dossier

L'IA au service de la sécurité ?

L'intelligence artificielle est plus que jamais d'actualité dans le monde de la sécurité. Tant chez les fabricants de solutions que chez les utilisateurs. Mais, concrètement, que permet-elle de faire et dans quelles mesures ?

© Getty images

SOMMAIRE

2 QUESTIONS À

FANCH FRANCIS

Directeur général d'OAK Branch

© DR

En quoi l'IA peut-elle permettre aux entreprises et organisations de mieux lutter contre les fraudes, l'espionnage… ? Contre les actes de malveillance ?

La prise de décision d'un être humain est souvent dépendante de ses expériences passées. Néanmoins, un être humain ne peut avoir connu une infinité d'expériences et il est difficile pour lui de généraliser cette prise de décision de manière précise lorsque ce nombre augmente fortement.
Par exemple, pour de la lutte contre la fraude, un être humain peut observer au bout de nombreux cas de fraude que celle-ci peut être corrélée avec un grand nombre de versements, de gros versements ou la combinaison des deux. Cependant, il va être difficile pour lui d'estimer si ce qui doit tirer une sonnette d'alarme est le fait d'effectuer 100 ou 150 virements par semaine, ou peut-être simplement 75 virements mais avec de très gros montants. L'IA permet d'estimer précisément l'ensemble de ces facteurs afin de répondre à une question précise (ex : maximiser le nombre de fraudes détectées, minimiser le pourcentage de fausses alertes, etc.). Il est possible de lutter contre l'espionnage en utilisant des algorithmes permettant de détecter des intrusions dans des systèmes, en détectant des fausses informations (fausses identités, fake news, etc.).
Ou encore, il est possible de superviser les métadonnées (des données qui permettent de décrire d'autres données telles que date de collecte, niveau de confiance, sensibilité, etc.) c'est-à-dire autre chose que le contenu lui-même (conformité au RGPD oblige).
Cette supervision permet la génération d'alertes sur des accès non conformes, des effacements illégaux ou encore du stockage anormal. Là où une plateforme analytique apporte le plus d'atout c'est dans le domaine du croisement et de la fusion de données. Aujourd'hui des millions d'euros sont dépensés pour la collecte de données de toutes sortes. Cependant, l'analyse de ces données est confiée à un simple tableur. Sans une plateforme analytique telle que celle que propose OAK Branch et le groupe Deveryware, impossible de trouver le lien entre des lignes de bases de données, des emails et des rapports stockés dans un file system.
Les sujets où le recoupement de données au moyen d'une plateforme analytique sont multiples : fusion de données sécuritaires (rapport d'experts, retours terrains, réseaux sociaux) pour estimer le niveau de risque d'un pays ; analyse de contenu anonyme pour détection d'accès illicites, détection de fraudes complexes, etc.

Le domaine de l'IA a un véritable intérêt stratégique pour les États et les OIV. Comment pourrait-on soutenir les Français qui développent des solutions face aux géants asiatiques et autres ? Ne serait-ce que pour protéger les données exploitées…

Il ne faut pas confondre la capacité logicielle et la capacité fonctionnelle. OAK Branch utilise différentes plateformes pour adresser différents sujets. La souveraineté dépend du niveau de maîtrise de la plateforme, pas seulement de l'origine du code source. Ainsi une plateforme nationale, mais dont le client ne maîtrise pas les capacités n'est pas une plateforme souveraine.
La souveraineté est l'absence de monopole capacitaire. Pour protéger les Français qui développent des solutions logicielles et/ou fonctionnelles, il faut empêcher le nivellement par le bas qui surviendrait si l'État ne subventionne que les géants français du domaine.