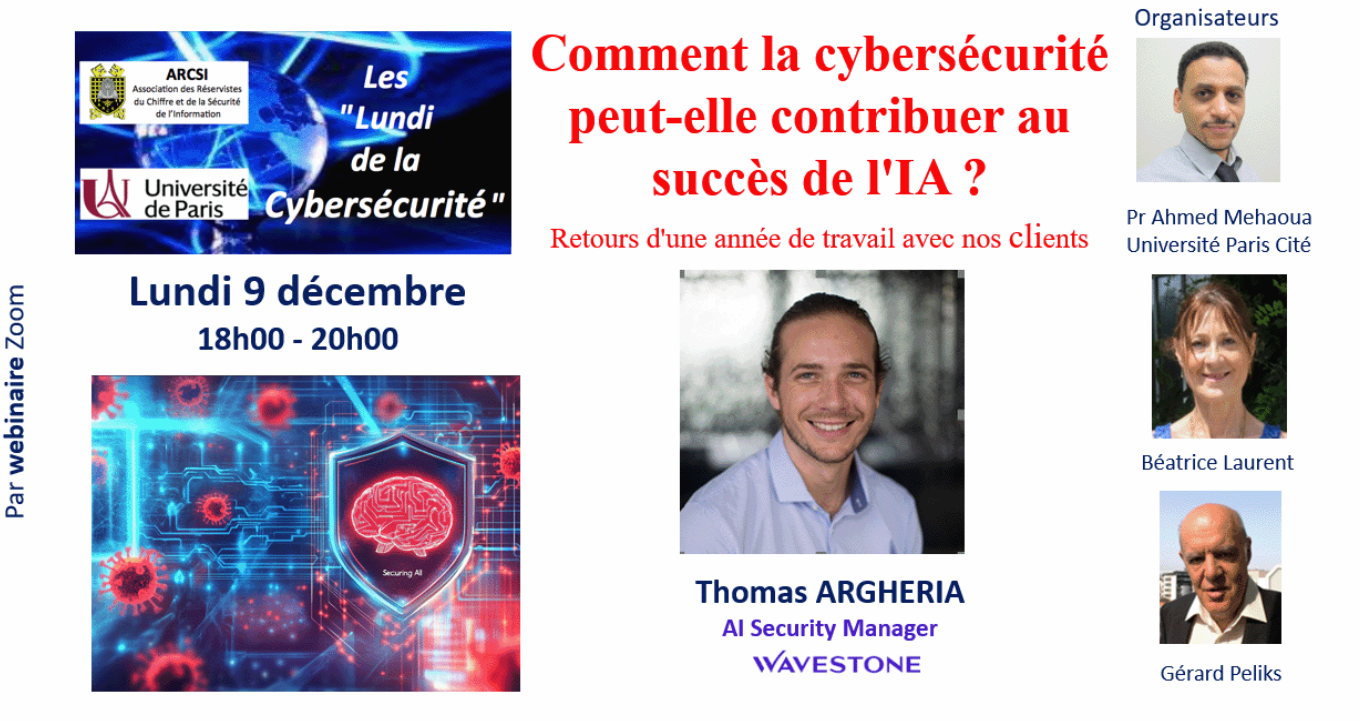
Lettre des "Lundi de la cybersécurité" n° 76

Comment la cybersécurité peut-elle contribuer au succès de l'IA ?

Retours d'une année de travail avec nos clients



Dans les produits de cybersécurité, les éditeurs de logiciels ne manquent pas de le préciser quand leurs solutions intègrent de l'IA, et en particulier de L'IA générative, car il s'agit d'une réelle rupture technologique.

Comment la cybersécurité peut-elle contribuer au succès de l'IA ?

Côté entreprises et particuliers, l'Intelligence Artificielle rend les produits plus fiables, plus rapides, plus adaptés à leurs utilisateurs et finalement plus « à la mode » … et plus vendables. Effectivement, une contre-mesure qui prend en compte la connaissance universelle recueillie à partir de multiples attaques déjà survenues un peu partout dans le monde, qui connait l'ensemble des vulnérabilités qui peuvent affecter un système d'Information, et qui les corrige, un produit qui anticipe les problèmes que pourraient rencontrer les utilisateurs plongés dans ce cybermonde qui ne fait pas de cadeaux, évidemment on ne peut pas s'en priver et on achète.

