About the Lecturer

- Lead Auditor for Management Systems (information security)
- Member of the **Institute for Artificial Intelligence** and founder of Safer.bg NGO.
- Managing director of **Zucchetti Bulgaria**
- Leading the Innovation ecosystem network of EDIH Trakia
- Assistant Professor at **UniBIT and Plovdiv university**:
  - Cybersecurity Standards
  - Cybersecurity fundamentals
  - ISO 42001:2023

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Sector use cases: how the CRA shows up in real products

CRA training session

Medical IoT device and **Connected household robot**

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

Sector use cases: how the CRA shows up in real products

From regulation text to real devices

- One regulation, very different products
- Example 1: Medical IoT device
- Example 2: Connected household robot
- Focus: risk, vulnerabilities and practical implications

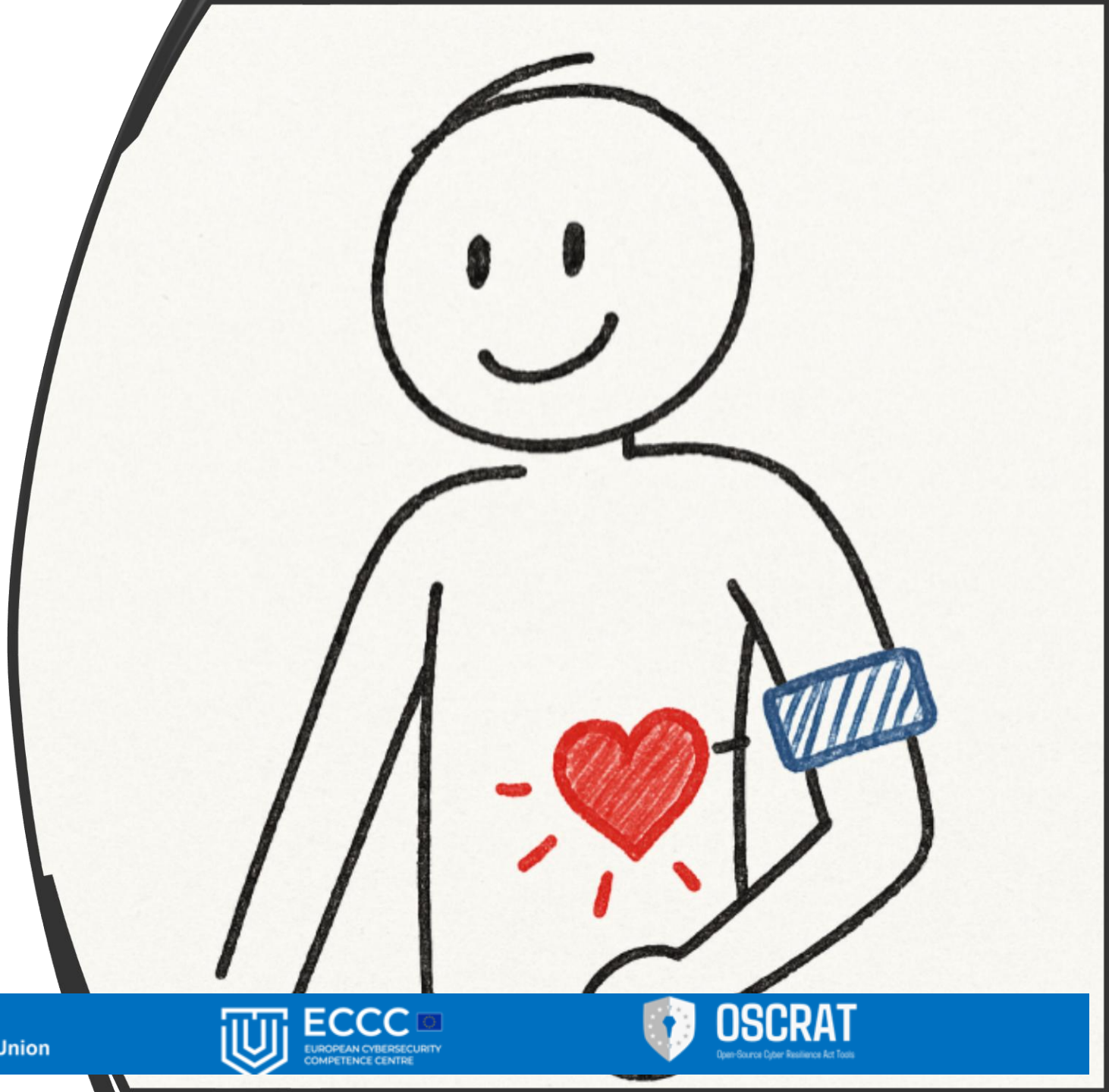
How we'll look at the cases

A simple lens for CRA product analysis

- What is the product and where is it used?
- Which regulations and standards apply?
- What are the key risks and typical vulnerabilities?
- How does the CRA affect design, maintenance and documentation?

Case 1: Medical IoT – context

- Remote patient monitoring device (e.g. wearable or home device)
- Sends medical data to a hospital or healthcare provider
- Part of a wider healthcare ecosystem (patient – device – backend – clinician)
