Communiqués de presse

IBM Watson for Cyber Security alimente les centres d'opérations de sécurité cognitifs

Plus de 40 entreprises dans une douzaine de secteurs exploitent la technologie de sécurité Watson
Les nouvelles innovations comprennent un assistant virtuel conçu avec Watson et un projet de recherche concernant un assistant vocal de sécurité

CAMBRIDGE, MA - 13 févr. 2017: La division Sécurité d'IBM (NYSE: IBM) a annoncé aujourd'hui la disponibilité de Watson for Cyber Security, la première technologie d'intelligence augmentée du secteur conçue pour les centres d'opérations de sécurité cognitifs (SOCs). Au cours de l'année dernière, Watson a été formé au langage de la cybersécurité, en ingérant plus d'1 million de documents de sécurité. Watson peut désormais aider les analystes en sécurité à analyser des milliers de rapports de recherche en langage naturel qui n'avaient jamais été accessibles auparavant aux outils de sécurité modernes.

Selon l'entité de recherche d'IBM, les équipes de sécurité passent au crible plus de 200 000 événements de sécurité par jour en moyenne, conduisant à plus de 20 000 heures par an gaspillées à chasser des faux positifs.[1] La nécessité d'introduire des technologies cognitives dans les centres d'opérations de sécurité sera essentielle pour faire face au doublement attendu des incidents de sécurité au cours des cinq prochaines années et à une réglementation accrue à l'échelle mondiale.[2]

Watson for Cyber Security sera intégré à la nouvelle plateforme de SOC cognitif d'IBM, réunissant des technologies cognitives avancées et des opérations de sécurité, fournissant la capacité de répondre aux menaces à travers les périphériques, le réseau, les utilisateurs et le Cloud. La pièce maîtresse de cette plateforme est IBM QRadar Advisor with Watson, le premier outil qui exploite le corpus de connaissances en cybersécurité de Watson. Cette nouvelle application est déjà utilisée par Avnet, l'Université du New Brunswick, Sopra Stéria et 40 autres clients dans le monde pour augmenter les investigations des analystes en sécurité sur les incidents de sécurité.

IBM a également investi dans la recherche pour ajouter des outils cognitifs à son réseau mondial X-Force Command Center, dont un assistant virtuel conçu avec Watson actuellement utilisé pour interagir avec les clients d'IBM bénéficiant de services de sécurité managés. IBM a également annoncé un nouveau projet de recherche novateur, ayant pour nom de code Havyn, qui consiste en un assistant vocal de sécurité qui exploite la technologie de conversation de Watson pour répondre aux commandes verbales et au langage naturel des analystes en sécurité.

"Les menaces de cybersécurité sophistiquées actuelles s'attaquent à de multiples fronts pour dissimuler leurs activités et nos analystes en sécurité sont confrontés à la tâche difficile de localiser ces attaques au sein d'un océan de données liées à la sécurité", déclare Sean Valcamp, Responsable de la sécurité des systèmes d'information d'Avnet. *"Watson rend les efforts de dissimulation plus difficiles en analysant rapidement de multiples flux de données et en les comparant avec les dernières informations relatives aux attaques de sécurité pour fournir une image plus complète de la menace. Watson génère également des rapports sur ces menaces en quelques minutes, ce qui accélère considérablement le temps entre la détection d'un événement potentiel et la capacité de mon équipe de sécurité à réagir en conséquence. »*

Le SOC cognitif d'IBM

Au fur et à mesure que les équipes de sécurité font évoluer leurs stratégies et leurs tactiques pour déjouer les cybercriminels, l'introduction de technologies cognitives dans les centres d'opérations de sécurité actuels sera essentielle pour maintenir le rythme. Une récente étude IBM a révélé que seulement 7 % des professionnels de la sécurité utilisent des outils cognitifs aujourd'hui, mais cette l'utilisation devrait tripler au cours des 2-3 prochaines années.[3]

La plateforme de SOC cognitif d'IBM place les technologies cognitives dans les mains des analystes en sécurité, améliorant ainsi leur capacité à combler les lacunes en matière de renseignement et à agir avec rapidité et précision. L'application IBM QRadar Advisor with Watson apporte des capacités cognitives pour aider les analystes en sécurité dans leurs investigations et la remédiation via la plateforme de renseignements de sécurité QRadar d'IBM. La solution aide dans l'analyse de menaces potentielles en corrélant les capacités de Watson en matière de traitement du langage naturel à travers les blogs de sécurité, les sites Internet, les documents de recherche et d'autres sources, avec les renseignements sur les menaces et les données d'incidents de sécurité de QRadar, ce qui peut raccourcir les analyses en matière de cybersécurité de quelques semaines ou jours à quelques minutes.

