kaspersky

L'avenir de l'IA dans la cybersécurité : à quoi faut-il s'attendre ?

Une nouvelle ère de cybersécurité est arrivée

Peu d'industries affichent une vitesse de croissance comparable à celle de la sécurité. L'innovation et la persévérance des pirates informatiques en font un secteur qui n'est jamais immobile. En 2024, par exemple, le temps moyen pour enquêter et signaler les cyberincidents a augmenté de 48 % par rapport à l'année précédente, reflétant une augmentation significative de la complexité des attaques.[1]

L'IA a également facilité l'augmentation du volume des attaques, les acteurs malveillants automatisant des tâches comme le codage, la rédaction et la reconnaissance. La barrière à l'entrée a également été abaissée, les adversaires moins qualifiés pouvant en faire davantage avec le même ensemble limité de compétences.

Vladislav Tushkanov, directeur de groupe au centre Kaspersky AI Technology Research Center, explique :

> Les personnes déjà qualifiées sont en mesure de travailler plus rapidement, et celles qui ne le sont pas du tout acquièrent davantage de capacités. C'est ce qu'on appelle un « uplift », ou une élévation, lorsqu'un parfait novice en matière de scripts parvient à faire quelque chose qu'il ne savait pas faire auparavant. Au lieu de passer un mois à étudier la programmation, il peut simplement demander à ChatGPT.

1. Kaspersky, Rapport d'analyse de MDR 2024, (Kaspersky, 2025)

Il n'est donc pas surprenant qu'en 2024, la plupart des professionnels de l'InfoSec aient constaté une augmentation notable des cyberattaques par rapport à l'année précédente.[2] En effet, l'IA est passée d'un rôle offensif périphérique à un rôle central. Il en va de même pour la défense, l'IA permettant de détecter rapidement les anomalies et d'alléger la charge de travail du personnel chargé de la sécurité informatique.

Et c'est ainsi que la course à l'armement dans le domaine de l'IA a débuté. L'un des leaders dans cette course est Kaspersky, qui exploite l'IA en arrière-plan de ses solutions depuis 2004. Contrairement à de nombreux fournisseurs qui s'efforcent encore d'appréhender son potentiel défensif, Kaspersky a déjà acquis une expertise éprouvée, comme le démontre son Centre de recherche sur les technologies d'IA.

Cela signifie que l'entreprise est idéalement placée non seulement pour anticiper les menaces, mais également pour façonner l'avenir, en veillant à ce que ses clients puissent prospérer dans des conditions de plus en plus tumultueuses.

Les cybermenaces deviennent inhérentes à l'IA

Les acteurs malveillants adoptent des outils d'IA afin de maximiser la vitesse et la furtivité de leurs attaques. Les deepfakes, qui englobent les images, les vidéos et les contenus audio générés par IA, figurent parmi les technologies les plus dangereuses. La société d'ingénierie britannique Arup a été victime de ce type de contenu lorsqu'un employé a été trompé par un appel vidéo généré par IA et a envoyé 25 millions de dollars à des criminels.[3] Par ailleurs, des escrocs ont gagné 35 millions de dollars après avoir falsifié des emails et des enregistrements audio pour convaincre un employé d'une société des Émirats arabes unis qu'un dirigeant avait besoin d'argent dans le cadre d'une acquisition.[4]

Vladislav Tushkanov ajoute :

> Les médias synthétiques permettent aux pirates informatiques de décrire des événements qui n'ont pas eu lieu et les utilisent à la fois contre les utilisateurs finaux et les entreprises. La communauté des cryptomonnaies en souffre souvent. Par exemple, les escrocs collectent de l'argent prétendument destiné à des œuvres de bienfaisance ou se font passer pour votre patron et vous demandent d'effectuer un virement bancaire.

De ce fait, les attaques sont devenues plus personnelles et plus ciblées que jamais. Elles jouent sur les émotions de la victime, que ce soit la peur, la cupidité ou la confiance, pour la pousser à agir. Cependant, les deepfakes ne sont pas les seuls à poser problème. L'IA peut améliorer ou automatiser les différentes étapes d'une cyberattaque. Elle peut augmenter de manière significative la vitesse, l'efficacité et l'adaptabilité de l'attaque, par exemple en fournissant à un pirate informatique des conseils contextuels sur la façon d'éviter d'être détecté par les solutions de sécurité.

Elle peut permettre à des pirates informatiques moins qualifiés d'en faire davantage, plus rapidement. Cette méthode de copier-coller donne néanmoins lieu à des attaques extrêmement similaires dans leur exécution. Ainsi, bien qu'elles soient incessantes, elles ne sont pas particulièrement difficiles à repérer.

