The Cyber Resilience Act

Beyond Buzzwords!

Dr. Cédric LEVY-BENCHETON (cetome)
Attila SZÁSZ (BugProve)

BUGPROVE

cetome
we make cyber work

1. Introduction to the CRA

2. Product security in the CRA

3. How to secure products?

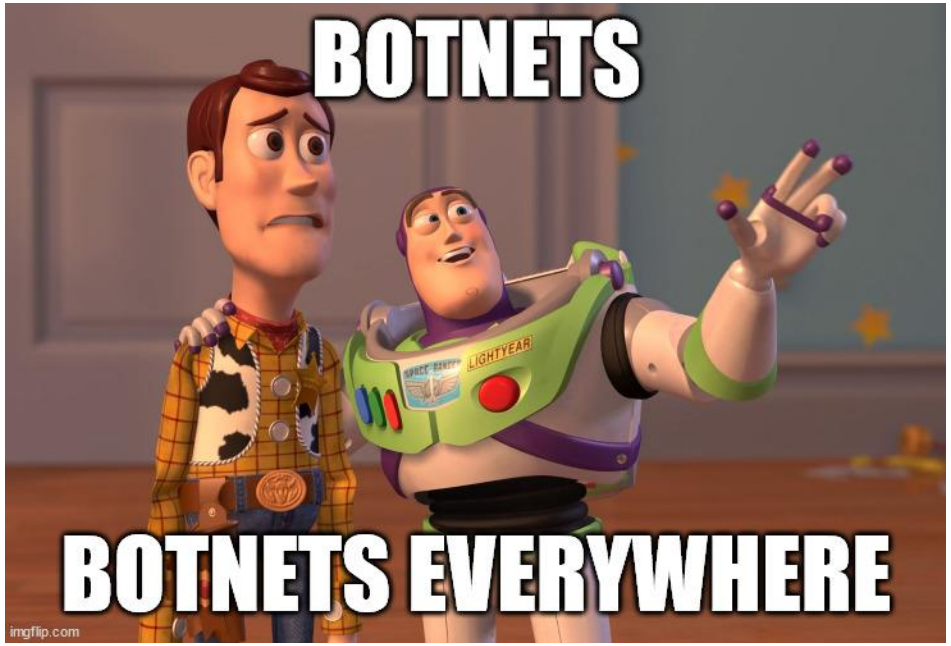
4. Conclusions

BUGPROVE

cetome
we make cyber work

1. Introduction to the CRA

Why do we need IoT cyber security regulations?



TheMoon creates a botnet of IoT devices of ~7,000 new users per week
Source: Lumen Technologies / March 2024

Thousands of video doorbells sold on online marketplaces can be accessed by anyone from the Internet
Source: Consumer Reports / March 2024

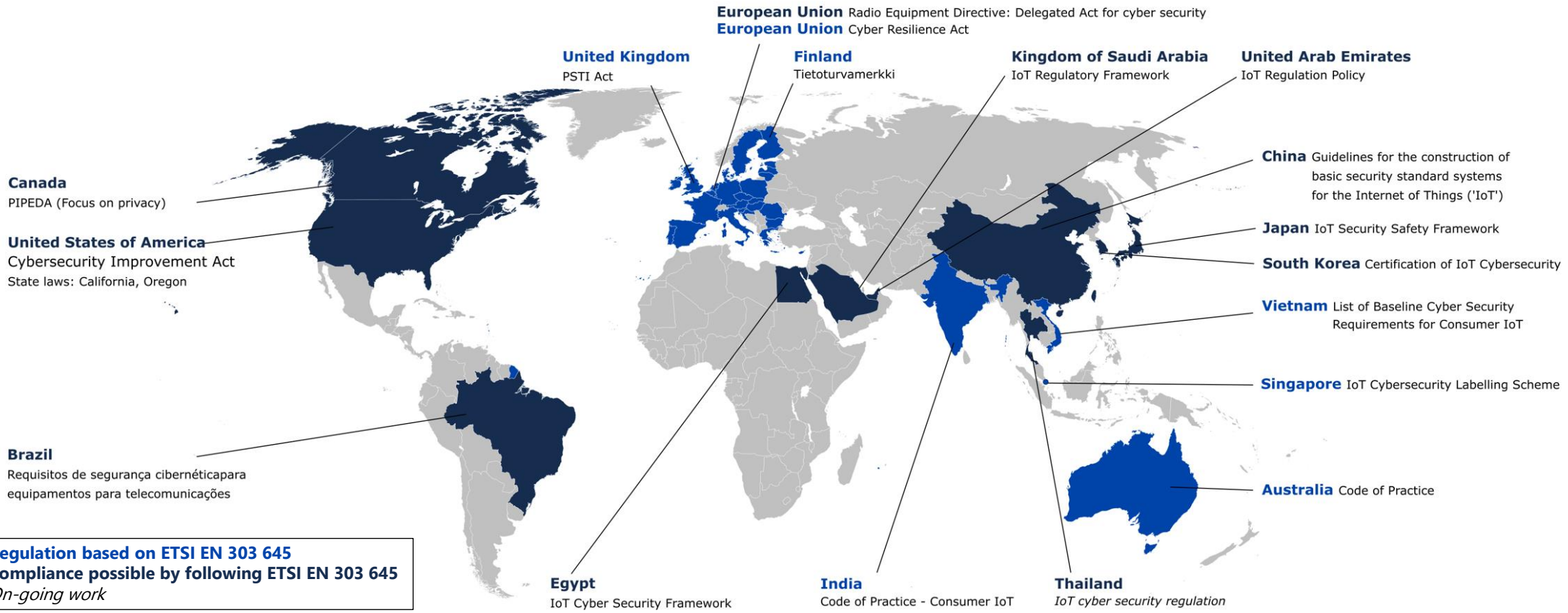
New flaws in TPM 2.0 library allow out-of-bound read/write posing threat to billions of IoT Devices
Source: Quarkslab / March 2023

