Communiqués de presse

IBM Watson for Cyber Security : lancement de la version bêta avec 40 clients dans le monde

Les systèmes cognitifs sont cités comme une nouvelle priorité par quasiment 60% des professionnels de la sécurité

Paris - 06 déc. 2016: L'entité sécurité d'IBM annonce ce jour que des leaders mondiaux dans la banque, la santé, l'éducation et d'autres industries clefs ont rejoint le programme pilote d'IBM Watson for Cyber Security. Ces 40 organisations vont tester les capacités de Watson à les assister dans leur combat contre les cybercriminels.

L'environnement actuel de la sécurité nécessite davantage de renseignements pour identifier et prioriser les menaces, conduisant à une augmentation de la charge de travail des analystes avec plus d'alertes et d'anomalies à gérer qu'il n'y en a jamais eu. Watson for Cyber Security utilise des technologies intelligentes comme le "machine learning" et le traitement du langage naturel, pour aider les analystes de sécurité à prendre plus rapidement de meilleures décisions, dans le cadre de la défense d'une organisation, en les basant sur des données structurées et sur un volume massif de données non-structurées qui étaient inutilisables jusqu'à présent. Cette solution bénéficie de la technologie cognitive d'IBM, leader en la matière, qui a été formée à comprendre le langage spécifique de la sécurité[1].

Une étude récente de l'IBM Institute for Business Value montre que quasiment 60% des professionnels de la sécurité considèrent que l'émergence des technologies cognitives a joué un rôle critique dans l'inversion des tendances concernant la lutte contre les cybercriminels.

"*Les clients en sont aux prémices de l'implémentation des technologies cognitives*" a déclaré**Sandy Bird, Chief Technology Officer, IBM Security**. "*Nos études laissent penser que cette adoption va tripler en volume durant les trois prochaines années, avec des outils comme Watson for Cybersecurity qui vont s'affiner et se généraliser dans les SOCs (security operations centers). Actuellement, seulement 7% des organisations déclarent utiliser des solutions cognitives.*"

Lancement du programme bêta d'IBM Watson for Cyber Security

Des organisations du Fortune 500 de différents secteurs comme la finance, le transport, l'énergie, l'automobile ou l'éducation travaillent actuellement avec Watson for Cybersecurity, affinant ses capacités en cybersécurité avec des pilotes basés sur des cas du monde réel.

Ces 40 clients bêta utilisent Watson dans leur propre environnement de sécurité afin d'ajouter du contexte à leurs données de cybersécurité, avec de nouveaux cas d'utilisation tels que :

- Déterminer si une attaque est liée ou non à un logiciel malveillant ou une campagne d'attaques connue. Dans ce cas, Watson apportera entre autres, les informations sur le logiciel malveillant utilisé, les vulnérabilités exploitées, l'étendue des menaces.
- Mieux identifier les comportements suspects. Watson élargira le contexte étudié pour les activités des utilisateurs permettant d'être plus précis pour déterminer si une activité est malveillante ou non.

Travaillant avec ces clients bêta, IBM continu à améliorer la compréhension des données de sécurité par Watson et à affiner la manière dont celui-ci peut s'intégrer quotidiennement dans les opérations de sécurité.

Une étude montre que la sécurité cognitive est en progression

IBM Institute for Business Value a interrogé récemment plus de 700 professionnels de la sécurité pour évaluer les perspectives sur les défis, les bénéfices et les opportunités des technologies cognitives pour la sécurité.

Presque 60% des sondés sont convaincus que les technologies cognitives seront rapidement assez matures pour diminuer significativement les cyber-attaques dans un futur proche. Alors que seulement 7% disent que leur organisation est en train d'implémenter une solution cognitive pour la sécurité, 21% déclarent qu'ils vont en mettre une en œuvre dans les 2 à 3 ans qui viennent, soit un triplement de l'adoption.

Les professionnels de la sécurité ont aussi souligné, pour 40% d'entre eux, que le principal bénéfice qu'ils attendent des technologies cognitives est l'amélioration de la prise de décision pour la détection et la réponse aux incidents de sécurité. Actuellement, une organisation met en moyenne 201 jours pour identifier une fuite de données et 70 jours pour la contenir[2]. Les professionnels de la sécurité s'attendent à ce que le cognitif apporte beaucoup à la réduction de ces délais grâce à de meilleures informations et des prises de décisions plus rapides.

Le rapport complet est disponible ici : ibm.biz/cyberimmunity

Etendre le cognitif et les renseignements dans le portefeuille des offres IBM Sécurité

Alors que le développement de Watson for Cybersecurity continue, IBM rajoute des capacités cognitives et

analytiques avancées dans d'autres parties de son portefeuille d'offres de sécurité :

- Appliquer de l'analyse comportementale pour mieux comprendre les usages et comportements de l'interne - employés, sous-traitants et partenaires – afin de déterminer si leurs identifiants ont été compromis grâce à IBM QRadar User Behavior Analytics.
- Utiliser des analyses brevetées, du machine learning et des capacités biométriques comportementales pour empêcher la fraude bancaire avec IBM Trusteer Pinpoint Detect, qui analyse la façon dont les utilisateurs interagissent avec les sites bancaires, créant des modèles gestuels qui deviennent de plus en plus pertinents avec le temps.
- Utiliser le "machine learning" pour aider les clients à trouver plus rapidement des vulnérabilités potentielles dans les applications avec IBM Security AppScan
- Aider les clients à détecter les failles et à y remédier avant qu'elles ne soient utilisées, grâce à de nouvelles capacités de détection des anomalies pour l'ensemble de leurs données avec IBM Security Guardium
- Recruter 2 000 experts du domaine de la sécurité, développeurs, consultants et chercheurs, dont 600 aux Etats-Unis, au court des deux dernières années.

A propos de la division sécurité d'IBM

La division sécurité d'IBM 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 35 milliards d'événements de sécurité par jour dans plus de 130 pays et possède plus de 3 000 brevets de sécurité.

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

Blog US : www.securityintelligence.com

Suivez notre actualité sur Twitter @IBMSecurityFR

Avertissement : Les déclarations d'IBM concernant ses plans, orientations et intentions sont sujettes à modification ou retrait sans préavis à la seule discrétion d'IBM. Les informations sur les produits futurs potentiels sont destinées à décrire l'orientation générale de la stratégie produit d'IBM et ne doivent pas être prises en compte pour prendre une décision d'achat. Les informations mentionnées sur les produits futurs potentiels ne créent pas d'engagement, promesse ou obligation juridique de fournir un quelconque produit, code ou fonctionnalité. Les informations sur les produits potentiels futurs ne peuvent être incorporées dans un contrat. Le développement, la mise sur le marché ou le calendrier associé à des caractéristiques ou fonctionnalités futures décrites pour nos produits restent à notre seule discrétion.

[1] IBM Institute of Business Value Study: Cybersecurity in the Cognitive Era

[2] IBM / Ponemon Cost of a Data Breach study, 2016