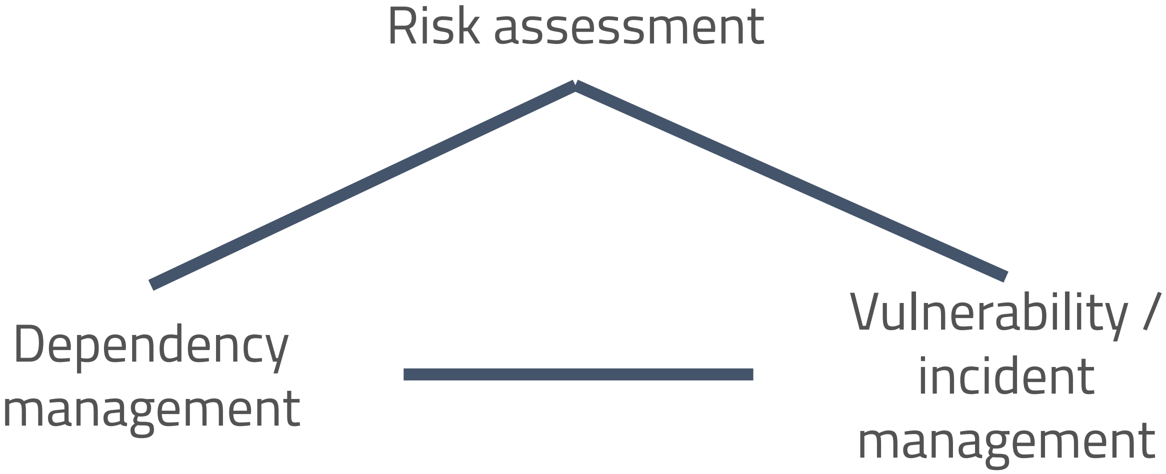
Software Bill of Materials (SBOM)

Vulnerability Coordination and Disclosure

Secure-by-Default

Risk Management

Main points



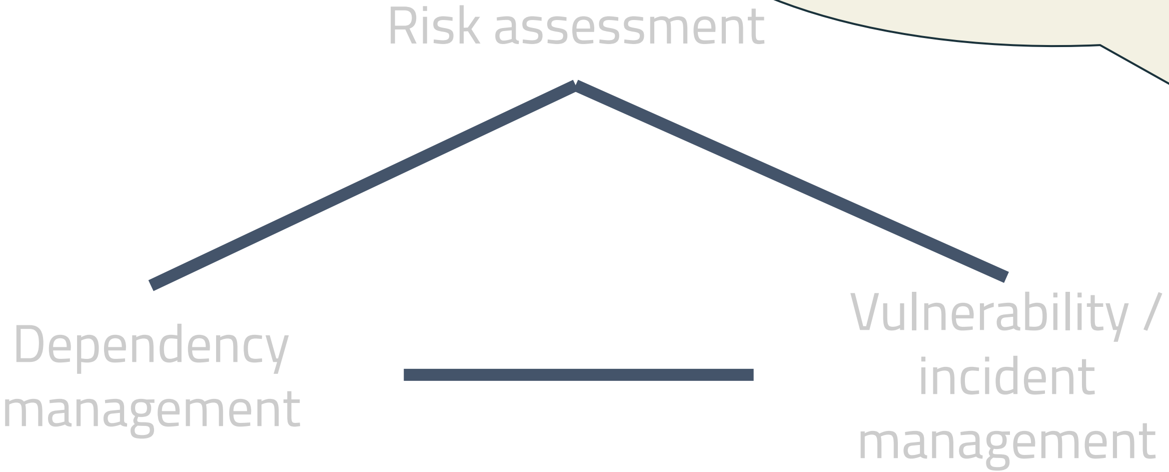
Risk assessment

Dependency management

Vulnerability / incident management

Main points

But, CRob, aren't companies doing this already?



