Secutec

Cybersecurity Intelligence

Prevent now, secure tomorrow

Secutec

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

Secutec

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

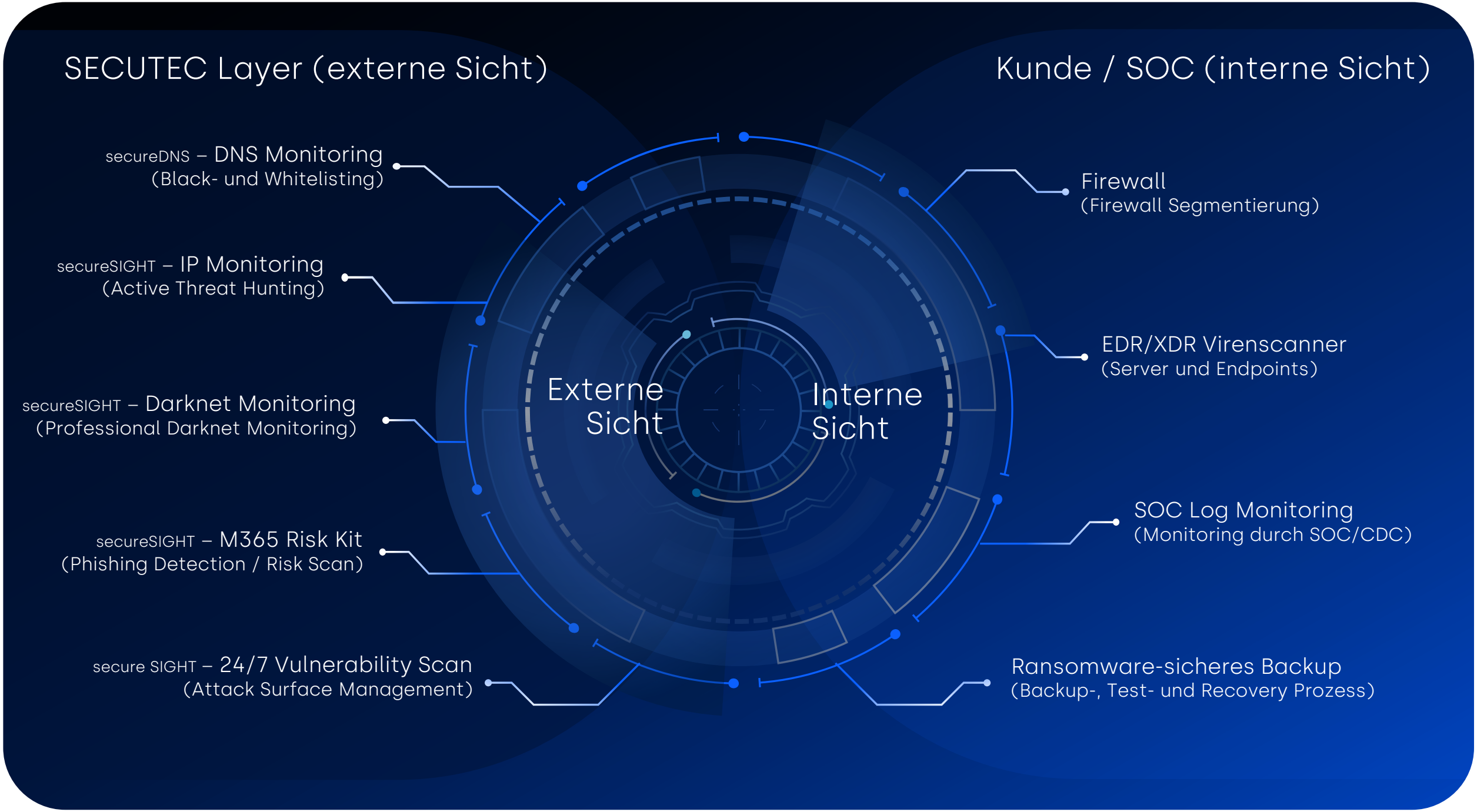
Behörden Datenquellen in den Bereichen IOC, APT, Botnet, Darknet Investigation und Threat Actors News

Datenquelle 4: Secutec Hunting Feed

Cyber Bedrohungen, die durch Checks von Secutec erkannt und an Behörden und Partner weitergegeben werden

Secutec

Secutec Integrated Advanced Malware Database (SIAM)


SECUTEC Layer (externe Sicht)
Kunde / SOC (interne Sicht)
secureDNS – DNS Monitoring
(Black- und Whitelisting)
secureSIGHT – IP Monitoring
(Active Threat Hunting)
secureSIGHT – Darknet Monitoring
(Professional Darknet Monitoring)
secureSIGHT – M365 Risk Kit
(Phishing Detection / Risk Scan)
secure SIGHT – 24/7 Vulnerability Scan
(Attack Surface Management)
Externe Sicht
Interne Sicht
Firewall
(Firewall Segmentierung)
EDR/XDR Virenscanner
(Server und Endpoints)
SOC Log Monitoring
(Monitoring durch SOC/CDC)
Ransomware-sicheres Backup
(Backup-, Test- und Recovery Prozess)


SECUTEC Webinar
„Einblicke ins Darknet, Hacker Organisationen und Cyber Security Intelligence Technologien“
Danke euch, einmal mehr grandios!
Super Webinar, bis bald
🙏
Sehr interessantes und spannendes Webinar!
richtig stark!
Sehr interessanter Vortrag! Vielen Dank.
Einzigartig !!!
💖
Super spannend, herzlichen Dank!!
War sehr Interessant! Danke!

Secutec Webinar – „„Darknet, Hacker & Co – Ein Blick hinter die Kulissen von Cyberkriminellen.“

W04.1 = Dienstag, 08.04.2025 / 15.00 – 16.30 Uhr
Secutec Webinar W04.1 - 08.04.2025 / Einblicke ins Darknet, Hacker Organisationen und Cyber Security Intelligence

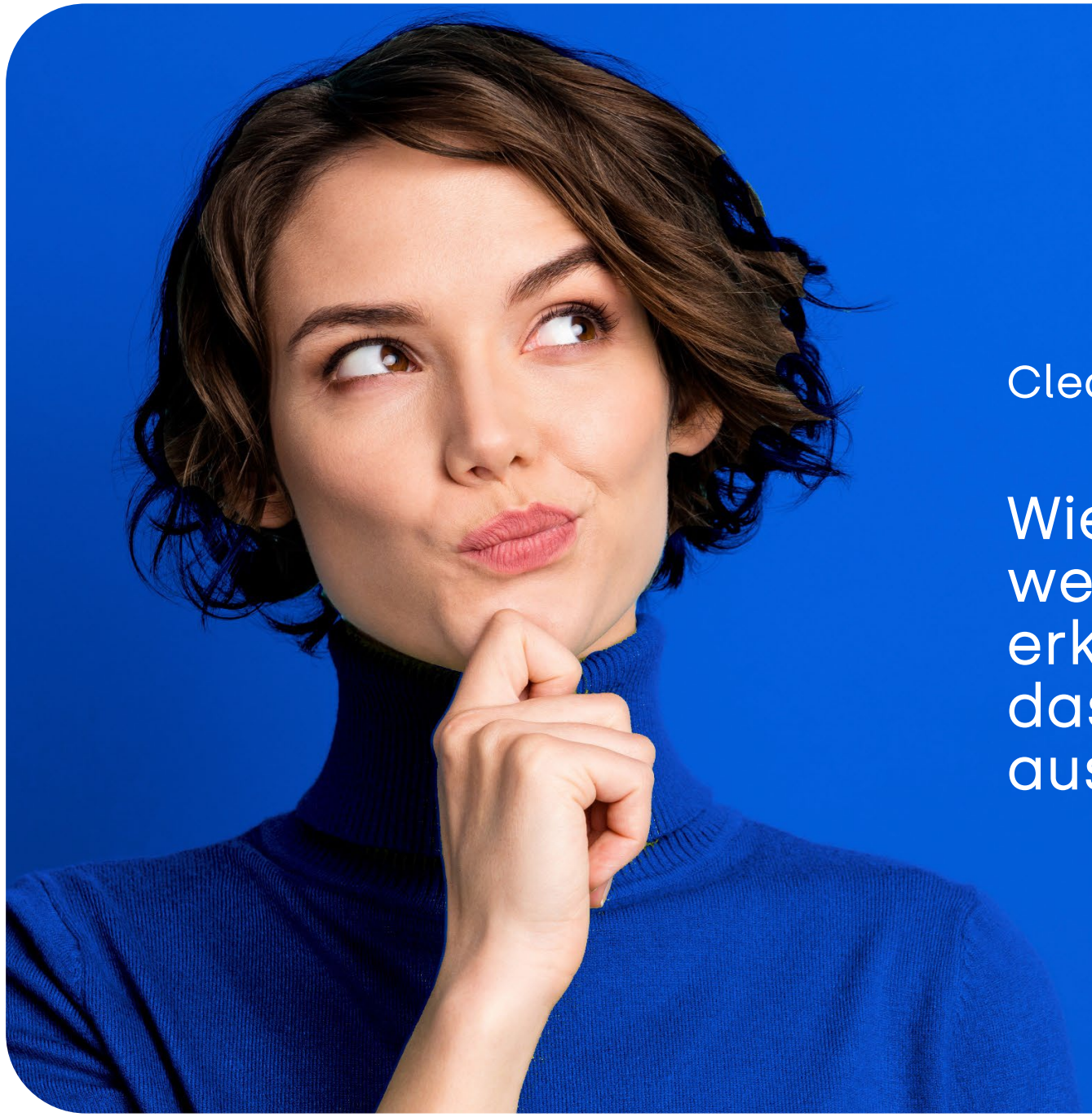
W04.2 = Donnerstag, 24.04.2025 / 08.30 – 10,00 Uhr
Secutec Webinar W04.2 - 24.04.2025 / Einblicke ins Darknet, Hacker Organisationen und Cyber Security Intelligence

