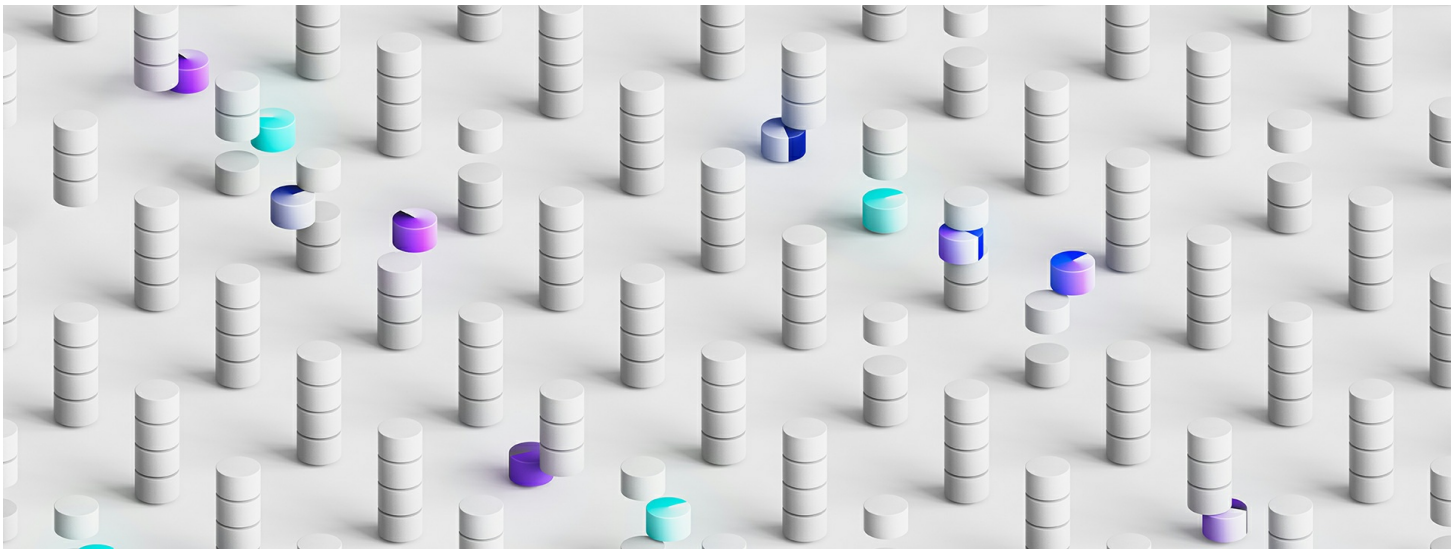
Communiqués de presse

IBM lance la nouvelle suite de sécurité QRadar pour accélérer la détection et la réponse aux menaces



L'interface modernisée et unifiée rationalise la réponse des analystes sur l'ensemble du cycle de vie de l'attaque

Les capacités sophistiquées d'IA et d'automatisation permettent d'accélérer le triage des alertes de 55 % en moyenne[1]

ARMONK, NY, le 24 avril 2023 : IBM (NYSE: IBM) a dévoilé aujourd'hui sa nouvelle suite de sécurité conçue pour unifier et accélérer l'expérience des analystes de sécurité tout au long du cycle de vie des incidents. La suite IBM Security QRadar représente une évolution et une expansion majeures de la marque QRadar, qui couvre toutes les technologies de détection, d'investigation et de réponse aux menaces, avec des investissements significatifs dans les innovations de l'ensemble du portefeuille.

Fournie en mode as a service, la suite IBM Security QRadar est construite sur une base ouverte et conçue spécifiquement pour les exigences du Coud hybride. Elle présente une interface utilisateur unique et modernisée pour tous les produits - dotée d'une IA et d'une automatisation avancées conçues pour permettre aux analystes de travailler avec davantage de rapidité, d'efficacité et de précision sur l'ensemble de leurs principaux outils.

Aujourd'hui, les équipes des centres d'opérations de sécurité (SOC) protègent une empreinte numérique en expansion rapide qui s'étend aux environnements Cloud hybride, ce qui crée de la complexité et rend difficile de suivre le rythme des attaques qui s'accélère. Elles peuvent être ralenties par des processus d'investigation et de réponse aux alertes qui génèrent une charge de travail importante et requièrent d'assembler manuellement des informations et de jongler entre des données, des outils et des interfaces déconnectés les uns des autres. Selon une enquête récente[2], les professionnels du SOC déclarent passer environ 1/3 de leur journée à enquêter et à valider des incidents qui s'avèrent ne pas être de véritables menaces.

