
Secutec
Cyber security intelligence

Mythos Darknet, Hacker & Co.

Secutec
Cyber security intelligence

Geert Baudewijns
CEO & Founder

Cyber Security Technologie seit 2005 sowie Erfahrungen aus hunderten Incident Response Fällen, Verhandlungen mit Cyberkriminellen und Lösegeldzahlungen.


Secutec
Cyber security intelligence
Secutec wurde 2005 gründete mit der Vision, weltweites Wissen über Bedrohungen in einer Technologie zu bündeln.
Cyber Security = Multi-Vendor-Strategie


Datenquelle 1:
Antivieren- und Firewall Hersteller Feeds
Globale Security Hersteller Feeds aus den Bereichen Spam, Malware, Phishing, Scam, Botnet, APT, sowie neu registrierte Domains.
Datenquelle 2:
Threat Intelligence Feeds
Globale hochspezialisierte Threat Intelligence Feeds aus den Bereichen Attack Surface Management, Darknet Monitoring, Netflow Daten
Datenquelle 3:
CERT und Geheimdienst Feeds
Behörden Datenquellen in den Bereichen IOC, APT, Botnet, Darknet Investigation und Threat Actors News
Datenquelle 4:
Secutec Hunting Feed
Cyber Bedrohungen, die durch Checks von Secutec erkannt und an Behörden und Partner weitergegeben werden
Secutec
Cyber security intelligence
SIAM Datenbank

Secutec
Cyber security intelligence

secureDNS

Secutec Plattform zur Analyse und effizientem Schutz des DNS-Datenverkehr.

secureSIGHT

Cyber Threat Intelligence Plattform zum permanenten Monitoring von Cyber Risiken.

secureRESPONSE

Hochspezialisierter Incident Response Service von der Forensik bis hin zur Verhandlungsführung mit Hackern.

Secutec
Cyber security intelligence

Externe Sicht

Secutec Managed-Services fokussieren auf die Sicht eines externen Angreifers/Hackers.

24/7 Monitoring DNS- und IP-Datenverkehr

24/7 Darknet Monitoring

24/7 Vulnerability Monitoring

Kunde + SOC + IT-Partner

Interne Sicht

Ihr IT-Team / Dienstleister haben die interne Sicht auf Ihre Infrastruktur.

“Darknet & Co.”

Secutec
Cyber security intelligence

ClearWeb, DeepWeb, Darknet ...

Wieviel Prozent der weltweiten Internetseiten erkennt Google bzw. machen das uns bekannte Internet aus?

Secutec
Cyber security intelligence

4%

Clear Web

-Internet, wie wir es kennen
-Sichtbar für alle Benutzer
-Erreichbar über Google & Co.

96%

Deep Web

-Zugriffsbeschränkte oder nicht indexierte Webseiten
-Datenbanken, Webseiten und Dienste von Regierungen, Organisationen oder Universitäten

Darknet

-Über “normale” Wege nicht auffindbare Webseiten
-Verschlüsselte Kommunikation
-Betreiber und Besucher möchten anonym bleiben
-Illegaler Inhalt, politischer Protest, geheime Kommunikation

Russisches Darknet

Persisches Darknet

Englisches Darknet

Chinesisches Darknet

Rund 150 bekannte Schwarzmärkte – 2,2 Mio. tägliche Darknet User

VON SPIONEN ENTTARNT

Österreicher buchten Auftragsmörder im Darknet

Österreich | 27.07.2023 06:00

Killer bestellt: 2000 Euro extra für qualvollen Tod

Seine Ex-Frau solle besonders leiden, ihre Leiche zerstückelt werden. Dafür wollte ein Wiener 9000 Euro im Darknet zahlen.

Mord per Mausklick: Über versteckte Internet-Foren im Darknet bestellten zwei Männer Auftragsmörder für ihre Ex-Ehefrauen. Auch der britische Geheimdienst und das FBI halfen beim Vereiteln der Bluttaten. Beiden droht lebenslange Haft. Die Hintergründe.

Wiener wollte im Darknet Auftragsmörder für Ex-Frau bestellen

Der 32-Jährige soll den Auftragsmörder auch bereits bezahlt haben. Er fiel jedoch auf eine Fake-Website herein und es kam nicht zum Mord

“Die Welt der Hacker”


Secutec
Cyber security intelligence
Wieviel Prozent
von 100 Unternehmen
könnte einer der besten
Hacker in Europa hacken?


Secutec
Cyber security intelligence
100%
Schlecht gesicherte Unternehmen in 2 Minuten und 2 Jahre unerkannt.
Sehr gut gesicherte Unternehmen in 2 Jahre und 2 Minuten unerkannt.

Wirtschaftlichen Hacker Gruppen

Lockbit, BlackCat, Play, …

Weltweit 80 professionelle Hacker Gruppe, die Unternehmen angreifen, um Lösegeld zu erpressen.

Die Top Organisation erpressen im Jahr teilweise bis zu 100 Mio. USD Lösegelder.

ZIELE: Lösegeld erpressen von Unternehmen und Organisationen

Politischen Hacker Gruppen

APT28 – FanyBear
- Dt. Bundestag - Angela Merkel
- US Wahlkampf – Hillary Clinton
- OPCW - Syrien, Sergej Skripal

Einheit 74455 – Sandworm
- Ukraine – Stromversorgung
- NTC Vulkan – Software Hersteller

ZIELE: Destabilisierung durch Falschinformationen, Zensur, Durchsetzung Eigeninteressen

Einzelhacker und politisch motivierte Gruppen

Anonymous
Hacktivismus - als Protestmittel, um politische und ideologische Ziele zu erreichen.

NoName057(16), Killnet
Pro russische Hackergruppen, die gezielt westliche Organisationen angreifen.

ZIELE: Politische und Ideologische Ziele erreichen, Privatpersonen

Cybergang Lockbit entschuldigt sich für Angriff auf Kinderkrankenhaus

Lockbit-Regelverstoß

Zum Jahreswechsel hat die Lockbit-Cybergang das Entschlüsselungstool für das Krankenhaus kostenlos freigegeben und sich für den Angriff entschuldigt. "Wir entschuldigen uns in aller Form für den Angriff auf sickkids.ca und geben den Decryptor kostenlos heraus. Der Partner, der dieses Krankenhaus angegriffen hat, hat gegen unsere Regeln verstoßen, ist blockiert und ist nicht mehr in unserem Partnerprogramm", schreiben die Cyberkriminellen auf ihrer Darknet-Webseite. Lockbit bietet Ransomware-as-a-Service an, ein kriminelles Geschäftsmodell.

lockbitapt2d73krlbewgv27tquljgxr3

Mit DuckDuckGo suchen oder Adresse eingeben

THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.

NCA National Crime Agency

ROCU

METROPOLITAN POLICE

EUROPOL

POLITIE

Kanton Zürich

SH Schleswig-Holstein

POLIISI

POLICE

FILES ARE PUBLISHED

Deadline: 29 Nov, 2022 22:26:02 UTC

continental.com

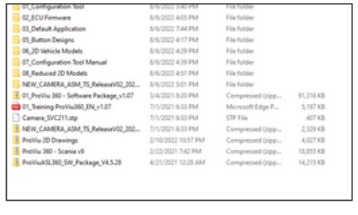
Wolfgang Reitzle was a very greedy man, so we are ready to sell 40 terabytes of the company's private information in one hand for just 40 million dollars, with a list of stolen files you can read here.

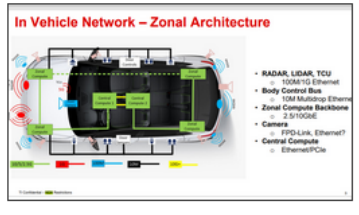
ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 02 NOV, 2022 15:45 UTC UPDATED: 07 APR, 2023 18:37 UTC

EXTEND TIMER FOR 24 HOURS	DESTROY ALL INFORMATION	DOWNLOAD DATA AT ANY MOMENT
$ 100	$ 40000000	$ 40000000

1-4 of 4





Cyber-Risiken Trends

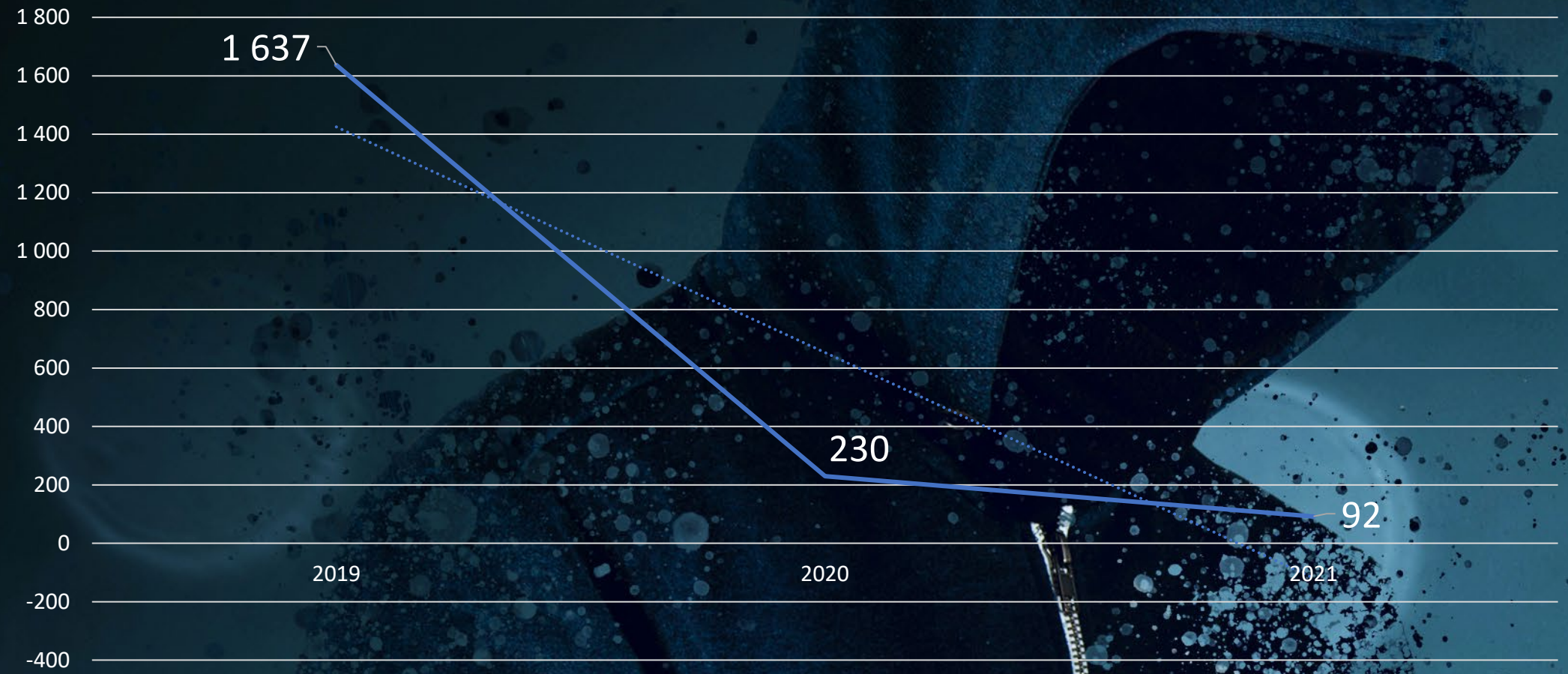
- Supply-Chain-Attacken
- Deep Fake (KI) / Deep Fake Audio-/Visuals
- Professionelle/Trendy Phishing Attacken
- Geopolitische Konflikte – Wiper Funktionalität
- Cyber-War-Klauseln in Versicherungsverträgen
  Geringe Deckungssummen
- 3,5 Mio. fehlende Cybersecurity Spezialisten


