Programme

Événements associés

CF
CYBERSECURITY FOR INDUSTRY

ID &KYC FORUM

TRUST &SAFETY FORUM

W3S
WEB3 SECURITY SUMMIT

INCYBER INVESTOR DAY

JOURNÉE OSINT

FORUM INCYBER EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Ready for AI?

Réinventer la cybersécurité à l'ère de l'IA

FORUM IN CYBER EUROPE

Nos activités professionnelles, nos vies personnelles, nos façons de penser, de décider, d'agir, de consommer, de produire, de nous soigner vont s'en trouver durablement bouleversées. Mais le monde de demain dépendra surtout de ce que nous allons collectivement décider de faire-ou de ne pas faire - avec l'intelligence artificielle et de la « confiance » que nous arriverons à construire « dans » et « par » ces technologies.

Pour être « de confiance », les IA 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 non seulement de l'augmentation de la surface d'attaque mais aussi de leurs vulnérabilités intrinsèques (attaques par empoisonnement, attaques adverses...).

Le progrès technologique étant ambivalent par nature, les IA sont également utilisées par les attaquants 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. Données et intelligence artificielle sont en effet indissociables. 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 nos capacités d'authentification, de sécurisation des données, de détection des menaces, d'analyse de code, d'orchestration, de réponse à incident etc. Un bond technologique qui doit aussi nous conduire à réinventer en profondeur nos doctrines, nos organisations, nos compétences, pour qu'elles soient « AI - ready ».

Liste des parcours thématiques

→ TABLES RONDES

- CFI
- ID&KYC Forum
- Trust & Safety Forum
- Web3 Security Summit
- InCyber Investor Day
- Journée OSINT

CFI

CYBERSECURITY
FOR INDUSTRY

FORUM INCYBER EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Cybersecurity For Industry, est l'événement associé du Forum InCyber dédié aux problématiques de cybersécurité du monde industriel. Unique en Europe, il est un carrefour d'échanges et de découverte des solutions de cybersécurité pour l'industrie, ainsi que des solutions industrielles sécurisées.

Tables rondes

Mise en place de la cybersécurité dans les réseaux OT et les systèmes industriels : retours du terrain

Les technologies opérationnelles (TO) et les systèmes de contrôle industriel (SCI) jouent un rôle fondamental pour les infrastructures critiques, dans des domaines tels que l'énergie, les transports et l'approvisionnement en eau. Cependant, ces systèmes font face à des menaces croissantes de la part d'acteurs malveillants. Il est crucial de comprendre comment ces attaquants exploitent les vulnérabilités spécifiques de ces systèmes et d'évaluer les conséquences potentielles d'une intrusion réussie. Le renforcement de la résilience des systèmes TO/SCI est de la plus haute importance pour assurer la continuité des services essentiels dans notre société moderne. Un retour du terrain pour appréhender concrètement ces enjeux cruciaux.

Comment assurer la protection des systèmes autonomes ?

L'avènement des systèmes autonomes, tels que les véhicules autonomes, les drones et les robots industriels, promet d'améliorer l'efficacité, la précision et la sécurité dans divers domaines. Cependant, cette autonomie croissante engendre un défi majeur en matière de cybersécurité, en particulier dans les Technologies Opérationnelles (OT). La question centrale est de concilier l'autonomie des systèmes avec leur cybersécurité. Comment concevoir des systèmes autonomes capables de prendre des décisions complexes tout en résistant aux attaques sophistiquées ? Comment protéger les infrastructures critiques basées sur des systèmes OT autonomes ?

Tables rondes

Sécuriser l'ensemble de la chaîne logistique dans le cadre de l'usine connectée

La sécurisation de l'ensemble de la chaîne logistique au sein d'une usine connectée est une préoccupation majeure dans l'ère de l'industrie 4.0. Dans ce contexte, l'objectif principal est de garantir la continuité des opérations tout en protégeant les données et les processus industriels sensibles. Les usines connectées intègrent des technologies avancées telles que l'Internet des objets (IoT), l'automatisation, la robotique, et les systèmes de gestion informatisée. Cela permet une efficacité accrue, une meilleure gestion des stocks et une traçabilité améliorée, mais cela expose également l'ensemble de la chaîne logistique à de nouveaux risques de sécurité. Quels sont les risques potentiels dans l'usine connectée, et comment peuvent-ils être évalués pour mettre en place des mesures de sécurité adéquates ? Comment garantir la cybersécurité des systèmes de contrôle industriel (SCI) tout en maintenant la disponibilité et la performance des équipements dans une usine connectée ?

