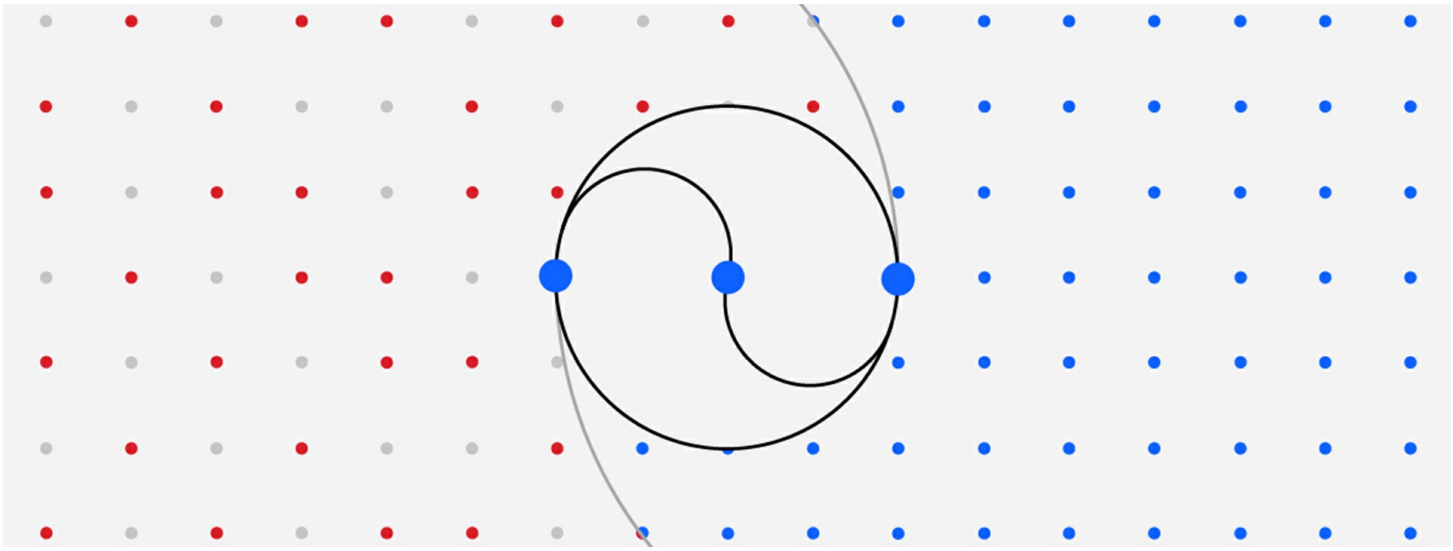
Communiqués de presse

IBM annonce de nouveaux services de détection et de réponse aux incidents alimentés par l'IA

Ingère et analyse les données de sécurité provenant d'un vaste écosystème de technologies et de fournisseurs

Offre une surveillance, une investigation et une remédiation automatisée des alertes de sécurité 24h/24 et 7j/7



ARMONK, N.Y., le 05 octobre 2023 : IBM (NYSE : IBM) a dévoilé aujourd'hui la prochaine évolution de ses offres de services managés de détection et de réponse avec de nouvelles technologies d'IA, notamment la capacité de faire remonter ou de clôturer automatiquement jusqu'à 85% des alertes[1], contribuant ainsi à accélérer les délais de réponse de sécurité pour les clients.

Les nouveaux services de détection et de réponse aux incidents (TDR : Threat Detection and Response Services) assurent la surveillance, l'investigation et la remédiation automatisée, 24h/24 et 7j/7, des alertes de sécurité provenant de toutes les technologies pertinentes présentes dans les environnements Cloud hybrides des clients - y compris les outils et les investissements de sécurité existants, ainsi que les technologies Cloud, sur site et industrielles (OT). Les services managés sont fournis par l'équipe mondiale d'analystes en cybersécurité d'IBM Consulting via la plateforme de services de sécurité avancée d'IBM, qui applique plusieurs couches d'intelligence artificielle et de renseignements contextuels sur les menaces provenant du vaste réseau de sécurité mondial de la compagnie, permettant ainsi d'automatiser l'élimination du bruit tout en escaladant rapidement les menaces critiques.

« Aujourd'hui, les équipes de sécurité sont non seulement submergées par le nombre d'attaquants, mais aussi par le nombre de vulnérabilités, d'alertes, d'outils et systèmes de sécurité qu'elles sont chargées de gérer au quotidien », a déclaré **Chris McCurdy, General Manager, Worldwide IBM Consulting Cybersecurity**

Services. *« En combinant des analyses avancées et des renseignements en temps réel avec l'expertise humaine, les nouveaux services de détection et de réponse aux incidents d'IBM peuvent renforcer les défenses de sécurité des organisations avec une capacité évolutive, en constante amélioration et suffisamment solide pour faire face aux menaces de demain. »*

Adapter intelligemment les défenses contre les menaces

Les nouveaux services TDR s'appuient sur un ensemble de technologies de sécurité alimentées par l'IA qui aident déjà des milliers de clients à travers le monde, en surveillant des milliards d'événements de sécurité potentiels par jour. Ils s'appuient sur des modèles d'IA qui apprennent en permanence à partir des données des clients, y compris les réponses des analystes sécurité, et sont conçus pour clôturer automatiquement les alertes de faible priorité et les faux positifs en fonction d'un niveau de confiance défini par le client. Cette fonctionnalité permet également d'escalader automatiquement les alertes à haut risque qui nécessitent une action immédiate de la part des équipes de sécurité et de fournir un contexte d'investigation.

