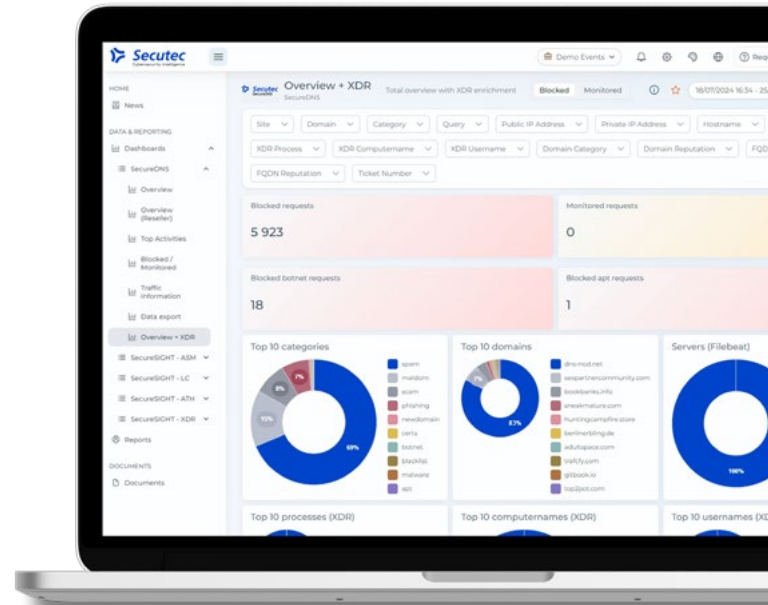


SecureDNS-Integration mit XDR

*In der sich ständig weiterentwickelnden Cybersicherheitslandschaft ist es von entscheidender Bedeutung, den Akteuren von Cyberbedrohungen immer einen Schritt voraus zu sein. Die **Integration unserer SecureDNS-Lösung mit SentinelOne und dem Sophos XDR-Service (Extended Detection and Response)** setzt neue Maßstäbe für erweiterte Cyber-Resilienz*

Die Integration von SecureDNS-Daten in Ihre XDR-Lösung ermöglicht eine noch schnellere Erkennung und Reaktion auf neue Bedrohungen und Cyberangriffe.

Die Implementierung von SentinelOne XDR ist sogar bidirektional. SecureDNS Blocks werden mit XDR-Daten angereichert, wodurch mehr Informationen über bestimmte blockierte Abfragen zur Verfügung stehen, z. B. über den Benutzer und den Prozess. Dies hilft Ihnen, die Ursache und den Kontext von blockierten DNS-Anfragen besser zu analysieren. Secutec SecureDNS kann je nach Bedarf als verwalteter Dienst oder als eigenständige Lösung in SentinelOne's XDR integriert werden.



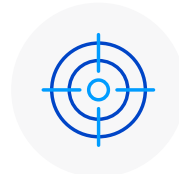
Eingehendere Betrachtung und besseres Verständnis von Bedrohungen



Umfassende Automatisierung für mehr betriebliche Effizienz



Stärkere Priorisierung von Sicherheitsvorfällen



Schnellere Erkennung und Reaktion auf neue Bedrohungen



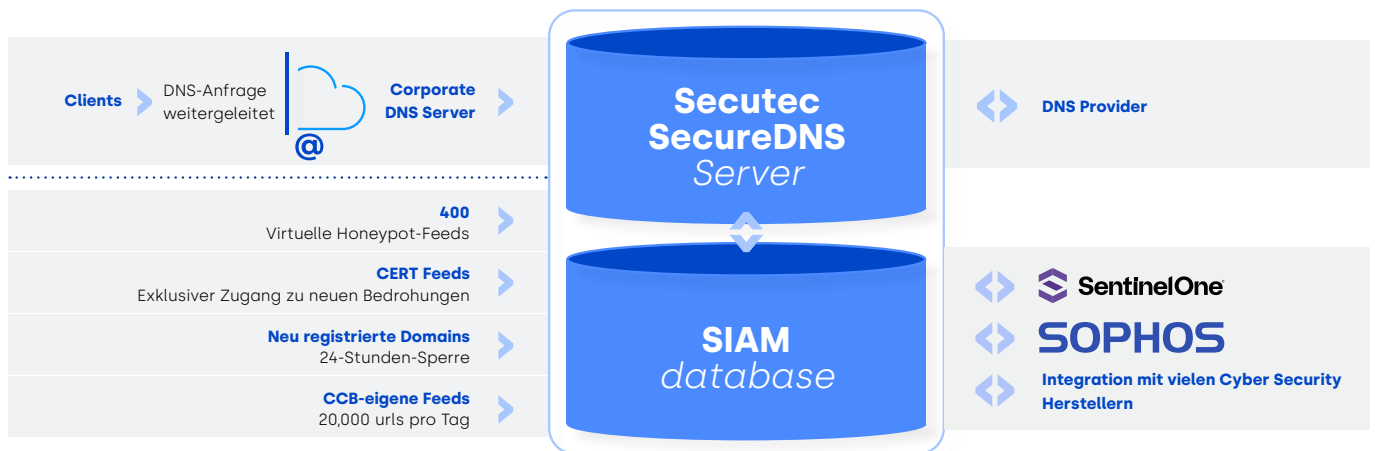
Wirksamere Reaktionen auf Cyberangriffe



Date []	DNS Category []	DNS Query []	Client Name []	Public IP Address []	Site Name []	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-100252weeblysite.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-100252weeblysite.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

Blockierte Anfragen können auf dem Secutec-Portal überwacht werden (nur für Secutec SecureDNS-Kunden)

Wie funktioniert unsere SIAM-Datenbank?



Die Secutec Integrated Advanced Malware Database (SIAM) ist eine Cyber-Bedrohungsdatenbank, die Informationen aus Tausenden von Quellen zusammenführt. Sie ist das Herzstück der Secutec SecureDNS Lösung und wird rund um die Uhr aktualisiert, um Benutzer vor Bedrohungen zu schützen, bevor sie gefährlich werden. **Durch den Abgleich ausgehender DNS-Anfragen mit der SIAM-Datenbank werden bösartige Domains automatisch blockiert, so dass Viren, Ransomware und Phishing-Angriffe keine Chance haben, gefährlich zu werden.**

Wussten Sie schon...

91 % aller Malware basiert auf der DNS-Auflösung.

Über SecureDNS

Secutec SecureDNS erhöht die Sicherheit des Unternehmensnetzwerks, indem es bösartige Domains erkennt und blockiert, die von bestehenden Anti-Spam-, Firewall- und Proxy-Lösungen übersehen werden. Es verhindert Verbindungen zu schädlichen Websites, fügt eine zusätzliche Sicherheitsebene hinzu und schützt so vor Malware, Phishing und anderen Cyber-Bedrohungen.

- Kostengünstige Multi-Vendor-Lösung
- Automatische Überwachung und Alarmierung
- Anpassbar
- Portal-Dashboard
- Einfache Implementierung < 60 Min.
- Systemunabhängig

