2 February 2025

The CHERI Alliance

Getting security embedded into electronic systems

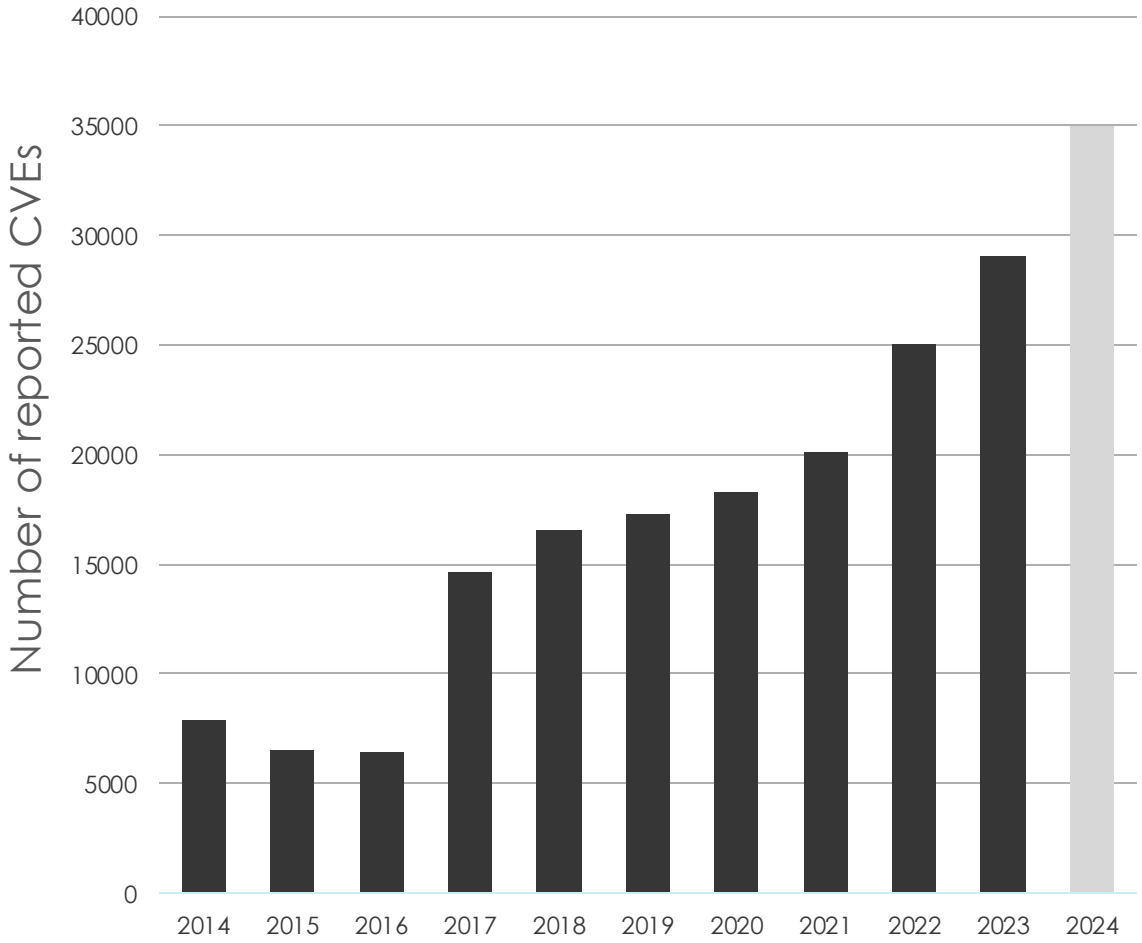
John Thomson
lowRISC – Founding Member of the CHERI Alliance

