Capgemini

L'INTELLIGENCE ARTIFICIELLE, UN OUTIL ESSENTIEL DANS LA LUTTE CONTRE LES CYBERMENACES

Protéger les organisations contre les cyberattaques est plus crucial que jamais. Or établir une défense efficace se révèle également de plus en plus difficile. Les meilleures solutions développées récemment s'appuient sur l'IA, mais exigent également des organisations qu'elles repensent tout, des fournisseurs qu'elles utilisent à la façon dont elles configurent leurs solutions de sécurité. Il est nécessaire qu'elles s'y préparent dès à présent.

La cybersécurité est un enjeu fort depuis les débuts d'Internet, mais de nombreuses évolutions, constatées au niveau global, l'ont remise au premier plan. La cyberguerre, les attaques visant à perturber les infrastructures d'importance vitale et les attaques de type social engineering sont désormais parties prenantes des conflits d'aujourd'hui. Dans le même temps réseaux criminels et autres acteurs malveillants récoltent les fruits des rançongiciels, de l'usurpation d'identité et autres attaques contre les particuliers et les entreprises.

Quiconque aurait besoin d'une preuve de l'ampleur du problème n'aurait qu'à étudier une liste des principales violations de données du 21ème siècle. Deux vérités apparaîtront clairement. Premièrement, ces attaques sont de plus en plus fréquentes. Deuxièmement, leur impact est énorme, chacune impliquant des centaines de millions de personnes, d'enregistrements de données ou de comptes.

De manière tout à fait significative, les cibles de nombre de ces attaques sont de grandes entreprises à la pointe de la technologie, telles que Facebook, LinkedIn, Adobe, Alibaba et Sina Weibo, mais aussi les entités gouvernementales, les PMEs, … toutes les entreprises sont des cibles. De telles violations ont incité le Forum économique mondial à faire de la cybersécurité l'un des dix principaux problèmes à résoudre dans les années à venir.

Exacerbant les problèmes de sécurité, la pandémie de COVID-19 a accéléré l'évolution vers la numérisation et l'interconnexion à l'échelle mondiale. Mais avant même l'influence profonde de la pandémie sur la croissance du numérique, les experts en sécurité ont admis qu'ils étaient confrontés à d'énormes défis.

> Lors d'entretiens conduits en 2019 dans le cadre de la rédaction de « Réinventer la cybersécurité grâce à l'intelligence artificielle », un rapport du Capgemini Research Institute, 56 % des entreprises interrogées ont admis que leurs analystes en cybersécurité étaient débordés, 42 % ont signalé une augmentation des incidents de cybersécurité par le biais d'applications sensibles au facteur temps, et 23 % ont noté qu'elles n'étaient pas en mesure d'enquêter avec succès sur tous les incidents identifiés.

Trois ans plus tard, les défis restent importants. L'écosystème de la cybersécurité est diversifié et complexe : il englobe des gouvernements, des organismes à but non lucratif, des entreprises privées, des personnes, des processus et des dispositifs. Et ces divers acteurs interagissent toujours plus fréquemment, ce qui génère des quantités de données également toujours plus importantes.

DE NOUVELLES RÉALITÉS

Les organisations ont été contraintes de s'adapter à de nouvelles réalités, parmi lesquelles :

- Le travail à distance, qui a augmenté le nombre d'appareils se connectant à l'organisation depuis l'extérieur de son périmètre.
- Un plus grand nombre d'employés et de clients utilisant des mobiles, des ordinateurs, des tablettes et autres technologies pour interagir avec les organisations.
- De nouveaux outils commerciaux à forte intensité de données, tels que les solutions de connaissance et d'expérience client alimentées par l'IA.

Ces changements ont créé davantage d'opportunités pour ceux qui adoptent des comportements malveillants, et davantage de travail pour des experts en cybersécurité déjà débordés.

BONNE NOUVELLE : L'INTELLIGENCE ARTIFICIELLE EST LÀ !

L'IA peut traiter de grandes quantités de données, rechercher et contrer des risques tels que la fraude, les logiciels malveillants et les intrusions. Certes, l'IA est encore un domaine émergent et son utilisation en cybersécurité est loin d'être mature. Mais la plupart des experts en cybersécurité reconnaissent aujourd'hui le rôle émergent de l'IA. En outre, ces experts apportent des changements significatifs à la manière dont les informations sont traitées et sécurisées afin de faciliter les fonctions de l'IA.

ZERO TRUST

La philosophie *Zero Trust* est un exemple significatif de cette évolution. Elle bouleverse l'approche traditionnelle d'une cybersécurité basée sur la défense d'un périmètre, qui consistait à empêcher les menaces d'entrer dans le réseau d'une organisation, tout en supposant que tout ce qui se trouvait déjà dans le réseau était sûr. Comme son nom l'indique, le *Zero Trust* suppose que toute activité sur le réseau est potentiellement malveillante jusqu'à ce qu'elle ait été vérifiée comme étant digne de confiance.

Cette philosophie existe depuis des années, mais elle a reçu un soutien important en janvier 2022 lorsque *l'Office of Management and Budget* de la Maison Blanche a publié sa stratégie fédérale visant à faire évoluer le gouvernement américain vers un modèle de cybersécurité *Zero Trust*. Cela encouragera d'autres pays ainsi que des organisations privées à suivre le mouvement.