W05.1 = Donnerstag, 15.05.2025 / 15.00 – 16.30 Uhr
Secutec Webinar W05.1 - 15.05.2025 / Einblicke ins Darknet, Hacker Organisationen und Cyber Security Intelligence

W06.1 = Donnerstag, 05.06.2025 / 08.30 – 10.00 Uhr
Secutec Webinar W06.1 - 05.06.2025 / Einblicke ins Darknet, Hacker Organisationen und Cyber Security Intelligence

W06.2 = Donnerstag, 26.06.2025 / 15.00 – 16.30 Uhr
Secutec Webinar W06.2 - 26.06.2025 / Einblicke ins Darknet, Hacker Organisationen und Cyber Security Intelligence


Secutec
Das Darknet



ClearWeb, DeepWeb, Darknet ...

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

Secutec

4%

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

96%

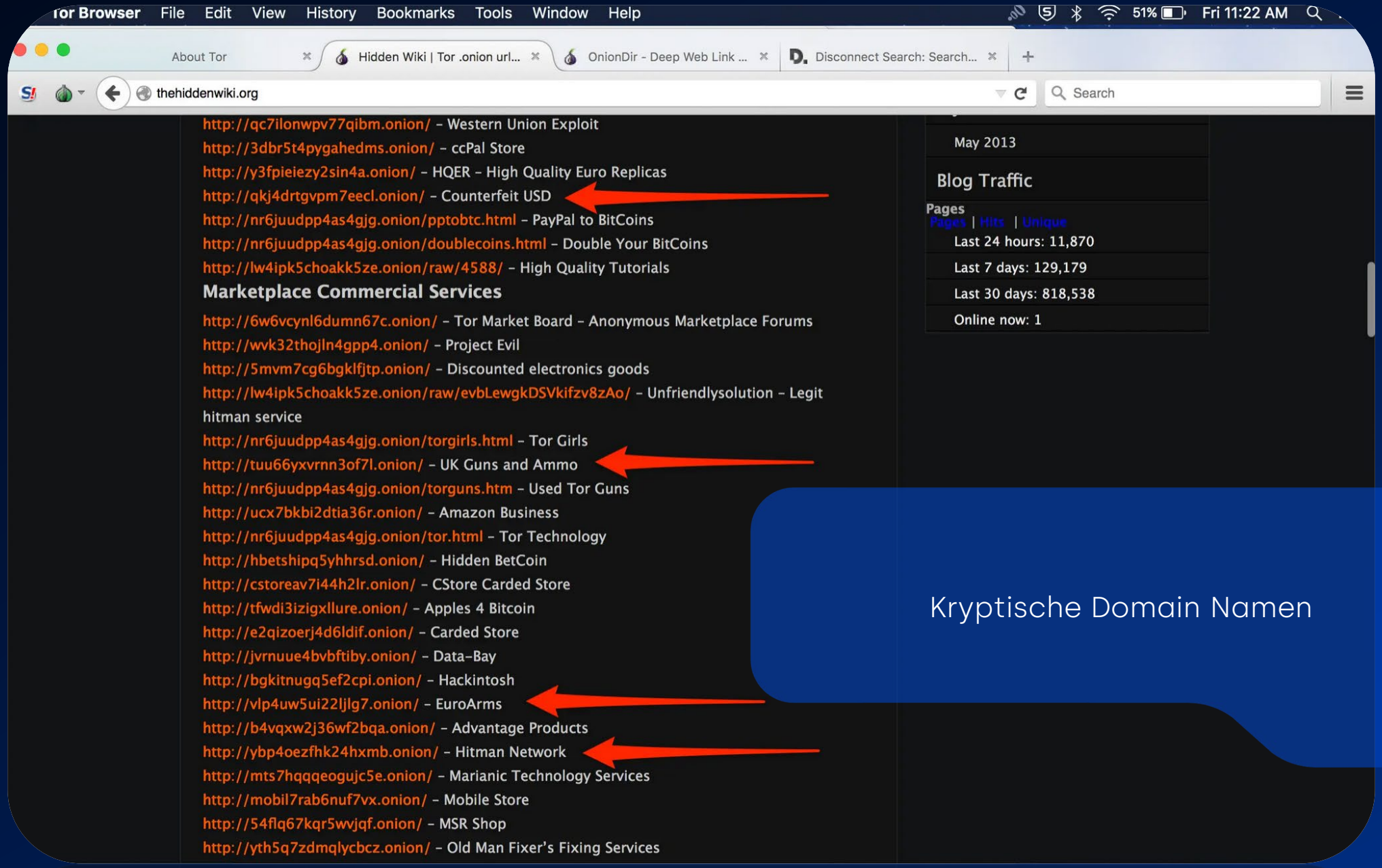
Deep Web
-Zugriffsbeschränkte / nicht indexierte Webseiten
-Datenbanken, Regierungen, Universitäten

Darknet
-Über “normale” Wege nicht auffindbare Webseiten
-Verschlüsselte Kommunikation
-Illegaler Inhalt, politischer Protest

Secutec

- Russisches Darknet
- Persisches Darknet
- Englisches Darknet
- Chinesisches Darknet

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



Kryptische Domain Namen

venus7rnkrbtdctbdtmvydn5kvjiaqmf2kgtzfup4muavc6wx4clwyqd.onion

ABOUT US | ADD $550 TO YOUR ACCOUNT AND GET FREE $150 | $ US DOLLAR

Wallet | Sign In | Register | 0

SORTED BY CATEGORIES

- CANNABIS & HASH
- BENZOS
- DISSOCIATIVES
- ECSTASY
- STIMULANTS
- OPIOIDS
- PSYCHEDELICS
- SOFTWARE & MALWARE
- COUNTERFEIT ITEMS
- POISON
- GOLD & JEWELS
- DIGITAL PRODUCTS
- STEROIDS
- ASSASSINATION

DRUGS & CHEMICALS

1/2 POUND SYNTHETIC K2 INCENSE BAGS (DAMIANA)

K2World — 1/2 Pound

Leaf (Damiana) Information: Potency: 10/10 Type of Leaf: Damiana Shipping Policy We ship orders everyday; some of our rules: -..

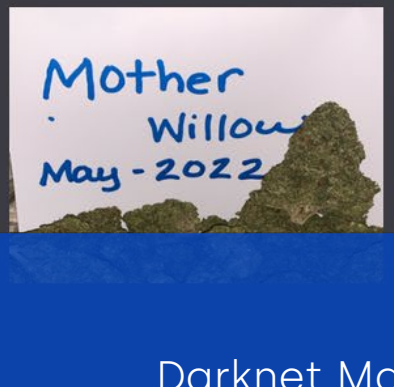
$850.00

1000 GRAMS S-ISOMER NEEDLE-KETAMINE HIGHEST QUALITY DISSOCIATIVE

drugshub — 1 kg

One of the Highest quality DUTCH Ketamine, available in needles (kind of little glass pieces) and as a powder. Exceptional space, good lasting and..

$12,762.00

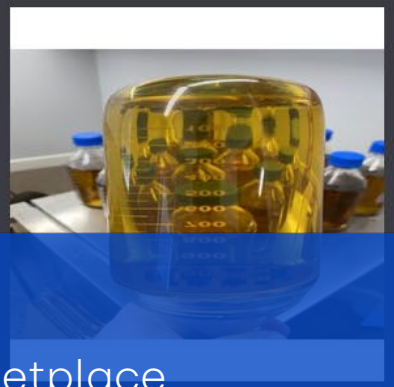


4 OZ OF WEDDIDNG CAKE!!! $500 112 GRAMS

Motherwillow — 4 oz

This is someone very nice potent smoke or an amazing deal. do yourself the favor xoxoWE USE USPS PRIORITY OR EXPRESS INTERNATIONAL SHIPPING . UP TO ..

$500.00



40 ML - THC DISTILLATE - EU - WW - ORANGE ZKITTLES TERPENES

jungleboyzeu — 40 ml

40 - 1000 ml of flavored THC distillate. Current strain Orange Zkittles Interested in starting your own cannabis business? Level up your clients..

$380.00

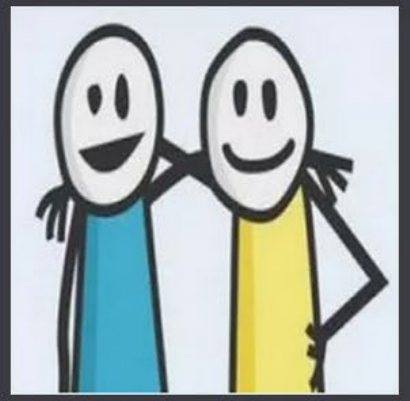
Darknet Marketplace

venus7rnkrbtdctbdtmvydn5kvjiaqmf2kgtzfup4muavc6wx4clwyqd.onion

VENUS MARKET

Wallet | Sign In | Register | 0

OTHERS



HOW TO MAKE 150K IN 21 DAYS CRYPTO SIGNALS,BOTS WORTH MILLIONS IN THE RIGHT HAND

Melvinbankz — Digital

3 Reasons To Join Our Rare Trading Community Right Away= * High-Performance Signals|Analysis Verified By Countless Of Trading Proofs. * 5 St..

$400.00

BUY NOW

FULLY VERIFIED USA, U K OR EU CRYPTO.COM ACCO UNT

feggmann — Digital

You will be getting the fullz, an d account details of the crypto.com with this account, you can attach a card or a bank account to buy crypto. the n..

$450.00

BUY NOW

SHORT PATH DISTILLATION ORIGINAL BLUEPRINT - INDUSTRIAL CAPACITY

datadudeKE — Digital

THC oil extraction is one main use for short path distillation go to www.uic-gmbh.de/en for more descriptive info included is a full scale plant..

$2,000.00

BUY NOW

TRAVEL PASSPORTS FOR USA, MEXICO AND GUATEMALA

Document

I provide genuine travel passports from the following countries for now USA, Mexico and Guatemala. countries will add as the pandemic reduces. con..

$2,800.00

BUY NOW

Darknet Marketplace

Dark Web Hackers

Products | Register | Login

Welcome to the Dark Web Hackers

Have you tried to buy hacking services on the dark web before? Not happy with the results? Only empty promises but no one getting the job done?

Then you should try Vladimir and George, the dark webs most trusted hackers for getting things done.

Unlike others, our prices are not the cheapest, but if we can't do a job, you will get a full refund!

Vladimir

Hello, my name is Vladimir.
I am the technical expert at dark web hackers.

My expertise is programming, running exploits, setting up DDOS attacks and i like the challenge of doing things where most others give up.
I can "recover" passwords of most social networks easily, remote control smartphones, and most other things that are useful because i spent years to find methods that really work.
Here you can find a list of my services, if it is not listed, then minimum price will be $600 and we will discuss the final price once you gave me all information and i accept the job.

Hacker as a Service

Full package deal, getting access to personal or company devices and accounts and searching for the data you need.	1800 USD = 0.09353 ฿	1 X Buy now
DDOS for protected websites for 1 month	900 USD = 0.04676 ฿	1 X Buy now
DDOS for unprotected websites for 1 month	400 USD = 0.02078 ฿	1 X Buy now
Hacking webservers, game servers or other internet infrastructure	1300 USD = 0.06755 ฿	1 X Buy now
30 days full service, i will work 8 hours per day for 30 days only on your project	9500 USD = 0.49361 ฿	1 X Buy now
Other services, final price will be discussed	600 USD = 0.03118 ฿	1 X Buy now
Only additionaly: Add this item if your target is a high profile VIP or large public company	2500 USD = 0.12990 ฿	1 X Buy now

Hacker as a Service

George

Hello, my name is George.
My hacking skills are not as perfect as Vladimir's, but i am really good with social engineering.
And i really like messing with people, i don't care what you want to do to them.
If there is something i can't do then Vladimir will help and teach me for next time.

Product	Price	Quantity
Destroying someones life: Your target will have legal problems or financial problems, proven methods including child porn that always works	1700 USD = 0.08833 ฿	1 X Buy now
Spreading false information about someone on social media, not as life ruining but still nasty	450 USD = 0.02338 ฿	1 X Buy now
Social engineering to get secrets from a person, private or from some employee	450 USD = 0.02338 ฿	1 X Buy now

Social Engineering as a Service


Secutec
Die Welt der Hackergruppen

Wieviel Prozent
von 100 Unternehmen
könnte einer der besten
Hacker in Europa hacken?

Secutec

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, ...

50-70 professionelle Hacker Gruppe, die Unternehmen angreifen, um Lösegeld zu erpressen.

Die Top Organisation erpressen im Jahr teilweise bis zu 500 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

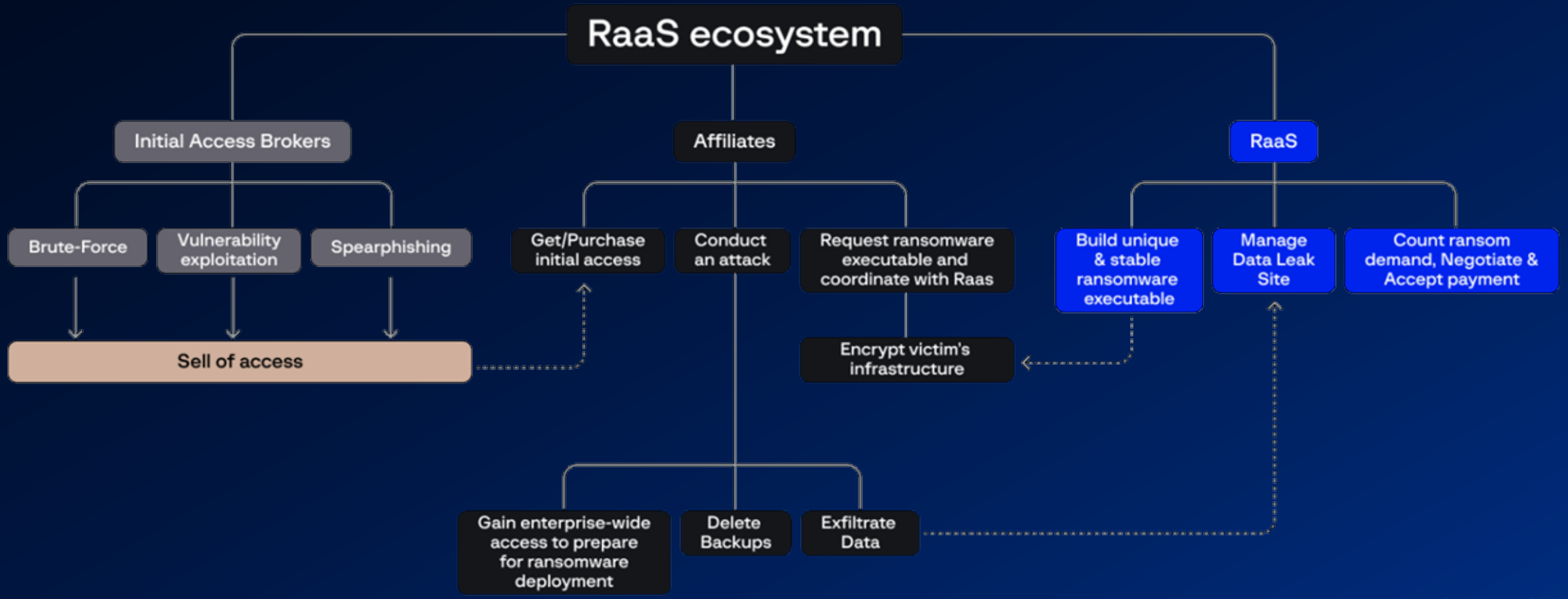
Einzeltäter und politisch motivierte Gruppen

