Vectra AI met le Machine Learning au service de la détection des menaces sur le réseau

Retour aux sources pour Christophe Jolly. L'ex-directeur de la sécurité en France de Cisco, qui avait intégré le géant américain suite au rachat de SourceFire pour lequel il était directeur des ventes en Europe, revient à la détection des activités malveillantes sur le réseau en prenant la tête en France de Vectra AI, ex-Vectra Networks, une start-up américaine. S'il s'agit bien comme chez SourceFire de détecter les événements suspects au sein du trafic réseau, la solution de Vectra mise sur l'intelligence artificielle pour effectuer le tri. « *L'IA est capable de réaliser des choses que nous n'étions pas en mesure de réaliser auparavant. Le tout en proposant une solution d'un moindre niveau de complexité aux utilisateurs* », assure Christophe Jolly. Bref, la promesse de davantage de pertinence dans une interface utilisateurs simplifiée. « *Avec des solutions classiques, le travail de réconciliation des événements nécessite trop d'opérateurs humains alors qu'on parle ici de tâches répétitives et fastidieuses. Le travail d'un SOC consiste à qualifier et traiter les attaques contre une organisation, pas à faire de la corrélation d'événements !* », ajoute Christophe Jolly.

WannaCry et NotPetya pour campagnes marketing

Sous la houlette de Gérard Bauer, un ancien de Riverbed devenu il y a deux ans vice-président EMEA de Vectra, l'ex-cadre de Cisco est en train de monter l'activité française de cette start-up née en 2012 et employant aujourd'hui quelques 150 personnes. « *Déjà, l'intérêt pour notre solution est énorme* », assure-t-il. Il est vrai que les crises sécuritaires WannaCry puis NotPetya sont passées par là. Des crises où la rapidité de réaction des entreprises confrontées à ces menaces s'est avérée essentielle. « *Or, l'objectif de notre solution est précisément de réduire le délai de détection en indiquant aux opérateurs du SOC les machines déjà corrompues* », indique Christophe Jolly.

Plutôt que de faire tourner son IA sur la console qui centralise les logs du réseau – « *approche qui manque de souplesse et qui implique de convaincre les différents départements de l'entreprise d'envoyer le bon niveau d'information* » -, Vectra AI se base sur des sondes déployées sur le réseau, sondes qui renvoient leurs données vers un point central, un serveur maison conçu pour les calculs

massivement parallèles où tournent les algorithmes de Machine Learning de Vectra. La facturation est fonction du nombre d'adresses IP sur le réseau et de la durée d'abonnement à la solution.

Vectra mise sur l'apprentissage supervisé

Si la technologie de Vectra rappelle celle de Darktrace, start-up britannique montée par l'ancien patron d'Autonomy et qui a levé récemment 75 M$, sa philosophie en est différente, selon Christophe Jolly. « L*'apprentissage non supervisé, la voie choisie par ce concurrent, implique de bâtir des gabarits pour diminuer le taux de faux positifs. Or, c'est très complexe et cela demande beaucoup d'interventions humaines dans des contextes de grandes entreprises* », assure le nouveau DG France de Vectra AI. A l'inverse, la solution de ce dernier repose à 80 % sur des approches supervisées, avec des algorithmes entraînés par les équipes de l'éditeur sur les comportements types des assaillants, ceux qu'ils seront, à un moment ou un autre, forcés d'adopter pour activer leur menace.

« *Au total, 55 familles de comportements sont ainsi proposées avec l'outil et nous en ajoutons environ une nouvelle chaque mois*, détaille Christophe Jolly. *Notre R&D regroupe tant des mathématiciens chargés d'entraîner les réseaux de neurones que des hackers qui jouent des scénarios d'attaque face à ces IA.* » S'y ajoute le trafic fourni par 120 clients de la start-up qui vient nourrir les algorithmes. Pour améliorer sa solution, Vectra AI travaille aujourd'hui à l'intégration de sources externes de données sur les menaces (comme les données STIX, un langage structuré de threat intelligence), mais aussi à l'identification de campagnes malveillantes, caractérisées par toute une série d'événements différents sur le réseau.

A lire aussi :

Threat intelligence : les entreprises craignent l'indigestion de données

ThreatQuotient livre une bibliothèque universitaire automatisée des menaces

Apave traque les malwares et les ransomwares avec Darktrace