Committed to Europe

How can cybersecurity certification schemes enhance Europe's security and competitiveness?

Orange position in a nutshell

Cybersecurity Event
25 September 2018

Increase in cybersecurity threats and crimes is driving EU policy

“Cyber-attacks know no borders, but our response capacity differs very much from one country to the other, creating loopholes where vulnerabilities attract even more the attacks. The EU needs more robust and effective structures to ensure strong cyber resilience and respond to cyber-attacks. We do not want to be the weakest links in this global threat.”

Jean-Claude Juncker, Tallinn Digital Summit, 29 September 2017

Today’s cyber threats

+ 4 000 ransomware attacks per day in 2016

80% of European companies experienced at least one cybersecurity incident last year

Security incidents across all industries **rose by 38%** - the biggest increase in the past 12 years.

In some Member States **50% of all crimes committed** are cybercrimes

+150 countries and +230 000 systems across sectors and countries were affected by Wannycry attack in May 2017 with a substantial impact on essential services connected to the internet, including hospitals and ambulance services.

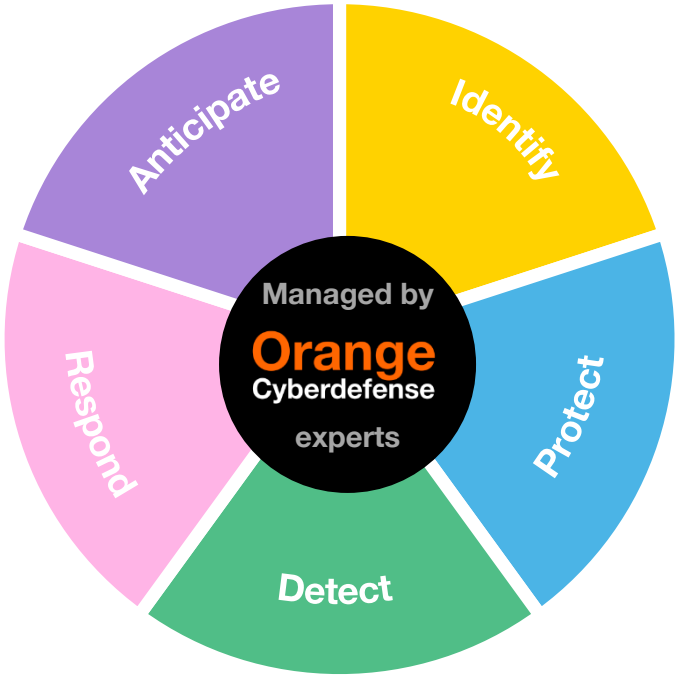
Source: STOEU Building strong Cybersecurity in Europe 12th Sept 2018

Contributing to a stronger Cyber resilient and Cyber secure EU by helping customers manage digital risk

Orange is an end-to-end service provider

Threat intelligence
Hunt and investigate emerging threats, fraud and data leaks

Crisis management and remediation
Qualify, contain and remediate attacks



Audit and consulting
Prepare your security strategy and ensure it is working

Infrastructure, access & data security
Defend and monitor your critical assets and data against cyber threats

Advanced threat detection
Analyze security events and detect breaches

Orange Cyberdefense
our dedicated security business unit

€272m FY 2017 revenue

720 multinational customers

30 years of experience in securing critical infrastructures

Top security services provider in France and a leader in Europe

ISO 27001 and NATO certified

+20% yearly revenue growth

1,200+ Orange Cyberdefense experts

Addressing all verticals: banks & insurance, transportation & logistics, health, manufacturing, utilities…

Cyberdefense Academy

A global presence and industry-leading capabilities

Independent CERT

Incidence response

Digital forensics

IoT / SCADA security

- 4 CyberSoc that bring together the best expertise in threat analysis
- 8 SoC around the world monitoring and responding to events 24/7/365
- 4 CERT around the world monitoring and responding to events 24/7/365
- 3 scrubbing centers to mitigate DDoS attacks

The EC : ‘Building a strong cybersecurity in Europe”

The EC has put forward proposals, building on the previous initiatives to:

1 Strengthen our resilience to cyber-attacks by:

Supporting effective implementation of the first EU cybersecurity law (NIS Directive) with:

- Improving Member States cybersecurity capabilities
- Increasing EU-level cooperation
- Risk prevention in key sectors to prevent and handle cyber incidents

Working with Member States on:

- Strengthening the EU Agency for cybersecurity to better assist Member States
- **Developing an EU Certification Framework to ensure that products & services are cyber-secure**
- Ensuring fast and coordinated responses to large scale cyber-attacks

2 Pooling resources and expertise in cybersecurity technology:

- Creating a network of competence centres & an EU Cybersecurity Industrial, Technology and Research Competence Centre relying on existing expertise in Member States

Source: STOEU Building strong Cybersecurity in Europe 12th Sept 2018

Cybersecurity Act :
A welcome framework for EU Cybersecurity Certification Schemes

- **Strengthen ENISA**
- **Create a framework for EU certification scheme of ICT products and services, to be applied on a voluntary basis**

Agenda

➔ Next trilogues : 01/10
➔ Political agreement sought by end 2018

Some key elements of the debate for Orange

Role of Industry

To be strengthened, allowing EU industry to suggest working on a given scheme and to be consulted during the adoption process

Voluntary nature of EU Cybersecurity Certification Schemes

This is an essential feature of the EC proposal taking into account the current heterogeneity among Member States and various bodies and entities involved in security assessment

Notion of Self Assessment

Is welcome as long as it is foreseen for basic level of assurance only and is not confused with the concept of a certificate

Cybersecurity Information Document on certified products and services for end-users

This risks raising serious difficulties to avoid over interpretation of such information by end users, and too complex procedures for manufacturers and providers

Thank You

More information: https://oran.ge/2D3hZ5q
Follow us on Twitter: @Orange_Brussels