Navigating the panorama of regulations and security solutions: What you need for IoT?

IoT London, 21 March 2023

Dr. Cédric LEVY-BENCHETON

cetome.com

cetome
we make cyber work

CETOME

we make cyber work

Who are we?

- We are a human-size cyber security advisory created in 2017
- We are based in the UK and in the EU (France)

What makes us different?

- We make cyber work for you and your customers
- We focus on IoT and Critical Infrastructure
- We are technology-agnostic

Who do we work with?

- Manufacturers and users of IoT and Industrial IoT systems
- Critical infrastructure operators and asset owners
- Governments and public sector organisations

Why Choose cetome?

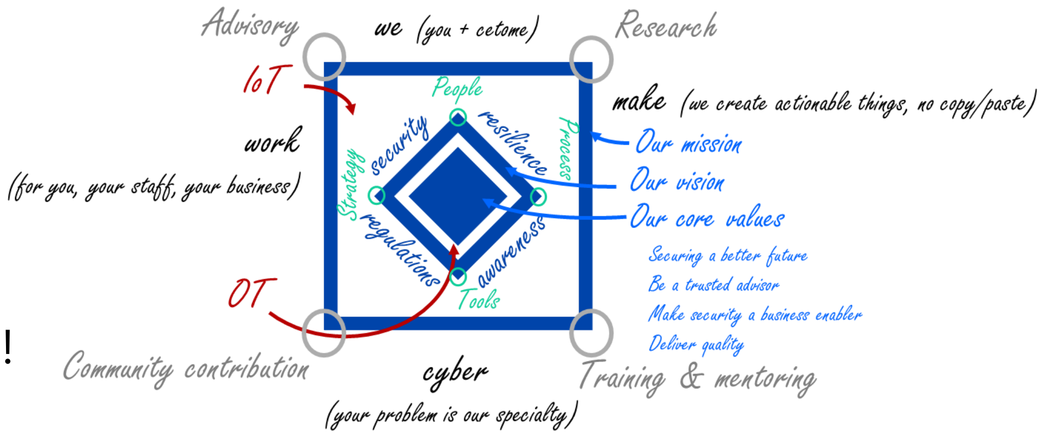
We are proud of making the difference

We support your business

- **We make cyber work** for your business, your staff and your customers
- We optimize your existing practice and reduce your investment

We are expert in IoT cyber security

- We understand your challenges and risks
- We know how to make cyber security appropriate and efficient
- We are a leader on IoT cyber security standards and regulations!



You can trust us

- We are technology and vendor-agnostic
- We work with your teams at every level of your organisation

1. **Introduction to IoT security**

2. **Panorama of regulations**

3. **Solutions and priorities**

I.

Introduction to IoT Security

IoT Question Time

What does the S in IoT stand for?

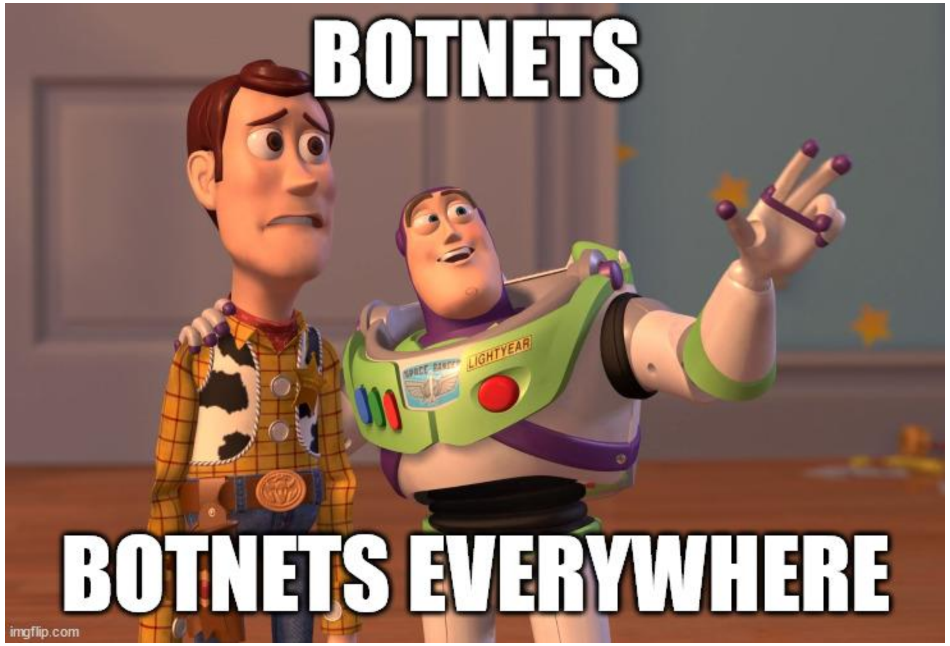
It's 2023 and the S in IoT stands for:

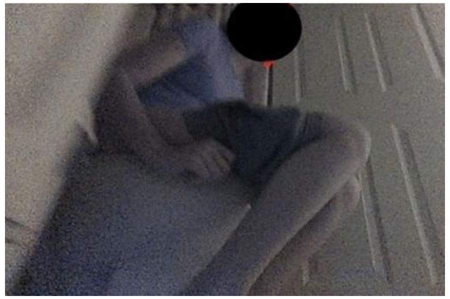
"So many new regulations, you will only buy IoT products with the S in it".

In the UK, it's called the Product Security and Telecommunications Infrastructure Act 2022 (or PSTI).

But why do we need IoT security regulations?

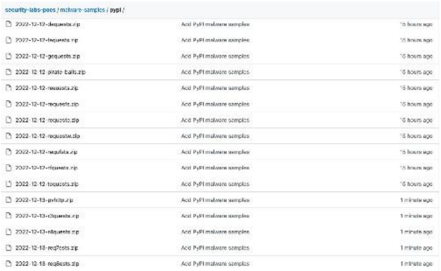
IoT is still insecure… Some issues reported recently





Roomba vacuum cleaner recorded a picture of a woman on the toilets and posted it on Facebook.

Source: Multiple newspapers / October 2022



security-labs-pocs / malware-samples / pypi /

2022-12-12-dequests.zip	Add PyPI malware samples	16 hours ago
2022-12-12-fequests.zip	Add PyPI malware samples	16 hours ago
2022-12-12-gequests.zip	Add PyPI malware samples	16 hours ago
2022-12-12-pirate-balls.zip	Add PyPI malware samples	16 hours ago
2022-12-12-reauests.zip	Add PyPI malware samples	16 hours ago
2022-12-12-requests.zip	Add PyPI malware samples	16 hours ago
2022-12-12-requeste.zip	Add PyPI malware samples	16 hours ago
2022-12-12-requestw.zip	Add PyPI malware samples	16 hours ago
2022-12-12-requfsts.zip	Add PyPI malware samples	16 hours ago
2022-12-12-rfquests.zip	Add PyPI malware samples	16 hours ago
2022-12-12-tequests.zip	Add PyPI malware samples	16 hours ago
2022-12-13-pyhttp.zip	Add PyPI malware samples	1 minute ago
2022-12-13-r3quests.zip	Add PyPI malware samples	1 minute ago
2022-12-13-r4quests.zip	Add PyPI malware samples	1 minute ago
2022-12-13-req7ests.zip	Add PyPI malware samples	1 minute ago
2022-12-13-req8ests.zip	Add PyPI malware samples	1 minute ago

100s of Pypi dependencies compromised with malware

Source: Christophe Tafani-Dereeper / December 2022

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

Source: Quarkslab / March 2023

What else can we do about it?

Not much...

Make IoT products secure by default

Blame users for not securing their products

Change your password!

Use MFA!

Get a VPN!

Don’t buy IoT!

BLCOKHCAIN!11!

Patch your devices!

Use a dedicated network!

2.

