IN CYBER FORUM EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Programme


IN CYBER
FORUM
EUROPE
Ready for AI ?
THEME 2024

Ready for AI ?

Réinventer la cybersécurité à l'ère de l'IA

IN CYBER FORUM 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

→ SOMMET D'OUVERTURE

L'Europe est-elle prête pour l'IA ?

→ SÉANCES

Réinventer la cybersécurité à l'ère de l'IA

Révolution numérique et bousculements géopolitiques : l'Europe est-elle toujours dans la course ?

IA en quête de confiance

Bouclier cyber : le défi de la solidarité européenne

→ TABLES RONDES

Lutte anti-cybercriminalité

Management des risques cyber

Sécurité des données et transformation numérique

Sécurité et stabilité du cyberespace

Souveraineté numérique

Sécurité opérationnelle

IN CYBER FORUM EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Sommet d'ouverture

L'Europe est-elle prête pour l'IA ?

16H00 à 19H00 le 26 mars

IN CYBER FORUM EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

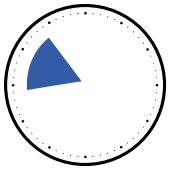
Séances plénières

IN CYBER FORUM EUROPE

J2

27 mars

8H45 à 11H15



Réinventer la cybersécurité à l'ère de l'IA

50% des organisations affirment déjà utiliser l'IA. Nous n'en sommes pourtant qu'aux prémices de cette révolution qui va bouleverser durablement l'Humanité. Parce qu'elle permet de sécuriser les usages du numérique et de créer la confiance dans un monde de plus dématérialisé, distant et complexe pour les utilisateurs, la cybersécurité doit être au cœur de cette révolution. Comment doit-elle se réinventer pour répondre à ces nouveaux défis ? Comment assurer la cybersécurité des IA qui seront de plus en plus la cible des attaquants ? Comment faire "face" aux attaques, de plus en plus sophistiquées et rapides grâce à l'utilisation de ces mêmes technologies par les attaquants ? Quels sont les impacts prévisibles et les nouvelles menaces générées par la montée en puissance des IA génératives spécialisées dans la production de code ? Comment, enfin, tirer parti de l'intelligence artificielle pour renforcer la cybersécurité collective, notamment pour renforcer et automatiser notre défense et faire de l'IA un véritable bouclier ? Dans un contexte de pénurie durable de compétences, ces technologies vont-elles permettre de « démocratiser » la cybersécurité grâce à l'automatisation ?

J2

27 mars

16H45 à 19H00

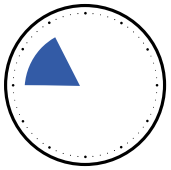
Révolution numérique et bousculements géopolitiques : l'Europe est-elle toujours dans la course ?

L'émergence de l'intelligence artificielle va bouleverser en profondeur la géopolitique mondiale. Les Etats se livrent en effet une course effrénée pour développer ces technologies compte tenu de l'avantage économique et industriel mais aussi politique et militaire qu'elles procurent. Au point qu'Elon Musk disait en 2018 : « la lutte entre nations pour la supériorité de l'IA causera probablement la 3ème guerre mondiale » . Dans cette course, quelle place pour l'Europe qui est aujourd'hui distancée par les Etats-Unis et la Chine ? Ces technologies vont-elle au contraire rebattre les cartes en bouleversant les modèles d'affaires qui en font la fortune des GAFAM et BATX ? Au plan technologique, le développement de « l'Edge AI », c'est-à-dire de capacités locales, au plus proche des données est-elle une opportunité ? A l'ère de l'IA, quels sont les nouveaux leviers de puissance sur lesquels appuyer une stratégie ? Comment exploiter le formidable vivier de compétences dont nous disposons ? Quelle politique industrielle développer pour soutenir les ambitions européennes ? Puissance d'équilibre par nature, l'Union européenne peut-elle faire de la notion d'IA de confiance une opportunité au niveau mondial ?

J3

28 mars

9H00 à 11H00



IA en quête de confiance

La confiance est la clé d'adoption et d'appropriation des technologies, a fortiori en matière d'intelligence artificielle. En effet, Deep learning et réseaux de neurones rendent impossible par le commun des mortels la compréhension des mécanismes utilisés et des résultats proposés par la machine. Ainsi, il faut « objectiver » avec des critères clairs et précis une « IA de confiance ». L'AI Act proposé par la Commission Européenne et adoptée en juin 2023, la définit comme étant légale, éthique, robuste et sécurisée.

Mais ces critères sont-ils suffisants ? A l'inverse, risquent-ils d'entraver l'innovation ? La confiance dans ces technologies peut-elle aller jusqu'à accepter que des systèmes prennent des décisions en toute autonomie ? Quelles limites à cette confiance, notamment en termes de biais idéologiques, de respect de nos vies privées et de protection de nos données personnelles et privées ? L'avènement de l'IA, par elle-même, ne va-t-elle pas finir par éroder la confiance ? Au contraire, l'IA peut-elle contribuer à renforcer la confiance dans le numérique au travers de ses nombreuses applications en matière de cybersécurité ? Enfin, sur le plan pratique, comment mesurer la confiance de manière audible et vulgarisable ? Serons-nous capables de la certifier?

27 mars

Pour une IA responsable, condition de la cybersécurité

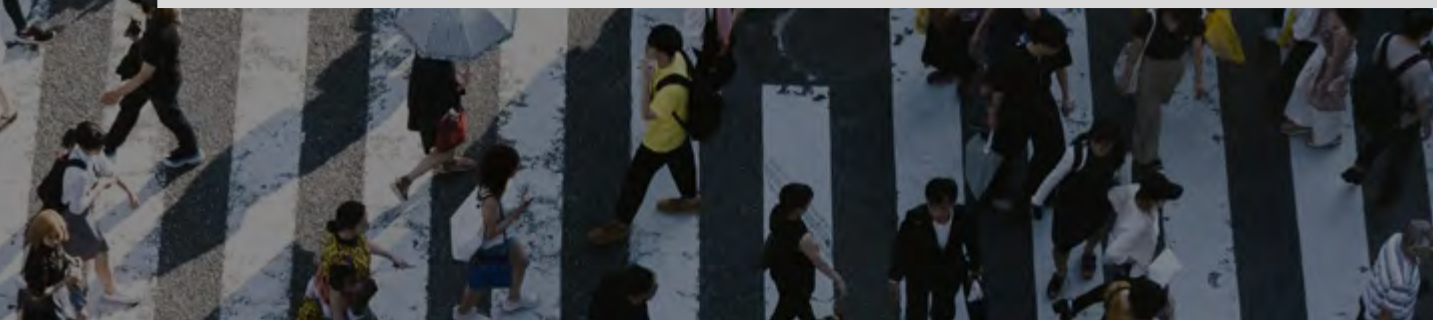
L'intelligence artificielle subjugue en même temps qu'elle inquiète. Son immense potentiel, non encore exploré dans sa dimension, sa puissance, son impact, nous transporte dans l'inconnu, dans un futur imprévisible laissant la voie ouverte à toutes les hypothèses.

L'intelligence est sans aucun doute ce qui distingue l'humain de toute autre espèce. Toutes les technologies, dans leur phase d'émergence ont suscité des interrogations, des peurs, fragilisant parfois leur développement initial. L'intelligence artificielle connaît cette phase de doute qui se mêle à celle d'exaltation.

Une chose est certaine, plus que toute autre technologie, l'intelligence artificielle impose que l'on porte sur elle toute notre intelligence humaine, en perçant le nuage de l'invisible et du mystérieux. Plus que toute autre technologie, elle appelle une réponse à la question « pourquoi ? », c'est-à-dire une recherche de sa finalité, un encadrement qui lui préserve sa liberté, sans jamais porter atteinte à ce qui fait l'essence même de l'humain : son identité - c'est-à-dire son unicité - son intimité, sa liberté de penser, de s'exprimer, de décider.

La confiance est sans doute le maître-mot des années à venir. Elle ne peut s'établir sans une IA responsable. Pour atteindre cet idéal,il est nécessaire de s'appuyer sur des principes clés, mais aussi sur une approche collaborative à laquelle chaque partie impliquée dans l'intelligence artificielle (chercheurs, développeurs, responsables du déploiement, universitaires, société civile, gouvernements et utilisateurs, y compris les individus, les entreprises et les autres organisations) devrait collaborer.

Comment parvenir ensemble à maîtriser notre futur ? Donnons la parole aux experts, mais prenons-là aussi ! Telle est l'ambition de cette Agora !



agora
INCYBER FORUM

IN CYBER FORUM EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Lutte anti-cybercriminalité

TABLES RONDES

Coopération internationale : clé d'un avenir numérique sécurisé face à la cybercriminalité ?

Face au cybercrime, la coopération internationale entre les services de police et autorités judiciaires s'organise. En témoignent les nombreuses opérations internationales menées. Pourtant les discussions à l'ONU sur la Convention sur la cybercriminalité s'enlisent et montrent la fracture sur la vision de ce qui représente une menace cyber. Ainsi, la diplomatie cybernétique est confrontée à des échecs, notamment en raison de désaccords fondamentaux sur la définition des comportements responsables des Etats dans le cyberespace et lsur ce qu'est la responsabilité des États. Quelles sont les avancées récentes dans le cadre de la Convention de Budapest ? Quels résultats pour la conférence contre les rançongiciels organisée par les Etats-Unis en octobre 2022 ? Quel est le bilan des opérations menées par Europol ? Quel bilan et limites pour la stratégie mondiale initiée par Interpol ?

Comment exploiter l'IA dans les investigations numériques ?

La révolution numérique a profondément transformé le paysage des enquêtes, en insufflant une dimension numérique sans précédent et un volume de données inégalé. Dans ce contexte, l'IA peut devenir un allié de l'enquêteur dans la collecte, l'indexation et l'analyse de ces données. Quels sont les changements à anticiper pour les enquêteurs dans ce nouveau paysage numérique ? Comment les enquêteurs peuvent-ils se préparer pour être « AI ready » ? Comment concilier les décisions prises par les systèmes d'IA avec les normes éthiques et juridiques ? Comment garantir que les enquêtes menées avec l'aide de l'IA demeurent transparentes et opposables ?

Les arnaques dopées à l'IA

Deepfake, deep voice et vishing… : les nouvelles techniques de phishing utilisant l'IA pour créer des textes, des voix, des images et des personnages numériques plus vrais que nature se multiplient. Avec pour conséquence des arnaques au président quasiment indétectables. À horizon 2023, Gartner estime que 20 % de toutes les attaques de phishing utiliseront des outils d'IA. Comment s'en prémunir ? Quels processus mettre en œuvre au plan organisationnel ? Quelles solutions pour lutter contre ces attaques ?

Dispositifs de captation : quelle régulation pour une technologie d'enquête des plus intrusives ?

Les «logiciels-espions», objets de fantasmes parmi le grand public, sont devenus en réalité le seul recours possible des services de l'Etat lorsque le chiffrement des communications masque des éléments-clés de leurs enquêtes. Cependant, le scandale Pegasus a mis en lumière l'impact extrêmement négatif de ces logiciels dans les cas où ils sont utilisés sans garde-fous. Une commission spécialement constituée du Parlement Européen s'est récemment attachée à évaluer les risques de tels usages, pour ensuite émettre un ensemble de recommandations en direction de la Commission Européenne. Mais quel doit être le rôle des Etats-membres au sein de ce mouvement ? Se saisir du sujet et contribuer à l'initiative communautaire - au risque de voir un durcissement des conditions d'emploi de la captation - ou bien adopter une prudente attitude de mise en avant du principe de « sécurité nationale », synonyme de statu quo ? Un travail transdisciplinaire (chercheurs de vulnérabilités, spécialistes de sécurité des télécoms, systèmiers, ...) pourrait-il définir un dispositif efficace et, dans le même temps, garant du respect de la vie privée ?

IN CYBER FORUM EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Management des risques cyber

TABLES RONDES

Comment évaluer et valider en continu son niveau de sécurité ?

Pour faire face à l'évolution constante des menaces et garantir un niveau de sécurité optimal, il est essentiel d'évaluer en continu son exposition aux menaces. La validation de la sécurité comprend un ensemble de techniques, de processus et d'outils qui permettent d'identifier comment les attaquants pourraient exploiter les vulnérabilités détectées. Face aux défis du multicloud, de l'edge computing ou encore de la *supply chain* logicielle, la surface d'attaque ne cesse de se complexifier et de s'élargir. Les programmes de CTEM *(Continuous Threat Exposure Management)* prennent alors toute leur importance. Comment mettre en place une plateforme unifiée de validation de la sécurité qui combine des éléments tels que la gestion de la surface d'attaque externe, la simulation de chemins d'attaque (Breach & attack simulation ou BAS) et les tests de pénétration automatisés ? En quoi cette intégration pourrait-elle améliorer la capacité à anticiper et contrer les menaces ? Quel apport de l'IA pour une évaluation en continu ?