S'appuyant sur sa position de leader dans 12 catégories de technologies de sécurité[3], IBM a réorganisé son portefeuille de détection et de réponse aux menaces, leader sur le marché, afin de maximiser la vitesse et l'efficacité et de répondre aux besoins spécifiques des analystes de la sécurité d'aujourd'hui. La nouvelle suite IBM Security QRadar comprend un EDR/XDR, un SIEM, un SOAR, ainsi qu'une nouvelle capacité de gestion des logs dans le Cloud, le tout conçu autour d'une interface utilisateur commune, d'informations partagées et de workflows connectés, avec les principaux éléments de conception suivants :

- **Expérience unifiée pour les analystes** : affinée en collaboration avec des centaines d'utilisateurs réels, la suite propose une interface utilisateur commune et modernisée pour tous les produits : elle est conçue pour augmenter considérablement la vitesse et l'efficacité des analystes sur l'ensemble de la chaîne d'attaque. Elle intègre des capacités d'IA et d'automatisation qui ont permis d'accélérer l'investigation et le triage des alertes de 55 % en moyenne au cours de la première année[1].

- **Disponibilité dans le Cloud, rapidité et échelle**: fournis en mode as a service sur Amazon Web Services (AWS), les produits de la suite QRadar permettent un déploiement, une visibilité et une intégration simplifiés dans les environnements Cloud et les sources de données. La suite comprend également une nouvelle fonctionnalité de gestion des logs « Cloud-native », optimisée pour une ingestion des données très efficace, une recherche rapide et des analyses à grande échelle.

- **Une base ouverte, des intégrations prédéfinies**: la suite rassemble les principales technologies nécessaires à la détection, à l'investigation et à la réponse aux menaces. Elle s'appuie sur une base ouverte, un vaste écosystème de partenaires et plus de 900 intégrations prédéfinies qui assurent une forte interopérabilité entre les outils d'IBM et ceux de tiers.

« Face à une surface d'attaque croissante et à des délais d'attaque de plus en plus courts, la rapidité et l'efficacité sont fondamentales pour le succès des équipes de sécurité aux ressources limitées », a déclaré **Mary O'Brien, General Manager, IBM Security**. *« IBM a conçu la nouvelle suite QRadar autour d'une expérience utilisateur unique et modernisée, intégrant une IA et une automatisation sophistiquées afin de maximiser la productivité des analystes de sécurité et d'accélérer leur réponse à chaque étape de la chaîne d'attaque. »*

La co-innovation au service des exigences de sécurité du monde réel

La suite QRadar est l'aboutissement d'années d'investissements, d'acquisitions et d'innovations d'IBM dans le domaine de la détection et de la réponse aux menaces. Elle comprend des dizaines de capacités d'IA et d'automatisation matures qui ont été affinées au fil du temps avec des utilisateurs et des données du monde réel, y compris des engagements de services de sécurité managés d'IBM (IBM Managed Security Services) avec plus de 400 clients. Elle comprend également des innovations développées en collaboration avec IBM Research et la communauté de la sécurité open source.

Il a été démontré que ces capacités alimentées par l'IA améliorent considérablement la rapidité et la précision des opérations des SOC : en permettant par exemple aux services de sécurité managés d'IBM d'automatiser plus de 70 % des clôtures d'alertes[4] et de réduire leurs délais de triage de 55 %[2] en moyenne au cours de la première année de mise en œuvre.

En réunissant ces capacités via l'expérience unifiée pour les analystes, la suite QRadar contextualise et hiérarchise automatiquement les alertes, affiche les données dans un format visuel pour une consommation rapide et fournit des informations partagées et des workflows automatisés entre les produits. Cette approche peut réduire considérablement le nombre d'étapes et d'écrans nécessaires pour enquêter sur les menaces et y répondre. Voici quelques exemples :

- **Triage des alertes par l'IA** : hiérarchisation ou clôture automatique des alertes sur la base d'une analyse des risques pilotée par l'IA, à l'aide de modèles d'IA entraînés sur la base de modèles de réponse d'analystes antérieurs, ainsi que de renseignements sur les menaces externes provenant d'IBM X-Force et d'informations contextuelles plus larges provenant de l'ensemble des outils de détection.
- **Enquête automatisée sur les menaces** : identifie les incidents hautement prioritaires pouvant justifier une enquête, et lance automatiquement cette dernière en récupérant les artefacts associés et en rassemblant des preuves par le biais de l'exploration de données dans tous les environnements. Le système utilise ces résultats pour générer une chronologie et un graphique d'attaque de l'incident sur la base du framework ATT&CK de MITRE, et recommande des actions pour accélérer la réponse.
- **Recherche accélérée des menaces** : utilise un langage open source de recherche des menaces et des capacités de recherche fédérée pour aider les « chasseurs » de menaces à découvrir des attaques furtives et des indicateurs de compromission dans leurs environnements, sans déplacer les données de leur source d'origine.

En aidant les analystes à réagir plus rapidement et plus efficacement, les technologies QRadar peuvent également aider les équipes de sécurité à améliorer leur productivité et à libérer le temps des analystes pour des tâches à plus forte valeur ajoutée.

Une suite de sécurité ouverte, connectée et modernisée

La suite QRadar exploite des technologies et des normes ouvertes dans l'ensemble du portefeuille, ainsi que des centaines d'intégrations prédéfinies avec les partenaires de l'écosystème IBM Security. Ce modèle permet d'approfondir les connaissances partagées et les actions automatisées dans les Clouds de tiers, les produits spécialisés et les lacs de données, ce qui peut réduire les délais de déploiement et d'intégration de plusieurs mois à quelques jours ou semaines.

La suite IBM QRadar comprend les principaux produits suivants, initialement fournis en mode SaaS et mis à jour avec la nouvelle expérience unifiée pour les analystes :

- **QRadar Log Insights** : une nouvelle solution de gestion des logs et d'observabilité de la sécurité « Cloud-native », offrant une ingestion des données simplifiée, une recherche en moins d'une seconde et une analyse rapide. Elle s'appuie sur un lac de données de sécurité élastique optimisé pour collecter, stocker et effectuer des analyses sur des téraoctets de données avec une vitesse et une efficacité accrues. Elle est conçue pour une gestion rentable des logs de sécurité ainsi que pour la recherche et l'investigation fédérées.

- **QRadar EDR et XDR** : aide les entreprises à protéger leurs terminaux contre les menaces zero-day inconnues jusqu'à présent - en utilisant l'automatisation et des centaines de modèles de machine learning et de comportement pour détecter les anomalies comportementales et répondre aux attaques en temps quasi réel. Il s'appuie sur une approche unique qui surveille les systèmes d'exploitation de l'extérieur, ce qui permet d'éviter les manipulations ou les interférences de la part d'adversaires. Pour les entreprises qui souhaitent étendre leurs capacités de détection et de réponse au-delà du terminal, IBM propose également XDR avec une corrélation des alertes, une investigation automatisée et des réponses recommandées sur l'ensemble du réseau, du Cloud, de la messagerie électronique et plus encore, ainsi que la détection et la réponse managées (MDR).

- **QRadar SOAR** : récent lauréat d'un Red Dot Design Award pour l'interface et l'expérience utilisateur ; il aide les organisations à automatiser et à orchestrer les workflows de réponse aux incidents et à s'assurer que leurs processus spécifiques sont suivis d'une manière cohérente, optimisée et mesurable. Il comprend 300 intégrations prédéfinies et offre des playbooks prêts à l'emploi pour répondre à plus de 180 réglementations mondiales en matière de violation de données et de protection de la vie privée.

- **QRadar SIEM** : le SIEM QRadar d'IBM, leader sur le marché, a été amélioré avec la nouvelle interface unifiée pour les analystes qui fournit des informations et des workflows partagés avec des ensembles d'outils d'opérations de sécurité plus larges. Il offre une détection en temps réel - en tirant parti de l'IA, de l'analyse du comportement du réseau et de l'utilisateur, et des renseignements sur les menaces réelles – conçue pour fournir aux analystes des alertes plus précises, contextualisées et hiérarchisées. IBM prévoit également de rendre le SIEM QRadar disponible en mode as a service sur AWS d'ici la fin du deuxième trimestre 2023.

La suite IBM Security QRadar est disponible dès aujourd'hui via des offres SaaS individuelles. Pour en savoir plus : https://www.ibm.com/qradar

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

À propos d'IBM Security

IBM Security fournit 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 plus de

150 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.ibm.com/fr-fr/about/secure-your-business, suivez IBM Security sur Twitter ou consultez le blog IBM Security Intelligence.

Contacts Presse :

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

Weber Shandwick pour IBM

Louise Weber / Jennifer Tshidibi

Tél. : + 33 (0)6 89 59 12 54 / + 33 (0)6 13 94 26 58

ibmfrance@webershandwick.com

---

[1] Based on IBM's internal analysis of aggregated performance data observed from Managed Security Service engagements with 400+ clients from 2018-2019, which showed that average alert triage timeline was reduced by 55% during the first year using AI and automation capabilities that are now part of QRadar. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided.

[2] Global Security Operations Center Study Results, administered by Morning Consult and commissioned by IBM, March 2023. Based on responses from 1,000 surveyed security operation center professionals from 10 countries.

[3] Based on security product evaluations from external analyst firms including Gartner, IDC, Forrester, KuppingerCole and Omdia, which rank IBM as a leader in 12 security product categories: SIEM, SOAR, Fraud Reduction Intelligence Platform, Risk Based Authentication, Identity Governance and Administration, Access Management, Identity and Access Management as a Service, Access Governance & Intelligence and Identity Governance, Authentication, Customer Identity and Access Management, Data Security, Unified Endpoint Management.

[4] IBM Institute for Business Value report, "AI and automation for cybersecurity," 2022. Results based on IBM analysis of aggregated annual performance data observed from hundreds of global clients using AI and automation capabilities that are now part of QRadar Suite. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided.