Communiqués de presse

IBM lance une technologie ouverte pour accélérer la réponse aux cybermenaces à travers les Clouds

Elle offre une capacité inédite permettant de rechercher les menaces à travers les outils de sécurité et les Clouds sans déplacer les données

ARMONK, NY - 20 nov. 2019: IBM (NYSE: IBM) a annoncé aujourd'hui le Cloud Pak for Security, qui présente des innovations révolutionnaires qui lui permettent de se connecter à n'importe quel outil de sécurité, Cloud ou système en local sans avoir à déplacer des données de leur source d'origine. Disponible dès aujourd'hui, la plateforme inclut une technologie open source pour rechercher les menaces, des capacités d'automatisation pour aider à accélérer les réponses aux cyberattaques et la possibilité de fonctionner dans n'importe quel environnement.

Cloud Pak for Security est la première plateforme à tirer parti de la nouvelle technologie open source lancée par IBM et capable de rechercher et de convertir des données de sécurité provenant de diverses sources, rassemblant ainsi des informations de sécurité essentielles issues de l'ensemble de l'environnement informatique multicloud d'une entreprise. La plateforme est extensible, ce qui permet l'ajout de solutions et d'applications supplémentaires au fil du temps.

À mesure que les entreprises progressent dans l'adoption du Cloud, les applications et les données se retrouvent fréquemment dispersées sur une multitude de Clouds privés et publics et de ressources en local. Toute tentative pour protéger cet environnement informatique fragmenté oblige souvent les équipes de sécurité à entreprendre des opérations d'intégration complexes et de passer en permanence d'un écran et d'un produit à un autre. Dans une enquête récente de l'Institut SANS, sponsorisée par IBM Security, plus de la moitié des équipes de sécurité interrogées affirment éprouver des difficultés à intégrer des données à des outils de sécurité et d'analyse disparates et à combiner ces données dans leurs environnements Cloud pour repérer les menaces avancées.[1]

Voici trois fonctionnalités initiales du Cloud Pak for Security:

- **Utilisation n'importe où. Connecter la sécurité de manière ouverte.** IBM Cloud Pak for Security s'installe facilement dans n'importe quel environnement, que ce soit en local, sur un Cloud privé ou public. Il se compose de logiciels conteneurisés préintégrés à Red Hat OpenShift, la plateforme Kubernetes d'entreprise la plus complète du marché. Par le biais de l'OASIS Open Cybersecurity Alliance, IBM a également noué des partenariats avec des dizaines d'entreprises afin de promouvoir l'interopérabilité et d'aider à réduire la dépendance à un fournisseur au sein de la communauté dédiée à la sécurité via des technologies open source développées conjointement.

- **Obtention des informations relatives à la sécurité sans déplacer une seule donnée.** Transférer des données dans le but de les analyser génère une complexité additionnelle. IBM Cloud Pak for Security peut relier toutes les sources de données d'une entreprise pour mettre en lumière les menaces cachées et

l’aider à prendre de meilleures décisions fondées sur les risques, tout en laissant les données où elles se trouvent. Grâce à l'utilisation de standards ouverts et aux innovations d'IBM, les clients peuvent accéder aux outils d'IBM et de tiers pour rechercher des indicateurs de menaces dans n'importe quel cloud ou en local. Grâce à l'application Data Explorer du Cloud Pak for Security, les analystes sécurité peuvent rationaliser leur recherche de menaces à travers les outils de sécurité ou les Clouds. Sans cette capacité, les équipes de sécurité devraient rechercher manuellement les mêmes indicateurs de menace (tels qu’une signature de logiciel malveillant ou une adresse IP malveillante) dans chaque environnement. Cloud Pak for Security est le premier outil qui permet ce type de recherche sans qu’il soit nécessaire de transférer ces données dans la plateforme en vue d’une analyse.

- **Réponse plus rapide aux incidents de sécurité grâce à l'automatisation** . IBM Cloud Pak for Security relie les workflows de sécurité à l’aide d’une interface unifiée pour aider les équipes à répondre plus rapidement aux incidents de sécurité. Selon les estimations d'IBM Security, les équipes de sécurité doivent gérer en moyenne 200 000 événements de sécurité potentiels par jour et coordonner les réponses entre des dizaines d'outils. IBM Cloud Pak for Security permet aux clients d'orchestrer et d'automatiser leur réponse de sécurité afin de mieux prioriser le temps de leur équipe. La plateforme permet aux entreprises d'orchestrer leur réponse à des centaines de scénarios de sécurité courants, en guidant les utilisateurs tout au long du processus et en fournissant un accès rapide aux données et aux outils de sécurité appropriés. La capacité d’orchestration, d’automatisation et de réponse d’IBM s’intègre à Red Hat Ansible pour proposer des protocoles d’automatisation supplémentaires. En formalisant les processus et les activités de sécurité dans l'ensemble de l'entreprise, les sociétés peuvent réagir rapidement et efficacement, tout en se dotant des informations nécessaires pour aider à répondre aux exigences réglementaires.

« Nous assistons à une dispersion des données de sécurité entre une multitude d’outils, de Clouds et d’infrastructures informatiques à mesure que les entreprises transfèrent des applications critiques vers des environnements multiclouds hybrides. Il peut en résulter des failles permettant à certaines menaces de passer inaperçues, ce qui conduit les équipes de sécurité à élaborer et à entretenir des plans d’intégration et de réponse manuelle coûteux et complexes », a déclaré **Mary O’Brien, General Manager d’IBM Security** *. « Avec Cloud Pak for Security, nous aidons à jeter les bases d’un écosystème de sécurité plus connecté conçu pour le monde du multicloud hybride. »*

IBM a collaboré avec des dizaines de clients et de fournisseurs de services au cours du processus de conception pour élaborer une solution capable de résoudre les problèmes d'interopérabilité majeurs qui touchent le domaine de la sécurité. Cloud Pak for Security dispose de connecteurs destinés à des intégrations préconstruites avec des outils de sécurité populaires d'IBM, de Carbon Black, de Tenable, d’Elastic, de BigFix et de Splunk, et avec des fournisseurs de Cloud publics, dont IBM Cloud, Amazon Web Services[2] et Microsoft Azure2. La solution repose sur des normes ouvertes de sorte à pouvoir connecter des outils et des données de sécurité supplémentaires provenant de l’infrastructure d’une entreprise.

« Les entreprises ont rapidement adopté de nouvelles technologies de sécurité pour faire face aux menaces les plus récentes, mais elles jonglent maintenant avec des dizaines d'outils déconnectés qui ne fonctionnent pas toujours bien ensemble », a indiqué **Jon Oltsik, Senior Principal Analyst, Enterprise Strategy Group**. *« L'industrie doit résoudre ce problème pour les clients en passant à des technologies plus ouvertes et à des plateformes unifiées qui peuvent servir de liaison entre des outils de sécurité isolés. L'approche d'IBM répond à cette exigence et a la capacité de réunir chaque couche de la pile de sécurité dans une interface unique et simplifiée. »*

Afin d'accélérer davantage la transition de l'industrie vers une sécurité ouverte, IBM mène également des projets open source visant à faire fonctionner les outils de sécurité de manière coordonnée et native dans l'ensemble de l'écosystème de sécurité. En tant que membre fondateur de l'Open Cybersecurity Alliance, IBM et plus de 20 autres organisations travaillent ensemble à l'élaboration de normes ouvertes et de technologies open source facilitant l'interopérabilité entre les produits et réduisant la dépendance à un fournisseur au sein de la communauté dédiée à la sécurité.

Conçu pour le monde du multicloud hybride

76% des organisations déclarent utiliser pas moins de 2 à 15 Clouds, et 98% d'entre elles prévoient d'utiliser plusieurs Clouds hybrides d'ici trois ans.[3] IBM Cloud Pak for Security repose sur des technologies open source qui prennent en charge les environnements Clouds des entreprises - dont Red Hat OpenShift.

Étant conçu sur des éléments de base ouverts et flexibles, Cloud Pak for Security simplifie le déploiement « conteneurisé » sur n'importe quel Cloud ou n'importe quel environnement en local. Alors que les entreprises continuent d'effectuer de nouveaux déploiements et de nouvelles migrations sur le Cloud, Cloud Pak for Security peut s'adapter à ces nouveaux environnements et ainsi permettre aux clients d'intégrer leurs applications sensibles et stratégiques sur le Cloud tout en conservant la visibilité et le contrôle à partir d'une plateforme de sécurité centralisée.

Cloud Pak for Security fournit également un modèle pour aider les fournisseurs de services de sécurité gérés (MSSP) à agir efficacement à grande échelle, de connecter les silos de sécurité et de rationaliser leurs processus de sécurité. Les entreprises peuvent également faire appel à IBM Security pour un large éventail de services supplémentaires, tels que des services de conseil à la demande, de développement personnalisé et de réponse aux incidents.

IBM Cloud Pak for Security est désormais disponible dans le monde entier.

Pour en savoir plus : https://www.ibm.com/products/cloud-pak-for-security

A propos d'IBM Security

IBM Security offre aux entreprises l'une des gammes de produits et services de sécurité les plus performantes et intégrées du marché. Ce portefeuille, qui repose sur les recherches du mondialement célèbre IBM X-Force®, permet aux organisations de gérer efficacement les risques et de se défendre face aux menaces émergentes. IBM compte parmi les plus grandes organisations mondiales dédiées à la recherche, au développement et à la conception de solutions de sécurité, gère 70 milliards d'évènements de sécurité par jour dans plus de 130 pays, et possède plus de 10 000 brevets dans le domaine de la sécurité. Pour de plus amples informations, rendez-vous sur https://www-03.ibm.com/security/fr-fr/, suivez IBMSecurity sur Twitter ou consultez le blog IBM Security Intelligence.

---

[1] Enquête de l'Institut SANS, Effectively Addressing Advanced Threats, 2019.

[2] Disponible en Q4 2019

[3] IBM Institute for Business Value, 2018

Contact(s) relations externes

IBM

Gaëlle Dussutour Tel. : + 33 (0)6 74 98 26 92 dusga@fr.ibm.com

Weber Shandwick pour IBM

Robin Legros / Morad Salehi Tél : + 33 (0) 6 68 04 57 83 ibmfrance@webershandwick.com