Cybersécurité : quand l'IA rebat les cartes

L'intelligence artificielle transforme en profondeur le paysage de la cybersécurité. En démocratisant certaines capacités offensives et en accélérant la préparation des attaques, elle élargit considérablement la surface de menace des entreprises. Mais l'IA constitue aussi un puissant outil de défense. Pour Jérémy Voisin, directeur de la division Cyber du groupe CHEOPS Technology et RSSI de CHEOPS Technology Switzerland, l'enjeu est désormais d'automatiser davantage tout en conservant l'humain au cœur de la décision.

Jérémy Voisin
Directeur de la division Cyber
du groupe CHEOPS Technology et RSSI
de CHEOPS Technology Switzerland

Jérémy Voisin, les cyberattaques n'ont pas attendu l'intelligence artificielle pour devenir sophistiquées. Qu'est-ce que l'IA change réellement ?
L'IA a complètement rebattu les cartes en démocratisant des capacités offensives auparavant réservées à des groupes très structurés disposant de compétences pointues. Aujourd'hui, une personne sans réelle expertise peut accéder à des outils lui permettant de construire des attaques de plus en plus crédibles. L'autre transformation majeure est la vitesse : collecte massive d'informations, génération de contenus convaincants, déplacement latéral intelligent… L'IA amplifie les capacités des attaquants et rend plus difficile encore la distinction entre le vrai et le faux.

Quelles menaces les entreprises doivent-elles particulièrement anticiper ?
Le grand changement est l'élargissement de la surface de menace. Désormais, toute personne ayant accès à Internet peut potentiellement devenir une menace. Cela entraîne une explosion des attaques opportunistes : on attaque à foison, puis on regarde là où « ça mord ». Les attaques ciblées existent toujours, mais la vitesse et le volume des attaques opportunistes changent véritablement la donne.

Dans ce contexte, comment construire une stratégie de cybersécurité efficace ?
Il faut d'abord revenir aux fondamentaux. La cybersécurité n'est pas un produit que l'on achète : c'est un état. Un système d'information est en état de cybersécurité lorsqu'il est capable de résister aux cyberattaques dans le cyberespace. Pour y parvenir, il faut avant tout appliquer rigoureusement les bonnes pratiques en matière de systèmes, de réseaux et de programmation, puis mettre en place une gouvernance et une stratégie permettant de faire évoluer cet environnement. Les solutions et services, comme ceux d'un SOC (Security Operations Center), viennent ensuite maintenir cet état de cybersécurité.

L'IA va-t-elle rendre l'expertise humaine moins nécessaire dans les SOC ?
Au contraire. Notre SOC existe depuis 2014 et nous sommes également un CERT accrédité, c'est-à-dire une équipe spécialisée dans la réponse aux incidents de cybersécurité. Cette expérience nous donne un certain recul sur l'évolution des technologies. L'IA excelle pour traiter des volumes massifs de données et détecter des signaux faibles. Mais la compréhension de ce qui se passe et le jugement restent humains. Nous défendons le principe du « human in the loop » : l'IA assiste et accélère le travail de nos analystes, mais c'est toujours l'expert qui, en fonction du contexte et de son expérience, détermine s'il s'agit d'un vrai positif, d'un faux positif ou s'il faut approfondir l'investigation.

Comment utilisez-vous concrètement l'IA pour renforcer la cybersécurité ?
L'IA en cybersécurité ne date pas des IA génératives. Nous utilisons depuis de nombreuses années le machine learning et le deep learning pour détecter des signaux faibles, identifier des anomalies ou corréler différents éléments qui ne correspondent pas nécessairement à des chemins d'attaque connus. Cela fait au moins dix ans que nous utilisons le machine learning dans notre détection. Nous avons désormais intégré l'IA générative comme assistant de nos ingénieurs, notamment pour effectuer des tâches répétitives et leur fournir un travail déjà largement préparé, afin qu'ils puissent se concentrer sur leur valeur ajoutée.

L'humain est souvent présenté comme le maillon faible de la cybersécurité. Peut-il devenir un atout ?
L'humain est à la fois la première ligne de défense et la dernière. S'il est mal formé, il peut effectivement être le maillon faible. Mais bien sensibilisé, il devient au contraire le maillon le plus fort. C'est pourquoi nous privilégions des sensibilisations sur mesure, avec des démonstrations en direct. Nous montrons concrètement ce qui peut se produire lorsqu'un utilisateur adopte un comportement à risque. L'objectif est de créer un véritable effet « waouh » : les démonstrations marquent davantage les esprits que de simples diapositives.

Comment abordez-vous l'équilibre entre innovation, Cloud et sécurité ?
Tout est une question d'équilibre entre le risque, le coût et le bénéfice. Nous ne sommes pas dans une logique consistant à dire qu'il faut tout mettre on-premise ou, à l'inverse, tout basculer dans le Cloud. Chaque décision doit être pragmatique. Notre devise est simple : la bonne application dans le bon Cloud avec le bon niveau de sécurité. Une application critique manipulant des données sensibles n'a évidemment pas les mêmes exigences qu'un outil collaboratif. Il faut donc analyser chaque situation et trouver le bon équilibre, souvent dans une logique d'hybridation.

La souveraineté numérique prend également de l'importance. Quelle est votre approche ?
Elle est primordiale pour nous. En Suisse comme en France, nous maîtrisons nos propres datacenters, nos réseaux et nos équipements. La souveraineté n'est pas pour nous un simple argument marketing : les données de nos clients suisses restent en Suisse et sont opérées par des équipes suisses. Il n'y a pas de sous-traitance : nous maîtrisons la chaîne de bout en bout.

Quel sera, demain, le rôle de l'IA dans la cybersécurité ?
Nous allons automatiser toujours davantage l'investigation, la réponse, le « hunting » et différentes tâches opérationnelles. Nous avons déjà commencé à intégrer de l'IA agentique. Mais nous voulons conserver une supervision humaine. Chez nous, une IA ne prendra jamais seule la décision, par exemple, d'isoler une machine. Elle fournit son analyse, son niveau de confiance et les éléments factuels sur lesquels elle s'appuie. L'humain prend ensuite la décision. Le triptyque « people, process, technology » restera donc essentiel : la technologie va évoluer avec l'IA, mais l'humain et les processus resteront au cœur de la cybersécurité.

Interview **Océane Kasonia**

Plus d'informations sur
www.cheops-technology.ch

CHEOPS TECHNOLOGY
The Cloud & Data Centric Company