jan 30, 2024 10:00 CET

Logpoint lance de nouvelles fonctionnalités pour optimiser les performances en matière de cybersécurité

- **Logpoint améliore sa plateforme Converged SIEM pour aider les entreprises et les MSSP à améliorer leurs performances en matière de cybersécurité et à libérer du temps et des ressources au niveau de la gestion de leurs opérations de sécurité.**
- **La nouvelle version réduit la charge de travail au niveau des tâches opérationnelles, permettant ainsi aux équipes SOC de gagner en efficacité dans la détection, l'investigation et la réponse aux menaces.**

COPENHAGUE et LONDRES, 30 janvier 2023 : Logpoint annonce le lancement de nouvelles fonctionnalités au sein de sa plateforme Converged SIEM, améliorant ainsi la détection des menaces et les opérations de sécurité et rationalisant la gestion des cas. Les entreprises pourront désormais se concentrer sur les problèmes de sécurité véritablement essentiels grâce aux nouvelles fonctionnalités en réduisant la charge de travail, en simplifiant l'automatisation et en libérant des ressources.

La nouvelle version offre une stabilité et une fiabilité accrues au niveau du système ainsi qu'une utilisation plus efficace des ressources en introduisant une gestion adaptative de la mémoire qui optimise automatiquement son utilisation. Cette capacité permet aux utilisateurs d'éviter les interruptions de service et de libérer le temps consacré auparavant au paramétrage manuel de la mémoire. Ils pourront également ajouter plus de nœuds et augmenter la visibilité grâce à la disponibilité de mémoire supplémentaire.

Logpoint améliore l'expérience en matière de configuration des alertes avec une seule fenêtre de visualisation et moins de clics. De plus, la manière avec laquelle les utilisateurs remplissent et mettent à jour les listes a été simplifiée. Désormais, ils pourront télécharger une liste, par exemple, d'IoC, de domaines malveillants, d'adresses IP, etc., dans un fichier .CSV ou .TXT. Cette possibilité offrira aux utilisateurs un moyen flexible d'ajouter des listes provenant de différentes sources, facilitera leur travail et permettra de maintenir la détection des menaces à jour.

Logpoint permet désormais la configuration complète de la phase de collecte en un seul clic à partir des modèles LogSource et permet une mise en œuvre à grande échelle pour les MSSP à partir de Logpoint Director, une plateforme permettant de gérer de vastes déploiements. Cette amélioration facilitera la configuration initiale de Logpoint avec des modèles préconfigurés pour toutes les principales sources de logs.

« La visibilité, le temps de réponse et la confiance dans l'investigation sont des facteurs importants pour repousser avec succès les cyberattaques, et nous sommes ravis d'aider les entreprises à améliorer ces tâches avec cette nouvelle version de Logpoint », a déclaré Edy Almer, Directeur Produits chez Logpoint. « Nous aidons principalement les entreprises à obtenir davantage de ressources pour se concentrer sur ce qui est important pour leur sécurité. Une telle capacité est essentielle car la pression sur les professionnels de la cybersécurité augmente sans cesse en raison du développement permanent

des réglementations au niveau des données et de la cybersécurité en général, mais aussi des méthodes innovantes, en constante évolution, des acteurs malveillants.

Avec cette nouvelle mise à jour, Logpoint rationalise le SOAR (Security Orchestration, Automation and Response) ainsi que la gestion des cas. Par exemple, les artefacts d'incident sont automatiquement extraits dans des cas, ajoutant du contexte, réduisant la charge de travail des analystes et améliorant la détection et la réponse. Les playbooks peuvent lire automatiquement les incidents et ajouter toutes les données extractibles en tant qu'artefacts au cas en question. De plus, les équipes de sécurité peuvent rechercher des logs directement à partir de l'outil de gestion de cas en un seul clic et réintégrer le résultat dans ce dernier, simplifiant ainsi les investigations.

La nouvelle mise à jour permet aux MSSP et à ceux qui travaillent avec différentes entités de gagner du temps et de réduire les erreurs lors de la diffusion des playbooks auprès des clients. Logpoint publie des playbooks génériques liés aux cas d'usage de sécurité courants qui peuvent être mis à jour une fois diffusés auprès des entités. Ces playbooks ne dépendent pas de l'intégration, de sorte que les entités, avec différentes intégrations, pourront en bénéficier. De plus, les MSSP gagneront un temps précieux au niveau de leur processus de diffusion.

Logpoint Converged SIEM est une plateforme de cybersécurité de bout en bout qui couvre l'ensemble du processus TDIR (Threat Detection and Incident Response). La plateforme ajoute automatiquement aux observations des informations sur les menaces, le contexte commercial et les risques au niveau de l'entité pour transformer les signaux faibles en investigations significatives et permet aux analystes de répondre plus rapidement grâce à l'automatisation et à l'orchestration.

Pour en savoir plus sur toutes les mises à niveau et améliorations de la plateforme d’opérations de cybersécurité de Logpoint, visitez le blog de Logpoint ici.

À propos de Logpoint

Logpoint est le créateur d'une plateforme d'opérations de cybersécurité fiable et innovante, permettant aux entreprises du monde entier d’évoluer et se développer dans un monde constitué de menaces en constante évolution. En combinant une technologie sophistiquée et une compréhension approfondie des défis de ses clients, Logpoint renforce les capacités des équipes de sécurité tout en les aidant à lutter contre les menaces actuelles et futures. Logpoint propose les technologies de sécurité SIEM, UEBA, SOAR et SAP convergées dans une plateforme complète qui détecte efficacement les menaces, minimise les faux positifs, priorise les risques de manière autonome, répond aux incidents et bien plus encore. Basée à Copenhague, au Danemark, et possédant des bureaux dans le monde entier, Logpoint est une entreprise multinationale, multiculturelle et inclusive. Pour plus d'informations, visitez https://www.logpoint.com/.

Contacts

Maimouna Corr Fonsbøl
Contact presse
PR Manager
PR & Communications
mcf@logpoint.com
+45 25 66 82 98