Les services TDR d'IBM sont conçus pour fournir :

- **Des règles de détection collaborative, des alertes optimisées** . S'appuyant sur des informations en temps réel provenant des engagements d'IBM en matière de gestion des menaces, les nouveaux services utilisent l'IA pour évaluer en permanence et recommander automatiquement les règles de détection les plus efficaces, ce qui permet d'améliorer la qualité des alertes et d'accélérer les temps de réponse. Cette fonctionnalité a permis de réduire de 45 % les alertes SIEM de faible criticité et de remonter automatiquement 79 % des alertes de plus haute criticité nécessitant une attention immédiate. Les organisations peuvent approuver et mettre à jour les règles de détection en seulement deux clics via un portail cogéré.

- **Une évaluation MITRE ATT&CK**. Pour rester prêtes à faire face aux attaques de ransomware et destructives, les organisations pourront voir comment leur environnement couvre les tactiques, techniques et procédures du référentiel MITRE ATT&CK par rapport à leurs homologues sectoriels et géographiques. En utilisant l'IA, les nouveaux services sont conçus pour réconcilier les multiples outils et politiques de détection actuellement en place au sein d'une organisation, offrant ainsi une vue d'entreprise sur la meilleure façon de détecter les menaces et d'évaluer les lacunes à mettre à jour dans un référentiel ATT&CK.

- **Une intégration transparente de bout en bout.** Grâce à leur approche par API ouvertes, les nouveaux services peuvent rapidement s'intégrer aux actifs de sécurité de l'entreprise d'un client, qu'ils soient sur site ou dans le Cloud. Les organisations peuvent continuer à accéder à leur écosystème tout en ayant la possibilité de se connecter, de collaborer et de définir leurs propres plans de réponse par le biais d'un portail cogéré. Cela permet d'avoir une vision unifiée de l'entreprise, de disposer de capacités de remédiation précises et d'appliquer de manière cohérente les politiques de sécurité dans les domaines de l'IT et de l'OT.

- **Une assistance mondiale 24h/24 et 7j/7.** Les entreprises auront accès à plus de 6 000 professionnels d'IBM Cybersecurity Services à travers le monde, 24 heures sur 24, 7 jours sur 7 et 365 jours par an, pour les aider à renforcer leurs programmes de sécurité. Le vaste réseau mondial d'IBM Consulting Cybersecurity Services dessert plus de 3 000 entreprises dans le monde et gère plus de 2 millions de terminaux et 150 milliards d'événements de sécurité par jour.

« Les responsables de la sécurité tentent aujourd'hui d'échapper au cercle vicieux de la pénurie de personnel, de l'augmentation des menaces et des demandes croissantes de la part de la direction pour faire évoluer leur programme de cybersécurité sans se ruiner. Pour de nombreuses organisations, la vieille méthode consistant à remplacer leurs outils par la plateforme à la mode ne fonctionne pas, car elles ne peuvent pas se permettre d'annuler les investissements antérieurs dans les SOC », a déclaré **Craig Robinson, IDC Research VP of Security Services**. *« Un service tel que l'offre de détection et de réponse aux incidents d'IBM peut fournir un échappatoire à ces préoccupations, sans nécessiter un remplacement complet de leurs investissements antérieurs en matière de sécurité et aider à faire évoluer leur capital humain dans le SOC vers un mode plus proactif. »*

Pour soutenir l'amélioration continue des capacités des opérations de sécurité, les services TDR d'IBM, désormais disponibles, comprennent l'accès aux services de réponse aux incidents d'IBM X-Force ainsi que la possibilité d'inclure des services de sécurité proactifs supplémentaires d'IBM X-Force, tels que les tests de pénétration, la simulation d'attaques ou la gestion des vulnérabilités. X-Force fournira également des conseils pour aider les clients à améliorer leurs opérations de sécurité au fil du temps, sur la base du paysage actuel des menaces, de l'évolution de l'environnement informatique des clients et des informations recueillies dans le cadre de projets auprès de milliers de clients d'IBM Cybersecurity Services dans le monde.

Sources supplémentaires

- Pour en savoir plus sur les services IBM TDR, vous pouvez consulter le site https://www.ibm.com/services/threat-detection-response.
- Vous pouvez vous inscrire à un webinaire pour en savoir plus sur les nouveaux services TDR et les défis d'une approche fragmentaire de la détection et de la réponse le **mercredi 1er novembre 2023, à 17h00** ici.

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 :

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

Weber Shandwick pour IBM

Louise Weber

Tél. : + 33 (0)6 89 59 12 54

ibmfrance@webershandwick.com

[1] 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 rather than human intervention, using AI capabilities that are part of IBM's Threat Detection and Response service. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided.