FIC 2019: THE KEY TAKEAWAYS

The International Cybersecurity Forum (FIC) was held on 22 and 23 January at Lille Grand Palais. With nearly 10,000 participants, the Forum confirms its position as a key event in Europe.

The 11th edition of the FIC was characterised by a marked increase in the number of participants and partners. As a forum open to the entire digital security and trust community, but also as a business fair dedicated to public and private cybersecurity operators, the FIC is now looking to play a key role in the development and promotion of a European vision for cybersecurity. As a dedicated forum with strong convictions, it now acts as a "think-tank" and "do-tank" throughout the year thanks to its many activities (Observatory, awards, publications, acceleration programme, etc.).

A Committed European Forum

Nearly 10,000 people (9,700 in total) were present in Lille on 22 and 23 January to participate in the International Cybersecurity Forum. An attendance up 15% compared to the previous year despite the heavy snowfall that disrupted transport to the Hauts-de-France Region. Many political figures made the trip: Laurent Nunez, State Secretary from the Ministry of the Interior, Florence Parly, Minister of the Armed Forces, Mariya Gabriel, European Commissioner for Digital Economy and Society, Julian King, European Commissioner for the Security Union.

Increased Internationalisation

The percentage of foreign visitors increased sharply (+20%), confirming the positioning of the FIC as a benchmark event in cybersecurity on the European and international stage. "Lille, for two days, stands as the world capital of cybersecurity," announced Richard Lizurey, Director General of the National Gendarmerie, during the opening speech. While the most represented countries are European, thus reinforcing the theme of this 2019 edition "Europe kicks off", the forum also hosted foreign delegations from more than 40 different countries (America and Asia, North Africa, West Africa, Middle East), who were specially present for the event.

A Space for Exchange between Experts and Non-Experts

More than 400 people took part in the forum segment of the event. The programme included a mix of specialists from industry, academia and government, digital transformation actors (CIOs, CDOs...), lawyers (DPOs, lawyers...) and business leaders. Philippe Knoche, CEO of Orano, pointed out for example in his opening keynote how, without being a player in the field, "cybersecurity had made its way into his business".

The FIC also provided an opportunity to welcome five "cyber commanders" (Germany, Switzerland, Estonia, Australia, Japan) who discussed their vision of "cyber" operations, while a delegation of French parliamentarians discussed the issue of digital identity in an "agora".

THE FIGURES FOR 2019

- 9,700 participants (+15%)
- +20% foreign visitors
- 40 foreign delegations
- 400 speakers
- 400 public & private partners

A meeting place for "end users", solution providers, service providers and innovative start-ups.

More than 400 public and private partners (including our main partner Hexatrust, as well as Orange Cyberdefence, a diamond partner) were present at the conference to showcase and unveil new cybersecurity solutions.

About a hundred SMEs and start-ups exhibited their latest innovations, including about thirty gathered in a dedicated space thus confirming French dynamism in this field.

A Space for Technical and Strategic Innovation

The quest for technical excellence was also expressed through the technical challenges (Capture The Flag or Defend The Flag) that this year attracted about 300 engineers and "ethical hackers".

A select gathering of public and private stakeholders was also held. This was initiated by the Ministry of Foreign Affairs to discuss the follow-up to President Macron's 'Paris Call' of November 2018. Meantime, a strategic challenge, based on an attack scenario involving critical infrastructure, was won by the prestigious West Point U.S. Military Academy.

FIC 2019: THE KEY TAKEAWAYS

Mariya Gabriel, the European Commissioner for Digital Economy and Society, announced an increase in ENISA's budget as well as the creation of a common cybersecurity certification system, the development of a new "Digital Europe" programme (cybersecurity, AI...), and support for the training and feminisation of the sector...

Trends for 2019

- **Fear of Attacks with Systemic Impacts.** Guillaume Poupard, ANSSI's DG, after the *Wannacry* and *NotPetya* attacks, stressed that a "Digital Pearl Harbor" is likely, recalling the Agency's slogan *“all connected, all involved, all responsible.”*
- **Attacks targeting all levels of the digital space**: infrastructures (denial of service, sabotage), data (data theft, ransomware...) and public opinion ("fake news").
- **Specific threats** to the cloud, the Internet of Things or industrial systems.
- **Proteiform attackers:** aggressive behaviour by some States, the rise of structured cybercriminal groups.
- **A shared certainty**: digital transformation will not continue without user confidence, and therefore without cybersecurity. Cybersecurity is gradually becoming a marketing tool.

What solutions ?

- **"By design", the theme of the 2019 edition,** which consists in integrating security and privacy upstream of projects and managing this throughout the entire product lifecycle.
- **The development of a cooperative approach** between citizens, between companies, between companies and States, between States themselves (see the keynote address of John Frank, Microsoft Vice-President for European Affairs.)
- **The emergence of a "European Model"**: the European Union is at the forefront thanks to a unique legislative and regulatory environment (GDPR, NIS Directive, Cyber Act) and a strong commitment to investment and "capacity building."
- **The contribution of artificial intelligence**, to anticipate and detect threats or to orchestrate incident response.
- **The development of Cyber Threat Intelligence capabilities** and the advent of "autoimmune" systems to reverse the balance of power ("We must move from cyber security to cyber immunity", said antivirus publisher Eugène Kaspersky).
- **Capacity building for training and education** to meet the need for skills in the field (larger "Careers & Jobs" space in the forum; more schools, training offers and operational training centres).

www.forum-fic.com

@FIC_fr · FIC · Forum FIC