ETSI
The Standards People

Security Conference

Unveiling CyberPass:
Streamlining Cybersecurity Assessment & Certification for IoT Products in Compliance with ETSI EN 303 645

Presented by:

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS

17/10/2023

Challenges

125 Bn+
of IoT Devices

2030

50%+ are vulnerable

62% of attacks exploit customers' trust in their suppliers.

> "Supply Chain attacks such as Solarwinds worry me, because I don't see at this point how we can protect ourselves from it. Even for a company that strictly follows all the recommendations of the ANSSI - and that doesn't exist - it will remain very complicated."

Guillaume Poupard,
ANSSI CEO, 2022

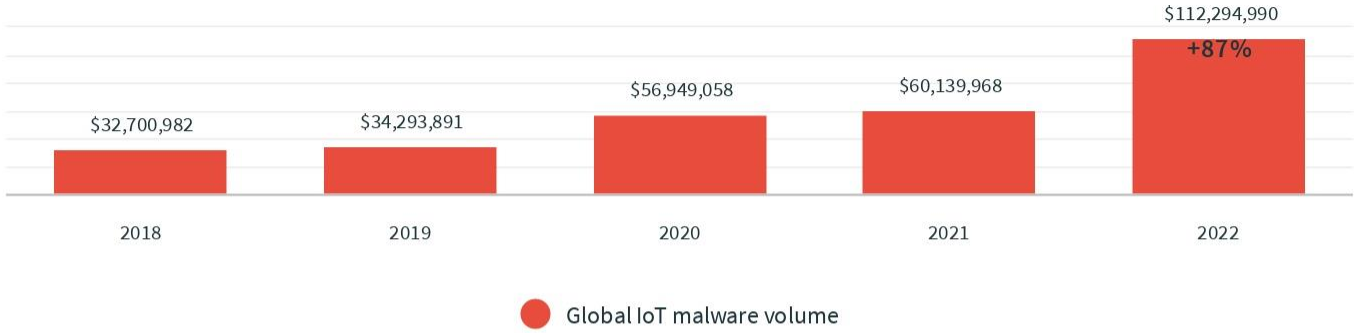
> "The lack of transparency and the inability to conduct audits (expertise, time, costs) lead to a serious a serious risk for trust within the supply chain."

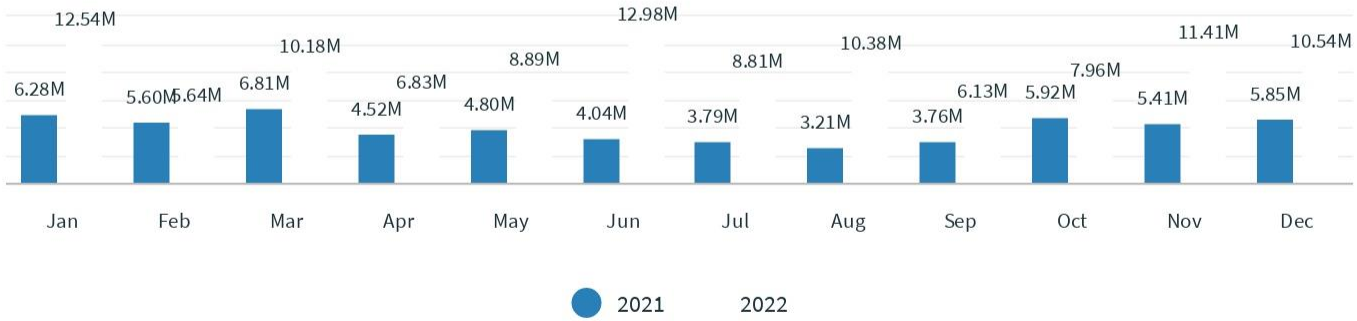
Supply Chain
report, ENISA 2021

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS

Soaring of...

IoT Malware





CYBERPASS
TRUST YOUR CONNECTED PRODUCTS

Proactive Solutions

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS

IoT risk management

Maintain an up-to-date list of connected products to identify and manage vulnerable components (SBOM)

Secure integration

Secure integration of third-party libraries; MUD file, follow best practices and standards.

Evaluation (internal or third-party labs)

Vulnerability scanners, pentesting, ...

Compliance Validation

Based on standards, regulations and certification schemes (for products and suppliers)

Anticipating and preventing problems before they arise is essential to minimize the risk of attacks on the supply chain.

But several challenges remain...

Manual and costly process

Manual supply management is cumbersome and costly. Non-Scalable!

Difficulty monitoring compliance

It's difficult to track compliance across multiple products and suppliers. Multi-Components, Multi-Standards, Multi-Regulations!