"Le SOC cognitif est désormais une réalité pour les clients qui cherchent à garder un avantage contre les légions croissantes de cybercriminels et les menaces de nouvelle génération", **a déclaré Denis Kennelly, vice-président du développement et de la technologie, IBM Security**. *« Nos investissements dans Watson for Cybersecurity ont donné naissance à plusieurs innovations en un peu moins d'un an. Combiner les capacités uniques de l'intelligence de l'homme et de la machine sera crucial pour la prochaine étape dans la lutte contre la cybercriminalité avancée ».*

Pour étendre la capacité du SOC cognitif aux périphériques, la division sécurité d'IBM annonce également une nouvelle solution de détection et de réponse (EDR : endpoint detection and response) appelée IBM BigFix Detect. La solution permet aux entreprises d'obtenir une visibilité complète sur le parc des périphériques en constante évolution tout en comblant l'écart entre la détection de comportements malveillants et la remédiation. BigFix Detect rend l'EDR accessible et exploitable, permettant aux analystes en sécurité de voir, de comprendre et d'agir sur les menaces à travers leurs périphériques via une seule plateforme et fournit une remédiation ciblée en quelques minutes sur les périphériques affectés à l'échelle de l'entreprise.

S'ils le couplent aux capacités d'orchestration et d'automatisation de la plate-forme de réponse aux incidents d'IBM Resilient (IRP), les clients peuvent transformer les informations issues de leur SOC cognitif en actions par le biais de fonctions d'enrichissement, de remédiation et d'atténuation. Le SOC cognitif d'IBM rassemble également d'autres technologies de l'entité sécurité d'IBM, dont i2 pour la chasse aux cybermenaces et IBM X-Force Exchange.

Services de sécurité cognitifs et innovations

IBM aidera également les clients à concevoir, construire et gérer des centres d'opérations de sécurité cognitifs à l'échelle mondiale par le biais d'IBM Managed Security Services. Au cours des 5 dernières années, IBM a construit plus de 300 centres d'opérations de sécurité pour des clients dans des dizaines de secteurs, dont la fabrication de biens de grande consommation, le commerce de détail, le secteur bancaire et l'éducation. Les clients peuvent choisir entre faire construire par IBM leur SOC cognitif sur site ou le faire gérer virtuellement via le Cloud IBM dans le cadre du réseau IBM X-Force Command Center.

Le réseau mondial de centres de commande X-Force d'IBM utilise les capacités cognitives d'IBM telles que QRadar Advisor with Watson pour améliorer l'analyse des événements de sécurité. Un autre cas d'utilisation prometteur est un nouveau projet de recherche portant le nom de code Havyn, qui dote le SOC cognitif d'une voix. Le but de Havyn est de créer un assistant vocal de sécurité qui peut interagir avec les analystes en sécurité sur des sujets tels que les nouveautés en temps réel sur les menaces et les informations sur la sécurité d'une entreprise.

Le projet Havyn utilise les API Watson, Bluemix et IBM Cloud pour fournir une réponse en temps réel aux requêtes et commandes vocales, accéder aux données de renseignements de sécurité open source, y compris

IBM X-Force Exchange, ainsi qu'aux données historiques spécifiques de clients et à leurs outils de sécurité. Par exemple, Havyn peut fournir aux analystes en sécurité des mises à jour sur les nouvelles menaces qui sont apparues et sur les étapes de remédiation recommandée. Havyn est actuellement testé par des chercheurs et des analystes sélectionnés au sein d'IBM Managed Security Services.

Watson travaille actuellement avec des clients tous les jours via un nouvel outil d'assistant virtuel déployé dans le réseau des centres de commande X-Force d'IBM, qui gère plus de 1000 milliards d'événements de sécurité par mois. Les clients peuvent choisir de poser des questions à Watson via la messagerie instantanée sur leur sécurité ou leurs configurations de réseau. Par exemple, les clients peuvent poser des questions à Watson sur l'état d'un périphérique ou d'un ticket. L'outil est également capable d'exécuter des commandes de clients IBM MSS, comme la réaffectation d'un ticket à un nouveau propriétaire.

Pour plus d'informations sur Watson for Cyber Security et le SOC cognitif d'IBM : http://www-03.ibm.com/security/cognitive/

Les journalistes et les blogueurs peuvent télécharger un teaser et la vidéo sur Watson for Security et le SOC cognitif d'IBM ici : http://ibm.newsmarket.com/Global/Latest-News/ibm-delivers-watson-for-cyber-security-to-power-cognitive-security-operations-centers/s/27b21670-d4c9-4177-ba8f-d64203678aea

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 : http://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] Infographic: Watson for Cyber Security: Shining a light on Unstructured Data

[2] IBM 2016 Cyber Security Intelligence Index analysis

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

Contact(s) relations externes

IBM

Gaëlle Dussutour 01 58 75 17 96DUSGA@fr.ibm.com

Text100 for IBM

Amélie Chipaux 06 62 49 20 50amelie.chipaux@text100.fr