- In scope of the CRA as a product with digital elements
- Also impacted by healthcare regulations (e.g. medical devices, NIS-type rules for hospitals)



Medical IoT: risk and CRA-driven requirements

Medical IoT: risk and CRA expectations

Key risks:

- Compromised or manipulated medical data
- Service unavailable at a critical moment
- Unauthorised access to sensitive health information
- Malicious change of device behaviour or parameters

How the CRA shows up here:

Secure-by-design

strong authentication and protected communication
minimised attack surface and least-privilege access

Updates & patches

security updates without interrupting life-critical functions
tested, documented and planned update rollout

Logging & monitoring

logs for access and security-relevant events
monitoring to detect anomalies and abuse

Vulnerability management

process for handling known vulnerabilities (CVE, SBOM)
structured communication with hospitals and users on critical issues

High safety and data protection impact → stricter requirements in practice.

Case 2: Household robot – context

- Consumer robot used at home (e.g. cleaning robot or home assistant)
- Connected to the internet and/or smart home ecosystem
- Uses sensors and often cameras/microphones + a mobile app
- In scope of the CRA as a product with digital elements
- Typically aligned with consumer IoT security expectations

Household robot: risk and CRA-driven requirements

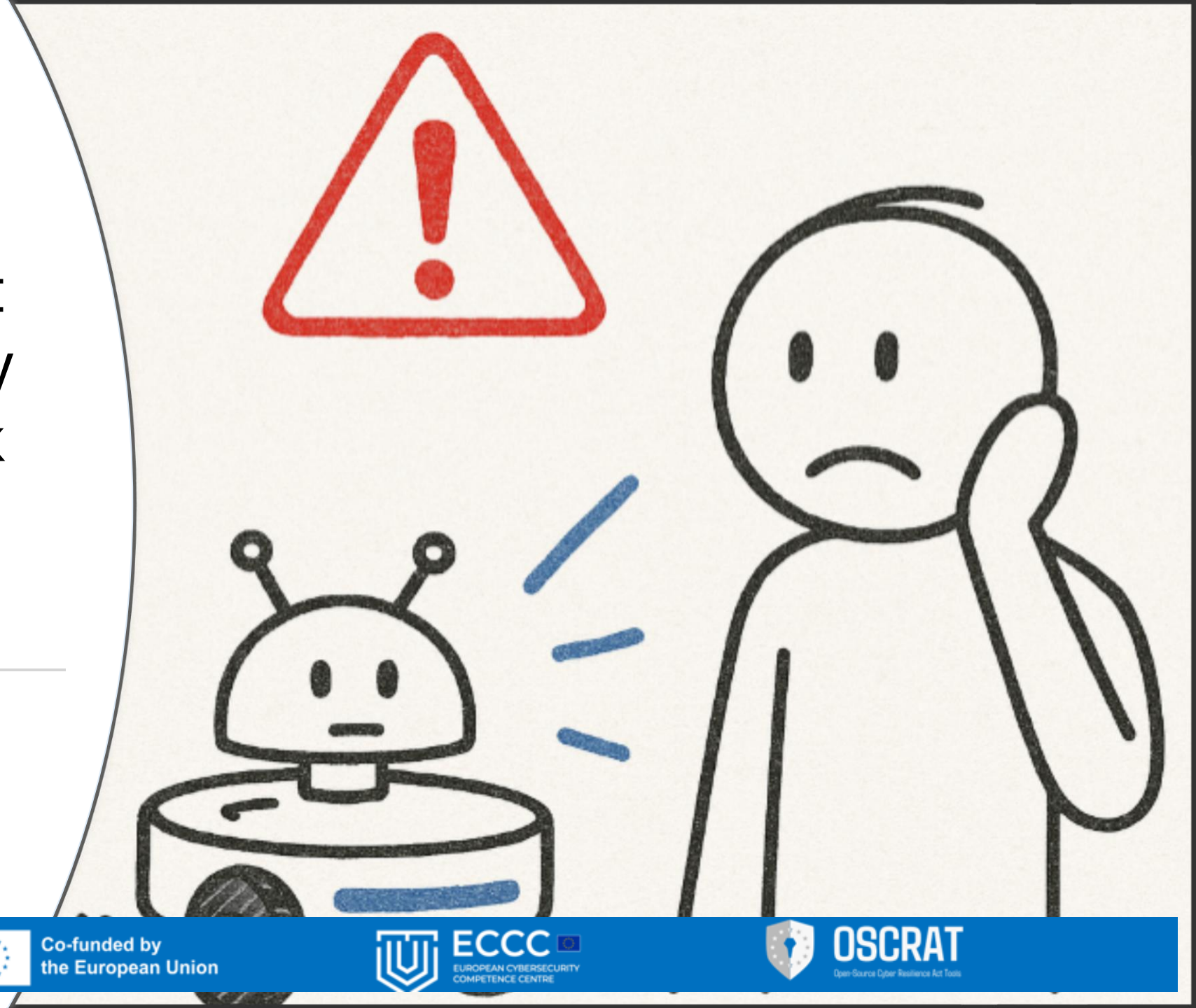
Key risks:

