

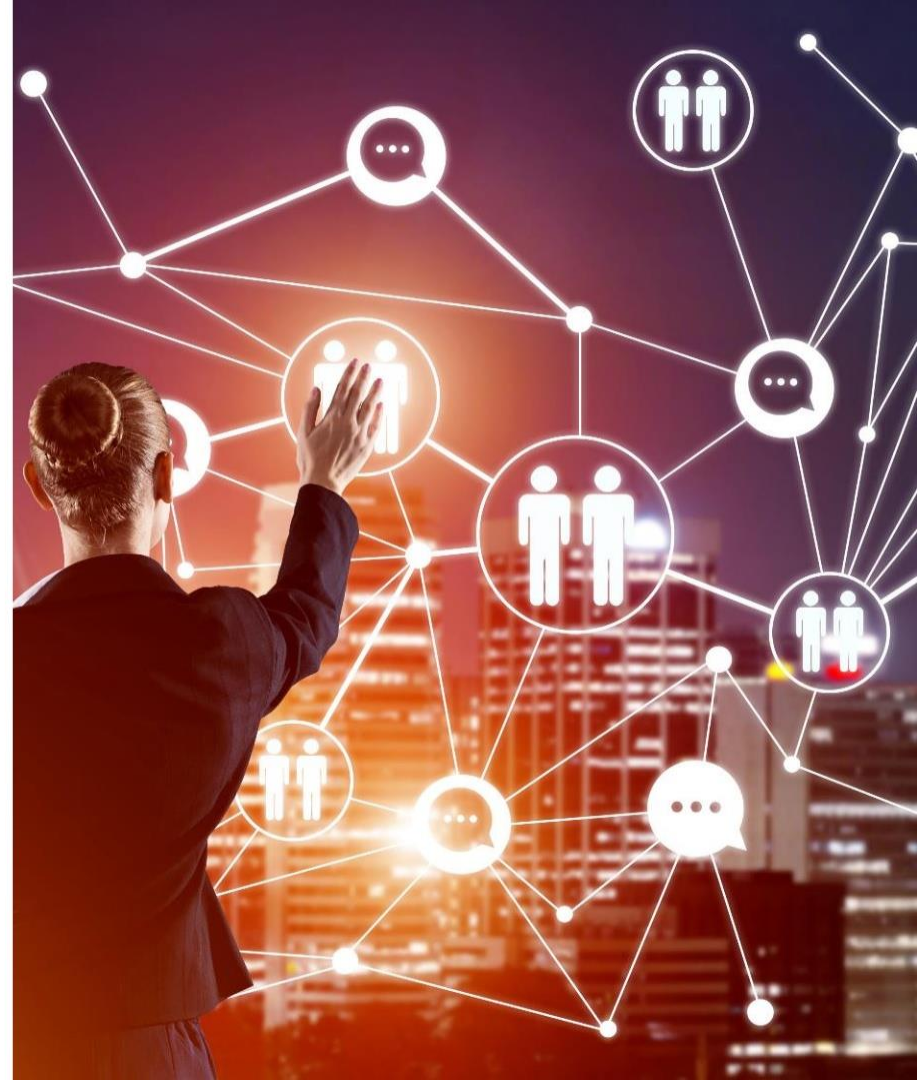
Would You Still **Trust** Your IoT Product Supplier from now on... ?

