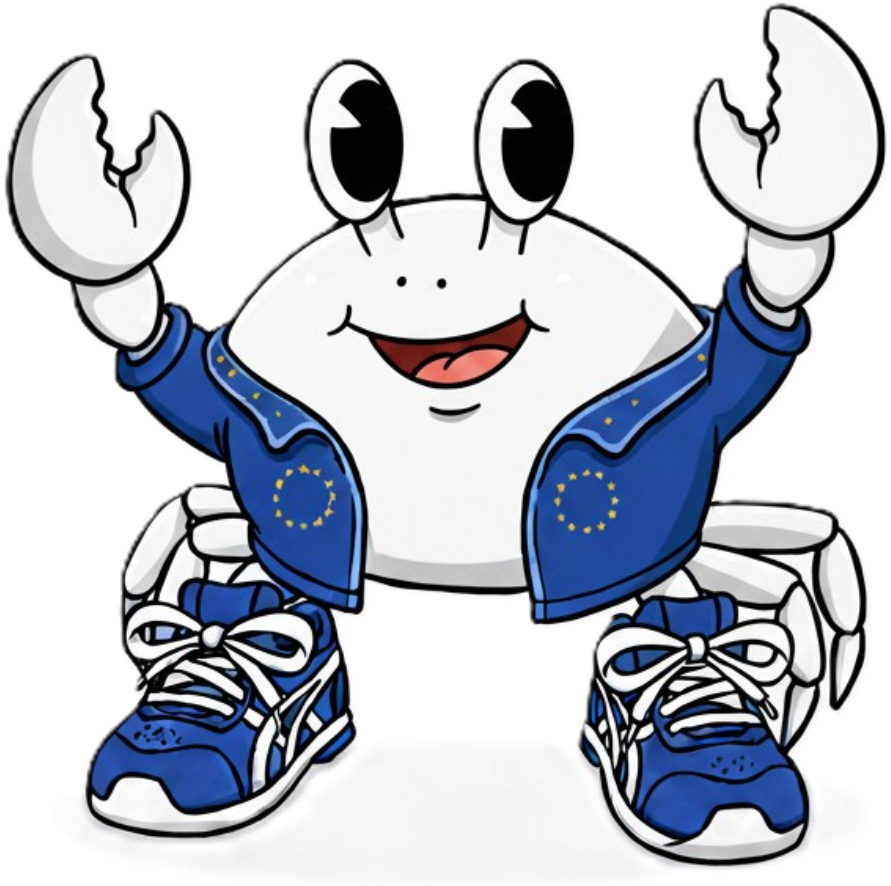
Introduction to CRA Compliance

CRABasics.com



RS Strategy

cetome
we make cyber work

Who are we?

2 people who buy a lot of IoT products and have spent some time on vulnerability management



Rayna STAMBOLIYSKA

- Strategic advisory to tech & cyber companies
- Compliance (NIS2, CRA, RED, GDPR, Data Act)
- Working on CVD and vuln treatment since 2016 (incl. with OECD)
- Fun fact: I have audited most connected se*toys on the EU market



Cédric LEVY-BENCHETON

- Strategic advisory to IoT manufacturers
- Compliance with regulations (RED, CRA)
- Daily use of international standards
- Fun fact: I have over 80 IoT devices at home

RS Strategy

cetome
we make cyber work

Introducing CRA Basics

CRABasics.com



Cyber Resilience Act Compliance Simplified

- Easy-to-understand guidance
- Free practical resources
- CRA maturity evaluation tool
- And more to come…

RS Strategy

cetome
we make cyber work

What we'll talk about today

1. **Introduction to the CRA**
2. **Achieving compliance**
3. **Conclusion**

I.

INTRODUCTION TO THE CRA



Official Journal
of the European Union

EN
L series

2024/2847

20.11.2024

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 October 2024

on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

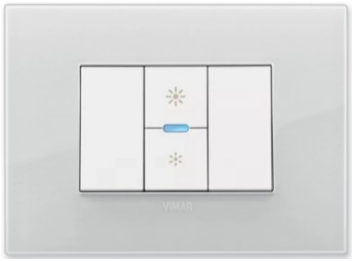
(Text with EEA relevance)

An increase of cyber attacks

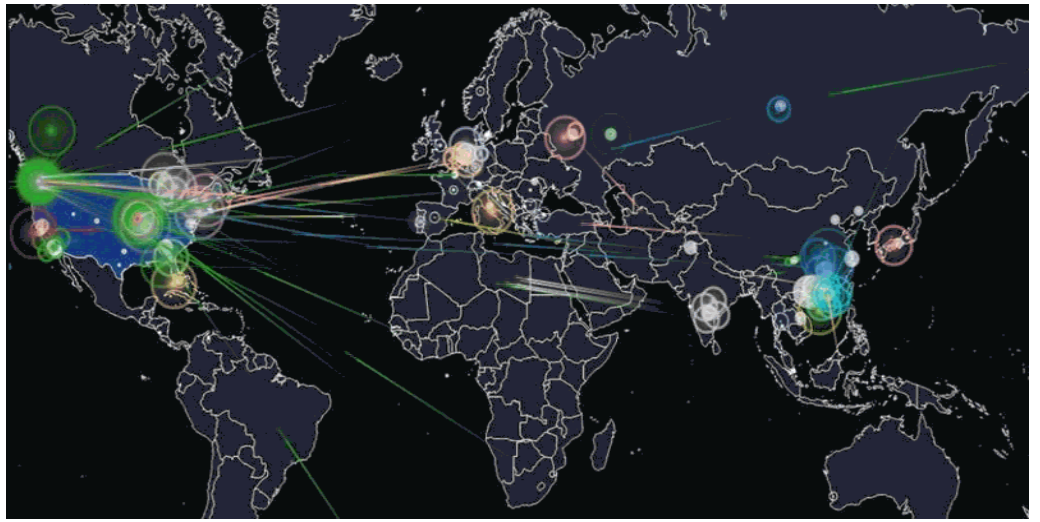
Massive IoT Botnet dismantled with 75% of infected devices located in North America and Europe.
Source: FBI – 18th September 2024



Dray:Break – 14 new vulnerabilities in DrayTek routers can be exploited to fully compromise devices
Source: Forescout – 2nd October 2024



A botnet began targeting zero-day and recently fixed vulnerabilities to infect more than over 15,000 industrial and smart home devices.
Source: Ars Technica – 22 January 2025



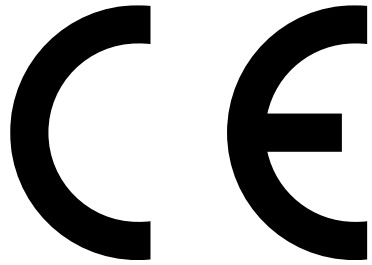
RS Strategy

cetome
we make cyber work

Introducing the Cyber Resilience Act (CRA)

EU regulation for "products with digital elements" (PDE)

- 23 Essential Requirements, including 8 on vulnerability management
- For the entire lifecycle of products in scope, and beyond (*at least 5 years!*)
- PDE are treated as products for compliance purposes = concrete technical obligations.



What is a secure PDE?

- No known exploitable vulnerability at the time of market release
- Secure configuration by default
- New vulnerabilities and cyber incidents are addressed for the entire product lifecycle

RS Strategy

cetome
we make cyber work

Requirements of the CRA for product manufacturers

Risk-based product development

- Start with a cyber risk assessment based on the context of use
- Identify appropriate cyber security requirements to mitigate these risks
- Document these cyber risks and update them as appropriate

These requirements are formalised in Annex I

Part I Cybersecurity requirements relating to the properties of products with digital elements

(1) Secure product development lifecycle *1 req.*
(2) Technical requirements *13 requirements*

Part II Vulnerability handling requirements

8 requirements

Cyber security requirements

- Cryptography and access control to protect data
- Secure boot and anti-tampering to protect product integrity
- Input filtering, no hardcoded secrets, unused interfaces disabled by default to reduce the attack surface
- Resilience and degraded mode to protect from cyberattacks including DDoS
- Software Bill of Materials (SBOM)
- Coordinated vulnerability disclosure policy with a single point of contact
- Regularly check for new vulnerabilities and provide security updates (for 5 years)
- Monitor and manage cyber incident
- Inform regulators and customers about important cyber security issues