Secutec
Cyber security intelligence
“Ransomware Attacke”


Secutec
Cyber security intelligence
Wie viele Stunden benötigen Hacker 2021 von der Schwachstelle bis zur Verschlüsselung?
2019 waren es 1.637 Stunden oder 68 Tage

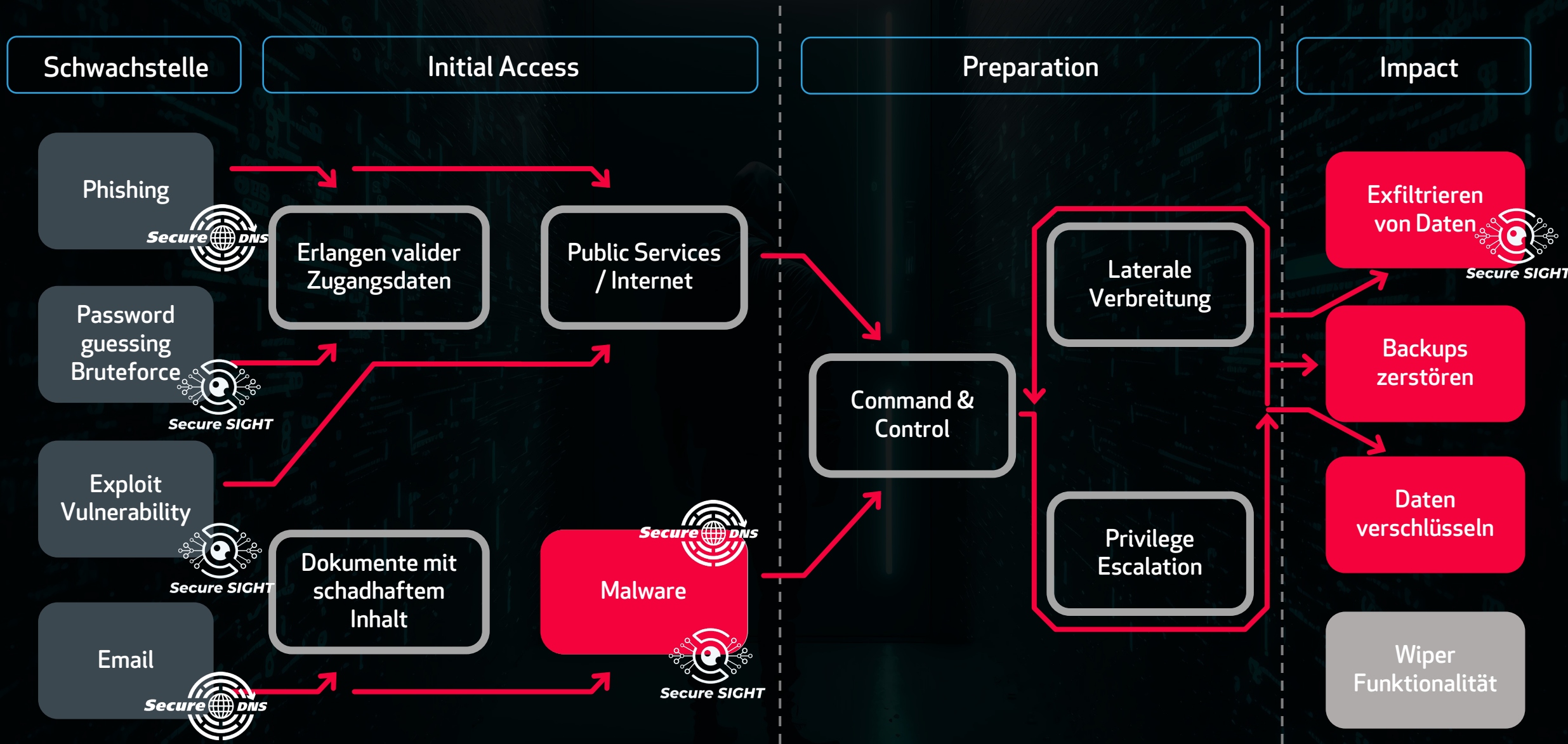
Secutec
Cyber security intelligence

Initial Access via Broker zum Ransomware Deployment (Stunden)



Lifecycle einer Ransomware Attacke

Secutec
Cyber security intelligence



Secutec
Cyber security intelligence

Ransomware Attacke – BlackCat


Secutec
Cyber security intelligence
User Session mittels Citrix
Attacke
31.01.
23:18 Uhr
RDP-Anmeldung Domaincontroller
02.02.
Start Daten Exfiltration 124GB über 29 Hosts
03:29 Uhr
04.02.
06:40 Uhr
Auffälligkeiten intern erkannt
Start der internen Alarmierungskette
04.02.
Server lokalisiert
Alle Admin Accounts kompromittiert
2 Standorte mit verschlüsselter VM
Notfallprotokoll gestartet
07:10 Uhr
04.02.
11:04 Uhr
Start Forensik Secutec
04.02.
Hacker RDP-Session vom kompromittieren Server übernommen
Nachmittag
04.02.
Abend
Deepweb Server der Hacker lokalisiert, 124GB gestohlenen Daten retour geholt
04.02.
KIRCHDORFER
GROUP

Die ersten 48 Stunden nach der Attacke

-Die Server nicht herunterfahren!

-Start der Forensik (Wie, Wer, Was)

-Darknet Monitoring

-Keine Verhandlungen in den ersten 48 Stunden

-Klare Strategie / Organisation (intern/extern)

-Priorisieren der Daten und Systeme

Secutec
Cyber security intelligence

Die Monate nach der Attacke

-Permanentes Monitoring der Systeme

Gehen Sie davon aus, dass Ihre Systeme noch kompromittiert sein können und gehen Sie davon aus, dass Sie erneut gehackt werden können.

Lösegeld-forderungen

- In vielen Fällen deckt sich die Summe der liquiden Mittel eines Unternehmens mit der Lösegeldforderung der Hacker. Vermutlich sind die Bilanzen in vielen Fällen bekannt. Start Forderung meist 10% vom Umsatz.

- Argumente in der Verhandlung über nicht liquide Mittel werden oftmals mit aktuellen Bankauszügen durch die Hacker widerlegt.

[AKIRA]

AKIRA

Well, you are here. It means that you're suffering from cyber incident right now. Think of our actio
ns as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
fair price to make it all go away.

Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow o
ur instructions to get back to your daily routine, by cooperating with us you will minimize the dama
ge that might be done.

Those who choose different path will be shamed here publicly. The functionality of this blog is extr
emely simple - enter the desired command in the input line and enjoy the juiciest information that c
orporations around the world wanted to stay confidential.

Remember. You are unable to recover without our help. Your data is already gone and cannot be traced
to the place of final storage nor deleted by anyone besides us.

guest@akira:~$ help

List of all commands:

leaks	– hacked companies
news	– news about upcoming data releases
contact	– send us a message and we will contact you
help	– available commands
clear	– clear screen

guest@akira:~$

Hi friends,

Unabhängig davon, wer Sie sind und welchen Titel Sie tragen, wenn Sie dies lesen, bedeutet dies, dass die interne Infrastruktur Ihres Unternehmens ganz oder teilweise tot ist, alle Ihre Backups - virtuell, physisch - alles, was wir erreichen konnten, ist vollständig entfernt. Außerdem haben wir einen großen Teil Ihrer Unternehmensdaten vor der Verschlüsselung entwendet.

Nun, lassen Sie uns die Tränen und den Groll erst einmal für uns behalten und versuchen, einen konstruktiven Dialog aufzubauen. Wir sind uns voll und ganz bewusst, welchen Schaden wir mit der Sperrung Ihrer internen Quellen angerichtet haben.
Im Moment müssen Sie das wissen:

1. Wenn Sie mit uns zusammenarbeiten, werden Sie VIEL sparen, denn wir sind nicht daran interessiert, Sie finanziell zu ruinieren. Wir werden Ihre Finanzen, Bank- und Einkommensauszüge, Ihre Ersparnisse, Investitionen usw. gründlich studieren und Ihnen einen angemessenen Vorschlag unterbreiten. Wenn Sie eine aktive Cyber-Versicherung haben, lassen Sie es uns wissen, und wir werden Ihnen zeigen, wie Sie diese richtig nutzen können. Wenn Sie den Verhandlungsprozess in die Länge ziehen, wird das Geschäft nicht zustande kommen.