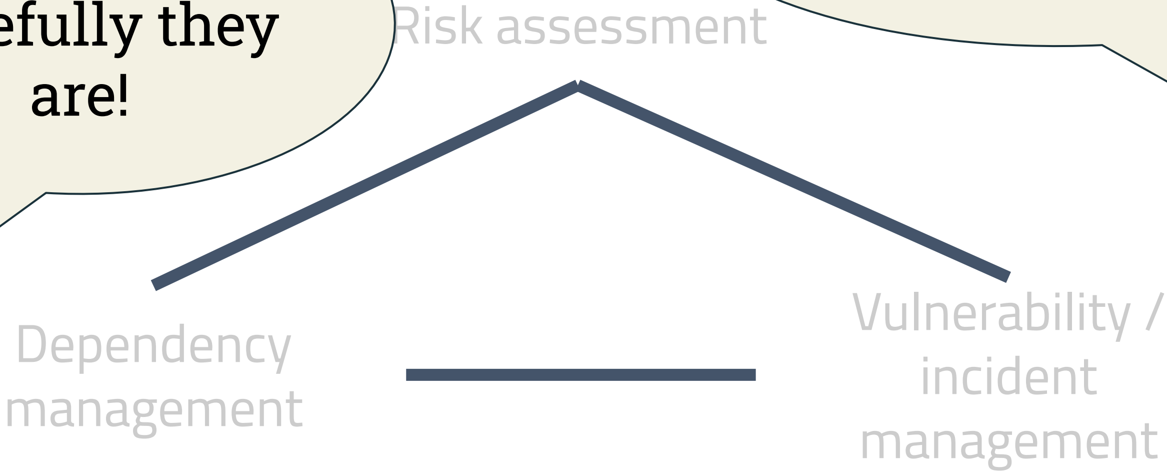
Risk assessment

Dependency management

Vulnerability / incident management

Main points

Well, Mike, hopefully they are!


Risk assessment
Dependency management
Vulnerability / incident management

But, CRob, aren't companies doing this already?

Penalties

Article 64 lays out the framework for Penalties of non-compliance….

Emphasis *added*

Penalties

Article 64 lays out the framework for Penalties of non-compliance….

***Emphasis** added*

2. Non-compliance with the **essential cybersecurity requirements** set out in Annex I and the obligations set out in Articles 13 and 14 *shall be subject to administrative fines of up to EUR 15 000 000 or, if the offender is an undertaking, up to 2,5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher*.

3. Non-compliance with the obligations set out in Articles 18 to 23, Article 28, Article 30(1) to (4), Article 31(1) to (4), Article 32(1), (2) and (3), Article 33(5), and Articles 39, 41, 47, 49 and 53 *shall be subject to administrative fines of up to EUR 10 000 000 or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher*.

4. **The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities** in reply to a request *shall be subject to administrative fines of up to EUR 5 000 000 or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.*

Penalties

Article 64 lays out the framework for Penalties of non-compliance….

Emphasis added

2. Non-compliance with the **essential cybersecurity requirements** set out in Annex I and the obligations set out in Articles 13 and 14 *shall be subject to administrative fines of up to EUR 15 000 000 or, if the offender is an undertaking, up to 2,5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher*.

3. Non-compliance with the obligations set out in Articles 18 to 23, Article 28, Article 30(1) to (4), Article 31(1) to (4), Article 32(1), (2) and (3), Article 33(5), and Articles 39, 41, 47, 49 and 53 *shall be subject to administrative fines of up to EUR 10 000 000 or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher*.

4. **The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities** in reply to a request *shall be subject to administrative fines of up to EUR 5 000 000 or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.*

What products?

What products?

What products?

- Cybersecurity for “Products with Digital Elements"
  - “PDEs” in the EU
    - hardware and software
    - for businesses and consumers
    - Various “classes”, inc. important, critical

What products?

