RED ALERT LABS
IoT Security

BRINGING TRUST TO THE INTERNET OF THINGS

1st of February 2018

THE INTERNET OF THINGS

IoT is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided the ability to transfer data without human-to-human or human-to-computer interaction...

WITH HIGH SECURITY RISKS

Fraud & Misuse

Hundreds of millions of internet-connected TVs are potentially **vulnerable to click fraud, botnets, data theft and even ransomware.**

Smart toasters are used as botnets to **get access to your Facebook account or trigger your webcam'.**

Privacy

Hackers have broken into the massive hospital network of the University of California, Los Angeles, **accessing computers with sensitive records of 4.5 million people.**

Data volumes are increasing so fast so that vendors and businesses lack the time to protect it properly.

Safety

Potentially **deadly vulnerabilities** in dozens of devices such as insulin pumps and implantable defibrillators.

The US National Nuclear Security Administration experienced **19 successful cyber attacks** during the four-year period of 2010 - 2014.

THE PROBLEM / WHY ?

Consumers would always favourite the nice features over security features in a connected product meaning there is no incentive to spend extra money on secure products. A big part of IoT devices cannot support high security development costs for that reason.

Incentive & Awareness

Most of the organizations are unable to calculate the financial impacts or risks they take by not having thought security measures in place

Unknowns

Lack of Security Experts

35% of IoT manufacturers are experiencing shortage of specialized security experts in their organizations as a key challenge to securing IoT products

Compliance, Regulations & TTM

All organizations have set priorities to focus on there own market value and loses too much time thinking up security, trying to meet security requirements and regulations set for each vertical. They often fail in whether meeting TTM or gain the trust of their customers

THE SOLUTION(S)

MISSION

Bring trust
to the Internet of Things

VISION

Become the **reference global market leader** in providing security assurance certifications for all IoT products and solutions covering full cross sectors industries

WE INVEST ON R&D TO PROVIDE YOU WITH THE FOLLOWING SERVICES

- *SECURITY* **CONSULTING**
- *SECURITY* **EVALUATION**
- *SECURITY* **TRAINING**

by providing **IoT Security Assurance Services** designed to help IoT manufacturers, service providers and businesses take a more **informed decision** when designing, implementing, buying or selling IoT products/solutions.

OUR WAY

INNOVATION - Create/Adapt

Create/adapt innovative tools and dedicated IoT security assurance frameworks for having consistent terminology, measurement

SUPPORT

TRANSFORMATION - Analyse

Risk analysis per IoT vertical. Identify the critical assets to be protected, decide how strong the protection must be and the suitable security solutions according to the needs

SUPPORT

MODELLING - Evaluate

Exhaustive security testing and entire review of the product life-cycle ecosystem, from hardware to software, for a perfect balance between risks and time-to-market pressures and conduct security benchmarking

YOUR IOT SECURITY STRATEGY

01. RISK ASSESSMENT

Red Alert Labs IoT Security Scope and Gap analysis or Standards such as ISO 27001 or 27002, IEC 62443, IoTSF Certification Framework, GSMA IoT Security Guidelines and Protection Profiles, provide support and metrics to your developers and decision makers enabling them to measure risks.

02. DESIGN

Red Alert Labs IoT Security Robustness analysis helps you formulate your design strategy for developing a secure architecture from Hardware (Secure Elements, TEE, TPM, HSM, etc.), to Software (white-box crypto, secure coding, etc.).

03. PRE-LAUNCH

Red Alert Labs IoT Security Trust analysis, can help you provide trusted IoT products/solutions, eliminate security vulnerabilities, increase the value of your product/solution, reduce insurance costs and access new markets.

04. POST-LAUNCH

Red Alert Labs supports you both in developing secure life-cycle development & management processes and maintaining your compliance or certifications. From security guidelines, to customized training, secure updates & patch management, to vulnerability triage & action plans.

IOT SECURITY SERVICES

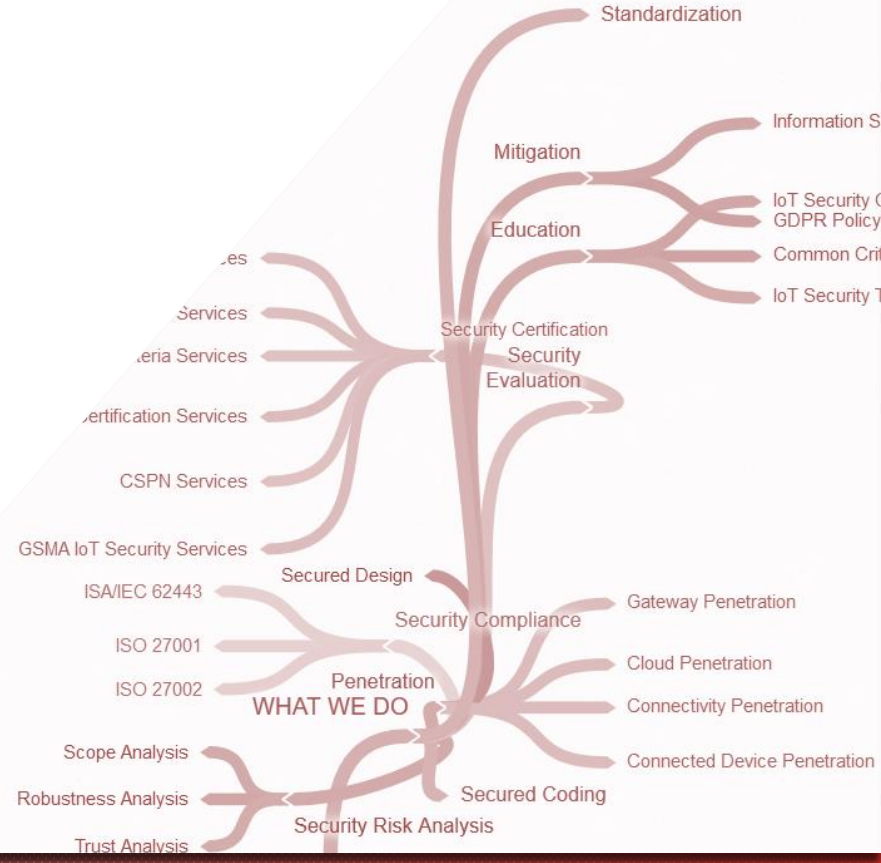
As your security partner, we help you create, reach, and maintain your IoT security goals.