- Remote access to camera or microphone (surveillance/privacy)
- Lateral movement into the home network (pivot to other devices)
- Manipulation of behaviour (mapping the home, unsafe movement)
- Insecure mobile app or cloud backend exposing user data

How the CRA shows up here:

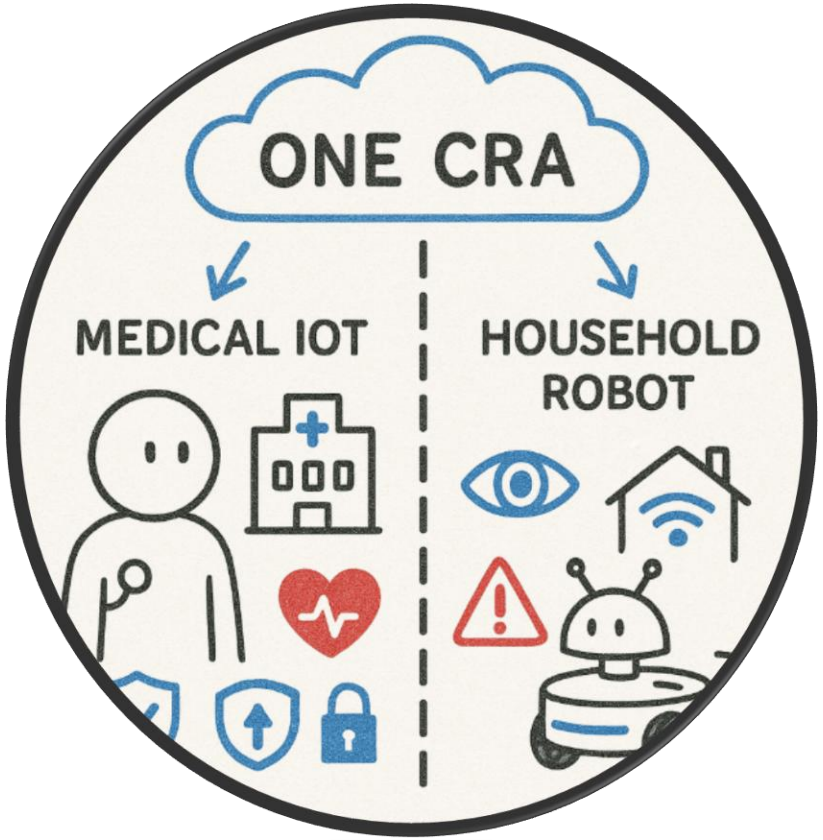
- **Secure configuration & defaults**
  - no weak/default passwords
  - secure onboarding and pairing process
- **Secure communication & updates**
  - encrypted communication with app/cloud backend
  - signed and trusted firmware/software updates
- **Vulnerability management**
  - tracking vulnerabilities in third-party components (SBOM)
  - timely security patches and clear update policy
- **User-facing security information**
  - transparent support and update lifetime
  - clear communication on serious vulnerabilities and fixes

Here the dominant themes are privacy and home network exposure, not patient safety.