2. Wenn Sie uns bezahlen, sparen Sie Ihre ZEIT, Ihr GELD, Ihren Aufwand und sind innerhalb von 24 Stunden wieder auf dem richtigen Weg. Unser Entschlüsselungsprogramm funktioniert bei allen Dateien und Systemen einwandfrei, so dass Sie es überprüfen können, indem Sie zu Beginn unseres Gesprächs einen Test-Entschlüsselungsdienst anfordern. Wenn Sie sich für eine Wiederherstellung auf eigene Faust entscheiden, bedenken Sie, dass Sie den Zugriff auf einige Dateien dauerhaft verlieren oder sie versehentlich beschädigen können - in diesem Fall können wir Ihnen nicht helfen.

3. Der Sicherheitsbericht oder die exklusiven Informationen aus erster Hand, die Sie bei Abschluss einer Vereinbarung erhalten, sind von großem Wert, da KEINE vollständige Prüfung Ihres Netzwerks Ihnen die Schwachstellen aufzeigt, die wir aufdecken und nutzen konnten, um in Ihr Netzwerk einzudringen, Backup-Lösungen zu finden und Ihre Daten hochzuladen.

4. Was Ihre Daten betrifft, so werden wir, wenn wir uns nicht einigen können, versuchen, persönliche Informationen/Geschäftsgeheimnisse/Datenbanken/Quellcodes - allgemein gesagt, alles, was auf dem Schwarzmarkt einen Wert hat - an mehrere Bedrohungsakteure auf einmal zu verkaufen. All dies wird dann in unserem Blog veröffentlicht - https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fakiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion&c=E,1,dJXYIYKI-r4ni_emkQ2CG1rW-DGjxYVPWw4O_MIQQokmy_gdVwkUBvfzCg3NqAJ6C8exu647IlHIiABBHWQFCJCXZUfqNc8BbVLM_7t1b-J2FADO&typo=1

5. Wir sind mehr als verhandlungsbereit und werden mit Sicherheit einen Weg finden, die Angelegenheit schnell zu regeln und eine Einigung zu erzielen, die uns beide zufrieden stellt.

Wenn Sie tatsächlich an unserer Hilfe und den von uns angebotenen Dienstleistungen interessiert sind, können Sie sich mit uns in Verbindung setzen, indem Sie die folgenden einfachen Anweisungen befolgen:

1. Installieren Sie den TOR-Browser, um Zugang zu unserem Chatroom zu erhalten - https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fwww.torproject.org%2fdownload%2f&c=E,1,J0kXbGjEb6C9clIaVzAU-pSdhuYDg8m7aileLbNrCdp-ZeZT_jDLp4VmSDZtvjoYtOTZKpD5K60aZOYAytRkK5SVRECtoCaC0GJCKgNqfLQtx1Q,&typo=1.

2. Fügen Sie diesen Link ein - https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fakiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion&c=E,1,eUm7ptlW0C6Z6Rt8eY4x-cKl9Mb-KjJU6Jcxk-waKKRA3RRi4VHdaUhoEDA-Ez1cOCXf2Qd2N5vhBl_-60w45DSozru3VeHCzfrKbJA7QpA,&typo=1

3. Verwenden Sie diesen Code - 5391-OY-PYET-ZUOF - um sich in unseren Chat einzuloggen.
Denken Sie daran, dass je schneller Sie sich melden, desto weniger Schaden entsteht.

Empfehlungen

-Monitoring des ausgehenden DNS Traffics
Auch IoT Devices beachten

-Externes Schwachstellen Monitoring
Aus Sicht eines externen Angreifers – Darknet/Vulnerabilities

-Vorbereitung auf einen Incident
Es gibt kein 100% Playbook, aber 70%

-Notfall Handbuch und Ransomware Playbook
Unterschiedliche Szenairen (Blackout, Hacker Attacke, ...)

-Multifaktor Authentifizierung
Hier Bedarf es neben dem Passwort eine weiteren Faktor für Hacker

Empfehlungen

-EDR/XDR – Endpoint Detection Response auf Server
Nur “Virenscanner” der next Generation können Gefahren erkennen.

-Alternatives Linux Backup
Hacker gehen in der Regeln den einfach Weg

-Server Logs Backup
Je länger desto besser für die Forensik, min. 90 Tage

-Netzwerk (Mikro)Segmentierung
Netzwerk in kleinere, separate Subnetzwerke unterteilen

-Keine Admin Rechte auf lokalen Geräten
Wenn die Notwendigkeit besteht nur temporäre Rechte zulassen

Empfehlungen Privatperson

- Multifaktor Authentifizierung
  Für alle privaten Applikationen und Online Plattformen.

- Passwort Manager
  Sichere Passwörter verwenden, die in keinem Zusammenhang stehen

- VPN Verbindung
  Anbieter wie z.B. NordVPN erhöhen die Sicherheit und Anonymität

Secutec
Cyber security intelligence

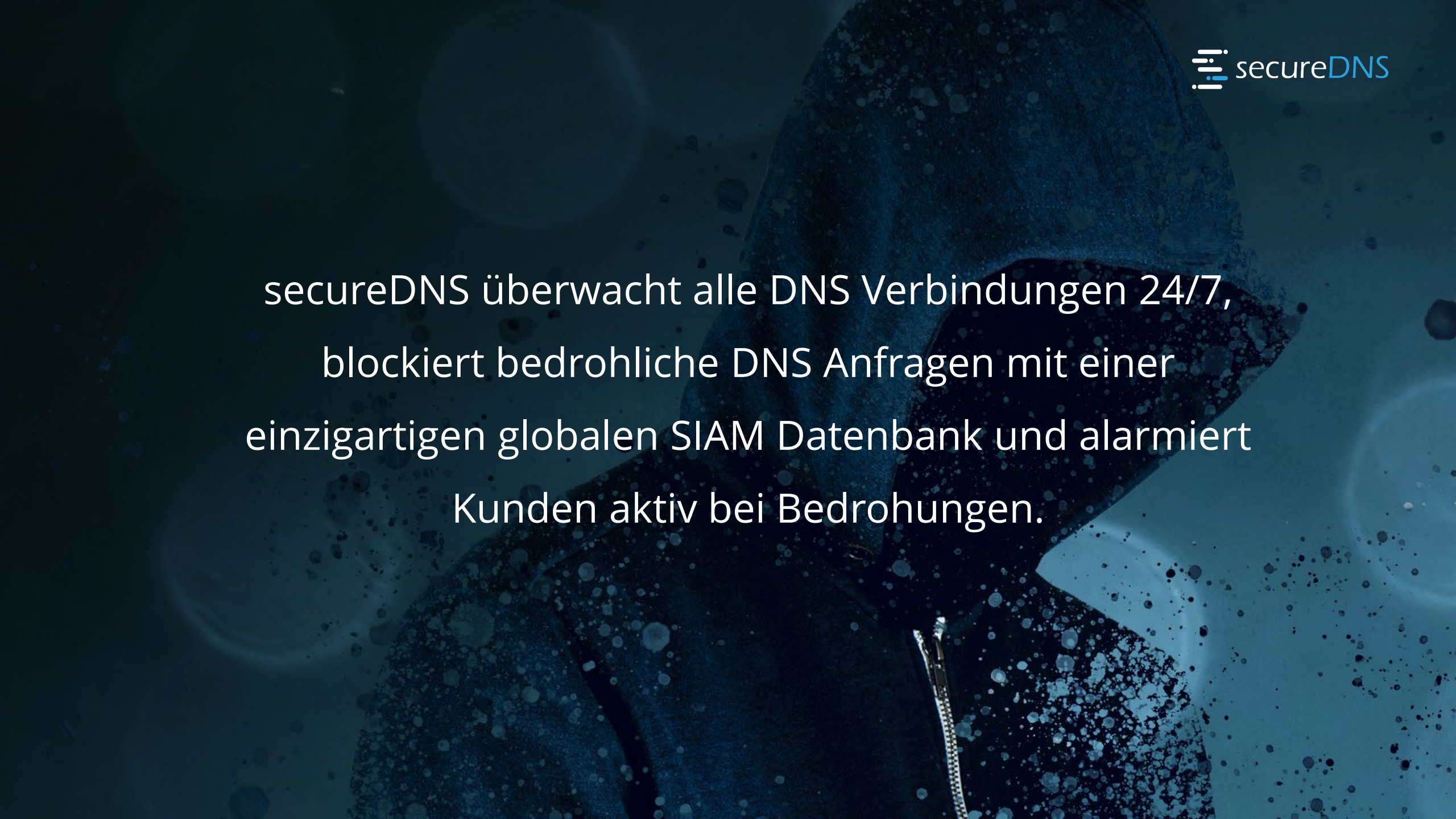
Einfach in einem POC testen ...

Modul	Kosten	Aufwand
secureDNS	kostenlos	20-30 min.
secureSIGHT Darknet Monitoring	400 Euro	kein Aufwand
secureSIGHT Active Managed Threat Hunting	600 Euro	20-30 min.
secureSIGHT Attack Surface Management	1.300 Euro	kein Aufwand

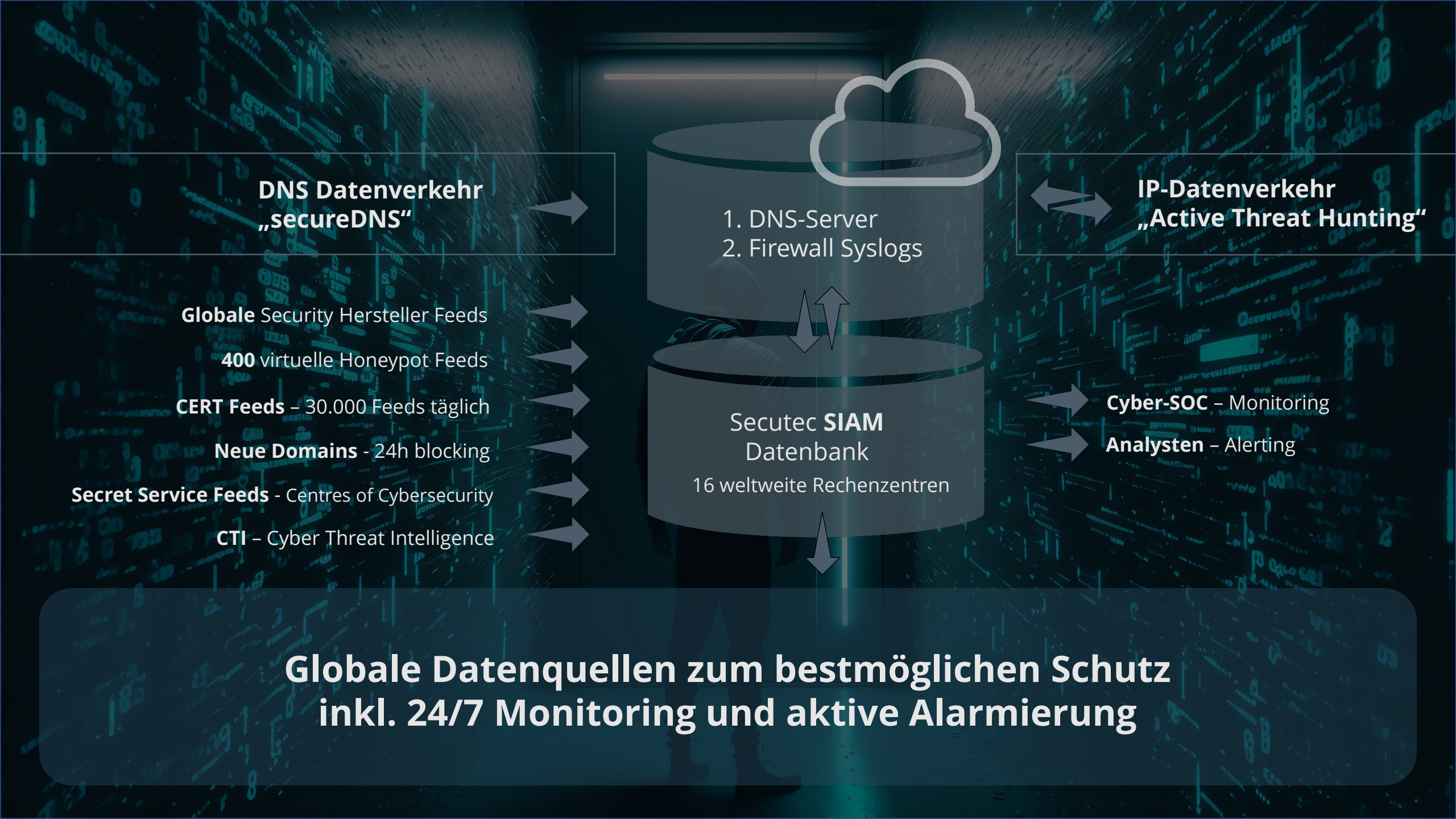

Secutec
Cyber security intelligence

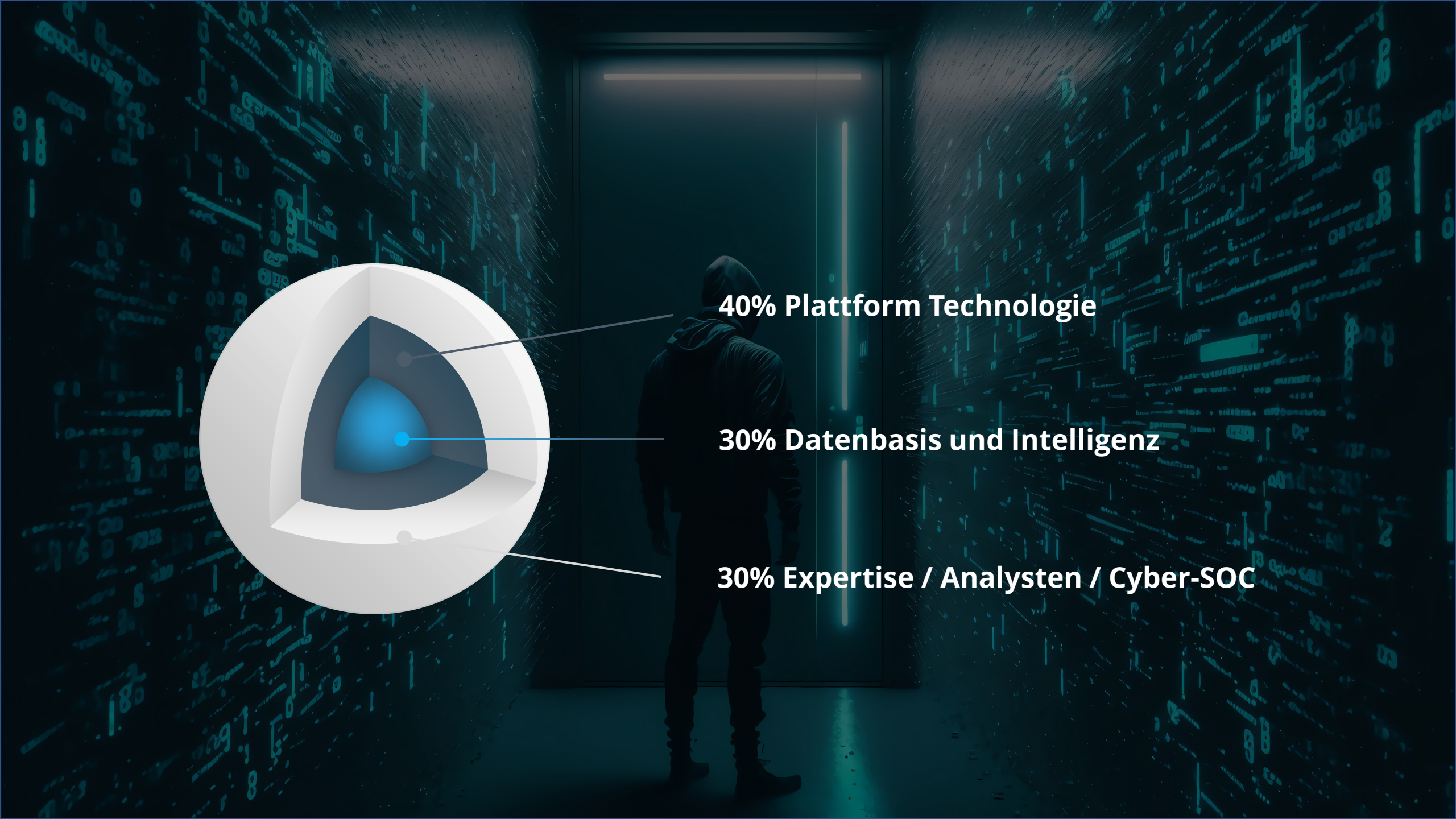
secureDNS

NOCH NIE WAR CYBER-SECURITY EINFACHER



secureDNS überwacht alle DNS Verbindungen 24/7, blockiert bedrohliche DNS Anfragen mit einer einzigartigen globalen SIAM Datenbank und alarmiert Kunden aktiv bei Bedrohungen.


DNS Datenverkehr
„secureDNS“
1. DNS-Server
2. Firewall Syslogs
IP-Datenverkehr
„Active Threat Hunting“
Globale Security Hersteller Feeds
400 virtuelle Honeypot Feeds
CERT Feeds – 30.000 Feeds täglich
Neue Domains - 24h blocking
Secret Service Feeds - Centres of Cybersecurity
CTI – Cyber Threat Intelligence
Secutec SIAM
Datenbank
16 weltweite Rechenzentren
Cyber-SOC – Monitoring
Analysten – Alerting
Globale Datenquellen zum bestmöglichen Schutz
inkl. 24/7 Monitoring und aktive Alarmierung


40% Plattform Technologie
30% Datenbasis und Intelligenz
30% Expertise / Analysten / Cyber-SOC

Datenbasis

SIAM Datenbank mit weltweiten Hersteller Datenbanken

Hersteller Datenbank ~100MB
Secutec Datenbank 410 GB

Schnelligkeit

Integration von 20.000-30.000 täglichen CERT Feeds

Behörden Daten ergänzen die restlichen Datenquellen

Analysten

Sämtliche Daten werden 24/7 vom SOC überwacht

Kunden bekommen eine proaktive Information bei möglichen Bedrohungen

Darknet

Eine Kombination mit Darknet Monitoring ist möglich

Bedrohungen auch außerhalb der eigenen Sicht rasch finden

New Domain

Neue Domains werden innerhalb der ersten 24 Stunden blockiert

Mehr als 22% aller neu registrierten Domains werden für Cyberkriminalität verwendet

False Positive

Bewertung von mehreren hundert Mio. DNS-Requests täglich

Keine spürbaren False Positive Bewertungen

secureDNS

Mehrwerte im Vergleich zu anderen Lösungen.

Expertise

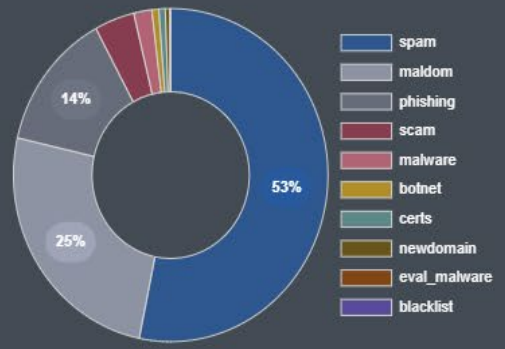
Unser Expertenteam aus dem SOC- und Incident Response Team kann bei Bedarf jederzeit mit Praxiserfahrung und Know-how unterstützen

HOME
News
DATA & REPORTING
Dashboards
Reports
DOCUMENTS
Documents
PARTIES INVOLVED
Users
Organizations

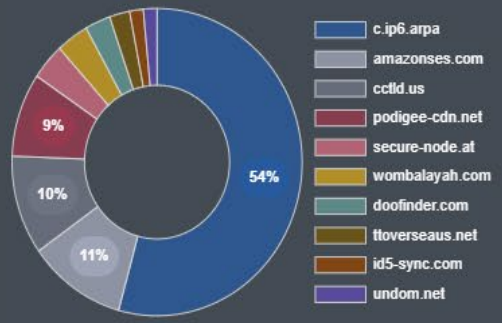
Domain | Query | Category | Public IP | Processes | Users | Computers | Private IP

All requests	Blocked requests	Monitored requests	Blocked botnet requests	Blocked apt requests
512 176	512 176	0	3 668	0

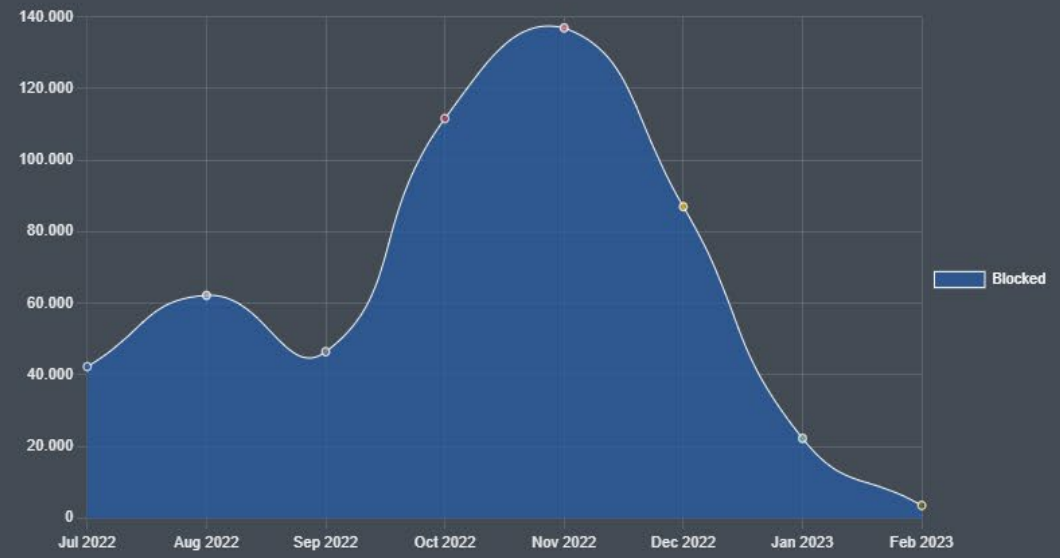
Top 10 categories



Top 10 domains

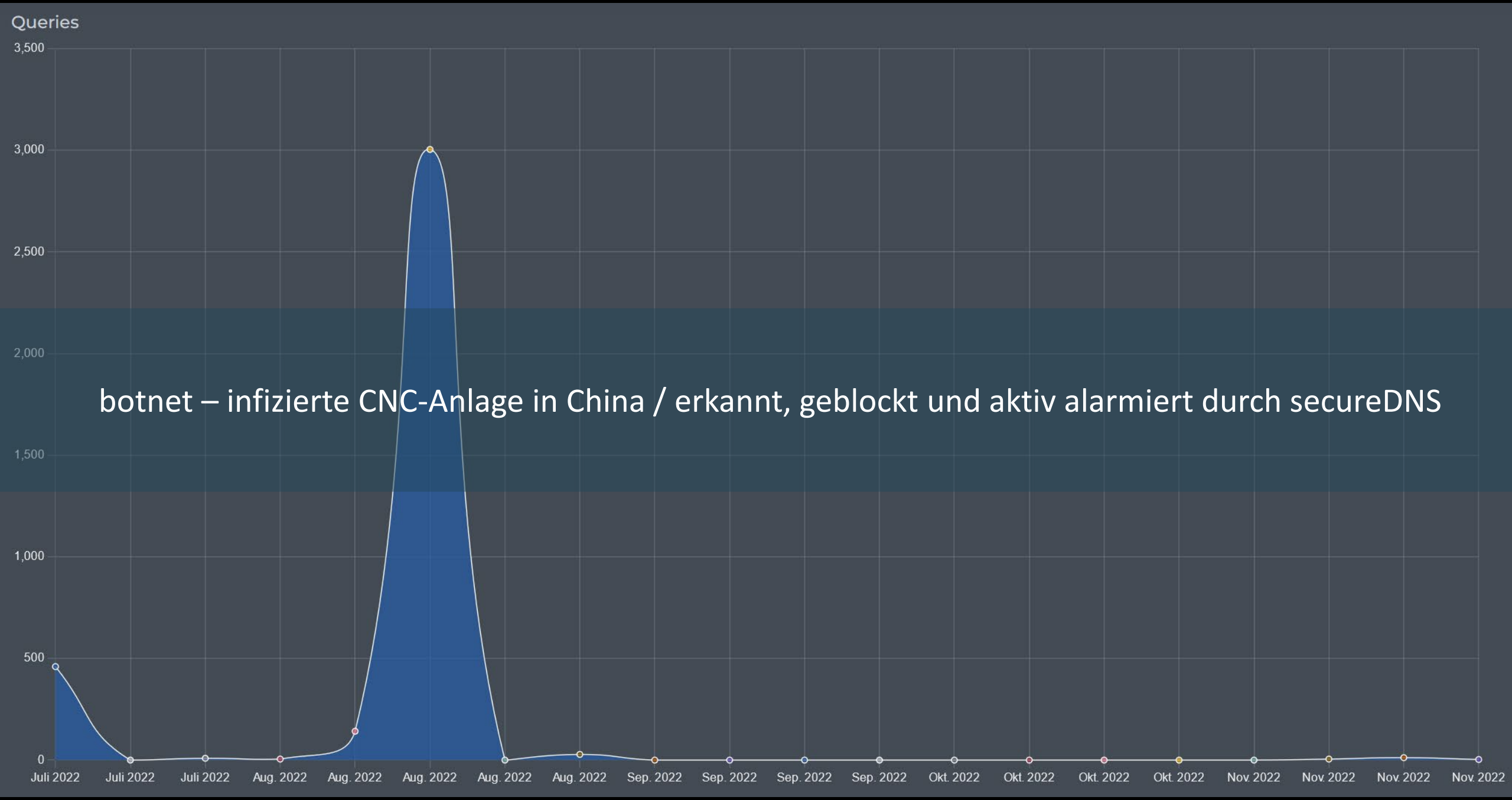


Queries

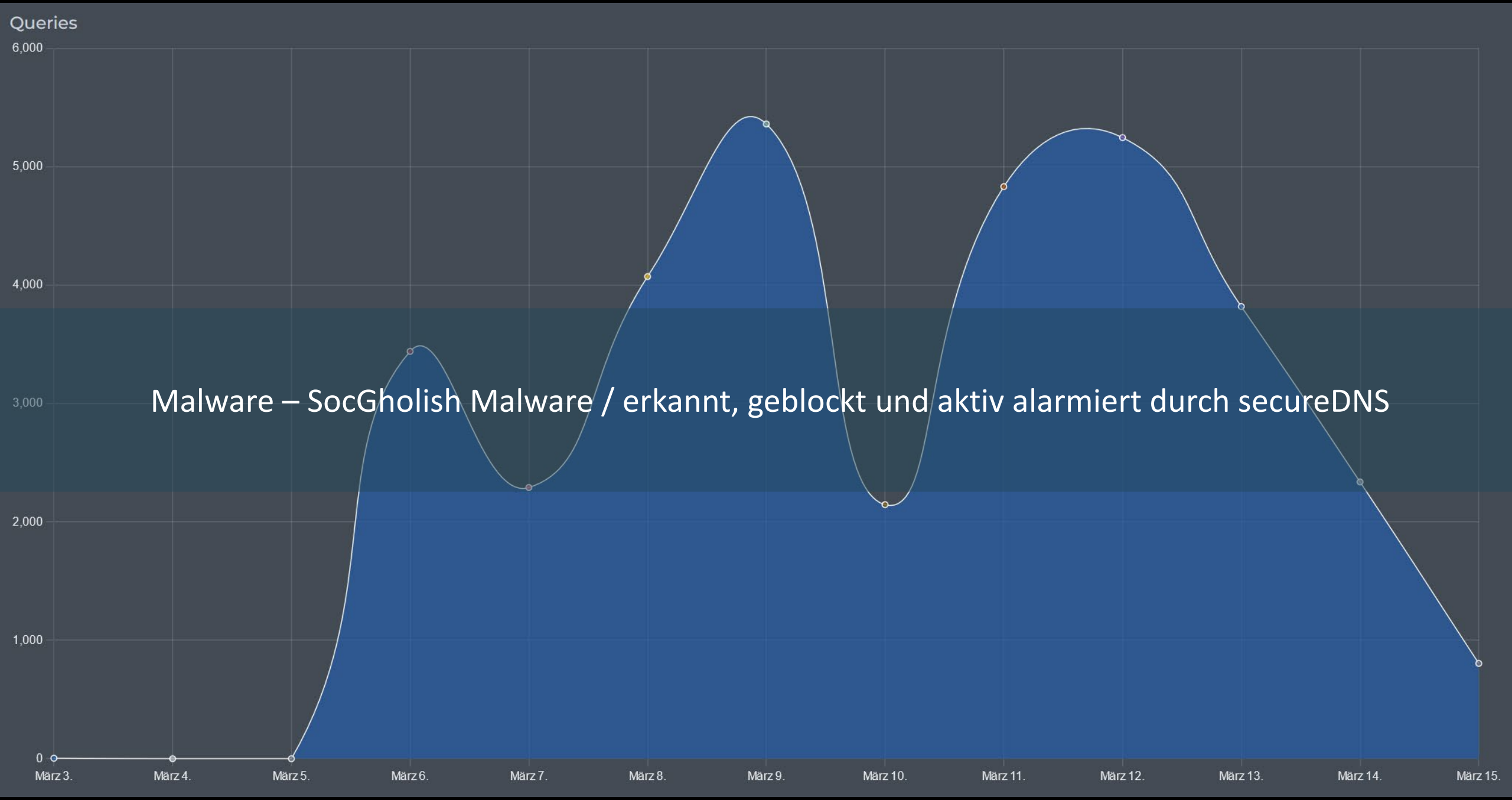


Queries

Date	DNS Category	DNS Query	Client Name	Public IP Address	Site Name	Agent Hostname	Private IP Address	VirusTotal Score	FortiGuard Rating	McAfee Rating	Ticket Number	Whitelisting
02/02/2023 13:39:05	spam	ad.turn.com										Request whitelisting
02/02/2023 13:36:47	spam	ad.turn.com										Request whitelisting
02/02/2023 13:36:47	spam	ad.turn.com										Request whitelisting



botnet – infizierte CNC-Anlage in China / erkannt, geblockt und aktiv alarmiert durch secureDNS



