



**BUREAU
VERITAS**

BUREAU VERITAS PARTNER OF YOUR CYBERSECURITY

CONTEXT & CHALLENGE :

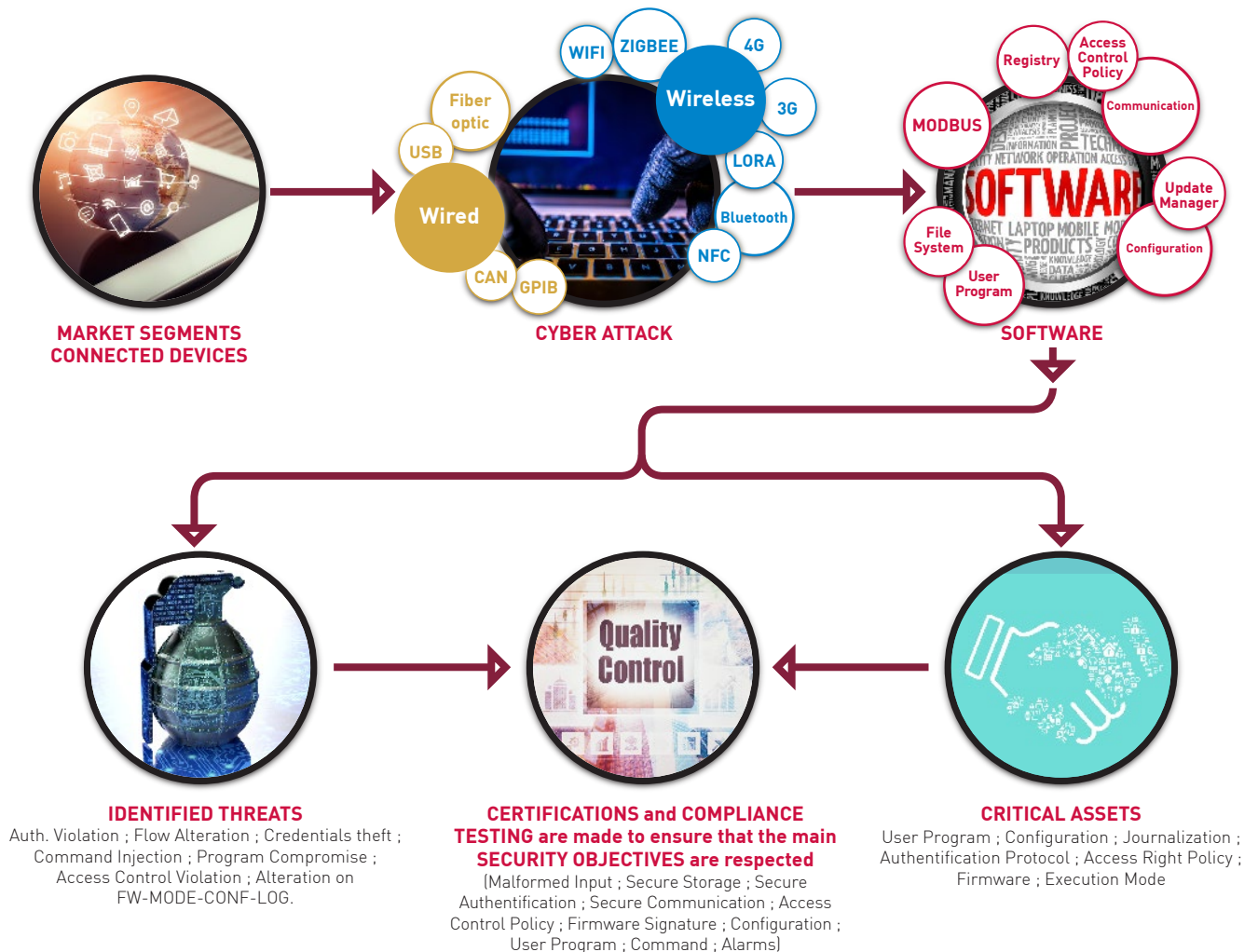
Cyber-attacks are about to become more aggressive and complex, especially within the IOT market area. It is estimated that by 2020, around 50 billion connected objects will be launched into markets, and more than one out of two devices will have an IoT security attack. As a trusted third party, Bureau Veritas can bring support to manufacturers and developers worldwide making their products safer and more secure.

Bureau Veritas compliance verification, testing and certification services can help you to develop a comprehensive and effective cybersecurity strategy that gathers a full spectrum of services and disciplines, from developing proactive defence capabilities to minimize damage if a violation happens.

Our experts can help you handle the following aspects :

- Threat management
- Cyber risks and standard compliance
- Security assessments
- Security architecture
- Security operations
- Analytics and reporting

Bureau Veritas helps you to identify security risks in products and systems and can suggest methods for mitigating those risks in a wide range of industry functions: industrial control systems, medical devices, automotive, HVAC, lighting, smart home, appliances, alarm systems, fire systems, building automation, smart meters, Marine & Offshore, network equipment, and consumer electronics.