Panorama of IoT Cyber Security Regulations

#IoTPanorama

cetome.com/panorama

#IoTRegulations



The CRA introduces mutual recognition

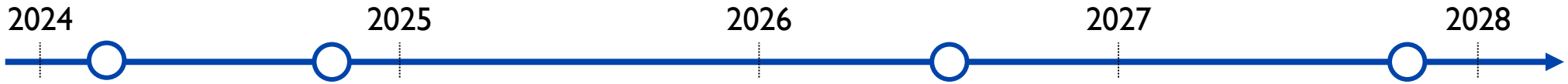
Introducing the Cyber Resilience Act (CRA)

The first worldwide regulation to impose cyber security requirements to products with a "digital element"

- Obligations for manufacturers, importers, distributors ("economical operators")
- For the entire lifecycle of products in scope, and beyond (10 years!)
- With a mix of governance and technical requirements
- That are appropriate to the level of cyber risks

CE

Timeline for IoT product manufacturers (estimate)



12 March 2024
Vote at the EU Parliament

Q3/Q4 2024
Entry into Force

June-August 2026
Reporting obligations for actively exploited vulnerabilities and severe incidents

Q3/Q4 2027
All mandatory requirements

Real-world Cyber Risk Example

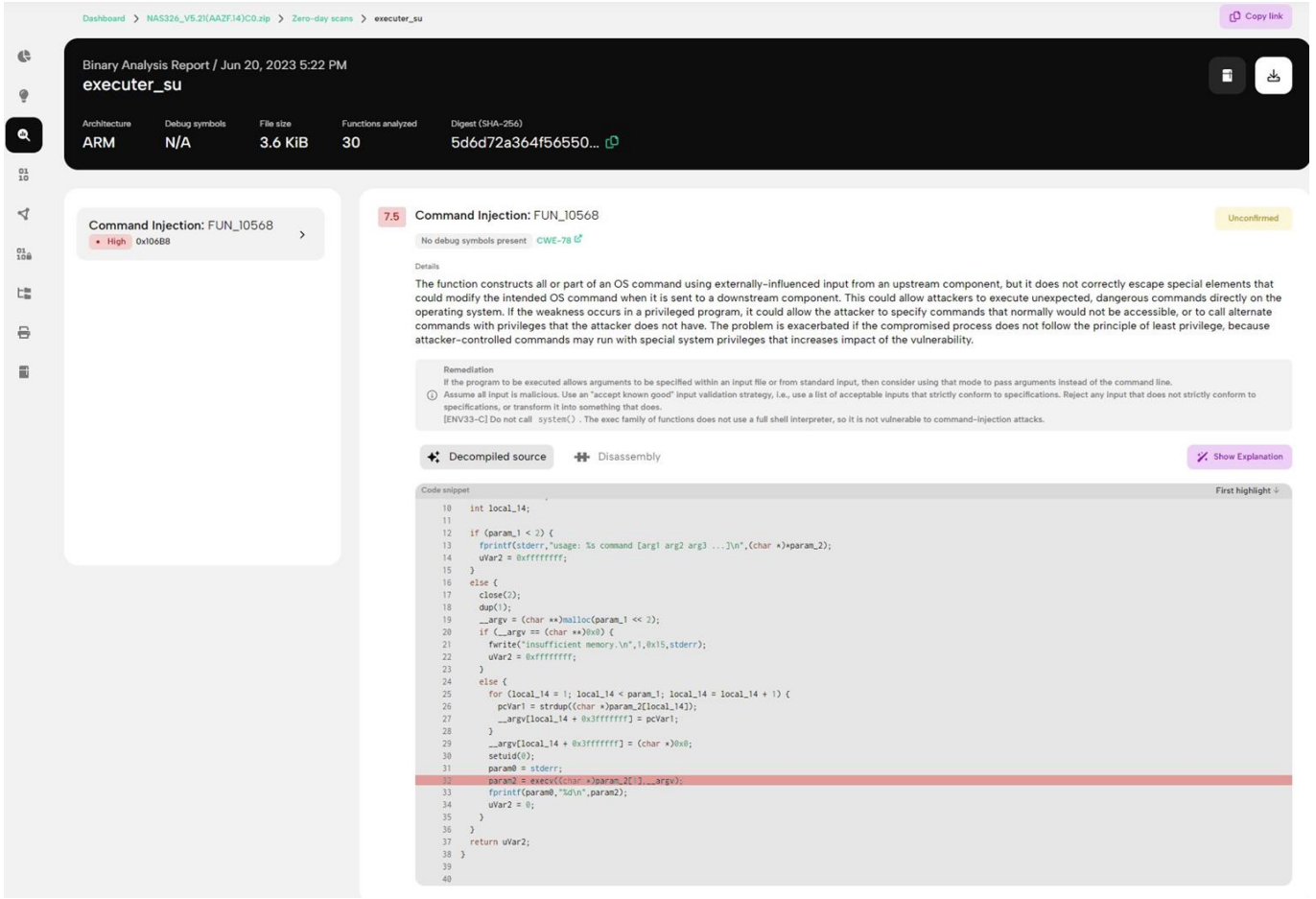
Zyxel NAS326

- Zyxel NAS326
- CVE-2023-37927, CVE-2023-37928, CVE-2023-4473, CVE-2023-4474, CVE-2023-5372
- Root cause: Code injection flaws and authentication bypass
- Secure coding issues and lack of design-time security fundamentals (e.g., Web server access controls)
- Could occur in most IoT organizations
- Overall impact: Unauthenticated, remote attackers **can completely take over the device.**

Real-world Cyber Risk Example

Discovery Process

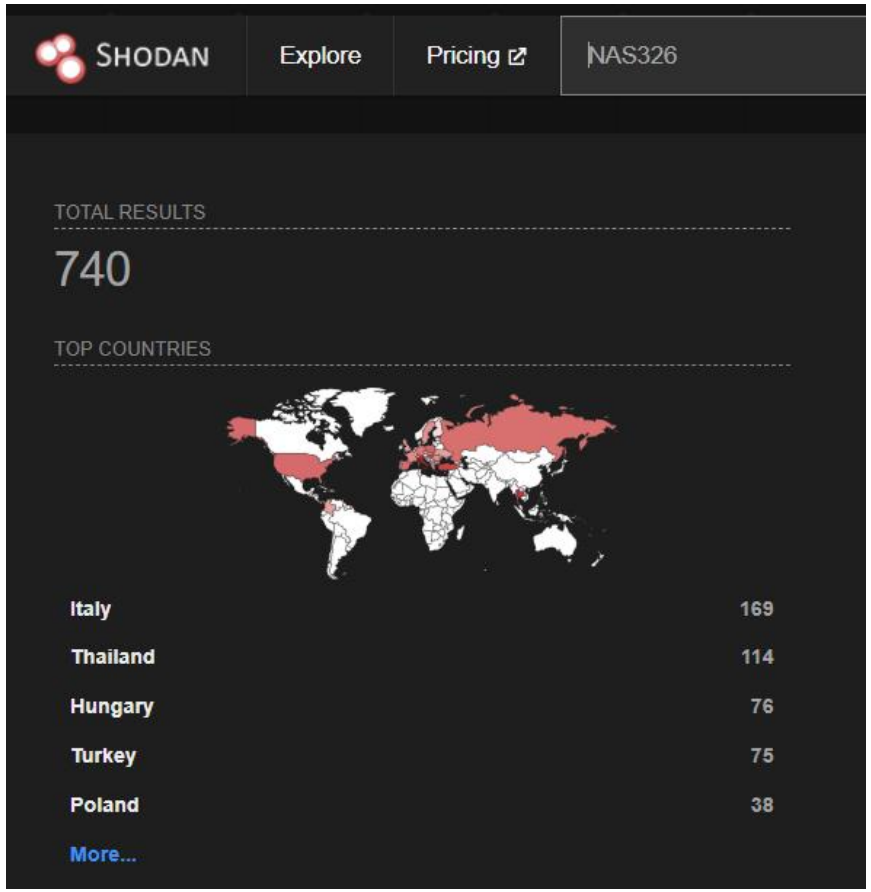
- Platform flagged a command injection (caught by one of our non-technical colleagues!)
- Identified incomplete fix
- Further investigation revealed a lot of **new** issues on upper layers (kudos to Gábor, he was relentless until the 5th CVE)



Real-world Cyber Risk Example

Resolution of Issues

- Coordination occurred in batches, spanning July 2023 to Jan 2024
- Utilized existing PSIRT team and processes at Zyxel
- Issues resolved; however, the device and **entire NAS product line were End-Of-Life'd**.
- Imagine what would happen to a vendor with no security engineers or incident response process in place
- **Consequences are devastating** for vendors lacking security engineers or incident response processes.



Real-world Cyber Risk Example

Takeaways

- Similar mistakes are commonplace
- Post-market vulnerability management is slow and difficult
- Consumers face **critical** risks
- Automatic updates are crucial; devices remain vulnerable without them, as you can't expect consumers to read technical security disclosures and base their manual updates on that.

2. Product security in the CRA

A look at the Cyber Resilience Act

The text is available online: [europarl.europa.eu/doceo/document/**TA-9-2024-0130_EN.html**](europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html)

The CRA text is 338 pages long mandating "what" is required:

- 131 paragraphs of recital
- 71 articles
- 8 annexes

But it doesn't explain "how" to secure products in scope

What is a secure product?

- There are no known exploitable vulnerability at the time of release
- The product start with a secure configuration by default
- If new vulnerabilities or cyber incidentS happen, they can be resolved as long as the product is supported

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

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 modes to protect from cyber attacks 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

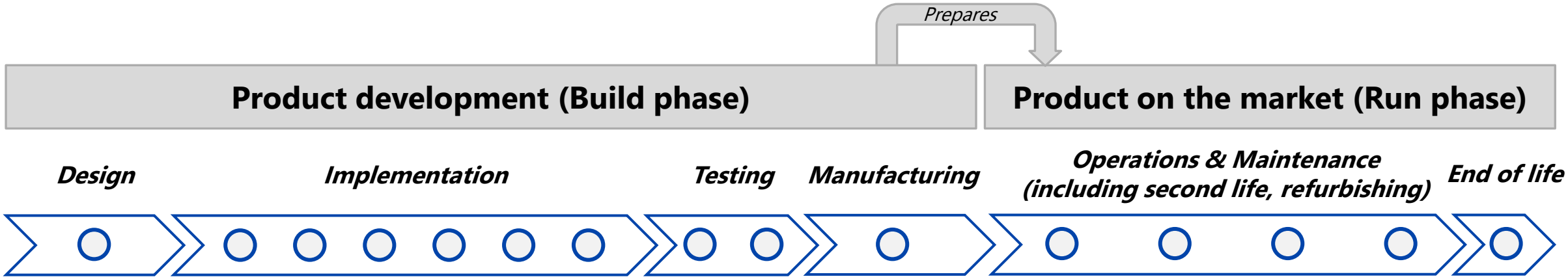
- Declaration of conformity
- Information to customers about the product and the manufacturer: product identification, website, etc.
- Keep documentation for 10 years

Our analysis of the CRA requirements

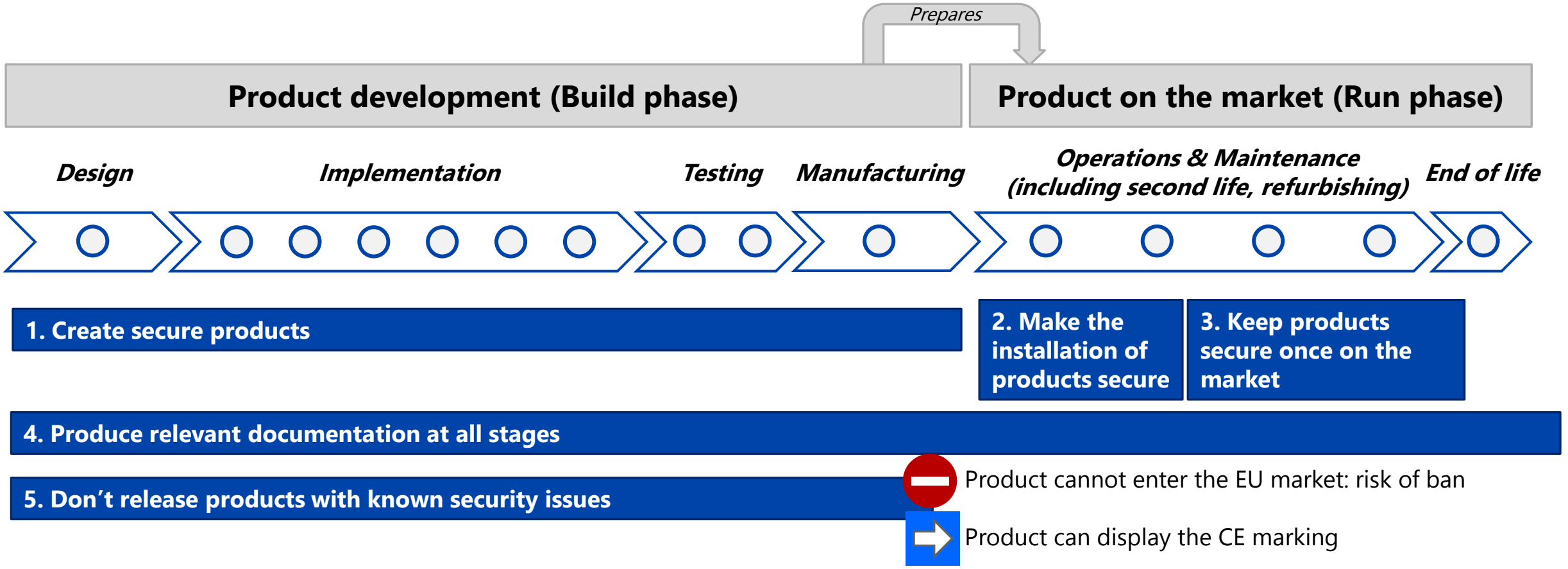
The Cyber Resilience Act has 5 high-level requirements :

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

Reminder: the product lifecycle



CRA REQUIREMENTS IN THE PRODUCT LIFECYCLE



3. How to secure products?

Start with a risk assessment

The CRA requires an initial risk assessment

- You are free to use any methodology
- Objective: evaluate the risks of your product on users and systems
- Document these risks and keep the document for **10 years!**

Identify cyber security measures to mitigate these risks

- We developed #FAST for that (fast.cetome.com)

FAST
Revolutionary Automatic Threat Modeling

Common risks found in IoT products

- Privacy
- Safety
- Mass compromise
- Unauthorised access
- Leaked secrets

The CRA introduces products categories

Product categories give an idea of what is expected

- Higher categories lead to higher risks
- Higher categories require stronger cyber security measures
- Higher categories require more in-depth assurance methodologies
- Most consumer IoT products will fall in the “basic” category or in Class I

The European Commission can

- Add or remove products in these categories
- Change the category of specific products
- Set new requirements for specific categories!