Key takeaways

•One CRA, but different impact in healthcare vs. consumer smart home
•Same horizontal principles: secure-by-design, updates, vulnerability handling
•Medical IoT → safety-critical, regulated healthcare environment
•Household robot → privacy, consumer protection and home network security
•In both cases, the CRA pushes structured processes, not just ‘best effort’



Next, we'll zoom in on the CRA obligations around vulnerabilities: patch management, monitoring and reporting

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Vulnerabilities under the CRA: Patch, Monitor, Repor

CRA training session

Goal: Give participants a clear mental model of what CRA expects around vulnerabilities, tied back to the Medical IoT and Household robot examples.

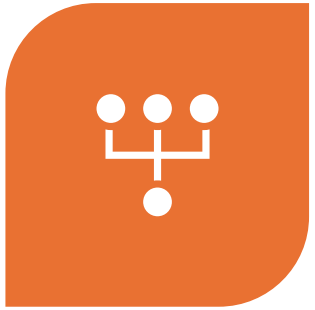
Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

Vulnerabilities under the CRA: Patch – Monitor – Report



FROM “WE’LL FIX IT WHEN WE CAN” TO STRUCTURED OBLIGATIONS

CRA = EXPLICIT DUTIES AROUND VULNERABILITIES

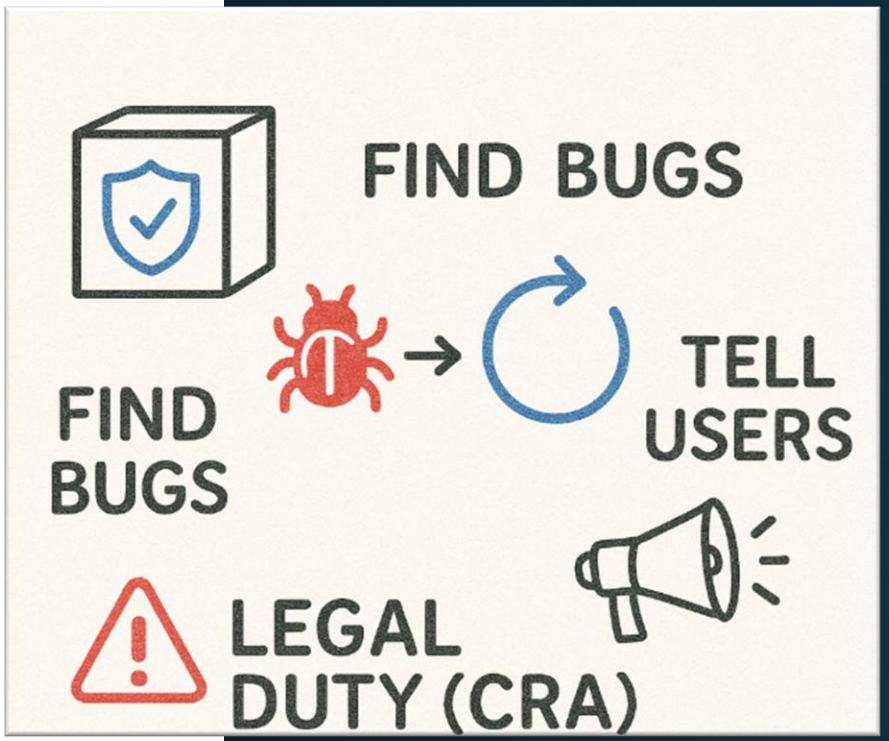
THREE KEYWORDS: **PATCH – MONITOR – REPORT**

