LogRhythm accélère ses capacités de détection des menaces avec les innovations de sa Suite logicielle

Les nouvelles versions de la plateforme SIEM, des solutions NDR et UEBA de LogRhythm améliorent l'efficacité et renforcent la sécurité pour les activités des clients

Boulder, Colorado (États-Unis) — 5 juillet 2022 — LogRhythm, l'entreprise qui aide les équipes responsables des opérations de sécurité à la fois très occupées et en sous-effectif à mener à bien leur mission, jour après jour, a annoncé aujourd'hui le lancement de la version 7.9 de la plateforme LogRhythm SIEM et des mises à jour de LogRhythm NDR et LogRhythm UEBA.

« LogRhythm renforce les équipes de sécurité avec des outils d'analyses intelligentes et de réponses automatisées, afin de réduire leur exposition à la cybersécurité, éliminer les angles morts et neutraliser rapidement les attaques », a déclaré Kish Dill, chef de produit et chargé de clientèle chez LogRhythm. « L'entreprise transforme notre façon de travailler en adoptant une approche centrée sur le client à tous les niveaux de notre organisation. Nous écoutons attentivement nos clients et nous nous engageons à leur fournir des innovations trimestrielles pour résoudre leurs défis quotidiens. Nous savons que les équipes de sécurité n'ont pas de temps à perdre avec des processus longs et des flux de travail inefficaces. Grâce à ces dernières mises à jour, les équipes de sécurité disposeront des outils nécessaires pour améliorer l'efficacité et l'efficicience de leurs opérations, et défendre leur organisation contre les principales menaces actuelles. »

Avec les nouvelles fonctionnalités de LogRhythm 7.9, LogRhythm NDR (anciennement Mistnet NDR) et LogRhythm UEBA (anciennement CloudAI), les équipes de sécurité peuvent surmonter des obstacles quotidiens grâce à l'accélération des réponses aux menaces, à l'amélioration des flux de travail et la simplification des processus, notamment :

Rentabilité accélérée par l'amélioration des flux analytiques

- **Automatisation améliorée avec l'API Admin** : LogRhythm 7.9 améliore l'API Admin en ajoutant des terminaux de gestion de la surveillance du système (LogRhythm SysMon) à la bibliothèque d'API. Les administrateurs SIEM peuvent ainsi se connecter via l'API Admin et gérer l'agent SysMon, et bénéficier ainsi du regroupement automatisé des processus.
- **Expertise embarquée :** LogRhythm réduit les délais de rentabilité du client grâce à sa solution prête à l'emploi LogRhythm SmartResponse™. LogRhythm 7.9 comprend des SmartResponses ajoutées et améliorées à sa bibliothèque déjà très complète de plus de 120 intégrations.
- **Activation de la capture de paquets dans l'interface utilisateur :** Les utilisateurs de LogRhythm NDR peuvent télécharger des fichiers PCAP pour des incidents et des cas spécifiques, afin d'obtenir plus de détails, et renforcer les investigations et la chasse aux menaces.
- **Filtrage des journaux d'événements plus facile et plus rapide** : LogRhythm 7.9 intègre un nouveau mode de filtrage des journaux au niveau de l'agent. Les utilisateurs peuvent

maintenant sélectionner les types de journaux d'événements Windows que l'agent interroge, ce qui accélère le traitement des journaux et soulage le pipeline de collecte.

Capacités étendues de détection des menaces

- **Modèles de détection améliorée LogRhythm NDR :** Les utilisateurs peuvent détecter un plus large éventail d'attaques par ransomware, grâce aux capacités analytiques améliorées de LogRhythm NDR.
- **Modèles d'analyse avancée :** LogRhythm UEBA réunit des capacités analytiques UEBA avancées, dans un module complémentaire cloud natif, facile à déployer pour les utilisateurs de LogRhythm 7.9. Des modèles ont été améliorés et de nouveaux modèles ont été ajoutés afin d'assurer la détection des attaques complexes actuelles et l'identification des anomalies nécessitant une attention prioritaire. Ils réduisent donc la pression exercée par les alertes et les temps de réponse.
- **Alertes des violations de politique** : LogRhythm NDR émet des alertes sur les certificats expirés, les chiffrements faibles utilisés dans les connexions, et les activités d'authentification en clair, élargissant ainsi le contexte et les connaissances sur les potentiels de risques.

Flexibilité étendue

- **Rapports puissants sur le comptage des licences** et les dépassements : LogRhythm bénéficie maintenant d'une nouvelle fonction de rapport qui rend les dépassements de licences plus visibles et plus faciles à comprendre, avec un affichage actualisé des 30 derniers jours. Cette fonction aidera les équipes à mieux gérer l'utilisation et les coûts des licences.
- **Intégrations étendues aux terminaux :** LogRhythm inclut désormais Cisco Secure Endpoint (anciennement AMP for Endpoints) dans sa famille d'intégrations EDR.

Pour en savoir plus sur les solutions de LogRhythm, planifiez une démo avec un expert de LogRhythm.

À propos de LogRhythm

LogRhythm aide les équipes responsables des opérations de sécurité à la fois très occupées et en sous-effectif à mener à bien leur mission, jour après jour. Les professionnels de la sécurité ont une mission capitale : la réputation et le succès de leurs activités, la sécurité des citoyens et des organisations à travers le monde, la sécurité des ressources critiques, la charge de protéger le monde.

LogRhythm vient alléger cette charge. Notre entreprise est en première ligne pour lutter contre les cyberattaques les plus importantes au monde. Elle apporte aux équipes de sécurité les moyens de naviguer en toute confiance dans un paysage de menaces en constante évolution. En tant qu'allié dans ce combat, LogRhythm combine une plateforme opérationnelle de sécurité complète et flexible, des partenariats technologiques et des services de conseil pour aider les équipes SOC à combler les écarts. Avec LogRhythm, votre défense devient plus efficace. Plus d'informations sur logrhythm.com.