IoT Security Assessment

Red Alert Labs helps you:

1. **qualify** quickly and accurately the cybersecurity risks covering your IoT product or solution using a simple tool created especially for decision makers.
2. **create** an IoT security risk analysis supported by tools and adapted to cross-market verticals taking into account the scope of attacks, the sensitivity of the assets and assumptions on the system's environment.
3. **define** the right set of security requirements and countermeasures to be implemented

➔ Benefit now from our accurate and quick results.



IOT SECURITY SERVICES

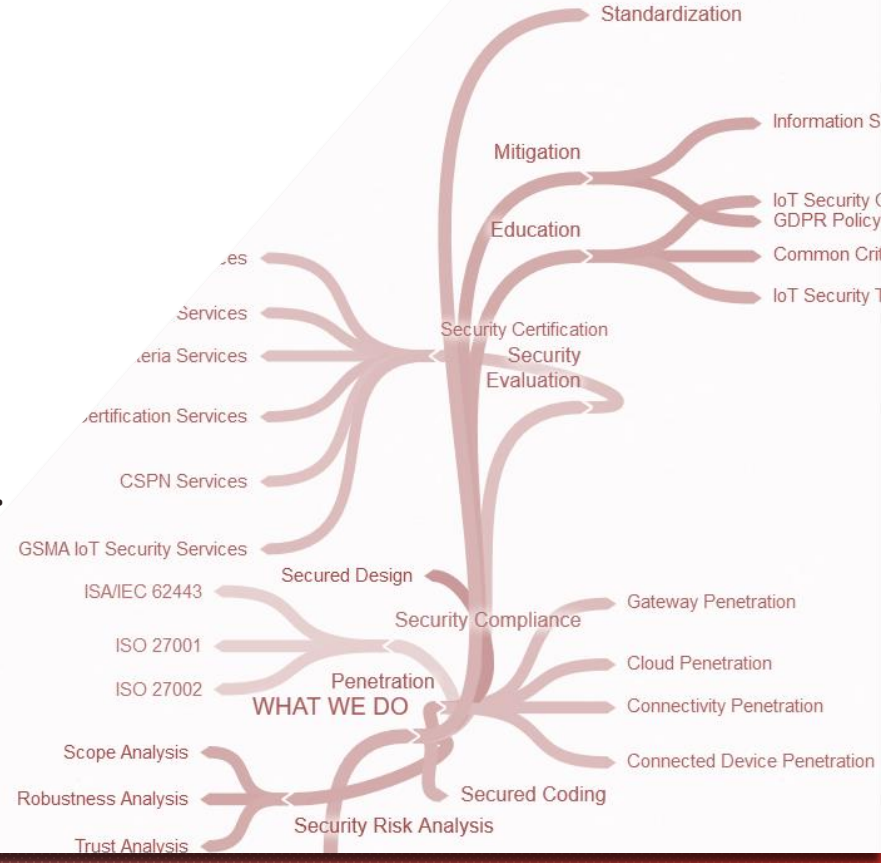
As your security partner, we help you create, reach, and maintain your IoT security goals.

IoT GDPR

Red Alert Labs provides you a:

1. **quick and free** diagnostic allowing you to identify your company's posture with regards to the General Data Protection Regulation (GDPR). We're here to turn getting prepared for GDPR into an opportunity to:
2. **add value** for your company. It's not just a cost to be added but an opportunity to:
3. **leverage** "privacy by design" for building Trust in your organization.

Let us help you fill-in the gap.



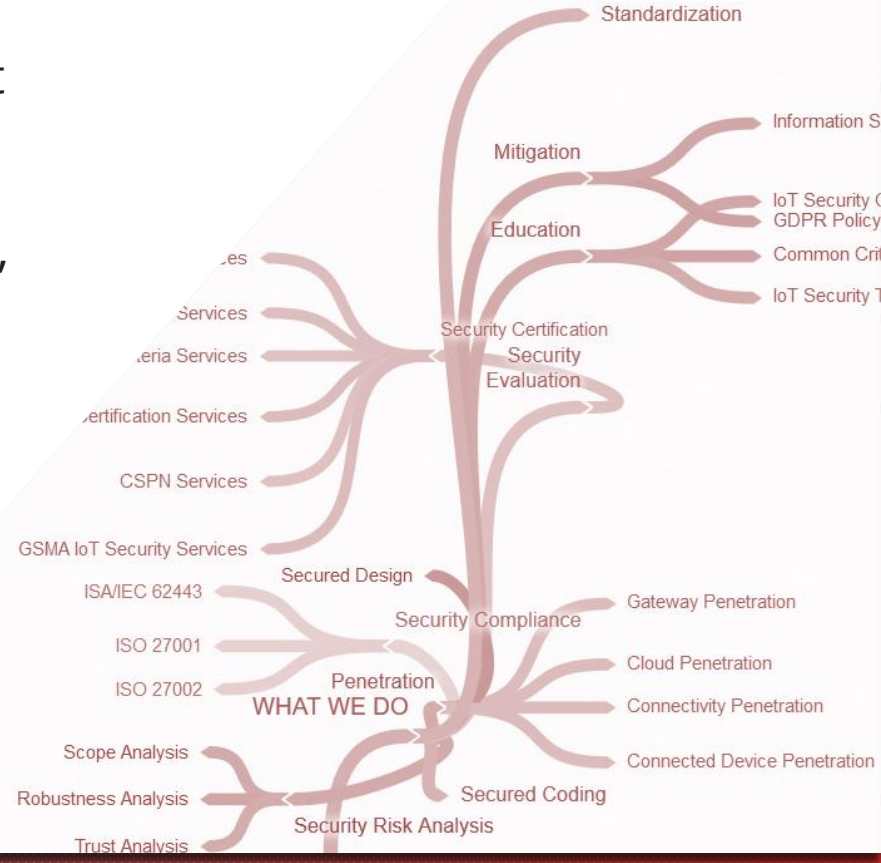
IOT SECURITY SERVICES

As your security partner, we help you create, reach, and maintain your IoT security goals.

IoT Cyber Risk Insurance

As part of its mission to bring Trust to the Internet of Things, Red Alert Labs has developed an IoT cyber insurance offer based on **accurate** cyber risks measuring techniques allowing you to **insure** your organization's IoT solutions and environment and stay **secure**, **vigilant**, and **resilient**.

We simply help you reduce your risk and **reduce** your insurance bill. Please get in touch to learn more.



IOT SECURITY SERVICES

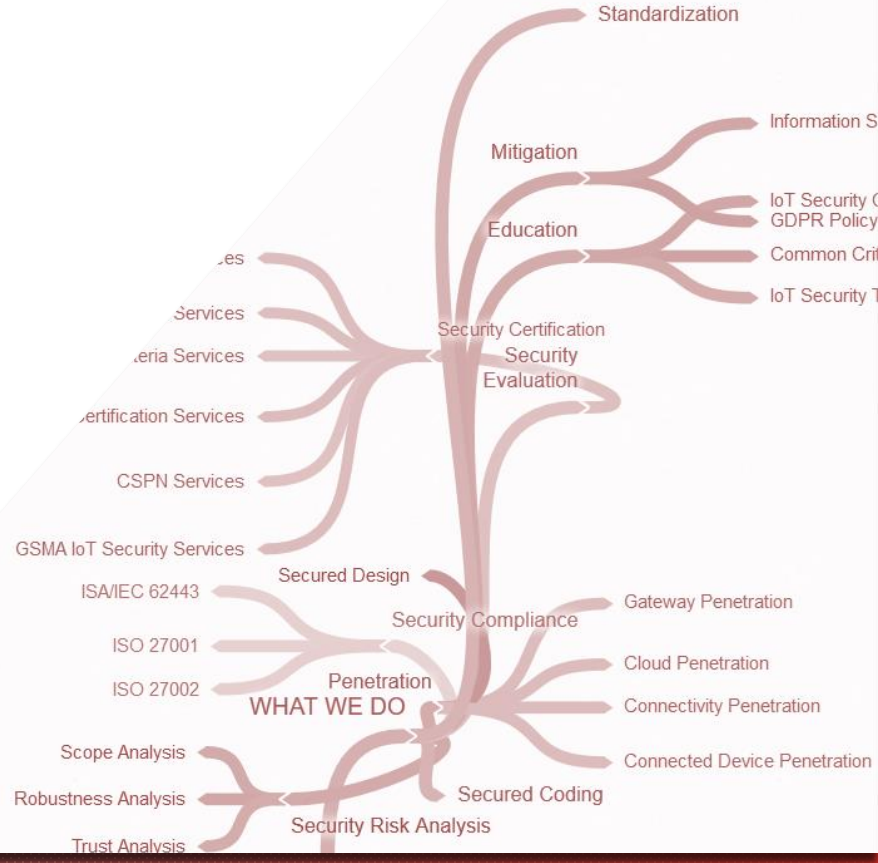
As your security partner, we help you create, reach, and maintain your IoT security goals.

Certification

We **assist** vendors on their effort to security **certify** their products or systems. These services are conducted in various ways, from initial workshops, to delivering complete documentation set, training and project management services.

We also help private and government organizations building full security certification schemes.

CC, FIPS 140-2, ISO27K, CSPN, IoT SF, EMVCo, GSMA IoT, OWASP IoT, EU cybersecurity



IOT SECURITY LAB EVALUATION

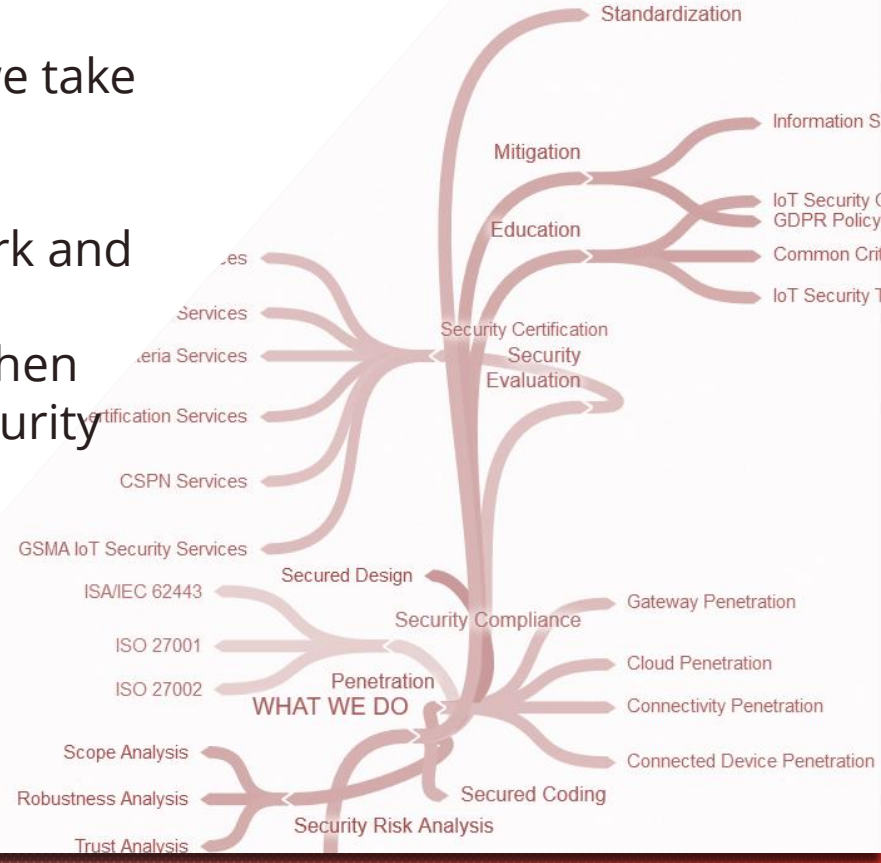
As your security partner, we help you create, reach, and maintain your IoT security goals.

