Automobile & IA : la révolution sous le capot !

3 questions à Daniele Mancini, Field CISO chez Fortinet

L'intelligence artificielle donne aux individus et aux entreprises la capacité de s'adapter rapidement. Charles Darwin avait déjà abordé ce sujet il y a longtemps en disant que : « *l'animal qui survit n'est ni le plus fort, ni le plus intelligent, mais celui qui sait s'adapter le plus rapidement à son environnement.* » Et c'est exactement ce qu'offre l'IA.

Nous avons donc demandé à **Daniele Mancini, Field CISO chez Fortinet** de nous expliquer plus en détail les enjeux que représente cette technologie pour le secteur automobile car ce dernier a été profondément transformé par la révolution IA au cours des dernières années.

Pourquoi les hackers s'intéressent-ils particulièrement au secteur automobile ?

« La chaîne d'approvisionnement est une cible idéale pour les hackers car elle est à la fois complexe et hyper connectée. Chaque élément est relié au cloud et à d'autres systèmes pour fournir des services.

L'intégration croissante de technologies, avec notamment des systèmes avancés d'aide à la conduite (ADAS) et des services de conduite autonome, nécessite de faire appel à un écosystème de fournisseurs tiers, élargissant ainsi la surface d'attaque pour les hackers. Les gains financiers sont donc potentiellement plus importants, en raison du nombre de cibles affectées.

En outre, la digitalisation de l'outil industriel (ex : jumeaux numériques) génère un volume important de données, un vrai trésor de guerre pour les cybercriminels qui leur permet d'identifier de nouvelles cibles, d'améliorer leurs attaques ou, simplement, revendre les données. »

Comment l'IA contribue à renforcer la chaîne d'approvisionnement ?

« Le premier domaine à bénéficier de l'IA est *la maintenance prédictive*. L'IA est capable, à partir de données pertinentes, d'anticiper les opérations de maintenance, d'en analyser l'impact et, in fine, d'accélérer la mise à disposition des pièces nécessaires.

L'IA présente également des avantages en matière de *gestion des stocks*, qui représente un budget particulièrement important. Grâce à l'IA, la disponibilité de données de maintenance préventive et l'optimisation des inventaires favorisent la maîtrise des coûts.

Le troisième volet porte sur *la compréhension du comportement des utilisateurs*. Au-delà de certaines préoccupations légitimes en matière de confidentialité, le volume impressionnant de données recueillies à partir des capteurs d'un véhicule permet de définir un environnement confortable pour les conducteurs et ouvre l'expérience de la conduite à de nouveaux horizons. Avec l'IA, il devient aussi possible de prendre en compte les conditions environnementales, renforçant ainsi la sécurité à bord. Une solution

particulièrement bénéfique pour les chauffeurs de poids lourd, qui s'exposent à des risques supplémentaires lorsqu'ils glissent sur le bord de l'autoroute, notamment le vol de marchandises. »

Comment améliorer la sécurité dans la chaîne d'approvisionnement automobile ?

« La chaîne d'approvisionnement automobile est complexe mais plusieurs leviers permettent de l'optimiser comme le contrôle en temps réel mais également la collaboration et la cyber résilience.

L'innovation permet de *contrôler en temps réel* des informations émises tout au long de la chaîne d'approvisionnement. C'est ce qu'on appelle *la cartographie de la chaîne d'approvisionnement*. Elle permet d'identifier les flux de données et les différentes informations propre à la chaîne d'approvisionnement pour réagir plus rapidement à un éventuel cyber-incident et y apporter la réponse la plus pertinente.

L'IA améliore également la *collaboration*. En disposant de données détaillées sur les différents maillons de la chaîne d'approvisionnement, il devient plus facile de coordonner les actions. Chaque technologie doit s'inscrire dans un processus de collaboration. L'univers des menaces est complexe et les cybercriminels unissent souvent leurs forces pour mener des attaques plus efficaces. Nous devons en faire de même, autrement dit, collaborer. Pour y parvenir, nous avons besoin de volumes importants de données pertinentes, détaillées et d'éléments de contexte.

Enfin, la *cyber-résilience*, à savoir disposer des technologies et capacités nécessaires pour que la stratégie de réponse aux incidents devienne efficace et pérenne. Dans le domaine de l'automobile et de la production industrielle de manière générale, cet objectif nécessite des investissements et des ressources supplémentaires. »

L'IA va-t-elle se généraliser à l'ensemble de l'écosystème automobile ?

« À court terme, c'est certain. L'adoption de l'IA multimodale nous permet de traiter des informations au format texte, image et CAO (conception assistée par ordinateur). A l'avenir, il sera possible de traiter encore plus de sources et de formats. La même direction est prise dans le domaine de la cybersécurité. Les progrès s'accélèrent et désormais les entreprises savent comment bâtir un lac de données pour fournir des informations pertinentes aux clients. L'industrie automobile doit suivre cette voie, avec des acteurs capables de corréler les informations avancées de cybersécurité avec leurs données internes. L'IA contribue à ce changement, améliorant la stratégie de gestion des risques en entreprise.

Pour autant, déployer efficacement l'IA n'est pas si simple, car pour être pertinent, il faut mettre en place un lac de données interne. Pour cela, l'une des manières les plus répandues consiste en l'adoption de *données synthétiques*. Ce sont des données générées artificiellement pour entraîner les modèles d'IA. Mais ces données ne sont utiles que si elles sont reliées à un usage précis. Ainsi, pour accélérer les processus financiers par exemple, l'inventaire des ressources ou encore la maintenance prédictive, ces données synthétiques seront de plus en plus précises, tout en étant respectueuses de la vie privée de l'utilisateur final. »

À propos de Fortinet

Fortinet, acteur majeur de la cybersécurité, contribue activement à faire converger réseau et sécurité. La mission de Fortinet est de protéger les utilisateurs, les dispositifs et les données, où qu'ils soient. Aujourd'hui, Fortinet déploie une cybersécurité sur le périmètre de choix du client, grâce à une offre de plus de 50 produits professionnels. Plus d'un demi-million de clients font confiance aux solutions de Fortinet, des solutions déployées à grande échelle, bénéficiant de multiples brevets et reconnues par le marché. Fortinet Training Institutepropose un programme de formation particulièrement riche en matière de cybersécurité à l'intention de tous, et notamment de celles et ceux qui souhaitent s'orienter vers les métiers de la cybersécurité. Fortinet collabore avec des organismes reconnus (CERT, instances gouvernementales et institutions de l'enseignement), s'ancrant fortement dans l'engagement de Fortinet à renforcer la résilience cyber à l'échelle mondiale. FortiGuard Labs, la division de Fortinet dédiée à la veille et aux études sur les menaces, conçoit et utilise des technologies IA et de Machine Learning performantes pour apporter aux clients une protection optimale et une veille décisionnelle sur les menaces. Pour en savoir plus, consultez le site https://www.fortinet.com/fr, le blog Fortinetou Fortiguard Labs.