Secureworks®

FICHE TECHNIQUE

Secureworks® Taegis™ XDR

Une plate-forme Cloud native ouverte qui combine la puissance de l'intellect humain avec des informations issues de l'analytique de sécurité, afin d'unifier la détection et la réponse à l'échelle des points de terminaison, du réseau et des environnements Cloud pour assurer de meilleurs résultats et simplifier les opérations de sécurité.

Lorsque l'analytique de sécurité rencontre l'expertise en intelligence sur les menaces

Avec XDR, vous pouvez prendre en main la sécurité et transformer la manière dont vos analystes en sécurité détectent, analysent et répondent aux menaces à l'échelle de vos points de terminaison, de votre réseau et de votre Cloud.

Créé par des experts affichant plus de 20 années d'expertise en sécurité, XDR vous assure une rentabilité rapide avec des cas d'utilisation de la sécurité prêts à l'emploi qui sont continuellement mis à jour avec l'intelligence sur les menaces fournie par l'unité CTU™ de Secureworks (Secureworks Counter Threat Unit™).

La combinaison de l'analytique de sécurité et de l'expertise en intelligence sur les menaces permet à vos analystes d'identifier avec précision les menaces inconnues et complexes grâce à une analytique avancée, à une investigation et réponse accélérée et à des renseignements collectés à l'échelle de la communauté.

Les menaces modernes exigent une intelligence sur les menaces modernisée

Les menaces évoluent. Du périmètre au Cloud, les données se déplacent dans tous les sens, en quantités inimaginables et à la vitesse de l'éclair. En conséquence, les attaques sont devenues plus sophistiquées et plus difficiles à détecter. Si vous y associez la visibilité limitée du Cloud, les pénuries de personnel et de compétences des équipes de sécurité et l'augmentation des coûts et de la complexité de gestion de systèmes de sécurité disparates, vous pouvez comprendre l'importance d'une intelligence sur les menaces modernisée. À ce titre, les cas d'utilisation de détection par les solutions SIEM passent à côté des menaces avancées et provoquent un afflux de faux positifs qui entraînent un gaspillage des ressources consacrées à y répondre. Vous vous retrouvez à essayer de créer, d'appliquer et de constamment mettre à jour un contenu de sécurité personnalisé dans votre environnement. Pendant ce temps, les cybercriminels continuent à faire évoluer leurs tactiques et se dissimulent derrière le bruit pour agir en toute discrétion.

Taegis XDR a été créé pour relever ces défis. L'intelligence sur les menaces et les détecteurs reposant sur une analytique avancée de XDR sont mis à jour en permanence pour s'aligner sur le paysage des menaces le plus récent. Vous n'avez rien à faire pour que des indicateurs de menaces appropriés soient chargés dans le système ou que les indicateurs obsolètes en soient supprimés.

Pourquoi choisir Taegis XDR ?

Analytique avancée

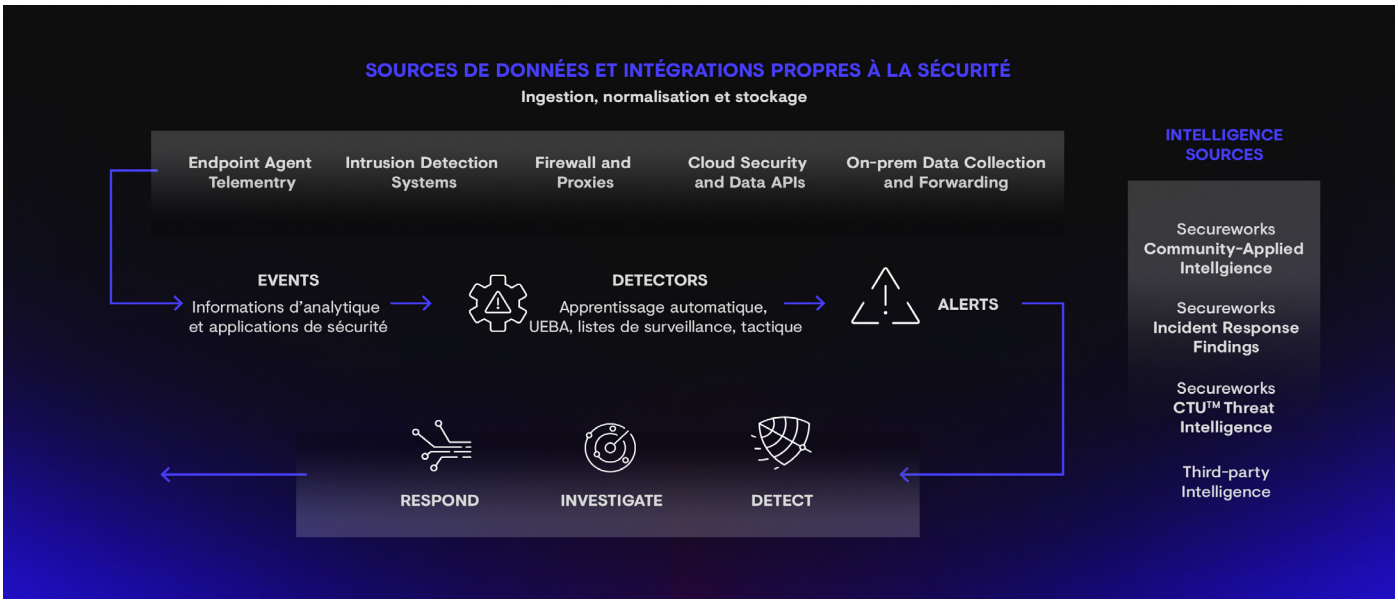
Protégez-vous contre les menaces modernes grâce à l'apprentissage automatique, aux algorithmes de Deep Learning et à l'UEBA

