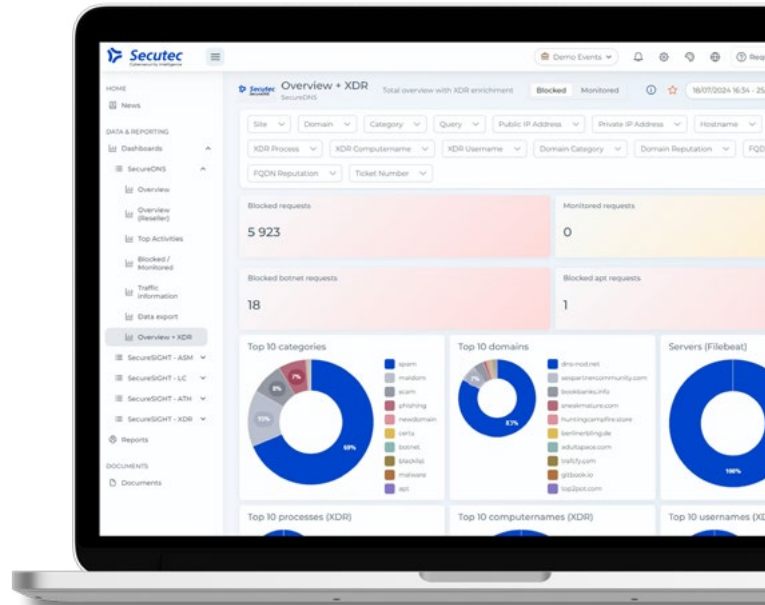


SecureDNS integratie met XDR

In het steeds veranderende landschap van cyberbeveiliging is het van cruciaal belang om cyberdreigingen steeds een stap voor te blijven. De integratie van onze SecureDNS-oplossing met SentinelOne en Sophos XDR (Extended Detection and Response) zet een nieuwe standaard voor geavanceerde cyberweerbaarheid.

Uw XDR-oplossing injecteren met SecureDNS-gegevens zorgt voor een nog snellere detectie en reactie op nieuwe bedreigingen en cyberaanvallen.

De integratie van SentinelOne XDR is zelfs bidirectioneel. SecureDNS-blokkeringen worden verrijkt met XDR-gegevens, waardoor meer informatie beschikbaar komt over bepaalde geblokkeerde query's, zoals de gebruiker en het proces. Deze helpt u de oorzaak en context van geblokkeerde DNS-query's te onderzoeken. Secutec SecureDNS kan geïntegreerd worden met SentinelOne's XDR als een managed service of als stand-alone oplossing, afhankelijk van uw behoeften.



Een meer
diepgaande
inzicht en begrip
van bedreigingen



All-round
automatisering
voor betere
operationele
efficiëntie



Betere prioritering
van beveiligings-
incidenten



Snellere detectie
en reactie op
opkomende
bedreigingen



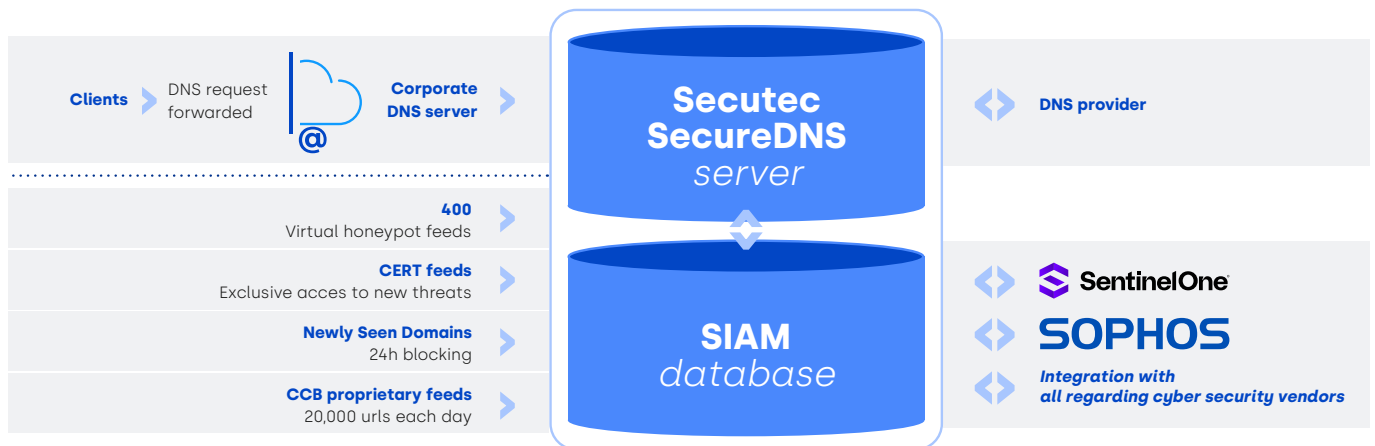
Effectievere
reacties op
cyberaanvallen



Queries														
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	linkwelltheloc.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	Adult and Pornography	56	
30/07/2024 06:58:44	phishing	at5inc-100263weeblysite.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	linkwelltheloc.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	Adult and Pornography	56	
30/07/2024 06:58:37	phishing	at5inc-100263weeblysite.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	
Showing 6 of 6 queries														
Records 1 to 50 of 7570 in total														

Geblokkeerde query's kunnen worden gemonitord op het Secutec-portal (alleen voor Secutec SecureDNS-klanten)

Hoe werkt de SIAM database?



De Secutec Integrated Advanced Malware Database (SIAM) is een database met informatie over cyberbedreigingen die data uit duizenden bronnen samenbrengt. Het is het kloppende hart van de Secutec SecureDNS oplossing en wordt 24/7/365 bijgewerkt om gebruikers te beschermen tegen bedreigingen voordat ze gevaarlijk worden. **Door uitgaande DNS-verzoeken te vergelijken met de SIAM-database, worden schadelijke domeinen automatisch geblokkeerd. Hierdoor krijgen virussen, ransomware en phishingaanvallen geen kans om gevaarlijke payloads te activeren.**

Wist u dat...

91% van alle malware vertrouwt op DNS-resolutie.

Over SecureDNS

Secutec SecureDNS verbetert de beveiliging van bedrijfsnetwerken door het detecteren en blokkeren van domeinen die niet opgemerkt worden door bestaande anti-spam, firewall en proxy-oplossingen. Het voorkomt verbindingen met schadelijke sites en voegt dus een extra beschermingslaag toe tegen malware, phishing en andere cyberbedreigingen.



- Betaalbare multi-vendor oplossing
- Automatische monitoring en waarschuwingen
- Aanpasbaar
- Rapportagedashboard
- Eenvoudige implementatie in minder dan 60 minuten
- Systeem agnostisch