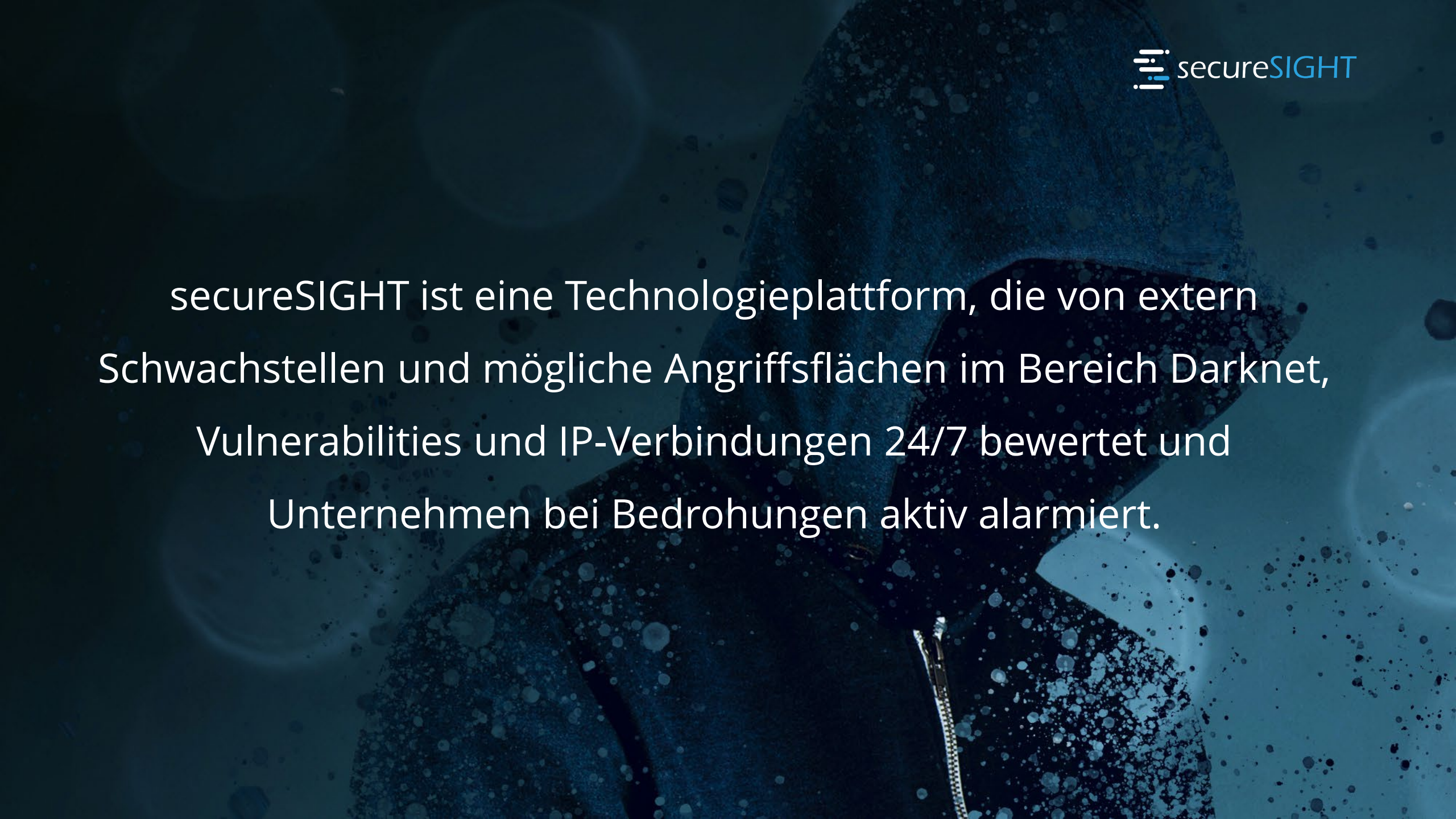
Malware – SocGholish Malware / erkannt, geblockt und aktiv alarmiert durch secureDNS

secureSIGHT

IHR DIGITALER UNTERNEHMENS FOOTPRINT

secureSIGHT

secureSIGHT ist eine Technologieplattform, die von extern Schwachstellen und mögliche Angriffsflächen im Bereich Darknet, Vulnerabilities und IP-Verbindungen 24/7 bewertet und Unternehmen bei Bedrohungen aktiv alarmiert.



secureSIGHT

Permanenter Vulnerability Scan

- Externes monitoring möglicher Schwachstellen

  (Vulnerabilities, Malware, Open-Ports, SSL-Zertifikate, Industrial Control Service, IoT Devices)

- Scanning auch außerhalb bekannter IP-Ranges

- Neubewertung erfolgt alle 24-48 Stunden

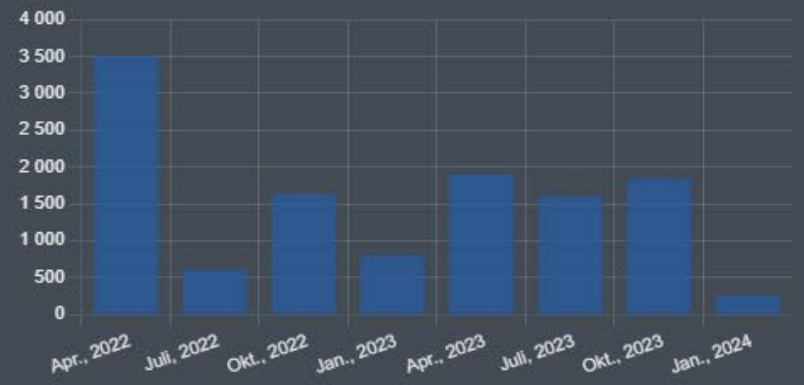
- Aktive Alarmierung bei Bedrohungen

secutecat | Nur Organisation

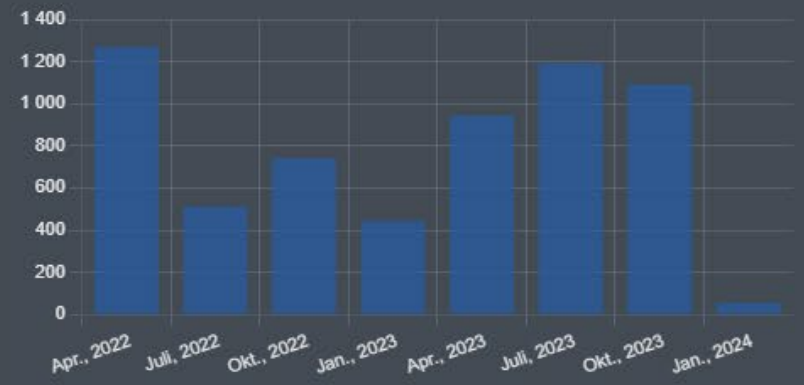
Security Rating | Title

F - Critical Risks	E - High Risks	D - Low Risks	C - Recommendations	B - Improvements	A - Informational
26	29	249	366	4 964	122

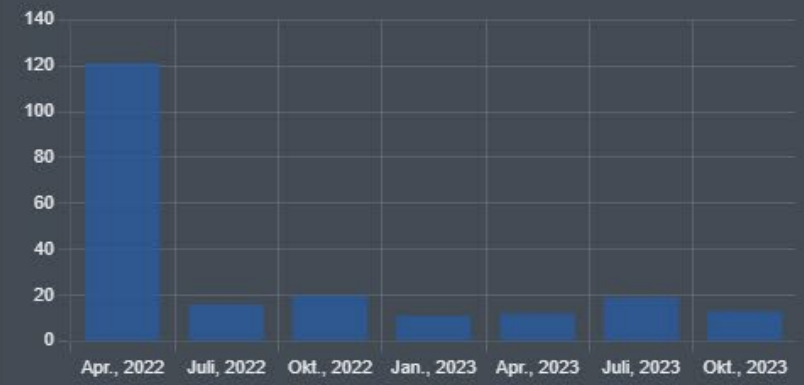
Risks Discovered



Risks Solved



Risks Mitigated



High and Critical Open Risks (Security Rating F & E)

Security Rating	Asset Title	Discovered	Title	Description	Proposed Action	ID
f	[redacted]	13.05.2022 03:33:15	Vulnerable software found - openssl/1.1.1k (highest CVE score 10.0)	We discovered software with the following potential vulnerabilities.	Update the software listed in this risk, by contacting your provider or hosting party. Also, take note that this information should not be publicly accessible, as this might help the hacker in their attack preparation.	12627
f	[redacted]	13.05.2022 13:06:48	Vulnerable software found - php/5.3.29 (highest CVE score 10.0)	We discovered software with the following potential vulnerabilities.	Update the software listed in this risk, by contacting your provider or hosting party. Also, take note that this information should not be publicly accessible, as this might help the hacker in their attack preparation.	16358

secutecat | Nur Organisation

Security Rating | Type

Assets with F Rating	Assets with E Rating	Assets with D Rating	Assets with C Rating	Assets with B Rating	Assets with A Rating
25	22	231	217	2 076	17 050

Confirmed Assets - These are linked to your company, including IPs, subnets and domains

Security Rating	Title	Discovered	Type	ID
f	[redacted]	29.04.2022 19:01:30	Application	876
f	[redacted]	29.04.2022 23:50:28	Application	3887
f	[redacted]	02.05.2022 15:31:55	Application	5358
f	[redacted]	12.05.2022 18:53:04	Application	11101
f	[redacted]	13.05.2022 13:06:03	Application	16181
f	[redacted]	06.06.2022 23:47:15	Application	29976
f	[redacted]	06.06.2022 23:47:45	Application	29983
f	[redacted]	06.06.2022 23:48:43	Application	29997
f	[redacted]	06.06.2022 23:49:13	Application	30004
f	[redacted]	06.06.2022 23:50:11	Application	30018

secureSIGHT

Managed Darknet Monitoring

- Aktives Darknet Monitoring im Bereich Darknetseiten, Foren, Chats, Marktplätze

- Überwachung von Domains, Benutzerkonten, strategischen Personen, Keyword, Produkten, usw.

