Paris, le 28 janvier 2019

FIC 2019 : CE QU'IL FAUT RETENIR

Le Forum International de la Cybersécurité (FIC) s'est tenu les 22 et 23 janvier au Grand Palais de Lille. Avec près de 10 000 participants, le Forum confirme sa place d'événement leader au niveau européen.

La 11ème édition du FIC a été marquée par une forte progression du nombre de participants et de partenaires. Forum ouvert à l'ensemble de l'écosystème de la sécurité et de la confiance numérique, mais aussi salon « business » dédié aux acteurs publics et privés de la cybersécurité, le FIC entend aujourd'hui jouer un rôle clé dans l'élaboration et la promotion d'une vision européenne de la cybersécurité. Forum engagé portant des convictions fortes, il agit aujourd'hui comme un « think-tank » et un « do tank » tout au long de l'année grâce à des activités multiples (observatoire, prix, publications, programme d'accélération…).

Un Forum européen engagé

Près de 10 000 personnes (9700 au total) étaient présentes à Lille les 22 et 23 janvier pour participer au Forum International de la Cybersécurité. Une affluence en hausse de 15% par rapport à l'édition précédente malgré les fortes chutes de neige ayant perturbé les transports vers la Région Hauts-de-France la semaine dernière. De nombreuses personnalités politiques avaient fait le déplacement : Laurent Nunez, secrétaire d'Etat auprès du Ministère de l'intérieur, Florence Parly, ministre des Armées, Mariya Gabriel, commissaire européenne à la société et à l'économie numérique, Julian King, commissaire européen à l'Union de la sécurité.

Une internationalisation accrue

Le pourcentage de visiteurs étrangers connait une forte hausse (+20%), confirmant le positionnement du FIC comme événement de référence en matière de cybersécurité sur la scène européenne et internationale. « *Lille est pendant deux jours la capitale mondiale de la cybersécurité* » annonçait Richard Lizurey, Directeur général de la Gendarmerie nationale, lors du discours d'ouverture. Si les pays européens sont les plus représentés, confortant le thème de cette édition 2019 "*Europe kicks off*", le forum accueille également des délégations étrangères de plus de 40 pays différents (Amérique et Asie, Afrique du Nord, de l'Ouest, Moyen-Orient), spécialement présentes pour l'occasion.

Un lieu d'échange entre experts et non-experts

Plus de 400 personnes sont intervenues sur la partie forum de l'événement, avec un programme faisant interagir des spécialistes issus du monde industriel, universitaire et étatique, des acteurs de la transformation numérique (DSI, CDO…), des juristes (DPO, avocats…) et des dirigeants d'entreprises. Philippe Knoche, CEO d'Orano soulignait par exemple dans sa *keynote* d'ouverture comment, sans être un acteur du domaine, « *la cybersécurité s'était invitée dans son business* ».

Le FIC fut aussi l'occasion d'accueillir 5 « cyber commanders » (Allemagne, Suisse, Estonie, Australie, Japon) qui ont échangé sur leur vision des opérations « cyber », tandis qu'une délégation de parlementaires français échangeait sur la question de l'identité numérique dans une « agora ».

LES CHIFFRES 2019

- 9 700 participants (+ 15%)
- +20% d'internationaux
- 40 délégations étrangères
- 400 intervenants
- 400 partenaires privés et publics

Un lieu de rencontre entre « utilisateurs finaux », offreurs de solutions, prestataires de services et startups innovantes

Plus de 400 partenaires publics et privés (dont Hexatrust, partenaire principal et Orange Cyberdéfense, partenaire *diamond*) étaient présents sur le salon pour présenter et découvrir de nouvelles solutions en matière de cybersécurité.

Les PME et startups étaient une centaine à exposer leurs dernières innovations, dont une trentaine réunie sur un espace dédié, confirmant le dynamisme français en la matière (voir le Panorama de l'Innovation Cyber FIC 2019).

Un lieu d'innovation technique et stratégique

La recherche d'excellence technique s'est également exprimée à travers les challenges techniques (*Capture The Flag* ou *Defend The Flag*) qui ont attiré cette année environ 300 ingénieurs et « hackers éthiques ».

Une réunion restreinte, réunissant acteurs publics et privés, a également été organisée, à l'initiative du Ministère des affaires étrangères, pour réfléchir aux suites de l'Appel de Paris lancé par le Président Macron en novembre 2018, tandis qu'un challenge stratégique, basé sur un scénario d'attaque touchant des infrastructures critiques a été remporté par la prestigieuse Académie américaine de West Point.

FIC 2019 : CE QU'IL FAUT RETENIR

La commissaire européenne a également annoncé l'augmentation du budget de l'ENISA, la création d'un système de certification de cybersécurité commun, le développement d'un nouveau programme "Europe numérique" (cybersécurité, IA..), l'accompagnement pour la formation et la féminisation du secteur…

Tendances 2019

- **La crainte d'attaques aux impacts systémiques.** Après les attaques *Wannacry* et *NotPetya, un* « Pearl Harbor numérique » est probable, a souligné Guillaume Poupard, DG de l'ANSSI, rappelant le mot d'ordre de l'Agence « *tous connectés, tous impliqués, tous responsables* ».
- **Des attaques visant toutes les couches de l'espace numérique** : les infrastructures (déni de service, sabotage), les données (vol de données, ransomware…) et les opinions publiques (« fake news »).
- **Des menaces spécifiques** visant le cloud, l'Internet des objets ou les systèmes industriels.
- **Des attaquants protéiformes** : comportements agressifs de certains Etats, montée en puissance de groupes cybercriminels structurés.
- **Une certitude partagée** : la transformation numérique ne pourra plus se poursuivre sans confiance des utilisateurs, et donc sans cybersécurité. La cybersécurité devient progressivement un argument marketing.

Quelles solutions ?

- **Le « by design », thème de l'édition 2019,** qui consiste à intégrer la sécurité et la « privacy » en amont des projets et à la gérer tout au long du cycle de vie des produits.
- **Le développement d'une approche coopérative** entre les citoyens, entre les entreprises, entre les entreprises et les Etats, entre les Etats eux-mêmes (voir la keynote de John Frank, Vice-Président de Microsoft pour les affaires européennes.)
- **L'émergence d'un « modèle européen »** : l'Union européenne est en pointe grâce à un environnement législatif et normatif unique (RGPD, NIS, Cyber Act) et à une volonté forte d'investissement et de « capacity building ».
- **L'apport de l'intelligence artificielle,** qu'il s'agisse d'anticiper et de détecter les menaces ou d'orchestrer la réponse à incident.
- **Le développement des capacités de Cyber Threat Intelligence** et l'avènement de systèmes « auto-immunes » pour inverser le rapport de force (« Nous devons passer de la cyber-sécurité à la cyber-immunité » a déclaré l'éditeur d'antivirus Eugène Kaspersky).
- **Le renforcement des capacités de formation et d'entrainement** pour combler le besoin en compétences dans le domaine (espace « Careers & Jobs » renforcé sur le forum, présence davantage d'écoles, de formations et de centres d'entrainement opérationnels).