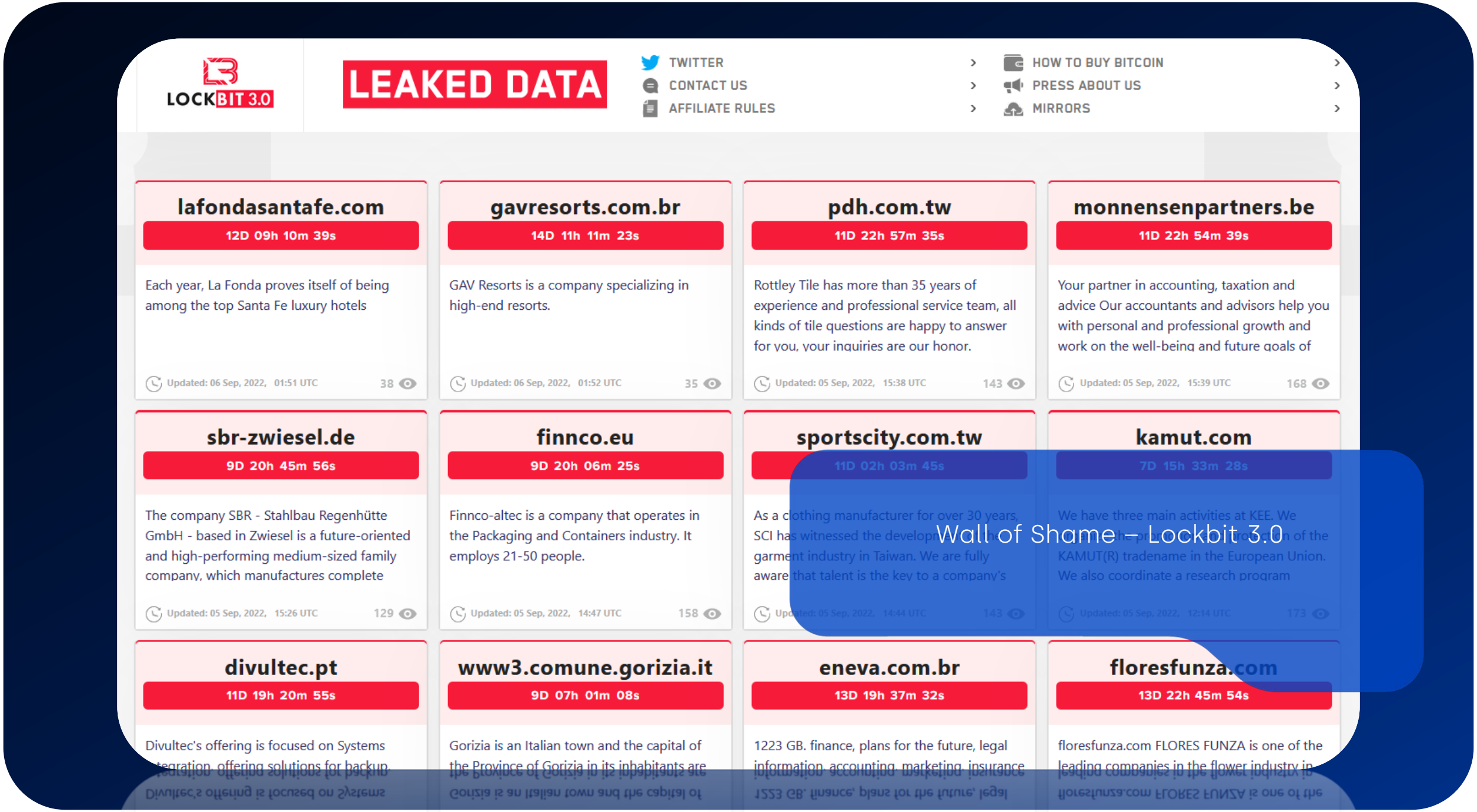
Anonymous
Hacktivismus - als Protestmittel, für politische und ideologische Ziele.

NoName057, Killnet
Pro russische Hackergruppen, die gezielt den Westn angreifen.

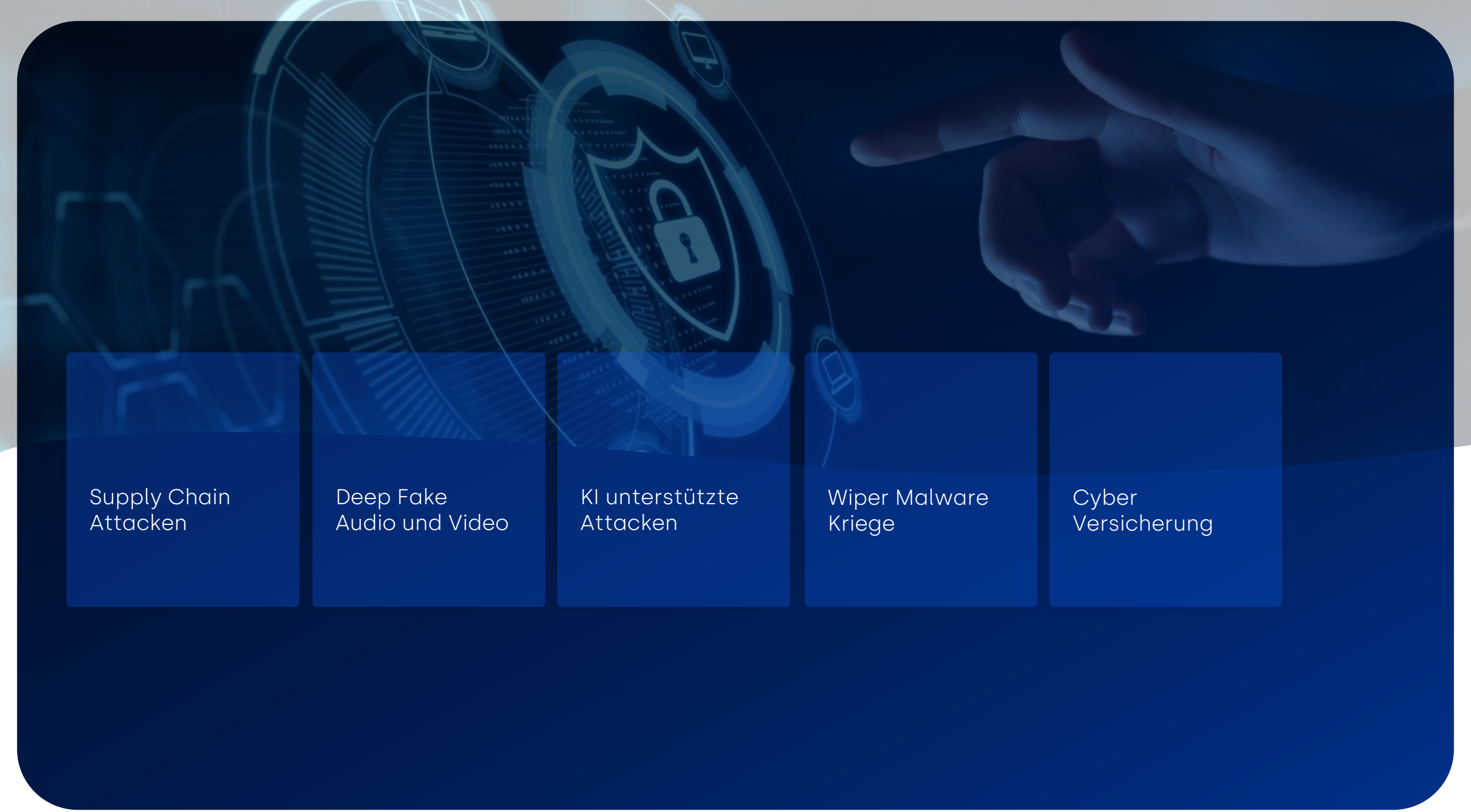
ZIELE: Politische und Ideologische Ziele erreichen, Privatpersonen

Secutec


RaaS ecosystem
Initial Access Brokers
Affiliates
RaaS
Brute-Force
Vulnerability exploitation
Spearphishing
Get/Purchase initial access
Conduct an attack
Request ransomware executable and coordinate with Raas
Build unique & stable ransomware executable
Manage Data Leak Site
Count ransom demand, Negotiate & Accept payment
Sell of access
Encrypt victim's infrastructure
Gain enterprise-wide access to prepare for ransomware deployment
Delete Backups
Exfiltrate Data



Wall of Shame – Lockbit 3.0



Supply Chain Attacken

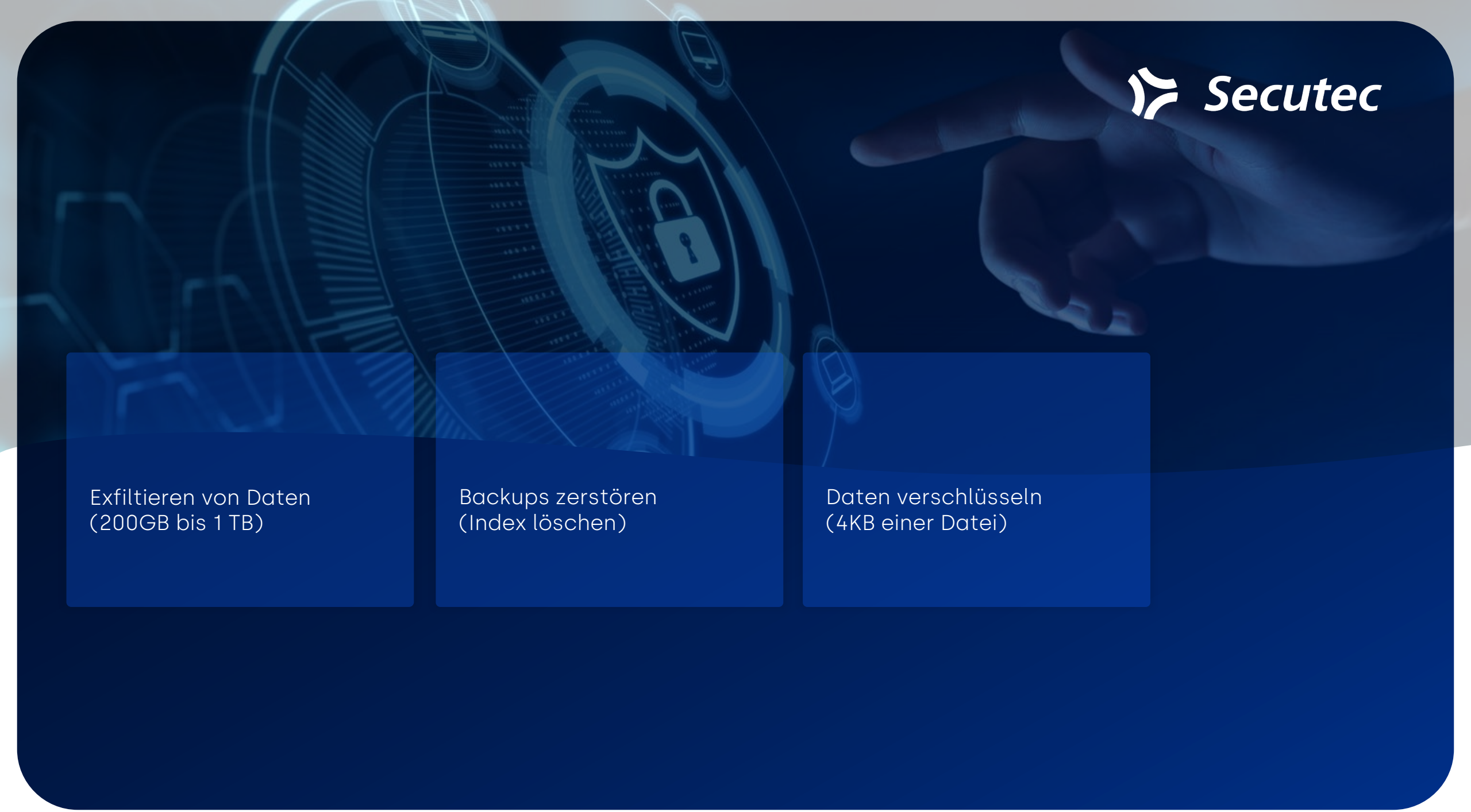
Deep Fake Audio und Video

KI unterstützte Attacken

Wiper Malware Kriege

Cyber Versicherung


Secutec
Die Ransomware Attacke



Secutec

Exfiltieren von Daten
(200GB bis 1 TB)

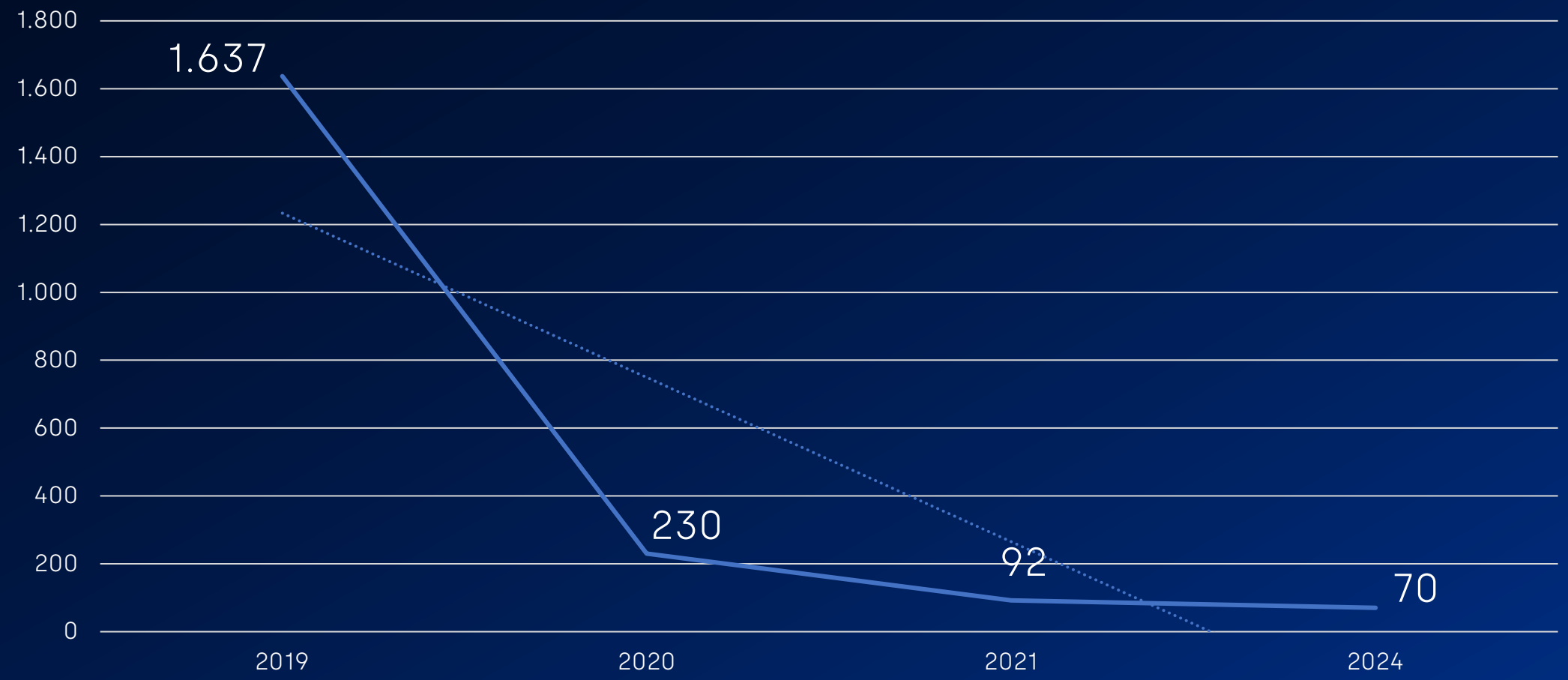
Backups zerstören
(Index löschen)

Daten verschlüsseln
(4KB einer Datei)

Wie viele Stunden benötigen Hacker 2021 von der Schwachstelle bis zur Verschlüsselung?