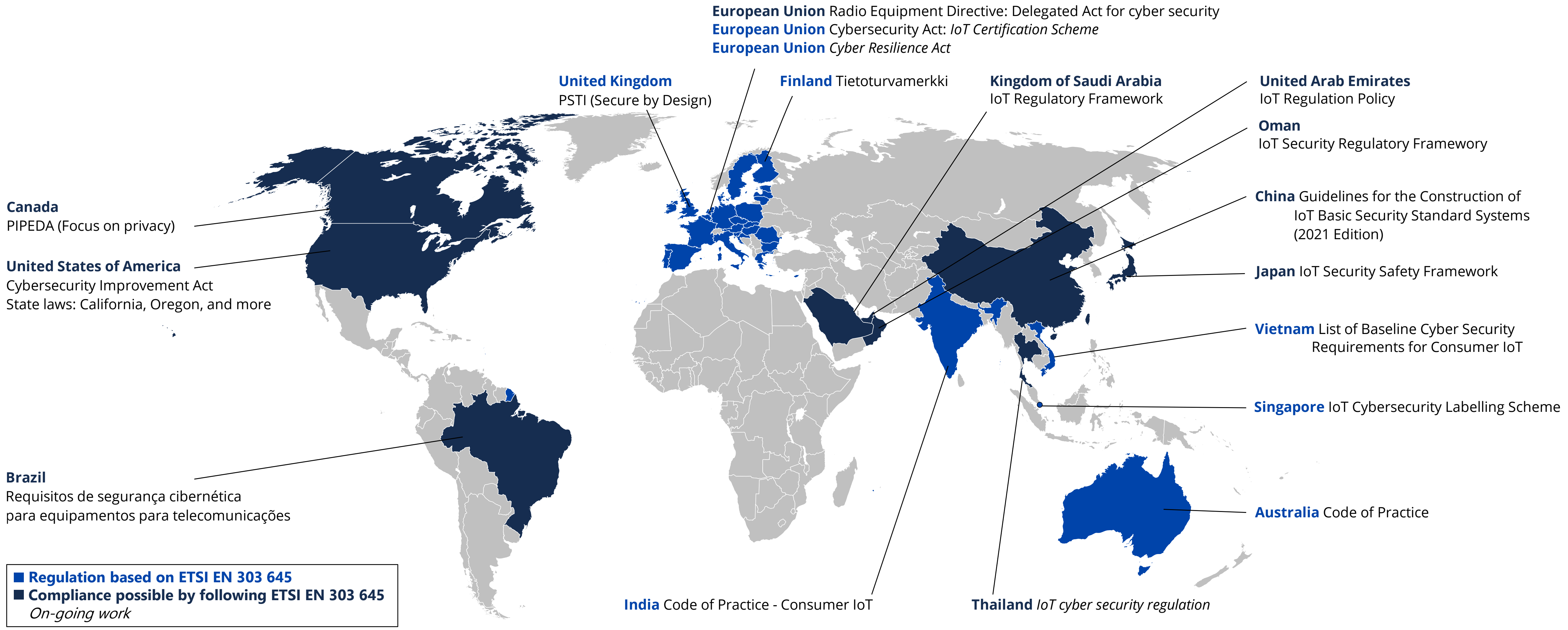
Panorama of regulations

Panorama of IoT Cyber Security Regulations

#IoTPanorama

cetome.com/panorama

#RegulateVendors



European Union Radio Equipment Directive: Delegated Act for cyber security
European Union Cybersecurity Act: *IoT Certification Scheme*
European Union *Cyber Resilience Act*

United Kingdom
PSTI (Secure by Design)

Finland Tietoturvamerkki

Kingdom of Saudi Arabia
IoT Regulatory Framework

United Arab Emirates
IoT Regulation Policy

Oman
IoT Security Regulatory Framewory

Canada
PIPEDA (Focus on privacy)

United States of America
Cybersecurity Improvement Act
State laws: California, Oregon, and more

China Guidelines for the Construction of
IoT Basic Security Standard Systems
(2021 Edition)

Japan IoT Security Safety Framework

Vietnam List of Baseline Cyber Security
Requirements for Consumer IoT

Singapore IoT Cybersecurity Labelling Scheme

Brazil
Requisitos de segurança cibernética
para equipamentos para telecomunicações

Australia Code of Practice

India Code of Practice - Consumer IoT

Thailand *IoT cyber security regulation*

🟦 **Regulation based on ETSI EN 303 645**
⬛ **Compliance possible by following ETSI EN 303 645**
On-going work

WHAT SHALL YOU DO TO COMPLY WITH REGULATIONS?

