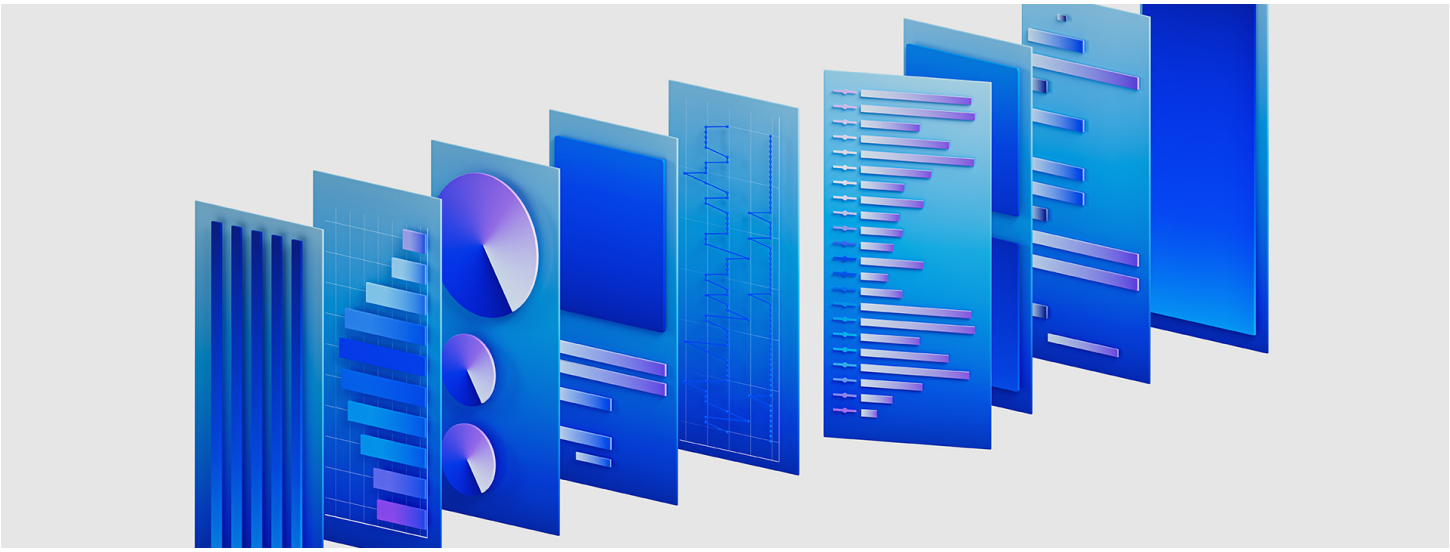
Communiqués de presse

# IBM dévoile un SIEM « Cloud-native » pour optimiser le temps et le talent des équipes de sécurité

**Permet aux analystes de sécurité et à l'IA de travailler côte à côte plus efficacement grâce à un socle modernisé et une expérience utilisateur repensée.**



**ARMONK, N.Y., le 23 novembre 2023** : IBM (NYSE: IBM) a annoncé aujourd'hui une évolution majeure de sa solution phare IBM QRadar SIEM : repensée sur une nouvelle architecture « Cloud-native », conçue spécifiquement pour la performance, la vitesse et la flexibilité du Cloud hybride. IBM a également dévoilé ses projets visant à fournir des capacités d'IA générative au sein de son portefeuille de détection et de réponse aux incidents - en s'appuyant sur watsonx, la plateforme de données et d'IA de la compagnie, conçue pour l'IA d'entreprise.

Les environnements Cloud hybride d'aujourd'hui évoluent et se développent à un rythme exponentiel, créant une surface d'attaque plus vaste et plus complexe à protéger. Cette empreinte informatique croissante rend plus difficile la détection rapide des véritables menaces parmi le bruit - ralentie par des technologies en silos, des recherches manuelles et une surcharge d'alertes, sans contexte ni visualisation clairs. En fait, selon une étude mondiale[1] récente, les professionnels du SOC traitent moins de la moitié (49 %) des alertes qu'ils sont censés examiner au cours d'une journée de travail normale.

Le nouveau SIEM QRadar « Cloud-native » est conçu pour maximiser les capacités des équipes de sécurité d'aujourd'hui. Il est conçu pour augmenter et améliorer le travail quotidien des analystes de sécurité - en exploitant l'IA pour gérer les tâches chronophages et répétitives tout en leur permettant de trouver les menaces hautement prioritaires et d'y répondre de manière plus efficace.

*« Notre nouveau SIEM « Cloud-native » est un élément central de la mission d'IBM visant à inaugurer la prochaine génération d'opérations de sécurité, conçue pour l'ère du Cloud hybride et de l'IA », a déclaré* **Kevin Skapinetz, Vice President, Strategy and Product Management, IBM Security***. « Au lieu de forcer les analystes à contourner la complexité des technologies de sécurité, nous concevons une technologie qui supprime la complexité - en éliminant le bruit, en simplifiant l'expérience utilisateur et en donnant aux analystes les moyens de s'attaquer aux menaces urgentes avec davantage de rapidité et de confiance. »*

Le SIEM «Cloud-native » d'IBM s'appuie sur les 13 années de leadership de QRadar sur le marché et sur la reconnaissance des analystes[2] en matière d'analyse approfondie de la sécurité - avec une architecture repensée pour une ingestion des données très efficace, une recherche rapide et une analyse haute performance. Conçu sur un socle ouvert, c'est le dernier ajout à la suite QRadar (QRadar Suite), le portefeuille intégré de logiciels de détection et de réponse aux incidents d'IBM.

Le nouveau SIEM QRadar « Cloud-native » sera disponible sur le marché en mode SaaS au quatrième trimestre 2023 et il est prévu de le proposer en déploiement sur site et multi-cloud en 2024.

**Ouvert par nature**

Construit sur un socle Red Hat OpenShift, QRadar SIEM est conçu pour être structurellement ouvert - permettant une interopérabilité plus approfondie avec des outils et des Clouds divers. Il s'appuie sur l'open source et les standards ouverts pour les fonctions principales, notamment les règles de détection et le langage de recherche, ce qui lui permet de fonctionner avec les piles technologiques de toutes les entreprises.

- **Exploiter les détections de la communauté cybersécurité** : exploite un langage commun et partagé pour les règles de détection (SIGMA), ce qui permet aux clients d'importer rapidement de nouvelles détections provenant directement de la communauté cybersécurité au fur et à mesure de l'évolution des menaces.
- **Enquêter sur différentes sources de données** : offre des fonctionnalités uniques de recherche fédérée et de traque des menaces (« threat hunting ») basées sur des technologies open-source, permettant aux analystes de rechercher de manière proactive et d'enquêter sur les menaces à travers les sources de données dans le Cloud et sur site de manière unique et unifiée - sans déplacer les données de leur source d'origine.

- **Un réseau de partenaires étendu** : s'appuie sur l'écosystème QRadar, l'un des plus grands réseaux de partenaires du secteur avec plus de 700 intégrations prédéfinies.

**Suite complète pour une réponse de sécurité connectée et proactive**

Dans le cadre de QRadar Suite, le nouveau SIEM « Cloud-native » offre aux clients l'accès à un large éventail de fonctionnalités intégrées qui peuvent permettre une détection, une investigation et une réponse plus proactives à travers des ensembles d'outils. Avec QRadar Suite, les entreprises peuvent gagner en visibilité sur leurs actifs exposés grâce à des capacités de gestion de la surface d'attaque (ASM), rechercher des menaces à travers des ensembles d'outils, protéger le terminal avec un EDR, et se connecter à des playbooks automatisés pour accélérer la réponse (SOAR). QRadar SIEM permet aux utilisateurs de partager des informations et des actions automatisées dans leurs principaux ensembles d'outils - accessibles directement à partir de leur interface utilisateur principale, sans avoir besoin de passer d'un outil à l'autre.

**L'IA conçue pour les entreprises accélère la réponse aux menaces critiques**

QRadar SIEM applique plusieurs couches d'IA et d'automatisation pour améliorer la qualité des alertes et l'efficacité des analystes de sécurité. Ces capacités d'IA matures ont été pré-entraînées sur des millions d'alertes provenant du vaste réseau de clients d'IBM et sont encore affinées après le déploiement pour tenir compte de l'environnement unique de chaque client. A titre d'exemple :

- **Réduire le bruit et améliorer les alertes :** les capacités de hiérarchisation des alertes utilisent l'IA pour supprimer automatiquement les alertes de faible priorité, tout en regroupant, contextualisant et escaladant automatiquement les alertes de haute priorité - en tenant compte du contexte de risque à partir des renseignements sur les menaces en cours et des modèles de réponse des analystes. Cette fonctionnalité a permis à IBM Consulting Cybersecurity Services d'automatiser 85 % de la gestion des alertes pour les clients[3] et d'accélérer leurs délais de tri des menaces de 55 % au cours de la première année d'utilisation[4].

- **Investigations accélérées** : la capacité d'IA exécute automatiquement des recherches fédérées dans les systèmes connectés, générant une chronologie visuelle de l'attaque, des correspondances MITRE ATT&CK et des actions recommandées - donnant aux analystes une avance significative sur les tâches

d'investigation.

- **Mise à jour automatique des détections** : les analyses de QRadar SIEM sont automatiquement et en permanence mises à jour avec de nouvelles règles de détection et des renseignements sur les menaces, afin de suivre l'évolution des ces dernières.

Les fonctionnalités de sécurité de l'IA d'IBM sont intégrées nativement dans l'interface analyste de QRadar Suite, mettant des informations contextuelles à la portée des analystes et les aidant à tirer parti de l'IA de manière plus intuitive au sein de leurs flux de travail habituels.

**L'IA générative au service de la productivité du SOC**

IBM prévoit également de lancer des fonctionnalités de sécurité d'IA générative (GAI) pour QRadar Suite début 2024 - basées sur watsonx, la plateforme d'IA et de données de la compagnie. IBM conçoit l'IA générative pour aider à optimiser le temps et les talents des équipes de sécurité en gérant certaines tâches fastidieuses pour le compte des analystes, tout en leur permettant d'effectuer plus facilement des travaux plus difficiles et à plus forte valeur ajoutée. Par exemple :

- **Automatiser le reporting** : créer des résumés simples des cas et des incidents de sécurité qui peuvent être partagés avec diverses parties prenantes en un seul clic.
- **Accélérer la traque des menaces** : générer automatiquement des recherches pour détecter les menaces sur la base de descriptions en langage naturel du comportement et des modèles d'attaque, ce qui permet d'accélérer la réponse aux nouvelles campagnes de menaces.
- **Interpréter les données générées par les machines** : aider les analystes à comprendre rapidement les données des journaux de logs de sécurité en leur fournissant des explications simples sur les événements qui se sont produits sur un système - en réduisant les obstacles techniques et en accélérant leurs investigations.
- **Analyser les renseignements sur les menaces** : interpréter et résumer les renseignements sur les menaces les plus pertinents, en se concentrant sur les campagnes les plus susceptibles d'affecter les clients en fonction de leur profil de risque unique.

IBM développe également des capacités d'IA générative prédictives qui seront entraînées pour créer des réponses actives qui s'optimisent au fil du temps - par exemple, en aidant l'équipe de sécurité à trouver des

incidents similaires, à mettre à jour les systèmes affectés et à corriger le code vulnérable.

Au-delà de ces cas d'usage, IBM prévoit d'intégrer l'IA générative dans l'ensemble de son portefeuille de logiciels et de services de cybersécurité. Ces capacités s'appuieront sur l'infrastructure watsonx ainsi que sur les modèles d'IA watsonx, qui ont été entraînés sur des ensembles de données sélectionnées et spécifiques à un domaine - conçus pour offrir davantage de confiance, de transparence et de précision.

Pour en savoir plus sur QRadar SIEM, vous pouvez consulter le site suivant :
https://www.ibm.com/products/qradar-cloud-native-siem

Pour en savoir plus sur l'IA pour la sécurité, vous pouvez consulter le site suivant :
https://www.ibm.com/security/artificial-intelligence

*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 aide à sécuriser les plus grandes entreprises et les gouvernements du monde entier grâce à un portefeuille intégré de produits et de services de sécurité, infusé de capacités dynamiques d'IA et d'automatisation. Ce portefeuille, qui repose sur les recherches du mondialement célèbre IBM X-Force®, permet aux organisations de prévoir les menaces, de protéger les données à mesure qu'elles se déplacent et de réagir avec rapidité et précision sans entraver l'innovation commerciale. Des milliers d'organisations font confiance à IBM en tant que partenaire pour l'évaluation, la stratégie, la mise en œuvre et la gestion des transformations en matière de sécurité. 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-03.ibm.com/security/fr-fr/, suivez IBMSecurity sur Twitter ou consultez le blog IBM Security Intelligence.

**Contacts Presse** :

**Weber Shandwick pour IBM**

Louise Weber

**IBM**
Gaëlle Dussutour
Tél. : + 33 (0)6 74 98 26 92

dusga@fr.ibm.com Tél. : + 33 (0)6 89 59 12 54

ibmfrance@webershandwick.com

---

***[1]*** *Global Security Operations Center Study, 2022 conducted by Morning Consult, sponsored by IBM.*

***[2]*** *QRadar has been identified as a market leader for SIEM in multiple third party analyst reports for the past 13 years, including reports from Gartner, Forrester, KuppingerCole, IDC and Omdia.*

[3] *Based on IBM's internal analysis of aggregated performance data observed from engagements with 340+ clients in July 2023. Up to 85% of alerts were handled through automation using AI capabilities that are part of QRadar SIEM. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided.*

[4] *Based on IBM's internal analysis of aggregated performance data observed from 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 part of QRadar SIEM. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided*