Cybersecurity regulations—a paradigm shift

Technology Six Pack

March 2024

Cybersecurity: a rapidly growing problem

Cybercriminals launched around 10 million DDoS attacks worldwide

Ransomware attacks alone are estimated to have cost the world roughly $20 billion

Every 11 seconds, there is a ransomware attack

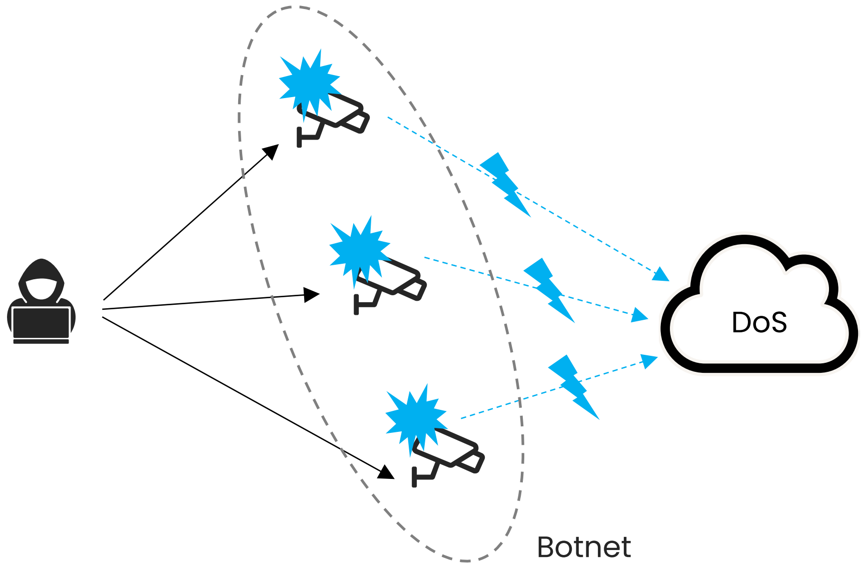
Source: CYBER RESILIENCE ACT - Fact Sheet 2023 (statistics 2021) (https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet)

Device security is getting more of a concern

- Encryption of connections and authentication in networks must become a common practice
- However, it is not enough: many vulnerabilities on devices can be exploited by hackers, including:
  - Inappropriate device configuration
  - Weakness in the access control mechanisms on the device (e.g. default password)
  - SW bugs in communication stack, OS or application SW, leading to undefined device behaviors
  - Lack of verification on executed FW/SW
  - Unpatched vulnerabilities
- This usually ends up with device and service unavailability, installation of malicious code, leakage of authentication keys, data eavesdropping, etc.

Security incidents extend their impact way beyond individual equipment

- The largest attack to date (Mirai malware) turned networked devices running Linux (IP cameras and home routers) into remotely controlled bots
- The botnet was used to execute the worst, large-scale distributed denial of service attack (DDOS) against Internet
- As a result, several websites went offline
- Botnet cases keep making the headlines



Regulators react to foster a more secure cyberspace: a pivotal step

- **Cyber Resilience Act (CRA)**, first ever EU wide legislation of its kind, introducing mandatory cybersecurity requirements for hardware and software products, throughout their whole lifecycle.

- **U.S. Cyber Trust Mark**, a cybersecurity labeling program for smart devices designed to give consumers the tools needed to make informed decisions regarding security, when purchasing products to bring into their homes.

- **Other regulations** emerge, such as PSTI in UK (Product Security and Telecommunications Infrastructure)

European Commission

CYBER RESILIENCE ACT

New EU cybersecurity rules ensure more secure hardware and software products

#SOTEU

#DigitalEU #SecurityUnion #Cybersecurity

SEPTEMBER 2022 – UPDATED DECEMBER 2023

A first ever EU wide legislation of its kind: the **Cyber Resilience Act** introduces **mandatory cybersecurity requirements for hardware and software products**, throughout their whole lifecycle.

A change in paradigm: regulations get strong and broad

	U.S. Cyber Trust Mark	Cyber Resilience Act (CRA)
Market where devices are marketed and sold	U.S. only	All EU member states
Scope	Consumer Smart Products	Finished products with digital elements and SW/HW sub-components, for all verticals except automotive and medical
Product definition	A "product" consists of the Smart Consumer (IoT) Device(s), companion app. (smartphone) & backend services	A "product" is a device, MCUs, commercial software, OS, servers, desktops, smart TVs, smart phones, appliance, industrial PLC, …
Enforcement	Voluntary (for now)	Mandatory (CE Mark)
Fine	-	€ 15 million or 2.5% of the annual turnover, whichever is higher.
Requirements	NIST 8425	Essential Cybersecurity Requirements (ANNEX I – Cyber Resilience Act)
Launch	Expected Q3 2024	Expected 2024, with full enforcement in 2027

CRA & U.S. Cyber Trust Mark require a security process beyond device capabilities, leading to deep transformation of organizations

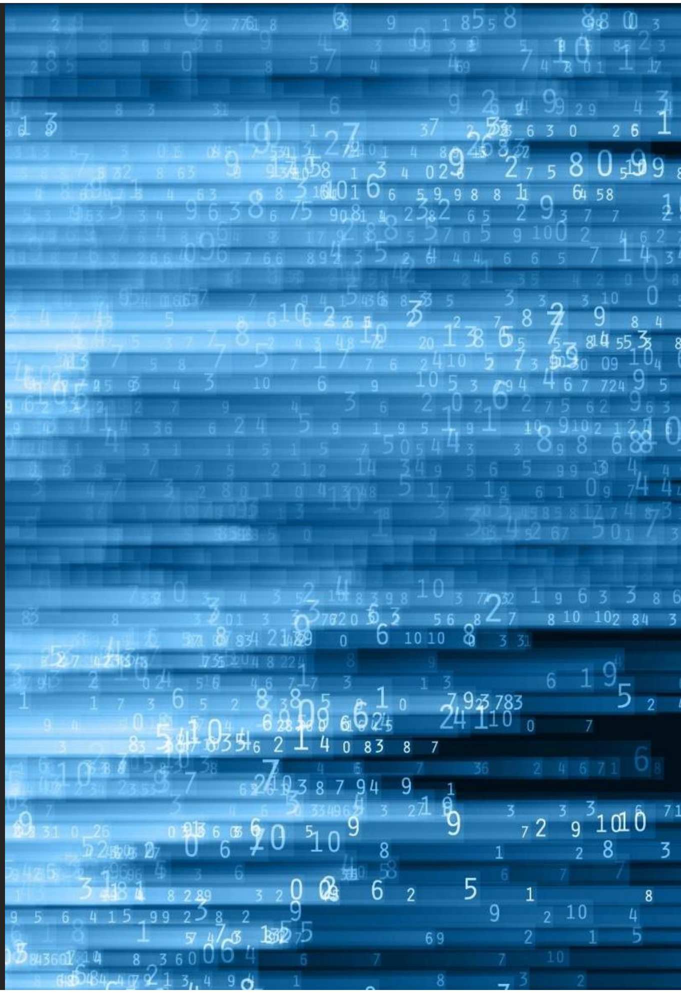
Product security capabilities

Provide means to:

- minimize exposure and risk
- manage vulnerabilities
- minimize impact of vulnerabilities

Security process

Assess risks,
Document (requirements, design, SBoM, …)
Educate & inform customers,
Collect information on vulnerabilities,
Report & respond to incidents



The regulations set device security principles without specifying ‘how’

CRA & U.S. Cyber Trust Mark **DO SCOPE**:

- Product configuration
- Product authentication
- Access to product
- Data Protection
- Product monitoring and Cyber State Awareness
- Vulnerability fix and product update
- Reduction of incidents’ impact and product availability

CRA & U.S. Cyber Trust Mark **DON’T SPECIFY:**

Level of security

Level of protections must reflect the level of risks, depending on product type, use case and application

Functional requirements

Cryptographic algorithms, protocols, PKI, X509 certificate format, etc.

Technological implementations

Security hardware, software, etc.

NXP supports OEMs in accessing regulated markets and building resiliency

nxp.com/security

Security functions on-chip with EdgeLock technology, EdgeLock 2GO services, secure provisioning tools/SDK

Extensive ‘toolbox’ to implement and activate product security capabilities as required by regulators

EdgeLock Secure Enclave (integrated on MCU/MPUs), EdgeLock Secure Elements & Authenticators

Enhanced HW protections of security functions: minimize risks of retrofit, maximize resilience in field, facilitate demonstrability of security robustness and assurance

Certified EDGELOCK® ASSURANCE by NXP

EdgeLock Assurance program

Procurement of secure components, with NXP Security Maturity Process & chip security certifications (SESIP[1] – EN17927), providing ‘Security by Design’ at component level, independent 3rd party assessment and Product Security Incident Response handling (PSIRT)

EdgeLock hardware

EdgeLock 2GO

Security functions available on NXP products map to regulation requirements

Required security capability (regulations)	Supporting security functions by NXP solutions[1]
Product configuration	Device lifecycle management Secure SW & credential Install Secure boot, Secure Update
Product authentication	Identification & Authentication, Attestation Secure key storage/management
Access to product	Secure debug, Secure connect Secure key storage/management Crypto services for access control
Data Protection	Data encryption/authentication Tamper detection, Tamper resistance Secure key storage/management Privileged access to data, secure connect
Product monitoring & Cyber State awareness	Authentication Device (runtime) attestation Secure Event Audit/Logging
Vulnerability fix and product update	Secure update Secure key storage/management
Reduction of incidents' impact Product availability	Tamper/anomaly detection SW/data/processing isolation Damage control & device recovery Secure key storage/management

[1] Please check NXP product datasheets/security manual for availability of specific security functions

NXP advanced security technologies,
Made for resilience in a dynamic cybersecurity landscape

EdgeLock Secure Enclave

Dedicated security unit integrated in NXP MCU/MPU

- ✓ Enhanced isolation for protection of critical security functions required by regulations
- ✓ Advanced capabilities for device monitoring and availability protection
- ✓ Protection of sensitive data and credentials
- ✓ Available on latest NXP MCU/MPUs

EdgeLock SE05x/A5x

Secure elements and secure authenticators

- ✓ Secure vault for credentials with protection against SW and advanced HW attacks
- ✓ Certified Common Criteria EAL6+, FIPS
- ✓ Optional personalization with custom credentials at NXP manufacturing
- ✓ Can be plugged to any type of ASIC or processor

EdgeLock 2GO

NXP cloud services for credential management

- ✓ Easy deployment of root of Trust credentials on devices
- ✓ Management of credentials over-the-air and over device lifecycle
- ✓ Native integration on EdgeLock Secure Enclave, Secure Elements and Secure Authenticators

Cyber Resilient Act: a conformance process based on device criticality[1] but same requirements for all product categories

Category	Important Product “Class I”	Important Product “Class II”	Critical Products	Default category
Examples (End products & components)	- Routers & modems for internet connection, switches - Smart home virtual assistants - Internet-connected toys - Smart Lock - Wearables - Password managers; - PKI and digital certificate issuance software - Physical and virtual network interfaces	- Hypervisors and container runtime systems - Firewalls - intrusion detection and/or prevention systems - Tamper-resistant MCUs/MPUs	- Smart meter gateways - Devices for advanced security purposes - Smartcards, secure elements, hardware devices with security boxes	**90% of the product:** - Industrial PLC - Smartphone - EV chargers - Industrial HMI - Docking station
Minimum conformance mechanism	**Harmonized standards** (ensuring CRA principles are met)	**3rd Party product assessment** (product and/or process)	**Common Criteria certification by default**	**Self-assessment** (!! Legal uncertainty of compliance….)

[1] Please note this slide reflects current state of knowledge and understanding; Also, this regulation is still under discussion and evolving.

Cyber Resilient Act: conformance steps for product belonging to default category

1

OEM fills in declaration of conformity and provides documentation

OEMs can leverage guidance that will be issued in future by European standardization organizations (ETSI, CENELEC, etc.) for risk assessment and self-declaration

2

OEM safely stores the self-declaration for at least 10 years in case of control by surveillance authorities

3

OEM can affix the CE mark on the product

CE

1. Please note this slide reflects current state of knowledge and understanding; Also, this regulation is still under discussion and evolving.

US Trust Mark: conformance steps

1

Product owner selects one of the approved certification programs (private bodies)

OEM fills in a security questionnaire (declaration)

2

Private body reports to FCC products meeting the criteria for NIST 8425

A 3rd party lab might have to verify the self-declaration[1]

3

FCC issues a QR code and registers the product in a central, public database.

This will later give consumers access to up-to-date information on the adherence state of the product to cybersecurity standard

4

OEM is authorized to display the U.S. Cyber Trust Mark logo on product

Product owner

UL

csa connectivity standards alliance

FCC

U.S. CYBER TRUST MARK

[1] Please note this slide reflects current state of knowledge and understanding; Also, this regulation is still under discussion and evolving.

Towards a common certification program for consumer IoT devices

- Fragmented IoT cybersecurity standards landscape: a challenge for OEMs
- Connectivity Standards Alliance (CSA) takes initiative to **consolidate** widely adopted international standards into a single specification and certification program
- **IoT Device Security Specification (V1.0)** and **'Product Security Verified Mark'** launched in March 2024
- Version 1.0 includes requirements from **ETSI EN 303 645 and NIST IR 8425**
- CSA alliance is working towards recognition of Verified Mark by national authorities
- **NXP is ready** for Verified Mark Certification

Interoperability standards complement regulations focused on device security

Interoperability – Smart Home

Matter standard

Device attestation certificates
Device pairing protocol (PASE[2])
Connection protocol (CASE[3])
Operational credentials
Access control protocol
Cryptographic suites

U.S. Cyber Trust Mark (NIST 8425)

The product must have the following capabilities:

Authentication
Interface access control
Changeable configuration
Default settings
State awareness
SW updatability
Data protection

Interoperability – Industry 4.0

OPC UA

OPC-UA[1] standard

User authentication
Installations & SW certificates
Security policies (crypto algos)
Security modes
Global discovery server

Cyber Resilience Act

The product must have the following capabilities:

Proof of origin
Secure by default configuration
Access control
Availability essential funct.
Monitoring & reporting
Security updates
Data protection

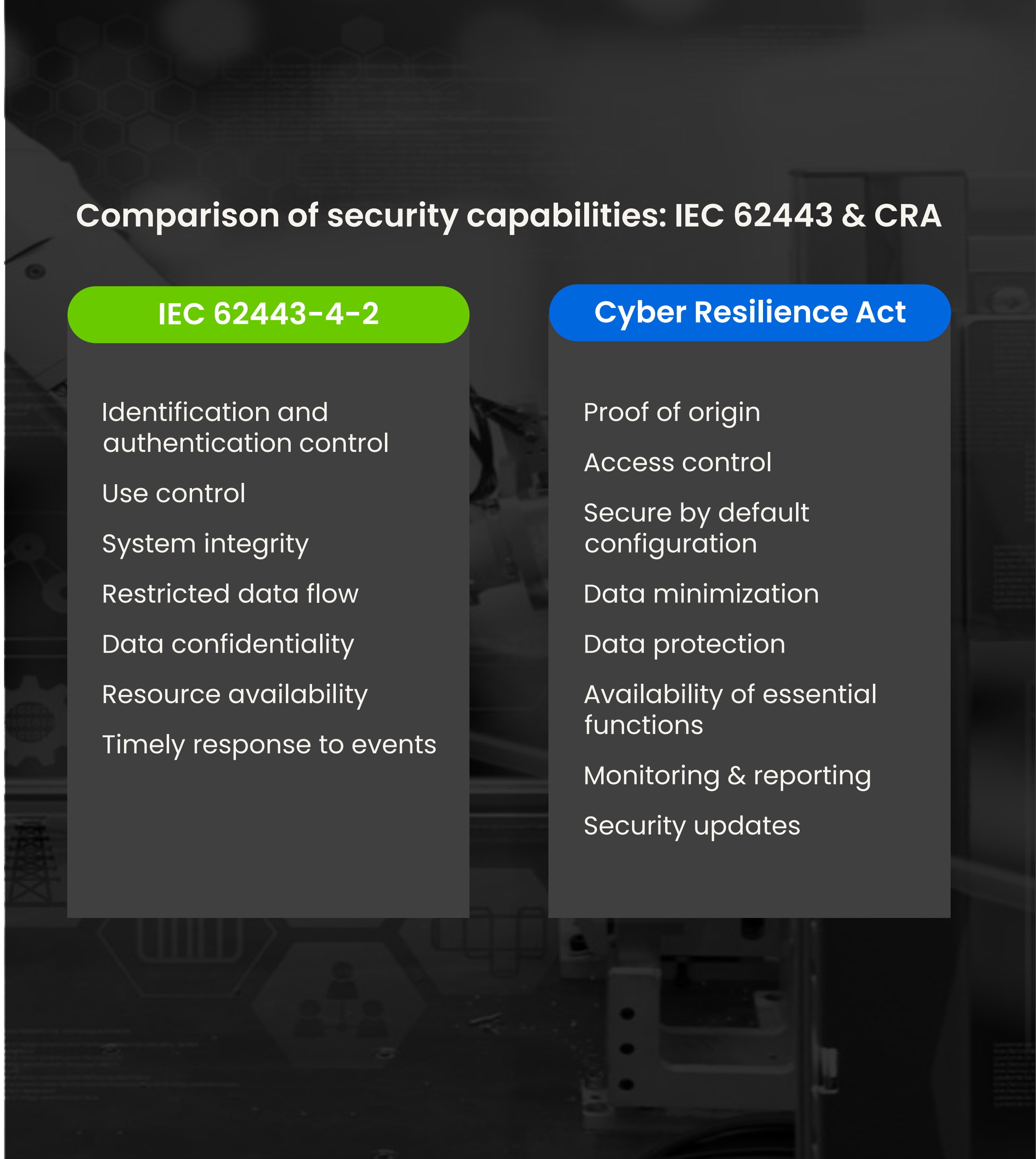
[1] Open Platform Communications – Unified Architecture

[2] PASE: Passcode-Authenticated Session Establishment

[3] CASE: Certificate-Authenticated Session Establishment

IEC 62443 and Cyber Resilience Act: A convergence on the principles for industrial security

- Both IEC 62443 standard and CRA specify:
  - Security process (IEC 62443-4-1)
  - Device security capabilities (IEC 62443-4-2)
- Both converge high-level on the security capabilities to a large extent
- However, there is currently no mechanism of (partial) CRA conformance based on the 62443 certifications; also, CRA has additional obligations not covered by 62443, among others towards vulnerability detection, reporting, handling and patching, as well as open source.
- The legal implications of CRA require careful demonstrability of security functionality, security robustness and security assurance level, based on device exposure to risk



Comparison of security capabilities: IEC 62443 & CRA

IEC 62443-4-2

Identification and authentication control

Use control

System integrity

Restricted data flow

Data confidentiality

Resource availability

Timely response to events

Cyber Resilience Act

Proof of origin

Access control

Secure by default configuration

Data minimization

Data protection

Availability of essential functions

Monitoring & reporting

Security updates

- NXP offers a **scalable portfolio** of security protections, integrated in MPU/MCUs or based on companion secure elements, to meet different levels of cyber risks
- NXP EdgeLock technology combined with NXP security expertise and assurance program allows device manufacturers to **accelerate release** of compliant products to market
- NXP comprehensive **security solutions** extend to device’s lifecycle, bringing resilience in a dynamic regulation landscape

nxp.com/security

Annex

Key principles
Cyber security regulations

Key principles of NIST 8425 (U.S. Trust Mark)

- Asset identification
- Interface access control
- Product configuration
- Software update
- Data protection
- Cybersecurity state awareness

IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A)

+

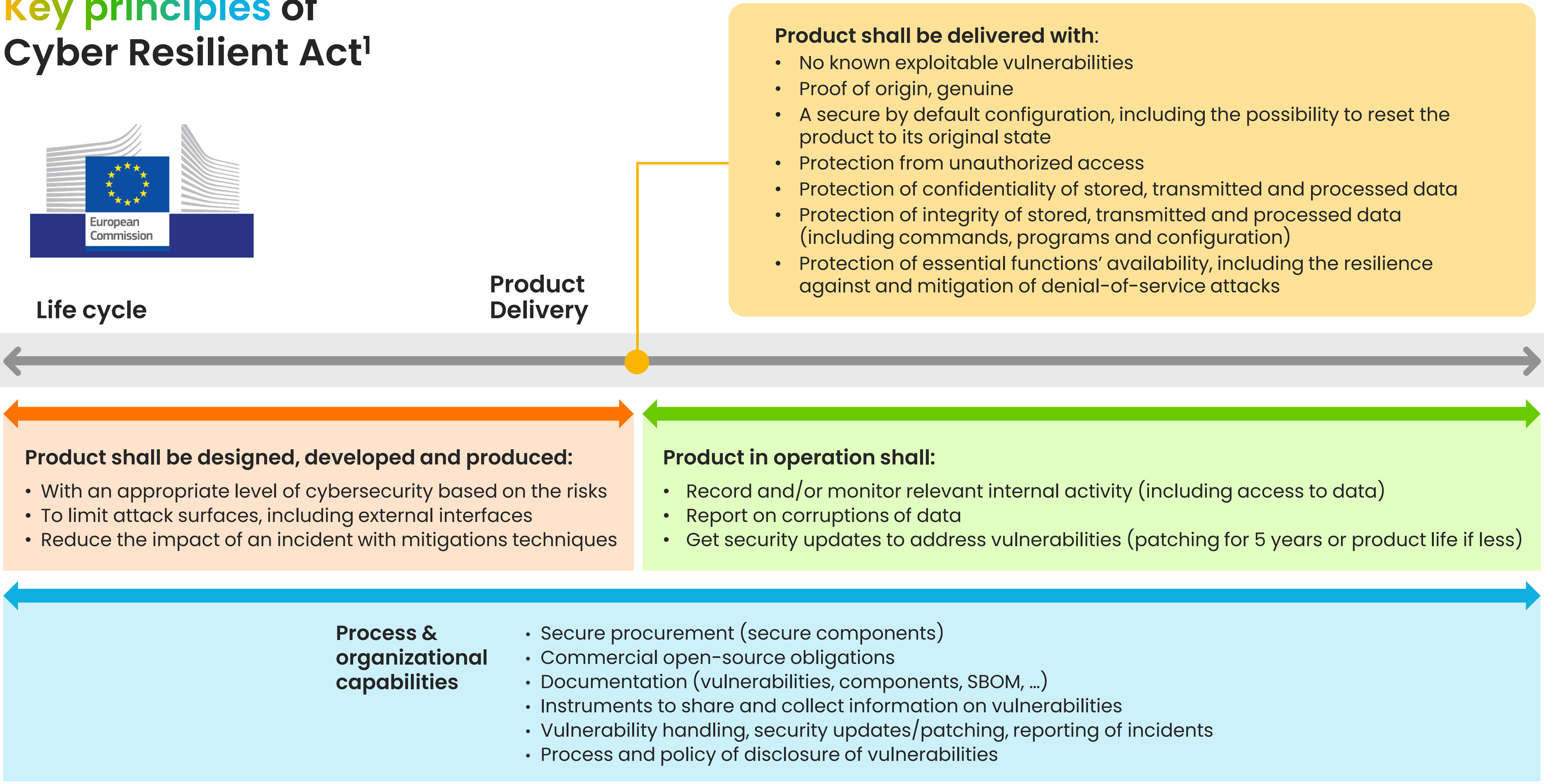
- Documentation
- Information and query reception
- Information dissemination
- Product education and awareness

IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259B)

NIST 8425 also requires OEMs to document design decisions
(including selected security technology)

Notes and sources

Key principles of Cyber Resilient Act[1]



Product shall be delivered with:

- No known exploitable vulnerabilities
- Proof of origin, genuine
- A secure by default configuration, including the possibility to reset the product to its original state
- Protection from unauthorized access
- Protection of confidentiality of stored, transmitted and processed data
- Protection of integrity of stored, transmitted and processed data (including commands, programs and configuration)
- Protection of essential functions' availability, including the resilience against and mitigation of denial-of-service attacks

Product shall be designed, developed and produced:

- With an appropriate level of cybersecurity based on the risks
- To limit attack surfaces, including external interfaces
- Reduce the impact of an incident with mitigations techniques

Product in operation shall:

- Record and/or monitor relevant internal activity (including access to data)
- Report on corruptions of data
- Get security updates to address vulnerabilities (patching for 5 years or product life if less)

Process & organizational capabilities

- Secure procurement (secure components)
- Commercial open-source obligations
- Documentation (vulnerabilities, components, SBOM, ...)
- Instruments to share and collect information on vulnerabilities
- Vulnerability handling, security updates/patching, reporting of incidents
- Process and policy of disclosure of vulnerabilities

1. Please note this slide reflects current state of knowledge and understanding; Also, this regulation is still under discussion and evolving.

nxp.com