Evaluation/certification waiting times

Waiting for supplier certification prolongs the supply cycle.

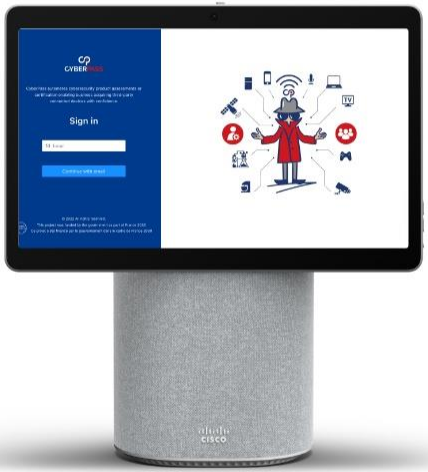
Insufficient checks

Unreliable or non-objective verification of third-party suppliers, which increases the risk of attacks

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS

The **Solution**

CYBERPASS provides enterprises with a cost-effective and scalable solution to assess and manage the level of cybersecurity of their connected products provided by third-party suppliers.



EU CYBERSECURITY ACT

COMMON CRITERIA

ETSI EN 303 645

ISA IEC

How it works ?

#1 IDENTIFIED NEED

YOU: want to buy or distribute connected cameras

#2 STANDARD SELECTION

YOU - select the standard/policy/certification and level of trust/security applicable to the target market (ex. EN 303 645)

#3 SEND REQUESTS

YOU - send request for proposal to one or several suppliers

#4 LAUNCH

The 5 suppliers receive the request by email to connect to CyberPass, and launch the evaluation procedure

#5 SELF-ASSESSMENT OR BY A THIRD-PARTY

run an assessment according to the level requested by the buyer

#6 SHARE RATING/CERTIFICATE REPORT

Purchasing Department receives the results of the 5 suppliers with a comparative dashboard

#7 TAKE INFORMED DECISION

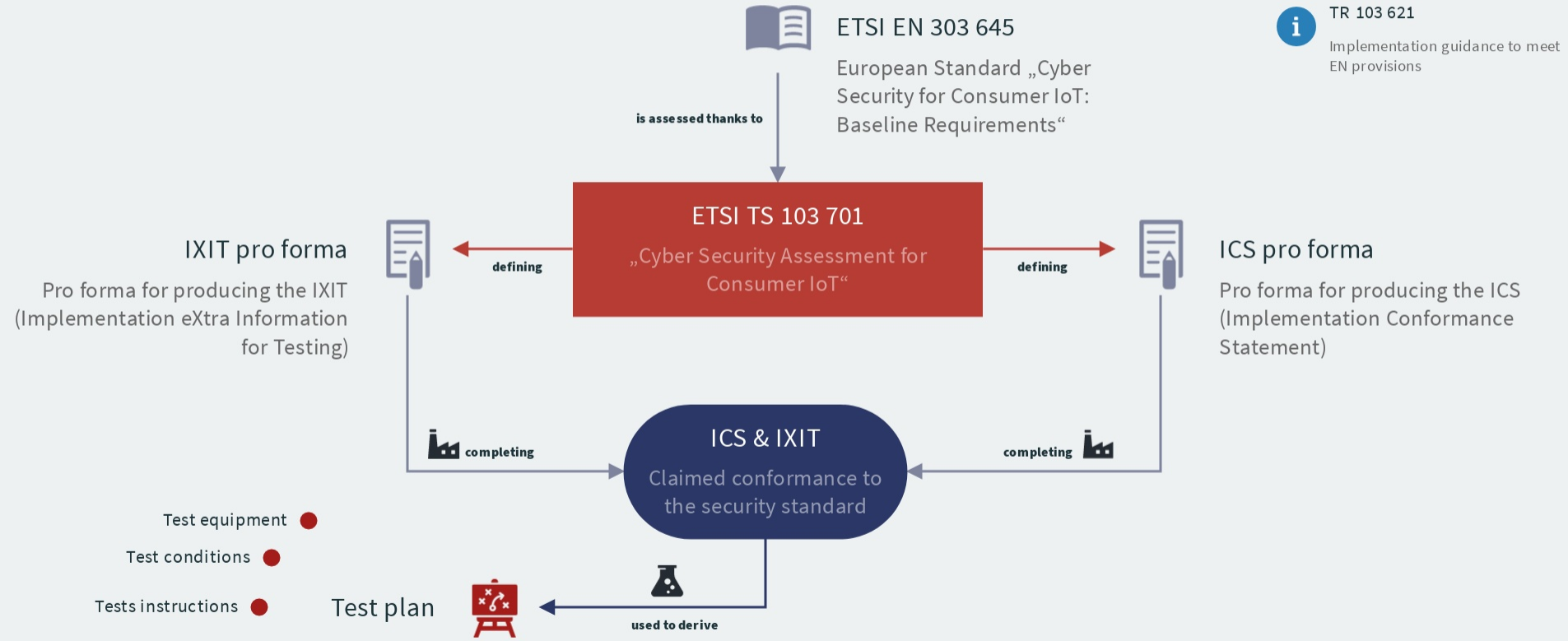
YOU - Decide on whether to buy or reject the supplier's offer-

#8 MANAGE & MAINTAIN

YOU - Monitor the conformity status of all your products

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS

Pinciples of the evaluation




Now that you finished the ICS you still have the IXIT
you are almost there! don't worry it's digital and automated
IXIT
IXIT
ICS

Evaluation Levels Selection

Based on ETSI EN 303 645

Basic

The vendor declares conformity with security requirements publicly.

Evaluation tasks:

- ✓ Public Statement of Conformity
- ✓ Consistency and Completeness
- ✓ Security Functionalities
- ✓ Evidence Documentation (ICS)

Enhanced

An independent third-party assesses the product security based on technical documentation, minimizing basic cyber risks.

Including Basic tasks, plus:

- ✓ ETSI Certification Badge
- ✓ Third-party Assessment
- ✓ Risk Assessment / Security Profile
- ✓ Secure Development Life-Cycle
- ✓ Known-vulnerabilities Assessment

Substantial

An independent third-party assesses the product security to minimize cyber risks from actors with limited skills and resources.

Including Enhanced tasks, plus:

- ✓ Evidence Documentation (IXIT)
- ✓ Conformance Testing
- ✓ Installation and Maintenance
- ✓ Cryptography Analysis

High

An independent third-party assesses the product security including penetration testing, to minimize advanced cyber attack risks from skilled actors with significant resources.

Including Substantial tasks, plus:

- ✓ Penetration Testing

CLAIMED | REVIEWED | TESTED

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS

Labels/Certificates

Based on ETSI EN 303 645

Self Declaration

Lab Reviewed

Firmware Tested

Pen-Tested

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS

The Ambiguity of Pass, Fail, and Inconclusive Outcomes

Limited Information

Pass/fail status provides limited information about the actual security of a product.

No Benchmarking

Impossible to compare the security of different products that simply have a pass status.

Unclear Scope

A pass status does not clarify what specific requirements or aspects have actually been assessed.

No Granularity

Pass/fail does not allow for risk management based on granular scoring of security posture.

No Incentives

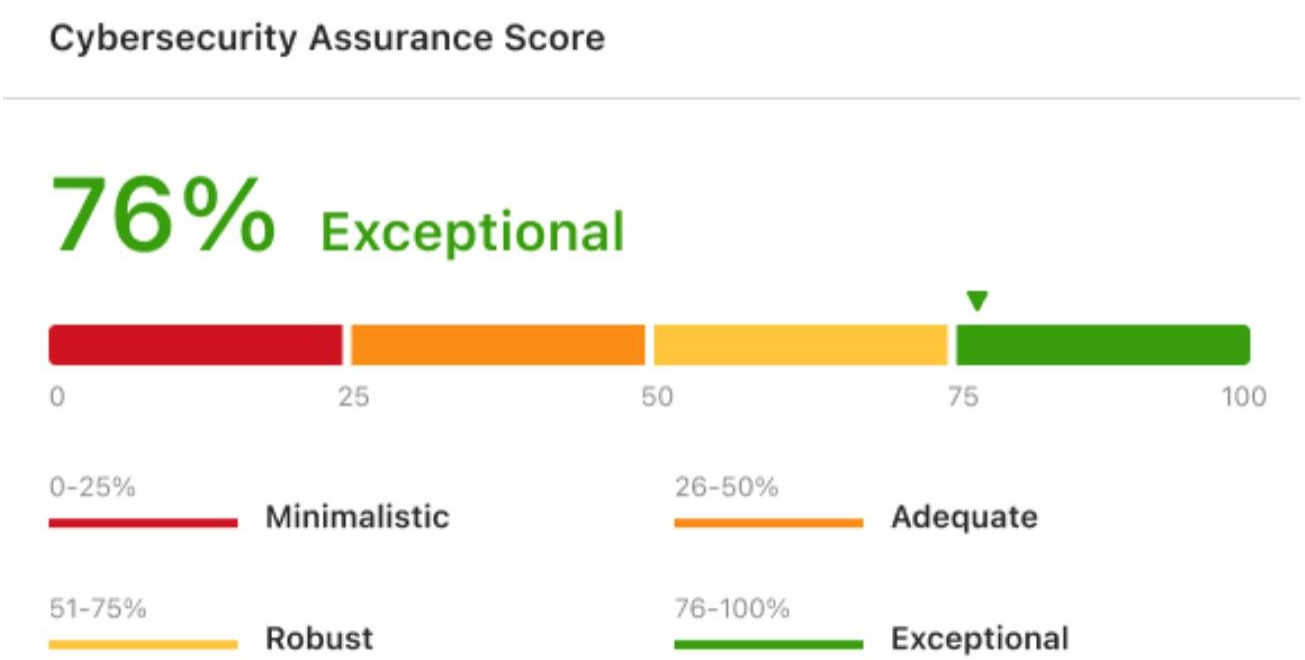
With only pass/fail, there are limited incentives for vendors to aim higher than just passing.

False Sense of Security

A passed status may provide a false sense of security for products with only basic requirements tested.

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS

Introducing Cybersecruity Assurance Score



Categories

- Minimalistic
- Adequate
- Robust
- Exceptional

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS

Added Value ?

Buyers

- Streamline cybersecurity sourcing for your products
- Centralize compliance
- Proactive risk management
- Build confidence
- Keep track of your regulatory obligations

Suppliers

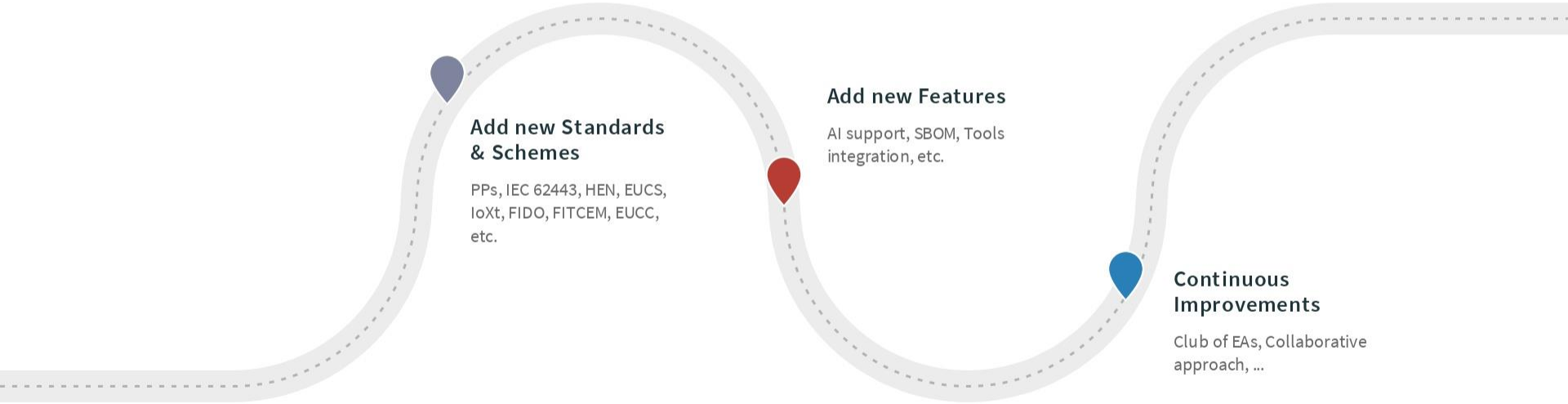
- Simplify conformity assessment and certification processes
- Extend your reach
- Centralized proof
- Keep track of your regulatory obligations
- Offer certified products
- Stand out from the competition

Laboratories

- Speed up evaluations
- Expand your market
- Improve communications
- Gain visibility in the cybersecurity industry.

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS

What's Next ?



Add new Standards & Schemes

PPs, IEC 62443, HEN, EUCS, IoXt, FIDO, FITCEM, EUCC, etc.