WE’LL SEE WHAT THIS MEANS FOR REAL PRODUCTS

Big picture: CRA and vulnerabilities

What the CRA expects around vulnerabilities

- Products must be designed to handle vulnerabilities over their life cycle
- Manufacturers must:
  - detect and assess vulnerabilities
  - provide security updates within a reasonable time
  - inform users and, in serious cases, authorities
- This is not just “best practice” anymore – it’s a legal obligation



P = Patch management

What it means:

- Defined process for security updates
- Patches are prioritised based on risk
- Updates are **tested**, documented and traceable
- Clear support period for security updates

In our use cases:

- **Medical IoT device**
  - updates must not interrupt life-critical functions
  - downtime and rollbacks need careful planning
- **Household robot**
  - convenient and secure update mechanism for consumers
  - no risky “silent” updates that break core functions

If you can’t show a structured patch process, you’ll struggle to show CRA conformity.

M = Monitoring

What it means:

•Monitoring for:

- new vulnerabilities in components (CVE, libraries, OS, firmware)
- abnormal behaviour and security events in the field

•Using **SBOM** (software bill of materials) or similar to know what you run

•Feeding monitoring results back into risk assessment and patch planning

In our use cases:

•**Medical IoT device**

- watch for vulnerabilities in comms stacks, OS, crypto libraries
- monitor anomalies in device behaviour or connections to backend

•**Household robot**

- monitor cloud and app for abuse patterns
- detect suspicious access to camera/mic or control functions

Monitoring is what stops you from finding out about your vulnerabilities from Socials.

R = Reporting

What it means:

•Clear process for:

- internal escalation of serious vulnerabilities and incidents
- communication with customers/users (advisories, release notes)
- notifying authorities where required (e.g. serious, exploited issues)

•Integration with vulnerability disclosure / CVD processes

In our use cases:

•Medical IoT device

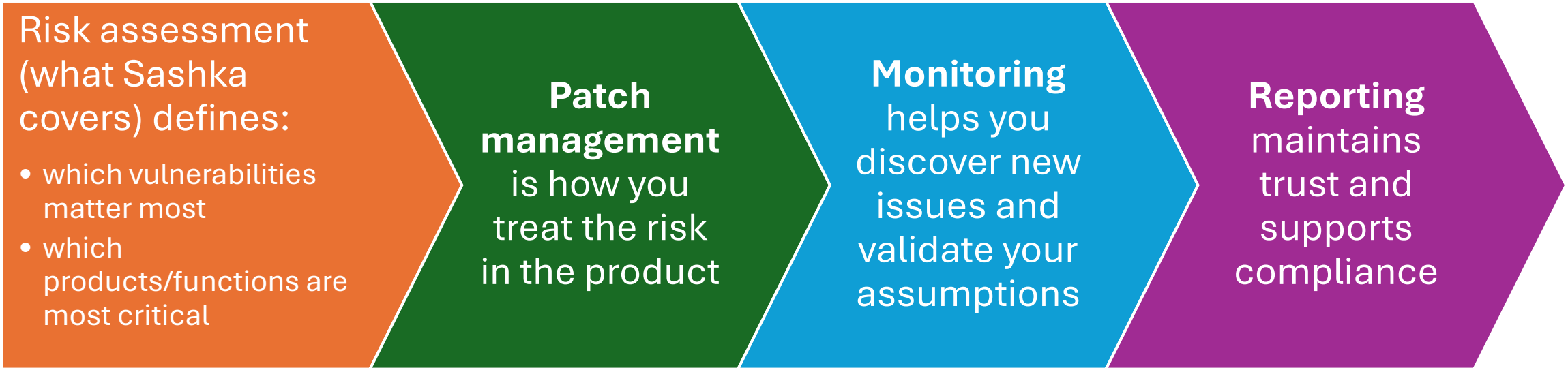
- hospitals and clinicians must know:
  - what is affected,
  - how to mitigate,
  - when a fix is available

•Household robot

- consumers need simple, understandable information:
  - “Update now – critical privacy fix”
  - support & end-of-life dates for security updates

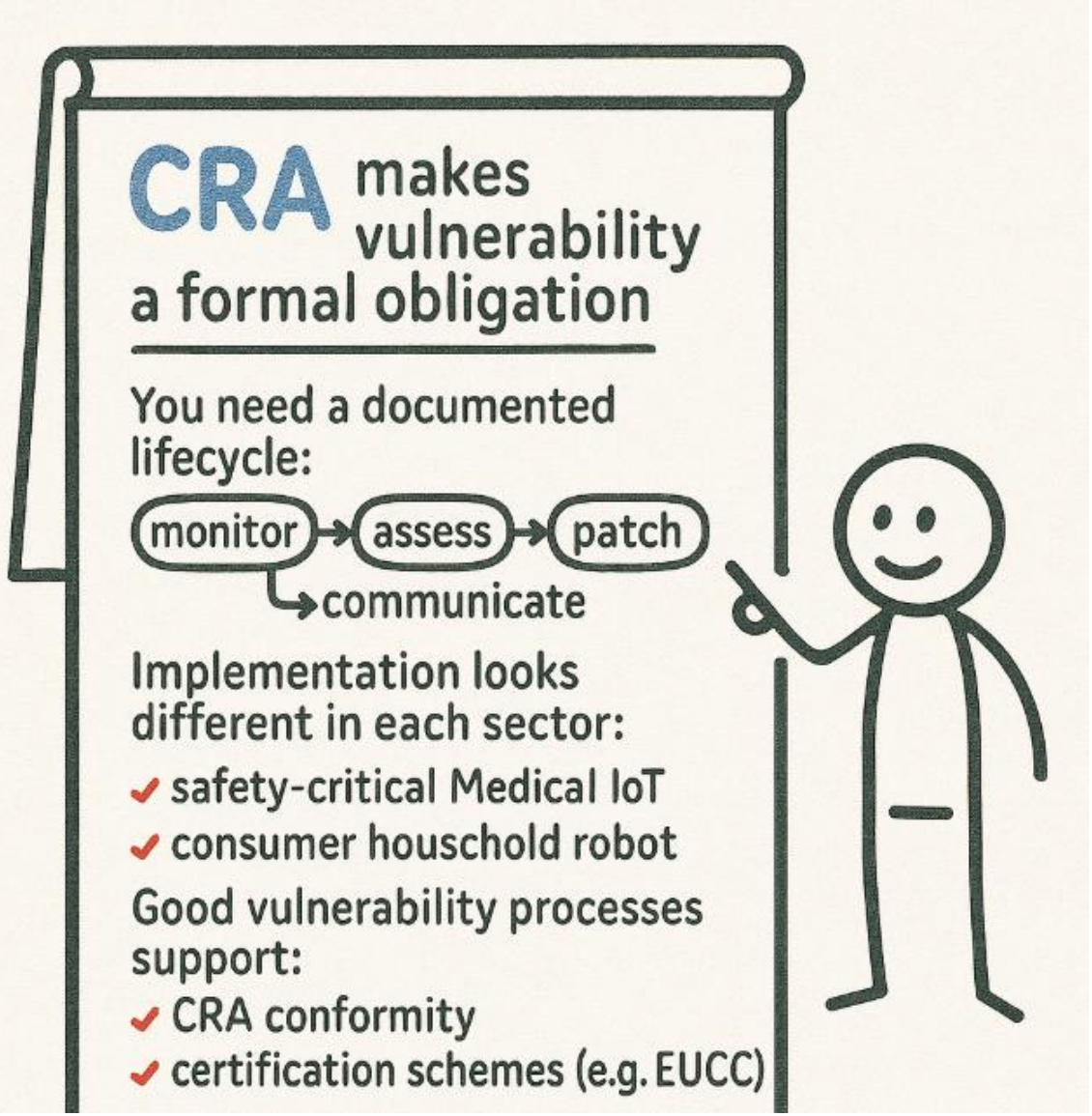
If you patch but don’t communicate, your risk is still high – users can’t act on what they don’t know.

Patch, Monitor, Report – as a risk loop



Key takeaways: vulnerabilities under the CRA

https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en



Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

The lab!

CRA training session

detailed & guided slide plan :Security Target exercise: which vulnerabilities are really covered?

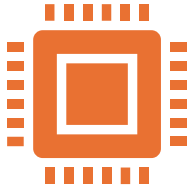
Digital Innovation Hub Trakia

Co-funded by the European Union

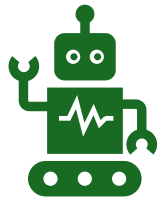
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

Security Target exercise: which vulnerabilities are really covered?