- Aktive Suche nach internen und externen Usern mit infizierten Clients (Keylogger, Password Stealer)

- Aktive Alarmierung bei sicherheitsrelevanten Findings

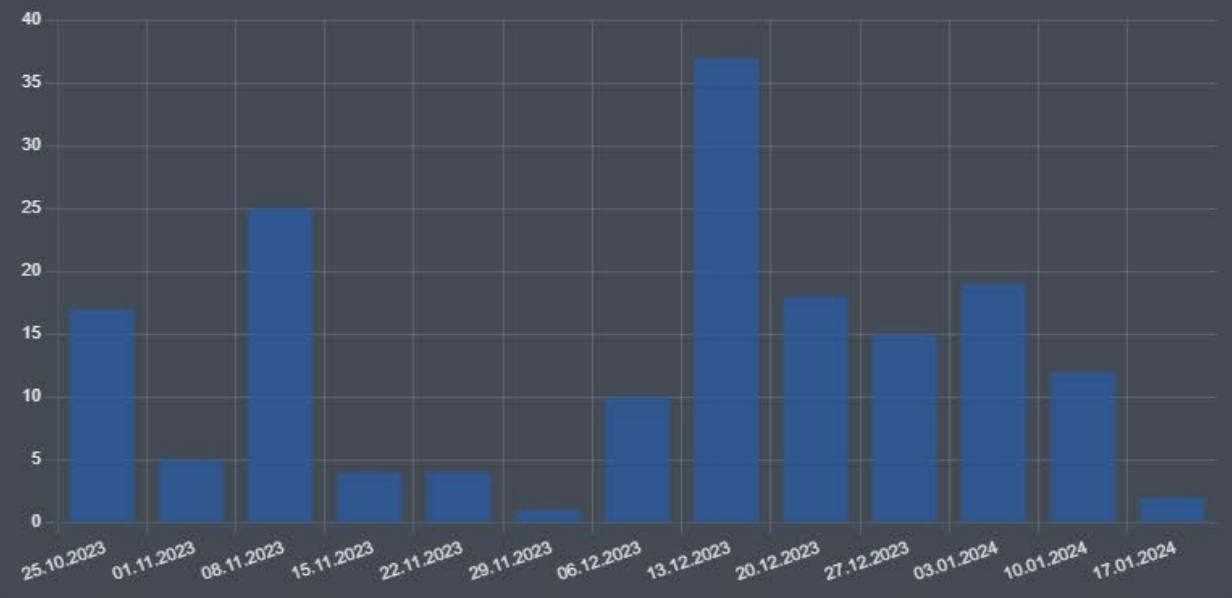
Dashboard | Leaked Credenti... | SecureSIGHT - Dashboard - Leaked Credentials

secutecat | Nur Organisation | 24.10.2023 08:12 - 22.01.2024 08:12

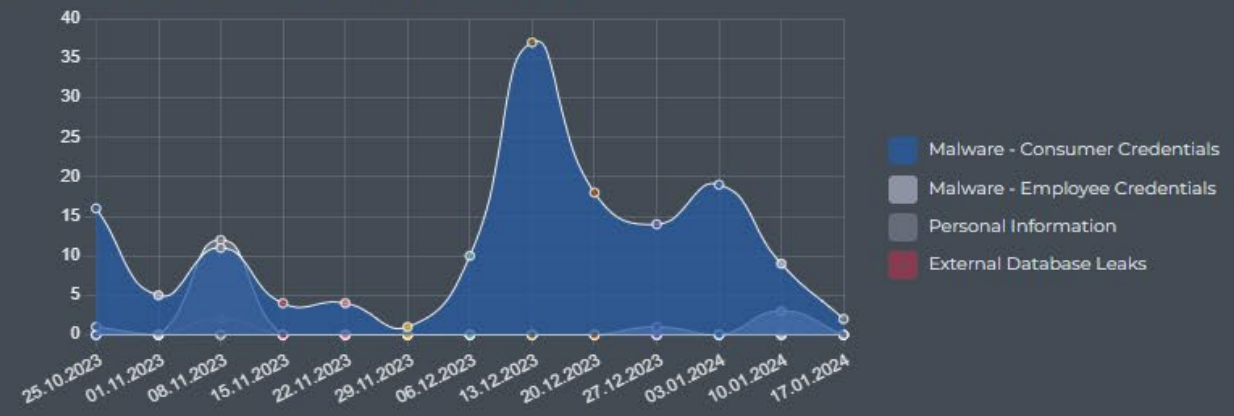
Domain | Breach Title | Email Address | Email Domain | User Domain | Hostname | OS | Leak Source IP

Total Leaked Credentials	Malware - Employee Credentials	Malware - Consumer Credentials	External Database Leaks	Personal Information	Email Only
169	5	150	2	12	0

Detected Leaked Credentials



Detected Leaked Credentials (per category)



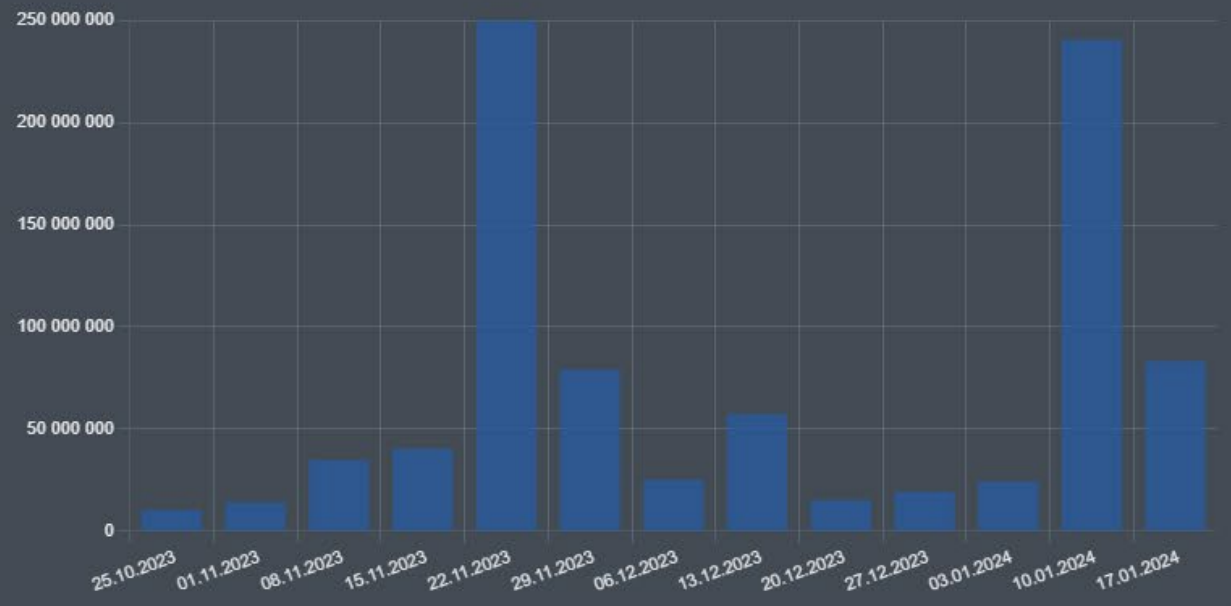
Malware Breaches - Employee Credentials - Login/Email linked to your company

Publish Date	Breach Date	Breach Title	Email Address	Username	Password Type	Target URL	Infected Time	Hostname	OS	IP
14.01.2024 01:00:00	14.01.2024 01:00:00	LummaC2 Stealer	[redacted]		plaintext	https://vpn-[redacted]a.com/		DESKTOP-RALLRC0	Windows 10 (10.0.19045) x64	86.5[redacted]

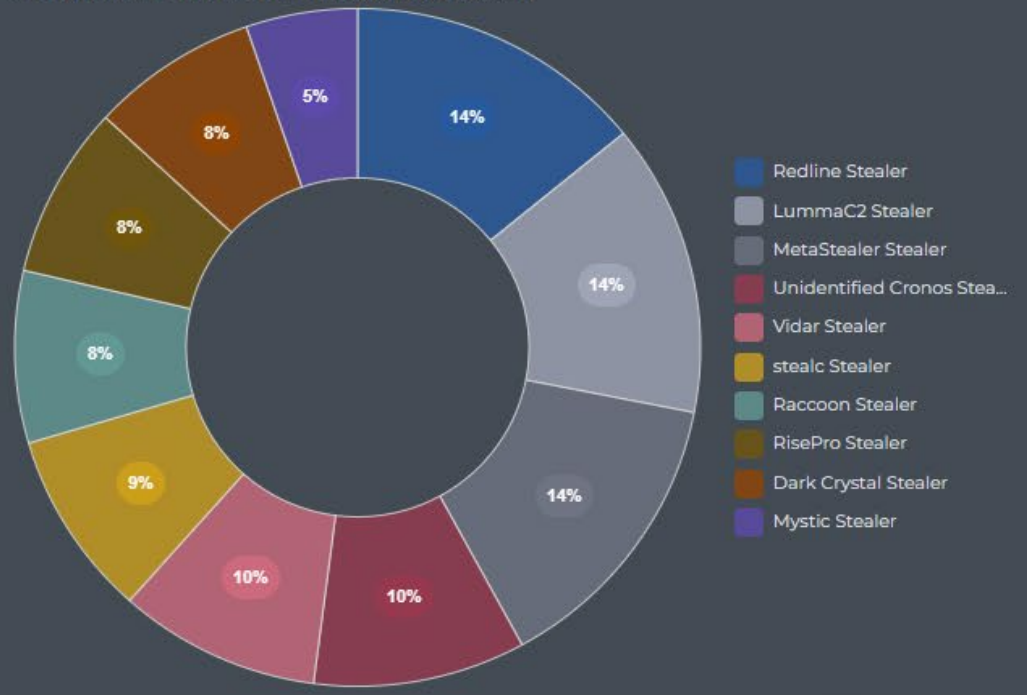
secutecat | Nur Organisation | 24.10.2023 08:12 - 22.01.2024 08:12

Breach Title | Target Site

Global Detected Leaked Credentials



Global Detected Leaked Credentials (per malware)



Global Detected Leaked Credentials

Breach Title	Publish Date	Total Records	Breach Date	Breach Type	Breach Description	Target Site	Target Description
Vidar Stealer	21.01.2024 01:00:00	170	20.01.2024 01:00:00	PRIVATE	Vidar Stealer is a Windows-targeted stealer designed to grab form data such as IP addresses, browsing history, saved passwords, cryptocurrency, private messages and/or screenshots from affected users. Operators of Vidar can set messages for when jobs are completed. Vidar is typically delivered via the Fallout exploit kit. The stealer can be purchased easily for only $700.00 USD.	n/a	Vidar is a stealer that affects Windows users. It is typically delivered via exploit kit and can compromise passwords, browsing history, cryptocurrency, private messages, screenshots and other personal data from affected users.

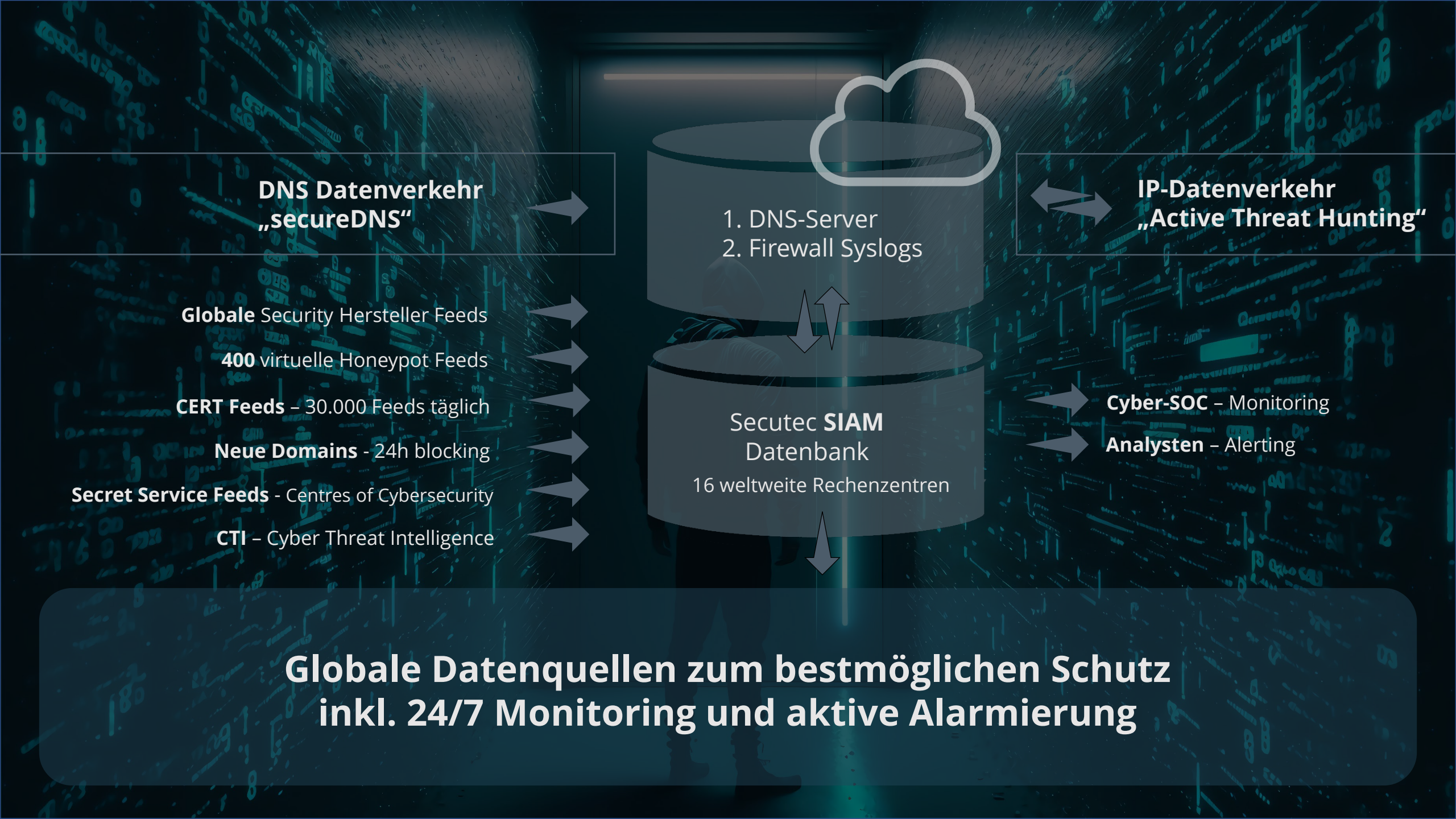
secureSIGHT

Active Managed Threat hunting

- 24/7 Überwachung aller IP-Datenverbindungen, die von der Firewall nicht blockiert wurden.

- Aktive Alarmierung bei schadhaften Verbindungen

- Zugang zu TIER1 Netflow Daten der Internet eXchange Knotenpunkte und Kategorisierung dieser Daten


DNS Datenverkehr
„secureDNS“
1. DNS-Server
2. Firewall Syslogs
IP-Datenverkehr
„Active Threat Hunting“
Globale Security Hersteller Feeds
400 virtuelle Honeypot Feeds
CERT Feeds – 30.000 Feeds täglich
Neue Domains - 24h blocking
Secret Service Feeds - Centres of Cybersecurity
CTI – Cyber Threat Intelligence
Secutec SIAM
Datenbank
16 weltweite Rechenzentren
Cyber-SOC – Monitoring
Analysten – Alerting
Globale Datenquellen zum bestmöglichen Schutz
inkl. 24/7 Monitoring und aktive Alarmierung

secutecat | Nur Organisation | 24.10.2023 08:12 - 22.01.2024 08:12

Device Name | Threat Indicator IP | Protocol | Classification

High Risk Events (High Potential Impact)

2

Medium Risk Events (Medium Potential Impact)

34

High Risk Events (High Potential Impact)

Time of Alert	Device Name	Threat Indicator IP	Protocol	Source IP	Destination IP	Destination Port	Destination Country Name
19.01.2024 13:33:42	FortiGate-100F	185.230.63.171	http	[redacted]	185.230.63.171	80	United States
04.01.2024 05:52:27	S7GR-FW-FORTI01	64.190.63.111	intuit-web	[redacted]	64.190.63.111	443	Germany

Showing 1 to 2 of 2 « ‹ 1 › » 10

High Risk Events Classification (High Potential Impact)

Threat Indicator IP	Threat Type	Classification	Associated Threat Name	Threat Description	Threat List	VirusTotal Rating	VirusTotal Classification
185.230.63.171	Trojan	Malware, Mobile Malware, Bot C&C	Trojan-Downloader.Win32.Minix, Virus.Win32.Sality, Trojan-Spy.Win32.Zbot, Trojan-Ransom.Win32.Cryptodef	A Trojan is a type of malware that disguises itself as legitimate software to deceive users into unwittingly installing it. Once installed, Trojans can perform malicious actions, such as stealing information or damaging files, without the user's knowledge.	N/A	6/89	Suspicious
64.190.63.111	Trojan	Malware, Fraud, Bot C&C	CnC.Win32.Generic, Trojan-Spy.Win32.Ursnif, Trojan-Spy.Win32.Noon, Backdoor.AndroidOS.Ahmyth	A Trojan is a type of malware that disguises itself as legitimate software to deceive users into unwittingly installing it. Once installed, Trojans can perform malicious actions, such as stealing information or damaging files, without the user's knowledge.	N/A	8/89	Malicious

secutecat | Nur Organisation | 24.10.2023 08:12 - 22.01.2024 08:12

Firewall Name | Package Name

Amount of Logs

3 710 499 434

Timeline of the Amount of Logs (Static)

Logs per Firewall

Firewall ↑↓	Amount of Logs ↑↓
[redacted]	172736
[redacted]	186
[redacted]	380
[redacted]	278043103
[redacted]	957958
[redacted]	83
FortiGate-100F	29848623
S7GR-FW-FORTI01	152560077
S7GR-FW-FORTI02	296434

Load more

secureRESPONSE

FORENSIK UND NEGOTIATION - WENN ES DARAUF ANKOMMT

secureRESPONSE

Incident Response

- Vorbereitung auf einen Incident (Ransomware Playbook)
- Technologie, Forensik, Analyse und Reporting
- Monitoring im Cyber-SOC
- Aktives Darknet Monitoring
- Verhandlungsführung mit Hackern
- Zahlungsabwicklung von Lösegeld
- Monitoring/Schutzschirm nach dem Incident


Secutec
Cyber security intelligence