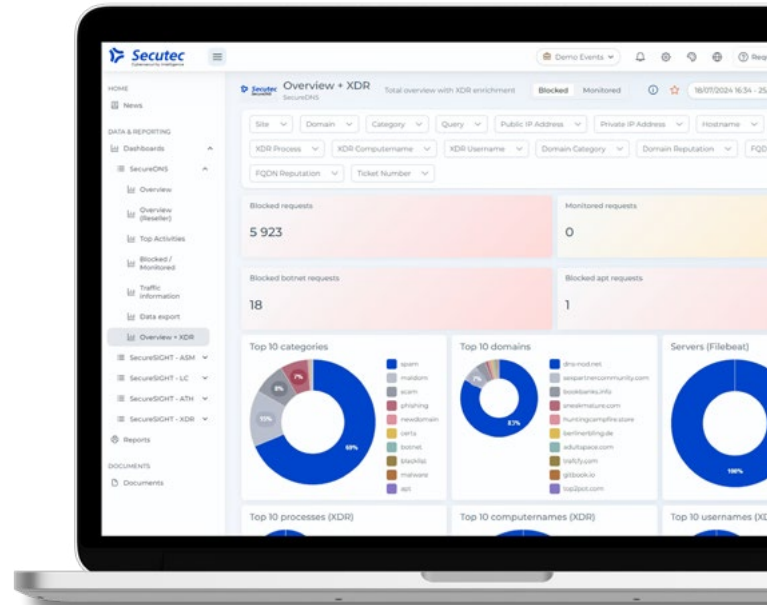


Intégration de SecureDNS avec XDR

Dans le paysage en constante évolution de la cybersécurité, il est crucial de toujours garder une longueur d'avance sur les cybermenaces. L'intégration de notre solution SecureDNS avec SentinelOne et Sophos XDR (Extended Detection and Response) établit une nouvelle norme en matière de cyber-résilience avancée.

L'injection des données SecureDNS dans votre solution XDR permet une détection et une réponse encore plus rapides aux nouvelles menaces et cyberattaques.

L'intégration de SentinelOne XDR est même bidirectionnelle. 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. Secutec SecureDNS peut être intégré à XDR de SentinelOne en tant que service géré ou en tant que solution autonome, selon vos besoins.