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 lorsqu'elle équipe des systèmes critiques, elles peuvent devenir des points de fragilité. Comment pouvons-nous garantir que les systèmes critiques ne seront pas compromis par des défaillances d'IA ? Quelles sont les recettes et les meilleures pratiques pour créer des IA résilientes, capables de s'adapter aux situations imprévues et d'assurer leur bon fonctionnement même en cas d'incidents critiques ? Comment pouvons-nous renforcer la robustesse, la fiabilité et la transparence des algorithmes d'IA pour répondre aux exigences de résilience dans des domaines stratégiques tels que la santé, la sécurité et les infrastructures essentielles ?

De la haute couture au prêt-à-porter : quelle cybersécurité pour les PME ?

« Il faut passer de la haute couture au prêt-à-porter » , déclarait Vincent Strubel, le directeur général de l'ANSSI en ouverture du Forum InCyber 2023. La démocratisation de la cybersécurité, en particulier auprès des PME, est un enjeu crucial, car elles sont souvent vulnérables aux attaques malveillantes en raison de ressources limitées et d'un manque de compétences spécialisées. L'intelligence artificielle peut jouer un rôle essentiel pour répondre à ce besoin en offrant une solution abordable pour renforcer la sécurité des PME en automatisant certaines tâches et en comblant le manque de compétences en cybersécurité. Quelles fonctionnalités spécifiques peut-elle apporter pour protéger efficacement les PME contre les menaces en ligne ? Quelles solutions concrètes peuvent être mises en place, par exemple, pour lutter contre le phishing en sécurisant les messageries ? Peut-on envisager de créer un « RSSI virtuel » à base d'IA pour les PME, permettant une gestion automatisée de leur sécurité informatique ?

Vers une IA « super oracle en cybersécurité » : quel rôle pour le RSSI demain ?

L'avènement de l'intelligence artificielle (IA) bouleverse le rôle traditionnel du RSSI. Cette révolution technologique offre un potentiel sans précédent, mais également des défis de taille pour les professionnels de la sécurité. En exploitant le potentiel de l'analyse en temps réel de volumes massifs de données, l'IA offre aux RSSI une meilleure prévision des comportements malveillants et des vulnérabilités, renforçant ainsi leur capacité de réponse face aux incidents de sécurité. Comment l'IA transforme-t-elle le rôle du RSSI au sein de l'entreprise ? Va-t-elle l'épauler ou le remplacer ? Peut-on imaginer, dans un avenir proche, le développement d'un futur LLM multimodal "super oracle en cybersécurité" ?

Comment piloter la mise en conformité NIS2 et la maintenir dans le temps ?

L'extension du champ d'application de NIS 2, qui comprend davantage de secteurs d'activités économiques, contribuera à accroître le niveau de cybersécurité en Europe avec un changement de paradigme notable. Alors que les menaces se concentrent sur les vulnérabilités très en aval des chaînes, la numérisation des chaînes d'approvisionnement génère des failles. L'un des objectifs de la directive NIS 2 est dès lors d'augmenter le niveau de cybersécurité des acteurs de la chaîne d'approvisionnement afin de limiter les risques d'attaques par rebond.

Quelles mesures les organisations concernées doivent-elles prendre ? Quelles sont les conséquences en cas de non-respect des règles NIS 2 ? Comment gérer les incidents en lien avec la chaîne d'approvisionnement et la chaîne de valeur ? Comment assurer une mise en conformité pérenne ?

Préserver l'intégrité de vos chaînes d'approvisionnement à l'ère de NIS 2

La directive NIS 2 met l'accent sur l'amélioration de la sécurité des acteurs de la chaîne d'approvisionnement, tels que les fournisseurs de services numériques, pour limiter les risques de compromissions. NIS 2 impose souvent aux tierces parties une supervision continue ainsi qu'une notification obligatoire d'incidents significatifs. Comment détecter et atténuer les risques liés à la chaîne d'approvisionnement ? Quelle est la manière adéquate pour gérer la sécurité de ses « tiers » en utilisant par exemple des solutions de scoring ou d'audit ? Quel sera l'impact de NIS 2 en la matière ?

Comment garantir la conformité réglementaire et la protection des données lorsqu'elles sont gérées par des tierces parties, qu'il s'agisse de fournisseurs de services cloud ou encore de sous-traitants ?

IN CYBER FORUM EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Sécurité des données et transformation numérique

TABLES RONDES

Les sauvegardes immuables, une parade absolue ?

Face aux rançongiciels qui s'attaquent aux sauvegardes, le stockage sécurisé a de plus en plus d'importance. Les sauvegardes sont plus qu'une simple seconde copie des données. Il faut en effet assurer à la fois la restauration rapide en cas de besoin, l'efficience des données, la durabilité… 75 % des organisations perdent au moins quelques-unes de leurs sauvegardes lors des attaques. Comment rendre ces sauvegardes immuables ? Quelles protections face aux attaques ? Comment s'adapter dans un avenir proche à une situation avec plus de données que de capacités de stockage ? Le stockage immuable risque de ne plus l'être vraiment.

EDR, XDR, MDR... solutions miracles pour les hôpitaux ?

Les équipements médicaux sont souvent vulnérables et leur mise à jour impossible. Pour continuer à les faire fonctionner malgré tout, il est essentiel d'analyser en permanence ce qui se passe sur les réseaux et *endpoints* pour détecter et réagir instantanément. Dans cette optique, les hôpitaux se sont fortement équipés en logiciels EDR, XDR ainsi qu'en solutions et services de MDR. Mais des questions persistent encore comme sur la complémentarité des technologies de type XDR avec les services fournis par le SOC et les technologies SIEM.

Alors que la sécurité ne peut pas être native dans les équipements, comment l'IA peut être utilisée pour surveiller les réseaux informatiques, détecter les comportements malveillants, prévenir les intrusions potentielles ? Est-ce une garantie pour la continuité des activités ? Comment la collaboration entre les établissements de santé, les fabricants d'équipements médicaux et les fournisseurs de solutions de cybersécurité peut-elle améliorer la protection des équipements vulnérables ?

Responsabilité et légalité : comment composer avec les fuites de données ?

La Recherche sur Internet de Fuites d'Informations (RIFI) désigne le processus de surveillance et d'analyse en ligne visant à identifier la divulgation non autorisée d'informations confidentielles, telles que des données personnelles ou des secrets d'entreprise, afin de prendre des mesures préventives ou correctives. Dans ces deux cas, ces collectes peuvent servir *in fine* à prévenir des clients ou influencer des décisions stratégiques. Or, ne s'agit-il pas ici de délit de recel ? En effet, il est officiellement illégal de récupérer des données issues de « *leak* »...sauf exception ! Les entreprises font face à des situations nouvelles où la connaissance du droit numérique français et européen devient une nécessité. Comment les entreprises peuvent-elles déterminer si elles sont dans un cadre légal lorsqu'elles traitent de telles données et poursuivent leurs activités ? La copie et l'anonymisation peuvent-elles être une piste de solution ? Faut-il revoir la loi et modifier nos pratiques ?

IN CYBER FORUM EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Sécurité et stabilité du cyberespace

TABLES RONDES

Intelligence artificielle : la course à la régulation

L'intelligence artificielle (IA) est au cœur d'une compétition mondiale pour la régulation. Les acteurs étatiques et internationaux cherchent à trouver un équilibre délicat entre l'innovation technologique et la nécessité de réglementer cette avancée disruptive. Tandis que l'UE se positionne en pionnière avec une législation stricte, les États-Unis privilégient la responsabilisation des acteurs privés par le biais de directives non contraignantes et d'investissements dans l'innovation. Le Royaume-Uni, bien qu'ambitieux pour devenir un régulateur mondial de l'IA, adopte une approche plus légère, en mettant l'accent sur les grands principes plutôt que sur des contrôles stricts. La Chine, quant à elle, entend réguler les produits de l'IA avec des évaluations obligatoires avant leur mise sur le marché. Comment la régulation de l'IA affectera-t-elle l'innovation et la compétitivité des entreprises selon leur géographie ? Quel équilibre entre innovation et contrainte législative dans la compétition mondiale ?

Armes autonomes : quelles perspectives en matière de régulation ?

Les armées de plusieurs pays utilisent déjà des algorithmes pour prendre des décisions et planifier des stratégies militaires, y compris l'utilisation de drones autonomes dans des opérations de lutte contre le terrorisme. Cependant, ces développements soulèvent des préoccupations juridiques, éthiques et sécuritaires. Pour progresser dans le débat sur l'utilisation de l'IA dans les opérations militaires, il est nécessaire de poursuivre des discussions indépendantes et de parvenir à un accord. Bien qu'il n'y ait pas de consensus sur une interdiction universelle des systèmes d'armes létaux autonomes (SALA), cet accord pourrait contribuer à établir de nouvelles normes sur les actions appropriées. Cela permettrait de contrôler la prolifération de ces technologies et de progressivement mettre en place de nouvelles pratiques dans le domaine militaire. Actuellement, de nombreuses questions et enjeux liés à l'autonomie militaire demeurent sans réponse. L'absence de réglementation offre aux États développant ces technologies la possibilité d'influencer les pratiques de combat. Quelles sont les initiatives mises en place par l'ONU sur la régulation des systèmes autonomes ? Quelles sont les perspectives pour poursuivre le débat et aboutir à une régulation potentielle ? Trop de régulation ne risque-t-il pas de nuire aux progrès technologiques ?

Après la guerre, quelles conditions pour la paix dans le numérique ?

Dans un contexte géopolitique complexe, les infrastructures numériques sont de plus en plus prises pour cible, comme en témoigne la menace de destruction des câbles sous-marins ennemis évoquée par Dimitri Medvedev après la destruction du pipeline Nord Stream. Face à de telles menaces, il est essentiel de s'interroger sur les mesures à prendre pour protéger ce que certains appellent le « cœur public » d'Internet, bien que ce dernier ne soit pas réellement public. Comment l'Appel de Paris peut-il influencer la protection des infrastructures numériques et la promotion de la collaboration entre les États? Les infrastructures numériques seront-elles de plus en plus prises pour cible demain ? Quelles solutions pour protéger ce « coeur public » ?

IN CYBER FORUM EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Souveraineté numérique

TABLES RONDES

Comment évaluer et « normaliser » la sécurité des IA ?

L'évaluation et la normalisation de la sécurité des IA sont des enjeux cruciaux dans un monde de plus en plus dépendant à ces technologies. Comment pouvons-nous évaluer efficacement les risques liés à l'utilisation de l'IA, tels que les biais ou les vulnérabilités techniques ? Quels critères et processus standardisés mettre en place pour garantir un développement et un déploiement sécurisés des IA ? Comment faire pour que la normalisation n'entrave pas l'innovation ? En quoi les normes existantes (27001, 9001) doivent-elles être adaptées au développement croissant des IA ? La normalisation n'est-elle pas aussi un enjeu de souveraineté ?

Espaces de données : la revanche européenne ?

L'Europe peine à rivaliser avec les États-Unis dans le domaine du cloud, mais elle pourrait regagner une forme de souveraineté numérique en développant des espaces de données mutualisés entre ses principaux secteurs économiques (banque, finance..). Comment un cadre légal, tel que le Data Act, peut-il faciliter et sécuriser cette mutualisation? Ces espaces de données partagées pourraient-ils être la clé pour renforcer la position de l'Europe sur la scène numérique mondiale ? Comment les entreprises et les gouvernements européens pourraient-ils collaborer pour créer et gérer efficacement ces infrastructures de données mutualisées ? Quels défis, avantages mais aussi limites cela impliquerait-il pour la sécurité, la confidentialité et l'innovation numérique en Europe ?

IA et cybersécurité : comment développer et « hybrider » les compétences ?

L'IA a fait son entrée dans le secteur de la cybersécurité depuis de nombreuses années et la recherche dans ces deux disciplines a permis de belles convergences sur les produits. La combinaison de ces deux domaines de compétences, déjà rares et précieux séparément, est en effet essentielle pour développer des modèles d'apprentissage automatique efficaces dans le domaine de la cybersécurité. Pourtant les experts, ingénieurs, développeurs et architectes possédant cette double compétence sont rares. Une pénurie directement liée au manque important de formations associant les deux disciplines et aux moyens que nous y affectons. Comment combler rapidement ce trou dans la raquette ? Comment faire évoluer les compétences des professionnels de la cybersécurité à l'ère de l'IA ? Comment faciliter la collaboration interdisciplinaire entre experts en IA et en cybersécurité pour créer des solutions robustes face aux cybermenaces actuelles ?

IN CYBER FORUM EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Sécurité opérationnelle

TABLES RONDES

Des tests d'intrusion à la vitesse de l'IA ?

Les tests d'intrusion exploitant la puissance de l'intelligence artificielle représentent une avancée majeure dans le secteur de la cybersécurité. Grâce à l'utilisation des capacités avancées de l'IA, ces évaluations automatisent et accélèrent l'identification des vulnérabilités et des tentatives d'intrusion au sein des systèmes informatiques. En tirant parti de techniques telles que l'analyse du code source, la détection des erreurs de configuration et la création d'attaques ciblées, l'IA peut rapidement mettre en évidence les points faibles et simuler des scénarios d'attaques réalistes. Cependant, il est primordial de noter que les tests d'intrusion à l'IA ne sauraient constituer une solution en soi. Ils doivent être intégrés dans une stratégie de cybersécurité globale, associés à d'autres mesures de protection, une surveillance continue et une gestion proactive des risques. De plus, les considérations relatives à la confidentialité des données et à l'éthique doivent servir de boussole pour une utilisation responsable de l'IA dans ce domaine, afin d'éviter toute mise en péril de la sécurité et de la vie privée.
Comment l'utilisation de l'intelligence artificielle dans les tests d'intrusion contribue-t-elle à une évolution de contre-mesures de défense et des tactiques d'attaque? Comment les attaquants pourraient-ils exploiter eux-mêmes l'IA pour contourner les défenses basées sur l'IA ?

Automatisation du SOC : jusqu'où aller ?

L'automatisation croissante des Centres Opérationnels de Sécurité (SOC) suscite des questionnements essentiels quant à son ampleur et à la place de l'intelligence artificielle au sein des solutions SOC, notamment les Systèmes d'Information et de Gestion de la Sécurité (SIEM), les technologies UEBA et les Orchestrateurs de Réponse et d'Automatisation de la Sécurité (SOAR). Cette révolution technologique invite à repenser en profondeur les structures organisationnelles et les compétences requises pour maintenir une cybersécurité robuste. Toutefois, une question centrale demeure : quelle est la juste place de l'humain dans cet écosystème automatisé ? Alors que l'IA peut accélérer la détection des menaces et les réponses aux incidents, l'expertise humaine reste-t-elle irremplaçable pour interpréter, anticiper et prendre des décisions en toute résponsabilité ?

IA, production et analyse du code : une révolution ?

L'arrivée déjà ancienne de l'intelligence artificielle (IA) dans l'analyse de code (tests d'API, tests unitaires, tests d'interface utilisateur...) mais aussi, grâce à ses variantes dites « génératives » , dans sa production marquent une révolution dans la programmation et le développement logiciel. Cette convergence ouvre des horizons innovants pour automatiser et perfectionner les processus liés à la création, à l'inspection et à l'optimisation du code source, ainsi qu'à l'interaction avec les interfaces utilisateur. L'IA, en s'appuyant sur des techniques comme l'apprentissage automatique et le traitement du langage naturel, non seulement identifie les problèmes potentiels dans le code, mais peut également suggérer des solutions, accroissant ainsi l'efficacité et la qualité du développement. Cependant, cette évolution suscite des interrogations concernant la fiabilité des choix opérés par l'IA, l'équilibre entre compétences humaines et capacités de l'IA, et les dilemmes éthiques entourant l'automatisation dans un domaine aussi crucial que la programmation. En fin de compte, l'adoption grandissante de l'IA entraîne indéniablement une transformation majeure dans la manière d'appréhender le développement logiciel, offrant la possibilité de redéfinir les normes et les pratiques de l'industrie.

Le défi de la complémentarité public-privé au niveau local

Alors que les attaques contre les collectivités territoriales peuvent affecter la gestion de l'état-civil ou encore le versement des prestations sociales et que leur fréquence ne cesse d'augmenter, seules 29 % des communes de 3 500 à 10 000 habitants avaient en 2022 un responsable de la sécurité des systèmes d'information (RSSI). Pour faire face à la territorialisation accrue de la menace, des CSIRTs régionaux ont été déployés. Ce dispositif n'est cependant pas uniforme sur leur territoire, certaines régions l'utilisant comme un outil d'animation du territoire alors que d'autres l'utilisant comme un outil de triage d'incident. Cette différence de modèle et de positionnement soulève des interrogations sur la pérennité de ces CSIRTs régionaux.

Les CSIRTs et autres Campus Cyber territoriaux vont-ils produire des effets adaptés aux enjeux locaux ? Quelle est l'articulation adéquate entre Cybermalveillance, les Campus Cyber régionaux et les différents CSIRTs ?

Est-il possible de renforcer la mutualisation pour que les plus petites communes puissent bénéficier de l'expertise et des moyens financiers des structures plus importantes ? Comment les collectivités territoriales doivent-elles s'adapter à NIS 2 ? Comment aider les collectivités à choisir des solutions technologiques et des prestataires de services à la fois performants et de confiance ?

Quelles solutions techniques pour sécuriser les IA ?

Attaques adverses, spoofing, empoisonnement de données, injection de code malveillant, exfiltration et rétro-ingénierie de modèles..., l'IA est fragile ! Pour la protéger, il est impératif d'effectuer une sélection et une gestion rigoureuse des données d'entraînement afin de prévenir les biais et d'assurer la qualité des modèles obtenus. Parallèlement, accorder une attention prioritaire à la prévention des biais implique une surveillance régulière et la mise en place de stratégies d'atténuation. La sécurité des données de l'IA, que ce soit via chiffrement ou gestion d'accès restreinte, se révèle cruciale pour éviter toute divulgation d'informations sensibles. En outre, garantir la protection des modèles contre les attaques adverses et assurer leur actualisation à travers des correctifs de sécurité sont des démarches essentielles. Pour véritablement ancrer la sécurité dans chaque aspect de l'IA, l'approche « secure by design » doit être une priorité dès la phase de conception. Comment se défendre contre ces attaques ? Comment corriger les vulnérabilités et sécuriser ces modèles ? Quel rôle pour "l'apprentissage fédéré" sans remettre en cause la confidentialité et la protection des données collectées ? Quels sont les défis et les avantages liés à la mise à jour régulière des modèles d'IA avec des correctifs de sécurité ?

L'IA réinvente les fondements de la CTI

Le renseignement d'intérêt cyber offre aux organisations une compréhension approfondie des menaces potentielles en collectant, analysant et interprétant des informations sur les acteurs malveillants. En anticipant les menaces avec le renseignement d'intérêt cyber, les organisations peuvent prendre des mesures préventives et améliorer leur capacité de réponse face aux incidents. L'IA peut automatiser une grande partie du processus d'analyse des données de CTI. Cela permet aux experts de se concentrer sur les aspects plus complexes et stratégiques de la sécurité. Les compétences humaines restent en effet primordiales pour interpréter correctement les résultats et évaluer les risques réels. Les faux positifs, c'est-à-dire les erreurs où une vulnérabilité inexistante est signalée, peuvent survenir en raison de la complexité des systèmes et de l'IA ne comprenant pas toujours parfaitement le contexte. De plus, l'IA nécessite une quantité significative de données d'entraînement pour être efficace, ce qui peut poser des défis en matière de confidentialité et de disponibilité des données. Comment avoir une approche progressive en démarrant par l'identification des données utiles ? Comment les modèles d'IA peuvent être continuellement formés et adaptés pour suivre l'évolution des tactiques et des techniques utilisées par les cybercriminels ? Comment assurer une collaboration fluide entre les équipes chargées du renseignement d'intérêt cyber et les équipes de sécurité opérationnelle ?

PhilosoFIC

Pensée artificielle ou pensée humaine? Notre intelligence à l'épreuve de l'IA

À l'ère où les technologies imprègnent chaque aspect de notre vie quotidienne, l'émergence d'une réflexion sur les défis psychologiques et sociaux auxquels nous sommes confrontés semble essentielle. Les conséquences de la surcharge informationnelle et de la fragmentation de l'attention provoquent ce qu'Anne Alombert appelle dans son ouvrage une « schizophrénie numérique », où nos pensées semblent se disperser dans un flot continu d'informations et de stimuli. Quelle est la véritable nature de la pensée dans ce paysage numérique en constante évolution ? Qu'en est-il de la liberté de l'esprit ? Allons-nous vers une forme d'industrialisation des esprits et d'uniformisation de la pensée ? Comment rendre les modèles d'intelligence artificielle plus transparents et plus compréhensibles pour les utilisateurs ?

IN CYBER FORUM
EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Contacts

partenariats

partenariat@forum-incyber.com

programme

programme@forum-incyber.com