Vladislav Tushkanov explique :

> Pour détecter l'IA et éviter que vos analystes ne s'enlisent dans la routine et dans l'analyse quotidienne d'un nombre toujours croissant d'alertes, vous avez besoin du machine learning (ML). Il répond parfaitement à ce besoin, et vos professionnels gagneront du temps pour se consacrer à des tâches complexes ou essentielles à l'activité de votre entreprise.

L'augmentation des volumes d'attaques a amené 72 % des entreprises à s'inquiéter sérieusement de l'utilisation de l'IA par les pirates informatiques.[5] Elles aspirent à des défenses tout aussi rapides et intelligentes, sachant peut-être que les défenses traditionnelles ont du mal à lutter contre les menaces évolutives et autoadaptatives. Il est donc essentiel que les entreprises puissent compter sur des fournisseurs expérimentés dans la mise en œuvre de l'IA pour garder une longueur d'avance sur les pirates informatiques.

Vladislav Tushkanov explique :

> Nous ne devrions pas nous dire : « Tout est perdu. Les cybercriminels vont pirater tout le monde maintenant. » Nous devrions nous dire « L'IA nous a apporté le même gain d'efficacité », car tous ceux qui travaillent dans le domaine de la cyberdéfense et de la surveillance des menaces aiment autant utiliser l'IA que les personnes malintentionnées.

2. Kaspersky, Cyber Defense & AI: Are You Ready to Protect Your Organization? (Kaspersky, 2024)
3. Milmo Dan, UK Engineering Firm Arup Falls Victim to £20m Deepfake Scam, (The Guardian, 2024)
4. Lemos Robert, Deepfake Audio Nabs $35M in Corporate Heist, (Dark Reading, 2021)
5. Kaspersky, Rising Concerns, Lingering Gaps: Most Organizations Fear AI-Driven Cyberattacks but Lack Key Defenses, (Kaspersky, 2024)

L'IA est la nouvelle pierre angulaire de la cybersécurité

Il est clair que l'IA est en train de devenir la pierre angulaire de la sécurité moderne, passant d'un outil de soutien à l'intelligence centrale qui pilote des systèmes de défense avancés. Son rôle croissant entraîne une évolution vers l'analyse prédictive et la connaissance contextuelle en tant que capacités fondamentales pour détecter les menaces et y répondre.

L'exploitation du potentiel de l'IA exige une expertise approfondie, une expérience éprouvée et une base de confiance. Elle requiert également la capacité de s'adapter et d'apprendre à partir de données télémétriques mondiales. C'est ce que Kaspersky fait depuis des années, en veillant à ce que ses défenses gardent une longueur d'avance dans un paysage de menaces en constante évolution. Son expertise approfondie dans l'application de ces technologies à la cybersécurité, associée à ses ensembles de données uniques, à ses méthodes efficaces et à son infrastructure avancée d'entraînement de modèles, est devenue le fondement de son approche pour résoudre des défis commerciaux complexes.

Mais quelle est la véritable différence entre un fournisseur comme Kaspersky et un nouveau venu talentueux ? Vladislav Tushkanov explique :

> Bien sûr, il s'agit d'une différence d'approche. Si vous exercez cette activité depuis longtemps, vous savez à quels défis vous pouvez être confronté, car il est très probable que vous les ayez déjà rencontrés auparavant. Cela réduit le risque de commettre des erreurs graves. Il est pratiquement impossible d'acquérir cette expérience autrement qu'en apprenant sur le terrain.

Ainsi, bien que l'IA devienne de plus en plus importante pour les fournisseurs de solutions de cybersécurité, il n'est pas simplement question de « se lancer ». Pour être efficace, elle doit être intégrée à des solutions et faire l'objet d'itérations au fil du temps, en s'appuyant sur un vaste ensemble de données télémétriques mondiales. C'est pourquoi Kaspersky est capable d'analyser et de classer plus de 460 000 échantillons malveillants chaque jour à l'aide de technologies d'IA.

Comment l'IA de demain transformera les opérations de sécurité

L'un des principaux objectifs de la cybersécurité n'est pas seulement de réduire le temps de réponse moyen, il s'agit également de prévenir les attaques avant qu'elles ne se produisent. L'IA est essentielle pour atteindre cet objectif, en permettant une détection plus rapide, une réponse automatisée et des capacités prédictives qui offrent aux entreprises la possibilité de passer d'une défense réactive à une défense proactive. En anticipant les menaces et en agissant en temps réel, l'IA peut considérablement réduire les délais de réponse et minimiser les dommages.