Roland Atoui | Red Alert Labs

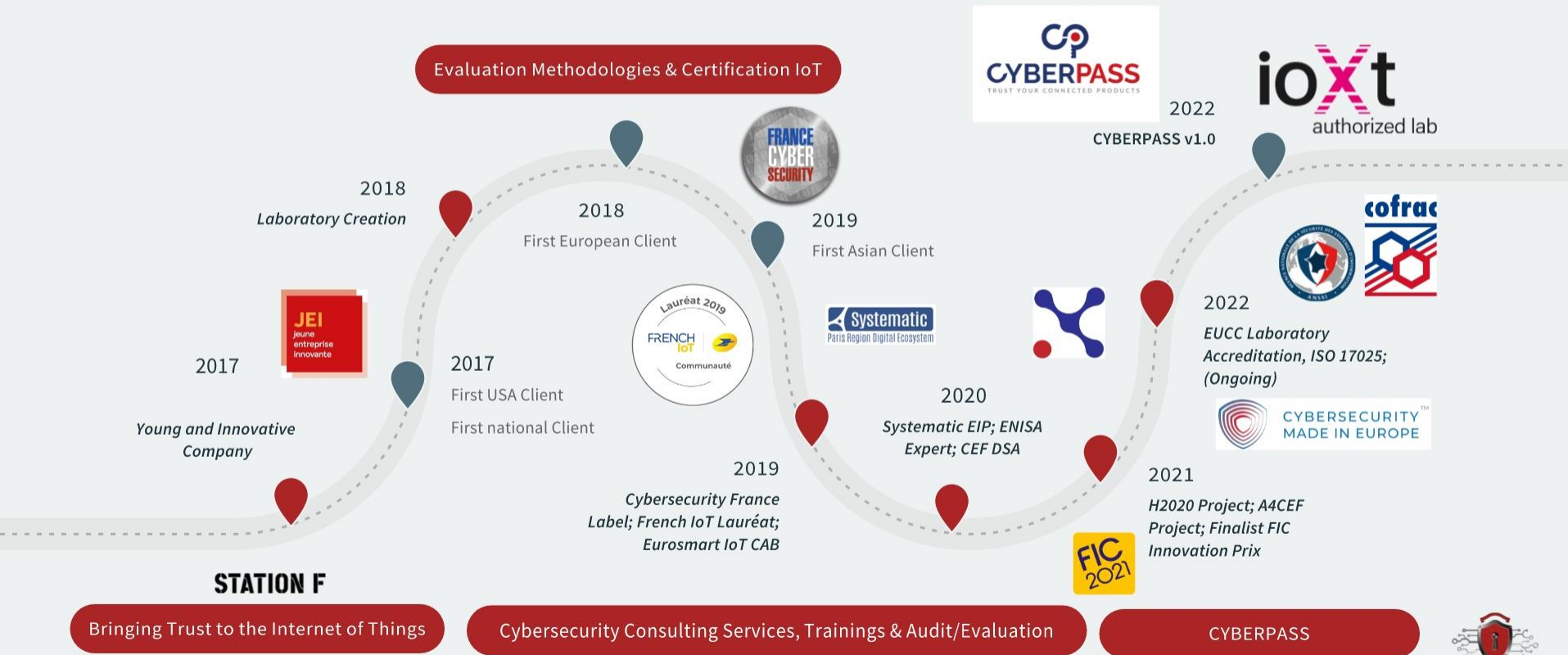
13/10/2022



RED ALERT LABS
IoT Security



Red Alert Labs



Main Challenge

60%

VULNERABLES

62%

OF ATTACKS EXPLOIT THE CUSTOMERS' TRUST WITHIN THEIR SUPPLIERS



“Lots of components made by companies all over the world are flowing across **many layers of suppliers and integrator** until they are placed under a framework, tested and packaged by OEM.”

FINITE STATE REPORT, 2019



“Because of the **attacks' cascade effect** across the supply chain, malicious actors can create damages extended to both companies and their customers.”

JUHAN LEPASSAR, ENISA



“The lack of **transparency and audits' inability** (expertise, time, costs) are causing a serious risk regarding the trust within the supply chain.”

SUPPLY CHAIN REPORT, ENISA 2021



QUESTION



So should we stop **trusting**
the **Suppliers** “themselves” ?



or

Could we, at least, find a smart
way to **trust** their **Products** ?



Trust

RISK OWNER

RISK OWNER

PRE-PROCUREMENT



Technical Means
evaluation methods, security
architecture review, code
audit and testing, ...