Agenda

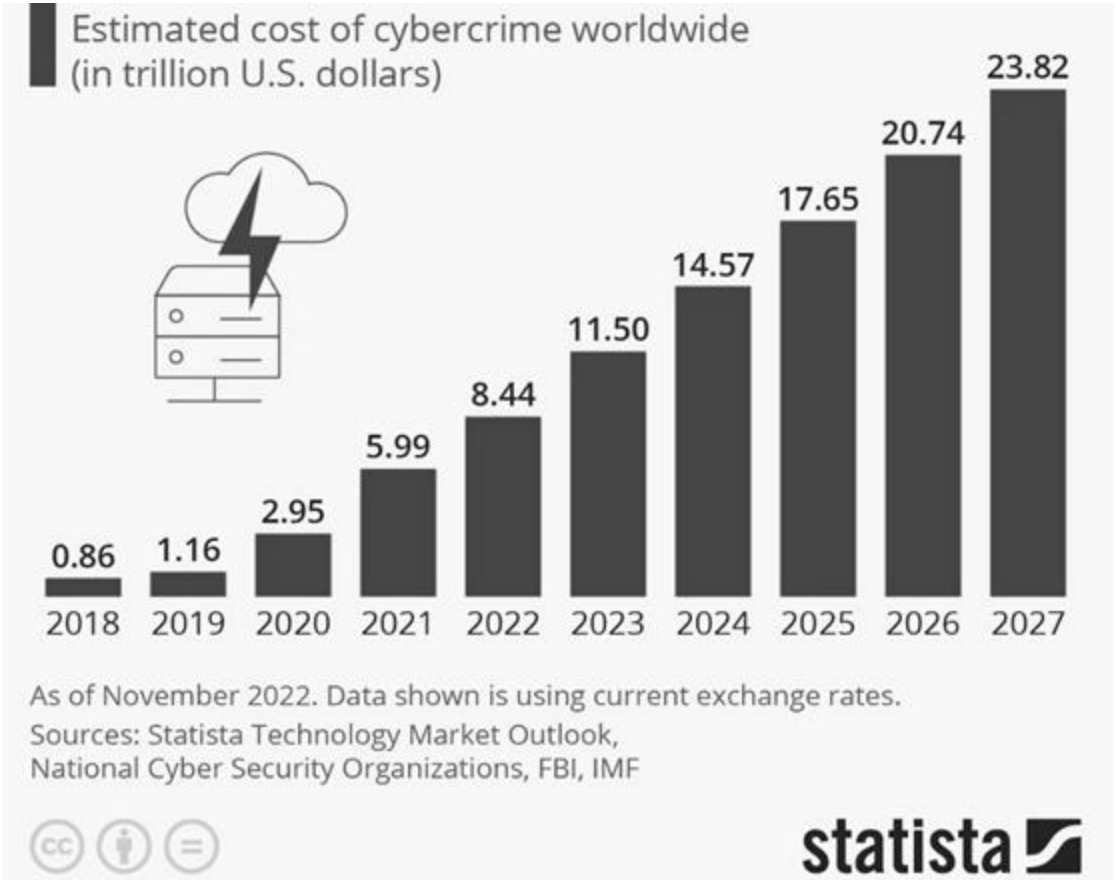
- The memory safety problem
- CHERI technology
- The CHERI Alliance