We'll look at a simplified Security Target for our household robot, and we'll see which vulnerabilities are clearly addressed – and where the gaps are.



Device: connected household robot (HomeBot 3000)

Document: Security Target (ST) for this device

Task: identify which vulnerabilities are covered – and which are not

What is an ST?

A **Security Target (ST)** is a product-specific security specification

It describes:

- the **Target of Evaluation (TOE)** – the product in scope
- threats, security objectives and security functions

Used in **Common Criteria (CC)** and **EUCC** evaluations:

- **CC (Common Criteria)** – international standard for security evaluation
- **EUCC** – EU cybersecurity certification scheme based on CC

The evaluation lab checks: *does the TOE really do what the ST claims?*

Think of the Security Target as a **security contract on paper**: what we promise the product will protect, and how. The lab evaluates the product against this document.

Our device: HomeBot 3000

TOE (Target of Evaluation): the HomeBot 3000 product being evaluated

•Includes robot firmware and mobile app
•Cloud backend is part of the operational environment, not part of the TOE
•In scope of the CRA as a product with digital elements

- This is the same device we used before. Now we look at it through the lens of a Security Target.
- The Target of Evaluation, or TOE, is simply the part of the product we are evaluating – here, the robot plus its mobile app

What is in our ST excerpt

- TOE description and assumptions about the environment
- List of assets and threats (T1–T4)
- Security objectives (O-AUTH, O-COMMS, O-UPDATE, O-AUDIT)
- Security functions (SF-AUTH, SF-COMMS, SF-UPDATE, SF-AUDIT)

These elements form a simple chain: threats → objectives → security functions.
That's the chain we want participants to review

Digital Innovation Hub Trakia
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT Open-Source Cyber Resilience Act Tools

Exercise: read the ST with a vulnerability lens

1

Step 1: Read the ST excerpt for the HomeBot 3000 (2–3 minutes)

2

Step 2: Focus on three areas:

- Authentication and account control
- Firmware updates and integrity
- Logging and monitoring

3

Step 3: For each area, answer:

- Which threats (T1–T4) are clearly covered?
- Which vulnerabilities are **not clearly addressed** in the ST?

Guided questions

Authentication & account control

- Does the **user authentication function (SF-AUTH)** really prevent unauthorised control (T1) and account takeover (T4)?

Updates & firmware integrity

- Does the **secure update function (SF-UPDATE)** protect against malicious firmware (T3)?
- Is there anything about downgrade attacks or end-of-support?

Logging & monitoring

- Does the **audit function (SF-AUDIT)** help detect abuse of control functions?
- Is misuse of camera/microphone or unusual robot behaviour covered at all?

Debrief: what is covered?

What is clearly covered by this Security Target?

What is clearly covered by this Security Target?

T1 – Unauthorised remote control

- Addressed by SF-AUTH (authentication) and SF-COMMS (protected channel)

T3 – Malicious firmware installation

- Addressed by SF-UPDATE (signed firmware, signature check)

T4 – Account takeover (partially)

- Addressed at basic level by SF-AUTH (password rules + lockout)

Traceability of actions

- Addressed by SF-AUDIT (logs for commands and updates)

Debrief: where are the gaps?

Where do we see gaps or vague areas?

Authentication:	nothing about **multi-factor authentication (MFA)** limited protection against automated brute-force attacks
Privacy and sensors:	camera and microphone protection not explicitly described no clear policy on what data is stored and for how long
Monitoring and behaviour:	SF-AUDIT logs events, but no description of analysis or alerting
Lifecycle:	ST does not say how long security updates are provided no mention of vulnerability disclosure or communication with users/authorities

From ST to CRA

From Security Target to CRA obligations

A good **Security Target (ST)**:

- gives a structured view of threats, objectives and security functions
- is essential for **Common Criteria (CC)** and **EUCC** evaluations

The **Cyber Resilience Act (CRA)** adds:

- ongoing vulnerability handling (patching, monitoring and reporting)
- clear communication and support lifetime for security updates

Together:

ST + strong vulnerability processes = a stronger basis for CRA conformity

https://chatgpt.com/g/g-6911e1ea4b2c8191bb50982718251302-security-target-analyst-gpt

So, the ST tells us what the product promises to do. The CRA then forces us to keep those promises alive over the whole lifecycle of the product.