

IBM améliore son Cloud Pak for Security afin de gérer les menaces à travers les outils, les équipes et les Clouds

- La plateforme ouverte exploite l'intelligence artificielle (IA) et l'automatisation pour rationaliser la gestion des menaces dans les environnements Cloud hybrides et les outils de sécurité disparates. - Une première dans l'industrie : la possibilité de relier la gestion des menaces, des données et des identités au sein d'une plateforme unique. - De nouveaux services de sécurité clés en main pour remédier à la pénurie de compétences en matière de cybersécurité et répondre aux besoins liés au télétravail.

ARMONK, N.Y., 14 octobre 2020 : IBM (NYSE : IBM) Security a annoncé aujourd'hui de nouvelles et prochaines fonctionnalités pour son Cloud Pak for Security, notamment une solution de sécurité des données unique en son genre qui permet aux entreprises de détecter les menaces pesant sur leurs données les plus sensibles, d'y répondre et de s'en protéger dans des environnements Cloud hybrides. Conçu pour unifier des technologies de sécurité auparavant déconnectées, IBM a élargi son Cloud Pak for Security pour y inclure de nouvelles sources de données, des intégrations et des services qui permettent aux équipes d'opérations de sécurité de gérer le cycle de vie complet des menaces à partir d'une console unique.

Avec ces prochaines capacités^[1], le Cloud Pak for Security comprendra l'accès à six flux de renseignements sur les menaces, 25 connexions pré-définies à des sources de données IBM et tierces, 165 intégrations de gestion de cas connectées par le biais d'une intelligence artificielle avancée afin de hiérarchiser les menaces, ainsi que des playbooks automatisés pour rationaliser les actions de réponse des équipes de sécurité.

Comme l'adoption du Cloud et le télétravail ont modifié le périmètre informatique traditionnel, les équipes de réponse en matière de sécurité peuvent bénéficier de connaissances plus approfondies sur la sécurité dans les environnements Cloud hybrides. Le comportement des utilisateurs, la gestion des identités et la sécurité des données ont traditionnellement été isolés de la gestion des menaces. Grâce à ces prochaines fonctionnalités, le Cloud Pak for Security deviendra la première plateforme du secteur à relier les informations sur les données et l'analyse du comportement des utilisateurs à la détection des menaces, aux enquêtes et aux réponses.

Aujourd'hui, IBM annonce des capacités pour améliorer davantage son Cloud Pak for Security, notamment :

- **Une réponse coordonnée à la menace + la sécurité des données** : IBM a développé une nouvelle approche, inédite dans l'industrie, pour offrir aux équipes de sécurité une visibilité sur l'activité, la conformité et les risques liés aux données, sans avoir à quitter leur principale plateforme d'intervention. Le nouveau hub intégré de sécurité des données, dont la disponibilité générale est prévue pour le quatrième

trimestre, permet aux analystes de connaître rapidement l'endroit où se trouvent leurs données sensibles dans les environnements Cloud hybrides, ainsi que les personnes qui y ont accès, la manière dont elles sont utilisées et la meilleure façon de les protéger. Combler le fossé entre la sécurité des données et la gestion des menaces peut réduire le délai de réponse aux violations des données, qui prennent actuellement plus de six mois en moyenne pour être identifiées et contenues pour les organisations ayant récemment fait l'objet d'une enquête[2].

- **Un accès à des informations de pointe sur les menaces** : Cloud Pak for Security élargit sa collecte de renseignements sur les menaces, aidant ainsi les clients à détecter les signes avant-coureurs de campagnes de menaces actives ayant un impact sur les entreprises du monde entier. Outre le flux de renseignements sur les menaces X-Force d'IBM (IBM X-Force Threat Intelligence Feed), la plateforme fournira également des intégrations pré-définies pour cinq flux supplémentaires de renseignements sur les menaces provenant de sources tierces telles que AlienVault OTX, Cisco Threatgrid, MaxMind Geolocation, SANS Internet StormCenter et Virustotal dont la disponibilité générale est prévue pour le quatrième trimestre, ainsi que des flux supplémentaires de renseignements sur les menaces qui devraient être ajoutés en 2021.
- **Des services et support dédiés** : IBM lance de nouvelles offres de services de sécurité dédiés pour aider les organisations à moderniser leurs opérations de sécurité avec le Cloud Pak for Security, en s'appuyant sur une approche globale reliant les produits et les services.

Grâce à une large gamme d'options de services flexibles, les experts d'IBM peuvent aider leurs clients à déployer et à gérer le Cloud Pak for Security dans n'importe quel environnement, incluant la gestion des menaces de bout en bout, les services de sécurité managés, ainsi que la stratégie, le conseil et le support à l'intégration.

*« La complexité est le plus grand défi auquel notre industrie est confrontée, car elle oblige les équipes de sécurité à court de ressources à relier manuellement des outils et des sources de données de sécurité disparates », a déclaré **Justin Youngblood, Vice President, IBM Security**. « Le Cloud Pak for Security est entièrement basé sur des technologies cloud natives ouvertes pour connecter n'importe quel outil au sein de l'écosystème de sécurité. Avec ces mises à jour, nous serons les premiers dans l'industrie à réunir les renseignements sur les menaces et la gestion des menaces externes avec la sécurité des données et identités, aidant ainsi les organisations à moderniser leurs opérations de sécurité et à créer les bases d'une stratégie de sécurité zero trust ».*

Des connexions ouvertes dans tout l'écosystème de la sécurité

Le Cloud Pak for Security exploite les technologies ouvertes pour créer une base d'interopérabilité et des connexions plus profondes entre les outils d'IBM et ceux de tiers. Par exemple, la plateforme utilise [STIX-Shifter](#), une bibliothèque open-source qui permet aux analystes de sécurité de rechercher des indicateurs de menaces dans toutes les sources de données connectées, en effectuant une seule requête. En outre, le Cloud Pak for Security est basé sur Red Hat [OpenShift](#), fournissant une base ouverte et conteneurisée qui peut être facilement déployée dans des environnements Cloud publics, privés ou en local.

Cette approche ouverte permet au Cloud Pak for Security d'être plus qu'un simple ensemble de fonctionnalités de sécurité, mais plutôt une plateforme permettant d'intégrer pleinement les processus de sécurité à travers les outils et les Clouds. La plateforme utilise une IA avancée, l'analytique et l'automatisation pour rationaliser le cycle de vie complet de la gestion des menaces, y compris des capacités natives pour la gestion de l'information et des événements de sécurité (SIEM), les renseignements sur les menaces, l'analyse du comportement des utilisateurs, la sécurité des données et l'analyse SOAR (orchestration, automatisation et réponse dans le domaine de la sécurité). Ces fonctionnalités sont fournies via une interface utilisateur unique et unifiée qui relie l'ensemble du processus de gestion des menaces par des workflows de bout en bout, de la détection à la réponse.

Grâce à la participation d'IBM Security à l'[Open Cybersecurity Alliance](#), la compagnie continuera à travailler avec la communauté pour faire progresser le développement et l'adoption de technologies ouvertes afin de rendre la sécurité plus interopérable.

Approche unifiée des produits et services

Le cadre ouvert du Cloud Pak for Security en fait une solution idéale pour la collaboration entre les équipes de sécurité et les prestataires de services externes qui augmentent les compétences et l'expertise des entreprises en matière de sécurité. Le Cloud Pak for Security prend également en charge la « multi-tenancy », permettant aux fournisseurs de services de tirer parti d'une seule instance de la plateforme pour servir plusieurs entreprises et sous-organisations tout en gardant leurs données isolées.

Les capacités étendues du Cloud Pak for Security peuvent être prises en charge par IBM Security Services et intégrées à cette entité, avec des offres unifiées qui relient les technologies et les services. Les clients peuvent profiter de l'[X-Force Threat Management](#), un service de gestion des menaces continu et de bout en bout qui utilise une approche programmatique pour aider les clients à faire mûrir leur stratégie globale de gestion des menaces au fil du temps. Les entreprises peuvent également tirer parti d'une grande variété de [services de](#)

[sécurité managés d'IBM](#), en utilisant le Cloud Pak for Security pour faciliter la collaboration et la visibilité en temps réel entre les clients et les équipes de service. Les entreprises peuvent également faire appel aux [consultants experts](#) d'IBM Security pour les aider à planifier, déployer et intégrer le Cloud Pak for Security à leurs investissements existants en matière de sécurité.

Pour en savoir plus sur l'IBM Cloud Pak for Security et se tenir au courant de ses dernières capacités, vous pouvez consulter le site suivant : <https://www.ibm.com/products/cloud-pak-for-security>.

Vous pouvez également vous inscrire au [webinaire](#) qui aura lieu le 29 octobre 2020 à 17h00.

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'événements 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 IBM Security sur Twitter ou consultez [le blog IBM Security Intelligence](#).

Avertissement : Les déclarations concernant les orientations et intentions futures d'IBM sont sujettes à modification ou retrait sans préavis et ne représentent que des buts et objectifs.

Contacts :

IBM

Gaëlle Dussutour

Tél. : + 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

[\[1\]](#) Scheduled for generally available within Q4 2020.

[\[2\]](#) 2020 Cost of a Data Breach Report, conducted by The Ponemon Institute and sponsored by IBM Security