2019 waren es 1.637 Stunden oder 68 Tage

Initial Access via Broker zum Ransomware Deployment (Stunden)




Angriffsvektoren
Phishing
(Fokus New Domains)
Lösung: SecureDNS
Brute-Force Attacken
(Wellen bei größeren Leaks)
Lösung: Darknet Monitoring
Passwort Stealer/Keylogger
(Private- und Firmengeräte)
Lösung: Darknet Monitoring
Exploit Vulnerability
(Platzierung von Backdoors)
Lösung: Attack Surface Management
Supply Chain Attacken
(Lieferketten und Kunden)
Lösung: ASM und Darknet Monitoring
Man in the Middle
(Fokus Rechnungsbelege)
Lösung: SecureDNS, Threat Hunting, M365 Kit
Deep Fake
(Audio und Video)
O365 Phishing
(Proxy/Cache - Logindaten/MFA)
Lösung: M365 Security Kit

Secutec

Die ersten 48 Stunden nach der Attacke

-Die Server nicht herunterfahren!

-Start der Forensik (Wie, Wer, Was)

-Darknet Monitoring

-Klare Strategie / Organisation (intern/extern)

-Priorisieren der Daten und Systeme

-Isolieren der verschlüsselten Systeme vom Rest

Secutec

Lösegeld-forderungen

- Decken sich oft mit den liquiden Mitteln.
  Bilanzen sind in vielen Fällen bekannt.
  Start Forderung meist 5-8% vom Umsatz.

- Argumente über nicht liquide Mittel warden
  oftmals mit aktuellen Bankauszügen widerlegt.

Hello!

Visit our Blog:

Tor Browser Links:
    http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/

Links for normal browser:
    http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/

>>> Your data is stolen and encrypted.

- If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

>>> If you have an external or cloud backup; what happens if you don’t agree with us?

- All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not agree with us, information pertaining to your companies and the data of your company’s customers will be published on the internet, and the respective country’s personal data usage authority will be informed. Moreover, confidential data related to your company will be shared with potential competitors through email and social media. You can be sure that you will incur damages far exceeding the amount we are requesting from you should you decide not to agree with us.

>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because the negotiations will make them look incompetent,After the incident report is handed over to the government department, you will be fined <This will be a huge amount,Read more about the GDRP legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>,The government uses your fine to reward them.And you will not get anything, and except you and your company, the rest of the people will forget what happened!!!!!

>>> How to contact with us?

- Install and run 'Tor Browser' from https://www.torproject.org/download/
- Go to http://an2ce4pqpf2ipvba2djurxi5pnxxhu3uo7ackul6eafcundqtly7bhid.onion/
- Log in using the Client ID:

Empfehlungen

Secutec

DNS Monitoring Auch IoT Devices beachten!	**Externe Scans Schwachstellen** Aus Sicht eines Cyberkriminellen	**Darknet Monitoring** User, Keylogger, VIPs, Keywords	**Incident Vorbereitung** Geschäftsleitung nicht vegessen!	**Playbook Notfallhandbuch** Hacker Attacke Blackout, usw.
Multifaktor Authentifizierung Nicht nur mit Bestätigung!	**EDR/XDR Virenscanner** Anomalie-erkennung	**Backup Konzept und Recovery** Testen nicht vergessen!	**Server Logs Backup** Rund 90 Tage für Forensik	**Netzwerk Segmentierung** Firewall nicht vergessen!
Keine lokalen Admin Rechte Nur temporäre Rechte zulassen	**Active Directory Tiering Struktur** Eigene User für Server und DC	**Passwort Manager** Verwaltung und sichere Passwörter (+Privatnutzung)		

Secutec

SecureDNS Teststellung kostenlos in 20 Minuten!
Das Beste aus Black- und Whitelist!

- XDR Integration Sentinel One
- Integrierte Phishing Rootkits Detection

NEU

Secutec

Mag. Daniel Rossgatterer, MBA
CEO Secutec GmbH

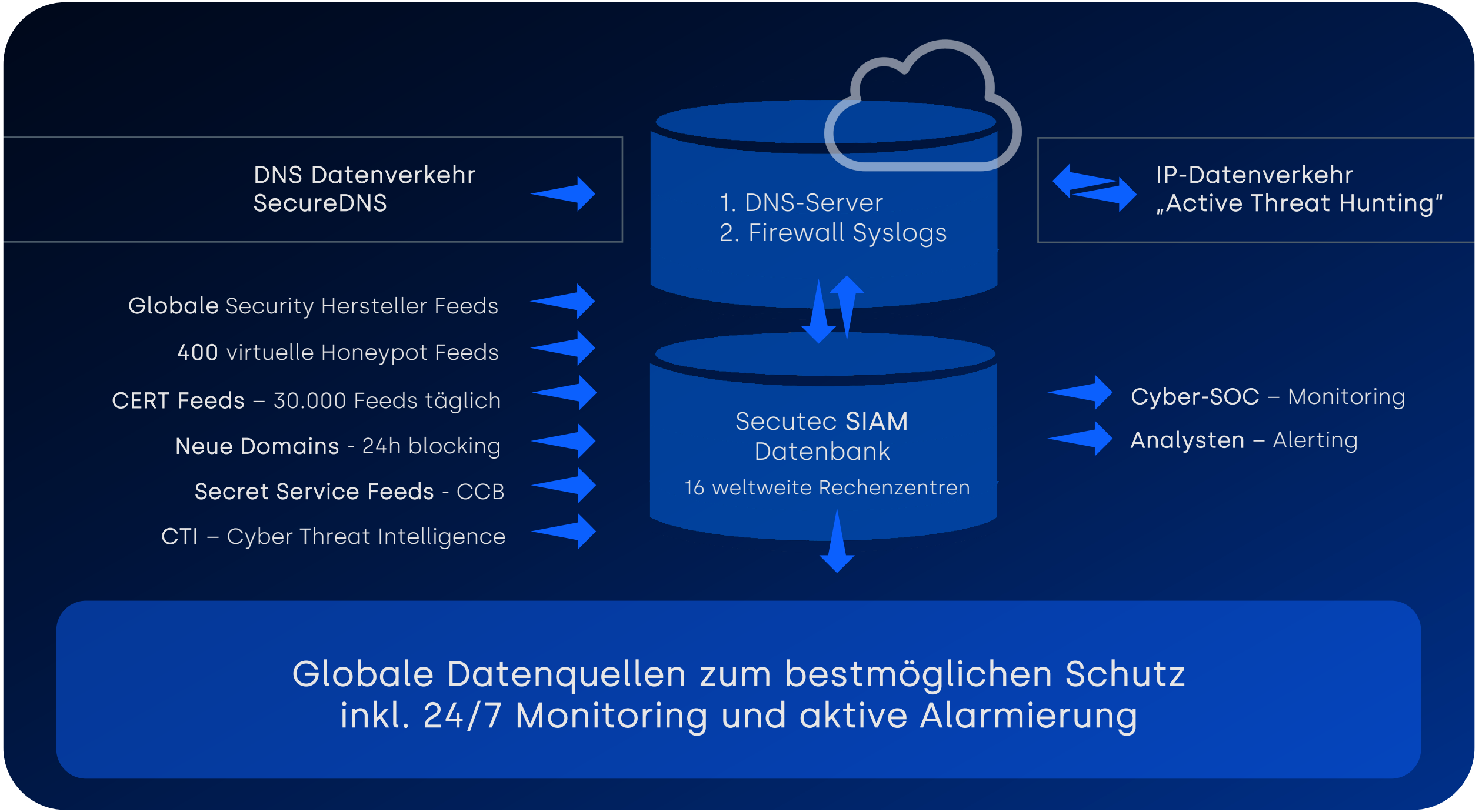
Let´s connect!