Mais l'IA apporte aussi son lot de problèmes potentiels dans les solutions qui l'intègrent. Elle est implémentée finalement par des logiciels et par des algorithmes qui peuvent venir avec leurs propres vulnérabilités. Mais aussi en plus des problèmes que peuvent poser les logiciels, on peut craindre aussi les attaques contre la signification des informations restituées. L'empoisonnement durant l'entrainement des modèles de l'IA générative qui injecte des données corrompues,

Du côté des attaquants, les outils d'IA qu'ils utilisent rendent leurs attaques plus sophistiquées, plus furtives et plus efficaces. Et quid de l'utilisation de l'IA justement pour apporter plus d'efficacité dans la défense des systèmes d'Information ? Et quid de la conformité nécessaire aux directives et aux règlements de l'Europe ?

Le marché de la sécurisation de l'Intelligence Artificielle est en plein essor mais la cybersécurité pourra-t-elle assurer le succès de l'IA ? Mais de quelle IA ?

Alors l'IA, ange ou démon ?

Wavestone a mené une enquête sur les nombreuses solutions, Thomas ARGHERIA, l'un de ses acteurs, nous présentera les résultats.

Je donne la plume à l'intervenant Thomas ARGHERIA

Depuis plus d'un an, l'IA est sur toutes les lèvres. Les actualités en la matière sont riches, et les équipes de Wavestone suivent ça de près ! Pendant cet atelier, nous aurons le plaisir de vous présenter les retours d'expérience de nos missions de sécurisation de l'IA chez plus de vingt grands comptes : sécurisation de projets IA développés en interne ou des modules IA des fournisseurs (Copilot, AzureOpenAI…), résultats, parfois surprenants, de nos pentests IA, etc…

Nous en tirerons le bilan de cette année riche pour l'IA et sa sécurité, et partagerons nos priorités pour 2025

Je reprends la plume

Qui est Thomas ARGHERIA ?

Thomas Argheria est manager en cybersécurité de l'IA au sein du cabinet Wavestone.

Titulaire d'un master en gestion de crise de l'Université de Leiden, il évolue dans le domaine de la cybersécurité depuis plus de 5 ans. Thomas a développé une expertise unique en sécurité de l'intelligence artificielle, en gestion de crise et en analyse des risques. Il a notamment mis en place une méthodologie de gestion des risques IA pour plus de 15 grandes organisations.

Aujourd'hui, il accompagne aussi bien des entreprises que des organisations publiques dans la définition de leur stratégie de cybersécurité de l'IA que dans son opérationnalisation.

Demande d'inscription pour le Lundi de la cybersécurité du mois de décembre 2024

Lundi 9 décembre, à partir de 18 h 00, par visio-conférence Zoom.

Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien vers la visioconférence.

Les demandes d'inscriptions sont à adresser à :

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution de mes lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail (gerard.peliks@arcsi.fr).

Et bien entendu, si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 9 décembre, dès 18 h 00.** La salle d'attente Zoom sera ouverte aux alentours de **17 h 00**. Prévenez-nous, dès que possible si vous êtes inscrits mais avez un empêchement qui ne vous permet pas d'assister à ce webinaire.

Quelques minutes avec une organisation : Le CyberCercle

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, autour de 19 h 15, nous donnons pour une quinzaine de minutes la parole à une organisation ou à une personne qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

Cette séquence du Lundi de décembre sera animée par **Bénédicte PILLIET**, présidente du CyberCercle (https://cybercercle.com/) qui est un cercle de réflexion, d'échanges et de rencontres sur la sécurité et la confiance numériques créé en 2011. Diplômée de Sciences Po Paris, Bénédicte est également membre du CESIN et membre fondateur du Cercle K2.

Comme nos « Lundi de la Cybersécurité », le CyberCercle favorise la diffusion d'une culture de sécurité numérique. Ses matinales remarquables se font autour des politiques publiques aux niveaux national et local.

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez tous les détails, slides, parfois aussi les enregistrements et des comptes rendus, écrits par Clarisse Véron, cette année élève du master2 « Cybersécurité et e-Santé » de l'université Paris Cité sur le web de l'ARCSI en **https://www.arcsi.fr/evt_passes.php**.

Mais attention, il n'est pas garanti qu'il y aura ces documents pour chacun de nos futurs lundis. Donc il est conseillé d'être connectés pour les suivre par Zoom.

Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ?

Prompt posée à Gemini (l'IA Générative de Google) **:**

L'IA est-elle une aide ou une menace pour la cybersécurité ?

Voici une partie de la réponse reçue :

L'intelligence artificielle (IA) représente à la fois une opportunité majeure et un défi considérable pour la cybersécurité. Son impact est double et mérite d'être examiné sous ces deux angles :

L'IA comme alliée de la cybersécurité

- **Détection proactive des menaces :** L'IA est capable d'analyser d'énormes volumes de données en temps réel, identifiant ainsi des anomalies et des patterns qui pourraient signaler une cyberattaque. Elle peut détecter des menaces émergentes bien plus rapidement qu'un humain.
- **Réduction des faux positifs :** En apprenant continuellement des nouvelles données, l'IA améliore sa précision dans la détection des véritables menaces, réduisant ainsi le nombre de fausses alertes qui peuvent surcharger les équipes de sécurité.
- **Automatisation des tâches répétitives :** L'IA peut automatiser de nombreuses tâches de routine, libérant ainsi les experts en sécurité pour se concentrer sur des activités à plus forte valeur ajoutée, comme la stratégie et l'analyse approfondie des incidents.
- **Amélioration de la réponse aux incidents :** L'IA peut aider à accélérer la réponse aux incidents en automatisant certaines actions et en fournissant des recommandations sur les mesures à prendre.
- **Renforcement de la sécurité des systèmes :** L'IA peut être utilisée pour renforcer la sécurité des systèmes en identifiant les vulnérabilités et en proposant des mesures correctives.

L'IA comme menace pour la cybersécurité

- **Création de nouvelles menaces :** Les cybercriminels peuvent utiliser l'IA pour concevoir des attaques plus sophistiquées et personnalisées, telles que des deepfakes, des attaques par phishing très ciblées ou des logiciels malveillants capables d'évoluer.
- **Détournement des systèmes d'IA :** Les attaquants peuvent détourner les systèmes d'IA pour les retourner contre leurs créateurs, par exemple en les utilisant pour lancer des attaques déni de service ou pour voler des données sensibles.
- **Complexification des défenses :** L'utilisation de l'IA par les attaquants rend la défense plus complexe, car les entreprises doivent non seulement faire face à des menaces traditionnelles, mais aussi à des attaques utilisant des techniques d'IA.

En conclusion

L'IA est un outil puissant qui peut être utilisé à des fins aussi bien bénéfiques que malveillantes. Pour tirer pleinement parti des avantages de l'IA en matière de cybersécurité, il est essentiel d'adopter une approche équilibrée et de mettre en place des mesures de sécurité robustes pour protéger les systèmes contre les attaques utilisant l'IA.

En somme, l'IA est un outil double tranchant. Son utilisation responsable et éclairée peut renforcer considérablement la sécurité de nos systèmes, mais elle peut également être utilisée pour les mettre en danger. Il est donc crucial de comprendre les enjeux liés à l'IA en cybersécurité et d'adopter une approche proactive pour y faire face.

Je reprends la plume.

Je n’aurais pas dit mieux.

Thomas ARGHERIA nous en dira plus le 9 décembre 18h et répondra aussi à nos questions. Les inscriptions sont ouvertes.

Ce graphisme en bas à gauche du visuel a été réalisé par Thomas à l’aide d’une IA générative.

Gérard