- Cybersecurity for “Products with Digital Elements”
    - “PDEs” in the EU
        - hardware and software
        - for businesses and consumers
        - Various “classes”, inc. important, critical
    - Not services (except where required by PDE)

What products?

- Cybersecurity for “Products with Digital Elements”
  - “PDEs” in the EU
    - hardware and software
    - for businesses and consumers
    - Various “classes”, inc. important, critical
  - Not services (except where required by PDE)
  - Some sectors have existing legislation (e.g. aviation, medical, automotive) that supersede or are superseded by the CRA

Product categories

Different requirements for different categories.

Product categories

- Default
- Important
  - Class I
  - Class II
- Critical

Product categories

- Default
- Important
    - Class I
    - Class II
- Critical → HSMs, smart meter gateways, smartcards, ...

Product categories

- Default
- Important
  - Class I
  - Class II → Hypervisors, firewalls, ...
- Critical → HSMs, smart meter gateways, smartcards, ...

Product categories

- Default
- Important
  - Class I → IDMs, boot managers, smart locks, OSes, ...
  - Class II → Hypervisors, firewalls, ...
- Critical → HSMs, smart meter gateways, smartcards, ...

Product categories

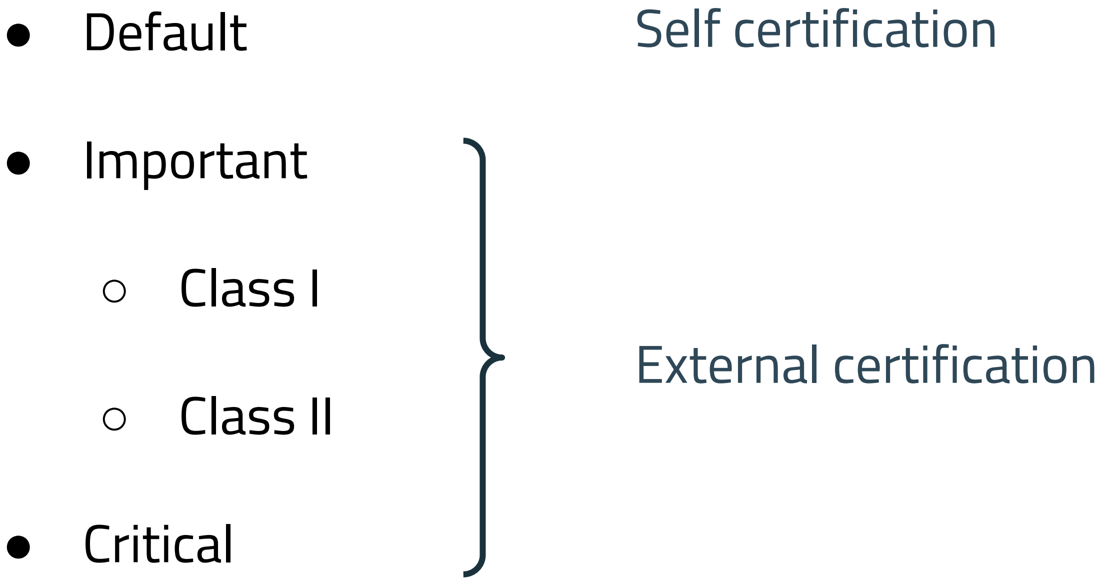
- Default → Most products
- Important
  - Class I → IDMs, boot managers, smart locks, OSes, ...
  - Class II → Hypervisors, firewalls, ...
- Critical → HSMs, smart meter gateways, smartcards, ...

Product categories

- Default ⟹ Most products
- Important
  - Class I ⟹ IDMs, boot managers, smart locks, OSes, ...
  - Class II ⟹ Hypervisors, firewalls, ...
- Critical ⟹ HSMs, smart meter gateways, smartcards, ...

Types of compliance?