IoT Security Evaluation

Using our innovating in-house tools, we do **support** you through your

- security auditing/evaluation using specialized techniques. Indeed, we take an exhaustive approach starting by
- **reviewing** the entire product life-cycle ecosystem, from hardware to software, covering physical and logical attacks on the device, network and service domains. All this while making sure we
- **identify** first your sensitive assets and the target of evaluation and then
- **prioritize** attack paths and vulnerabilities (through Model-based Security Testing) so you can smartly
- **balance** risk with time-to-market pressures.

Request now an IoT Security Label for your product or solution and get an early ticket to meet the upcoming European and International Standards.

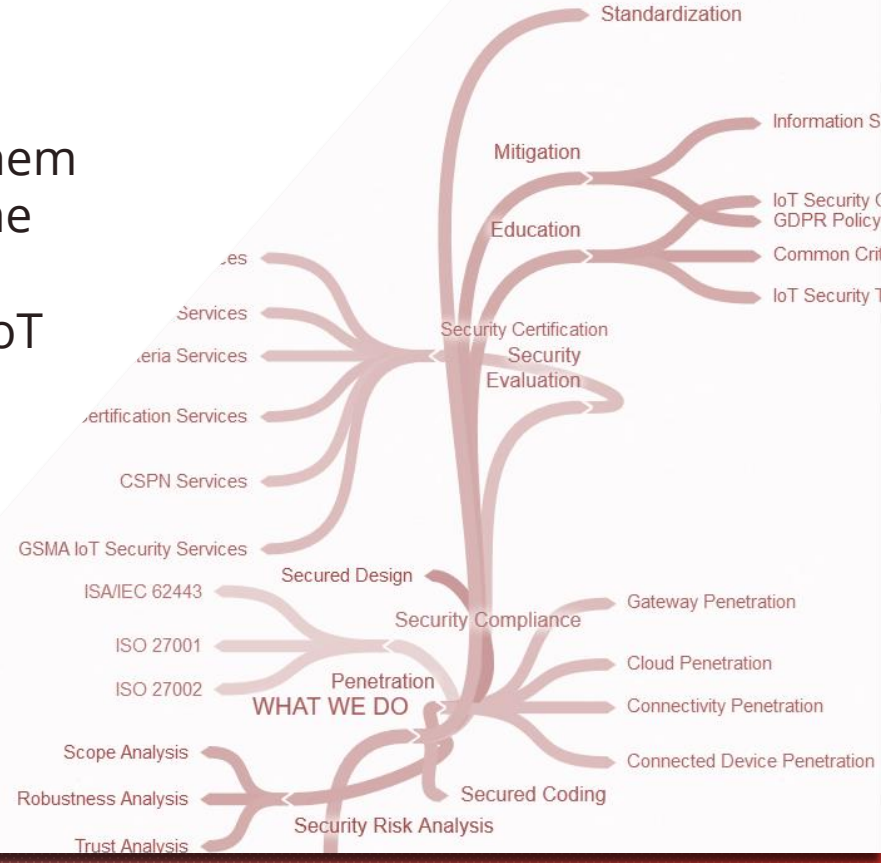


SECURITY TRAINING

As your security partner, we help you create, reach, and maintain your IoT security goals.

COMMON CRITERIA and IoT Security

The intention of this training program is to provide useful information generic to all parties involved in the CC certification process helping them understand all the key aspects of the CC evaluation process. It gives the beginners a good start and the experienced ones new techniques and best practices to improve the efficiency of CC evaluations applied on IoT products requiring a CC certification.



KEY BENEFITS

01 INCREASE SALES & REVENUES

By winning the trust of your customers, your sales and revenue will increase significantly.

02 ACCURATE SECURITY ASSURANCE

Optimize your security and provide a proven level of security assurance for your customers.

03 REDUCE COSTS

Chose exactly what level of security you need to provide and decide on the amount of money you want to invest.

04 FASTER TIME TO MARKET

Cut-off several months of efforts thinking up security and focus on your own market value.

05 REGULATION & SECURITY STANDARDS COMPLIANCE

Simplify traceability, making this step quick, easy and error-free.