Investigation et réponse accélérées

Bénéficiez d'une analyse approfondie sur les menaces émergentes pour mettre en place une réponse rapide aux attaques

Intelligence appliquée par la communauté

Partagez vos connaissances sur les menaces à l'échelle de toute votre clientèle pour conserver une longueur d'avance sur les nouvelles attaques



L'enrichissement des alertes fourni par l'intelligence sur les menaces de Secureworks, le contexte des entités, la géolocalisation et d'autres données d'enrichissement tierces assurent l'analyse en profondeur des menaces et des intentions et comportements des cybercriminels associés à vos alertes.

XDR offre une valeur tangible en vous permettant de détecter les menaces sophistiquées, de faire confiance à vos alertes, de rationaliser et de collaborer sur les investigations et de répondre rapidement avec assurance.

Détection des menaces sophistiquées

- Reconnaissez vos adversaires en fonction de leur comportement, soyez alerté des menaces connues et émergentes qui pèsent sur votre environnement et rendez rapidement compte à vos supérieurs si votre organisation a été victime dans le passé d'une attaque qui vient d'être découverte.

Alertes fiables

- Réduisez le volume d'alertes sur les menaces en limitant le nombre de faux positifs grâce à une analytique puissante et précise, pour que votre équipe ne voie que les informations exploitables recommandées qui comptent vraiment.

Rationalisation et collaboration

- Donnez à votre équipe les moyens d'être plus efficace en éliminant les silos pour qu'elle puisse partager ses connaissances et ainsi accélérer les investigations et visualiser l'activité des cybercriminels de bout en bout, afin de disposer rapidement d'une chronologie des événements. La fonctionnalité de chat « Demandez à un spécialiste » permet une collaboration en temps réel avec des analystes des intrusions expérimentés.

Réponse en toute confiance

- Soyez assuré de prendre les mesures correctes pour maîtriser une menace et laissez vos experts en sécurité se concentrer sur la sécurité et non sur l'administration de routine de la plate-forme.

Différenciateurs clés

Plus de 20

années de données sur les attaques et les menaces

Plus de 1 400

interventions de réponse aux incidents effectuées l'an passé

Plus de 80

chercheurs dans notre unité Counter Threat Unit™

52 000

base de données de 52 000 indicateurs de menaces uniques, gérée et mise à jour quotidiennement

FICHE TECHNIQUE

Transformer l'efficacité du centre d'opérations de sécurité

Taegis XDR permet à vos équipes chargées des opérations de sécurité de bénéficier d'une visibilité plus étendue pour répondre aux incidents. Avec des fonctionnalités telles que la rétention étendue des journaux, les requêtes de recherche, les rapports définis par l'utilisateur et la prise en charge de cas d'utilisation personnalisés, les analystes bénéficient de capacités accrues d'investigation et de recherche proactive des menaces dans votre environnement. En conséquence, XDR peut facilement remplacer votre solution SIEM actuelle en fournissant des fonctionnalités de détection des menaces avancées, ainsi que d'autres fonctionnalités SIEM permettant d'obtenir des informations exploitables sur les activités malveillantes. Notre objectif est de vous fournir suffisamment de contexte sur l'entreprise et la sécurité pour comprendre une investigation et prendre les mesures appropriées.

Analytique de sécurité avec fonctionnalités SIEM

- Ingérez et conservez en toute fiabilité les événements et les journaux bruts issus de sources de données standard et personnalisées
- Effectuez des recherches rapides et faciles sur les données pour rendre possible une procédure accélérée d'investigation et réponse
- Visualisez les requêtes de données et partagez les informations à l'échelle de votre entreprise avec des rapports flexibles et définis par l'utilisateur
- Personnalisez les alertes pour répondre aux besoins de cas d'utilisation uniques de la sécurité

Avantages de la solution XDR

- Identifiez rétroactivement les activités suspectes dans votre environnement à mesure de l'émergence de nouveaux indicateurs de compromission
- Accélérez la réponse et limitez les dommages avec des réponses optimisées par logiciel pour les cas d'utilisation de l'isolement courants
- Bénéficiez d'une tarification simplifiée fondée sur votre nombre de points de terminaison et qui inclut toutes les données mises en corrélation et contextuelles.*

* Remarque : La tarification XDR inclut un plafond de données par point de terminaison. Les clients qui dépassent ce plafond passent au niveau suivant de leur volume de données.

Pour plus d'informations, composez le **1-877-838-7947** pour parler à un spécialiste en sécurité Secureworks
secureworks.com

À propos de Secureworks
Secureworks® (NASDAQ : SCWX) est un leader mondial en cybersécurité qui protège l'évolution des clients à l'aide de Secureworks® Taegis™, une plate-forme d'analytique de sécurité native Cloud reposant sur plus de 20 ans d'intelligence sur les menaces et de recherche dans le monde réel. Les clients peuvent ainsi mieux détecter les menaces avancées, rationaliser et collaborer sur les investigations, et automatiser les mesures appropriées.