SECURE-IC

THE SECURITY SCIENCE COMPANY

Cyber Escort Unit (CyberEU)

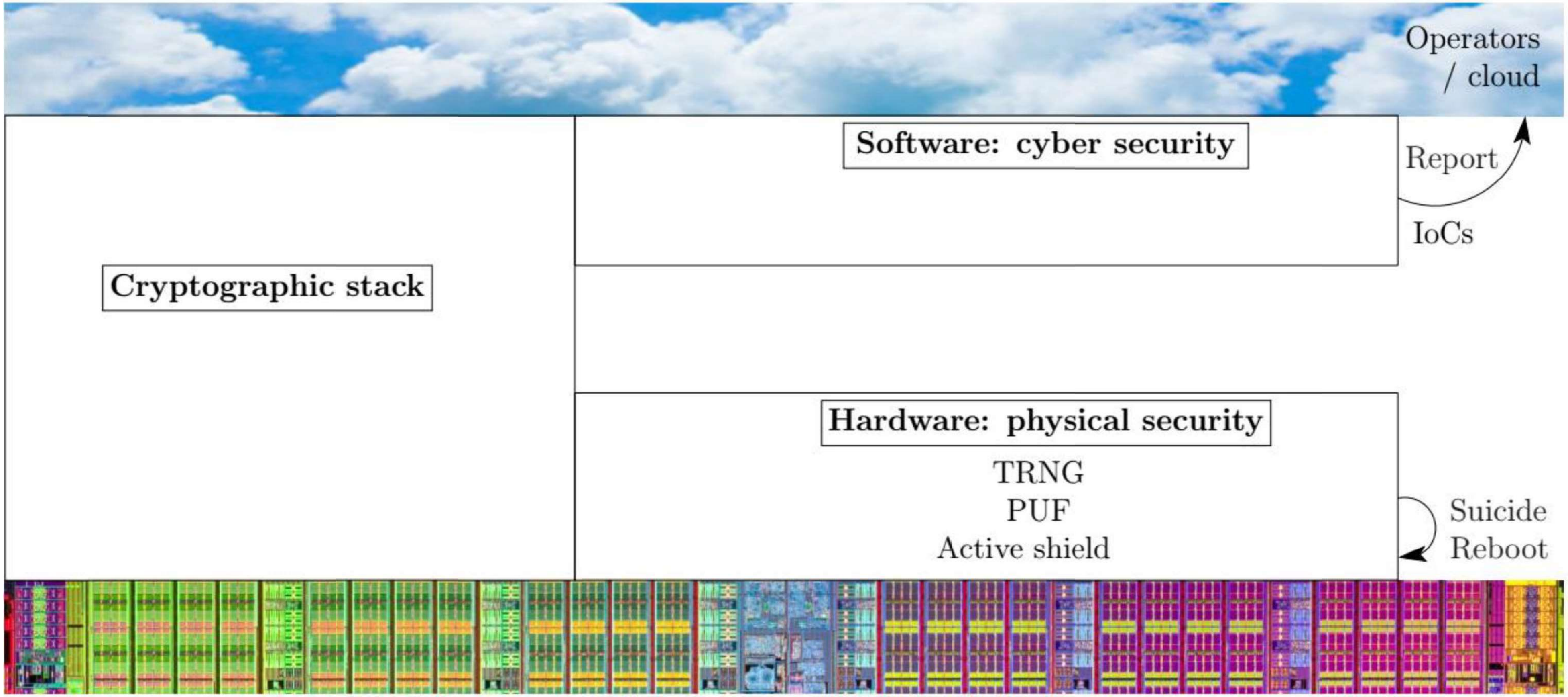
Hardware-Enabled Cyber-Security

EUROPE I APAC I AMERICAS I www.secure-ic.com I contact@secure-ic.com

CYBEREU

HW-ENABLED CYBER-SECURITY

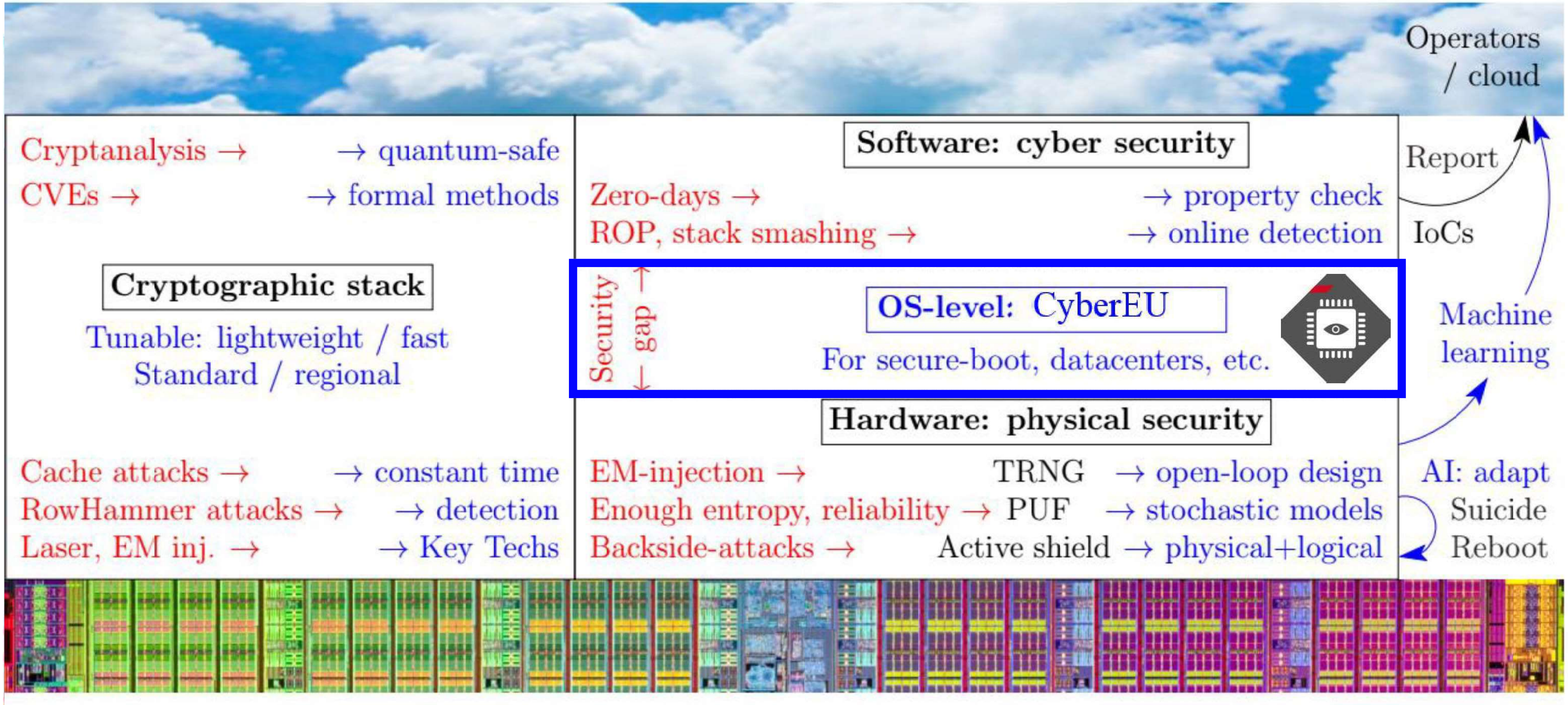
- SECURITY AT OSI LEVEL – OUR VISION



CyberEU

HW-ENABLED CYBER-SECURITY

- SECURITY AT OSI LEVEL – OUR VISION



Operators / cloud

Cryptanalysis → → quantum-safe

CVEs → → formal methods

Cryptographic stack

Tunable: lightweight / fast

Standard / regional

Cache attacks → → constant time

RowHammer attacks → → detection

Laser, EM inj. → → Key Techs

Software: cyber security

Zero-days → → property check

ROP, stack smashing → → online detection

Security ↑ gap ↓

OS-level: CyberEU

For secure-boot, datacenters, etc.

Hardware: physical security

EM-injection → TRNG → open-loop design

Enough entropy, reliability → PUF → stochastic models

Backside-attacks → Active shield → physical+logical

Report

IoCs

Machine learning

AI: adapt

Suicide

Reboot

Caption: attacks/threats in red, innovative solutions by SIC in blue.

CYBEREU

HW-ENABLED CYBER-SECURITY

- **VALUE PROPOSITION**

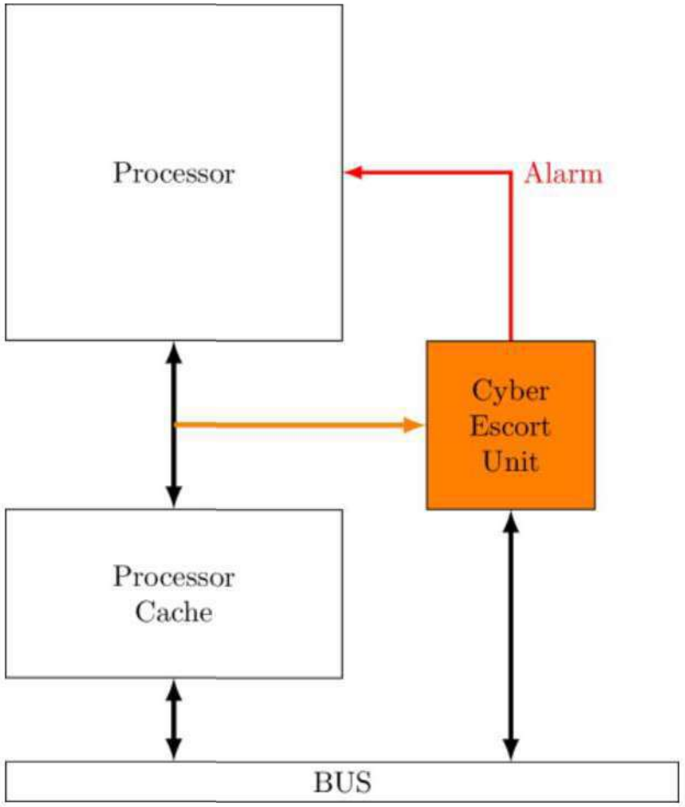
Real-time detection of 0-day attacks on code

- **BENEFITS**
  - Fill the security gap between SW cybersecurity and HW embedded security
  - High security for nearly zero impact on performance
  - Ideal for Secure Boot & protection of security-critical and crypto applications
  - Forensics reporting, threat analysis → reverse the advantage
  - Differentiator: High symbolic impact on the market
  - Think ahead: Ahead of DARPA's SSITH program

CYBEREU

HW-ENABLED CYBER-SECURITY

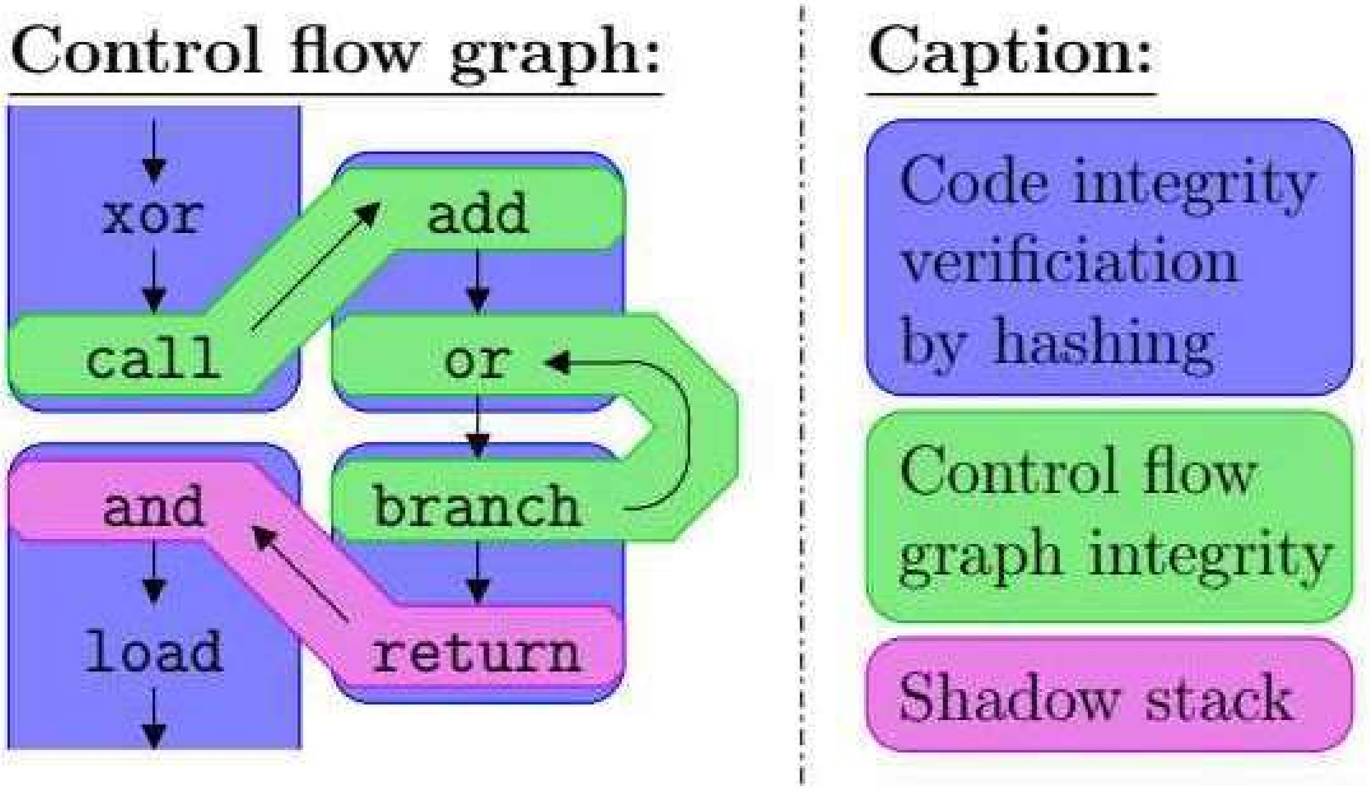
- **FEATURES**
  - No processor modification
  - Agnostic for the program
  - Real-time detection – no latency as for SW solutions
  - Resilient to cyber-attacks because inaccesible to hackers and to advanced FIA such as EMFI
  - Deployed on SPARC and RISC-V



CyberEU

HW-ENABLED CYBER-SECURITY

- **FEATURES**



CYBEREU

HW-ENABLED CYBER-SECURITY

- A TWO-FOLD TECHNOLOGY DEPENDING ON THE SECURITY YOU NEED

Secure CALL

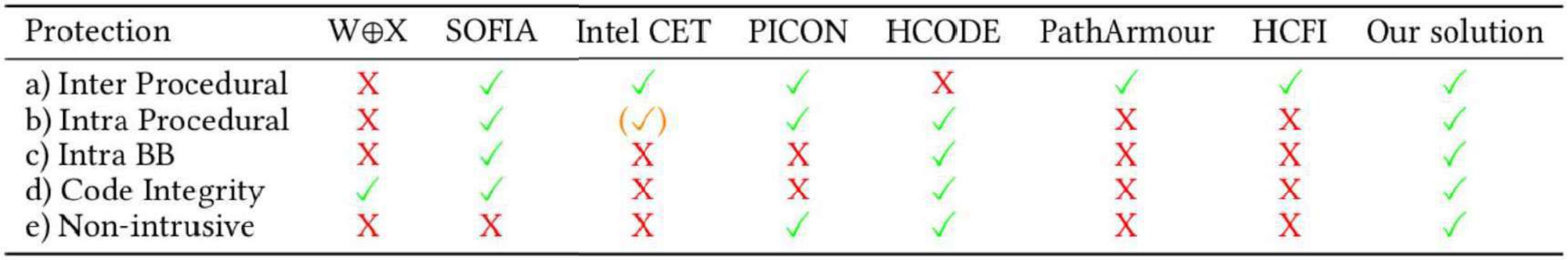
Anti- return address corruption

Execution time impact	0%
Hardware impact	12143 generic gates
Code memory fingerprint impact	0%
Need code recompilation/modification	NO

CCFI

Fine-grained code & control flow integrity

Execution time impact	~ 1%
Hardware impact	12757 generic gates + ICache size
Code memory fingerprint impact	2 times code size
Need code recompilation/modification	YES



Protection	W⊕X	SOFIA	Intel CET	PICON	HCODE	PathArmour	HCFI	Our solution
a) Inter Procedural	X	✓	✓	✓	X	✓	✓	✓
b) Intra Procedural	X	✓	(✓)	✓	✓	X	X	✓
c) Intra BB	X	✓	X	X	✓	X	X	✓
d) Code Integrity	✓	✓	X	X	✓	X	X	✓
e) Non-intrusive	X	X	X	✓	✓	X	X	✓

CYBEREU

HW-ENABLED CYBER-SECURITY

- A TWO-FOLD TECHNOLOGY DEPENDING ON THE SECURITY YOU NEED

Secure CALL

Anti- return address corruption

Protection perimeter:

- Stack smashing, via:
  - Buffer overrun
  - Integer underflow/overflow
  - Exploitation of signedness issue
- Return oriented Programming (ROP)

CCFI

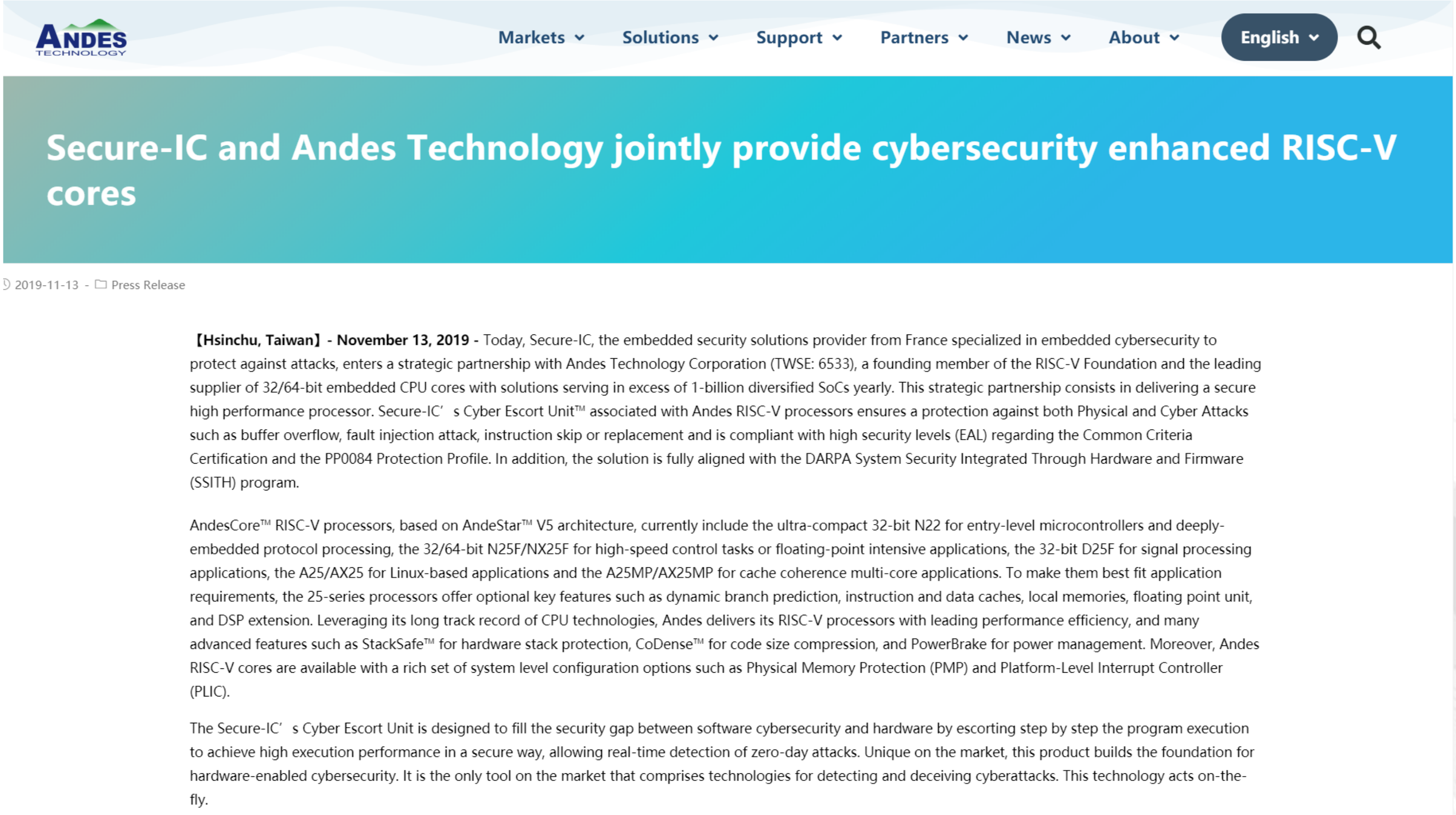
Fine-grained code & control flow integrity

Protection perimeter:

- Same as Secure CALL, plus:
- Jump oriented Programming (JOP)
- Indirect call/jump in an illicit location
- Code injection, overwritting, data/code confusion

CyberEU

DEMO AT ANDES



Secure-IC and Andes Technology jointly provide cybersecurity enhanced RISC-V cores

2019-11-13 - Press Release

【Hsinchu, Taiwan】 - November 13, 2019 - Today, Secure-IC, the embedded security solutions provider from France specialized in embedded cybersecurity to protect against attacks, enters a strategic partnership with Andes Technology Corporation (TWSE: 6533), a founding member of the RISC-V Foundation and the leading supplier of 32/64-bit embedded CPU cores with solutions serving in excess of 1-billion diversified SoCs yearly. This strategic partnership consists in delivering a secure high performance processor. Secure-IC’ s Cyber Escort Unit™ associated with Andes RISC-V processors ensures a protection against both Physical and Cyber Attacks such as buffer overflow, fault injection attack, instruction skip or replacement and is compliant with high security levels (EAL) regarding the Common Criteria Certification and the PP0084 Protection Profile. In addition, the solution is fully aligned with the DARPA System Security Integrated Through Hardware and Firmware (SSITH) program.

AndesCore™ RISC-V processors, based on AndeStar™ V5 architecture, currently include the ultra-compact 32-bit N22 for entry-level microcontrollers and deeply-embedded protocol processing, the 32/64-bit N25F/NX25F for high-speed control tasks or floating-point intensive applications, the 32-bit D25F for signal processing applications, the A25/AX25 for Linux-based applications and the A25MP/AX25MP for cache coherence multi-core applications. To make them best fit application requirements, the 25-series processors offer optional key features such as dynamic branch prediction, instruction and data caches, local memories, floating point unit, and DSP extension. Leveraging its long track record of CPU technologies, Andes delivers its RISC-V processors with leading performance efficiency, and many advanced features such as StackSafe™ for hardware stack protection, CoDense™ for code size compression, and PowerBrake for power management. Moreover, Andes RISC-V cores are available with a rich set of system level configuration options such as Physical Memory Protection (PMP) and Platform-Level Interrupt Controller (PLIC).

The Secure-IC’ s Cyber Escort Unit is designed to fill the security gap between software cybersecurity and hardware by escorting step by step the program execution to achieve high execution performance in a secure way, allowing real-time detection of zero-day attacks. Unique on the market, this product builds the foundation for hardware-enabled cybersecurity. It is the only tool on the market that comprises technologies for detecting and deceiving cyberattacks. This technology acts on-the-fly.

SECURE-iC

THE SECURITY SCIENCE COMPANY

THANKS FOR YOUR ATTENTION

CONTACT

EUROPE	sales-EU@secure-IC.com
APAC	sales-APAC@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com