Watson d'IBM, prochain Sherlock Holmes de la cybersécurité

Watson, l'outil d'informatique cognitif d'IBM, s'est essayé à nombre de métiers, docteur, agent immobilier, consultant météo ou encore conseiller bancaire. Il vient d'ajouter une corde à son arc : expert en cybersécurité. IBM vient de lancer en version beta un service dédié à ce domaine. Une quarantaine d'organisations vont s'appuyer sur le superordinateur de Big Blue pour détecter et bloquer les cybermenaces. On peut citer entre autres Sun Life Financial, le Centre Universitaire medical de Rochester, Avnet, SCANA Corporation, Sumitomo Mitsui Banking Corporation, l'école polytechnique de l'Etat de Californie, l'Université du New Brunswick et Smarttech.

Il y a quelques mois, David Kenny, responsable de la division Watson, avait évoqué les futures compétences de l'ordinateur cognitif et notamment la cybersécurité. Il était encore tôt pour en parler nous assurait le dirigeant. Les équipes d'IBM étaient déjà sur le pied de guerre, car pour utiliser Watson il faut le nourrir d'une grande quantité de données. Elles ont injecté à l'automne dernier plus de 15 000 documents par mois relatifs à la sécurité informatique. L'objectif est que le superordinateur soit capable de contextualiser les informations en combinant des données structurées comme des évènements de sécurité, et des données non structurées comme des livres blancs, des travaux de recherche et des articles de blog.

Un apprentissage pas à pas à la cybersécurité

Nos confrères de *Wired* rapportent une anecdote sur l'intérêt de la contextualisation avec le terme ransomware. Pour Watson, les premiers éléments lui ont fait comprendre que ce mot se rapprochait de « Ransom », nom porté par plusieurs villes. Il pensait donc que les requêtes étaient liées à un endroit. L'équipe de chercheurs a donc entré une définition de rançongiciel et Watson a immédiatement connecté les requêtes avec la cybersécurité.

Mais IBM avertit que la version beta du service de cybersécurité ne va pas transformer Watson en Sherlock Holmes. « *Dans un projet de développement continu, vous réalisez une matrice de test et vous analysez comment l'ordinateur passe ce test* », explique Caleb Barlow, vice-président de la division sécurité d'IBM. Et d'ajouter : « *Cela ressemble à l'apprentissage humain, il y a des choses qu'il est capable de faire à l'école primaire, au collège et au niveau professionnel. Watson va suivre ce même chemin.* » Il va dans un premier temps apprendre le langage propre à la sécurité informatique. Ce dernier est différent en fonction des secteurs, santé, industrie, etc. Watson va donc fournir des rapports et des recommandations aux différentes organisations citées précédemment. Il est capable d'identifier si un événement de sécurité est associé à des malwares connus, rappeler l'expérience liée à ces menaces et repérer les comportements suspects.

Watson ne prétend pas être le *deus ex machina* pour lutter contre les cybercriminels, mais il peut aider dans l'analyse des évènements de sécurité. En moyenne, une équipe traite jusqu'à 200 000 évènements significatifs par jour. Un petit coup de pouce non négligeable.

A lire aussi :

Le projet Intu d'IBM invite Watson sur les smartphones et l'IoT
Nicolas Sekkaki, IBM : « Watson entraîne toute notre activité »

Photo credit: gregwake via VisualHunt / CC BY-NC-SA