LogPoint

SOAR & SIEM nouvelle génération

Une solution de gestion des informations et des événements de sécurité (SIEM : collecte d'événements en temps réel, surveillance, corrélation et analyse des événements à travers des sources disparates.) est un outil essentiel de votre boîte à outils de gestion des risques. Un excellent outil SIEM permet aux entreprises de mieux détecter et répondre aux menaces en fournissant l'analyse des données en temps réel, la détection précoce des violations de données, la collecte, le stockage et un rapport précis sur les données.

Les avantages de l'offre LogPoint

Conformité

LogPoint rationnalise la surveillance des données et la sensibilisation à la sécurité pour garantir la conformité complète avec les exigences réglementaires.

Cybersécurité

Le moteur d'analyse de la sécurité permet aux utilisateurs d'identifier facilement les attaques, de répondre immédiatement et d'établir des rapports efficaces.

Opérations IT

LgPoint améliore l'efficacité opérationnelle en soutenant une approche plus proactive pour comprendre votre réseau et sa connexion au monde.

Business Analytics

Le moteur d'analyse transforme les données structurées provenant d'applications internes et les met en corrélation avec l'intelligence de LogPoint.

Distribué en France par MIEL

01 60 19 34 52 - www.miel.fr/logpoint

Orchestration, automatisation et réponse aux incidents en temps réel

LogPoint vous permet d'évaluer facilement l'état de vos systèmes et de vos applications grâce à la **corrélation** et **l'analyse uniques** de la solution.

Le **moteur intégré d'analyse de logs** détecte et signale automatiquement tous les incidents critiques de vos systèmes. Les événements surveillés peuvent être divers et comprendre une attaque en cours, un système compromis, une panne du système, des problèmes d'authentification de l'utilisateur, etc.

Les données de **log brutes** de vos systèmes peuvent être utilisées pour :

- **Réduire** le **temps de traitement** des problèmes
- **Améliorer** votre **posture de sécurité**
- **Obtenir plus de visibilité** dans l'organisation.
- **Automatiser** les **processus réglementaires**
- **Améliorer** l'**efficacité des investigations** (forensic)

Certifiée EAL3+

Seule solution européenne de SIEM certifiée EAL3+. Norme internationale de certification de logiciel de sécurité. Pour obtenir cette certification, le produit et les processus LogPoint ont été longuement examinés, vérifiés et documentés selon la norme des Critères Communs, également appelée ISO / IEC IS 15408.

UEBA (Apprentissage Automatique)

En utilisant l'apprentissage automatique, l'UEBA LogPoint bâtit des lignes directrices pour chaque entité du réseau, sans créer de règles, ni de signatures prédéfinies. Il agit ainsi comme un multiplicateur de forces pour vos analyses de sécurité en réduisant les règles expertes, les faux positifs et en priorisant les alertes.

LogPoint SOAR

LogPoint SOAR est une solution SOAR (Security Orchestration, Automation & Response) innovante qui apporte, aux entreprises de taille moyenne, efficacité et productivité.

L'intégration transparente avec **LogPoint SIEM** et les **API** ouvertes rend **LogPoint SOAR** très accessible et abordable, fournissant ainsi des solutions indispensables pour réduire les risques en matière de cybersécurité et augmenter la productivité du SOC (Security Operations Center).

Le reporting de cas structurés facilite l'évaluation et la documentation de l'efficacité de LogPoint SOAR et permet de mieux communiquer auprès de l'équipe dirigeante autour de la véritable valeur que représente la sécurité.

Création de valeur métier

LogPoint s'engage à offrir les avantages du SOAR à toutes les entreprises, notamment celles de taille moyenne (les ETI).

LogPoint SOAR offre une valeur immédiate et à long terme en matière de **gestion des risques de cybersécurité** et d'**amélioration de l'efficacité opérationnelle** de la manière suivante :

Réduction du risque de Cybersécurité

L'orchestration automatisée des données et les actions en réponse contiennent et suppriment rapidement les menaces, tout en minimisant le risque d'erreur humaine, allégeant ainsi la charge de l'analyste SOC.

Amélioration de la productivité du SOC

Les playbooks et les workflows permettent d'automatiser les tâches fastidieuses et souvent répétitives, et de guider les analystes vers la bonne décision.

Augmentation de l'efficacité du SOC

SOAR met de l'ordre dans le chaos, en rassemblant tous les cyber-incidents et les données complémentaires en un seul et même endroit.

