Appliquer l'intelligence artificielle à la cybersécurité au-delà du battage médiatique

Table des matières

Synthèse

L'intelligence artificielle (IA) est une technologie incontournable qui est très prometteuse dans de nombreux domaines, dont la cybersécurité. En fait, les fournisseurs de sécurité disposent de nombreux laboratoires de recherche sur les menaces, experts en mégadonnées (« big data ») et sécurité, qui l'utilisent pour suivre l'évolution constante du paysage des cybermenaces. Plus récemment, ces technologies sont appliquées aux informations de cybersécurité d' une d'une entreprise pour détecter les menaces qui ont pu contourner les cyberdéfenses traditionnelles. Dans certains cas, l'intelligence artificielle a même été distribuée aux points d'inspection existants pour bloquer les menaces en temps réel sans renseignements sur les menaces à l'échelle mondiale.

Pour évaluer la valeur réelle d'une solution d'intelligence artificielle, il faut couper court au battage médiatique et à l'ambiguïté. Les principaux éléments à prendre en compte sont les suivants :

- **Lieu et modèle de déploiement :** l'intelligence artificielle est-elle déployée dans un laboratoire de recherche sur les menaces à l'échelle mondiale, dans un lac de données clients propre à une entreprise ou dans le cadre de contrôles de sécurité en ligne ? Quels modèles d'intelligence artificielle sont utilisés pour générer des renseignements sur les menaces ?
- **Données générées par l'intelligence artificielle :** les renseignements sur les menaces bloquent-ils une menace lorsqu'ils sont reçus, déclenchent-ils une alerte ou une action de blocage immédiate ?
- **Couverture des menaces :** quelles catégories de menaces et quelles étapes de la chaîne de cybercriminalité sont couvertes par le modèle d'intelligence artificielle ?

Aucun lieu, ni aucune donnée générée, ni aucune étape de la chaîne de cybercriminalité n'est idéal(e) pour appliquer les technologies d'intelligence artificielle. Chaque entreprise doit déterminer la bonne combinaison en fonction de facteurs tels que son goût du risque, son budget, son personnel et son niveau de maturité en matière de sécurité.

« Le champ de bataille du futur est le numérique, et l'intelligence artificielle est l'arme de prédilection incontestée. »[1]

Introduction

Pour faire face au volume, à la vitesse et à la sophistication du paysage des cybermenaces d'aujourd'hui (et de demain), les entreprises doivent utiliser l'automatisation et, en fin de compte, l'intelligence artificielle. Cependant, comme Gartner le remarque[2], « l'intelligence artificielle (IA) est incontournable et très médiatisée. Les DSI (directeurs des systèmes d'information), ainsi que les responsables de l'intelligence artificielle, des données et de l'analyse dans de nombreux secteurs d'activité, sont à la recherche d'avancées, qui viendront à long terme. Mais pour l'instant, ils doivent se concentrer sur la recherche d'applications pratiques de l'intelligence artificielle qui auront un impact immédiat. »

Cette observation vaut en particulier pour la cybersécurité, où le battage médiatique abonde. L'identification de ces applications pratiques, afin de parer au volume, à la vitesse et à la sophistication croissants des cybermenaces, nécessite la prise en compte de trois facteurs :

1. Où réside l'apprentissage artificiel et donc les données auxquelles il peut être appliqué
2. Les données de sécurité reçues et la manière dont elles peut être utilisées
3. Les catégories de menaces et les étapes de la chaîne de cybercriminalité auxquelles il peut s'appliquer

Où réside l'intelligence artificielle ?

Laboratoires de recherche sur les menaces à l'échelle mondiale

Les fournisseurs de sécurité disposent de laboratoires de recherche sur les menaces qui ont ouvert la voie au développement de l'intelligence artificielle dans le domaine de la cybersécurité. Avec une vision et une portée mondiales, nombre de ces groupes ont été parmi les premiers à réaliser que l'analyse des menaces développée par l'homme ne serait pas en mesure de suivre l'évolution rapide du paysage des menaces.

En parallèle, la protection de centaines de milliers de clients (et son encouragement financier) constituait un solide argument en faveur d'un investissement dans l'analyse avancée. Aujourd'hui, il est courant que l'apprentissage automatique (AA) en particulier soit utilisé pour accélérer l'identification de nouvelles cyberattaques, et plus important encore, les indicateurs de compromission (IOC) qui y sont associés. Ces indicateurs de compromission représentent une grande partie des mises à jour de renseignements sur les menaces fournies aux produits et services de sécurité qui protègent les clients d'un fournisseur de sécurité.

Les principaux avantages des renseignements sur les menaces basés sur l'intelligence artificielle fournis par les laboratoires de recherche sur les menaces à l'échelle mondiale sont les suivants :

1. Un vaste ensemble de données couvrant plusieurs catégories de menaces et leur cycle de vie complet pour développer et affiner les modèles d'intelligence artificielle
2. Une puissance de traitement massivement évolutive dont le coût peut être réparti sur une large clientèle
3. Certains des plus grands experts en sécurité confirmant continuellement l'exactitude des données générées

Où réside l'intelligence artificielle ? (suite)

Laboratoires de recherche sur les menaces à l'échelle mondiale (suite)

Toutefois, cette approche ultra-centralisée présente également des limites importantes, telles que :

1. Le client individuel ne reçoit que des indicateurs de compromission concernant uniquement les menaces qui atteignent le laboratoire à l'échelle mondiale.
2. Le processus de confirmation et de mise à disposition de ces indicateurs de compromission prend généralement des heures, voire plus.
3. Dans des lieux de recherche aussi complexes, multidisciplinaires et distants, les clients ont une visibilité limitée sur la manière dont l'intelligence artificielle est réellement utilisée par le fournisseur de sécurité.

Les clients des laboratoires de recherche sur les menaces à l'échelle mondiale reçoivent les données générées par l'intelligence artificielle sous la forme de mises à jour de renseignements sur les menaces, conçues pour les aider à se protéger contre les dernières cybermenaces. Il peut s'agir de mises à jour de produits de sécurité déployés au sein de l'entreprise, comme des mises à jour antivirus pour un pare-feu de nouvelle génération (NGFW) ou une plateforme de protection des terminaux, ou un flux de données sur les menaces (sur abonnement), fournissant une liste brute des adresses IP malveillantes connues ou des indicateurs de compromission similaires.

« Les renseignements sur les menaces qui avertissent votre entreprise d'une cyberattaque imminente sont opportuns. Rassembler les indications qu'une attaque était imminente alors qu'elle a déjà eu lieu ne l'est pas. »[3]

Où réside l'intelligence artificielle ? (suite)

Lac de données centralisé sur les clients

Une approche contemporaine répandue consiste à internaliser et centraliser l'intelligence artificielle au sein de l'entreprise individuelle via un « lac de données ». Cette approche compense les limites des renseignements sur les menaces à l'échelle mondiale en combinant des modèles d'intelligence artificielle similaires à ceux utilisés dans les laboratoires de recherche avec des données propres à l'entreprise. Par conséquent :

1. L'entreprise protégée identifie les indicateurs de compromission propres aux cybermenaces auxquelles elle est exposée.
2. Ces indicateurs de compromission, ainsi que des informations connexes sur la campagne de menaces et ses étapes, sont souvent mis à la disposition du personnel après l'application de l'analyse basée sur l'intelligence artificielle.
3. L'entreprise connaît exactement le type (modèle) et la portée (catégorie de menace) de l'intelligence artificielle appliquée.

Toutefois, cette approche propre à l'entreprise présente également des inconvénients, tels que :

1. Une perte de visibilité sur l'activité des menaces à l'échelle mondiale, qui pourraient l'atteindre à l'avenir
2. Des infrastructures coûteuses, notamment le stockage, le traitement, l'espace et l'énergie, nécessaires à un lac de données centralisé
3. Le temps nécessaire à la collecte, à la normalisation et à l'analyse des données retardant les résultats

Ce dernier point est l'une des limites les plus importantes car il signifie que l'intelligence artificielle ne peut être déployée qu'à titre de fonctionnalité de détection. Au moment où l'analyse est terminée, l'attaque a déjà eu lieu et nécessite des mesures correctives.