OUR RENOWNED EXECUTIVES

Roland Atoui
CEO & Founder
roland.atoui@redalertlabs.com

ORACLE | GEMALTO | TRUSTED LABS
EDHEC EXECUTIVE MBA

Jean-Yves Bitterlich
CTO
jean-yves.bitterlich@redalertlabs.com

ORACLE | SUN MICROSYSTEMS | SIEMENS
EDHEC EXECUTIVE MBA

Heading an Outstanding Team of
5 IoT & Cybersercurity Experts

WHY CHOOSE US

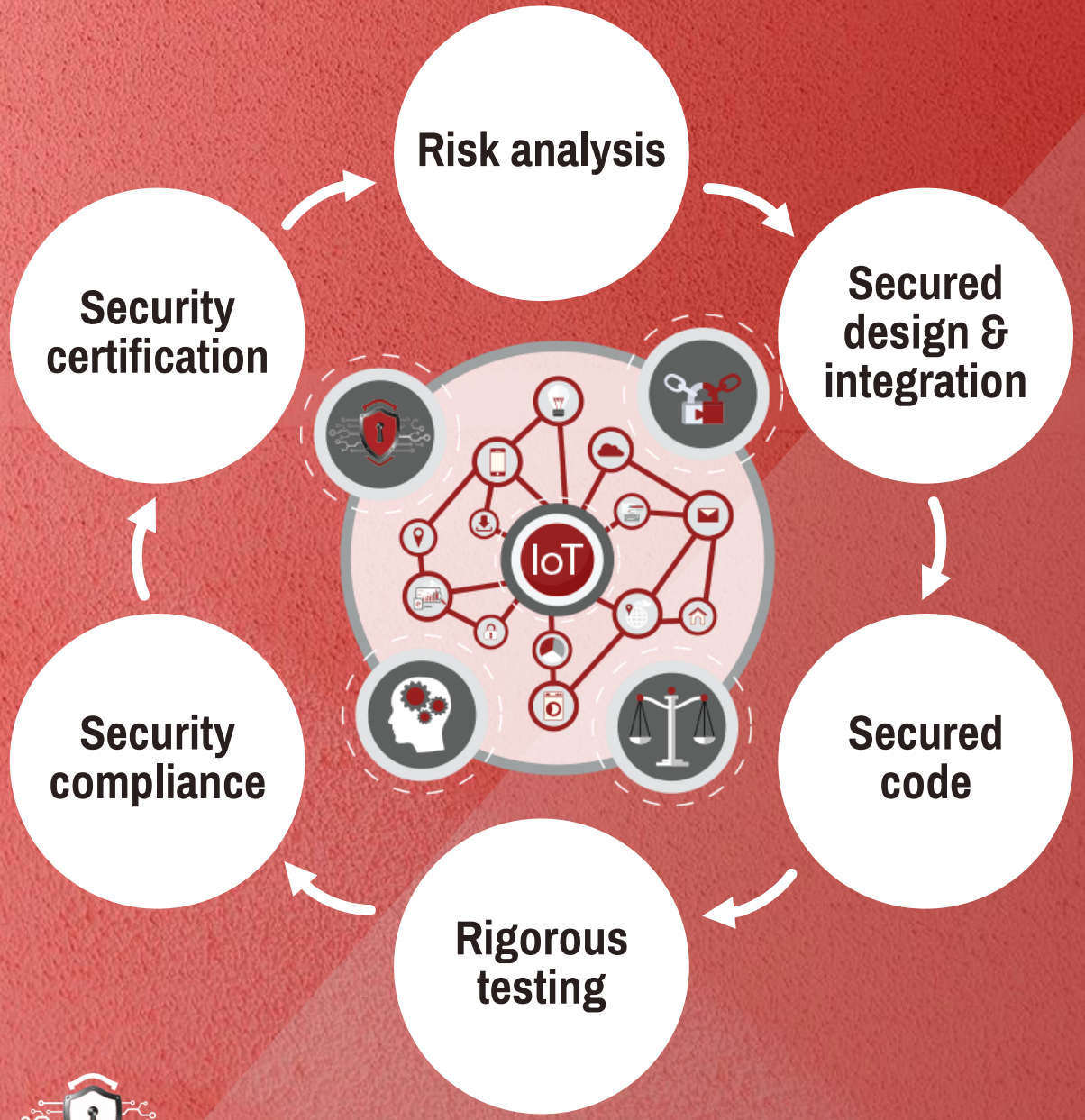
Red Alert Labs has significant expertise in embedded systems, IoT Cloud Platforms, SW and HW security architecture, Certification Standards, with Common Criteria, FIPS140-2, ECSO, IoTSF, OWASP IoT, Global Platform & Java Card specification.

Relying on its experts' unique experience, Red Alert Labs has earned the trust of several customers, and is recognized by the security labs community as a solid technical business partner.

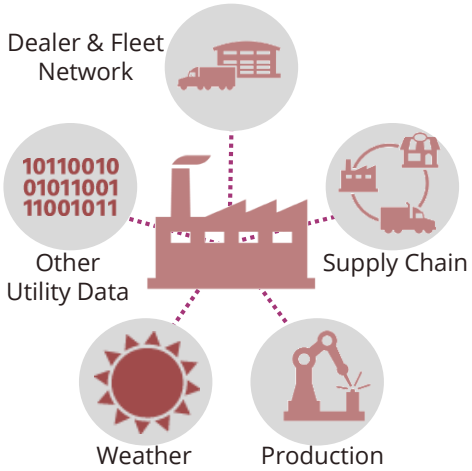
CIO Applications europe TOP 25 CYBER SECURITY COMPANIES - 2017

SOLUTIONS BY IOT INDUSTRY

IOT TRUSTED MODEL



MANUFACTURING



IoT has played an important role in modernizing manufacturing environments by providing them with real time data, allowing them to monitor and perform more easily in the product line. Despite all the benefits, IoT devices represent a real challenge in term of security as they were not created with security first, making modern manufacturing more vulnerable. As the industry relies on different operations process, any interruption in the line of process can have a dramatic impact on the business and his reputation.

Security concerns in Manufacturing Industry

- **Corporate data risks** through connected business systems
- **Industrial espionnage** through pishing e-mails
- **Data breach** that can result in incorrect data analysis with a drop of product quality.
- **DDOS and ransomware attacks** that uses connected objects to bring down servers, that can shut down the entire manufacturing process

RAL IoT trusted model solution

Risk Analysis → Secured design and integration → Secured Code → Rigorous Compliance → Security Certification

Red Alert Labs's approach

With both strategical and technical methodologies, Red Alert Labs provides companies with deep IoT security expertise helping them reduce security risks and gain trust in their IoT product or solution throughout every step of its life-cycle.

SMART HOME

The interconnectivity driven by IoT has moved households to a higher level of living. From the smart coffee machine making coffee just on time, to the smart speaker answering to all the users demands and controlling connected devices, smart home devices are making life easier and more efficient.

The case

In 2016, a DDoS attack names Mirai infected half of the internet network passing throught the WIFI of smart devices (routers and security cam), shutting down, for example, DYN's entire website. Attacks of its kinds is for now rare but will increase significantly as hackers are getting more inventive with more opportunities to conduct such attacks, due to a lack of security in the creation of smart devices.

RAL Trusted Model Solution

Risk Analysis → Secured design and integration → Secured Code → Rigorous Compliance → Security Certification

Red Alert Labs's approach

With both strategical and technical methodologies, Red Alert Labs provides companies with deep IoT security expertise helping them reduce security risks and gain trust in their IoT product or solution throughout every step of its life-cycle.

FINANCE

Finance is a fast growing industry that has adopt quickly the digital revolution. With the need of real-time data, the finance industry has taken advantage of IoT with real-time analytics, by connecting and understanding the purchasing behavior of their clients for example. With an instant access to their customers' data, it make Financial institutions more attractive to hackers and more vulnerable to pishing and ransomware attacks, exposing them to important financial loss and trust from their customers and investors.