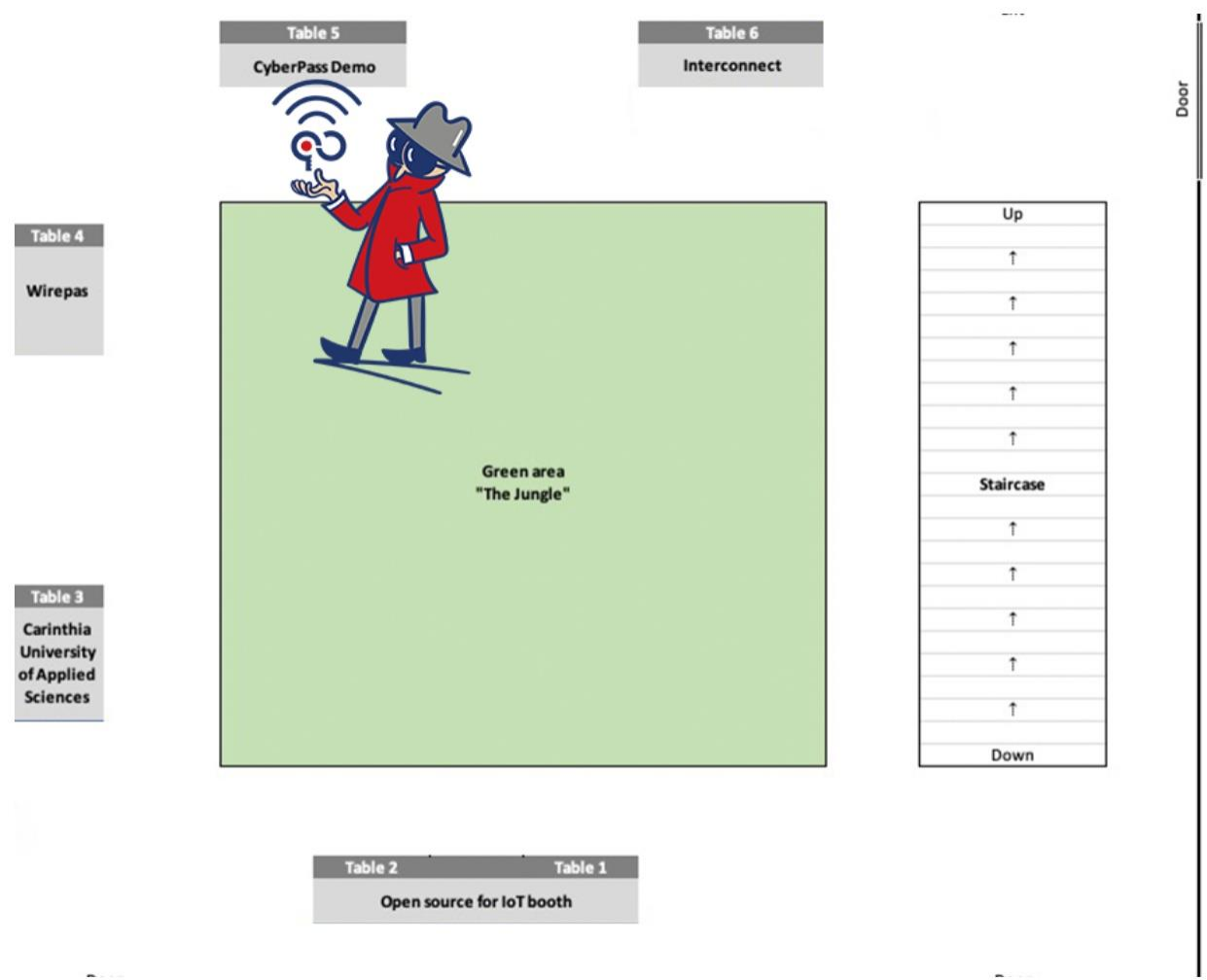
Add new Features

AI support, SBOM, Tools integration, etc.

Continuous Improvements

Club of EAs, Collaborative approach, ...

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS



CyberPass Demos

Coffee Breaks

Lunch Time

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS

Key Takeaway

Standards & Regulations

Use standards (ETSI 303 645) as often as possible to address cybersecurity by design and think about compliance and regulatory requirements to access new markets while minimizing your costs.

Anticipation

Even if directives only come into force by 2025, it is important to start incorporating them now into your processes.

E.g. “For devices that cannot have their software updated, the product should be isolable and the hardware replaceable.”

Automation

71% say their staff spends too much time on tasks that should be automated, and that number jumps to 82% among teams that say they don't have enough time for strategic tasks.

Trust Products...

Trust products and not just their suppliers.

Take accurate decisions ! Express your security needs to suppliers ! Rely on third-party when necessary.

RED ALERT LABS
IoT Security

Final quote...

> “Trust is hard. Knowing who to trust is even harder.”

Maria V. Snyder

RED ALERT LABS
IoT Security

Merci

CAMPUS CYBER - 5 rue Bellini, 92800, Puteaux, France

3 rue Parmentier, 94140, Alfortville, France

https://www.cyber-pass.eu

@RedAlertLabs

roland.atoui@redalertlabs.com

CYBERPASS

TRUST YOUR CONNECTED PRODUCTS

QUESTIONS ?