EU CYBER RESILIENCE ACT

A PRACTICAL GUIDE TO LAY THE FOUNDATIONS FOR COMPLIANCE

OCTOBER 2023

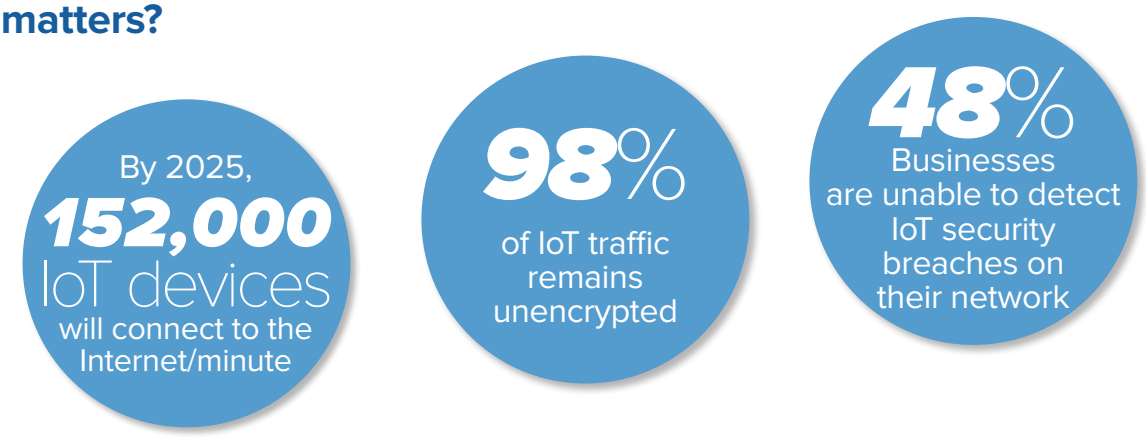
Introduction to CRA : the legislation

The proliferation of IoT devices has revolutionized industries. However, the increased connectivity also creates several vulnerabilities that malicious actors can exploit. An increasing number of cyber-attacks today target hardware and software products. Businesses continue to be exposed to risks such as unauthorized access, theft, tampering, unlawful reproduction, and even disruption of critical services. There is also the risk of such products entering the market with unaddressed vulnerabilities and customers/organizations using those products due to lack of transparency with respect to the security.

On September 15, 2022, the European Commission presented the Cyber Resilience Act "to safeguard consumers and businesses buying or using products or software with a digital component".

> *The proposal aims to ensure better protection for consumers through increasing the responsibility of manufacturers by obliging them to provide security support and software updates to address identified vulnerabilities and providing them with information about cybersecurity of products they buy and use. The act would provide a single set of rules for cybersecurity for companies in the EU. It would decrease the number of cybersecurity incidents and increase the transparency and trust of consumers in products with digital elements and guarantee better protection of their data and privacy.*

Why it matters?



The European Commission accurately points out that hardware and software products often face successful cyber attacks, due to 2 major problems that add costs for users and the society:

- a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and
- an insufficient understanding and access to information by users, preventing them from choosing products with proper cybersecurity features or using them in a secure manner.

What are the objectives?

The development of secure products with digital elements by ensuring that

- hardware and software products are placed on the market with fewer vulnerabilities and
- manufactures take security seriously throughout a product's life cycle;

Ensure users take cybersecurity into account when it comes to products with digital elements:

- improve the security of products from the development phase, throughout the life cycle
- ensure a coherent cybersecurity framework, facilitating compliance
- enhance the transparency of security properties
- Enable businesses and consumers to use the products securely

Who is concerned?

Manufacturers, importers and distributors of products with digital elements.

There are some exceptions for products, for which cybersecurity requirements are already set out in existing EU rules, for example on medical devices, aviation, or cars.

Products affected by the CRA

90% of products	10% of products	
Default category Self-assessment	**Critical "Class I"** Application of a standard or third-party assessment	**Critical "Class II"** Third-party assessment
Criteria: n/a	Criteria: - **Functionality** (e.g. critical software) - **Intended use** (e.g. industrial control/NIS2) - **Other criteria** (e.g. extent of impact) Critical products	
Exemples Photo editing Word processing Smart speakers Hard drives Games etc.	**Exemples (Annex III)** Password managers Network interfaces Firewalls Microcontrollers etc.	**Exemples (Annex III)** Operatiing systems Industrial firewalls CPUs Secure elements etc.

