Darktrace : le Machine Learning au service de la sécurité

Darktrace est le nouveau bébé de **Mike Lynch**, l'**ex-Pdg d'Autonomy**, éditeur britannique vendu quelque 11 milliards de dollars à HP. Rappelons que cet entrepreneur britannique, qui a monté un fonds d'investissement appelé Invoke Capital, est toujours en litige avec le groupe américain, ce dernier l'accusant d'avoir truqué les comptes d'Autonomy pour le vendre au meilleur prix.

Fruit de recherches de l'université de Cambridge sur de **nouvelles applications des mathématiques bayésiennes**, Darktrace a vu le jour en 2013 en Grande-Bretagne, grâce aux 20 millions de dollars injectés par Invoke. La société vient également de **s'implanter en France**, où la filiale est dirigée par **Emmanuel Meriot**, autre ancien d'Autonomy où il était directeur Europe du Sud.

Le principe de la solution Darktrace ? Installer au sein de l'entreprise un système auto-apprenant capable de détecter les comportements anormaux sur le réseau. « ***Nous ne modélisons pas les attaques****, car nous considérons que c'est impossible du fait de l'inventivité des assaillants. Tout comme nous ne modélisons pas les comportements normaux des utilisateurs de l'entreprise, c'est le système lui-même qui les établit* », explique Julien Fistre, spécialiste technique de la solution et lui aussi issu d'Autonomy. « *Nous n'avons pas l'ambition de dire que l'infiltration n'aura pas lieu. Nous cherchons plutôt à détecter les mouvements latéraux des assaillants et à en alerter les entreprises* », ajoute-t-il. La solution vise donc avant tout à détecter les conséquences d'une attaque (comme une APT) mais également la malveillance interne.

Le cœur du système : un modèle « boîte noire »

Ce système de détection basé sur du Machine Learning et reposant sur un modèle probabiliste scanne les machines, les réseaux et les usages des employés, via l'installation d'une **appliance en cœur de réseau.** Ce point de collecte central peut être suppléé par d'autres scanners répartis en d'autres points du réseau. Sans aller jusqu'à du déchiffrement de flux, Darktrace analyse les en-têtes des protocoles de communication. Ces logs sont agrégés dans **une interface 3D originale** (voir ci-dessus) servant à la fois à surveiller le réseau et à mener de premières investigations quand une alerte se déclenche. Signalons que les analyses issues de Darktrace peuvent aussi être intégrées à un SIEM (security information and event management, console de gestion et de corrélation des logs).

Si le cœur du système – le modèle mathématique – n'est **pas configurable** (on peut simplement le réinitialiser en cas de modification structurelle du réseau par exemple), la solution peut être adaptée ou alimentée en informations pour accélérer l'apprentissage. En restreignant la zone scannée (ne serait-ce que pour limiter le coût de la solution), en précisant la typologie des machines du réseau (via un export Active Directory par exemple), en configurant les rôles des employés et les niveaux d'alerte associés. Un moyen d'isoler par exemple des populations à risque, soit en raison des données qu'elles manipulent, soit en raison des usages afférents à leur métier (commerciaux sur le terrain par exemple). Les administrateurs de Darktrace influencent toutefois le modèle

lorsque, après analyse, ils acquittent une alerte, le système interprétant alors cette action comme un signal pour descendre le niveau de cet événement.

Une cartographie du réseau

« *Pour convaincre les entreprises de la pertinence de notre modèle, nous installons gratuitement notre appliance sur leur réseau pour un mois* », explique Emmanuel Meriot. Qui affirme que, par ce biais, plus de 90 % des testeurs se transforment en clients. Selon le dirigeant, la société compte **une cinquantaine de clients dans le monde** (dont Virgin Train ou l'énergéticien britannique Drax). Trois sociétés françaises testeraient en ce moment la solution. « *Et d'autres vont suivre*, assure Emmanuel Meriot. *Le premier bénéfice pour les clients est immédiat : ils savent enfin précisément quels équipements sont présents sur leur réseau. Or, pour patcher de façon exhaustive une faille comme ShellShock par exemple, avoir une cartographie précise du réseau est indispensable. Le second avantage que décèlent les entreprises, c'est qu'avec un seul outil, elles sont désormais en mesure d'isoler des attaques qu'elles détectaient auparavant avec un assemblage d'une dizaine d'outils.* »

A lire aussi :
5 questions pour comprendre le déchiffrement SSL
Une cyberattaque peut-elle paralyser une nation d'ici 2025 ?