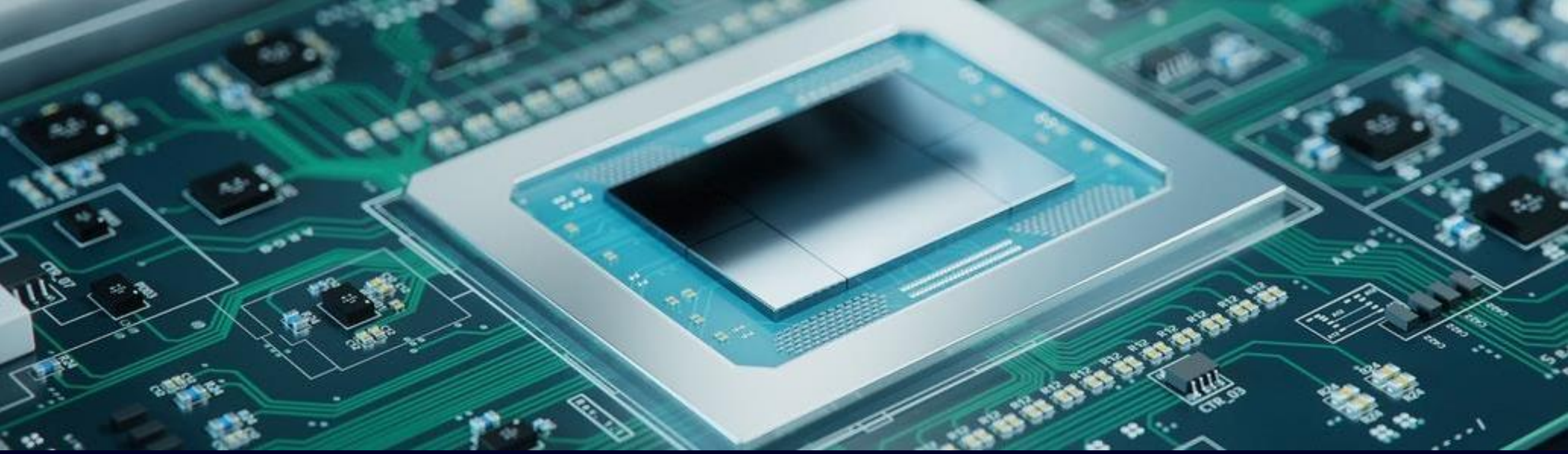


With Cheri, can we afford to ignore Hardware Security?

Joerg Bormann, CheriTech, November 2026

Unrestricted | © Siemens 2026 | Siemens Digital Industries Software

SIEMENS

Global Impact of Cybersecurity



USD 10.5 trillion by 2025
(= 1.05 * 10^{13})

estimated global annual cost of cybercrime



Hardware and Software products

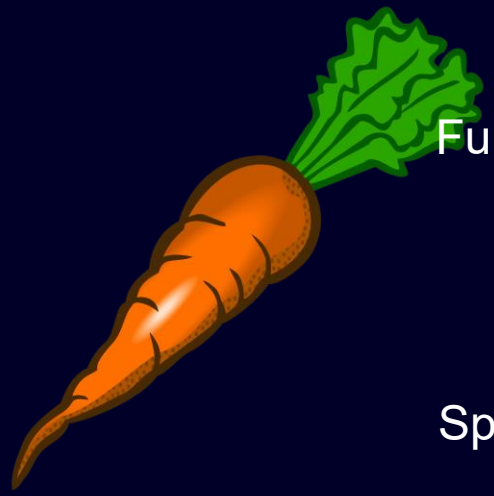
are the main targets of cyber attacks

Cyber attacks must be considered part of the normal execution environment of a digital product.

Unrestricted | © Siemens 2026 | Siemens Digital Industries Software

Source: https://cybersecurityventures.com/cyberwarfare-report-intrusion/

Governments respond with Carrots and Sticks



pngitem.com

Funding projects, e.g.

Scale4Edge
FKZ 16ME0124

VE-VIDES
FKZ 16ME0248

Special efforts, e.g.

cyberagentur



creativefabrica.com

Regulations



EU Cyber Resilience Act

Unrestricted | © Siemens 2026 | Siemens Digital Industries Software

SIEMENS

EU Cyber Resilience Act

For manufacturers, importers, distributors of products with digital elements.

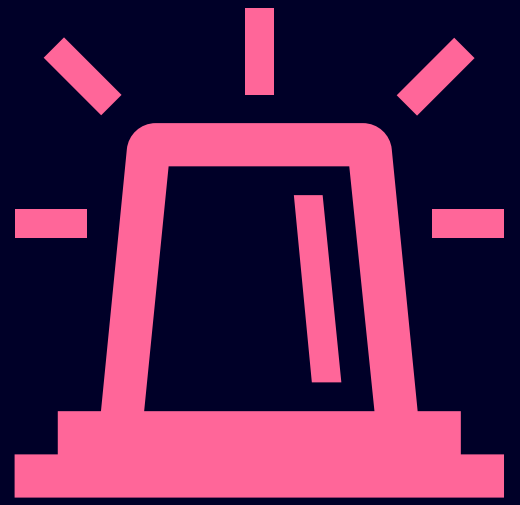
Requires:

- Design security into the product
- User documentation about secure deployment
- Report vulnerabilities and mitigations asap.

Introduction started Dec 11, 2024

- Fully effective from Dec 11, 2027

Fines: Up to 2.5% of worldwide annual turnover.



Unrestricted | © Siemens 2026 | Siemens Digital Industries Software

Why Formal Verification of HW Security?

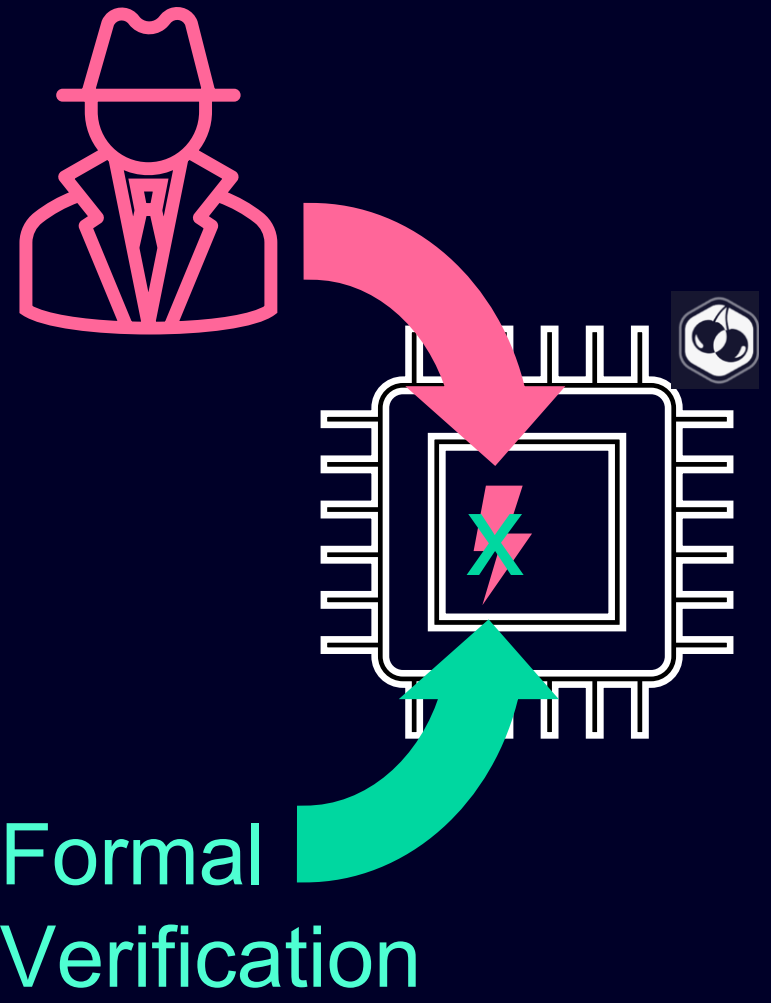
"Cheri allows to implement security in software ...
Isn't there a SW fix for every security issue of a Cheri based system?"

NO. CHERI *RELIES* ON HW.

Malicious modification == jackpot for an attacker.
Well hidden from RTL simulation and product test.

Formal verification helps:

- Questa GapFree: Formal verification of ***all*** functionality for ***all*** inputs.
- Every unusual I/O behavior will be detected.
- No matter how well hidden (= how rarely activated).
- ≠ Simulation
- Similar for Questa Processor and Questa Equivalence.



Unrestricted | © Siemens 2026 | Siemens Digital Industries Software

SIEMENS

Siemens EDA & Formal Security Verification

Portfolio

- Questa Verify Trust – Automated formal verification to detect basic security issues.
- Questa Verify Secure – Formal verification of security architectures
- Questa GapFree – Formal verification of all functionality of general RTL
- Questa Processor – GapFree for RISC-V
- Questa Equivalence – Detect supply chain attacks



Member of the security community

- CWE (Common Weaknesses Enumeration), HW special interest group
- IEEE P3164 standard (for security collaterals of HW IP)
- Cheri Alliance

Unrestricted | © Siemens 2026 | Siemens Digital Industries Software

SIEMENS

Call to Action

Do not rely on the security of your (Cheri) hardware!

Verify it!

With Formal!

Thank you.

Unrestricted | © Siemens 2026 | Siemens Digital Industries Software