Essential security requirements to fulfill

There are 2 sets of regulations that must be adhered to, for products with digital elements:

1. Relating to the properties of products with digital elements

2. Vulnerability handling requirements

At Quarkslab, we will focus on addressing the requirements mentioned in 1.

Security requirements relating to the properties of products with digital elements (as listed in annex I)

1 **Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;**

2 **Products with digital elements shall be delivered without any known exploitable vulnerabilities;**

3 **On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:**

a. be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

b. ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

c. protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;

d. protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

e. process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');

f. protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

g. minimise their own negative impact on the availability of services provided by other devices or networks;

h. be designed, developed and produced to limit attack surfaces, including external interfaces;

i. be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

j. provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

k. ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.

Adressing security requirements with QShield

QShield helps you secure your devices against data, code, and IP extraction or alteration, no matter where you are in your IoT journey - from conception to market deployment.

PROTECT

Sensitive **data, certificates & keys**, and **valuable intellectual property**

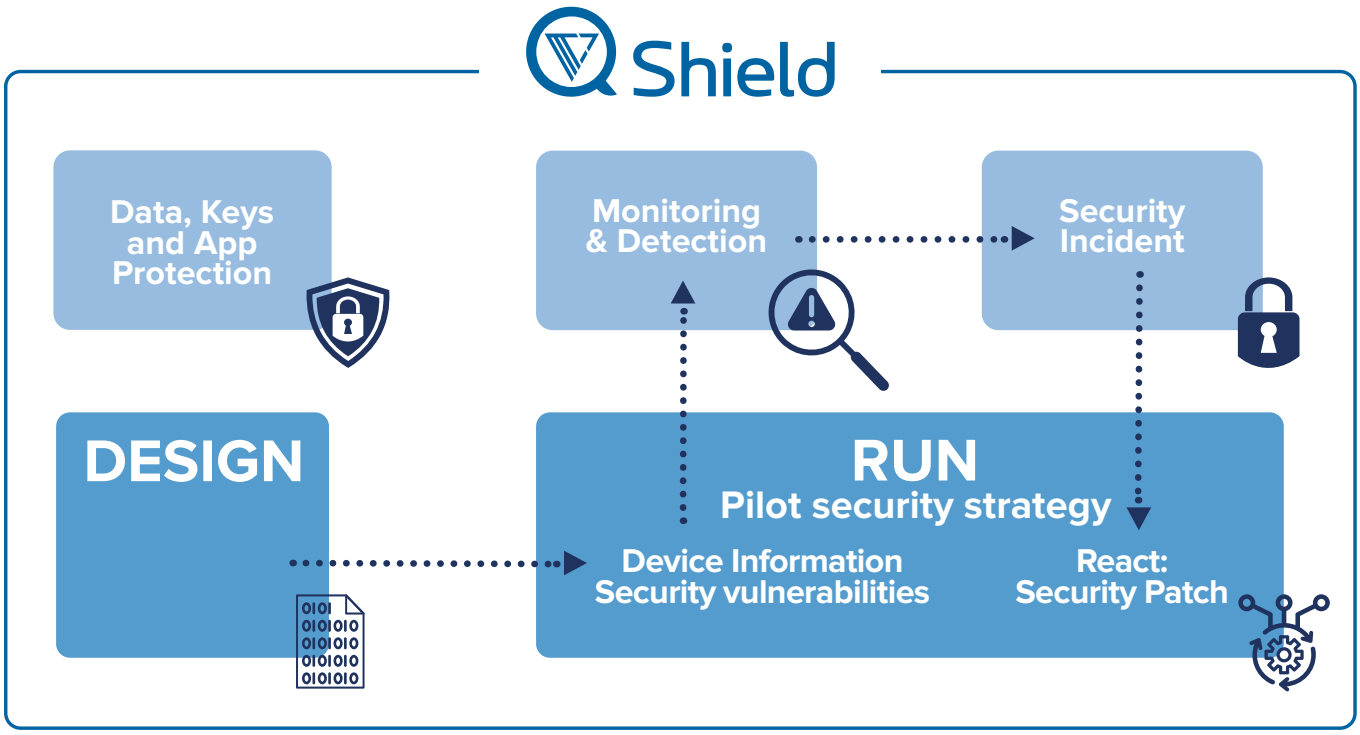
OBSERVE

Monitor **security sanity** & device usage in **real time**

RECOVER

Update security protections OTA during an attack

A set of custom-built solutions, help you mitigate potential threats, minimize financial and reputational damage, and ensure business continuity.



QShield App Protection (QAP)

- Code & data protection, dynamic protections and integrity checks thanks to obfuscation & RASP
- Prevent attackers from gaining access to your sensitive assets

QShield Keys Protection (QKP)

- Cryptographic keys protection against extraction thanks to white-box cryptography
- Protect your keys against software and hardware attacks without requiring any dedicated hardware component

QShield Data Protection (QDP)

- Safely store sensitive/value-added data using software and/ or hardware security components.
- Your data is always stored encrypted and can only be decrypted in authorised devices.

QShield Environment Checks (QEC)

- Monitor device fleet sanity and detect tampering in real time. Adapt security policies thanks to Moving Target Defense.
- Access actionable insights by monitoring on-field activity

EU cyber resilience act: in-depth coverage with QShield

	Requirements	Purpose	QShield Modules	Comments
100% coverage	(3) (b)	Protect assets (code, data) against unauthorized access	QAP	• Hinder code understanding/reverse engineering hence complicate the preparation of attacks • Set code and data integrity checking in code, with alarms fired upon intrusion detection • Data encryption at rest Data encryption and signing on transit • Hinder code understanding/reverse engineering hence complicate the preparation of attacks • Set code and data integrity checking in code, with alarms fired upon intrusion detection • Data encryption at rest • Data encryption and signing on transit • Hinder function understanding/ reverse engineering hence complicate the preparation of attacks • Set code and data integrity checking with alarms fired upon intrusion detection • Data encryption at rest if needed • Data encryption and signing on transit if needed • Monitor security information locally or remotely and triggers actions upon abnormal situations
	(3) (c)	Protect confidentiality of data at rest and on transit	QDP, QKP	
	(3) (d)	Protect integrity of data and code at rest, during processing and on transit	QAP, QKP, QDP	
	(3) (f)	Protect the availability of essential functions	QAP, (QKP), (QDP)	
	(3) (j)	Record/Monitor relevant security information on product	QAP, QEC	

	Requirements	Purpose	QShield Modules	Comments
Partial Coverage	(3) (a)	Existence of a secure by default configuration	QDP, QKP	• QShield allows to dynamically store these configurations securely if needed • QShield is designed to protect against attack based on software reverse engineering • QShield software security allows vulnerability update via software/ firmware updates at low cost (no recall of the device needed)
	(3) (h)	Limit attack surface	QAP	
	(3) (k)	Address vulnerabilities via security updates	QDP, QKP combined with a device management product	

Latest updates

The Cyber Resilience Act, once in force, will complement the existing NIS2 Directive & the EU Cybersecurity Act.

The regulation will become applicable **24 months** (at the latest by **Q1 2026**) after its entry into force, except for the reporting obligation on the manufacturer, which would apply from **12 months** (most probably by **Q1 2025**) after the date of entry into force.

In cases of non-compliance with the obligations set out in the proposal, the following maximum fines would apply based on the type of infringement and nature of the economic operator:

- Manufacturers could risk a fine of **€15million** or **2.5%** of their total annual turnover worldwide, whichever is higher, for non-compliance with the security requirements listed under Annex I.
- Manufacturers, importers, or distributors could risk a fine of **€10 million** or **2%** of their total annual turnover worldwide, whichever is higher, for non-compliance with any other obligation laid down in the draft regulation.

CONCLUSION

A response to the escalating wave of IoT cyber-attacks, the CRA is set to make a difference:

▶ Ensuring secure development of connected devices across their lifecycle.

▶ Empowering users to prioritize cybersecurity when selecting and utilizing connected devices.

Lay the foundation for compliance before the Act comes into force with QShield:

- Protect assets (code, data) against unauthorized access
- Protect confidentiality of data at rest and in transit
- Protect integrity of data and critical code at rest, during processing and in transit
- Protect the availability of functions
- Record/Monitor relevant security information on product

REFERENCE

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0454

https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0454

https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

https://iotac.eu/top-8-things-you-should-know-about-the-eu-cyber-resilience-act-cra/

Learn more and check our latest resources

Whitepapers: **https://quarkslab.com/resources/**
On demand webinar: **https://quarkslab.com/webinars/**

Quarkslab

Contact and follow us