Communiqués de presse

La division sécurité d'IBM s’attaque aux menaces internes avec l'analyse des données liées au comportement des utilisateurs

IBM étend les capacités d’analyse avancée de la plateforme QRadar pour lutter contre les identifiants piratés et les utilisateurs internes malveillants

Paris - 31 août 2016: La division sécurité d’IBM (NYSE: IBM) annonce aujourd'hui une nouvelle application pour IBM QRadar qui analyse les types de comportements des utilisateurs internes, dont les employés, les fournisseurs et les partenaires. Ceci afin de déterminer si leurs identifiants ou leurs systèmes informatiques ont été piratés par des cyber-criminels. IBM QRadar User Behavior Analytics, disponible gratuitement via IBM Security App Exchange, étend les possibilités de la plateforme de renseignement de sécurité d'IBM QRadar pour fournir une visibilité précoce des menaces potentielles provenant d'utilisateurs internes, avant qu'elles ne causent des dommages à une entreprise.

Les menaces internes sont actuellement responsables de 60% des attaques auxquelles font face les entreprises. Mais environ ¼ de ces attaques est le résultat des informations d'identification des utilisateurs qui tombent entre les mains des pirates via les employés, les fournisseurs ou les partenaires (trompés par des attaques de phishing via des logiciels malveillants téléchargés ou via d'autres techniques1.) Par exemple, la nouvelle application d’analyse du comportement des utilisateurs devrait alerter les analystes lorsqu’un utilisateur se connecte sur un serveur sensible pour la première fois, depuis un nouveau lieu, tout en utilisant un accès privilégié. Ce changement de comportement sera identifié parce que la solution IBM QRadar User Behavior Analytics aura créé un modèle de base de comportement normal pour cet employé et aura détecté un écart significatif.

« Les entreprises ont besoin d'une meilleure façon de se protéger contre les menaces internes - qu'elles proviennent d’acteurs involontaires ou de cyber-criminels malveillants ayant accès au fonctionnement interne d'une entreprise et à ses systèmes informatiques. », **déclare Jason Corbin, Vice President of Strategy and Offering Management, IBM Security.** *« Cette nouvelle application fournit aux analystes la possibilité d’agir rapidement en utilisant les données de cybersécurité existantes. Ceci pour identifier les signes avant-coureurs qui sont souvent dissimulés dans les activités suspectes des utilisateurs, aidant finalement les analystes à traiter plus systématiquement les violations des données avant qu'elles ne se produisent. »*

IBM QRadar User Behavior Analytics exploite les données des investissements existants des clients QRadar, en leur offrant, via une plateforme unique, la possibilité d’analyser et de gérer les événements et les données de sécurité. Cette intégration permet d'éviter aux analystes de sécurité d'avoir à recharger et à conserver les données à partir de plusieurs plateformes pour identifier et enquêter sur le comportement des utilisateurs, ceci

en parallèle avec d'autres indicateurs de violations des données que QRadar détecte. La solution aide les professionnels de la sécurité à se prémunir contre les menaces malveillantes à travers :

- **Des profils d'analyse des risques** - l'application analyse les actions risquées des utilisateurs et applique un score aux comportements anormaux, permettant d'identifier à la fois les utilisateurs internes malveillants et les cyber-criminels présumés, en utilisant les informations d'identification compromises.

- **Un tableau de bord d'analyse comportementale priorisée** - Les analystes peuvent obtenir une meilleure visibilité et compréhension des actions qui conduisent un utilisateur à ouvrir un document malveillant ou à savoir comment ils ont obtenu des accès privilégiés. Par exemple, un simple clic de souris, une pièce jointe ou un lien dans un e-mail de phishing, permettent d'ajouter l'activité suspecte de l'utilisateur à une liste de surveillance ou de générer une annotation en mode texte pour expliquer les observations de l'analyste.

- **L'amélioration des données de sécurité QRadar existantes** - Avec les informations utilisateurs issues de l'environnement informatique global, les équipes de sécurité seront en mesure de puiser dans le large éventail de sources de données et de renseignements existants sur les menaces dans QRadar pour les détecter à travers les utilisateurs et les actifs.

Avec l'acquisition récente de Resilient Systems, IBM permet de répondre facilement à des incidents importants dans la plateforme QRadar, via la nouvelle application User Behavior Analytics app. Disponible en téléchargement gratuit sur IBM Security App Exchange, l'application QRadar User Behavior Analytics fait partie de l'approche ouverte d'IBM pour le développement d'outils de sécurité pouvant être exploités dans la lutte contre la cybercriminalité.

Au cours des deux dernières années, IBM a pris des mesures importantes pour aider les professionnels de la sécurité dans le monde entier à collaborer pour prendre l'avantage sur les cyber-criminels. Cela via l'accès public à 700 To de données sur les menaces avec le lancement d'IBM X-Force Exchange. Construit sur X-Force Exchange intelligence, IBM Security App Exchange s'est développée pour devenir une place de marché en ligne en croissance pour les partenaires et les clients afin de partager et télécharger des applications basées sur les technologies de sécurité IBM, telles qu'IBM QRadar. La place de marché contient des dizaines de solutions tierces pour renforcer la capacité des clients à personnaliser leur environnement de sécurité en utilisant l'approche de plateforme ouverte d'IBM.

[1] IBM X-Force Cyber Threat Index, 2016

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