Micro-segmentation : Clé de la résilience OT ?

La micro-segmentation dans l'environnement industriel représente un enjeu majeur à l'ère de la numérisation et de l'automatisation croissante. Cette approche consiste à diviser les réseaux informatiques en segments, isolant ainsi les différentes parties de l'infrastructure industrielle les unes des autres, renforçant de fait la sécurité des systèmes industriels. En isolant chaque composant ou appareil, elle limite la propagation des menaces potentielles au sein du réseau. Chaque segment peut être configuré avec des règles spécifiques, autorisant ou interdisant la communication avec d'autres segments. En conséquence, elle offre une réponse proactive aux menaces cybernétiques, préservant l'intégrité et la performance des entreprises industrielles. Comment peut-elle aider les entreprises à renforcer leur sécurité dans un contexte industriel ? Quelles sont les meilleures pratiques pour maintenir une micro-segmentation efficace à long terme dans un environnement industriel en constante évolution ?

ID &KYC FORUM

Rencontres annuelles
26 et 27 mars 2024

FORUM IN CYBER EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

THÈME 2024
Le client au cœur des mutations technologiques

Santé, banque, transport, éducation, administration en ligne… : l'identité numérique est désormais au coeur des activités économiques et de la vie citoyenne.

Tables rondes

Spécial anniversaire 5 ans ID&KYC Forum

Bilan et perspectives de l'identité numérique (et de la KYC) en France et en Europe

A l'occasion de son cinquième anniversaire, l'ID&KYC Forum invite plusieurs personnalités nationales et internationales à s'exprimer sur le bilan et les perspectives de l'identité numérique.
Qu'est ce qui a été réalisé en France au cours des cinq dernières années ? Quels ont été les échecs et les réussites ? Ou se situe la France par rapport à l'évolution du paysage européen et aux progrès accomplis par ses voisins ? Comment les différents segments de marchés utilisent les solutions proposées par le gouvernement et le secteur privé ? Quelle est la courbe d'adoption par le grand public ? Quelles sont les priorités pour cinq prochaines années ? Existe-t-il un consensus vis à vis de ces priorités ?

« Package anti-blanchiment » et nouveau « cadre de l'identité numérique » : quels impacts en Europe ?

Au cœur des enjeux d'identité numérique et de connaissance des clients et partenaires, deux grands règlements européens suivent des calendriers parallèles et seront selon toute probabilité définitivement adoptés lors de notre Forum. Comment vont-ils impacter l'activité des entreprises et la vie des ménages ? En quoi ces textes marquent une évolution voire une révolution dans les pratiques de relation client et distribution des services numériques ? Existe-t-il des synergies et interactions entre ces règlements ? Quel seront leurs impacts respectifs et combiné ? Comment se préparer à l'arrivée des nouvelles règles ? Quels sont les textes d'accompagnement et d'implémentations ? Comment les interpréter ? Quelles évolutions ou mises à jour sont à prévoir pour les entreprises ?

Tables rondes

Portefeuille électronique : quelle stratégie d'intermédiation numérique pour demain ?

Aujourd'hui plus d'une transaction sur deux du commerce électronique dans le monde, est réalisée via les téléphones mobiles. Au travers de l'apport d'une simplicité ergonomique, d'une sécurité applicative et d'une garantie juridique, l'essor des portefeuilles électroniques d'identité, de paiement et de monnaie numérique, dessine une nouvelle capacité d'intermédiation pour les transactions et les services de demain. Quelle est l'ampleur de cette évolution ? Quels seront les acteurs bénéficiaires de cette nouvelle intermédiation ? Que doivent faire les entreprises et services financiers pour y participer ? Les projets européens de portefeuille numériques pourront ils rivaliser avec les géants du numériques ? Comment les écosystèmes transactionnels construits pour que les réseaux bancaires/postaux ou télécoms/ sectoriels utilisant l'identification numérique comptent faire face ou s'y intégrer ? Quelles sont les conséquences sociétales de cette nouvelle forme d'intermédiation ?