OUR SOLUTION

The Bureau Veritas Cybersecurity Evaluation solutions :

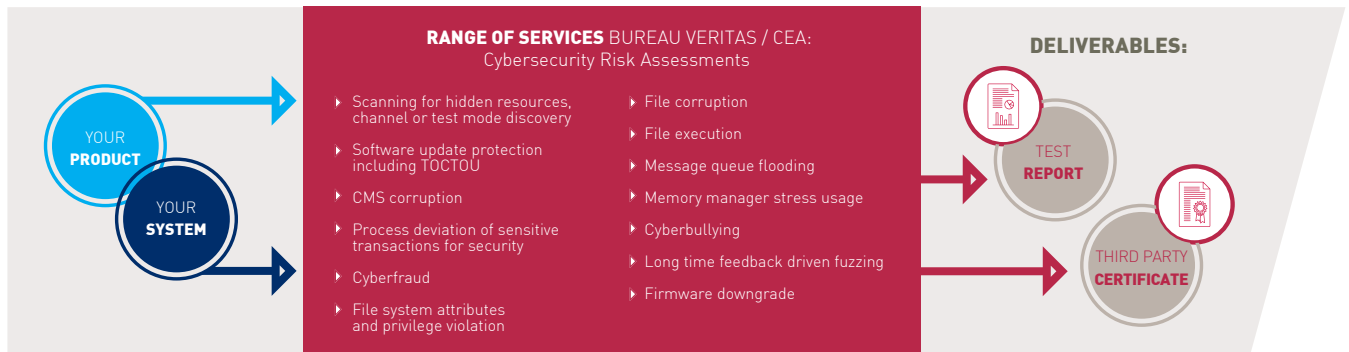
Assesment of network-connectable products and systems ; testing software and hardware to prevent vulnerabilities and weaknesses .

	Key points	Added Value & Results	Bureau Veritas Solution
Network System	<ul style="list-style-type: none"> Based on security standards Focused for Manufacturer & Supplier Several Security Levels Suitable for Automotive domain and all IoT domains 	<ul style="list-style-type: none"> Independent reference Pragmatic guidelines Possible issuing of a certificate of conformity Supplier specifications 	<ul style="list-style-type: none"> Technical documentation <ul style="list-style-type: none"> CAR CYBER SEC - 001 Working groups <ul style="list-style-type: none"> ECS0 WG IEC WG (CAR or SMB) ANSSI
Software	<ul style="list-style-type: none"> Based on security standards Focused on software development, validation and operation Leveraging source code analysis Including communication analysis (data protection & secure protocol) « White box » approach Suitable in all domains (IOT, Automotive, Industry, ...) 	<ul style="list-style-type: none"> Track software cybersecurity threats State-of-the-art methods Independent reference Pragmatic guidelines Possible issuing of a certificate of conformity Suitable for supplier specifications 	<ul style="list-style-type: none"> Technical documentation <ul style="list-style-type: none"> BV-SW-100 BV-SW-200 Testing <ul style="list-style-type: none"> Source code verification
Hardware	<ul style="list-style-type: none"> Based on security standards Focused for developers Emphasis on interfaces attacks : Abuse / Misuse / Fuzzing Automatic Compliance Testing : Quick results and reproducibility Several security levels « Black Box » approach Suitable in all domains (IOT, Automotive, Industry, ...) 	<ul style="list-style-type: none"> Track cybersecurity threats Innovative methodology Independent reference Possible issuing of a certificate of conformity Suitable for supplier specifications 	<ul style="list-style-type: none"> Technical documentation <ul style="list-style-type: none"> Good Practice Guidelines Testing <ul style="list-style-type: none"> Industrial Equipment Testing (Physical Conformity & Resistance)

Our testing process can help you to minimize exploitation, address known malware, review security controls and increase security awareness.

Bureau Veritas cybersecurity services for network-connectable product and systems include:

- Guidelines available on our website
- Evaluation and risk assessment of product security
- Testing security criteria based on cybersecurity standards or specified requirements
- Partnership Testing with CEA Leti, CEA List
- Issuing a certificate of conformity



DELIVERABLES:

Following the testing process, LCIE Bureau Veritas can deliver :
International compliance certificate : Bureau Veritas Cybersecurity Evaluation

WHY CHOOSE LCIE BUREAU VERITAS

A leading certifier within an international network of laboratories, we assess the compliance of Cybersecurity for electrical and electronic products and deliver national, European and international certification marks.

- LCIE Bureau Veritas is a worldwide recognized testing laboratory and certification body
- Multidisciplinary technical expertise under one roof
- Wide scope of testing capabilities
- Support at all stages of your product life cycle
- Third Party Laboratory, providing impartiality, consistency and confidentiality
- Partnership with CEA Leti, including access to Leti ITSEF for evaluations under the French Certification Scheme.

LCIE Bureau Veritas accompanies you from the development phase to the marketing of your products:

- Testing
- Assistance and expertise
- Audits and inspections

YOUR CONTACT :

contact@lcie.fr - +33.(0)1.40.95.60.60 - 33 Avenue du Général Leclerc, 92260 Fontenay-aux-Roses FRANCE