Secutec
Cyber Security Intelligence

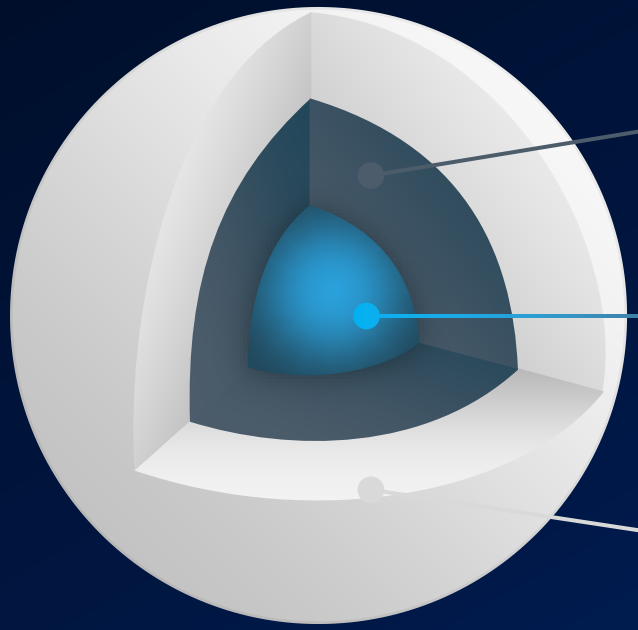

Secutec
Secutec SecureDNS

Secutec

SecureDNS überwacht alle DNS Verbindungen 24/7, blockiert bedrohliche DNS Anfragen mit einer globalen einzigartigen 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 - CCB
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

Secutec



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

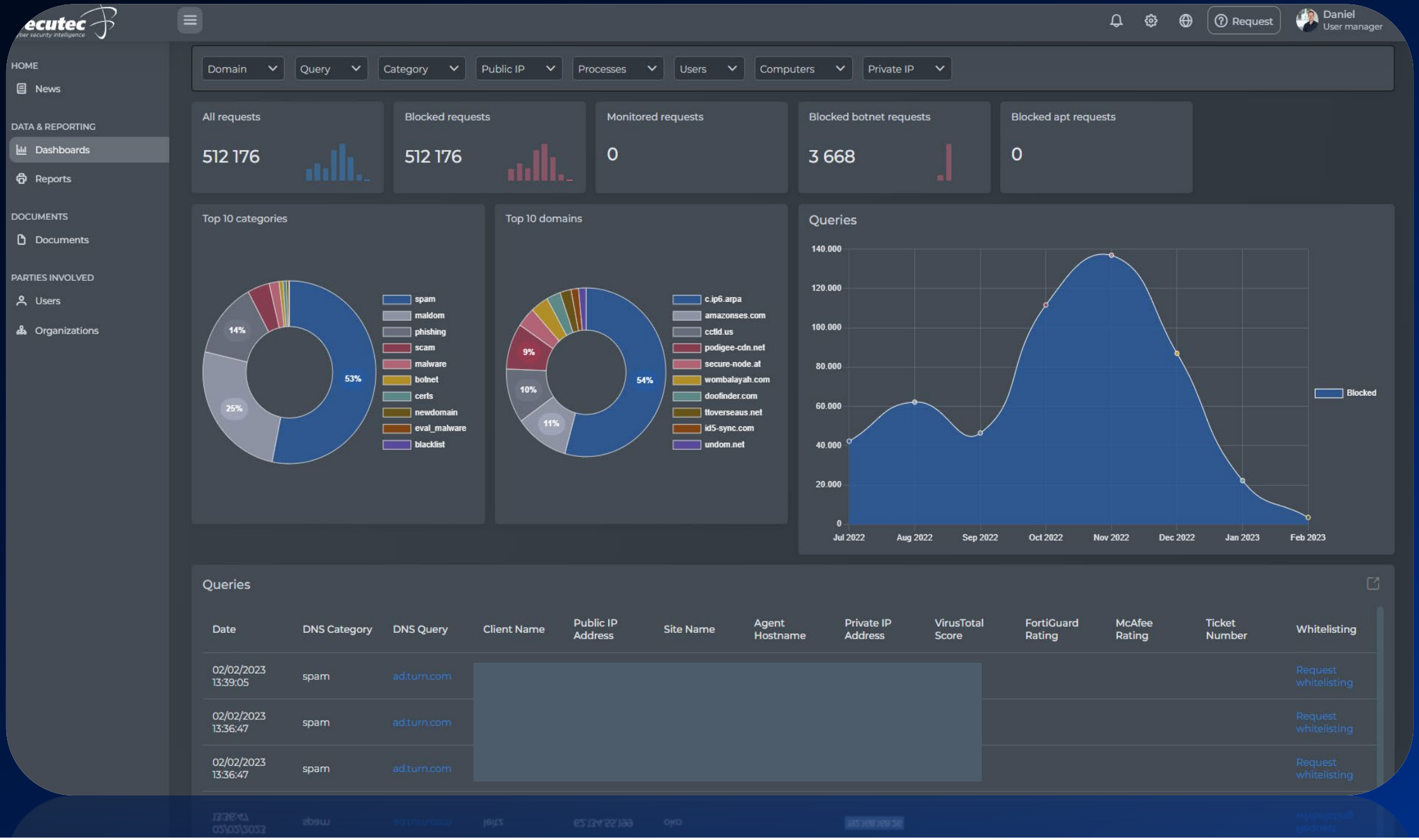
Keine spürbaren False Positive Bewertungen