Product categories



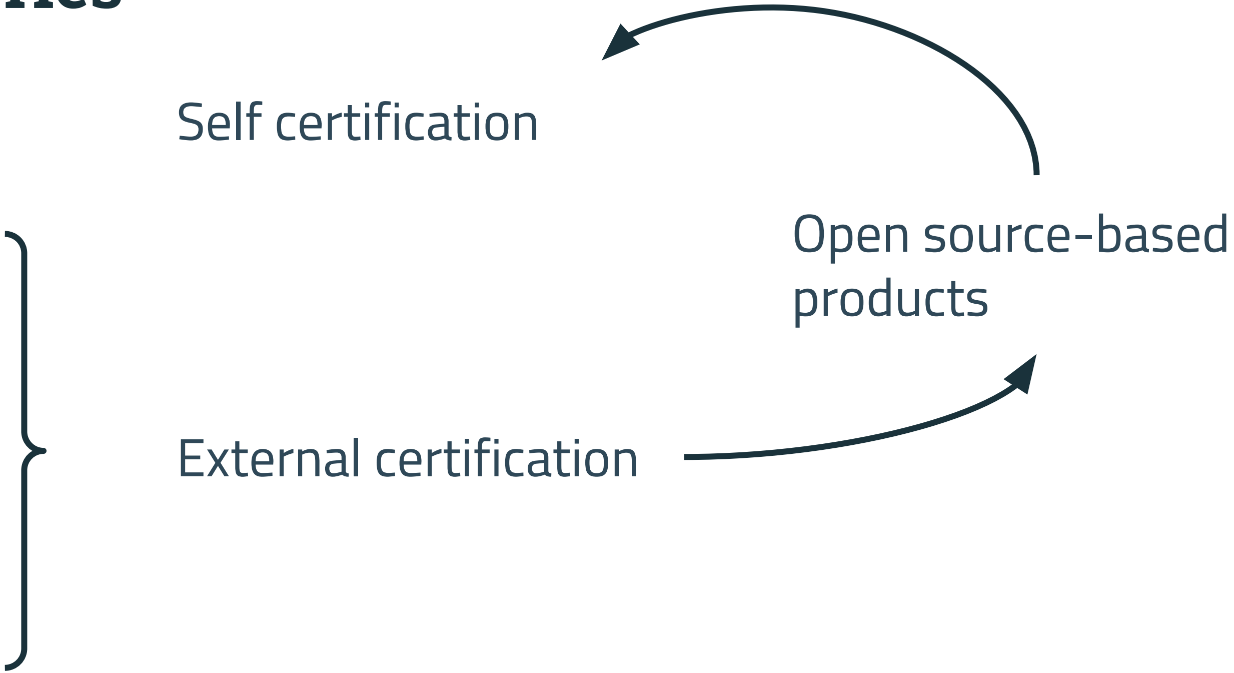
- Default
- Important
    - Class I
    - Class II
- Critical

Self certification

External certification

Product categories

- Default
- Important
  - Class I
  - Class II
- Critical



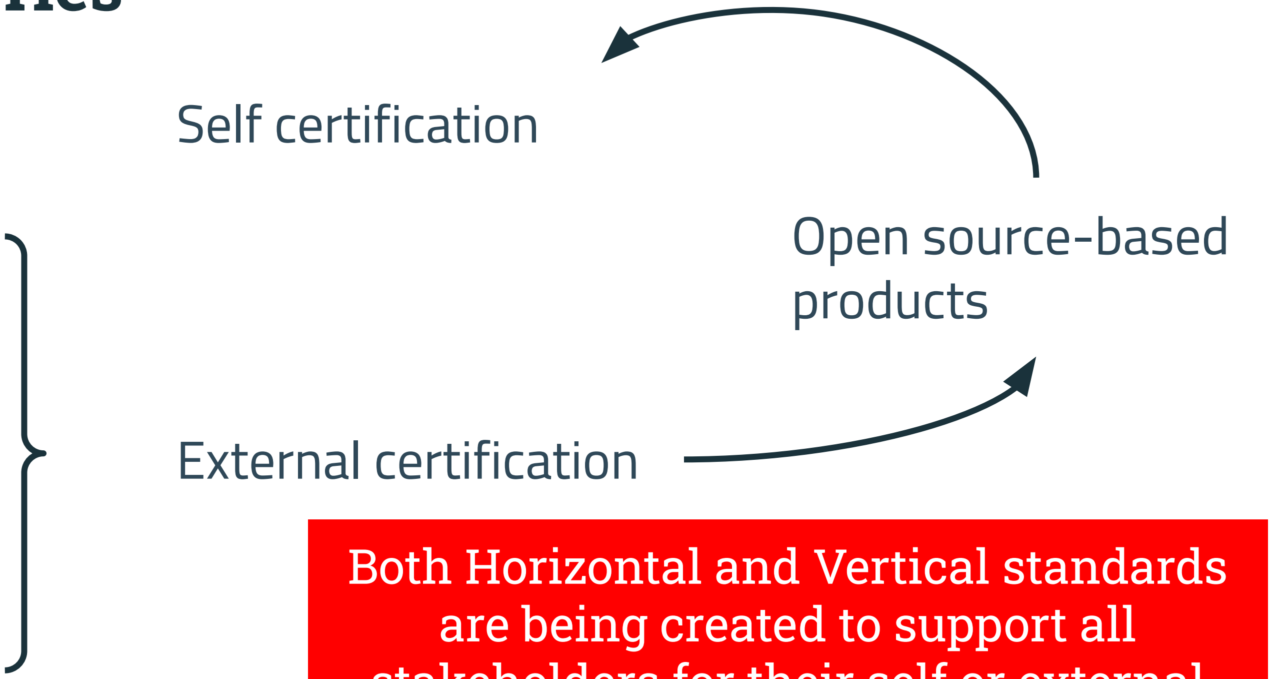
Self certification

Open source-based products

External certification

Product categories

- Default
- Important
  - Class I
  - Class II
- Critical



Self certification

Open source-based products

External certification

Both Horizontal and Vertical standards are being created to support all stakeholders for their self or external certification programs

What responsibilities?

Who am I?

- Manufacturer
- Open source steward
- Maintainer/contributor

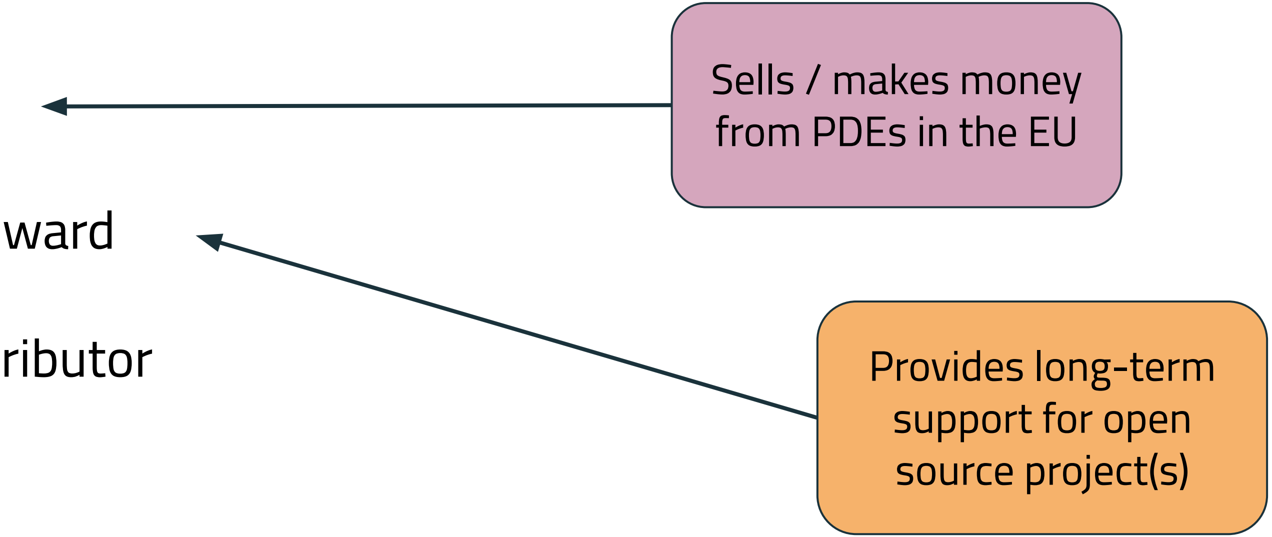
Who am I?

- Manufacturer
- Open source steward
- Maintainer/contributor

Sells / makes money from PDEs in the EU

Who am I?

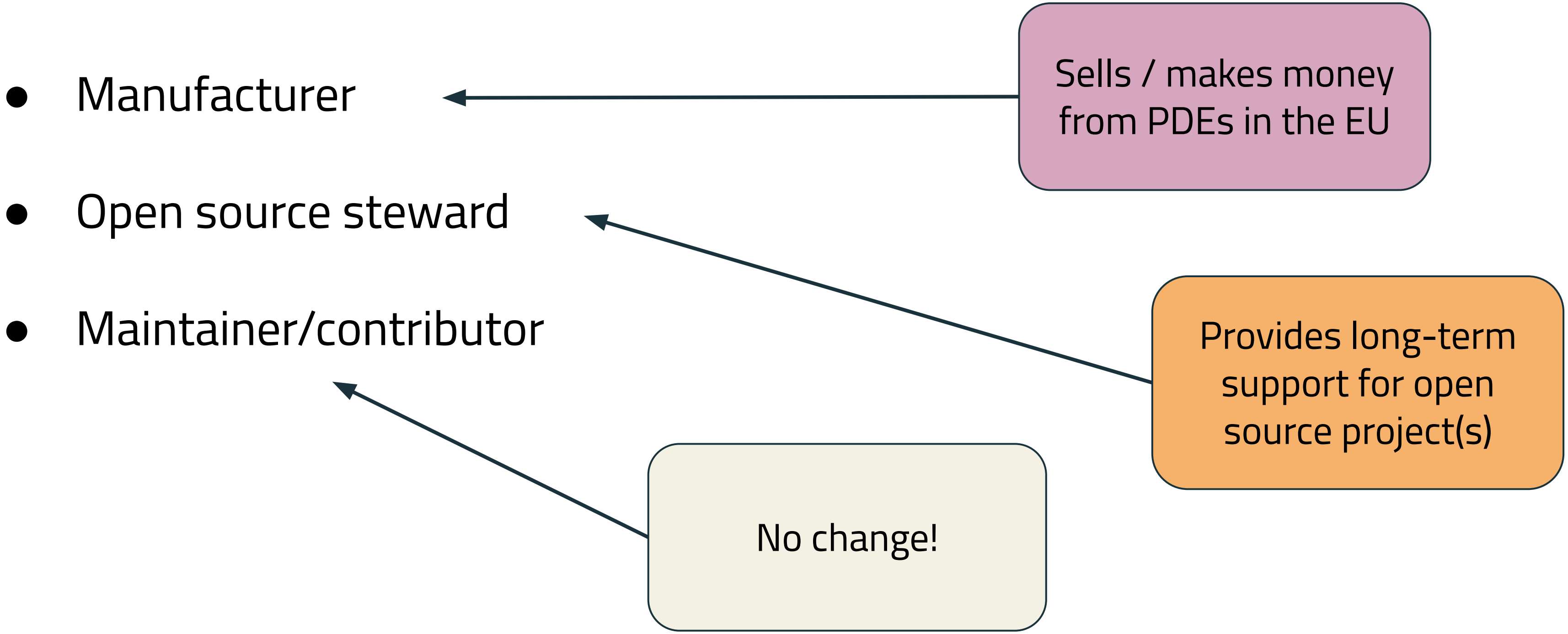
- Manufacturer
- Open source steward
- Maintainer/contributor



Sells / makes money from PDEs in the EU

Provides long-term support for open source project(s)

Who am I?