Legal Means
contracts
(commitment/responsibility)
and regulations

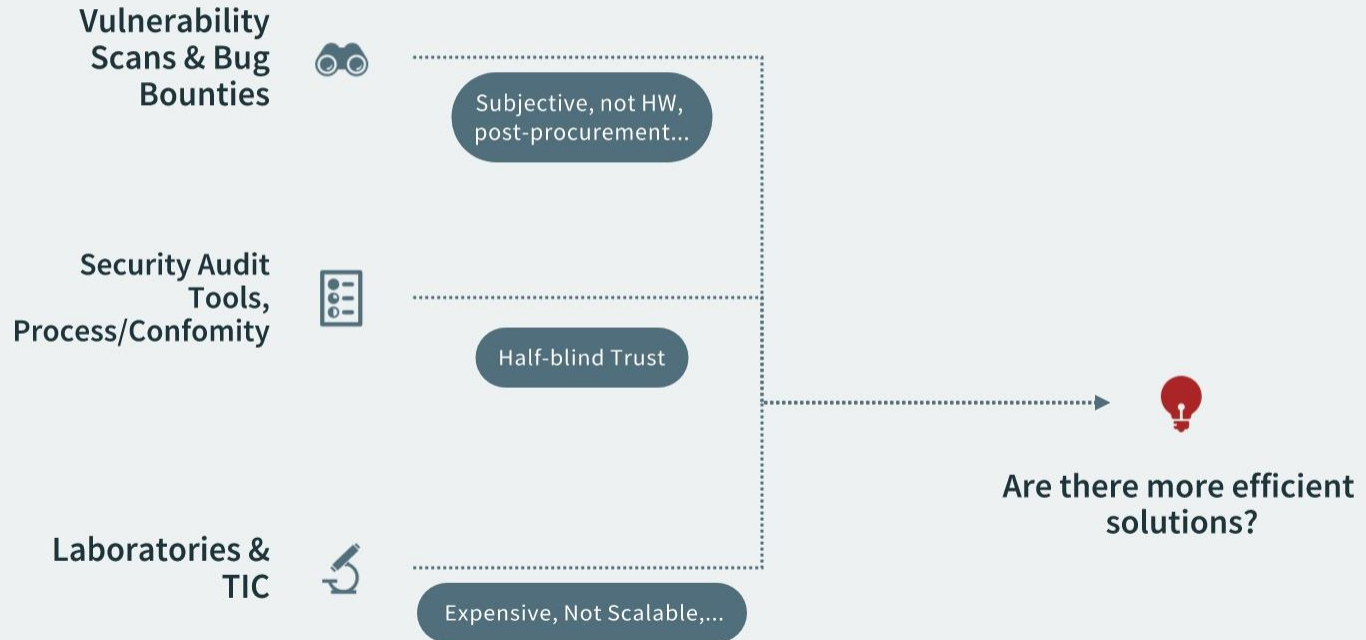


Social Means
reputation and transparency
of stakeholders

POST-PROCUREMENT

How do companies assess their suppliers today ?

Great Initiatives but ...



Imagine this!

Products Cybersecurity Assessment (from manufacturer to buyer)

Automate to Innovate



EN 303 645 Evaluations

allowing to evaluate the cybersecurity level of ICT/IoT connected products coming from third party suppliers.



Intuitive & User Friendly

Based on a methodology covering the main conformity and regulation cybersecurity standards adopted at the European and International level, especially EN 303 645, ...



Label & Certification

providing a standardized security evaluation, a label and a certificate to connected products constructors, which they can share with different customers, coming with an improvement plan to increase their products' maturity level.



Fast & Efficient

combining the speed from automation and the precision and efficiency from cybersecurity laboratories & their expertise.

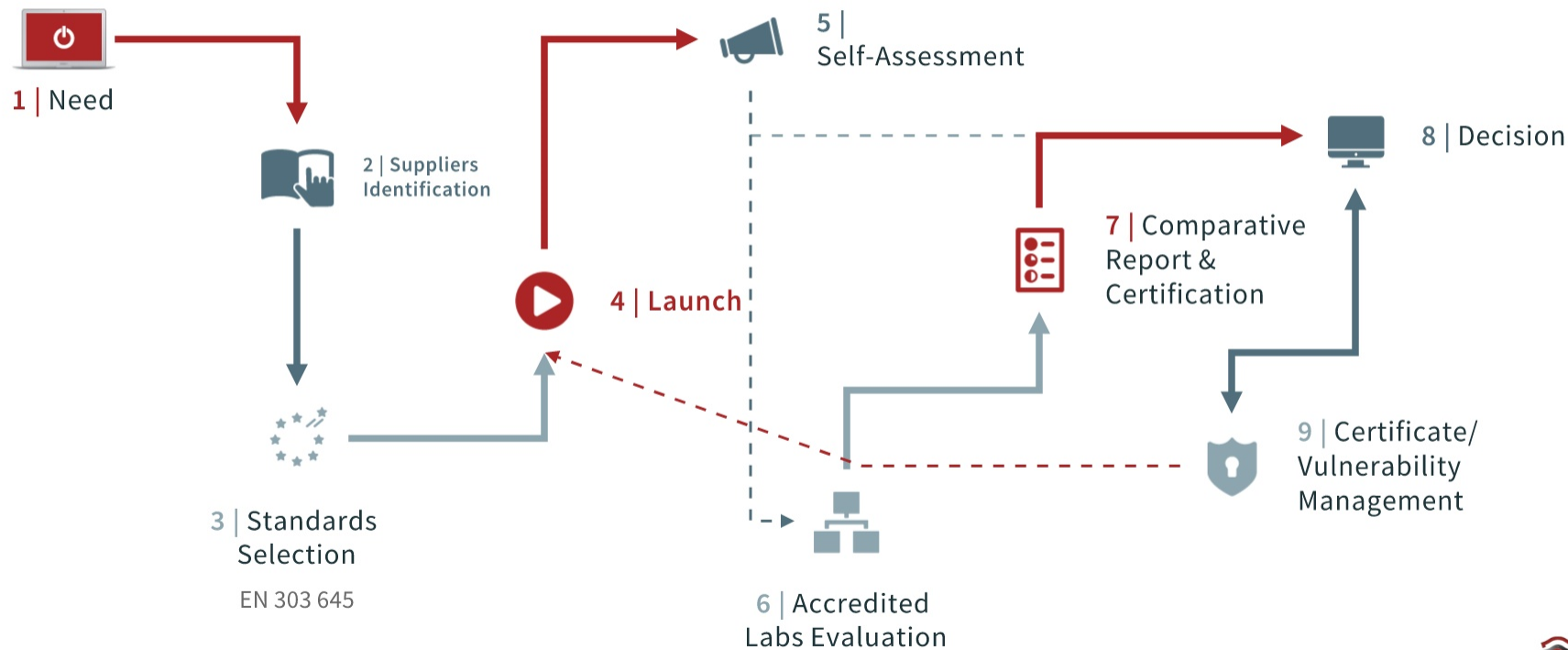


Commitment & Trust

engaging directly the connected products suppliers from all over the world with efficient evaluation processes and validating the results with accredited laboratories (COFRAC, ANSSI, ENISA,...)