Security concerns in Finance Industry

- **Sensitive data risks** through financial IoT systems. As Financial Institutions have an instant access to their customers' data, exposing companies to important financial loss and trust from their customers and investors
- **Financial pishing e-mails** that allows attackers to collect customer's data through mimicked legitimate banking pages.
- **Mobile banking malware** especially Androids that are more vulnerable to attacks.
- **DDOS and ransomware attacks** allowing attackers to destroy the company's data

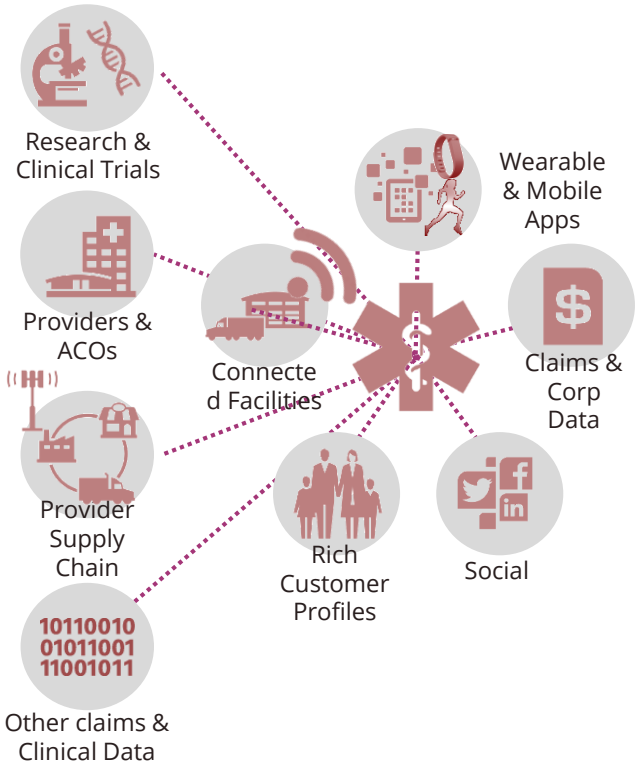
RAL IoT trusted model solution

Risk Analysis → Secured design and integration → Secured Code → Rigorous Compliance → Security Certification

Red Alert Labs's approach

With both strategical and technical methodologies, Red Alert Labs provides companies with deep IoT security expertise helping them reduce security risks and gain trust in their IoT product or solution throughout every step of its life-cycle.

HEALTHCARE



With the Internet of Things, Healthcare industry witness transformation and improvement in care, offering a lot of diverse potential in healthcare solutions such as keeping patients safe and healthy (even remotely), optimizing the workflow and also supplanting doctors' visits. Despite all the benefits, the use of IoT raise some security concerns and as a fact, trut issues, especially due to the increase of cyberattacks.

Security concerns in Healthcare Industry

- **Data privacy**. Sensitive and confidential information that could be accessed through healthcare systems, medical equipments and connected wearables, are very valuable not only for hackers, but also third parties like insurance companies, etc.
- **IoT medical device management**. Multiple devices from different vendors with no standardization, making updating and upgrading challanging and posing real security issues.
- **DDOS and ransomware attacks** allowing attackers to gain access to digital healthcare facilities and destroy datas making it extremely life threatening to patients.

RAL IoT trusted model solution

Risk Analysis → Secured design and integration → Secured Code → Rigorous Compliance → Security Certification

Red Alert Labs's approach

With both strategical and technical methodologies, Red Alert Labs provides companies with deep IoT security expertise helping them reduce security risks and gain trust in their IoT product or solution throughout every step of its life-cycle.

OIL & GAS

Nowadays, Oil & Gas industry is facing many challenges. Oil prices have dropped increasingly due to new source of supply that has been opened, making it difficult for companies to predict their business plan, manpower is aging and environmental regulation are becoming tougher, making accidents very expensive with an important impact on companies.
As a result, remote monitoring of oil rigs and wells has become primordial and IoT is the solution that answers the best to this demand.
But with IoT, the industry is not immune to cyberattacks, giving the industry a more important challenge.

Security concerns in Oil & Gas Industry

- **National security.** By accessing sensitive data, it is possible to
- **Sensitive data risks** present in Industrial IoT devices (sensors, actuators), IoT Platforms, etc.
- **Security vulnerabilities in OT protocols** that could lead to disrupting the connected devices.
- **DDOS and Malwares attacks** that are increasing significantly, causing millions of Dollar losses in the Oil & Gas Industry.

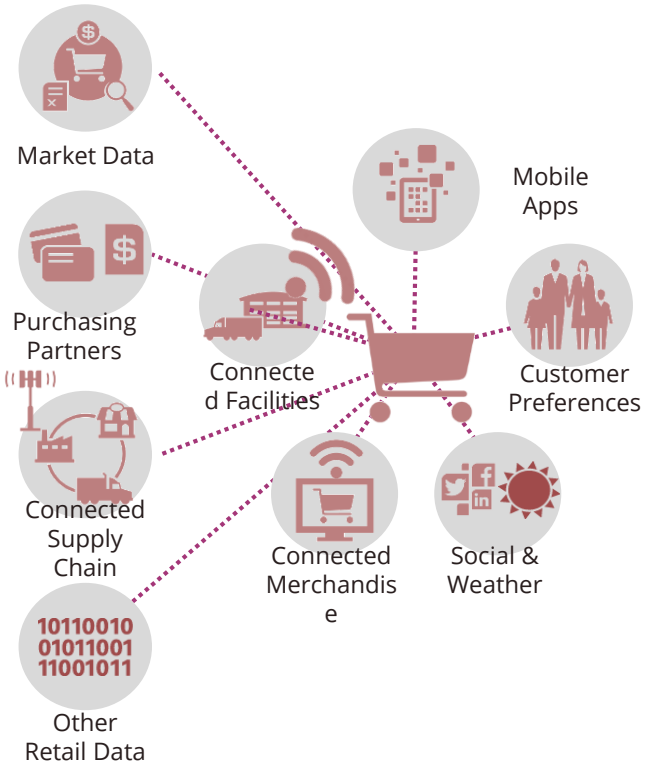
RAL IoT trusted model solution

Risk Analysis → Secured design and integration → Secured Code → Rigorous Compliance → Security Certification

Red Alert Labs's approach

With both strategical and technical methodologies, Red Alert Labs provides companies with deep IoT security expertise helping them reduce security risks and gain trust in their IoT product or solution throughout every step of its life-cycle.

RETAIL



Internet of Things is revolutionizing the Retail Industry by improving customer experience, optimizing supply chain and by creating new source of revenue.
With the IoT, it becomes easier and faster to collect data from customers, analyze it and use it to offer more personalized services to each customer. Also, with e-commerce or online stores, it becomes more convenient for customers to purchase products and see where their goods are in the delivery process.
Automating and optimizing the supply chain helps retailers in loss prevention with detailed information, optimizes the inventory management by automatically re-order products when inventories reach certain levels for example, but also tracking products by using RFID and sensors.

Security concerns in Retail Industry

- **Sensitive data risk** present in RFID and sensors
- **Data breach** that can result in incorrect data analysis and alter the supply chain
- **Sensitive data risk** present in retails IT infrastructure, gateway, etc.
- **DDOS and Malwares attacks** that are increasing significantly that can have an important impact on the companie's reputation but also an important loss of money

RAL IoT trusted model solution

Risk Analysis → Secured design and integration → Secured Code → Rigorous Compliance → Security Certification

Red Alert Labs's approach

With both strategical and technical methodologies, Red Alert Labs provides companies with deep IoT security expertise helping them reduce security risks and gain trust in their IoT product or solution throughout every step of its life-cycle.

TRANSPORTATION

Transportation is one of the industry that encounters the lowest improvement in the IoT. But this is about to change as we can already see it with smart cars, live stream information about the traffic, etc. With IoT, people are going to be able to access internet all the times in cars, buses, trains and planes. This is already happening, but it is not yet universal and it's still need some improvements. IoT will make transportation also more efficient by giving customer real-time information on traffic, bus schedules, late trains, etc.. Transportation is one of the first steps to develop a smart city. Important security issues are not yet happening, but they will if we don't act know with a proper strategical management of IoT.

Security concerns in Transportation Industry

- **National security.** A person or a group of person could access the transportation systems and infrastructure, altering traffics highway, sending bad information to flights operators and injure a lot of people
- **Sensitive data risk** present in companies transportation infrastructure, gateway, etc.
- **DDOS and Malwares attacks** that are increasing significantly, causing security issues by altering the data and, for example, tacking control of a car or simply robing it. That can have an important impact on the companies' reputation with a big loss of money but also endangering lives
- **Data privacy.** Hackers will be able to have access to a lot of users personal information, and knowing their habits, etc.

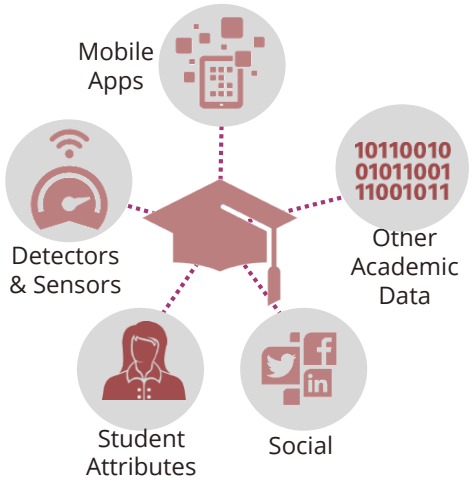
RAL IoT trusted model solution

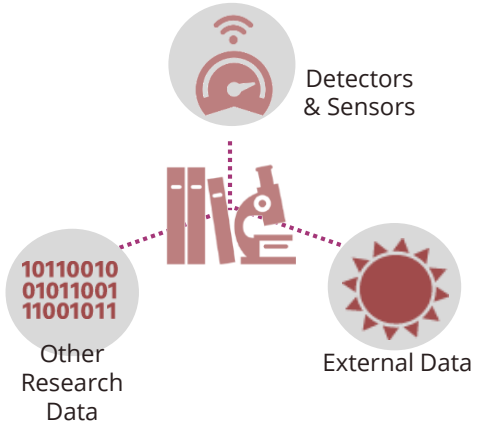
Risk Analysis → Secured design and integration → Secured Code → Rigorous Compliance → Security Certification

Red Alert Labs's approach

With both strategical and technical methodologies, Red Alert Labs provides companies with deep IoT security expertise helping them reduce security risks and gain trust in their IoT product or solution throughout every step of its life-cycle.

EDUCATION





With IoT devices schools and campuses will be able to offer a safer environment to their students, energy efficiency, improve resource management and enhance access to information. But it will also be useful in teaching, with smartboards, tablets or computer that will replace traditional books and notebooks, it will also allow a better interaction between students and teacher and even classmates (and parents in some cases). But, as connected objects are making education more efficient, it also comes with IoT problems, by causing security risks.

