Pourquoi l'intelligence artificielle est plus efficace contre les cyberattaques

Le mérite de l'intelligence artificielle en cybersécurité est de détecter les cyberattaques que les autres systèmes de protection ne voient pas. Cela comprend, bien entendu, les cyber-attaques inédites qui exploitent une faille dont personne n'avait connaissance jusqu'alors et que l'on appelle « zero-day ». Mais sur le terrain, nous observons que l'intelligence artificielle neutralise la plupart du temps des menaces qui existent en réalité depuis plus d'un an et contre lesquelles aucune contre-mesure n'a été déployée.

Les failles les plus fréquentes ne sont en effet pas celles qui tardent à être découvertes, mais celles qui demeurent. Soit par négligence, soit parce qu'elles existent sur des machines que l'on n'ose pas toucher, de peur qu'elles ne fonctionnent plus correctement après une mise à jour. A la décharge de nombreuses entreprises, les systèmes qui nécessitent des patches de sécurité sont souvent des configurations orphelines, dont le fournisseur a disparu. Nous dénombrons ainsi une quantité inquiétante de machines-outils chez les industriels qui sont pilotées par de vieux Windows que plus personne ne supporte.

L'intelligence artificielle n'a pas vocation à patcher ces systèmes, ni même à s'installer dessus pour les protéger, car il n'y a rien de plus facilement contournable qu'un antivirus qui fonctionne depuis une machine ciblée par des pirates. Au contraire, une bonne protection par intelligence artificielle opère depuis un point central du réseau pour analyser les flux qui passent et tirer le signal d'alarme quand elle repère un comportement malveillant contre une cible.

La reconnaissance des attaques d'après leur signature ne fonctionne plus

L'intelligence artificielle est plus efficace que les systèmes anti-intrusions habituels pour trois raisons :

La première est que les capacités de détection des attaques des systèmes traditionnels reposent sur une base de signatures connues. Problème, il est de plus en plus rare de devoir affronter des menaces dont la signature est inconnue, car les cyber-assaillants ne sont plus de simples hackers armés du code malveillant qu'ils ont mis au point. Désormais, l'écosystème des cybercriminels s'est organisé à la manière d'une place de marché : des groupes publient des exploits, d'autres des logiciels pour mettre en oeuvre ces exploits, des plateformes tierces les commercialisent et chacun propose des mises à jour régulières, voire des variations ponctuelles qui renouvellent sans cesse la signature de l'attaque.

Le risque de subir une attaque que l'on n'a pas encore référencée est donc de plus en plus grand. L'intelligence artificielle, au contraire, ne cherche pas d'empreinte dans les paquets qui véhiculent l'attaque, elle analyse plutôt comment ces paquets sont agencés et, dans ce cas, les schémas n'évoluent pas : il s'agit toujours pour le cyberassaillant d'accéder à quelque chose de précis (une base de données, par exemple), avec des points de progression déterminés.

Le second problème, qui découle du précédent, est que les systèmes traditionnels doivent analyser un nombre de signatures qui ne cesse de croître. Ils sont par conséquent susceptibles de dégrader les performances du SI à protéger. A titre d'exemple, une base Open source d'un éditeur de sécurité peut proposer de comparer chaque paquet entrant à plus de 50.000 signatures, alors qu'une solution basée sur l'intelligence artificielle peut n'avoir pas plus d'une cinquantaine de comportements-type à identifier. Cette considération est très importante lorsqu'il s'agit de protéger des réseaux qui véhiculent 40, 80 ou 100 Gbits/s et sur lesquels une chute de la bande passante se traduirait par des pertes financières. Par exemple chez les opérateurs télécoms ou d'énergie.

Le troisième problème, enfin, est que les cyberattaques réussissent dans la grande majorité des cas, non pas grâce à un malware qu'un firewall aurait pu stopper, mais parce que le cyber-assaillant a contourné le firewall : il a trompé la vigilance d'un utilisateur avec un phishing, ou, par exemple chez les industriels, avec une clé USB. Et une fois infiltré sur un réseau, le pirate utilise aujourd'hui des outils tout à fait légitimes. Ce sont typiquement ceux des systèmes ciblés, qui ne déclenchent aucune alarme, mais qui servent pourtant à obtenir des privilèges. Ici, les dispositifs de protection classiques sont impuissants car ils n'ont rien à évaluer. L'intelligence artificielle, en revanche, va détecter l'attaque car elle observe l'utilisation des comptes utilisateurs.

Le Deep Learning pour éliminer les faux positifs

Il convient néanmoins de préciser que le défi technique ici est de discerner une attaque véritable parmi une quantité colossale d'informations. Il existe ainsi des outils qui s'avèrent inefficaces car ils analysent les comportements des utilisateurs sans pour autant reposer sur un moteur de Deep Learning. A l'épreuve, ces outils sont désinstallés au bout d'un certain temps car ils produisent trop de faux positifs qui mobilisent les équipes de sécurité en vain.

Le machine Learning consiste à simplement apprendre les schémas comportementaux d'une attaque, tandis que les Deep Learning va plus loin en pondérant les observations avec des éléments de connaissance extérieurs. La force d'une solution reposant sur l'IA et sécurisant le SI avec du Deep Learning, est que les entreprises protégées acceptent la plupart du temps de partager leurs informations pour enrichir les algorithmes. Grâce à ce modèle « collaboratif » une simple particularité chez quelqu'un permettrait de résoudre des problèmes chez nombre d'autres clients quand elle était partout prise en compte. A l'inverse, cette base de connaissance supplémentaire permet de mieux entraîner l'intelligence artificielle pour qu'elle sache éliminer toute seule les faux positifs.

Bien entendu, la télémétrie issue des clients n'est possible que moyennant un accord de partenariat. Même si les données prélevées sont anonymisées, leur usage est encadré par des dispositions légales. Mais la pratique ne pose aucun risque et elle est de plus en plus courante.