Communiqués de presse

IBM met à disposition sa plateforme de renseignements de sécurité pour lutter contre les cyber-attaques

IBM partage ses données dans IBM X-Force Exchange, sa nouvelle plateforme de partage relative aux cyber-menaces

Paris - 16 avr. 2015: IBM annonce aujourd'hui qu'il rend disponible sa vaste base de données de renseignements de sécurité, IBM X-Force Exchange, une nouvelle plateforme de partage de renseignements liés aux cyber-menaces, fonctionnant sur le Cloud d'IBM. Cette plateforme collaborative fournit un accès à nombre de données concrètes en matière de menaces provenant du monde entier, issues d'IBM mais aussi de tiers. Cela inclut des indicateurs en temps réel des attaques en cours, qui peuvent être utilisés pour se défendre contre la cybercriminalité.

Le besoin de renseignements fiables concernant les menaces est plus important que jamais, d'autant que 80% des cyber-attaques sont générées par des réseaux criminels hautement organisés au sein desquels les données, les outils et l'expertise sont largement partagés 1. Si les pirates se sont mobilisés, ce n'est pas le cas de leurs cibles. Une majorité (65 %) des équipes internes de cyber-sécurité utilisent plusieurs sources de renseignements extérieures, fiables ou non, pour combattre les pirates 2.

X-Force Exchange s'appuie sur l'importante expérience d'IBM en matière de renseignements de sécurité, intégrant son important portefeuille de données approfondies liées aux recherches sur les menaces et de technologies telles que QRadar, des milliers de clients dans le monde, et l'expertise d'un réseau mondial d'analystes en sécurité et d'experts issus d'IBM Managed Security Services. Tirant profit de l'ouverture et de la puissance de l'infrastructure Cloud, les utilisateurs peuvent collaborer et puiser dans de multiples sources de données, y compris :

- L'un des catalogues les plus vastes et les plus complets du monde en matière de vulnérabilités;
- Des informations sur les menaces basées sur l'observation de plus de 15 milliards d'événements de sécurité surveillés par jour;
- Les renseignements de sécurité concernant les logiciels malveillants issus d'un réseau de 270 millions de terminaux;

- Les informations sur les menaces basées sur plus de 25 milliards de pages web et d'images;
- L’analyse approfondie de plus de 8 millions de spams et d’attaques d’hameçonnage ;
- Les données de réputation de près d’1 million d'adresses IP malveillantes.

Aujourd'hui, X-Force Exchange dispose de plus de 700 téraoctets de données agrégées brutes fournies par IBM. Celles-ci continueront à être enrichies, mises à jour et partagées dans la mesure où la plateforme peut ajouter jusqu'à un millier d’indicateurs malveillants chaque heure. Ces données comprennent des informations en temps réel qui sont essentielles dans la lutte contre la cybercriminalité.

« La plateforme IBM X-Force Exchange encouragera la collaboration à l’échelle requise pour contrer l’augmentation rapide et la complexité des menaces auxquelles les entreprises font face de la part des cybercriminels », déclare **Brendan Hannigan, General Manager, IBM Security**. « Nous prenons les devants en ouvrant notre propre réseau mondial de données liées à la cyber-menace issu de la cyber-recherche X-Force, de nos technologies et des experts ainsi que des informations anonymisées de clients. En invitant l’industrie à se joindre à cet effort en partageant ses propres renseignements de sécurité, nous comptons accélérer la formation des réseaux et des relations nécessaires pour contrer les pirates ».

Un partage de la menace ouvert, automatisé et collaboratif

Conçu par la division sécurité d’IBM, l’IBM X-Force Exchange est une nouvelle plateforme basée sur le Cloud qui permet aux entreprises de collaborer facilement sur les incidents de sécurité, et de bénéficier des contributions continues des experts IBM et des membres de la communauté. Depuis le lancement bêta de X-Force Exchange, de nombreux précurseurs ont rejoint la communauté.

En utilisant librement les renseignements liés aux cyber-menaces, en les partageant et en agissant dessus en temps réel, à partir de leurs réseaux et du répertoire d’IBM, les utilisateurs peuvent identifier et aider à arrêter les menaces via:

- Une interface collaborative et sociale permettant d’interagir facilement avec leurs pairs de l'industrie, des analystes et des chercheurs et valider les informations issues de ces derniers;
- La masse de renseignements issus de multiples tiers, dont la profondeur et l'ampleur vont continuer à croître au fur et à mesure que la base d'utilisateurs de la plateforme se développera;
- Un outil de recueil permettant d’organiser facilement et d’annoter les découvertes, mettant ainsi en avant les informations prioritaires;
- Un accès libre par le web pour les analystes et les chercheurs en sécurité;
- Une bibliothèque d'interfaces de programmation (APIs – Application Programming Interface) pour faciliter le

développement des requêtes entre la plateforme et les machines ainsi que les applications; permettant ainsi aux entreprises d'opérationnaliser l’analyse de la menace et de prendre les mesures adéquates.

Au sein de cette plateforme, IBM prévoit également de soutenir STIX et TAXII, la nouvelle norme pour le partage automatisé des renseignements de sécurité, afin de faciliter l’extraction et le partage vers et depuis la plateforme exchange, ainsi que l’intégration parfaite avec les systèmes de sécurité existants.

Remettre les cyber-menaces dans le contexte

Pour la première fois, les entreprises peuvent interagir directement avec les analystes et les chercheurs en sécurité d’IBM, ainsi que leurs pairs de l'industrie, par l'intermédiaire de la plateforme pour valider les découvertes et les présenter à d'autres sociétés luttant contre la cybercriminalité.

Par exemple, un chercheur en sécurité pourrait découvrir un nouveau logiciel malveillant et le mentionner dans la plateforme. De là, un analyste de la sécurité dans une autre entreprise pourrait trouver ce logiciel à partir de son réseau sur la plateforme et consulter d'autres analystes et experts pour valider le danger. L'analyste appliquerait alors des règles de blocage de cette présence digitale dans sa propre entreprise, arrêtant ainsi l’activité de ce logiciel malveillant et - via la plateforme – pourrait rapidement alerter le responsable de la sécurité des systèmes d’informations (RSSI) de son entreprise à propos de cette menace. Ce dernier ajouterait alors cette source de trafic malveillant dans une bibliothèque publique sur la plateforme pour la partager avec ses pairs de l'industrie, pour contenir et arrêter rapidement la menace avant qu'elle n’infecte d'autres entreprises.

Pour plus d’informations : http://xforce.ibmcloud.com/

A propos d’IBM Security

La plateforme de sécurité IBM apporte la sécurité intelligente pour aider les organisations à protéger les personnes, les données, les applications et les infrastructures. Les solutions IBM couvrent la gestion des identités et des accès, le SIEM (Security Information and Event Management), la sécurité des données, la sécurité des applications, la gestion du risque, la gestion des terminaux, la nouvelle génération de protection contre les intrusions et d’autres sujets. IBM dispose d’une des plus importantes organisations au monde de recherche et développement et des opérations dans le domaine de la sécurité.

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

Suivez notre actualité sur Twitter @IBMSecurityFR

- UNODOC Comprehensive Study on Cybercrime 2013
- ESG: http://bit.ly/1xzTmUW