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**

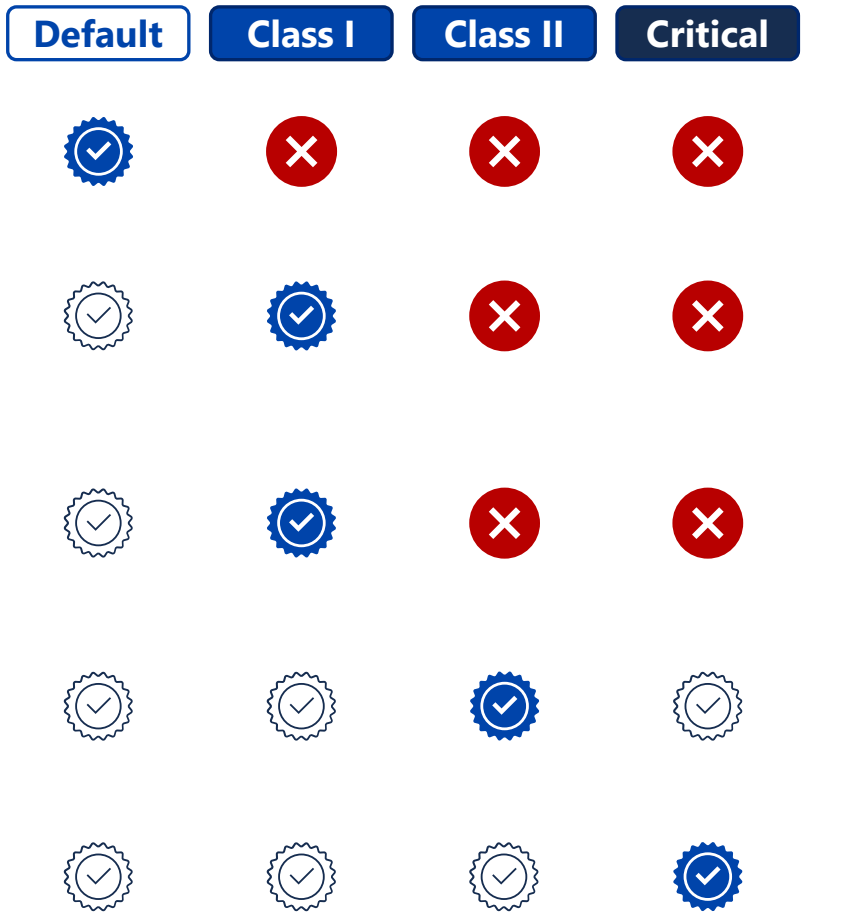
- **Products in class II:** Firewalls, tamper-resistant MCU, network interfaces
- **Recent attack:** vulnerabilities in Qualcomm mobile firmware can lead to memory corruption

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)

Assurance requirements

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



Mandatory if EU certification scheme is available

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 harmonised 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 meter manufacturer implements EUCC

And then? Identify your priorities

Create secure products

- 3 years to comply (anticipated Q3/Q4 2027)
- Obligation to implement cyber security and resilience measures in all new products
- Not very difficult but a lot of efforts:
  - How to ensure security is appropriate?
  - Are requirements in place for suppliers?
  - How about compliance with other markets?

Manage vulnerabilities and incidents

- Shorter deadline: 21 months to comply
- Obligation to report actively exploited vulnerabilities and severe incidents within 24 hours (detailed report within 72 hours)
- Not much effort but a lot of difficulties:
  - Are the pre-requisites in place?
  - Automation and tools required! Where are they?
  - What if we can't fix the issue?

Our recommendations

Build a secure product lifecycle

- Integrate the 5 high-level requirements of the CRA in existing processes
- Try to use automation where possible (e.g. for vulnerability management)

Use an existing standard and fill in the gaps later

- We recommend following ETSI EN 303 645 (ENISA too!)
- Other standards:
  - ISA/IEC 62443-4 (for industrial IoT with some tweaks)
  - CSA PSWG (designed to be cross-market)
  - Harmonized standard for the Radio Equipment Directive (focus on wireless devices)

Implement a Vulnerability Disclosure Policy urgently

- Get some insight on cetome.com/vdp

Train your product teams!

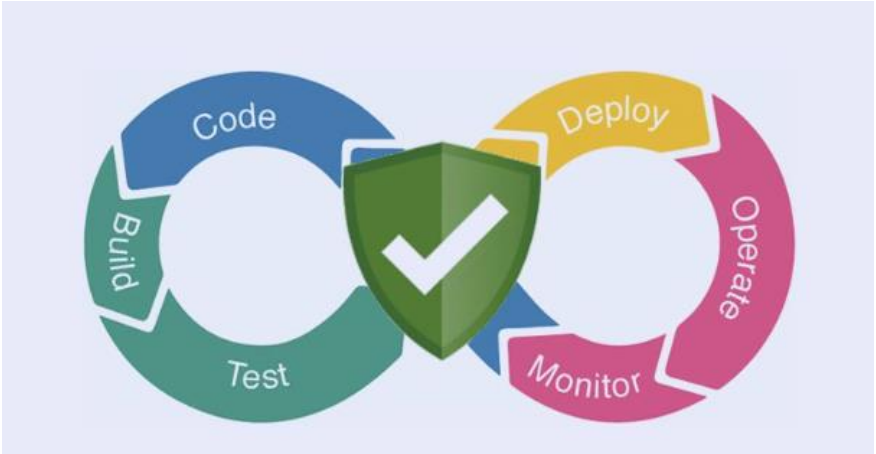
- Secure product lifecycle for product owners
- Secure coding practices for developers
- IoT cyber security standards for architects and engineers

BUGPROVE

cetome
we make cyber work

The Case for Automation

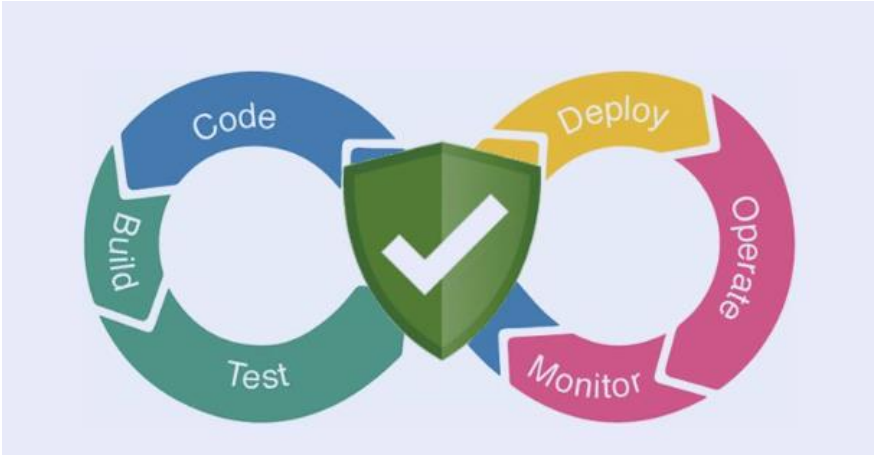
- DevSecOps integrates security testing at every software development stage.
- Many software practices absent in IoT
- Lack of uniform tech stack
- Diverse IoT deployments hinder mature security models
- CRA basically mandates **IoT DevSecOps** and beyond.
- Urges implementation across entire device portfolios, necessitating new tools and processes.



The Case for Automation

Tools for Secure Development

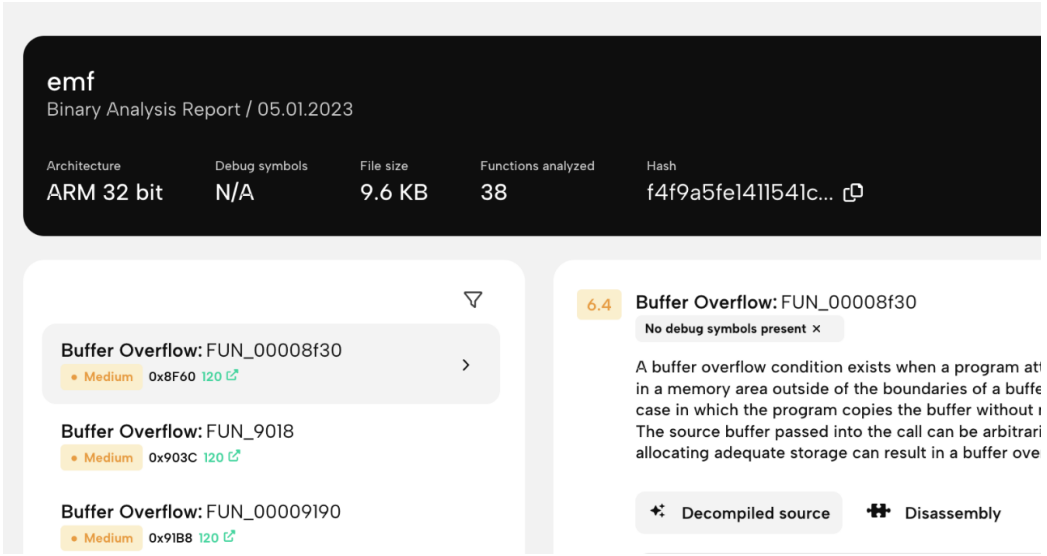
- Traditional tools: SAST aids secure coding, while SCA addresses supply chain risks.
- Software Composition Analysis suited for package-managed technologies, uncommon in IoT (e.g., C/C++).
- SAST is noisy for large code-bases, and lacks contextual understanding of devices.
- Existing tooling may struggle with technical requirements of regulations like ETSI 303 645.



The Case for Automation

Example of Requirement Complexity

Provision 5.13-1 The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.



- Discovered trivial buffer overflows in a consumer router*.
- "**emf**" file provided by Broadcom as a binary within their SDK.
- Potentially affects 15 other OEMs.

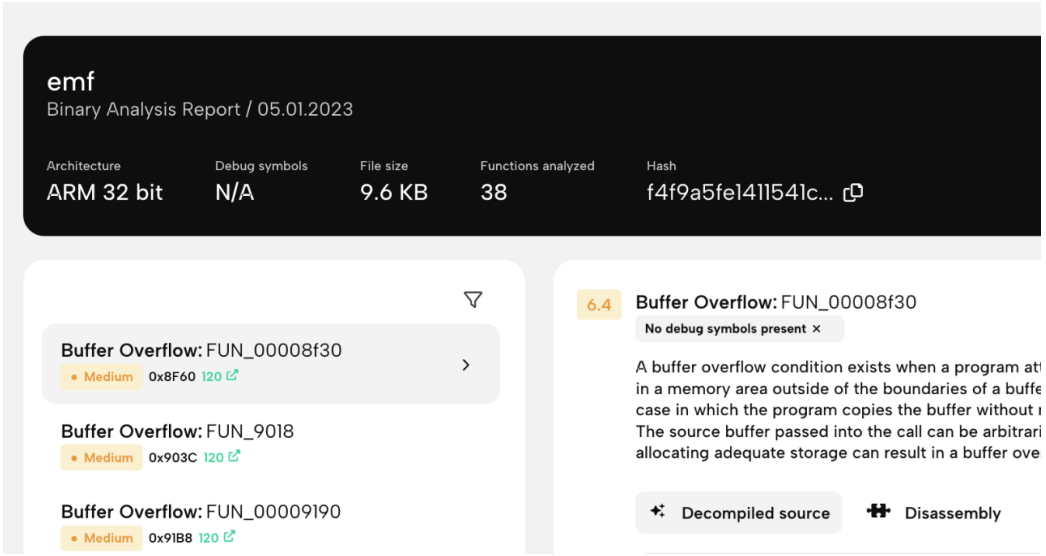
*https://kb.netgear.com/000065667/Security-Advisory-for-Post-authentication-Buffer-Overflow-on-Some-Routers-PSV-2023-0068

The Case for Automation

Compliance and Detection Challenges

- *Would this vendor be in violation of Provision 5.13-1 if CRA was already in place?*
- *How could they have possibly found it?*

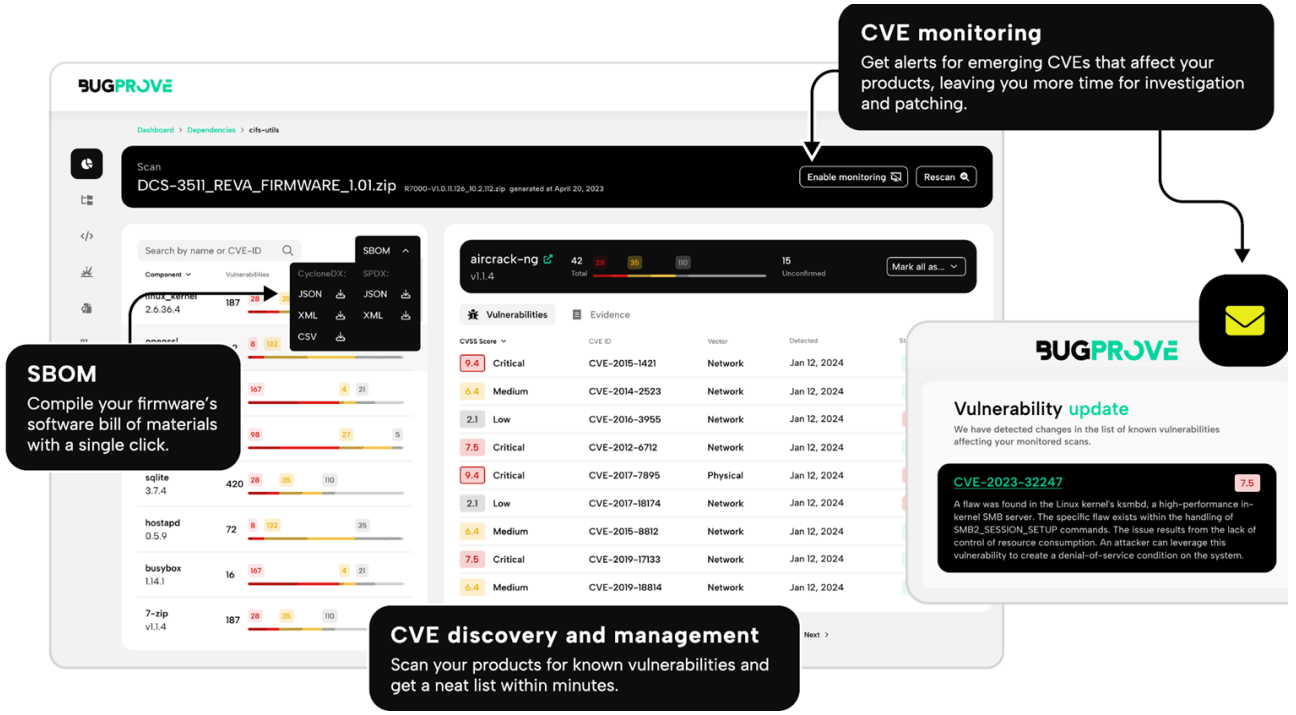
- Supply chain issue; SCA tools **may not** identify it.
- Secure coding mistake, but source code **may not be** available at build time for C/C++ SAST to detect.