Plus précisément, les lacs de données et l'analyse basée sur l'intelligence artificielle, générés sous forme d'alertes, doivent être hiérarchisés, examinés et confirmés ou non. Les indicateurs de compromission et autres renseignements sur les menaces sont identifiés par le personnel de sécurité de l'entreprise, plutôt que par les laboratoires de recherche sur les menaces à l'échelle mondiale, et doivent être ajoutés aux contrôles de sécurité de l'entreprise, soit manuellement, soit via l'automatisation. Et bien sûr, le personnel doit nettoyer les systèmes compromis.

« Il ne fait aucun doute que la possession de données peut conférer un avantage concurrentiel, mais il doit s'agir de données opportunes et pertinentes par rapport aux défis actuels et aux opportunités du marché. Avoir plus de données pour le plaisir n'apporte pas de résultats opérationnels bénéfiques. Cela crée une responsabilité. »[4] — Gartner

Où réside l'intelligence artificielle ? (suite)

Intelligence artificielle distribuée dans l'ensemble de l'entreprise

Une troisième approche de l'application de l'intelligence artificielle à la cybersécurité consiste à déployer les modèles d'intelligence artificielle où transitent ou résident les données (fichiers, adresses IP, activité du système, etc.) à analyser. En général, cela comprend les points d'entrée, de sortie et d'inspection interne du trafic, les périphériques hôtes des utilisateurs finaux et serveurs, ainsi que la mise à disposition d'applications sur site ou dans le cloud.

Cette approche de l'intelligence artificielle présente plusieurs avantages, tels que :

- La capacité à appliquer l'intelligence artificielle à des fins de prévention et de détection
- L'intelligence artificielle identifiant les menaces spécifiques auxquelles une entreprise est confrontée
- Une compréhension complète des types d'intelligence artificielle utilisés et des catégories de menaces auxquelles ils correspondent

Toutefois, cette approche a ses limites, notamment :

- Une attention particulière aux menaces au niveau de l'entreprise, plutôt que mondial
- Une puissance de traitement limitée pour l'intelligence artificielle distribuée
- Accent unique sur les catégories de menaces passant par un point d'inspection donné

Les données générées par les modèles d'intelligence artificielle distribuée peuvent être utilisées pour prévenir une menace potentielle ou générer une alerte en vue d'une analyse et d'une réponse plus poussées. La configuration optimale dépend des spécificités du déploiement, telles que le lieu de déploiement exact, les données analysées, la durée de l'analyse, la configuration souhaitée et d'autres facteurs similaires.

Par exemple, au niveau du terminal, l'apprentissage automatique qui inspecte les caractéristiques des fichiers ou les comportements précoces associés aux tentatives d'exploitation peut souvent être déployé comme un mécanisme de prévention. En revanche, un capteur léger qui transmet l'activité du système hôte à un cloud pour l'analyse basée sur l'apprentissage automatique génère généralement une alerte en vue d'une analyse plus poussée.

« Les équipes qui utilisent [l'intelligence artificielle] en complément de leurs analystes existants… sont plus efficaces que leurs pairs et même que les équipes SOC de plus de 10 membres qui n'utilisent pas l'intelligence artificielle. »[5]

À quel niveau de la chaîne de cybercriminalité l'intelligence artificielle est-elle appliquée ?

Outre l'emplacement physique de l'analyse et la nature des données générées, il est important de prendre en compte la phase de cyberattaque à laquelle elle s'applique. Lockheed Martin a créé la chaîne de cybercriminalité, en décrivant les sept étapes communes d'une cybermenace[6] , qui doivent toutes être réussies pour qu'un cybercriminel atteigne son objectif ultime : reconnaissance, armement, livraison, exploitation, installation, commande et contrôle, et action selon les objectifs. Si l'on parvient à contrer le cybercriminel à n'importe quel stade, il se trouve privé de son objectif ultime.

L'étape de la chaîne de cybercriminalité où l'entreprise agit détermine si une attaque est empêchée avant l'impact ou si elle nécessite une détection et une réponse plus coûteuses. Les renseignements sur les menaces générés dans les laboratoires de recherche sur les menaces mondiales sont souvent utiles pour la prévention. Les bases de données de réputation IP peuvent détecter les efforts de reconnaissance, et les renseignements sur les menaces fournis aux systèmes de sécurité déployés sont conçus pour interrompre les étapes de livraison, d'exploitation et d'installation.

