COMMUNIQUÉ DE PRESSE

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

FIC 2020
VERS LA CONSTRUCTION D'UNE EUROPE DE LA CYBERSÉCURITÉ

Lille, le 30 janvier 2020 - Le Forum International de la Cybersécurité qui vient de fermer les portes de sa 12ème édition, au Grand Palais de Lille, a rassemblé plus de 12 500 participants, dont près de 2500 visiteurs internationaux. Une édition qui souligne une nouvelle fois la dimension européenne prise par l'événement. Un FIC 2020 marqué par la signature du Contrat Stratégique de Filière et les annonces autour du Campus Cyber. L'indispensable rapprochement entre le public et le privé et la nécessité d'une Europe et d'une France souveraine ont également été au cœur des échanges.

LE FIC 2020 EN CHIFFRES

Plus de 110 pays représentés

Plus de 12 500 visiteurs (+25 %)

500 partenaires privés et publics

40 délégations étrangères

500 intervenants

Lille : un bel exemple de ce que peut faire l'Europe lorsqu'elle se réunit

Tout l'écosystème européen de la cybersécurité s'était donné rendez-vous au FIC 2020 : éditeurs de solutions, entreprises clientes (RSSI, DSI, CDO, risk managers, directeurs métiers...), juristes et avocats, autorités publiques (ministère de l'Intérieur, ANSSI, CNIL, ministère des Armées, ministère de l'Europe et des Affaires étrangères...), institutions et agences européennes (ENISA, SEAE, DG Connect...), hackers éthiques, enseignants-chercheurs, représentants de la société civile, universitaires, étudiants ... Des profils variés, techniques et non-techniques, pour un FIC résolument ouvert pour construire une Europe de la cybersécurité.

Contacts presse : Agence Cymbioz – Laëtitia Berché | Aurélien Rouby
06 14 48 02 95 / 06 70 68 49 32 fic@cymbioz.com

L'Humain au cœur de la cybersécurité

Alors que la cybersécurité est la plupart du temps abordée sous un angle purement technique ou technologique, le FIC a voulu cette année "Replacer l'Humain au cœur de la cybersécurité". Un Homme pluriel puisqu'il est à la fois l'utilisateur (comment réconcilier sécurité et expérience utilisateur ?), la victime, qu'il faut déculpabiliser mais aussi sensibiliser, l'attaquant (avec la nécessité de mieux comprendre les modes opératoires et les techniques d'ingénierie sociale utilisée dans 90% des attaques), le défenseur (le changement d'image de la cybersécurité et le besoin de créer des vocations restent des enjeux essentiels pour palier à la pénurie de talents dans la filière) et enfin le citoyen, nécessairement concerné par les grands enjeux stratégiques liés au numérique (protection des données personnelles...). Selon un sondage IFOP réalisé pour le FIC et Acteurs publics, **85% des français se disent ainsi inquiets des risques de cyber-attaques,** tandis que 87% expriment leur méfiance à l'encontre des réseaux sociaux lorsqu'il s'agit de leur confier des données personnelles.

Une souveraineté numérique ouverte essentielle pour l'Europe

"*L'Europe a besoin de la France et la France a besoin de l'Europe*" a déclaré **Guillaume Poupard, directeur général de l'ANSSI lors du FIC 2020**. Deuxième producteur de données mondial, l'Europe offre une opportunité unique pour construire une nouvelle forme de souveraineté à l'ère numérique. Une souveraineté forcément plus imbriquée, plus partagée, mais où chacun, société civile, entreprises et État jouent leur rôle. « *Le privé seul n'a pas la solution, le public non plus. La réponse est nécessairement coopérative et associe à la fois le public et le privé* », souligne **le général Marc Watin-Augouard, fondateur du FIC**.

Vers une prise de conscience des décideurs privés

La présence au FIC d'entreprises de très nombreux secteurs d'activité comme l'énergie, le transport, l'industrie ou bien encore la grande distribution (avec par exemple la présence de Siemens ou du groupe Carrefour) montre que la cybersécurité est devenue un véritable enjeu "métier" qui n'est plus circonscrit aux équipes sécurité, mais qui concerne et préoccupe désormais les décideurs. "*Toutes les entreprises se sont déjà faites attaquées ou le seront un jour. Il n'y pas de honte à avoir.*" souligne **Guillaume Tissier, Président de CEIS**. "Pour ces entreprises, la cybersécurité est non seulement une exigence opérationnelle mais également un véritable avantage business et marketing".

Coup d'accélérateur de la filière cyber

La menace ne faiblit pas et la surface de vulnérabilité progresse. Au point que la cybersécurité est devenue un "*enjeu majeur pour nos institutions, nos entreprises, nos citoyens. Nous devons faire de la France, la patrie de la cybersécurité*", a déclaré **Christophe Castaner, ministre de l'Intérieur.** Pour lutter contre toutes les formes de cybercriminalité, des mesures concrètes ont été annoncées au FIC 2020 dont la création prochaine de 9 antennes régionales du C3N et la plateforme Thésée pour lutter contre les escroqueries en ligne (90 000 personnes venues chercher de l'assistance sur la plateforme cybermalveillance.gouv.fr en 2019).

Temps fort du FIC 2020, la signature du Contrat Stratégique de Filière vient concrétiser l'engagement de l'État et des industriels français pour structurer la filière sécurité et fixer des objectifs pour chacune des parties prenantes. "*Ce contrat vient donner une nouvelle orientation à une filière qui représente aujourd'hui 28 milliards d'euros et 130 000 emplois, et regroupant tant des PME que des grands groupes*" a confié **Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'Économie et des Finances.**
Enfin, le Cyber Campus mené par **Michel Van Den Berghe, directeur général d'Orange Cyberdéfense**, qui verra le jour en 2021, vient, selon **Cédric O, Secrétaire d'État chargé du Numérique** : "*incarner la*

Contacts presse : Agence Cymbioz – Laëtitia Berché | Aurélien Rouby
06 14 48 02 95 / 06 70 68 49 32 fic@cymbioz.com

volonté du Président de la République de faire de la cybersécurité une priorité et témoigne de la volonté des acteurs de mettre en commun leurs forces pour travailler ensemble – un mot qui a marqué ce FIC 2020 – et engager un projet ouvert aux universités, aux écoles, aux start-up pour notamment susciter des vocations et trouver des réponses au déficit de talents que connait la filière".

10 TENDANCES CLÉS FIC 2020

1 | **Développement d'une cybercriminalité massive,** se traduisant par une multiplication des abus de confiance version "numérique" touchant à la fois les entreprises et le grand public. Le mail reste un vecteur d'attaque très fréquent mais n'est pas le seul (phishing, site web usurpés, logiciels infectés...).

2 | **Amplification des attaques par ransomware,** sans qu'il y ait eu beaucoup d'innovation technique puisque les recettes traditionnelles fonctionnent toujours. Les opérations sont en revanche plus ciblées, mieux préparées, avec donc de meilleurs retours sur "investissement" pour les attaquants.

3 | **Croissance des attaques sophistiquées** visant à la fois certaines infrastructures-cœur d'internet (BGP, DNS) et les protocoles et services critiques, ce qui renforce le besoin de sécurisation de ces infrastructures névralgiques.

4 | **Multiplication des attaques par rebond visant des sous-traitants.** Les attaquants déplacent leurs efforts vers des maillons plus faibles dans une chaine de valeur. Via un point d'entrée unique, cela leur permet ensuite de toucher davantage de cibles.

5 | **Progression de la surface de vulnérabilités** sous l'effet conjugué de l'IoT, du cloud computing et bientôt de la 5G qui va accélérer les usages nomades.

6 | **Nécessité d'un recentrage de la sécurité sur l'utilisateur** avec l'approche "zero trust", les technologies UEBA, de nouvelles technologies d'identification/authentification, l'amélioration de l'UX, etc.

7 | **Essor des technologies SOAR** visant à développer l'automatisation de la détection et de la réaction aux incidents.

8 | **Évolution progressive des SOC** vers des "fusion center" intégrant l'ensemble des domaines de sécurité, des données internes et externes.

9 | **Besoin de renforcer l'attractivité de la filière** pour attirer toujours plus de talents. Dans un contexte de développement des solutions à base d'IA, les compétences humaines restent clés...

10 | **Nécessité urgente de traduire en actions le concept de souveraineté numérique :** renforcement de l'achat public et privé, y compris auprès de PME, mobilisation des capacités d'investissement, meilleure intégration du marché européen...

Prochaine édition du FIC : les 19, 20 et 21 janvier 2021, au Grand-Palais à Lille.

À propos du Forum International de la Cybersécurité (FIC)

Véritable plateforme d'échanges et de rencontres, le Forum International de la Cybersécurité (FIC) s'est imposé comme l'événement de référence en Europe en matière de sécurité et de confiance numériques. Son originalité est de mêler : un FORUM favorisant la réflexion et l'échange au sein de l'écosystème européen de la cybersécurité, et un SALON dédié aux rencontres entre acheteurs et fournisseurs de solutions de cybersécurité. Il accueille aussi de nombreux événements partenaires comme les Vauban Sessions (organisé avec le CRR-FR et l'OTAN), l'ID Forum, la conférence Coriin (investigation numérique) ainsi que de nombreux challenges et compétitions de hacking. Le FIC regroupe ainsi chaque année l'ensemble de l'écosystème cyber. Le FIC (www.forum-fic.com) est organisé depuis 2013 conjointement par la Gendarmerie Nationale et CEIS avec le soutien de la région Hauts-de-France. Vous pouvez suivre @FIC_eu sur Twitter ou consulter la page Facebookk pour suivre l'actualité du FIC ou encore la page LinkedIn.

Contacts presse : Agence Cymbioz – Laëtitia Berché | Aurélien Rouby
06 14 48 02 95 / 06 70 68 49 32 fic@cymbioz.com