Communiqués de presse

IBM Watson pour lutter contre la cybercriminalité

Huit universités de premier plan aident Watson à se former à la cybersécurité

Paris - 10 mai 2016: Suite à un projet de recherche initié il y a un an, la division sécurité d'IBM (NYSE: IBM) lance **Watson for Cyber Security**, une nouvelle version cloud de l'intelligence artificielle formée au langage lié à la sécurité. Pour optimiser le système, IBM collaborera avec huit universités afin d'élargir considérablement les données de sécurité utilisées pour former le système cognitif.

La formation de Watson for Cyber Security est une étape critique dans les progrès liés à la sécurité cognitive. Watson apprend les nuances des résultats issus de la recherche en matière de sécurité, découvre des modèles et des preuves des cyber-attaques ainsi que des menaces qui n'auraient pas été identifiées autrement. Dès cet automne, IBM travaillera avec les universités suivantes ainsi que leurs étudiants afin de renforcer la formation de Watson au langage lié à la cybersécurité : California State Polytechnic University, Pomona; Pennsylvania State University; Massachusetts Institute of Technology; New York University; the University of Maryland, Baltimore County (UMBC); the University of New Brunswick; the University of Ottawa et the University of Waterloo.

Cette annonce fait partie d'un projet pionnier lié à la sécurité cognitive pour combler le déficit de compétences en matière de cybersécurité. Les efforts d'IBM sont destinés à améliorer les compétences des analystes en sécurité qui utilisent des systèmes cognitifs permettant d'automatiser les connexions entre les données, les menaces émergentes et les stratégies de remédiation des menaces. IBM a l'intention de commencer les déploiements de production en mode bêta dès cette année pour tirer partie d'IBM Watson for Cyber Security.

La bibliothèque de recherche de renommée mondiale IBM X-Force constituera le noyau dur d'IBM Watson for Cyber Security. Cet ensemble de connaissances comprend 20 années de recherche en matière de sécurité, des informations sur 8 millions de spams et d'attaques de phishing ainsi que plus de 100.000 vulnérabilités documentées.

Watson pour combler le déficit de compétences liées à la sécurité

Le volume des données de sécurité présenté aux analystes est stupéfiant. Une entreprise standard a plus de 200.000 données liées à des événements de sécurité par jour1, les entreprises dépensent 1,3 million de dollars par an pour traiter uniquement les

faux positifs gaspillant ainsi près de 21.000 heures2. Si l'on couple cela avec plus de 75.000 vulnérabilités logicielles connues rapportées dans la base de données nationale de la vulnérabilité3, 10.000 documents de recherche liés à la sécurité publiés chaque année et plus de 60.000 billets de blogs de sécurité publiés chaque mois 4 - les analystes en sécurité sont sérieusement défiés pour suivre ce flot d'information.

Conçu sur le cloud d'IBM, Watson for Cyber Security sera la première technologie à offrir la connaissance des données de sécurité à cette échelle en utilisant la capacité de Watson pour raisonner et apprendre des "données non structurées" – soit 80 % de toutes les données de l'internet que les outils de sécurité traditionnels ne peuvent pas traiter, y compris des blogs, des articles, des vidéos, des rapports, des alertes et d'autres informations. En fait, l'analyse d'IBM a constaté que l'entreprise standard exploite seulement 8 % de ces données non structurées. Watson for Cyber Security utilise également le traitement du langage naturel pour comprendre la nature vague et imprécise du langage humain dans les données non structurées.

En conséquence, Watson for Cyber Security est conçu pour fournir des indications sur les menaces émergentes, ainsi que des recommandations sur la façon de les arrêter, en augmentant la vitesse d'analyse et les capacités des professionnels de la sécurité. IBM intégrera également d'autres capacités de Watson y compris les techniques d'exploration des données, les outils et techniques de présentations graphiques pour trouver des connections entre les points de données connexes dans différents documents. Par exemple, Watson peut trouver des données sur une nouvelle forme de logiciel malveillant dans un bulletin de sécurité ainsi que des données sur le blog d'un analyste de la sécurité concernant une nouvelle stratégie de remédiation.

