mimecast

Livre Blanc

IA & cybersécurité

Promesses et attentes de la sécurité assistée par l'IA

Aperçu

S'agissant d'intelligence artificielle et de l'auto-apprentissage, les professionnels de l'informatique sont submergés par le battage médiatique. En effet, le Hype Cycle 2023 de Gartner montre qu'une grande majorité des fonctionnalités de l'IA continuent de se rapprocher du « pic des attentes exagérées ».[1] Malheureusement, le secteur de la cybersécurité ne fait pas exception à cette tendance. Les éditeurs de solutions de sécurité s'appuyant principalement sur les fonctionnalités de l'IA présentent souvent leurs produits comme des solutions miracles, malgré les nombreux obstacles et défis qui subsistent face à des attentes élevées propres à cette technologie émergente.

Cela dit, il serait bien imprudent de la part des professionnels de la cybersécurité de ne pas tenir compte du potentiel de l'IA. Alors que le paysage moderne des menaces se complexifie et fait de plus en plus intervenir l'IA, l'IA et ses disciplines associées sont en passe de devenir des outils de cybersécurité essentiels. Le recours à l'IA dans la cybersécurité, et plus particulièrement à court terme, à l'auto-apprentissage (ML) et au traitement du langage naturel (NLP), ne fera qu'augmenter à l'avenir. Il est donc crucial pour les entreprises de combiner l'IA avec des approches de cybersécurité plus traditionnelles afin de réduire au maximum les risques liés aux cybermenaces. Mais comment un professionnel de la sécurité informatique peut-il distinguer la réalité du battage médiatique et faire les bons choix pour protéger les communications, les personnes et les données de son entreprise ?

L'objectif du présent document est précisément de répondre à cette question en expliquant pourquoi l'IA est devenue cruciale pour la cybersécurité, comment elle s'y intègre, quels sont les meilleurs cas d'usage et quelles sont les perspectives d'évolution.

Sujets traités dans ce livre blanc :

- **Tendances**
  Comment l'évolution des technologies informatiques d'entreprise et les approches des cybercriminels pour les compromettre font de l'IA une condition préalable à la cybersécurité.
- **Avantages et dangers**
  Le potentiel et les risques que l'IA apporte à la cybersécurité.
- **Applications de la cybersécurité optimisée par l'IA**
  Cas particuliers où les fonctionnalités de l'IA améliorent la cyber résilience de l'entreprise.
- **Meilleures pratiques**
  Les meilleures façons dont l'IA peut améliorer la cybersécurité, au vu du développement actuel de l'IA.
- **Regard vers l'avenir**
  Comment les fonctionnalités de l'IA vont-elles évoluer en matière de cybersécurité ?

1. Gartner identifie quatre tendances à l'origine de l'innovation à court terme en matière d'intelligence artificielle, Gartner Inc. https://www.gartner.fr/fr/articles/nouveautes-en-matiere-d-intelligence-artificielle-presentees-dans-le-hype-cycle-de-gartner-2023

Les Tendances

La Pression Augmente en Matière de Sécurité à Mesure Que Les Entreprises Migrent Vers un Nombre Restreint de Plateformes

Le défi auquel les professionnels de la cybersécurité sont confrontés réside dans le fait que tout est connecté partout et en permanence. Les environnements de travail hybrides se sont développés dans la plupart des entreprises et ont créé un écosystème où les collaborateurs, les ressources, les équipements et les données sont distribués en permanence.

Dans le même temps, les technologies et les modes de travail continuent d'évoluer. L'IA générative a fait une entrée fracassante dans le monde du travail, démocratisant l'accès à une technologie incroyablement puissante dont le potentiel commence à être découvert par tout le monde, de l'employé ordinaire au cybercriminel le plus aguerri.

Si les outils collaboratifs continuent de se développer, la messagerie reste le canal principal de la communication d'entreprise.