The memory safety problem

Software vulnerabilities are causing increasing risk

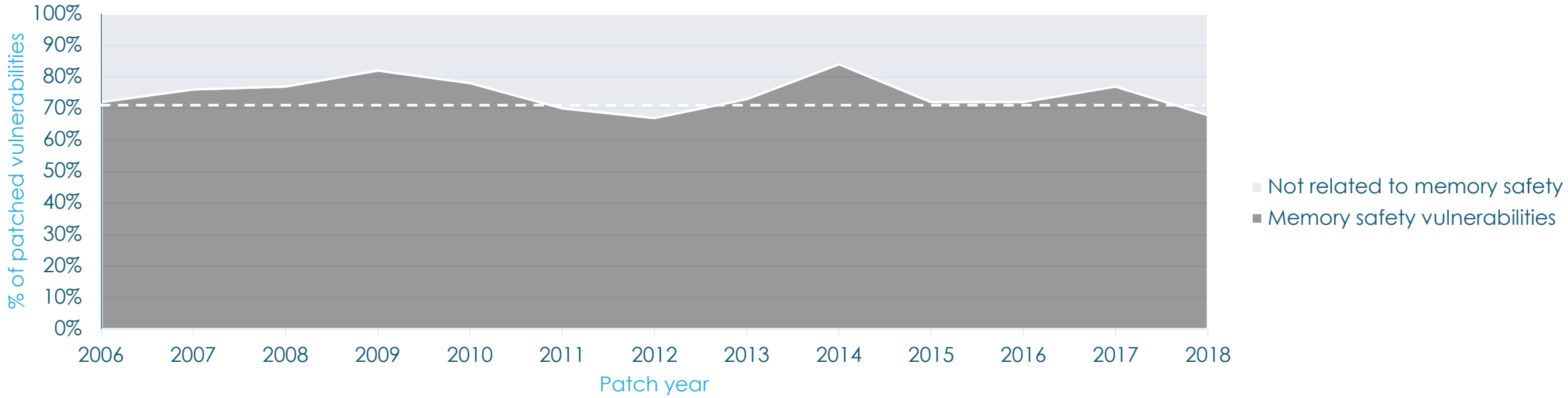


Source: Mitre



The main problem is (the lack of) memory safety

- Memory abuse (e.g. buffer overflows) is the main attack vector
- Constant ratio of over the past 20 years



Source: Trends, challenge, and shifts in software vulnerability mitigation - Microsoft 2019

Possible solutions for memory safety

✗ Use “memory safe” languages like Rust or .Net

- Requires rewriting trillions of lines of C/C++ code
- Possible for new code, but no compartmentalisation

✗ Use “coarse-grained” techniques like stack “canaries”

- Helpful, but they statistically leave too many holes
- Hacking techniques already developed

✓ Use “fine-grained” techniques like CHERI

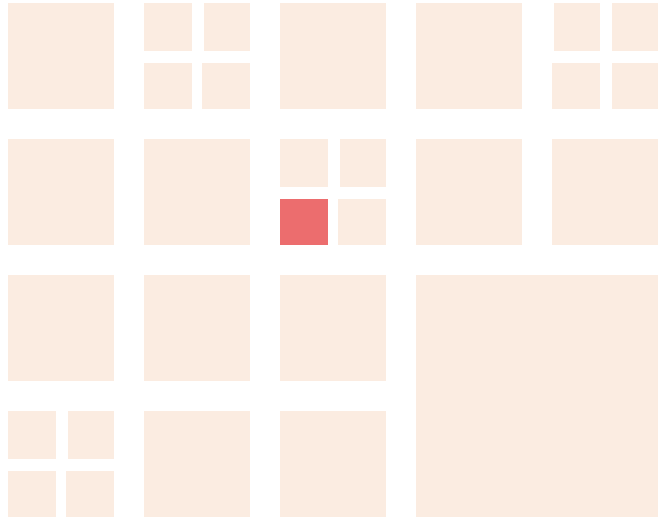
- Best option, but needs new hardware

CHERI technology

Capability
Hardware
Enhanced
RISC
Instructions

CHERI

- Benefits
  - Deterministic, fine-grained **memory protection**
  - Scalable **compartmentalization**
- An architectural solution
  - Works with existing software
  - Protects software with hardware
  - Extension of conventional hardware ISAs