BugProve

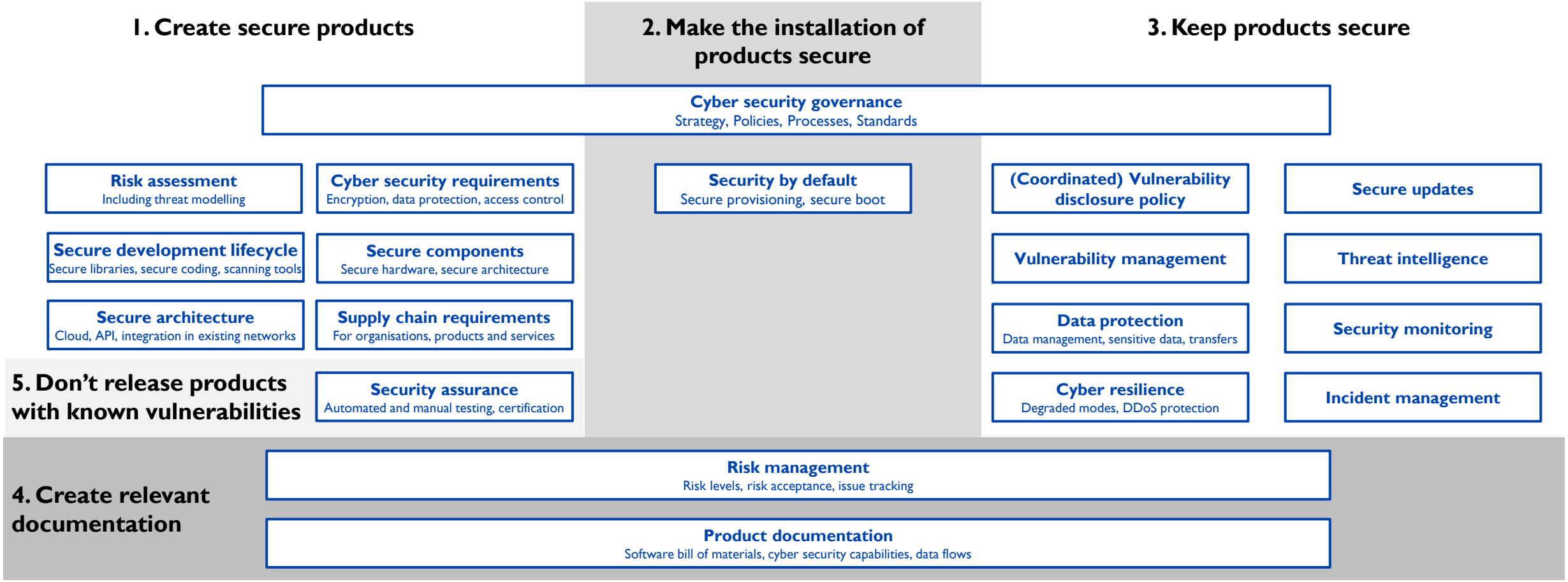
Security via Binary Analysis

- Comprehensive platform automates vulnerability management for embedded devices.
- Automatically generates SBOM for supply chain security pre-market.
- Identifies known vulnerabilities to prevent shipping products with issues.
- Continuously monitors firmware for emerging vulnerabilities to aid CRA post-market efforts.
- Provides PDF evidence for CRA documentation requirements.

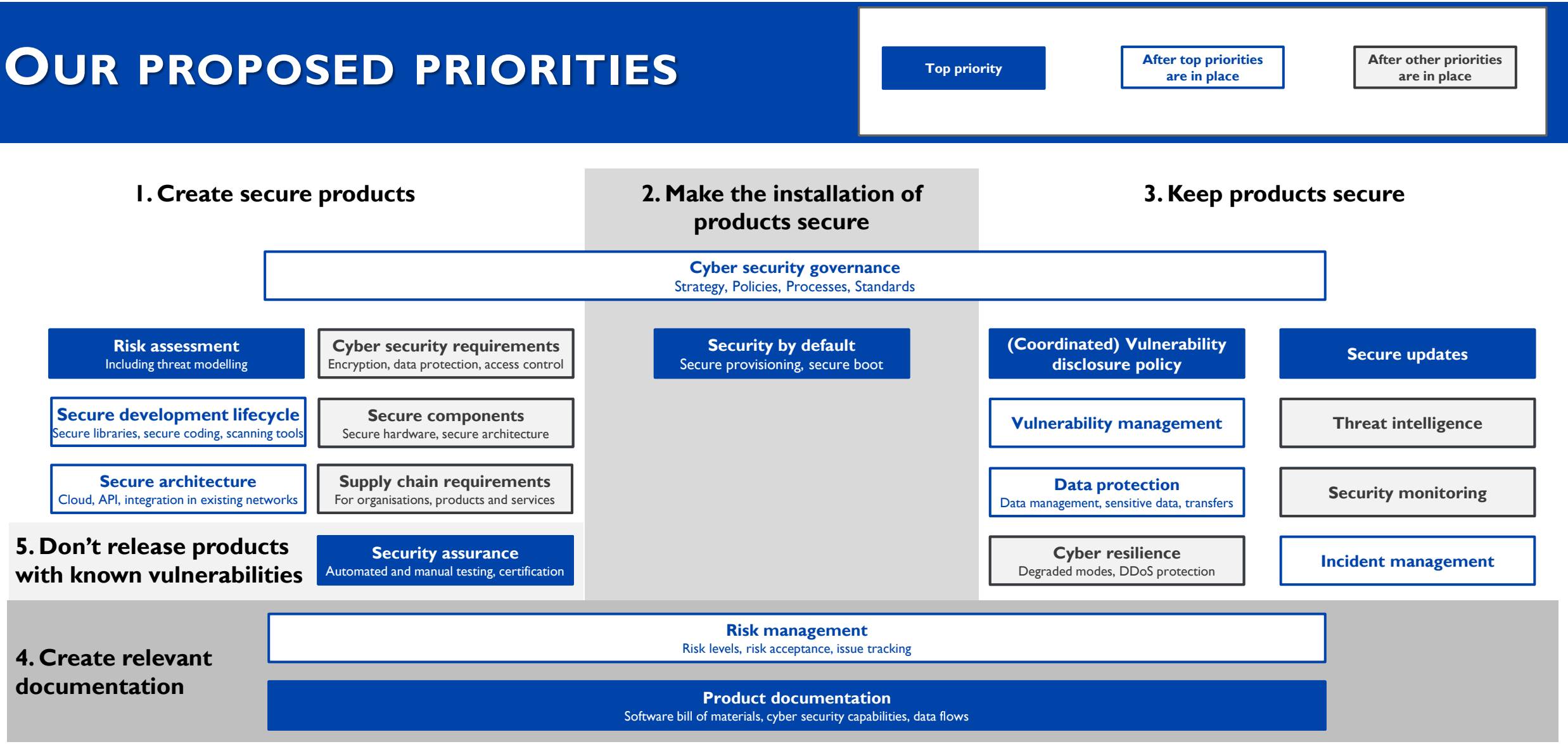


A ROADMAP TO CRA COMPLIANCE

Identify your priorities and implement security requirements for each box



Our proposed priorities



Conclusions

Conclusions

Don’t wait for 2027

The Cyber Resilience Act is a groundbreaking regulation

- All products with a digital element must integrate cyber requirements
- Important to keep products secure after release!
- The regulation mandates higher requirements for certain products

Define your priorities

- Top priority in 2024: implement a risk assessment methodology
- Use our roadmap to identify what is in place, gaps and other priorities

Our top recommendations

- Follow ETSI EN 303 645
- Integrate product security into existing processes
- Train product teams

THANK YOU!

Time for questions

BUGPROVE

cetome
we make cyber work

Reach out

Attila Szász

bugprove.com

Cédric Lévy-Bencheton

cetome.com