

Services gérés XDR

Secutec SecureSIGHT



Prevent now, secure tomorrow

Éviter l'impact des cyberattaques avec Managed XDR

Alors qu'une solution anti-malware traditionnelle est limitée dans sa capacité à détecter tous les types de menaces modernes, Endpoint Detection & Response (EDR) ne se concentre plus seulement sur les fichiers suspects mais examine également les comportements suspects sur tous les terminaux au sein de votre organisation.

Extended Detection & Response (XDR) est une évolution de l'EDR et fournit une visibilité encore plus complète et en temps réel sur les cybermenaces en **s'intégrant à diverses sources** telles que Secutec SecureDNS, les journaux de pare-feu et les journaux O365, entre autres. En agrégeant toutes ces données supplémentaires, XDR offre une meilleure visibilité, détection et réponse aux menaces.

De cette manière, XDR permet la création d'un centre d'opérations de sécurité (SOC) sur chaque point d'extrémité, pour ainsi dire.



Comment nos services gérés XDR vous protège ?

En proposant XDR en tant que **service géré** au sein de Secutec SecureSIGHT, vous bénéficiez d'une totale tranquillité d'esprit. Notre technologie vous protège jour et nuit et sécurise vos systèmes en temps réel. Nos analystes analysent vos données et interprètent les alertes, vous notifiant les menaces aiguës qui nécessitent que nous examinions ensemble les actions de suivi nécessaires.

Secutec vous conseille sur la mise en œuvre en fonction de vos besoins spécifiques et maintient la configuration pour vous, ce qui vous permet de vous concentrer sur vos défis informatiques internes pendant que nous sécurisons vos frontières numériques.

Intégration avec Secutec SecureDNS

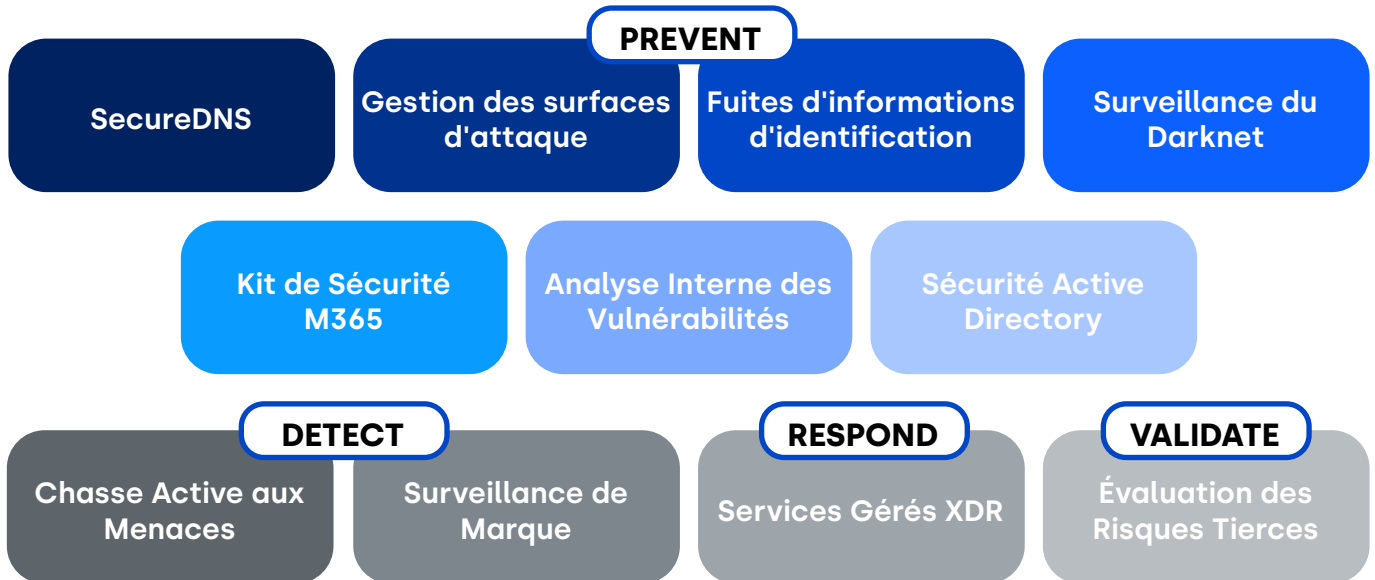
Secutec SecureDNS s'appuie sur **la base de données de logiciels malveillants la plus complète au monde**. Cette base de données Secutec Integrated Advanced Malware Database (SIAM) combine les connaissances et l'expertise des principaux fournisseurs de cybersécurité. En vérifiant les requêtes DNS sortantes par rapport à la SIAM, les domaines malveillants sont automatiquement bloqués, ce qui empêche les virus, les ransomwares et les attaques de phishing de déclencher des charges utiles dangereuses.

L'intégration de SentinelOne XDR avec Secutec SecureDNS permet un **enrichissement bidirectionnel** des deux plateformes et donc une protection encore plus profonde et plus efficace. L'injection de données SecureDNS dans votre solution XDR permet une détection et une réponse encore plus rapides aux nouvelles menaces et cyberattaques. D'autre part, les blocs SecureDNS sont enrichis de données XDR, ce qui permet d'obtenir davantage d'informations sur certaines requêtes bloquées, telles que l'utilisateur et le processus. Cela vous aide à enquêter sur la cause et le contexte des requêtes DNS bloquées.

Surveiller continuellement votre périmètre numérique

Le **service géré** de Secutec SecureSIGHT offre la solution la plus rentable qui couvre les aspects les plus cruciaux du cycle de vie d'une cyberattaque en analysant un large éventail de vecteurs d'attaque et d'indicateurs de compromission. Le **Security Operations Center (SOC)** de Secutec collecte toutes les données sur les attaques possibles, ajoute un contexte aux alertes et vous fournit des données exploitables et des informations interprétées

S'appuyant sur votre infrastructure de sécurité actuelle, Secutec SecureSIGHT présente **11 modules différents** adaptés à vos besoins spécifiques.



MySecutec | Prenez le contrôle de votre sécurité

Le portail MySecutec vous permet d'être plus impliqué dans les résultats de sécurité de votre organisation. Il propose un **tableau de bord clair et intuitif** qui regroupe **toutes les données de sécurité essentielles en un seul endroit**, telles que les actifs, les rapports, les menaces et les risques acceptés.

Grâce à des informations exploitables, vous pouvez rapidement identifier, prioriser et traiter les vulnérabilités les plus critiques, suivre les niveaux de risque des actifs et assurer un suivi des menaces avec des notes intégrées, des filtres et des options d'exportation. Des alertes en temps réel pour les menaces critiques sont envoyées par e-mail, garantissant que vous êtes toujours informé et en mesure d'agir immédiatement.

Votre hub de sécurité, toujours à portée de main

Secutec lancera bientôt la nouvelle application MySecutec, rendant votre cybersécurité accessible à tout moment, où que vous soyez.

- Accès immédiat à vos données de cybersécurité
- Alertes en temps réel pour les vulnérabilités critiques
- Données en direct sur votre score de sécurité, les menaces et les risques
- Surveillez et gérez les violations d'identifiants en un coup d'œil