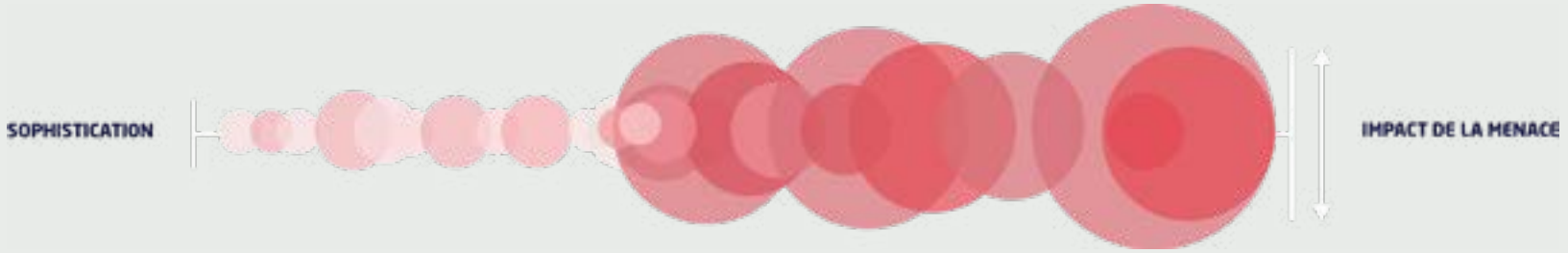
Des applications collaboratives telles que Microsoft Teams et Slack sont devenues des éléments indispensables du quotidien des collaborateurs. Des outils tels que SharePoint et OneDrive sont également largement utilisés, avec pour conséquence une surface d'attaque élargie et plus ciblée que jamais.

Ce risque cyber est aggravé par l'homogénéisation continue des mêmes outils utilisés par des centaines de millions d'utilisateurs aux quatre coins du monde. Les avantages potentiels liés à l'accès à de grands volumes de données ont fait d'éditeurs tels que Microsoft et Google des cibles de choix et l'impact sur les victimes ne doit pas être sous-estimé. Le coût moyen d'une violation de données est passé à 4,45 millions de dollars en 2023, soit le niveau le plus élevé enregistré en 19 ans d'histoire du rapport de 2023 d'IBM sur le coût d'une violation de données.[2]

> « La consolidation des outils numériques est l'un des principaux facteurs qui influencent le paysage des menaces aujourd'hui. La migration massive à des plateformes telles que Microsoft 365 a permis aux cybercriminels de développer des attaques plus sophistiquées, certains groupes de « phishing-as-a-service » ne vendant plus que des kits ciblant les environnements Microsoft. Dans le même temps, l'efficacité des défenses humaines s'est dégradée en raison de l'abus de services légitimes et de l'utilisation de comptes compromis pour lancer des attaques à partir de plateformes connues des utilisateurs et en lesquelles ils ont confiance. »
>
> **Dr. Kiri Addison – Responsable du product management chez Mimecast**

TIl n'y a guère de moyen d'échapper à la cybermenace, mais les entreprises sont prêtes à se battre.

Le dernier rapport de Mimecast sur l'état de la sécurité des messageries révèle que 76 % des entreprises se préparent aux conséquences d'une cyberattaque par e-mail au cours de l'année à venir et que 97 % ont été confrontées à au moins une attaque de phishing au cours des 12 derniers mois.



2. Rapport de 2023 d'IBM sur le coût d'une violation de données : www.ibm.com/fr-fr/reports/data-breach

Avantages et dangers
de l'IA dans la cybersécurité

Avec des attaques quotidiennes de plus en plus sophistiquées, rapides et invasives, on assiste à la naissance d'un mythe selon lequel l'IA serait LA solution miracle pour assurer la sécurité des communications, des personnes et des données. L'espoir que beaucoup placent dans l'IA est bien compréhensible. En effet, cette technologie représente une bouée de sauvetage pour les équipes de sécurité confrontées à des ressources limitées, à une complexité croissante et à des risques accrus. La vérité est cependant plus subtile. Il ne fait aucun doute que l'IA soit indissociable d'une stratégie de cyberdéfense moderne, mais comme toute innovation en matière de sécurité, il ne s'agit que d'un outil, même s'il est extrêmement puissant.

