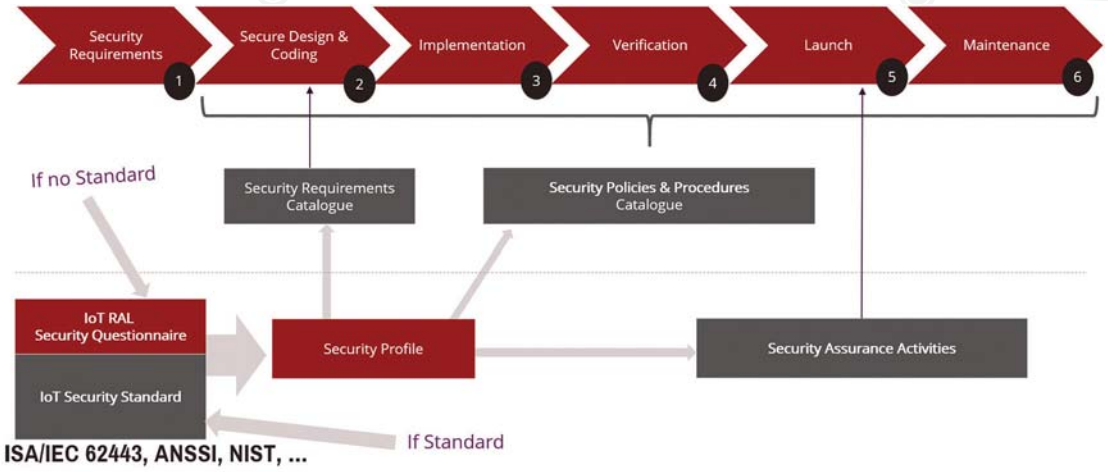
Bringing trust to the internet of things

IoT Security Assurance Framework

5 Steps for Building Trust

RED ALERT LABS
IoT Security



It's not up to you to decide if someone will want to steal your data or compromise your technology, but it's up to you to decide to protect it.

What is a framework? //

It consists of a set of strategic and technical guidelines, security profiles, tools, catalogues of security requirements, a risk-based evaluation methodology for classes of IoT devices, based on standards when they exist.

Does this Framework provide a single "checklist" applicable to all organizations / industries? //

NO, This Framework is dynamic. It should be customized for each business sector and operational environment to best meet their risks, situations and needs. Organizations will continue to have unique risks - different threats, different vulnerabilities, different risk tolerances - and how they will implement the Framework's practices to achieve positive results will vary. The framework should not be implemented in the form of a non-personalized checklist or a single approach for all critical infrastructure organizations.

Why is it important to implement your own framework? //

This Framework will help prioritize investments and maximize the budget impact on cybersecurity allowing organizations to better implement security measures, assess and certify their solutions and reduce cyber security risks while preserving a balance between security needs and business needs. In addition, it has been designed to simplify the communications between internal and external stakeholders of an IoT solution.

How is the Framework used today? //

Organizations use the Framework in different ways. Many found it useful to raise awareness and communicate with stakeholders in their organization, including leaders. The Framework also improves communications between organizations, enabling cybersecurity expectations to be shared with business partners, suppliers, and industries. By mapping the Framework to current cybersecurity management approaches, organizations learn and show how they fit with standards, guidelines, and best practices. Some parties use the Framework to reconcile and dissociate internal policy from legislation, regulations and industry best practices. The framework is also used as a strategic planning tool to assess risks and current practices.

Does the framework address the costs and cost-effectiveness of cybersecurity risk management? //

Yes. The framework was designed based on a risk approach to prioritize activities for development and operational environments. It thus makes it possible to significantly optimize investments in cybersecurity.

Red Alert Labs S.A.S.
Paris Area, 3 rue Parmentier,
94140 Alfortville, France

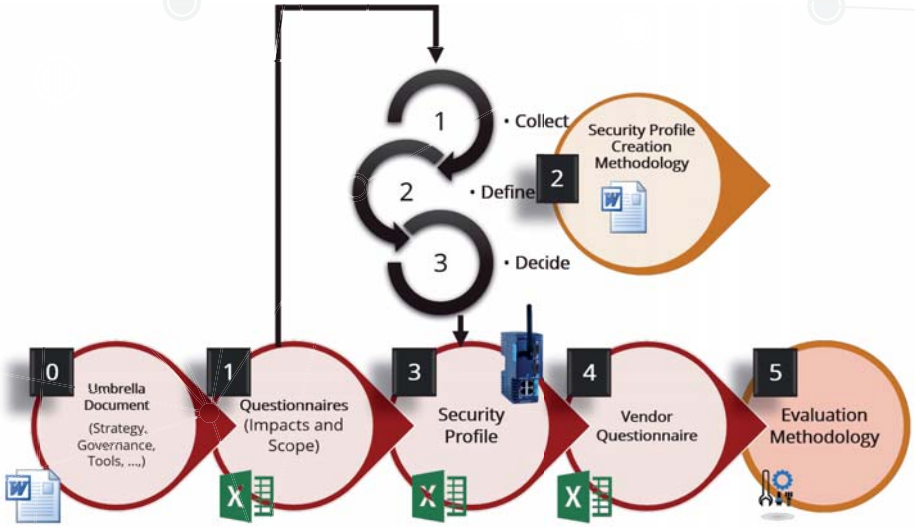
www.redalertlabs.com
contact@redalertlabs.com
+33 9 53 55 54 11

Bringing trust to the internet of things

IoT Security Assurance Framework

5 Steps for Building Trust

RED ALERT LABS
IoT Security



What is a "Security Profile" and how is it used? //

It is a dashboard representing a security specification specific to a type of connected product / solution (RTU, gateway, thermostat, smart camera, etc.) while taking into account the type and sensitivity of the data and the context of the product. the operational environment (for example, Consumer, Enterprise, Industrial) and the risk factor.

It is a step towards an economical way of dealing with safety assessment. They allow for staggering security and security policies based on the identified risks, that is, concentrating efforts where the risks are highest.

Security profiles can be agreed and standardized for certain product classes.

A standard security profile is the result of a detailed risk analysis for each new product instance. It provides an accepted standard on the security properties of a product.

Would the framework have prevented recent high-profile attacks? //

There is no "magic bullet" on cybersecurity and protecting an organization. For example, zero-day attacks exploiting previously unknown software vulnerabilities are particularly problematic. However, using this framework to assess and improve cybersecurity risk management should allow companies to minimize damage and impact as much as possible.

How can the Framework help an organization communicate with stakeholders? //

The Framework can be used as an effective communication tool with key stakeholders (CIO, CEO, Business Leaders, Board of Directors, etc.). It provides an overview of cybersecurity activities and results that could be used to share the context with stakeholders.

In addition, the Framework can be used to communicate with external stakeholders such as vendors, service providers and system integrators. More specifically, the choice to use human language (non-formal) to express security requirements, business dashboards and questionnaires makes it possible to simplify communication and guarantee a net gain in time.

How long does it take to implement this framework? //

The resources, capabilities, and cybersecurity needs of each organization are different. The time required to implement the Framework will therefore vary from one organization to another, ranging from 2 to 6 months. The Hierarchical Framework Framework design allows organizations to divide the steps between the current state and the desired state in a way that is appropriate to their resources, capabilities, and needs. This allows organizations to develop a realistic action plan to achieve the results of the framework in a timely manner, and then build on that success in future activities.

Red Alert Labs S.A.S.
Paris Area, 3 rue Parmentier,
94140 Alfortville, France

www.redalertlabs.com
contact@redalertlabs.com
+33 9 53 55 54 11