Compartmentalization prevents contagion

CHERI and the UK

- Initiated by a project from

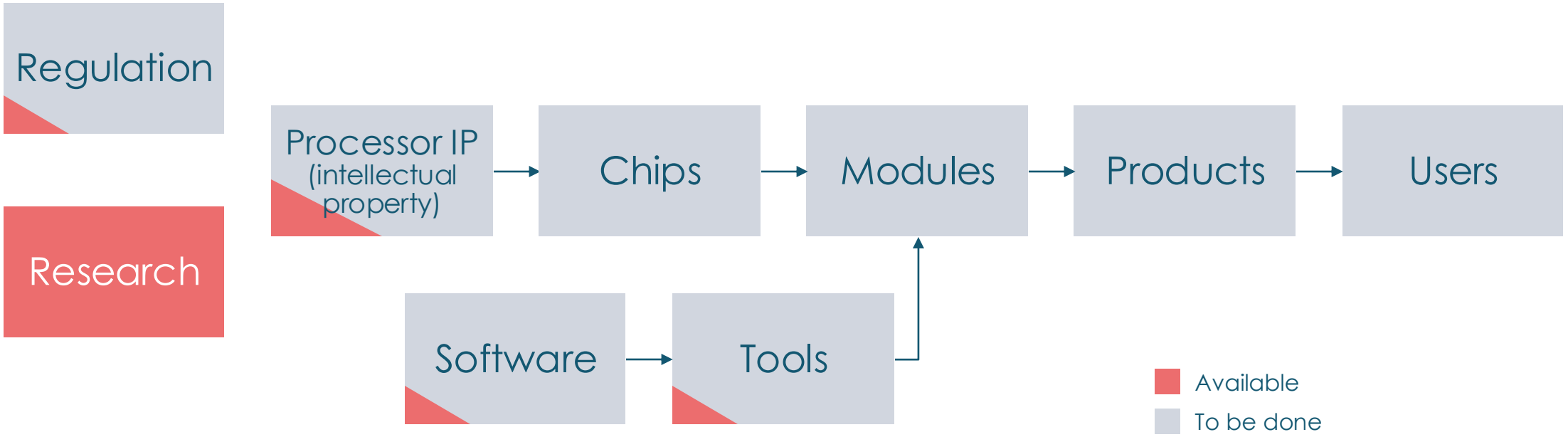
- Originally developed by

- Matured for 14 years
- Supported by

Getting CHERI adopted

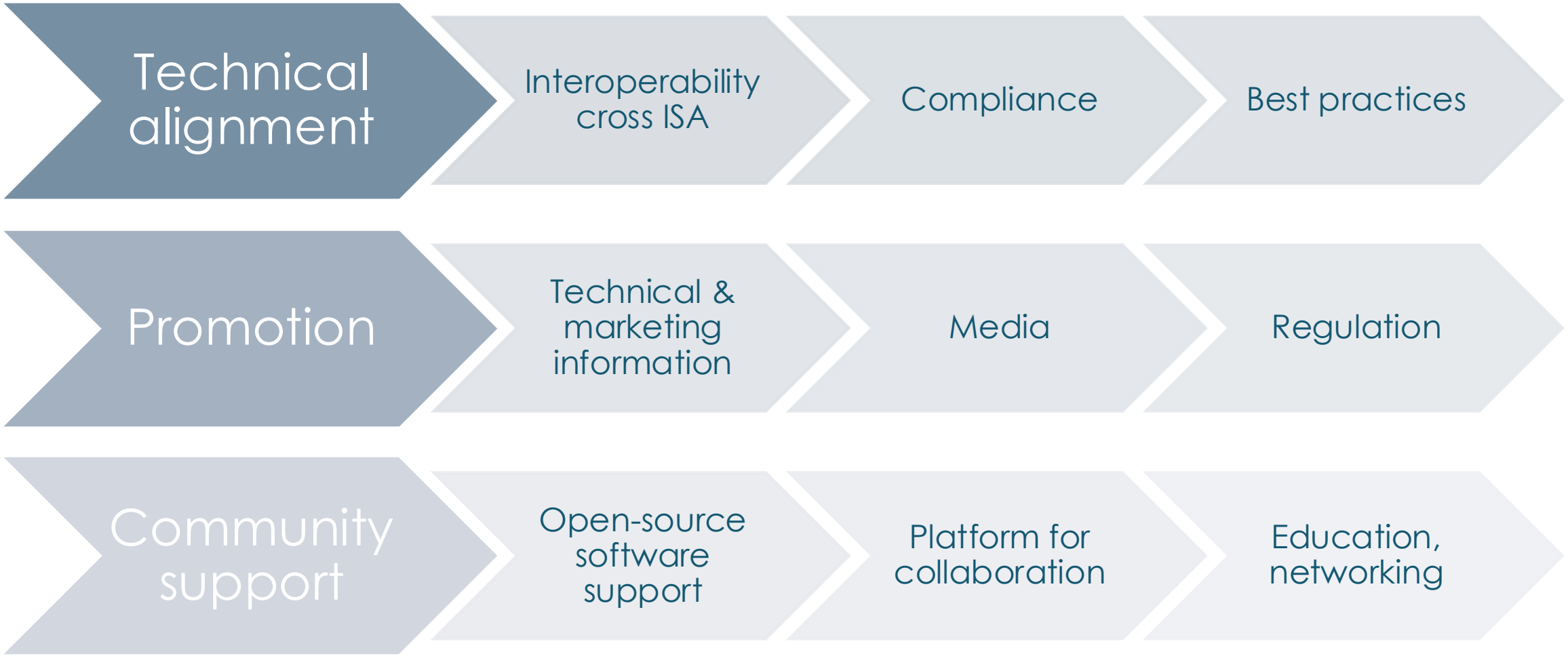
Show benefits
Make it easy to adopt
Highlight risks (lack of security / upcoming regulations)

How to stimulate the industry?



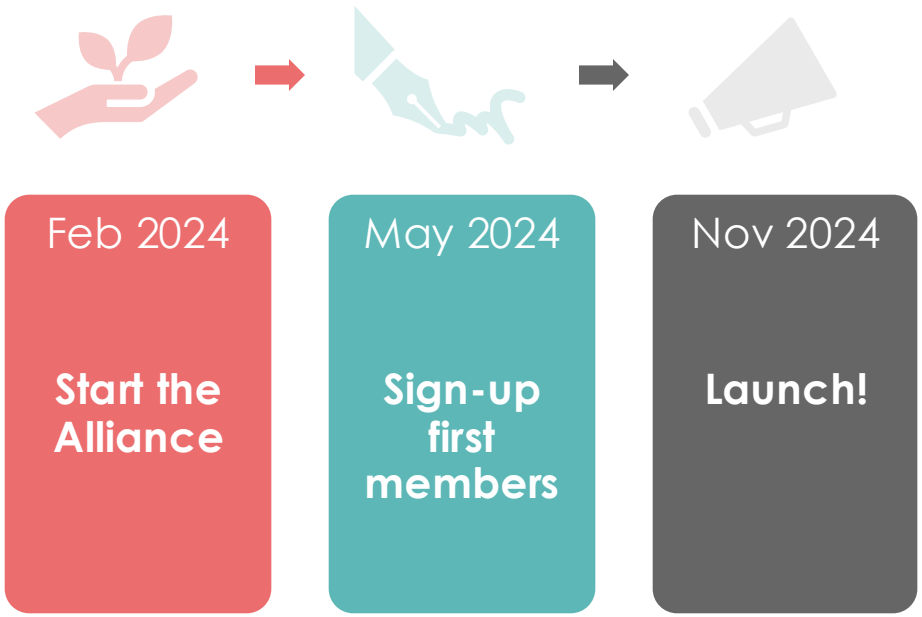
The CHERI Alliance

Role of the CHERI Alliance



An independent entity

- ISA-agnostic
  - CHERI could be added to Arm, x86, MIPS, RISC-V, …
- Worldwide reach
- Not just one company
  - Need broad industry adoption
  - Need a community
- Financed by the industry*



* with financial support from

Department for Science, Innovation, & Technology

Founding members of the CHERI Alliance

CHERI and the UK

- Largely developed by University of Cambridge
  - Involvement of many other UK universities
- Strong local expertise
  - E.g. CHERI design teams located in Bristol, Cambridge, …
- Support by

[dstl]

National Cyber Security Centre
a part of GCHQ

Department for Science, Innovation, & Technology

UK Research and Innovation

Benefits for members

Demonstrate security leadership

Network, collaborate and exchange

Accelerate adoption of CHERI

Share promotion costs

Activate the community

Join us!

CHERI

THANK YOU

Contact contact@cheri-alliance.org

Web www.cheri-alliance.org

This work © 2025 by CHERI Alliance is licensed under CC BY-SA 4.0 (Creative Commons Attribution-ShareAlike 4.0 International) – https://creativecommons.org/licenses/by-sa/4.0/