Communiqués de presse

IBM Security lance App Exchange pour favoriser une meilleure collaboration contre la cybercriminalité

Des partenaires et développeurs mettent à disposition de nouvelles applications QRadar en utilisant des outils de programmation ouverts

Paris - 08 déc. 2015: IBM annonce l'ouverture de sa plateforme d'analyse des données de sécurité, IBM Security QRadar, permettant aux clients, partenaires et autres développeurs de créer des applications qui tirent parti des capacités avancées de la plateforme en matière de renseignements de sécurité. La compagnie lance également IBM Security App Exchange, une place de marché dédiée à la communauté d'experts en sécurité pour créer et partager des applications basées sur les technologies de sécurité IBM.

L'ouverture de cette plate-forme d'analyse de la sécurité est la deuxième décision majeure qu'a pris IBM cette année pour faire avancer la collaboration et l'innovation dans l'industrie, ceci afin de lutter contre la cybercriminalité hautement organisée. Plus tôt cette année, IBM avait ouvert sa base de données IBM X-Force Exchange, composée de 700 To de données dédiées aux menaces liées à la sécurité. Plus de 2.000 organisations ont rejoint cette plateforme de partage depuis avril dernier. En combinant l'ouverture de sa plateforme d'analyse de la sécurité et de sa base de données de renseignements sur les menaces, IBM contribue à une collaboration approfondie et permet aux entreprises de partager non seulement des données mais aussi l'expertise qui permettra de devancer les cybercriminels.

IBM et ses partenaires, dont Bit9 + Carbon Black, BrightPoint Security, Exabeam et Resilient Systems ont déjà complété IBM Security App Exchange avec des dizaines d'applications qui étoffent IBM Security QRadar dans des domaines tels que le comportement de l'utilisateur, les données liées aux terminaux informatiques et la visualisation des incidents. Ces nouvelles applications tirent profit de nouvelles APIs* pour QRadar, la plateforme de renseignement de sécurité d'IBM. La plateforme utilise l'analyse de données et les renseignements sur les menaces pour détecter les incidents de sécurité dans des milliers de centres d'opérations de sécurité (SOC) à travers le monde, incluant près de la moitié de ceux des entreprises du classement Fortune 100.

« Avec des milliers de clients qui utilisent désormais les technologies de sécurité d'IBM, le fait d'ouvrir cette plateforme contribue à une collaboration et un développement plus étroit avec des partenaires et des clients et change la donne de la lutte contre la cybercriminalité », explique **Marc van Zadelhoff**, Strategy and Product Management, IBM Security. *« Partager notre expertise à travers l'industrie de la sécurité nous permettra d'innover plus rapidement afin d'aider à anticiper des attaques de plus en plus sophistiquées. »*

Les nouvelles applications offrent un accès rapide à une grande variété d'analyses des données de sécurité

Ouvrir le développement et la collaboration est essentiel pour accélérer l'innovation dans un paysage technologique en constante évolution. Plus de 77% des dirigeants disent que les pratiques de développement collaboratif ont profité à leur entreprise à travers un cycle de développement du produit plus court et une mise sur le marché plus rapide.[1]

Des dizaines d'organisations ont rejoint IBM App Exchange, qui a déjà stimulé le partage de 14 nouvelles applications QRadar par les développeurs et partenaires d'IBM tels que Exabeam, Bit9+Carbon Black, Resilient Systems, Stealthbits, Brightpoint et iSight. D'autres partenaires tels que STEALTHbits et iSIGHT Partners ont également des applications en cours de développement.

Grâce à l'intégration de technologies tierces, ces nouvelles applications sont conçues pour offrir aux clients une meilleure visibilité sur plusieurs types de données et offrent également de nouvelles fonctions de recherche automatisée et de reporting, ce qui aide les experts en sécurité à se concentrer sur les menaces prioritaires.

Les applications sont maintenant disponibles gratuitement sur IBM Security App Exchange, offrant aux clients un accès à une plus grande variété d'analyses qui sont étroitement intégrées dans l'environnement de renseignement de sécurité d'IBM QRadar.

