Proofpoint Managed SIEM

Renforcez la sécurité de votre environnement Splunk

Principaux avantages

- Détection optimisée pour une visibilité approfondie – Les indicateurs de compromission issus de notre threat intelligence sur les menaces émergentes vous permettent d'identifier les menaces cachées.
- Traque intelligente des menaces pour une réponse proactive – Nous étudions les comportements des cyberpirates et recherchons les preuves de leur présence dans votre environnement. Nous collectons des informations détaillées sur les facteurs contextuels, tels que l'étendue du ciblage, la chronologie et d'autres aspects, afin de favoriser une réponse et une correction proactives.
- Surveillance et détection 24 h/24, 7 j/7 – Nous optimisons rapidement votre environnement. En outre, notre équipe de traque des menaces renforce votre dispositif SIEM grâce à une surveillance continue et un délai moyen de correction réduit.
- Équipe d'ingénieurs en sécurité chevronnés – Notre équipe d'ingénieurs en sécurité figure parmi les meilleures au monde et assure le bon fonctionnement de votre environnement Splunk.

Cette suite de solutions fait partie de la plate-forme Human-Centric Security intégrée de Proofpoint et vise à réduire les quatre catégories clés de risques liés aux utilisateurs.

Proofpoint Managed SIEM vous donne accès à une équipe d'experts entièrement dédiés à la détection, à l'analyse et à la neutralisation des menaces. Ce service offre aux environnements Splunk une protection renforcée contre les menaces. Il vous permet de vous décharger d'une partie de la charge de travail liée à la gestion des événements et des informations de sécurité (SIEM) et d'acquérir des capacités avancées de traque des menaces.

Proofpoint Managed SIEM aide vos équipes informatique et de sécurité des informations à relever les défis quotidiens auxquels elles sont confrontées tandis qu'elles tentent de gérer les importants volumes d'alertes et d'y répondre rapidement. Sans notre service, ces tâches peuvent paraître insurmontables. D'autant que le problème ne fait que s'aggraver avec l'arrivée de nouvelles technologies de détection et la hausse du nombre d'alertes qui va de pair. Cette situation peut entraîner une baisse de vigilance face aux alertes, même si vos équipes suivent les bonnes pratiques et les runbooks, et mettent en œuvre les outils et analyses les plus récents.

Simplifiez les opérations de sécurité

Les clients Splunk qui utilisent Proofpoint Managed SIEM en tirent de nombreux avantages, notamment :

- **Détection améliorée.** Contrairement à d'autres services qui se contentent d'exploiter les alertes fournies par d'autres solutions SIEM, Proofpoint Managed SIEM améliore la détection grâce à la threat intelligence et aux indicateurs de menaces. Cela nous permet d'identifier des menaces qui échappent à d'autres services.
- **Traque des menaces et mise en corrélation.** Notre gamme de solutions de sécurité s'appuie sur de nombreux vecteurs de détection, un graphique des menaces de plus de 1 billion de nœuds basé sur l'apprentissage automatique et l'intelligence artificielle, ainsi qu'une équipe de recherche sur les cybermenaces comptant plus de 100 analystes. L'étendue de notre couverture nous permet non seulement de détecter les menaces, mais également de faire le lien entre des événements qui pourraient sembler sans rapport.
- **Protection contre les menaces 24 heures sur 24, 7 jours sur 7.** Le service Proofpoint Managed SIEM est assuré par une équipe internationale de professionnels de la sécurité et de la détection des menaces. Nos experts sont basés dans des centres d'opérations de sécurité implantés dans le monde entier. Ils identifient, trient et analysent les menaces pour nos clients 24 heures sur 24.