« EUDI Wallet » : quelles fonctions pour la promotion d'une nouvelle vie sur mobile ?

Authentification, signature électronique, paiement : quels sont les fonctionnalités promises par le portefeuille mobile européen (EUDI) ? Comment vont-elles s'articuler entre elles ? Pour quels usages ? A mi-parcours des pilotes européens des quatre consortiums dotés ensemble de 90 millions d'Euros, quels sont les enseignements qui se dégagent ? Services numériques, voyages, ouverture de compte bancaire, identités professionnelles : où se situent les innovations les plus marquantes ? Quels sont les impacts vis-à-vis des architectures techniques ? Le niveau de Sécurité « élevé » du portefeuille européen : comment le comprendre ? comment l'implémenter ? comment sera-t-il utilisé ? Quelles sont les options ? Les citoyens et consommateurs européens vont-ils bénéficier avec ces parcours d'une nouvelle vie sur le mobile ?

Tables rondes

Comment optimiser les parcours numériques avec KYC et l'IA, pour améliorer l'engagement client ?

La gouvernance des données permet aux organisations de tester et mettre en place des stratégies digitales. Les outils de la Connaissance Clients (KYC) et les techniques d'Intelligence Artificielle (AI) permettent d'aller plus loin, en combinant des propositions mieux calibrées en termes de risque et d'opportunités, et en améliorant la personnalisation du service. Quels sont les bénéfices de l'automatisation de la KYC et de l'Intelligence Artificielle sur les expériences utilisateurs (UX) ? Comment combiner les deux approches ? Quels sont les impacts sur la vérification en temps réel des données, l'enrôlement des clients, la gestion des consentements et la surveillance des transactions ? Quels sont les retours d'expérience sur le marché ?

Quels sont les piliers pour construire l'identité numérique du futur (2030–2050) ?

Outre les portefeuilles sur mobile, quels sont les approches les plus structurantes pour l'identité numérique du futur ? Nous abordons ici plusieurs thématiques essentielles. L'infrastructure d'Identité Numérique est un concept qui considère qu'il faut insérer l'identité numérique dans une approche plus large « d'infrastructure publique numérique » (UIT/G20). L'écosystème résultant associe notamment l'échange de données et la gestion des transactions, permettant à la société numérique de fonctionner de manière plus optimale. Plusieurs approches ou modèles d'architectures pouvant ensuite être déclinés (eg : décentralisée, centralisée, fédérée) pour les différentes applications. Les Cadres de Confiance des Identités et Attributs sont des ensembles de règles et de normes auxquels les opérateurs de confiance peuvent adhérer et vis-à-vis desquels ils peuvent aussi être certifiés pour démonter leur capacité à délivrer des données dont l'intégrité et la conformité sont garanties. La monnaie numérique de banque centrale (CDBC) a progressé, à l'image de la monnaie numérique européenne ou du e-krona suédois. Cependant il se heurte encore au besoin de pouvoir identifier les personnes et/ou les comptes de manière efficace avant de pouvoir être mis en place pour le grand-public.