Avantages

Malgré la complexité des algorithmes, les avantages de l'IA sont simples à exprimer :

- L'IA peut traiter de grandes quantités de données, bien plus que ce que les humains pourraient imaginer.
- L'IA est rapide : elle traite les informations beaucoup plus rapidement que n'importe quel être humain.
- L'IA prend des décisions « plus intelligentes » au fil du temps : elle peut apprendre, à condition que des data scientists surveillent et réentraînent les modèles si nécessaire.
- L'IA peut simplifier et/ou automatiser certaines tâches.

En matière de cybersécurité, les volumes de données sont considérables et un temps de réponse écourté de quelques minutes peut parfois faire la différence entre une attaque bloquée et une brèche aux conséquences désastreuses. Dans ce contexte, ces avantages revêtent une importance capitale pour l'entreprise.

L'impact de l'IA générative

L'IA générative est loin d'être un nouveau concept, mais l'introduction de Chat GPT fin 2022 a incontestablement changé la donne. Avec un outil aussi puissant facilement accessible à tout internaute, l'expérimentation a explosé, ainsi que les craintes quant à ce que l'IA générative pourrait finalement être capable de faire.

Le secteur de la cybersécurité ne fait pas exception à la règle et l'idée que Chat GPT intègre des mesures de protection n'est malheureusement pas rassurante. Il existe déjà des variantes en vente sur le Dark Web qui sont entrainées pour prendre en charge des objectifs malveillants.[3] Bien qu'il y ait encore beaucoup d'inconnues sur la façon dont ces technologies seront utilisées à l'avenir, certaines tendances précoces commencent à se dessiner.

Parmi les cybercriminels, l'un des principaux cas d'usage semble être la création d'e-mails de phishing extrêmement réalistes, à grande échelle : plus de fautes d'orthographe ni d'erreurs grammaire, plus de langage inapproprié révélateur. Et pour couronner le tout, plusieurs langues sont désormais disponibles afin de cibler des pays ou régions auparavant inaccessibles.

Il n'est pas simple d'évaluer l'ampleur de la recrudescence de l'IA générative dans ce domaine, car on ne sait toujours pas si les humains ou les machines peuvent détecter avec certitude un e-mail, un hameçonnage ou autre généré par l'IA. Cependant, il est clair que le nombre d'attaques de phishing augmente[4], 98 % d'entre elles étant transmises par la messagerie d'entreprise.[5] On peut supposer que cette augmentation puisse en partie être attribuée à l'IA générative.

3. https://cybersecuritynews.com/black-hat-ai-tools-xxxgpt-and-wolf-gpt | 4. https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-47-2-surge-phishing-attacks-last-year
5. Rapport Verizon de 2023 sur les violations de données

Applications de la cybersécurité assistée par l'IA

L'approche Mimecast : sécurité multicouche s'appuyant sur l'IA

Depuis toujours, la cybersécurité consiste à prendre des décisions drastiques. Que faut-il laisser passer ? Que faut-il bloquer ? Quels risques sommes-nous prêts à prendre ? L'IA ne change rien à ces questions, mais si elle est utilisée à bon escient, elle peut permettre d'y répondre plus rapidement, à grande échelle et de manière plus efficace.

Leader de la sécurité de la messagerie d'entreprise depuis 20 ans, Mimecast a toujours été à la pointe en matière de nouvelles technologies et stratégies pour se défendre contre des adversaires toujours plus aguerris. Cela passe par l'IA, que nous intégrons à chaque couche de nos solutions afin de renforcer les défenses de nos clients, à neutraliser davantage de menaces et à alléger la pression sur leurs équipes de sécurité. Mais l'IA est loin d'être une solution miracle. Notre pile de détection effectue les bonnes inspections au bon moment, avec des algorithmes d'IA travaillant aux côtés de technologies éprouvées que nous n'avons cessé d'améliorer depuis près de 20 ans.