Une meilleure cyber-intelligence

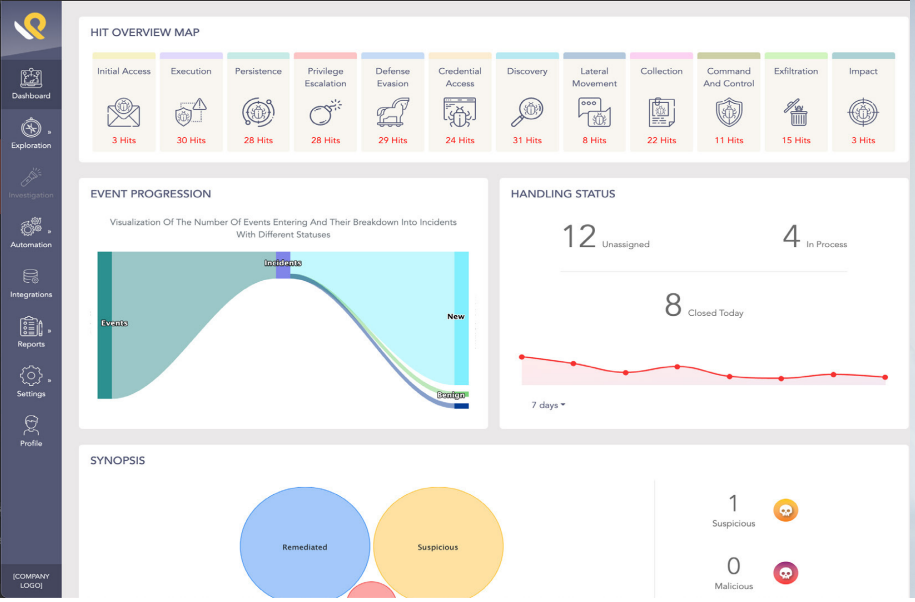
SOAR stocke et priorise les alertes et les données de sécurité provenant de nombreuses sources et systèmes hétérogènes, pour une détection et une réponse plus rapides aux menaces.

Répondre aux besoins des clients

LogPoint SOAR automatise et améliore votre capacité à **détecter**, **investiguer**, **répondre** et **signaler** rapidement chaque cyber-incident. Voici pourquoi les grandes marques choisissent LogPoint SOAR :

Playbooks intégrés

Un ensemble complet de playbooks LogPoint prêts à l'emploi en matière de détection, d'investigation et de réponse vous aide à automatiser immédiatement les processus standard et à les personnaliser facilement.



Time To Value

Les intégrations prêtes à l'emploi et les API ouvertes facilitent une connectivité rapide et transparente à d'autres systèmes de cybersécurité voire d'autres SOAR.

Décisions guidées

SOAR examine automatiquement les données d'alerte de plusieurs systèmes et propose une réponse. Les analystes approuvent ou exécutent simplement cette décision en conscience.

Une culture centrée sur le client

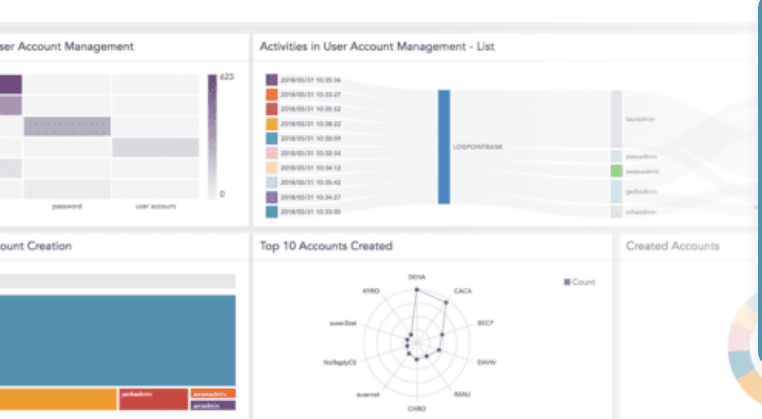
LogPoint repose sur une culture centrée sur le client. Ainsi, nous redoublons d'efforts pour résoudre les problèmes et intégrons régulièrement les suggestions des clients.

Facilité d'utilisation

LogPoint SOAR fait partie intégrante de LogPoint SIEM et est simple à appréhender, pour des profils allant de Junior à Senior.

Les meilleures pratiques

Notre communauté d'utilisateurs et de partenaires LogPoint partage les connaissances au niveau des playbooks.



SCAN ME

Scannez ce **QR Code** et obtenez une estimation de la quantité quotidienne de données ingérées par votre infrastructure.

Un **devis** peut vous peut vous être fourni pour l'estimation.

Distribué en France par MIEL

Appelez le 01 60 19 34 52