Tables rondes

Mieux lutter contre la fraude numérique dans la consommation, l'identité et le paiement

L'inflation et l'augmentation du cout de la vie ont conduit nombre d'autorités et d'organismes européens (EUROPOL, EBA, EPC, CIFAS UK) à alerter contre la prolifération des menaces d'arnaques et de cyber fraudes pénalisant les consommateurs dans leurs transactions d'achat, de paiement ou de services. Usurpations d'identité, manipulations en lignes ou par téléphone, escroqueries, fausses offres commerciales, logiciels espions, piratages et interceptions des données, les risques sont partout.
Quelles sont les transactions les plus ciblées ? Quels sont les objectifs des fraudeurs ? Comment mieux détecter les fraudes et prévenir les menaces ? Comment gérer la relation avec les clients dans un contexte de risques élevés ? Comment renforcer la culture de gestion des risques et des fraudes au sein des entreprises ? Quelles sont les retours d'expériences et les bonnes pratiques à mettre en place ? Quelles stratégies mettre en place : lien entre identité documentaire (et/ou biométrique) et numérique ; élévation du niveau de confiance ; monitoring transactionnel, ou se trouve les bonnes réponses ?

IAM–CIAM : augmenter la fluidité des données par l'orchestration des identités

Plus de fluidité et moins de frictions pour les utilisateurs : tel semble être la devise de la gestion des identités en entreprise aujourd'hui. Une pratique qui concerne toutes les clientèles internes et externes de l'entreprise : employés, partenaires, clients, entités non-humaines comme les applications ou les objets connectés. Grace aux plateformes d'orchestration, non seulement les différents publics de l'entreprise sont enregistrés, authentifiés et accompagnés dans la gestion de leurs autorisations, mais ils s'affranchissent aussi dans leurs parcours digitaux des complexités des différents environnements informatiques.
Sans programmation, sans efforts, sans mots de passe, comment l'orchestration des identités permet de générer une gestion fluide des données de l'entreprise ? Comment sont gérés les interfaces utilisateurs, connecteurs et APIs ? Quelles parties du cycle de vie peut-on automatiser et selon quels critères ? Comment les notifications d'évènements de gestion permettent automatiquement de reprovisionner les identités et les accès ? Quels sont les bénéfices selon la taille des entreprises ?

Tables rondes

Confiance des organisations et identités professionnelles : un vent de modernisation

Poussés par la facturation électronique, la signature numérique et par le développement des échanges transnationaux, les identités numériques des entreprises et celle des professionnels sont l'objet d'un intense travail de réflexion en vue d'une modernisation et d'une interopérabilité accrue. Tout en respectant les exigences très fortes de sécurité, de nouvelles possibilités émergent pour la gestion des attributs de confiance des entreprises et professionnels : registres d'entreprises, e-wallets professionnels, schémas de certification, informations de solvabilité, gestion des mandats.
Quels sont les initiatives structurantes ? Quelle confiance juridique accorder aux identités numériques ? Quelle sont les évolutions dans la gestion et l'utilisation des registres de sociétés en France et en Europe ? Qui sont les acteurs de ce changement ? Comment évoluent les pratiques de confiance et certification ? L'identité numérique des organisations va-t-elle passer du concept a la réalité ? Quelles sont les prochaines étapes ?

Vers un usage plus responsable de l'Internet, des réseaux sociaux et des plateformes ?

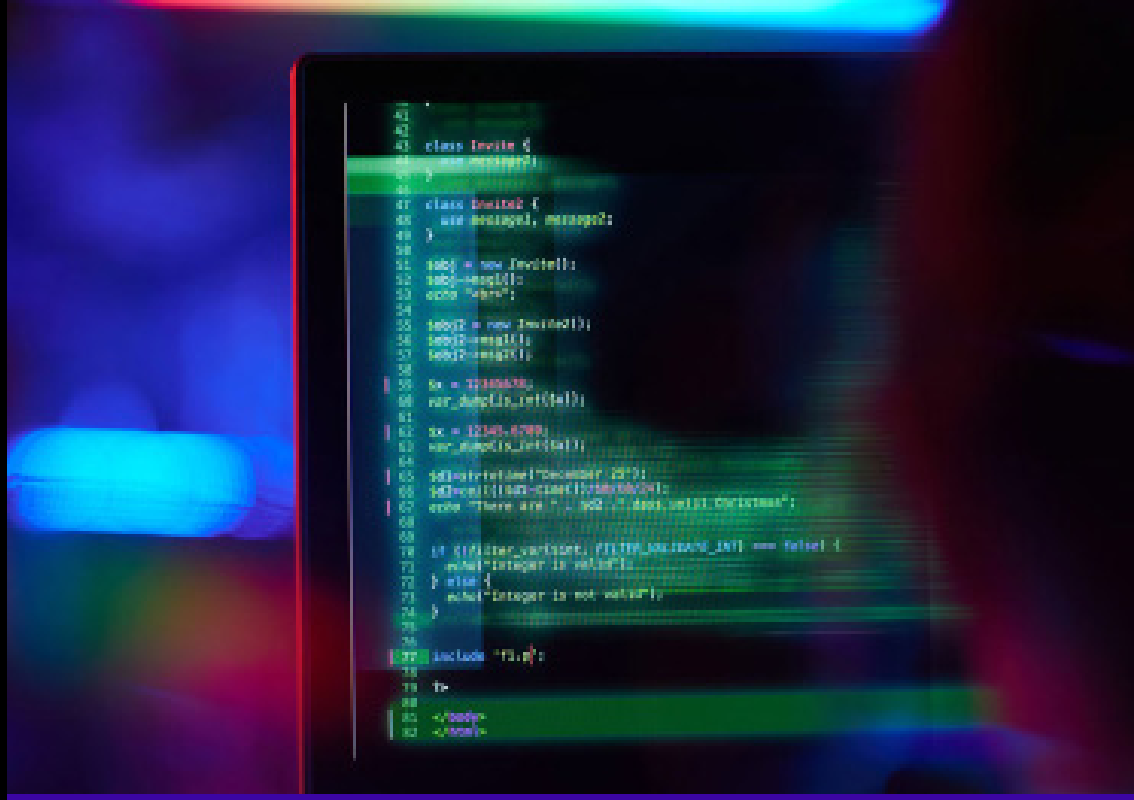
Alors que la vie sociétale en ligne a pris une dimension primordiale, les initiatives progressent pour mieux sécuriser les services numériques en ligne, clarifier le contenu des offres et mieux protéger les enfants et les adolescents des manifestations de haine, de la pornographie et des violences.
Au Royaume Uni, une nouvelle loi baptisée « Online Safety Bill » (OSB) a l'ambition de faire du Royaume Uni l'endroit le plus sur du monde pour l'Internet. En particulier de fortes mesures ont été prises visant à protéger les enfants et rendre responsable les plateformes des contenus hébergés. En France le projet de loi visant à sécuriser et réguler l'espace numérique (SREN), a des objectifs très similaires dans la lutte contre les arnaques en ligne et dans la protection de l'enfance.
DMA, OSB, SREN : le nouveau cadre législatif et réglementaire va-t-il enfin consacrer un usage plus responsable de l'Internet ? Comment serons-nous mieux protégés en ligne ? Quelles sont les obligations pour les plateformes et les services en ligne ? Quelles sont les pratiques de certification qui seront utilisées ? Quelles sont les mesures prises pour la vérification de l'âge ? Quel rôle est appelé à jouer l'identité numérique pour rendre l'Internet plus sûr ?

TRUST &SAFETY FORUM

FORUM IN CYBER EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS



Avec 100 000 professionnels dans le monde, 20 000 entreprises bientôt impactées par la future loi sur les services numériques, Trust & Safety s'efforce de devenir une discipline standard au sein de la grande famille de la sécurité.

Tables rondes

Comment l'IA protège-t-elle les données personnelles sur les plateformes ?

Tout le monde s'est construit une identité numérique au cours de la dernière décennie, mais comment la protéger contre le vol ou la falsification ? L'intelligence artificielle et d'autres technologies émergentes peuvent aider les individus et les entreprises à protéger leur identité numérique.

L'utilisation de l'IA dans le processus de recrutement T&S

Le paysage de l'emploi dans l'industrie de la confiance et de la sécurité a subi des transformations significatives ces dernières années, avec de nombreuses entreprises recherchant activement des candidats ayant des antécédents non conventionnels. Les départements des ressources humaines exploitent de plus en plus l'intelligence artificielle de manière éthique pour repérer les candidats adéquats tout en garantissant le traitement sécurisé de leurs données personnelles.

AviaTOR – Priorité aux rapports CSAM grâce à l'intelligence artificielle

32 millions de signalements d'abus sexuels sur mineurs ont été rapportés par les plateformes en 2022, et mis ensuite à la disposition des forces de l'ordre. Comment peuvent-ils hiérarchiser un tel volume de signalements ? AviaTOR est un outil qui utilise l'intelligence augmentée et la recherche ciblée pour aider les autorités à se concentrer sur l'identification des auteurs et le sauvetage des victimes.

Tables rondes

Quel sera l'impact des 79 élections de 2024 sur la communauté en ligne ?

In 2024, around 80 countries will be holding political elections, with social media platforms being the main communication channel to target voters. How can AI help in detecting and preventing misinformation so that voters get the information they need?

Le bien-être du personnel à l'ère de l'IA

Jusqu'à récemment, les équipes chargées de la confiance et de la sécurité ont dû faire face à des contenus nuisibles et illégaux avec un soutien limité de la technologie - telle que l'IA - pour analyser le contenu et minimiser l'exposition. La technologie est désormais disponible, mais quel a été l'impact sur les professionnels ? Les programmes de bien-être du personnel et les documents sur les meilleures pratiques ont-ils intégré ces évolutions ?

Créativité dans la protection des contenus contre l'exploitation criminelle

Nous aimons regarder des séries, des films ou des matchs sportifs en direct, et le crime organisé excelle à attirer notre attention et à nous faire entrer dans son économie souterraine, à nos risques et périls. Les professionnels de la protection collaborent et innovent avec la technologie pour garantir la sécurité du monde numérique, et leurs points de vue enrichissent la communauté Trust & Safety et garantissent.

Tables rondes

EXPOSÉ
Présentation de Checkstep sur l'IA et l'ASD

Découvrez comment le fournisseur de technologie Checkstep utilise l'intelligence artificielle pour s'assurer que ses clients sont en conformité avec la DSA et ses différentes règles.

CONFÉRENCE
Protéger les droits de propriété intellectuelle grâce à l'IA

L'IA est souvent considérée comme une technologie qui remet en question notre conception de la propriété intellectuelle. Dans cette présentation, nous explorerons l'utilisation des outils d'IA pour protéger les droits de propriété intellectuelle. Nous aborderons les différents types d'outils d'IA disponibles, la manière dont ces outils peuvent être utilisés pour identifier et suivre les infractions, prévenir la contrefaçon et faire respecter les droits de propriété intellectuelle. Nous aborderons également les considérations éthiques liées à l'utilisation de l'IA pour protéger les droits de propriété intellectuelle.

W3S

WEB3
SECURITY
SUMMIT

FORUM IN CYBER EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Les technologies web3 promettent d'accélérer la circulation des actifs et de créer un pont entre le réel et le virtuel. Mais l'absence de normes et d'autorité centralisée renforce le besoin d'établir un cadre adapté de management des risques.

Tables rondes

01 . Quels enjeux de sécurité en matière de tokenisation ?

02 . Blockchain et intégrité industrielle, une révolution inévitable

03 . Quel défi judiciaire en matière de Web3 ?

04 . Comment le Web3 redéfinit la protection de la propriété intellectuelle ?

INCYBER INVESTOR DAY

FORUM INCYBER EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Tables rondes

Le match des investissements en cybersécurité entre l'Europe et les USA, comment combler le retard du vieux continent ?

Dans la course des investissements en cybersécurité entre l'Europe et les États-Unis, l'Europe montre des signes encourageants malgré un certain retard. En 2022, les sociétés européennes du secteur ont levé un record de 2,4 milliards d'euros, reflétant une maturité croissante. Cette performance, bien que notable, souligne toutefois l'écart subsistant avec les investissements américains et israéliens. Comment combler ce retard ? En quoi les différences culturelles, réglementaires et d'investissement entre l'Europe et les États-Unis impactent-elles la croissance de l'écosystème européen de la cybersécurité ? Comment les politiques d'innovation, les incubateurs et les accélérateurs peuvent-ils être optimisés pour favoriser l'émergence de technologies de cybersécurité de pointe en Europe ?

