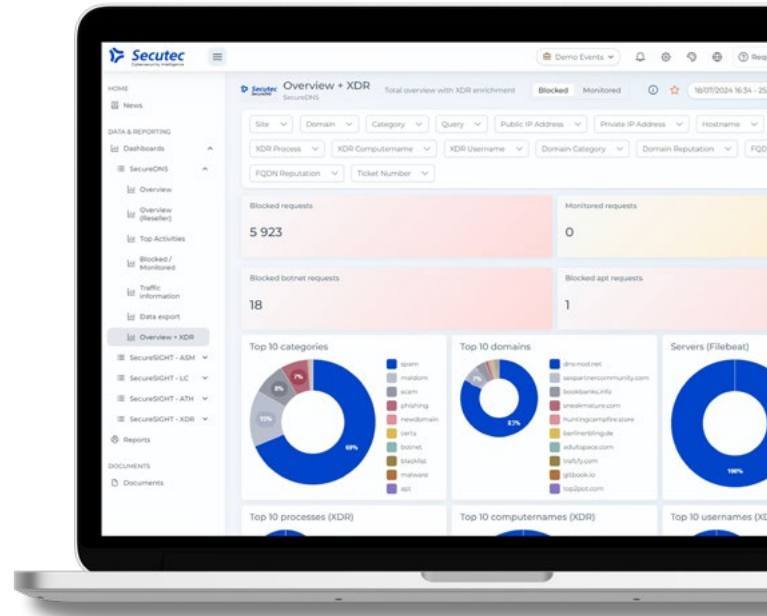


SecureDNS integration with XDR

In the ever-evolving landscape of cybersecurity, staying ahead of cyber threat actors is crucial. The integration of our SecureDNS solution with SentinelOne and Sophos XDR service (Extended Detection and Response) sets a new benchmark for advanced cyber resilience.

Injecting your XDR solution with SecureDNS data enables even faster detection and response to new threats and cyber attacks.

The integration of SentinelOne XDR is even bi-directional. SecureDNS blocks are enriched with XDR data, making more information available about certain blocked queries, such as the user and process. This helps you to better investigate the cause and context of blocked DNS queries. Secutec SecureDNS can be integrated with SentinelOne's XDR as a managed service or stand-alone solution depending on your needs.



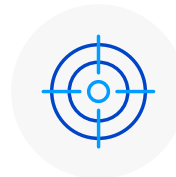
A more in-depth view and understanding of threats



All-around automation for better operational efficiency



Greater prioritization of security incidents



Faster detection and response to emerging threats



More effective responses to cyberattacks

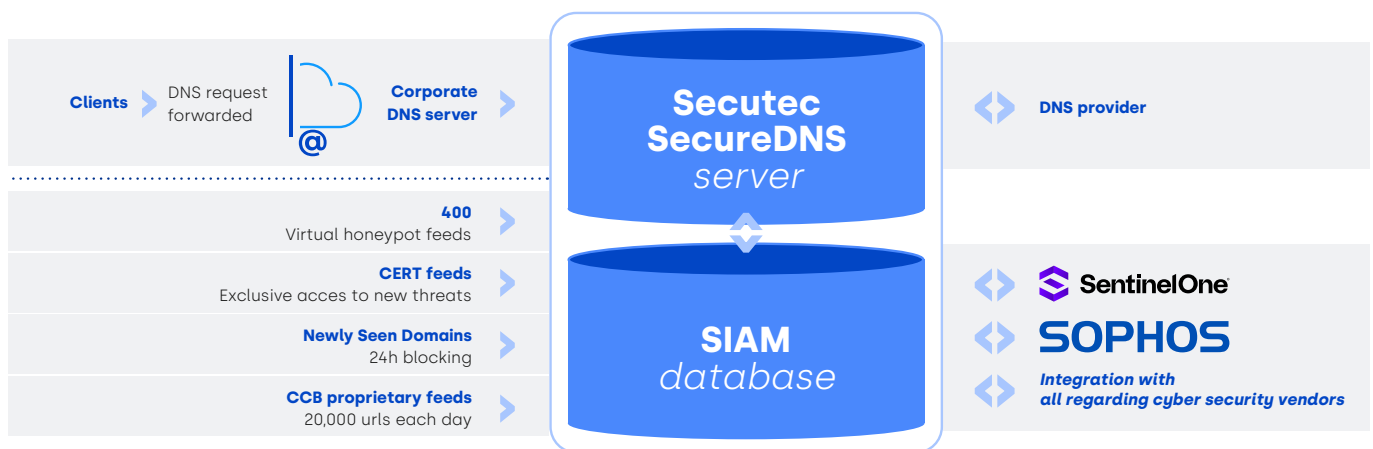


Date [1]	DNS Category [1]	DNS Query [1]	Client Name [1]	Public IP Address [1]	Site Name [1]	Private IP Address	Hostname	Server (Filebeat)	XDR Process	XDR Computer Name	XDR Username	Domain Category	Domain Reputation
30/07/2024 07:00:02	spam	sync.dns.nod.net	demo.events	1.2.3.4	hq	192.168.1.2	Laptop_XYZ	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-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	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-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

Blocked queries can be monitored on the Secutec portal (for Secutec SecureDNS customers only)

How does our SIAM database work?



The Secutec Integrated Advanced Malware Database (SIAM) is a cyber threat intelligence database that brings together information from thousands of sources. It is the beating heart of the Secutec SecureDNS solution and is updated 24/7/365 to protect users from threats before they become dangerous. **By checking outgoing DNS requests against the SIAM database, malicious domains are automatically blocked, giving viruses, ransomware and phishing attacks no chance to trigger dangerous payloads.**

Did you know...

91% of all malware relies on DNS resolution.

About SecureDNS

Secutec SecureDNS enhances corporate network security by detecting and blocking malicious domains missed by existing anti-spam, firewall, and proxy solutions. It prevents connections to harmful sites, adding an additional safety layer and thereby protecting against malware, phishing, and other cyber threats.

- Affordable multi-vendor solution
- Automatic monitoring and alerting
- Customizable
- Reporting dashboard
- Easy implementation in less than 60 min.
- System agnostic