Exemples de ce que ces nouvelles applications comprennent :

• **Le comportement utilisateur** - Exabeam User Behavior Analytics app intègre l'analyse du comportement de l'utilisateur et les profils de risque directement dans le tableau de bord QRadar. Cette visualisation des risques utilisateurs en temps réel permet aux entreprises de détecter les différences de comportement entre un employé classique et un pirate ayant les mêmes accès.

• **Renseignement sur les menaces** - une nouvelle application développée par IBM permet aux utilisateurs de QRadar d'utiliser les flux des renseignements de sécurité en utilisant les standards ouverts STIX et les formats TAXII, et d'utiliser ces données pour créer des règles personnalisées pour la corrélation, la recherche ou le reporting. Par exemple, les utilisateurs pourraient recenser les adresses IP dangereuses dans les bibliothèques publiques depuis IBM X-Force Exchange et créer une règle pour connaître l'importance des attaques comprenant les adresses IP de cette liste de surveillance.

• **Analytique pour les terminaux** - Une nouvelle application de Bit9 + Carbon Black permet aux utilisateurs QRadar de bénéficier d'une visibilité approfondie des menaces sur les terminaux, ordinateurs de bureau, ordinateurs portables et serveurs. En analysant les données sensibles issues des terminaux dans l'interface QRadar, l'application Carbon Black pour IBM QRadar permet aux clients de détecter et de répondre aux

attaques sur les terminaux plus rapidement et plus efficacement.

• **La visualisation des incidents** - la nouvelle application de visualisation des incident de IBM Security QRadar permet aux utilisateurs de mieux visualiser toutes les infractions au sein de leur installation QRadar en utilisant des bulles, des couleurs et des lignes de corrélation. La taille et la couleur de la bulle indique l'ampleur de l'incident, tandis que les lignes tracées entre les bulles indiquent les adresses IP partagées parmis les incidents associés. Ce type d'approche de visualisation intuitive aide les analystes en sécurité à identifier rapidement les éléments communs entre les incidents et à mieux les prioriser.

Ces applications sont fournies dans le cadre de la nouvelle application QRadar, qui permet à la communauté sécurité de construire rapidement de nouvelles applications QRadar via des API ouvertes et des kits de développement logiciel. IBM Security testera chaque application avant qu'elle ne soit recensée sur App Exchange, ceci pour assurer l'intégrité des contributions de la communauté.

IBM Security QRadar accélère les recherches et répond automatiquement aux menaces

IBM annonce également une nouvelle version de IBM Security QRadar, qui analyse les données à travers une infrastructure IT d'entreprises pour identifier les menaces de sécurité potentielles. IBM Security QRadar est leader sur le marché des incidents liés à la sécurité et la gestion des événements (SIEM)2. Il se positionne également en tête du Gartner's Magic Quadrant for SIEMsur les 7 dernières années3.

Pour la première fois, QRadar permettra aux clients de créer des règles qui prendront automatiquement des mesures une fois que des menaces spécifiques ont été détectées. Par exemple, les règles créées dans QRadar peuvent automatiquement déclencher des actions qui bloquent les adresses IP et contrôlent l'accès des utilisateurs en fonction de leur profil de risque. En outre, les applications qui sont développées en utilisant le nouveau cadre d'applications QRadar peuvent également exploiter des règles personnalisées pour répondre automatiquement aux menaces.

De plus, IBM intègre davantage QRadar à la gestion de la sécurité des terminaux d'IBM BigFix pour aider les clients à mieux hiérarchiser les menaces et les correctifs à apporter aux terminaux des utilisateurs. QRadar peut maintenant aussi identifier les terminaux exposés qui n'ont pas installé BigFix, aidant ainsi les clients à trouver plus rapidement des éléments qui posent problème.

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 de prestations de services dans le domaine de la sécurité.

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

Blog US : www.securityintelligence.com

Suivez notre actualité sur Twitter @IBMSecurityFR

**API : interfaces de programmation*

2 Gartner, "Market Share Analysis: Security Software, Worldwide, 2014," by Sid Deshpande, Ruggero Contu, May 15, 2015

3 Gartner "Magic Quadrant for Security Information and Event Management" by Kelly M. Kavanagh, Oliver Rochford, July 20, 2015

---

[1] Linux Foundation Collaborative Trends Report 2014.