Mais pour atteindre cet objectif, il n'est pas question de remplacer les professionnels de la cybersécurité, mais plutôt de leur donner les moyens d'agir. La collaboration entre l'humain et l'IA définira la prochaine ère de la cyberdéfense, l'IA prenant de plus en plus en charge les tâches répétitives et fournissant des informations qui guideront la prise de décision. Les analystes seront libres de se concentrer sur des enquêtes complexes et sur une planification stratégique, aidés par des systèmes intelligents qui apprendront et s'adapteront à leurs côtés. Vladislav Tushkanov ajoute :

> En ce moment, tout le monde parle d'« agents ». Il s'agit de systèmes ou de modules intelligents qui exécutent des tâches de manière autonome ou semi-autonome afin de protéger les environnements. Vous leur dites « J'ai ce script exécuté sur l'hôte. Qu'en penses-tu ? », et ils vous répondent « Dans des conditions normales, ce script ne devrait pas être exécuté. Je le signalerais. »
>
> Il en résulte donc une hypothèse : si vous pouvez créer un système d'agents dans lequel vous pouvez charger suffisamment de contexte pour qu'un analyste humain de première ligne puisse prendre une décision éclairée, alors, en théorie, les grands modèles de langage (LLM) seront capables de prendre des décisions avec la même fiabilité. Cela impliquerait davantage d'automatisation en première ligne. Il y a des choses qui sont faciles à programmer : une séquence claire d'actions nécessaires. Et en théorie, vous pouvez écrire un script qui effectuera ces actions, recevra les variables nécessaires pour la décision et prendra cette décision.
>
> Cependant, de nombreux scénarios ne fonctionnent pas de cette manière. Au cours de l'enquête, il existe de multiples possibilités quant aux endroits où aller et aux éléments à examiner. Seul un œil humain peut comprendre la direction que l'enquête doit prendre. À l'avenir, les agents LLM pourraient être en mesure de prendre de telles décisions. Mais pour l'heure, la touche humaine reste cruciale.

Développer une IA résiliente et fiable pour une défense plus intelligente

Kaspersky ne cherche pas seulement à préserver l'aspect humain de la sécurité dans le sillage de l'IA. L'entreprise se concentre également sur le développement d'une IA fiable et sûre, qui reste à l'affût des menaces émergentes. Le développement et l'application sécurisés de l'IA sont donc essentiels à sa stratégie commerciale, car ils garantissent que ses algorithmes sont dignes de confiance et fiables. Par exemple, l'entreprise entraîne son IA selon des normes de sécurité strictes, afin que ses détections ne soient jamais manipulées, et elle s'efforce de protéger ses modèles contre toute exploitation. Cela répond aux attentes croissantes en matière d'éthique, de transparence et de conformité et s'avère particulièrement avantageux pour les clients de Kaspersky dans des secteurs fortement réglementés. Pour renforcer la confiance, le fournisseur ouvre périodiquement ses portes pour dévoiler son fonctionnement interne.

Conclusion : l'avenir de la sécurité passe par l'IA

L'avenir de la cybersécurité sera fondé sur l'IA, façonné non seulement par la puissance des algorithmes, mais également par la confiance, la résilience et le jugement humain qui les sous-tendent. À mesure que les menaces deviendront plus complexes et plus rapides, les leaders de cette nouvelle ère seront ceux qui sauront combiner efficacement une IA de pointe avec des décennies d'expertise en matière de sécurité dans le monde réel.

L'héritage de Kaspersky en matière de cybersécurité, associé à ses investissements importants et continus dans l'IA, permet de proposer des solutions qui sont non seulement intelligentes, mais aussi résilientes, adaptatives et prêtes pour l'avenir. De la détection prédictive des menaces à la réponse autonome, l'entreprise développe des systèmes qui apprennent, évoluent et se défendent, ce qui permet aux entreprises de garder une longueur d'avance, et pas seulement de suivre le mouvement.

À propos de Kaspersky

Kaspersky est une entreprise mondiale de cybersécurité et de protection de la vie privée numérique fondée en 1997. Avec plus d'un milliard d'appareils protégés à ce jour contre les cybermenaces émergentes et les attaques ciblées, l'expertise approfondie de Kaspersky en matière de sécurité et de Threat Intelligence se traduit constamment par des solutions et des services innovants destinés à protéger les entreprises, les infrastructures critiques, les gouvernements et les consommateurs du monde entier. Le portefeuille de solutions de cybersécurité complet de l'entreprise comprend une protection des terminaux de haut niveau, des produits et services de sécurité spécialisés, ainsi que des solutions de cyberimmunité pour lutter contre les menaces numériques sophistiquées et en constante évolution. Nous aidons plus de 200 000 entreprises clientes à protéger ce qui compte le plus pour elles. Pour en savoir plus, rendez-vous sur www.kaspersky.fr.

www.kaspersky.fr