Le *Zero Trust* exige une vérification continue de tous les acteurs, réseaux, dispositifs, systèmes et services. Il s'appuie sur des contrôles d'identité et d'accès solides, tels que l'authentification multifactorielle. Cela n'est possible que si le *Zero Trust* s'appuie sur l'IA, et, pour faciliter cela, les experts en cybersécurité adaptent les modèles développés pour les solutions commerciales alimentées par l'IA.

Par exemple, les solutions à forte intensité de données qui fournissent des aperçus, des recommandations et de meilleures expériences client ont rendu les *data lakes* traditionnels ingérables. La quantité de données en jeu est si importante que l'application de l'IA à un *data lake* unifié peut dramatiquement ralentir un réseau. La solution consiste à remplacer les *data lakes* par des architectures de maillage de données qui distribuent les informations dans des domaines plus petits. Les experts en cybersécurité adoptent la même approche, ce qui crée des opportunités pour de nombreux petits fournisseurs spécialisés.

Les grands fournisseurs de cybersécurité proposent des solutions qui peuvent répondre à la plupart des besoins d'une organisation. Mais il existe des lacunes. Celles-ci sont comblées par des acteurs de niche, et il en existe des milliers, chacun proposant des solutions ciblées. La plupart des organisations constateront qu'elles doivent travailler avec une série de fournisseurs, petits et grands, pour couvrir la totalité de leurs besoins en matière de cybersécurité.

LA PLATEFORME OPEN XDR

Avec un grand nombre de petites solutions, la pièce manquante est un moyen de s'assurer qu'elles fonctionnent toutes ensemble. Là encore, la réponse se trouve dans les architectures de maillage de données, qui incluent des modèles de gouvernance garantissant l'interopérabilité par le biais de normes et de protocoles communs.

En Europe, certains acteurs de la cybersécurité se font les champions de l'interopérabilité par le biais de la plateforme *Open XDR*. Cette alliance a pour objectif de développer, maintenir et distribuer des normes techniques et organisationnelles favorisant une approche ouverte, transparente et collaborative de la cyberdéfense. La plateforme *Open XDR* vise à garantir que des solutions de cybersécurité distinctes fonctionnent ensemble afin d'offrir la meilleure protection possible aux organisations, tout en veillant à ce que le matériel, les logiciels et les autres composants soient conçus pour évoluer à mesure que de nouvelles menaces sont identifiées.

LES ORGANISATIONS DOIVENT PRÉPARER UNE FEUILLE DE ROUTE

Dans le cadre de mon travail, je fais comprendre aux clients de Capgemini que les cyberattaques ne sont pas près de disparaître et que les organisations doivent élaborer des stratégies modernes pour les contrer. Ces tactiques dépendront de plus en plus de l'IA et d'autres technologies de pointe à forte intensité de données.

Il est donc essentiel que le plan de cybersécurité de chaque organisation comprenne une feuille de route pour l'aider à se préparer aux besoins futurs. Cette feuille de route doit refléter trois impératifs fondamentaux. Premièrement, les organisations doivent insister pour que toutes les solutions de cyberdéfense soient interopérables. Deuxièmement, elles doivent fonctionner avec des principes *Zero Trust*. Enfin, elles doivent être dynamiques et faire appel à l'intelligence artificielle afin d'être en mesure d'apprendre et d'évoluer, pour contrer les nouvelles menaces dès leur apparition.

À RETENIR

L'IA est essentielle : dans le monde actuel, où les données sont nombreuses, les experts en cybersécurité doivent s'appuyer sur l'IA pour détecter et neutraliser les menaces.

La philosophie Zero Trust permet une meilleure défense contre les cybermenaces et, avec le soutien du gouvernement américain, elle va être largement adoptée. Mais elle exige de nouvelles méthodes de stockage et de traitement des données.

La collaboration est reine : aucun fournisseur de cybersécurité ne peut offrir une solution parfaite, et les utilisateurs finaux ne doivent pas non plus s'enfermer dans la solution d'un seul fournisseur. Il est donc essentiel que le secteur adopte l'interopérabilité par le biais d'alliances telles que la plateforme Open XDR.

Auteur

Jérôme Desbonnet
VP, Cybersecurity CTIO,
Insights & Data, Capgemini

A propos de Capgemini

Capgemini est un leader mondial, responsable et multiculturel, regroupant 340 000 personnes dans plus de 50 pays. Partenaire stratégique des entreprises pour la transformation de leurs activités en tirant profit de toute la puissance de la technologie, le Groupe est guidé au quotidien par sa raison d'être : libérer les énergies humaines par la technologie pour un avenir inclusif et durable. Fort de 55 ans d'expérience et d'une grande expertise des différents secteurs d'activité, Capgemini est reconnu par ses clients pour répondre à l'ensemble de leurs besoins, de la stratégie et du design jusqu'au management des opérations, en tirant parti des innovations dans les domaines en perpétuelle évolution du cloud, de la data, de l'Intelligence Artificielle, de la connectivité, des logiciels, de l'ingénierie digitale et des plateformes. Le Groupe a réalisé un chiffre d'affaires de 18 milliards d'euros en 2021.

*Get The Future You Want**

Plus d'informations sur www.capgemini.com

** Capgemini, le futur que vous voulez*