« Même si l'industrie était en mesure de combler les 1,5 millions d'emplois vacants en matière de cybersécurité que l'on estime d'ici 2020, nous subirions encore une crise des compétences en matière de sécurité », **déclare Marc van Zadelhoff, General Manager, IBM Security**. *« Le volume et la vélocité du flux des données en matière de sécurité est l'un de nos plus grands défis dans le traitement de la cybercriminalité. En tirant parti de la capacité de Watson à apporter un contexte pour traiter des quantités énormes de données non structurées, qu'il est impossible de traiter seul, nous allons apporter de nouvelles idées, des recommandations et des connaissances aux professionnels de la sécurité, ce qui offrira une plus grande précision et vitesse d'analyse aux analystes en cybersécurité les plus avancés, et fournira aux analystes novices une formation sur le tas ».*

Des universités pour aider à entrainer IBM Watson for Cyber Security

IBM prévoit de collaborer avec huit universités qui bénéficient des meilleurs programmes de cybersécurité au monde pour renforcer la formation de Watson et initier leurs élèves à l'informatique cognitive. Les universités sont : California State Polytechnic University, Pomona; Pennsylvania State University; Massachusetts Institute of Technology; New York University; UMBC; the University of New Brunswick; the University of Ottawa et the University of Waterloo.

Les élèves aideront à former Watson au langage de la cybersécurité, travaillant d'abord pour aider à construire le corpus de Watson avec des connaissances en annotant et nourrissant les rapports et les données de sécurité du système. Comme les étudiants travaillent étroitement avec des experts en sécurité IBM pour apprendre les nuances de ces rapports de renseignements de sécurité, ils vont aussi être parmi les premiers au monde à acquérir de l'expérience pratique dans ce domaine émergent de la sécurité cognitive. Ce travail se fondera sur le travail d'IBM dans le développement et la formation à Watson for Cybersecurity. IBM prévoit actuellement de traiter jusqu'à 15.000 documents de sécurité par mois au cours de la prochaine phase en collaborant avec les partenaires universitaires, des clients et des experts IBM.

Ces documents comprennent des rapports de renseignements sur les menaces, des stratégies des cybercriminels et des bases de données des menaces. La formation de Watson aidera également à renforcer la taxonomie dans la cybersécurité, y compris la compréhension des identités numériques, les méthodes d'infection, les indicateurs de compromission et aidera à identifier les menaces persistantes avancées.

Dans un autre effort pour de nouvelles avancées scientifiques en matière de sécurité cognitive, UMBC a également annoncé aujourd'hui une collaboration de plusieurs années avec IBM Research pour créer un laboratoire de la cybersécurité cognitive accélérée (ACCL) dans le College of Engineering and Information Technology. La faculté et les étudiants travaillant dans le ACCL appliqueront l'informatique cognitive aux défis complexes de la cybersécurité, collaborant avec les scientifiques d'IBM et tirant parti des systèmes informatiques de pointe d'IBM pour aller plus vite et plus loin avec de nouvelles solutions de cybersécurité.

«Cette collaboration permettra à nos étudiants et à l'université de travailler avec IBM pour faire progresser l'état de l'art en matière d'informatique cognitive et de cybersécurité », **a déclaré Anupam Joshi, director of UMBC's Center for Cybersecurity and chair of computer science and electrical engineering, à UMBC**, qui dirigera l'ACCL à UMBC.

Pour plus d'informations sur l'annonce d'aujourd'hui et la sécurité cognitive:www.ibm.com/security/cognitive. Poursuivez la conversation sur @IBMSecurity#CognitiveSecurity

[1] IBM 2015 Cybersecurity Intelligence Index

[1] The Cost of Malware Containment, par Ponemon Institute, publié en janvier 2015

[1] The National Vulnerability Database

[1] IBM X-Force Analysis

A propos d'IBM Security

IBM Security propose un portefeuille de solutions de sécurité pour les entreprises parmi les plus avancés et les plus intégrés. Ce portefeuille est supporté par IBM X-Force, organisation de recherche connue mondialement et permet aux organisations de gérer efficacement les risques et de se défendre contre les menaces émergentes. IBM dispose d'une organisation de recherche et développement et de mise en œuvre parmi les plus importantes au monde, gère 20 milliards d'événements de sécurité par jour dans plus de 130 pays et possède plus de 3000 brevets de sécurité.

Pour plus d'informations : www.ibm.com/security/fr/fr

Blog US : www.securityintelligence.com

Suivez notre actualité sur Twitter @IBMSecurityFR

###