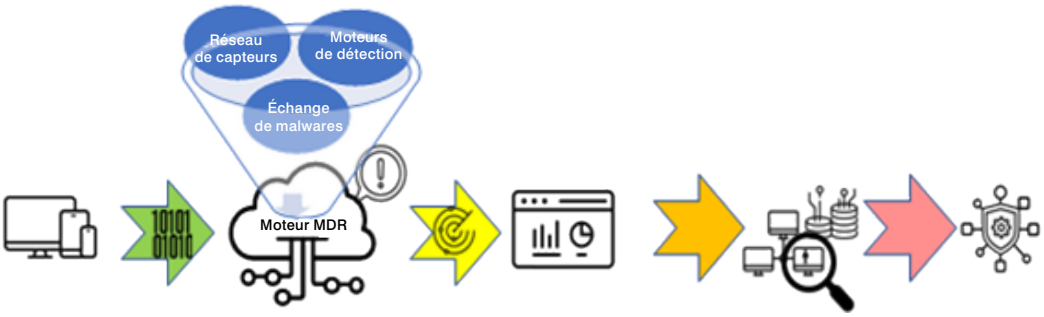

Figure 1. Les sources envoient les journaux au moteur MDR (Managed Detection and Response), qui utilise la threat intelligence de Proofpoint pour créer des alertes optimisées. Notre équipe trie, analyse et hiérarchise les alertes, puis effectue des analyses corrélationnelles et traque les menaces de façon proactive afin de les contenir et de les neutraliser.

Enrichissez les journaux Splunk grâce à la threat intelligence de Proofpoint

La threat intelligence de Proofpoint enrichit les journaux de votre réseau afin d'identifier les menaces qui auraient pu échapper à la détection et de créer de nouvelles alertes Proofpoint. Lorsque des alertes sont émises, nous les trions et les analysons de manière plus approfondie. Les détails des menaces (utilisateurs clés, cibles de grande valeur, modèles d'attaque, etc.) sont identifiés afin de faciliter la hiérarchisation et la neutralisation des attaques. Nous évaluons les menaces en vue de procéder à des traques des menaces avancées, le cas échéant.

L'équipe Proofpoint utilise un workflow d'approbation rationalisé pour neutraliser rapidement les menaces actives. Ce workflow contribue également à libérer les ressources de sécurité de votre entreprise, qui peuvent ainsi se consacrer à des projets de sécurité plus importants ou stratégiques.

Optimisez la détection des menaces au sein de votre entreprise

Proofpoint renforce les fonctionnalités SIEM traditionnelles grâce à une détection avancée basée sur des technologies et services de pointe, offrant ainsi les avantages suivants :

- **Expérience inégalée et expertise proactive.** La threat intelligence de Proofpoint nous permet de vous offrir une protection proactive. Notre réseau mondial de capteurs et notre équipe d'analystes et chercheurs spécialisés dans les menaces assurent la traque des menaces et la corrélation sur un grand nombre de plates-formes. Nos experts sont également tournés vers l'avenir et élaborent des défenses adaptées à vos besoins, basées sur les bonnes pratiques du secteur et les dernières mises à jour des solutions Proofpoint.
- **Opérations de sécurité économiques et continues.** Le recrutement, la formation et la fidélisation du personnel de sécurité constituent un véritable défi. C'est d'autant plus vrai dès lors qu'il est question de connaissances pointues telles que l'identification et la réponse aux incidents. Nos services managés vous donnent accès à notre équipe d'experts, qui sont disponibles en permanence. Vous pouvez ainsi réduire au minimum le temps, l'argent et les ressources nécessaires pour résoudre les problèmes de recrutement localisés.
- **Rapports réguliers et informations de haut niveau destinées à la direction.** Grâce à nos indicateurs, vous disposez d'informations précieuses sur les tendances en matière de sécurité, et pouvez identifier les nouvelles orientations nécessaires en matière de sécurité ainsi que prendre des décisions éclairées.

Proofpoint Managed SIEM intègre toutes ces fonctionnalités afin d'offrir une défense efficace. Notre équipe vous aide à assurer le bon fonctionnement de votre environnement. Nous optimisons en outre la configuration des règles dans Splunk afin de détecter les menaces avec précision. Cela inclut notamment l'implémentation des mises à niveau, des correctifs et des ajustements des systèmes selon les besoins. Nous allions détection avancée, hiérarchisation, neutralisation des menaces prioritaires et mesures de correction rapides. En bref, notre équipe offre des services de pointe en matière d'ingénierie de la sécurité. Laissez-nous vous aider à combler les failles de sécurité et à réduire votre surface d'attaque globale.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.