Here's how the journey could look like





EN 303 645

Software

- 1 No universal default password
- 2 Ensure that personal data is secure
- 3 Make the system resilient to outages
- 4 Validate input data



Hardware

- 1 Securely store sensitive security parameters
- 2 Communicate securely
- 3 Minimize exposed attach surfaces
- 4 Ensure software integrity

Company Policies

- 1 Implement a report system
- 2 Keep software updated
- 3 Examine system telemetry data
- 4 Make it easy for users to delete
- 5 Make installation and maintenance easy
- 6 Clearly explain what personal data is stored and what for

Key Takeaway



Proactivity

According to a study by Security Signals, only 39% of security teams' time is spent on prevention and they see no change in the next two years.

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.

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...

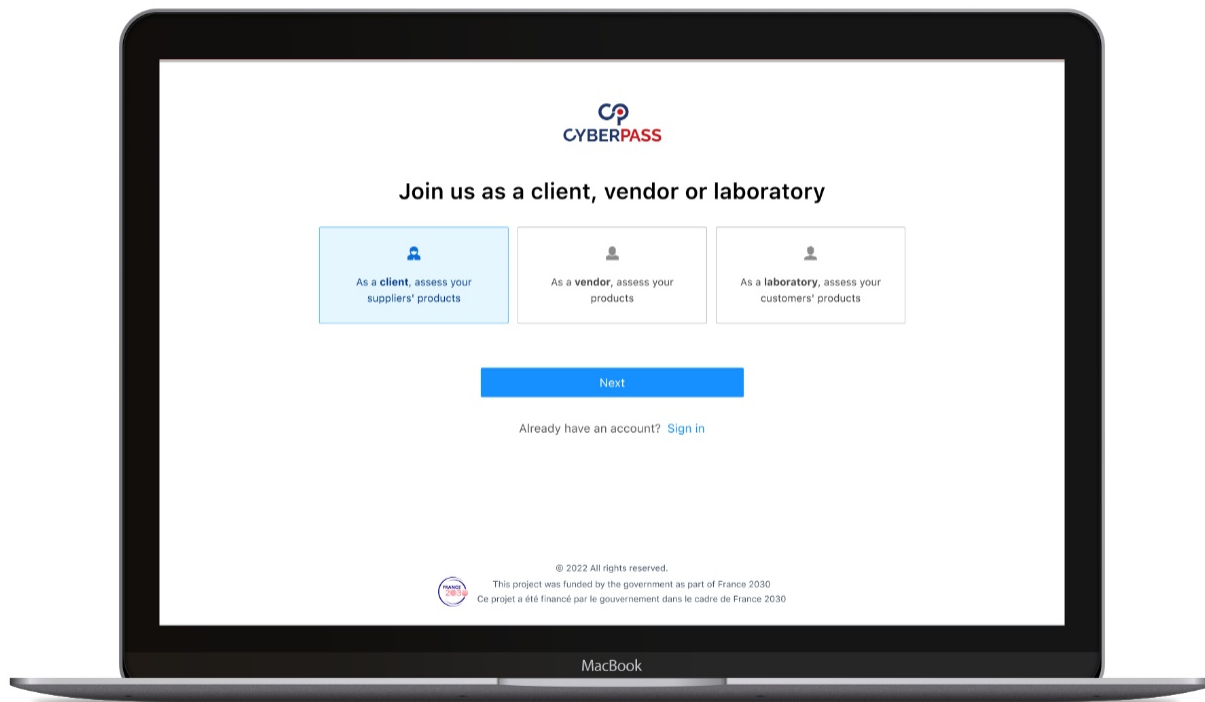
Final Quote...

“Trusting is hard. Knowing who to trust, even harder.”



Maria V. Snyder

Interested to learn more ? **Join us now...**



<https://www.cyber-pass.eu>

©2022 Proprietary and Confidential. All Rights Reserved.

Thank You



RED ALERT LABS
IoT Security

3 rue Parmentier, 94140, Alfortville, France 



<https://www.redalertlabs.com>



+33 9 51 79 07 87



@RedAlertLabs



roland.atoui@redalertlabs.com



QUESTIONS ?