Security concerns in Education

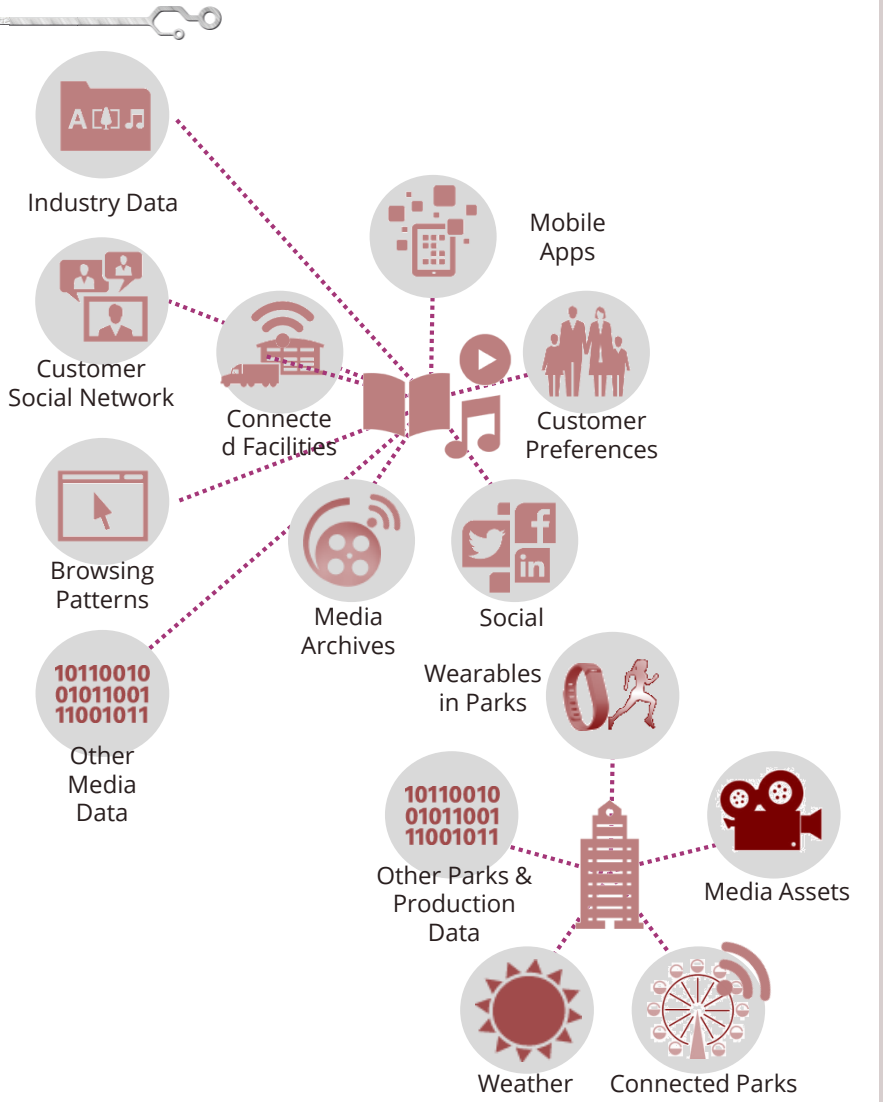
- **Data privacy.** For example, students are using smart printers that store and print intellectual property and personally identifiable information, making them interesting targets for hackers.
- **Sensitive data risk.** For example gaining access to exam's information, to class notes and changing them, etc.
- **DDOS and Malwares attacks** that are increasing significantly, causing security issues with the possibility of shutting down security cameras, playing with the energy, and even shutting down the all school

RAL IoT trusted model solution

Red Alert Labs's approach

With both strategical and technical methodologies, Red Alert Labs provides companies with deep IoT security expertise helping them reduce security risks and gain trust in their IoT product or solution throughout every step of its life-cycle.

MEDIA & ENTERTAINMENT



Internet of Things is going to considerably change the way Media & Entertainment Industry is operating, by helping the industry to manage and use valuable data. With the collected consumer's data, M&E companies will be able to have meaningful insights about their consumer's behaviors and preferences, allowing them to deliver personalized entertainment experience, improving the customer experience. For advertisers, IoT is a huge deal also as they are going to be able to target their ads to the right people.

Security concerns in M & E Industry

- **Data privacy** on consumer's data
- **Sensitive data risk** present in M&E systems and infrastructure, sensors, gateway, etc.
- **DDOS and Malwares attacks** that are increasing significantly, causing important loss and reputation to the M&E industry

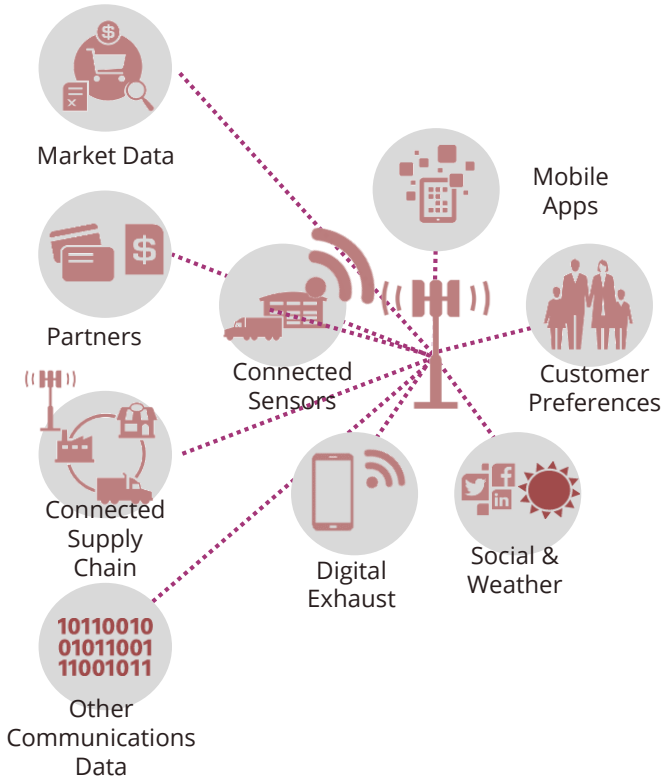
RAL IoT trusted model solution

Risk Analysis → Secured design and integration → Secured Code → Rigorous Compliance → Security Certification

Red Alert Labs's approach

With both strategical and technical methodologies, Red Alert Labs provides companies with deep IoT security expertise helping them reduce security risks and gain trust in their IoT product or solution throughout every step of its life-cycle.

COMMUNICATION



With the rise of IoT, Communication Industry had to adapt and change quickly their business strategy to stay up to date with the customer behaviors and providing with an always better network. IoT challenged the Communication Industry but also gave them with many opportunities to improve customer experience by collecting and analyzing valuable data.

Security concerns in Communication Industry

- **National security.** A person or a group of person could access the communication network and infrastructure and altering the communication or shutting it down, making all kind of communication impossible.
- **Sensitive data risk** present in Communication systems and infrastructure, sensors, gateway, etc.
- **Data privacy** on consumer's data
- **DDOS and Malwares attacks** that are increasing significantly, causing important loss and reputation to the Communication industry

RAL IoT trusted model solution

Risk Analysis → Secured design and integration → Secured Code → Rigorous Compliance → Security Certification

Red Alert Labs's approach

With both strategical and technical methodologies, Red Alert Labs provides companies with deep IoT security expertise helping them reduce security risks and gain trust in their IoT product or solution throughout every step of its life-cycle.

CONTACT

Red Alert Labs

71, rue Carnot | 94700 Maisons-Alfort

contact@redalertlabs.com

+33 9 53 55 54 11

www.redalertlabs.com

THANK YOU FOR YOUR TRUST

RED ALERT LABS
IoT Security