Quelles perspectives pour le marché de l'IA pour la cybersécurité à l'horizon 2030 ?

Le marché de l'intelligence artificielle (IA) dans le domaine de la cybersécurité offre des perspectives quantitatives prometteuses, illustrées par une croissance significative des investissements. Selon les prévisions, le marché mondial de la cybersécurité alimenté par l'IA devrait atteindre plusieurs dizaines de milliards de dollars d'ici les prochaines années. En 2022, les dépenses mondiales en cybersécurité alimentée par l'IA ont déjà dépassé les 15 milliards de dollars, marquant une augmentation substantielle par rapport aux années précédentes. Alors que ce marché pourrait dépasser les 30 milliards en 2025, quels sont les segments émergents et les opportunités associées ? Comment le marché de l'IA pour la cybersécurité sera t'il réparti à l'horizon 2030 en termes de produits, de services, de clients et de géographies ?

Tables rondes

De la startup à la scale-up : stratégie pour franchir les étapes critiques ?

Les pépites technologiques sont bien là, mais nombre d'entre elles peinent à franchir le cap. Ayant trouvé leur marché avec un plan de financement innovant, toutes n'arrivent pas à répondre aux enjeux d'après, à savoir l'internationalisation, la mise en place d'une stratégie marketing long-terme, voire la structuration de leur leadership en interne. Les dispositifs de soutien à l'innovation ne manquent pas : mécanismes publics (portés par exemple par le ministère des Armées, soutien de Bpifrance, stratégie cyber portée par l'ANSSI et le Campus Cyber, European Innovation Council) financements et soutiens privés (VC, incubateurs, accélérateurs)... Mais qu'en est-il du soutien à la croissance (notamment par le biais de la commande publique), souvent considéré comme insuffisant ? Que manque-t-il pour consolider la dynamique ? L'Europe est-elle en mesure de rivaliser avec les États-Unis et Israël en la matière ?

JOURNÉE OSINT

FORUM IN CYBER EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

L'OSINT est devenue une pratique à part entière.
De la lutte anti-criminalité (cyber, physique, financière..)
aux crypto-monnaies, en passant par la sécurité
des biens et des personnes en période de conflits
armés, l'OSINT est aujourd'hui utilisée
dans de nombreux domaines.

JOURNÉE
OSINT

Tables rondes

FORUM INCYBER EUROPE

SESSION 1: 26 MARS : 10H – 11H30

L'OSINT et ses communautés françaises

Du projet FOX à OSINT FR en passant par le Club AEGE OSINT & Veille, l'OSINT à la française compte des communautés particulièrement talentueuses, chacune ayant ses propres spécificités. Retrouver un suspect en fuite à l'autre bout du monde, démasquer des fraudeurs, suivre les mouvements de troupes armées... Ces experts français de l'OSINT vous expliqueront tout, dans les moindres détails.

SESSION 2: 26 MARS : 14H – 15H30

Parole de professionnel

Baptiste ROBERT, Camille DOLE, Oriana LABRUYERE, Dmytro BILASH, Daniel-Florin PITIȘ ou encore Matthieu AMIOT et Frédéric LENFANT viendront partager leur expérience en présentant l'utilisation qu'ils font de l'OSINT dans leur travail : lutte contre la contrefaçon d'œuvre d'art, lutte anti-fraude, cybersécurité, pentest...

SESSION 3: 26 MARS : 16H30 – 18H

Last but not least...

L'OSINT Day du Forum Incyber fait fi des frontières et réalise l'exploit de réunir, lors d'une même session, Micah HOFFMAN (Webreacher), Steven HARRIS (Nixintel), Leone HADAVI (BBC/Bellingcat), Neil SMITH (UK OSINT), Craig SILVERMAN (ProPublica) et Ritu GILL (OSINT Techniques).

FORUM IN CYBER EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Contact

partenariats

partenariat@forum-incyber.com

programme

programme@forum-incyber.com