Une vision et une compréhension plus approfondies des menaces



Automatisation complète pour une meilleure efficacité opérationnelle



Une meilleure hiérarchisation des incidents de sécurité



Une détection et une réponse plus rapides aux menaces émergentes



Des réponses plus efficaces aux cyberattaques

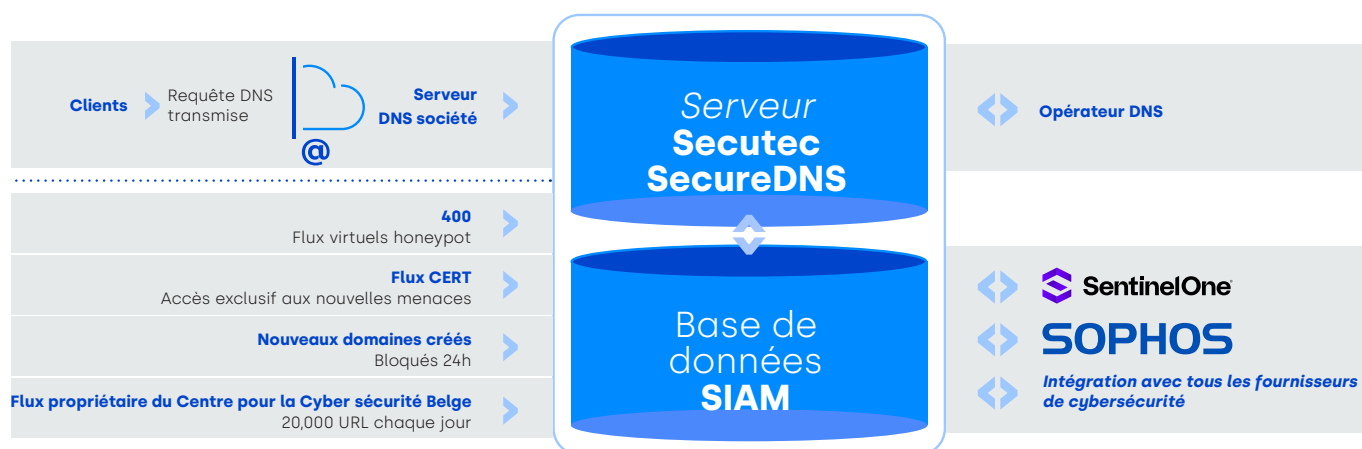


Date [1]	DNS Category [1]	DNS Query [1]	Client Name [1]	Public IP Address [1]	Site Name [1]	Private IP Address	Hostname	Server (Filebeat)	XDR Process	XDR Computer Name	XDR Username	Domain Category	Domain Reputation
30/07/2024 07:00:02	spam	sync.dns.nod.net	demo_events	1.2.3.4	hq	192.168.1.2	Laptop_XYZ	Server_XYZ	C:\PROGRAM FILES\Google\Chrome\Application\chrome.exe	Laptop_XYZ	DemoEvent\John.Doe		
30/07/2024 06:58:54	scam	linkwellthelocom	demo_events	1.2.3.4	hq	192.168.1.2	Laptop_XYZ	Server_XYZ	C:\PROGRAM FILES\Google\Chrome\Application\chrome.exe	Laptop_XYZ	DemoEvent\John.Doe	Adult and Pornography	56
30/07/2024 06:58:44	phishing	at5inc-100265weeblysite.com	demo_events	1.2.3.4	hq	192.168.1.2	Laptop_XYZ	Server_XYZ	C:\PROGRAM FILES\Google\Chrome\Application\chrome.exe	Laptop_XYZ	DemoEvent\John.Doe	Computer and Internet Info	69
30/07/2024 06:58:41	scam	linkwellthelocom	demo_events	1.2.3.4	hq	192.168.1.2	Laptop_XYZ	Server_XYZ	C:\PROGRAM FILES\Google\Chrome\Application\chrome.exe	Laptop_XYZ	DemoEvent\John.Doe	Adult and Pornography	56
30/07/2024 06:58:37	phishing	at5inc-100265weeblysite.com	demo_events	1.2.3.4	hq	192.168.1.2	Laptop_XYZ	Server_XYZ	C:\PROGRAM FILES\Google\Chrome\Application\chrome.exe	Laptop_XYZ	DemoEvent\John.Doe	Computer and Internet Info	69

Records 1 to 50 of 7570 in total

Les requêtes bloquées peuvent être surveillées sur le portail Secutec (pour les clients Secutec SecureDNS uniquement).

Comment fonctionne la base de données SIAM ?



La Secutec Integrated Advanced Malware Database (SIAM) est une base de données de renseignements sur les cybermenaces qui rassemble des données provenant de milliers de sources. C'est le cœur battant de la solution Secutec SecureDNS et elle est mise à jour 24/7/365 pour protéger les utilisateurs des menaces avant qu'elles ne deviennent dangereuses. **En comparant les requêtes DNS sortantes à la base de données SIAM, les domaines malveillants sont automatiquement bloqués. Cela empêche les virus, les ransomwares et les attaques de phishing d'activer des charges utiles dangereuses.**

Le saviez-vous ?

91 % des logiciels malveillants s'appuient sur la résolution DNS.

A propos de SecureDNS

Secutec SecureDNS améliore la sécurité des réseaux d'entreprise en détectant et en bloquant les domaines non détectés par les solutions anti-spam, pare-feu et proxy existantes. Il empêche les connexions aux sites malveillants et ajoute ainsi une couche supplémentaire de protection contre les logiciels malveillants, le phishing et d'autres cybermenaces.

- Solution multifournisseur abordable
- Surveillance et alertes automatiques
- Personnalisable
- Tableau de bord des rapports
- Déploiement facile en moins de 60 minutes
- Compatible avec tous les systèmes



CYBERSECURITY
MADE IN EUROPE