- Manufacturer
- Open source steward
- Maintainer/contributor

Sells / makes money from PDEs in the EU

Provides long-term support for open source project(s)

No change!

Who am I?

- Manufacturer
- Open source steward
- Maintainer/contributor

Conformance
Vulnerability reporting
Incident reporting

Few obligations
(Support and reporting)

project(s)

No change!

When?

What, when?

- CRA entered into force **11Dec 2024**
  - The text of the law is locked in, standardization process for assumption of conformity and other areas begins
- Reporting obligations are enforced **11Sept 2026**
  - Manufacturers and Stewards need to report known exploited vulnerabilities and “severe incidents” to ENISA and a Nation CSIRT through the forthcoming Single Reporting Platform (SRP)
- Law will be fully enforced **11Dec 2027**
  - All parties must meet the requirements in Annex 1 and the Articles and products should have their CE Mark approvals

CRA Reporting Clock

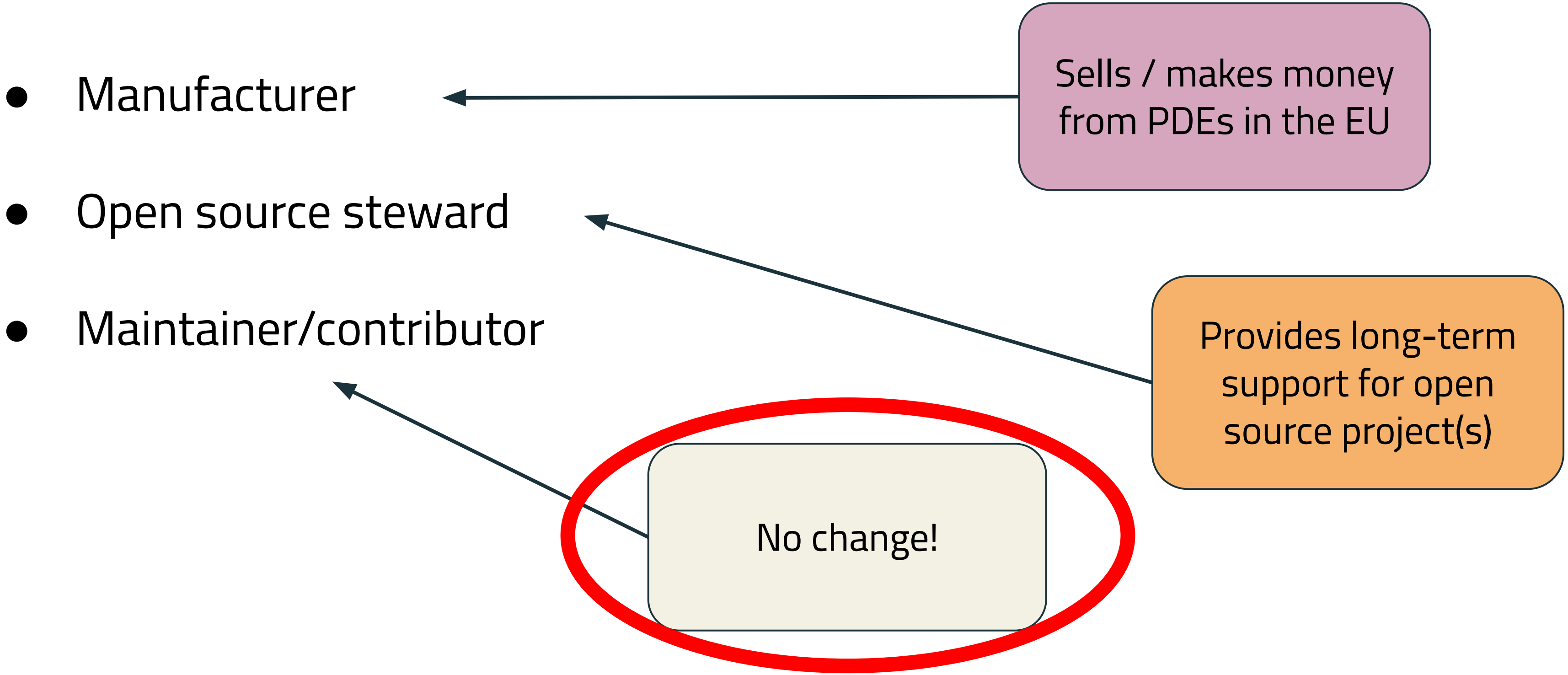
Severe Incidents and Exploited Vulnerabilities

24h – Early Warning to CSIRT/ENISA
72h – Incident/Vulnerability notification
1 Month – Final report

Created by Neon Banana with the prompt “Create an image of a worried looking goose next to a large hourglass with "CRA reporting timelines" on the top and with a crayfish in the bottom, all in the style of a 19th-century woodcut ”

Open source?

Who am I?



- Manufacturer
- Open source steward
- Maintainer/contributor

Sells / makes money from PDEs in the EU

Provides long-term support for open source project(s)

No change!

Getting a steward for your project, baseline…

- Open Source Stewards can assist in some of this work.
- Not every OSS project has or needs a steward, but EVERY COMPONENT of EVERY PDE MUST be able to be updated as exploited vulnerabilities are discovered.
- The Open Source Project Security Baseline (OSPS Baseline) is a great way to discover the security practices of upstream projects to either uses as a downstream check prior to ingestion into a product or as a “wish list” to go contribute upstream to the projects YOU find critical to YOUR portfolio.

How to get more information

- The Text of the CRA
  - https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Articles.html
- OpenSSF's Global Cyber Policy working group
  - Github - https://github.com/ossf/wg-globalcyberpolicy
  - Slack - https://openssf.slack.com/archives/C084A6XPX0F
  - Mailing List -https://lists.openssf.org/g/openssf-wg-globalcyberpolicy
  - CRA Brief Guide for OSS Developers - https://best.openssf.org/CRA-Brief-Guide-for-OSS-Developers
  - LFEL1001 Understanding the EU CRA free course - https://training.linuxfoundation.org/express-learning/understanding-the-eu-cyber-resilience-act-cra-lfel1001/
- OpenSSF Open Source Project Security Baseline
  - OSPS Baseline SIG - https://baseline.openssf.org/
  - ORBIT Working Group (tooling, templates, & automation) - https://github.com/ossf/wg-orbit
- There are many other groups collaborating around this legislation
  - OFE, Eclipse, and other open source communities have developed guidance for their communities and the general public too

CRA 101

Free educational course covering the CRA

Available NOW!

Additional courses are planned, including how to conduct Risk Assessments throughout the development and productization lifecycle

Understanding the European Union (EU) Cyber Resilience Act (CRA) (LFEL1001)

reserved. The Linux Foundation has registered trademarks and uses trademarks.

Created by Neon Banana with the prompt "Create an image of a goose as a student, studying hard in a classroom in the style of a 19th-century Japanese woodcut "

Cyber-process strong,
Protected by design now
Thank you, CRA

Image Source “Godzilla Great Wave Wall” poster

Arigatou gozaimasu (ありがとうございます)

✉ mike_at_p2pconsulting.dev

https://github.com/MikeCamel

▶ What is CyberSecurity?

in https://www.linkedin.com/in/mikebursell/

✉ CRob_at_OpenSSF_dot_org

@~~SecurityCRob~~

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

▶ The Security Unhappy Hour,
Chips & Salsa
What's in the SOSS?

in https://www.linkedin.com/in/darthcrob/