Nous combinons des dizaines d'approches différentes, renforcées par l'IA, afin d'obtenir une protection maximale en matière de sécurité qui fait aujourd'hui la réputation de Mimecast.

« Les techniques d'intelligence artificielle et d'apprentissage automatique ne sont pas des boîtes noires qui assurent la sécurité comme par magie. En fin de compte, ce sont des outils qui nous aident à résoudre des problèmes. La clé d'une utilisation sûre et efficace dans le domaine de la cybersécurité réside dans l'utilisation correcte de ces outils par du personnel compétent et des données de bonne qualité ».

Robin Moore – Responsable produit IA et machine learning chez Mimecast

« Les grands modèles de langage et les techniques de traitement du langage naturel ont beaucoup évolué ces dernières années, ce qui a permis aux cybercriminels de créer des attaques toujours plus sophistiquées. L'IA est nécessaire pour contrer efficacement les acteurs malveillants qui utiliseraient ces technologies à mauvais escient et garder une longueur d'avance ».

Guhan Sukumaran – Responsable data science et machine learning chez Mimecast

Cas d'usage : détection d'URL malveillantes

La capacité de détection d'URL malveillantes illustre parfaitement la philosophie de Mimecast en matière d'IA. Malgré la pertinence de cette tâche, il ne s'agit certainement pas d'une fonction ou d'un produit unique. Des dizaines de couches d'analyse travaillant ensemble sont combinées pour détecter les URL à haut risque, de la manière la plus efficace et rapide possible.

Certaines tâches consistent en de simples recherches visant à détecter des menaces simples. D'autres sont de véritables algorithmes basés sur des règles détectant des attaques plus complexes, mais néanmoins courantes. Les algorithmes de l'IA interviennent en cas de besoin. Utiliser l'IA permet de prendre des décisions rapides là où d'autres technologies ne parviennent pas à déterminer si le risque est suffisamment faible pour afficher la page ou si une analyse plus approfondie est nécessaire.

Pourquoi Mimecast n'utilise-t-il pas exclusivement des algorithmes d'IA ? En fin de compte, la puissance de la solution ne réside pas dans une seule fonction discrète, mais bien dans la combinaison de toutes ces fonctions, s'agissant d'IA ou non.

Lorsque Mimecast décide d'intégrer de l'IA dans un produit, il le fait avec un avantage décisif : plus les algorithmes de données sont entraînés, mieux ils apprennent. Mimecast protège plus de 42 000 clients dans le monde et inspecte 1,7 milliard d'e-mails au quotidien.

Tout cela alimente l'intelligence artificielle qui permet à Mimecast de proposer des solutions de pointe en matière de sécurité des e-mails, afin d'assurer la sécurité de nos clients. Notre équipe de data scientists utilise ces données pour créer des modèles d'IA dans les solutions Mimecast, puis surveille continuellement l'efficacité de ces modèles dans le contexte de menaces en constante évolution et décide quand réentraîner nos modèles afin qu'ils conservent des performances optimales.

Fonctionnalités de l'IA de Mimecast

Voici quelques illustrations de la manière dont les algorithmes d'IA renforcent l'efficacité de la solution Mimecast en matière de sécurité

Protéger la messagerie d'entreprise et fournir des informations pertinentes aux utilisateurs.

Même les utilisateurs les plus avertis peuvent se laisser piéger par un e-mail malveillant, en particulier lorsque les attaquants utilisent des technologies avancées pour recueillir des informations sur les employés et les cibler par des attaques de spear-phishing. Mimecast utilise des algorithmes d'IA et de NLP pour détecter les menaces perpétrées par e-mail, fournir des informations pertinentes aux utilisateurs et limiter le vol de données sensibles. Comme la plupart de l'IA de Mimecast, cette solution apprend en permanence et son efficacité s'améliore à chaque attaque déjouée.

Comment ça marche ?

- Mimecast utilise la technologie Social Graphing, alimentée par l'auto-apprentissage, pour cartographier les communications et comprendre les modèles de communication typiques qui servent de référence pour détecter les comportements inhabituels.
- Le texte extrait du corps de l'e-mail est analysé par NLP pour déterminer la gravité en fonction des catégories de risques, des caractéristiques du message ou des règles. Différentes stratégies peuvent être appliquéeffs aux messages pour les rejeter ou en autoriser l'examen par un administrateur.
- Le cas échéant, Mimecast décide d'ajouter des bannières d'avertissement contextuelles aux e-mails pour alerter les utilisateurs. Les bannières sont mises à jour en temps réel sur tous les équipements lorsque les niveaux de risque changent.
- Mimecast détecte et désactive les traqueurs intégrés aux e-mails, empêchant ainsi toute divulgation involontaire d'informations sensibles aux attaquants.

Empêcher les e-mails sortants et les données sensibles de tomber entre de mauvaises mains.

Les cybercriminels ne sont pas la seule menace qui pèse sur votre organisation. Vos propres collaborateurs peuvent également représenter un danger pour eux-mêmes et pour l'entreprise lorsqu'ils envoient un e-mail à un mauvais destinataire, de manière intentionnelle ou non. Dans le meilleur des cas, il s'agit d'une erreur bénigne et sans conséquences. Dans le pire des cas, cela peut provoquer la fuite de données sensibles, ce qui peut entrainer des conséquences désastreuses, notamment des amendes, des atteintes à la réputation de l'entreprise et des violations des règles de conformité. La fonctionnalité Mimecast de protection contre les erreurs de destinataires utilise l'IA pour surveiller les échanges d'e-mails, identifier les anomalies et avertir les utilisateurs s'ils s'apprêtent à envoyer un e-mail à une adresse inhabituelle, suspecte ou inconnue.

Comment ça marche ?

- Les activités de communication inhabituelles sont détectées en utilisant la technologie Social Graphing, basée sur l'apprentissage automatique, qui permet de comprendre les habitudes des utilisateurs.
- Au lieu d'être expédiés, les e-mails mal adressés sont conservés sur le gateway, puis l'expéditeur est alerté.
- Une seconde chance est donnée à l'expéditeur de confirmer les identités de(s) destinataire(s), afin de garantir un traitement des e-mails à la fois pertinent et conforme.

Détecter les e-mails malveillants maquillés en messages légitimes provenant de sources crédibles.

La collecte d'identifiants est en hausse, alors qu'un nombre croissant d'entreprises utilisent au quotidien des services collaboratifs de partage de fichiers tels que Microsoft OneDrive et SharePoint, notamment pour le télétravail. Les cybercriminels font référence à ces liens partagés dans des e-mails malveillants pour contourner les défenses, redirigeant ainsi leurs victimes vers des URL factices où elles peuvent involontairement partager leurs identifiants professionnels.

La protection contre la collecte d'informations d'identification de Mimecast utilise l'apprentissage automatique et la vision par ordinateur pour vérifier si une URL est légitime, avec des analyses si précises qu'elles peuvent remarquer si même un seul pixel est éteint sur une page Web à l'apparence inoffensive.

Comment ça marche ?

- Les algorithmes de vision par ordinateur détectent les anomalies dans les messages marketing, les informations de connexion ou les champs des formulaires qui apparaissent à l'écran.
- En fonction du niveau de suspicion et du risque associé, les utilisateurs sont soit avertis, soit empêchés d'accéder à la page. L'algorithme de l'IA apprend de chaque analyse pour devenir plus précis au fil du temps et il aura beaucoup moins de mal à détecter une usurpation de marque sophistiquée que l'utilisateur ordinaire.

Catégoriser et trier les e-mails suspects

Comment ça marche ?

Lorsque les utilisateurs signalent des e-mails suspects au SOC de Mimecast, nous utilisons l'IA pour les catégoriser, les trier et les classer par ordre de priorité en vue de les analyser. Les métadonnées de chaque e-mail suspect sont automatiquement enrichies d'un score de risque ainsi que de l'historique des signalements antérieurs de l'utilisateur. Ces informations aident les analystes à décider rapidement si un e-mail est potentiellement malveillant ou non. Les décisions prises par nos analystes sont prises en compte dans nos modèles d'apprentissage de l'IA.

Catégorisation des sites Web

Comment ça marche ?

L'apprentissage supervisé catégorise les sites Web comme malveillants ou inappropriés, indiquant aux moteurs d'inspection de Mimecast de bloquer l'accès à ces sites.

Identifier les images « à risque pour l'entreprise »

Comment ça marche ?

Toutes les images reçues par e-mail ne sont pas forcément inappropriées. Le problème est de savoir comment distinguer ce qui est bon de ce qui est « à risque pour l'entreprise » ? Les algorithmes d'apprentissage profond et de vision par ordinateur fonctionnent de concert pour détecter les images inappropriées dans les e-mails, en mettant l'accent sur la pornographie et en aidant à maintenir un environnement de travail sûr et professionnel. Pouvoir contrôler ce type de contenu, qu'il soit reçu ou envoyé, est essentiel pour la réputation de la marque, car l'adresse e-mail d'un employé véhicule, par extension, l'image de l'entreprise qui l'emploie.

Détection de codes QR malveillants

Comment ça marche ?

Fréquemment utilisés pour partager des informations rapidement et facilement, les codes QR peuvent également présenter un risque de sécurité élevé car ils peuvent contenir des liens vers des malwares, des sites inappropriés ou d'autres contenus nuisibles. Non seulement la solution Mimecast est capable de détecter les codes QR grâce à ses algorithmes de deep learning et de vision par ordinateur, mais elle décode également le lien qui se trouve derrière le code QR pour le transmettre à la fonction de détection d'URL afin d'identifier les URL à haut risque. Comme décrit dans l'exemple d'URL illustré, une combinaison de technologies, comprenant l'apprentissage automatique, est utilisée pour déterminer si les liens du code QR sont malveillants. Le cas échéant, l'e-mail sera rejeté afin de protéger l'entreprise de ce type d'attaques par phishing.

Protection contre les malwares et les attaques zero-day

Comment ça marche ?

Mimecast exploite l'IA au sein de ses moteurs d'inspection et offre une protection contre les menaces inconnues et non répertoriées : APT, attaques de type zero-day et ransomware. Les algorithmes d'apprentissage automatique intégrés dans les différentes fonctionnalités d'inspection de fichiers extraient des fonctions d'échantillons ou de familles de malware existants, ce qui leur permet de prédire les futurs malwares sur la base de fonctionnalités communes similaires. La sandbox de Mimecast utilise des technologies d'apprentissage automatique et de détection des comportements, ce qui garantit que seuls les fichiers suspects nécessitant une analyse plus poussée sont envoyés à l'inspection pour améliorer le temps de réponse de l'analyse. Les fichiers envoyés à la sandbox sont analysés par des algorithmes avancés d'apprentissage automatique en plus des leurres, des techniques anti-évasion, de l'anti-exploit et de l'analyse agressive du comportement, ce qui permet une détection efficace des malwares. Les technologies de détection de malware qui intègrent des algorithmes d'apprentissage automatique sont plus efficaces que les systèmes basés sur les signatures, en raison de l'amélioration des taux de détection des nouvelles variantes de malwares.

Meilleures pratiques

Les fonctionnalités de l'IA doivent être intégrées dans une stratégie de défense multiniveaux qui sera déployée dans des solutions de sécurité pouvant tirer parti des points forts de l'IA, tout en faisant intervenir d'autres solutions de sécurité traditionnelles. L'ensemble forme un système de cyberdéfense multiniveaux qui combine les dernières avancées en matière d'IA avec le meilleur des contrôles de sécurité basés sur des règles, le tout éventuellement arbitré par les analystes de l'équipe SOC.

L'IA est capable de reconnaître et de neutraliser les menaces courantes à grande échelle et avec une plus grande précision que les êtres humains. Mais pour bloquer les attaques les plus dangereuses, les entreprises doivent pouvoir s'appuyer sur une architecture de sécurité dotée d'un système de filtrage alimenté par l'IA et conçu par des experts en science des données. Ces derniers sont capables de différencier les menaces évidentes des e-mails ou liens légitimes pour l'activité de l'entreprise. Comme aucun modèle de détection n'est parfait, il faudra également mettre en place des contrôles permettant d'identifier rapidement les domaines dans lesquels les modèles d'apprentissage automatique ne sont pas réellement efficaces.

En pratique, cela signifie qu'il faut d'abord déployer l'IA là où il y a beaucoup de données. L'IA est en effet utilisée dans le domaine de la cybersécurité où un ensemble de données volumineux est accessible, pour identifier des anomalies dans le comportement des utilisateurs ou pour détecter un trafic réseau inhabituel, suggérant une possible intrusion.

« Dans les domaines de l'IA et de l'apprentissage automatique, la forte synergie entre l'expertise humaine et les prouesses des algorithmes propulse l'innovation vers de nouveaux sommets. L'intégration d'une composante humaine constitue la clé de voûte permettant d'obtenir une précision et une souplesse inégalées. Au fur et à mesure que les algorithmes traitent d'immenses volumes de données, la perspicacité humaine apporte une compréhension contextuelle, un discernement éthique et une touche nuancée que les algorithmes seuls ne sauraient imiter. Cette synergie façonne un avenir où la convergence de l'intelligence artificielle et de l'intuition humaine devient le catalyseur d'avancées révolutionnaires. Cette harmonie surpasse non seulement les algorithmes, mais confère à l'IA une certaine touche d'humanité »

Vedant Ruparelia – Responsable machine learning appliqué chez Mimecast

« Les technologies d'intelligence artificielle et d'apprentissage automatique ne sont pas intrinsèquement supérieures. L'efficacité de l'apprentissage automatique dépend en grande partie de la qualité des données sur lesquelles il est entraîné. Dans ce contexte, le principe immuable de l'informatique « Garbage In, Garbage Out » s'applique : des données de mauvaise qualité risquent de produire des résultats erronés. De plus, l'intelligence humaine joue un rôle crucial en encadrant le développement de l'apprentissage automatique. Des décisions erronées au cours de cette phase peuvent entraîner des résultats biaisés ou inexacts. Il est extrêmement facile de tomber dans ces pièges tendus par l'apprentissage automatique ! »

Navya Vats, data scientist chez Mimecast

Regard vers l'avenir

Quelles évolutions pour la cybersécurité assistée par l'IA ?

La science-fiction regorge de cyberbatailles entièrement automatisées, opposant bonnes et mauvaises intelligences artificielles. Le terme anglais « cyberspace » fut inventé par le romancier américain William Gibson lors de la parution en 1984 de « Neuromancien », premier roman de sa « Trilogie de la Conurb ». Le sentiment général des experts militaires est qu'un tel scénario dystopique ne se produira vraisemblablement pas avant de nombreuses années. Cependant, comme le montrent les récents développements, l'IA est en train de progresser bien plus rapidement que prévu.

L'importance de l'IA ne doit pas être sous-estimée ni surestimée. L'IA joue aujourd'hui un rôle complexe et néanmoins essentiel dans les solutions de cybersécurité multicouches qu'utilisent les entreprises pour protéger leurs communications, leurs collaborateurs et leurs données sensibles. Son déploiement doit être mûrement réfléchi et nécessite de se concentrer sur les domaines qui exploitent ses points forts tout en minimisant ses limites intrinsèques.

Il ne fait aucun doute que l'utilisation de l'IA dans le domaine de la cybersécurité est appelée à se développer, même si nombre de questions restent actuellement sans réponse. Bien qu'il ne soit pas encore totalement compris ou exploité, le potentiel de l'IA est aussi vaste que l'imagination et les compétences de l'être humain. Seul l'avenir nous dira où et jusqu'où cela nous mènera.

WORK PROTECTED.™

Advanced Email & Collaboration Security

mimecast®

www.mimecast.com | ©2024 Mimecast | All Rights Reserved | GL06359