Follow a smart approach

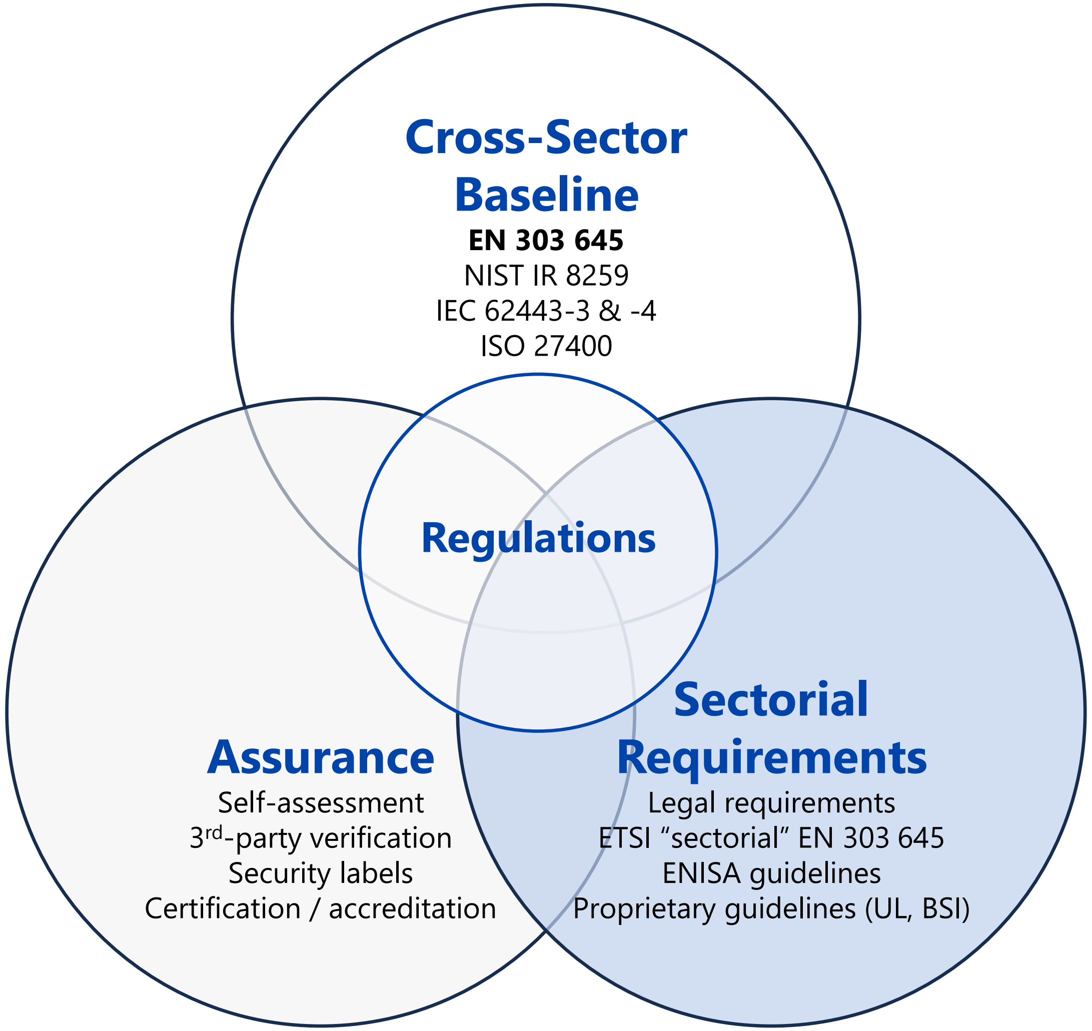
Most regulation require 3 things:

1. Create secure products
2. Make the installation of products secure
3. Keep products secure once on the market

It is important to be smart:
your approach must work for ALL markets.

How to navigate around regulations? Standards!

Compliance is not security: security makes compliance easier.



