NEWS RELEASE

FIC 2020 Forum International de la Cybersécurité 28, 29 & 30 janvier 2020 LILLE GRAND PALAIS

FIC 2020
TOWARDS A EUROPE OF CYBERSECURITY

Lille, 30 January 2020 - The International Cybersecurity Forum, which has just closed the doors of its 12th edition, at the Grand Palais in Lille, brought together more than 12,500 participants, including nearly 2,500 international visitors. An edition that once again underlines the European dimension of the event. The FIC 2020 was marked by the signature of the Strategic Sector Agreement and the announcements concerning the Cyber Campus. The essential rapprochement between the public and private sectors and the need for both a sovereign Europe and a sovereign France were also at the heart of the discussion.

THE FIC 2020 IN FIGURES

More than 110 countries represented

More than 12,500 visitors (+25 %)

500 public and private partners

40 foreign delegations

500 speakers

Lille: a great example of what Europe can do when it comes together

The entire European cybersecurity ecosystem met at the FIC 2020: publishers of solutions, client companies (CISOs, CIOs, CDOs, risk managers, business directors, etc.), lawyers and attorneys, public authorities (Ministry of the Interior, ANSSI, CNIL, Ministry of the Armed Forces, Ministry of Europe and European institutions and agencies (ENISA, EEAS, DG Connect...), ethical hackers, teacher-researchers, representatives of civil society, academics, students... A great variety of technical and non-technical profiles for a FIC that was resolutely open to building the 21st century Europe of cybersecurity.

Press Contacts: Cymbioz agency – Laëtitia Berché | Aurélien Rouby
+33 6 14 48 02 95 / +33 6 70 68 49 32 fic@cymbioz.com

Placing human beings at the heart of cybersecurity

While cybersecurity is most of the time approached from a purely technical or technological perspective, this year the FIC wanted to "*place human beings back at the heart of cybersecurity*". In fact, plural Human Beings, since they are at the same time the users (how to reconcile security and user experience?), the victims, who must be held harmless and educated, the attackers (with the need to better understand the operating methods and social engineering techniques used in 90% of attacks), the defenders (the change in the image of cybersecurity and the need to create vocations remain essential issues to overcome the shortage of talent in the sector) and finally the citizens, who are necessarily concerned by the major strategic issues related to digital technology (protection of personal data...). According to an IFOP survey carried out for the FIC and Acteurs publics, **85% of French people say they are concerned about the risks of cyberattacks**, while 87% express mistrust towards social networks when it comes to entrusting them with personal data.

Open digital sovereignty essential for Europe

"*Europe needs France and France needs Europe*," said **Guillaume Poupard, Director General of ANSSI** at the FIC 2020. As the world's second largest producer of data, Europe offers a unique opportunity to build a new form of sovereignty in the digital era. A sovereignty that is necessarily more nested and shared, but where everyone – civil society, companies and the State – plays a role. "*Neither private nor public sectors are the solution. The answer is necessarily cooperative and combines public and private sectors*," said **General Marc Watin-Augouard, founder of the FIC.**

Towards awareness of private sector decision-makers

The presence of companies from a wide range of sectors such as energy, transport, industry and retail (for example, Siemens or the Carrefour group) shows that cybersecurity has become a "business" issue that is no longer confined to security teams, but now concerns and preoccupies decision-makers. "*All the companies have already been attacked or will be attacked some day. There is no reason to be ashamed,*" says **Guillaume Tissier, CEO of CEIS.** "*For these companies, cybersecurity is not just an operational requirement, but it is also a real business and marketing advantage*".

Boosting the cybersecurity sector

The threat remains strong and the vulnerability surface expands. To the point where cybersecurity has become a "*major challenge for our institutions, companies and citizens. France has to become the nation of cybersecurity,*" said **Christophe Castaner, Minister of the Interior.** Concrete measures to fight all forms of cybercrime were announced at the FIC 2020 , including the forthcoming creation of 9 regional branches of the C3N and the Thésée platform to fight online scams (in 2019, 90,000 people visited the "cybermalveillance.gouv.fr" platform looking for help).

The highlight of the FIC 2020 was the ratification of the Strategic Sector Agreement, which solidifies the commitment of the State and the French industrials to give structure to the security domain and to set goals for each stakeholder. "*This agreement gives a new orientation to a sector that represents today 28 billion Euros and 130,000 jobs, and gathers SMEs as well as large industrial groups*," said **Agnès Pannier-Runacher, State Secretary to the Minister for Economic Affairs and Finance.**
Finally, the Cyber Campus, which will take shape in 2021 and will be led by **Orange Cyberdefence Chief executive Michel Van Den Berghe,** "*embodies the President of the Republic's desire to make cybersecurity a priority and demonstrates the stakeholders' desire to join their forces in order to work together a saying*

Press Contacts: Cymbioz agency – Laëtitia Berché | Aurélien Rouby
+33 6 14 48 02 95 / +33 6 70 68 49 32 fic@cymbioz.com

that marked this FIC 2020 and to initiate a project open to universities, schools, start-ups to generate vocations and find answers for the skilled people shortage that the sector is experiencing, amongst other purposes," announced **Cédric O, French Secretary of State for the Digital Economy.**

TOP 10 TRENDS AT THE FIC 2020

1 | **The development of a massive cybercrime,** leading to a multiplication of digital breaches of trust, affecting both businesses and the general public. Email remains a very frequent attack vector, but it is not the only one (phishing, hijacked websites, virus-infected software...).

2 | **Amplification of ransomware attacks,** with little technical innovation because traditional methods still work. However, operations are more targeted, better prepared, with better "returns on investment" for the attackers.

3 | **Increase in sophisticated attacks** targeting both selected core Internet infrastructures (BGP, DNS) as well as critical protocols and services, thus reinforcing the need to secure these key infrastructures.

4 | **Multiplication of rebound attacks targeting subcontractors.** Attackers are shifting their efforts towards weaker links in the value chains. This then allows them to hit more targets through a single point of entry.

5 | **The vulnerability surface is expanding** under the combined effect of IoT, cloud computing and soon 5G, which will accelerate nomadic uses.

6 | **Necessity of refocusing security on the user via the "zero trust" approach,** UEBA technologies, new identification/authentication technologies, UX improvement, etc.

7 | **Development of SOAR technologies** aiming to develop the automation of incident detection and response.

8 | **Gradual evolution of SOCs towards** "fusion centres" encompassing all areas of internal and external data security.

9 | **Need to strengthen the attractiveness of the sector** to attract more and more talented people. In a context of the development of AI-based solutions, human skills remain key...

10 | **The urgent need to translate the concept of digital sovereignty into action:** strengthening public and private purchasing, including from SMEs, the mobilisation of investment capacities, a better integration of the European market...

The FIC's next edition: 19, 20 & 21 January 2021, Grand Palais, Lille, France.

Key Facts About The International Cybersecurity Forum (FIC)

A genuine platform for meeting and discussions, the FIC positions itself as the reference event in Europe on digital trust and security. Its uniqueness: a FORUM for reflection and exchanges of best practices within the European cybersecurity ecosystem, and a TRADE SHOW dedicated to meetings between buyers and suppliers of cybersecurity solutions. It also hosts numerous partner events such as the Vauban Sessions (organised with CRR-FR and NATO), the ID Forum, the Coriin conference (digital investigation), as well as many hacking challenges and competitions. Each year, the FIC brings together the entire cyber ecosystem. Since 2013, the FIC (www.forum-fic.com) has been jointly organised by the Gendarmerie Nationale and CEIS, with the support of the Hauts-de-France region. You can follow @FIC_eu on Twitter or visit the Facebook page or the LinkedIn page to receive FIC news.

Press Contacts: Cymbioz agency – Laëtitia Berché | Aurélien Rouby
+33 6 14 48 02 95 / +33 6 70 68 49 32 fic@cymbioz.com