Cependant, une stratégie de prévention uniquement n'est pas toujours efficace, comme le montre le flux constant de gros titres sur les violations de données. La plupart des entreprises investissent dans des fonctionnalités de détection des menaces, qui sont, selon Gartner, « encore fortement axées sur la fin de la chaîne de cybercriminalité. »[7]

L'approche du lac de données sert souvent de pivot à la détection et la réponse sur les terminaux (EDR), l'analyse comportementale des utilisateurs et des entités (UEBA), et d'autres méthodes de détection basées sur l'intelligence artificielle. Ces contrôles sont appliqués après l'étape d'installation pour identifier les activités anormales souvent associées à la commande et au contrôle ou à l'action selon les objectifs, qui est souvent l'exfiltration des données. À ce stade, l'intelligence artificielle vise à identifier une attaque en cours, avant que les objectifs de l'étape finale, comme l'exfiltration des données, ne soient atteints.

Une approche distribuée de l'intelligence artificielle est très prometteuse, car elle permet l'application de modèles d'intelligence artificielle propres à l'entreprise au début de la chaîne de cybercriminalité. En ciblant les phases de livraison, d'exploitation et d'installation, une entreprise diminue la probabilité qu'une réponse coûteuse soit nécessaire.

Conclusion

Une entreprise peut appliquer l'intelligence artificielle à différents endroits, que ce soit dans des laboratoires de recherche à l'échelle mondiale ou en interne, et à différentes étapes de la chaîne de cybercriminalité. Les données générées par l'intelligence artificielle peuvent également être appliqués appliquées à des fins de prévention ou de détection. Chaque approche a ses avantages, mais aussi ses limites, et les entreprises doivent couper court au battage médiatique et aux fioritures afin d'identifier la combinaison d'approches optimale pour leur situation.

Elle doit comprendre une combinaison de chaque type d'intelligence artificielle. Le fournisseur de sécurité d'une entreprise doit fournir une large couverture des types et des catégories de menaces. Cela permet de déployer des contrôles de sécurité pour détecter et bloquer les menaces au début de la chaîne de cybercriminalité.

Ces renseignements sur les menaces doivent être complétés par des produits de sécurité, tels que des antivirus de nouvelle génération, des pare-feux d'applications Web (WAF), des passerelles de messagerie sécurisées et des sandbox, avec une intelligence artificielle intégrée. Cette intelligence artificielle intégrée permet souvent de prévenir des menaces propres à une entreprise ou de réagir rapidement à des épidémies mondiales.

Dans la mesure du possible, une entreprise doit également utiliser des systèmes de détection et de réponse avancés, tels que la détection et la réponse sur les terminaux (EDR), la gestion des informations et des événements de sécurité (SIEM) et l'analyse comportementale des utilisateurs et des entités (UEBA). Ces systèmes complètent les contrôles ciblant les premières étapes de la chaîne de cybercriminalité, permettant une détection et une réponse complètes pour les attaques qui échappent aux contrôles préventifs. Toutefois, il est essentiel que les équipes de sécurité présentant des effectifs suffisants et qualifiés pour réagir efficacement.

[1] William Dixon and Nicole Eagan, « 3 ways AI will change the nature of cyber attacks », World Economic Forum, 19 juin 2019.

[2] Kenneth Brant, et al., « Hype Cycle for Artificial Intelligence, 2019 », Gartner, 25 juillet 2019.

[3] Zane Pokorny, « 3 Key Elements of Threat Intelligence Management », Recorded Future, 8 août 2018.

[4] Nick Heudecker and Adam Ronthal. « How to Avoid Data Lake Failures », Gartner, 10 août 2018.

[5] Zeljka Zorz, « AI is key to speeding up threat detection and response », Help Net Security, 14 août 2017.

[6] « The Cyber Kill Chain », Lockheed Martin, consulté le 23 mars 2020.

[7] Craig Lawson, et al., « Market Guide for Managed Detection and Response Services », Gartner, 15 juillet 2019.

www.fortinet.fr

618115-0-0-FR

juin 30, 2020 12:56 PM

EB-FA--1