Cross-Sector Baseline

EN 303 645
NIST IR 8259
IEC 62443-3 & -4
ISO 27400

Regulations

Assurance

Self-assessment
3rd-party verification
Security labels
Certification / accreditation

Sectorial Requirements

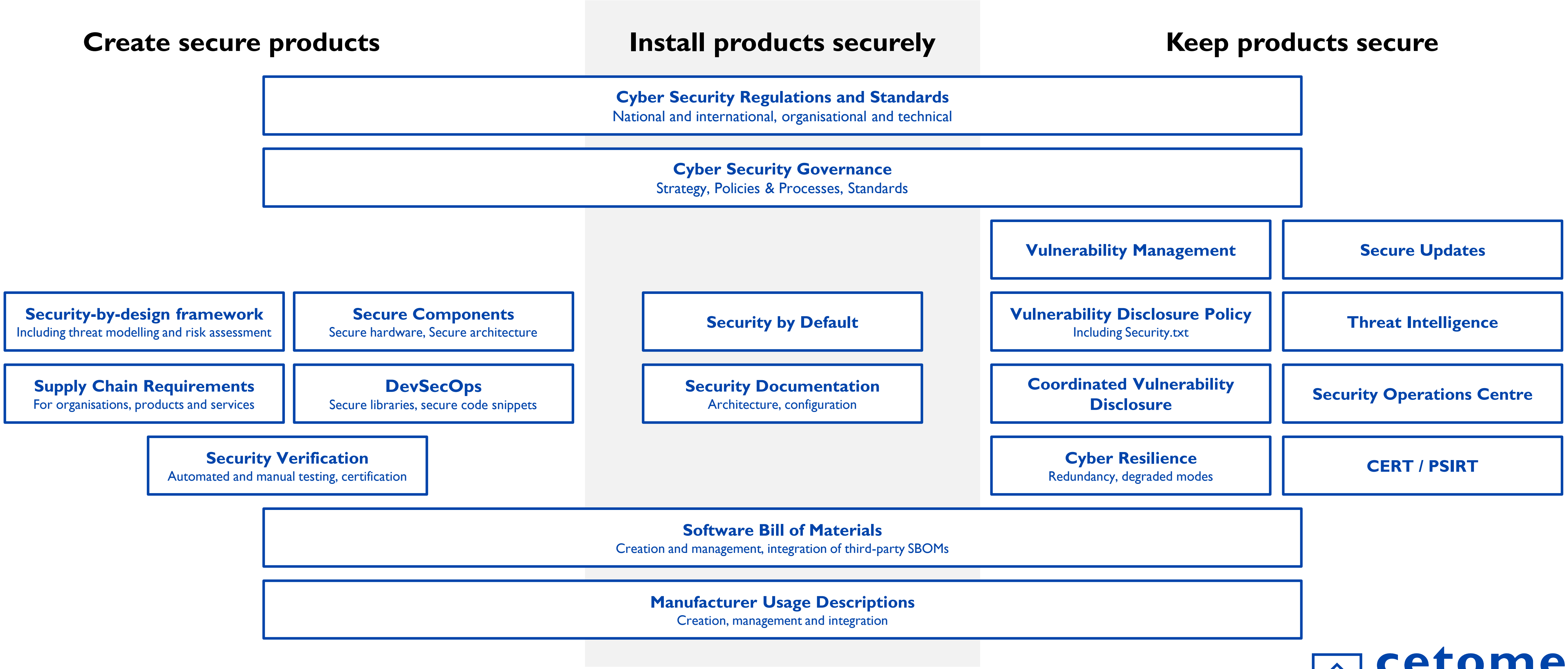
Legal requirements
ETSI "sectorial" EN 303 645
ENISA guidelines
Proprietary guidelines (UL, BSI)

3.

SOLUTIONS AND PRIORITIES

SECURE IOT PRODUCTS THROUGHOUT THEIR LIFECYCLE

What good looks like today



Create secure products

Install products securely

Keep products secure

Cyber Security Regulations and Standards
National and international, organisational and technical

Cyber Security Governance
Strategy, Policies & Processes, Standards

Security-by-design framework
Including threat modelling and risk assessment

Secure Components
Secure hardware, Secure architecture

Supply Chain Requirements
For organisations, products and services

DevSecOps
Secure libraries, secure code snippets

Security Verification
Automated and manual testing, certification

Security by Default

Security Documentation
Architecture, configuration

Vulnerability Management

Secure Updates

Vulnerability Disclosure Policy
Including Security.txt

Threat Intelligence

Coordinated Vulnerability Disclosure

Security Operations Centre

Cyber Resilience
Redundancy, degraded modes

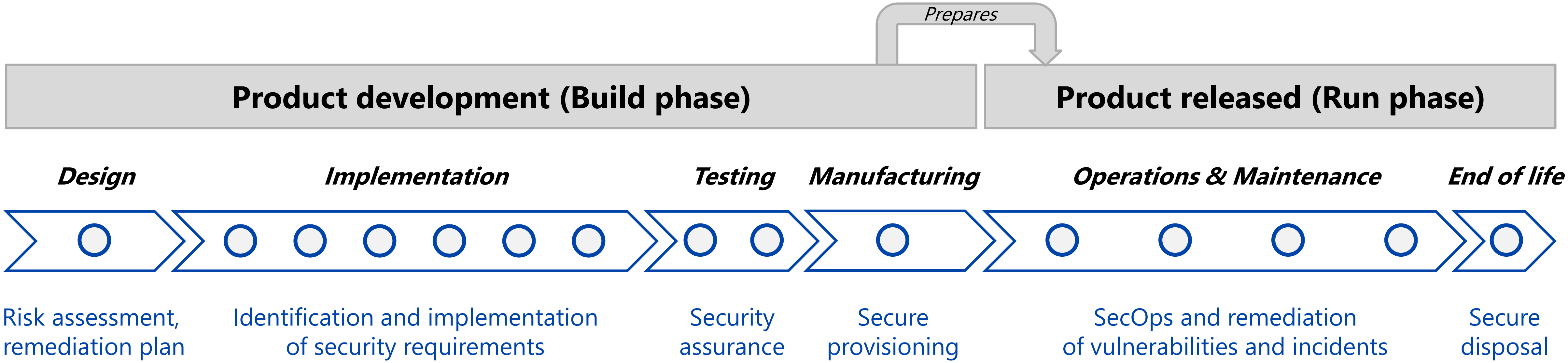
CERT / PSIRT

Software Bill of Materials
Creation and management, integration of third-party SBOMs

Manufacturer Usage Descriptions
Creation, management and integration

Security-by-design for IoT Products

Know how to do the right thing at the right time



Prepares

Product development (Build phase)

Product released (Run phase)

Design

Risk assessment, remediation plan

Implementation

Identification and implementation of security requirements

Testing

Security assurance

Manufacturing

Secure provisioning

Operations & Maintenance

SecOps and remediation of vulnerabilities and incidents

End of life

Secure disposal

Now we know what to do! But where do we start?

PRIORITIES, PRIORITIES, PRIORITIES

What you should do now (if not already)

RELEASE INSECURE IOT PRODUCTS AND RISK MARKET BAN
SPEND TIME AND MONEY ON IOT SECURITY
IOT MANUFACTURERS TODAY
JAKE-CLARK.TUMBLR
imgflip.com

- Implement **appropriate cyber security requirements** for IoT products:
  - Regular threat modelling and risk assessment. Not only at the beginning of the project!
  - Remove all hardcoded, shared or easy to guess default passwords! Passwordless is amazing (but hard)
  - Reduce the attack surface: deactivate unused interfaces, do not trust inputs by default
- **Accompany your teams** to know what to do around cyber security requirements
- **Document** what you do, how you do it, issues, risks, etc.
- Ensure your **partners and suppliers** follow your rules
- **Verify** that the **implementation** works as intended
- Keep **products secure** once **on the market** in conformity with new regulations:
  - Implement a vulnerability disclosure policy: contact form, security.txt, internal processes
  - Patch new vulnerabilities using secure over-the-air updates (including signed firmware)

How about we cut costs and just do a pentest?

IoT pentest companies? Not many specialists

Cut costs? An IoT pentest is expensive (even more with hardware, firmware reverse engineering, specific protocols like Matter)

Results? Your products are not more secure

Conclusions

Create a panorama of IoT cyber security regulations
People want to do IoT cyber security
I have to work more
I have to work more
imgflip.com

IoT cyber security is a regulatory requirement

- Regulations are mandating high-level requirements
- Most markets follow the same set of requirements
- Insecure products will be banned

Manufacturers must invest today

- Secure existing product development with quick wins
- Maintain these products once released to limit exploitable vulnerabilities
- Formalise their security-by-design process
- Train their product teams, even non-security people

THANK YOU!

Our website: cetome.com

cetome
we make cyber work