Communiqué de presse

Le Forum InCyber 2024 se tiendra du 26 au 28 mars à Lille sur le thème : « *Ready for AI?* »

L'ensemble de l'écosystème public et privé se réunira autour des enjeux de cybersécurité à l'ère de l'IA.

Paris et Lille, le 29 juin 2023 - Le Forum InCyber 2024 se tiendra du 26 au 28 mars, à Lille, autour du thème « *Ready for AI? - Réinventer la cybersécurité à l'ère de l'IA* ». Cette 16ème édition sera consacrée aux bouleversements engendrés par l'intelligence artificielle et à leur impact sur la sécurité et la confiance numérique.

Entre fantasme dystopique et techno-béatitude, difficile de savoir où l'intelligence artificielle (IA) va mener l'Humanité. Une chose est sûre : rien ne sera plus comme avant. Les activités professionnelles, vies personnelles, façons de penser, de décider, d'agir, de consommer, de produire, de se soigner vont s'en trouver durablement bouleversées. Mais le monde de demain dépendra surtout de ce que les utilisateurs vont collectivement décider de faire, ou de ne pas faire, avec l'intelligence artificielle et de la "confiance" qu'ils arriveront à construire "dans" et "par" ces technologies.

« *L'IA est au service de la cybersécurité ; et celle-ci contribue à une IA de confiance. Le Forum InCyber porte un regard clairvoyant et optimiste sur la rencontre entre l'IA et la cybersécurité, convaincu que notre avenir numérique repose sur la maîtrise de leur union* », précise **Marc-Watin-Augouard, président du Forum InCyber.**

Les "*IA de confiance*" devront, selon la Commission européenne, respecter 7 principes, parmi lesquels la robustesse technique et la sécurité, le respect de la vie privée et la gouvernance des données. La généralisation de ces technologies va en effet introduire des risques nouveaux en raison de l'augmentation de la surface d'attaque induite, de leurs vulnérabilités intrinsèques (attaques par empoisonnement, attaques adverses…) mais aussi de leur utilisation par les attaquants. Ceux-ci l'utilisent désormais tout au long de la "*kill chain*" pour reconnaître une cible, contourner les mécanismes de protection, construire des "*deep fake*", automatiser une attaque etc.

Le premier défi est donc de sécuriser les intelligences artificielles mais aussi les données qu'elles ingèrent et produisent. Et les chiffres donnent le vertige : chaque seconde, ce sont 7 mégabytes de données qui sont créées pour chaque personne, avec pour conséquence une quantité globale de données qui atteindra 181 zettaoctets en 2025 (contre 2 zettaoctets en 2010).

Heureusement l'IA révolutionne aussi "l'art de la cybersécurité" en nous permettant d'améliorer les capacités d'authentification des utilisateurs, de sécurisation des données, de détection des menaces, d'analyse de code, d'orchestration, de réponse à incident etc. Un bond technologique qui doit également conduire à réinventer en profondeur les doctrines, les organisations, les compétences, pour qu'elles soient "*AI - ready*".

« *Cantonnée depuis plusieurs années aux offres cyber annonçant toutes ou presque de l'IA inside, cette dernière vient de faire une entrée en fanfare dans l'agenda des RSSI. Qu'on le veuille ou non, il va falloir composer avec* » explique **Alain Bouillé, président du CESIN, membre du Comité scientifique du Forum.**

D'après **Yann Bonnet, directeur général délégué du Campus Cyber**, et autre membre du Comité **:** « *L'IA est à la fois un remède et un poison pour notre société. A nous, experts de la cybersécurité, d'agir pour qu'elle s'oriente vers un numérique de confiance* ».

« *Les capacités extraordinaires de l'IA peuvent contribuer à lutter contre la cybercriminalité et le cyberharcèlement. Mobiliser l'écosystème est alors essentiel pour en maîtriser collectivement l'usage. Toutes et tous ensemble soyons convaincus du rôle de l'IA et d'en utiliser pleinement les impacts dans un esprit éthique et de confiance pour réinventer la cybersécurité* », poursuit **Gaëlle Picard-Abezis, co-présidente de la commission Data et confiance de l'ACSEL, membre du Comité scientifique.**

"*De nombreuses solutions de cybersécurité utilisent déjà l'intelligence artificielle. Mais cette révolution technologique n'en n'est qu'à ses débuts. Nous allons devoir collectivement réinventer la cybersécurité, et, en miroir, faire évoluer le rôle des experts pour qu'ils soient "AI ready"*, conclut **Guillaume Tissier, directeur général du Forum InCyber - Europe.**

<u>Quelques thématiques proposées par le comité scientifique du Forum InCyber :</u>

- Les arnaques dopées à l'IA : deep fake, deep voice, les nouvelles techniques de phishing utilisant l'IA.
- L'IA va-t-elle changer la vie du RSSI ? Indicateurs, surface d'exposition, anticipation des menaces etc., l'IA peut-elle jouer un rôle de co-pilote ?
- Cherche IA résiliente pour systèmes critiques. L'IA est souvent considérée comme un avantage en termes de résilience globale en raison de l'automatisation de certaines tâches qu'elle permet. Mais la question de la résilience des IA se pose aussi, surtout pour nos systèmes critiques.
- Le Cyber Solidarity Act en pratique. Proposé par la Commission européenne le 18 avril 2023 et annoncé par Thierry Breton lors du FIC 2023, son objectif est de renforcer la préparation, la détection et la réponse aux incidents cyber.
- L'IA pour démocratiser la cybersécurité auprès des PME ? L'IA peut jouer un rôle clé pour faire face à la pénurie de ressources et répondre aux contraintes et besoins de petites structures.

A propos du Forum InCyber

Le Forum InCyber est aujourd'hui le principal événement européen sur la sécurité et la confiance numérique.
L'événement, qui associe un forum, un salon et un sommet en présence de nombreuses institutions et entreprises françaises et étrangères, regroupe l'ensemble de l'écosystème de la sécurité numérique et du numérique de confiance : clients finaux, offreurs de services et de solutions, administrations, collectivités, organismes de recherches, associations.
La deuxième édition Nord-américaine se tiendra les 25 et 26 octobre 2023 à Montréal, au Canada.

Contacts presse :
Agence Cymbioz : fic_presse@cymbioz.com - 06 14 48 02 95 I 06 64 90 32 47