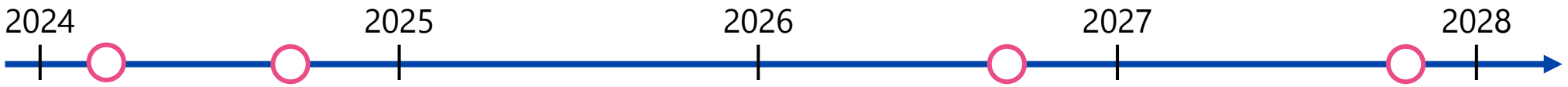
Market access

- Declaration of conformity
- Information to customers about the product and the manufacturer: product identification, manufacturer website, etc.
- Keep these documents for 10 years

Timelines and Penalties

Penalties for non-compliance

- Fines up to **15 millions €** or **2,5 %** of the total worldwide annual turnover
- Risk of product withdrawal or recall (costs supported by the manufacturer!)



12 March 2024
Vote at the EU Parliament

10 October 2024
Entry into Force (EIF)

11 September 2026
21 months after EIF

Reporting obligations for actively exploited vulnerabilities and severe incidents

11 December 2027
36 months after EIF

All requirements applicable

RS Strategy

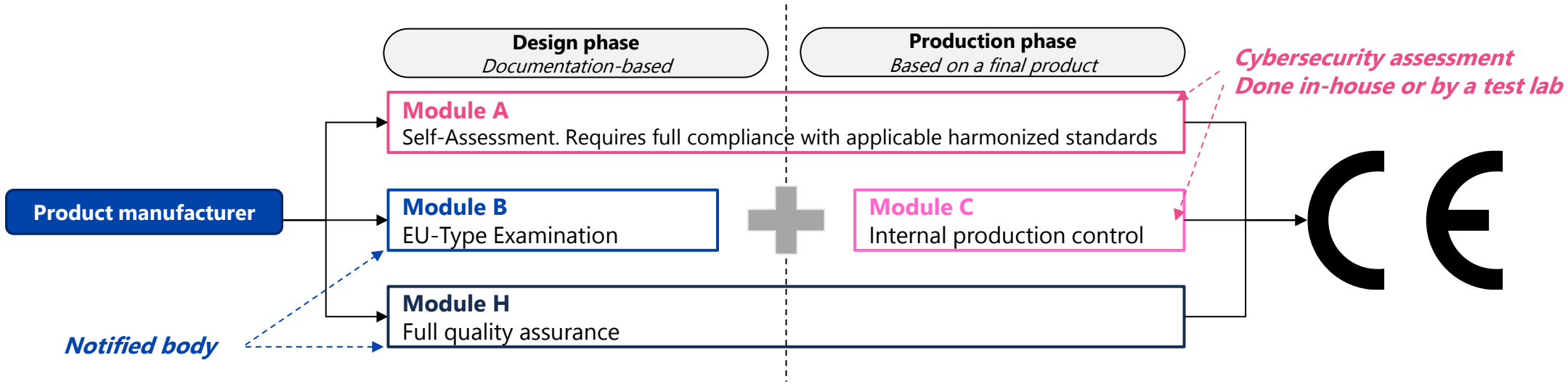
cetome
we make cyber work

Obtaining the CE label

EU Declaration of Conformity (self-assessment) or EU-Type certificate (via Notified Body)

- Signed document presenting all legal requirements applicable to the products, and how compliance is managed by the manufacturer.
- It must be publicly available (online and/or shipped with the product)

The CRA offers several possibilities to demonstrate compliance:



RS Strategy

cetome
we make cyber work

Product categories

Important products

Default **Most products with a digital element**

- **Products in the default category:** Smart TVs, connected thermostats, smart lightbulbs, and more
- **Recent attack:** attackers can bypass authentication on 91,000 LG smart TVs to gain root access



Class I **Products causing important health, security or safety risks**

- **Products in class I:** Smart door locks, baby monitoring systems, alarm systems, connected toys, personal wearable health technology, and more (see Annex III)
- **Recent attack:** Ring's privacy failures led to spying and harassment through home security cameras



Class II **Products with greater risks, greater negative impacts than products in Class I**

- **Products in class II:** Firewalls, tamper-resistant MCU, network interfaces
- **Recent attack:** vulnerabilities in Qualcomm mobile firmware can lead to memory corruption



