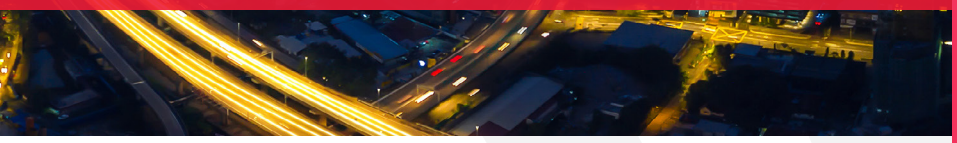
Secura
A BUREAU VERITAS COMPANY

Product Manufacturers



CONSUMER IOT
MEDICAL DEVICES
CONNECTED VEHICLES
INDUSTRIAL PRODUCTS
NETWORK EQUIPMENT

With the introduction and continuous expansion of the Internet of Things (IoT), the world becomes more and more connected. The combination of "smart" devices, mobile or web applications used to interact with them and cloud services allowing them connect with each other lead to the development of overlapped IoT ecosystems.

Moreover, as the IoT has long ago passed the barriers of consumer products, organizations are making use of such products and solutions, making them an integral part of the ecosystem. In the ecosystem of IoT, manufacturers of products hold one of the most important roles: they are ultimately the ones that decide which features will be included in their products.

Historically, the world of IoT has been driven in the past years strongly by functionality. The products with the most and more revolutionary features got an edge over their competition. Recently, the aspect of cybersecurity in IoT has become a topic that cannot be ignored.

Moreover, we are not at a point where cybersecurity issues associated with these products are not theoretical anymore, and can be very well take place on the products that we use in our daily life. Scaling up this idea to the fact that what we call today IoT is not anymore linked fully to smart gadgets, but also includes vehicles, medical devices, industrial and telecommunication equipment, and more, gives the perspective of how critical a cybersecurity attack can prove to be.

The IoT domain has lacked for many years a clear set of relevant standards and frameworks to support manufacturers in developing good security into their products.

Luckily, these days are gone. At the present moment, there are multiple internationally recognized standards, frameworks and certification programs that could help manufacturers decide which set of security functionalities they would like to include into their products.

There are several examples that can be highlighted. The IEC 62443 family has become over the years the reference standard for industrial cybersecurity, covering also the components and systems. UL 2900 is seen as a reference family for security in medical devices. ETSI EN 303 645 is a recently finalized standard seen as the main reference for consumer IoT products. Finally, ISO 21434 is becoming a majorly recognized standard for cybersecurity processes and functionalities in connected vehicles.

From a regulatory point of view, cybersecurity is also seen as a major topic, with the first examples being already in place, or in a final drafting state. Connected vehicles have their cybersecurity and software updates processes and functionalities mandated through the UNECE international regulations. Medical devices need to pass extensive requirements in order to be placed on various markets, including the USA (FDA regulation) and EU (MDR regulation). Finally, regulatory requirements targeting the area of consumer products will be set in place through the Radio Equipment Directive (RED).

What Standards to choose?

The fact that we have currently in place multiple examples of recognized standards, frameworks or certifications is the first step towards a better cybersecurity in our IoT products. At the same time, this could easily have the opposite effect: too many, partially overlapping standards could introduce confusion and make developers undecided regarding the best set of requirements to select for their products. Very often, developers will needs to fight strict budgets and timelines for the design of their products. Because of that, there is very little room for the process of selecting a reference standard, and a potential mistake made at that point can turn to have important outcomes in the product development lifecycle.

By making a good analysis on the recognition and acceptance rate of a particular standard, it is possible to focus on the best option for the specific product. With regulations, it is slightly easier, as manufacturers will know that they need to demonstrate certain compliance requirements in order to obtain market access. In that case, there will still be the aspect of converting regulatory requirements into concrete requirements, which will still ask for a meaningful selection.

Secura has a solid view on the standards and regulatory landscape across IoT, by actively researching and contributing in this field. Furthermore, Secura is an active member of various security organizations, therefore being able to often shape the contents of new standards and regulations. Because of this, we are happy to support IoT product manufacturers with the best options of security compliance, tailored to their specific needs.

Our Services

Secura is your partner in the world of product security evaluation, compliance and certification. Our portfolio of possible services includes a broad selection of standards and certification schemes, covering multiple product domains. Because of this, we define our services in line with Support and preparation, Compliance and Certification/regulatory, for various types of connected products. This is summarized below.

Consumer IoT

Support & Preparation:
- Design reviews
- Focused penetration testing

Compliance:
- ETSI EN 303 645
- GSMA IoT
- IoT Security Foundation

Certification/Regulatory:
- ETSI EN 303 645 certification
- Common Criteria certification
- BSPA certification
- Radio Equipment Directive (RED) compliance gap analysis

Medical Devices

Support & Preparation:
- Design reviews
- Focused penetration testing
- Focused code reviews
- Security processes reviews and support in drafting/implementation

Compliance:
- IEC 62443 compliance
- UL 2900 compliance

Certification/Regulatory:
- UL 2900 certification
- Common Criteria certification
- EU MDR compliance gap analysis
- FDA compliance gap analysis

Network Equipment

Support & Preparation:
- Design reviews
- Focused penetration testing

Compliance:
- IEC 62443 compliance

Certification/Regulatory:
- Common Criteria certification
- BSPA certification

Connected Vehicles

Support & Preparation:
- Review of processes and consultancy in drafting/ implementation
- Workshops on cybersecurity and regulatory requirements
- Risk assessments on vehicles and components
- Penetration testing of components and systems

Compliance:
- ISO/SAE 21434 compliance gap analysis

Certification/Regulatory:
- UNECE Cybersecurity (R155) and Software Updates (R156) compliance gap analysis
- UNECE Cybersecurity (R155) and Software Updates (R156) type approval
- Common Criteria certification

Industrial Products

Support & Preparation:
- Design reviews
- Focused penetration testing
- Review of development processes and consultancy in drafting/ implementation
- IEC 62443 workshops

Compliance:
- IEC 62443 compliance gap analysis

Certification/Regulatory:
- IECEE certification (IEC 62443)
- Common Criteria certification

Secura
A BUREAU VERITAS COMPANY

About Secura

Secura is an independent, specialised security expert. We help organisations by **providing valuable insight into their digital security** from a **people, process and technology perspective.**

Secura offers **audit, test & certification services in the world of IT, IoT and OT**. We link our audit and test work to international norms, standards and metrics. Secura is your independent, trusted security partner.

Interested?

Would you like to learn more about our services?

Contact us today!

+31 88 888 31 00

info@secura.com

secura.com

Follow us:

BUREAU VERITAS

Shaping a World of Trust