Critical **Products causing significant risk of disruption OR critical dependencies to NIS 2 essential entities**

- **Critical products:** Hardware Devices with Security Boxes, Smart meter gateways within smart metering systems, Smartcards or similar devices, including secure elements.
- **Recent attack:** unpatchable vulnerability in Apple chip leaks secret encryption keys (gofetch.fail)



RS Strategy

cetome
we make cyber work

CRA Assurance requirements

Recommended assurance level
Possible to use
Not allowed by CRA: insufficient assurance level

	Default	Class I	Class II	Critical
Basic self-assessment ▪ The manufacturer verifies its own conformity against any appropriate standard ▪ Example: the manufacturer verifies that the product implements EN 303 645 requirements	✓	✗	✗	✗
Self-assessment with the CRA harmonized European Standard (hEN) ▪ Identical to basic self-assessment but with a standard developed specifically for the CRA ▪ Example: the manufacturer ensures that the product aligned with the CRA hEN	○	✓	✗	✗
Conformity assessment validated by a Notified Body ▪ The manufacturer submits its self-assessment and other documents to a Notified Body ▪ The Notified Body verifies them and gives its conclusions ▪ Example: submit EN 303 645 ICS, IXIT and mandatory documentation to a Notified Body	○	✓	✗	✗
3rd-party assessment ▪ Use an accredited "conformity assessment body" to test the product for security ▪ Example: a manufacturer procures a security audit of its product (device, backend, etc.)	○	○	✓	○
EU certification scheme ▪ Implement an existing EU certification scheme (Cyber Security Act): EUCC, EUCS, EU5G, etc. ▪ Example: a smart metering gateway manufacturer implements EUCC	○	○	○	✓

Mandatory if Delegated Act published

RS Strategy

cetome
we make cyber work

Challenges for manufacturers in scope

Technical

- Diversity of products
- Resource constraints
- Visibility and inventory management
- Vulnerability detection and assessment
- Patch management and deployment/secure update mechanism
- SBOM creation and maintenance
- Lack of harmonised standards to date

Organisational / Business

- Awareness and familiarity with CRA requirements
- High initial investment and difficult-to-grasp ROI
- CVD consumption, timely incident and vulnerability reporting and treatment
- Vendor dependency and supply chain risks
- Scalability and maintenance

2.

Achieving compliance

Analysis Product security requirements in the CRA

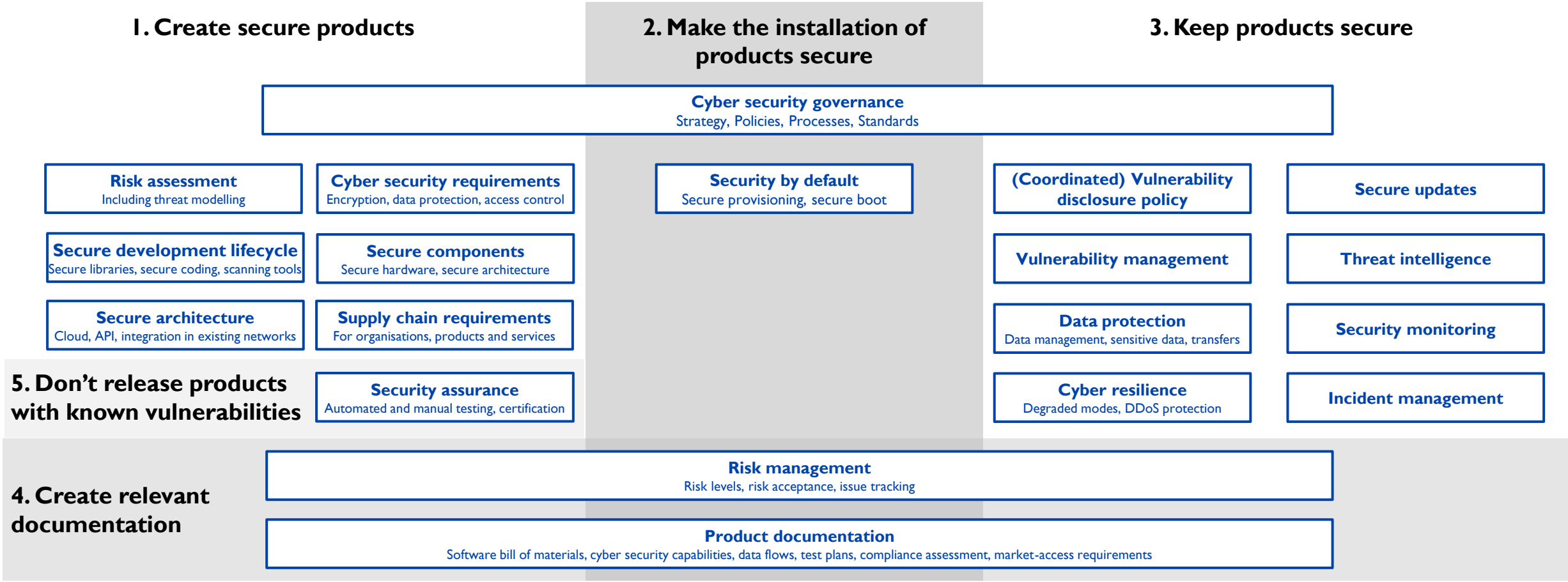
The Cyber Resilience Act has 5 high-level requirements :

1. Create secure products
2. Make the installation of products secure
3. Keep products secure once on the market
4. Produce relevant documentation at all stages
5. Don’t release products with known security issues

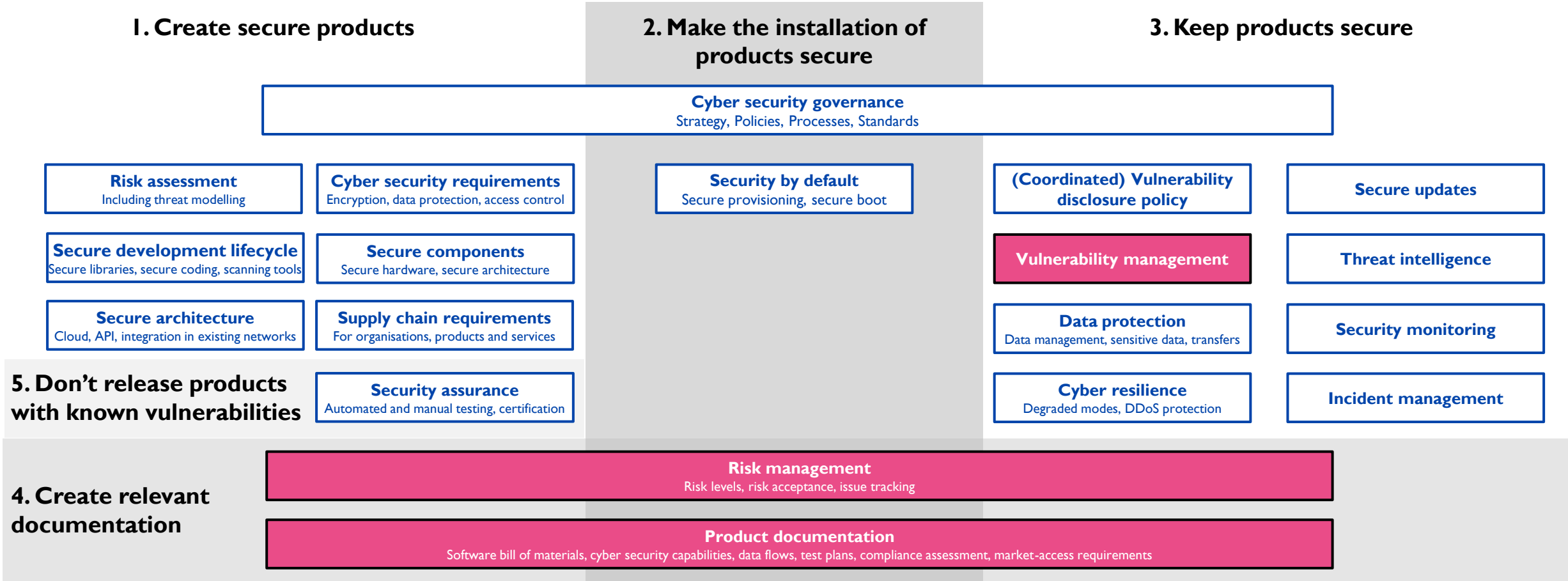
RS Strategy

cetome we make cyber work

Analysis Product security requirements in the CRA



Analysis Product security requirements in the CRA



Top 3 priorities for achieving compliance in 2026

1. Implement vulnerability management

Keep up-to-date with the latest vulnerabilities to ensure your product remains secure throughout its lifecycle.

2. Create an HBOM / SBOM to secure your supply chain

Identify all third-party components and software you use, and formalise your Hardware / Software Bill of Materials.

3. Manage risks related to exploitable vulnerabilities and incidents

Define and implement processes with clear roles, responsibilities and SLAs to identify, assess and remediate risks to the product.

Compliance roadmap

Compare your current practices and evaluate your maturity against CRA requirements.

Execute the plan, integrating security processes into your development lifecycle.



Develop a detailed plan to address identified gaps, including budget and timeline.

Establish a system for continuous monitoring, documentation, and reporting to maintain compliance.

Evaluate your maturity on CRABasics.com



CRA Maturity Evaluation

Evaluate your current maturity level and identify areas for improvement. This is a first step towards compliance.

Product Cybersecurity Questionnaire

1. Are product cyber security risks evaluated? — No / Yes

2. Is there a list of cyber security requirements implemented in the product? — No / Yes

3. For how long will the product receive security updates? *support period* — 1-3 years

4. Is there a public-facing Vulnerability Disclosure Policy? — No / Yes

Enter the URL of your VDP

https://example.com/vdp

5. Do you produce an SBOM? — No / Yes

Do you use the SBOM for vulnerability management? — No / Yes

6. Who manages vulnerabilities in the product?

Lead developer

Results

Score: 44/100.

Risk Management
You can use the results of your risk assessment to select appropriate cyber security requirements.

Support Period
You must demonstrate why your support period is shorter than 5 years.

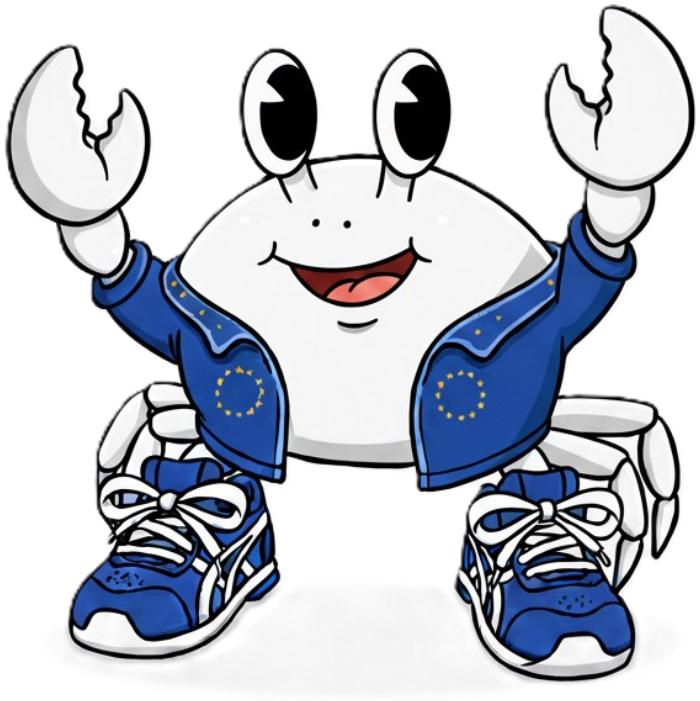
Vulnerability Management
You should set up a public-facing vulnerability disclosure policy. We recommend placing the link in your website's footer.

You should enhance the information in your SBOM by relying on public vulnerability databases (VEX). This will help your vulnerability management by evaluating whether they are exploitable or not in your product.

Lead developer is in charge of vulnerability management. Make sure that this person has time to carry out their responsibility, and that they are supported by their colleagues when necessary.

3.

CONCLUSION



Conclusions



IoT manufacturers should prepare for CRA compliance

- Focus on priorities: vulnerability management, SBOM, risk management
- Evaluate maturity against CRA requirements
- DO NOT wait for September 2026

CRABasics.com

- Learn about guidance
- Free practical resources
- And more to come…
- **Get your free roadmap now!**

Thank you!

Get concrete guidance with CRA Basics

CRABasics.com