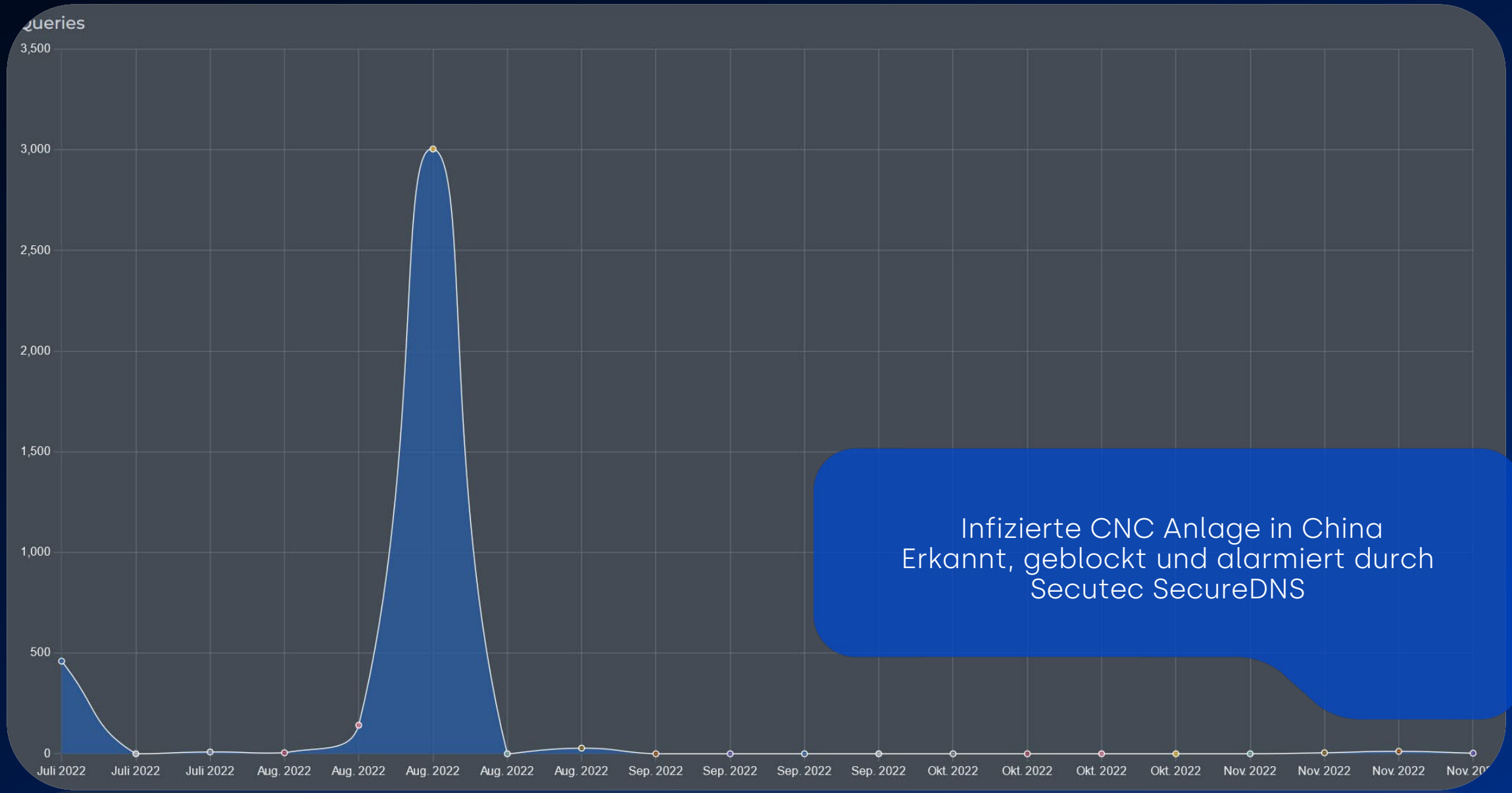
Secutec SecureDNS

Mehrwerte im Vergleich zu anderen Lösungen.

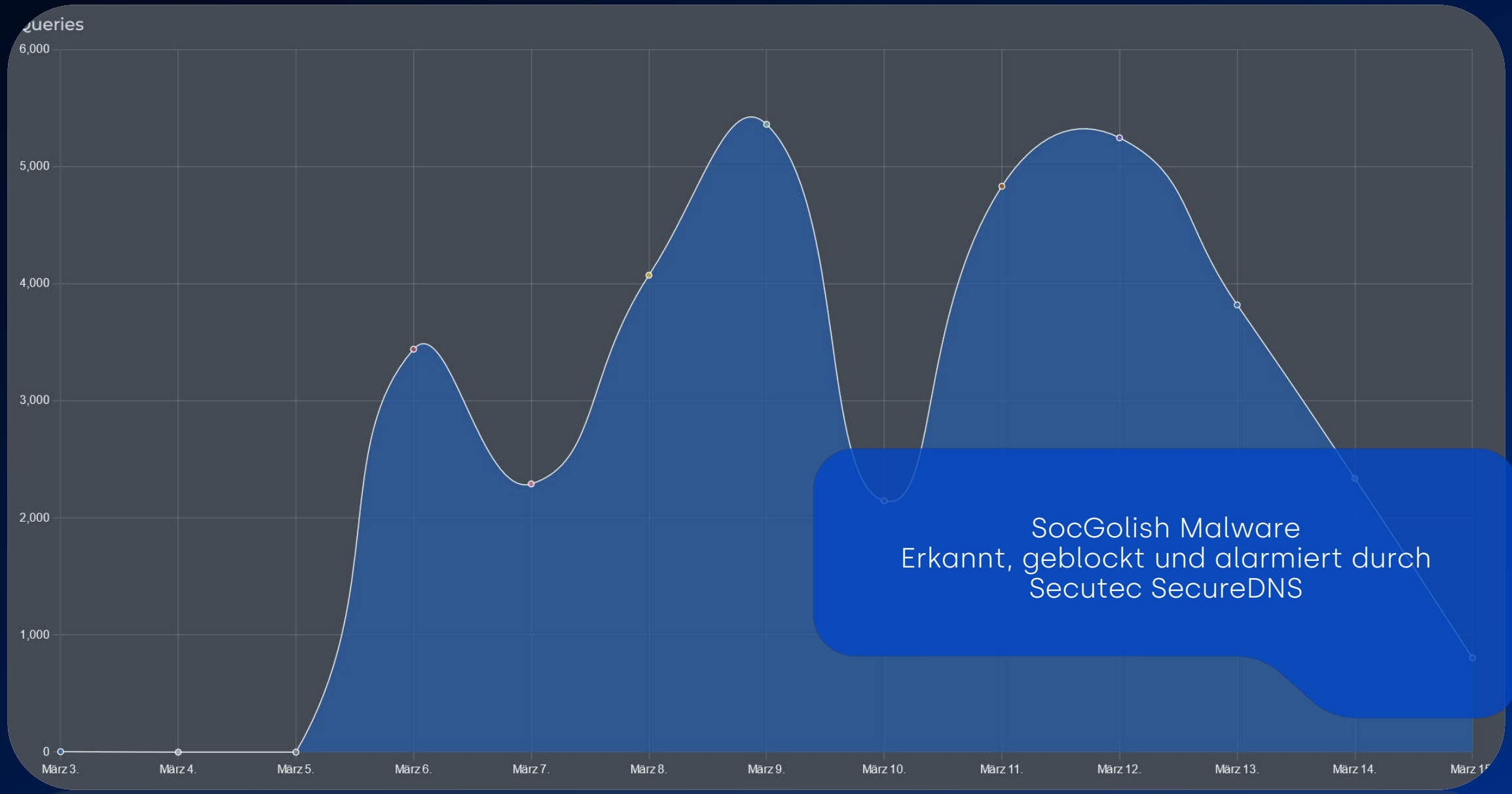
Expertise

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


ecutec
Request
Daniel
User manager
HOME
News
DATA & REPORTING
Dashboards
Reports
DOCUMENTS
Documents
PARTIES INVOLVED
Users
Organizations
Domain
Query
Category
Public IP
Processes
Users
Computers
Private IP
All requests
512 176
Blocked requests
512 176
Monitored requests
0
Blocked botnet requests
3 668
Blocked apt requests
0
Top 10 categories
spam
maldom
phishing
scam
malware
botnet
certs
newdomain
eval_malware
blacklist
53%
25%
14%
Top 10 domains
c.ip6.arpa
amazonses.com
cctld.us
podigee-cdn.net
secure-node.at
wombalayah.com
doofinder.com
ttoverseaus.net
id5-sync.com
undom.net
54%
11%
10%
9%
Queries
140.000
120.000
100.000
80.000
60.000
40.000
20.000
0
Jul 2022
Aug 2022
Sep 2022
Oct 2022
Nov 2022
Dec 2022
Jan 2023
Feb 2023
Blocked
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



Infizierte CNC Anlage in China
Erkannt, geblockt und alarmiert durch
Secutec SecureDNS


Queries
6,000
5,000
4,000
3,000
2,000
1,000
0
März 3.
März 4.
März 5.
März 6.
März 7.
März 8.
März 9.
März 10.
März 11.
März 12.
März 13.
März 14.
SocGolish Malware
Erkannt, geblockt und alarmiert durch
Secutec SecureDNS


Secutec
Secutec SecureSIGHT

Secutec

SecureSIGHT ist eine Threat Intelligence Plattform, die von extern permanten Cyber Risiken im Bereich Darknet, Vulnerabilities und IP- Verbindungen bewertet und bei Bedrohungen aktiv alarmiert .

Secutec

Attack Surface Management

- 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

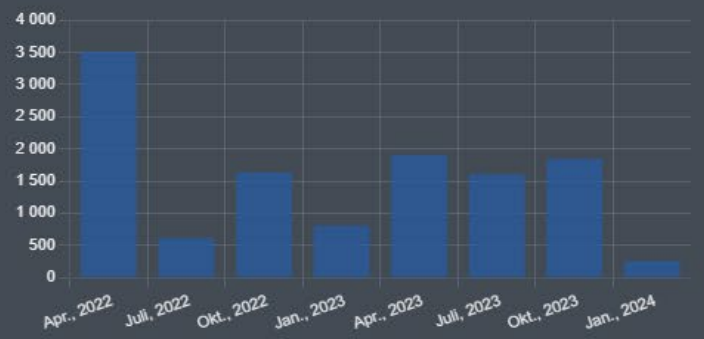
Dashboard | Attack Surface M... | SecureSIGHT - Dashboard - Attack Surface Management - Risks

secutecat | Nur Organisation

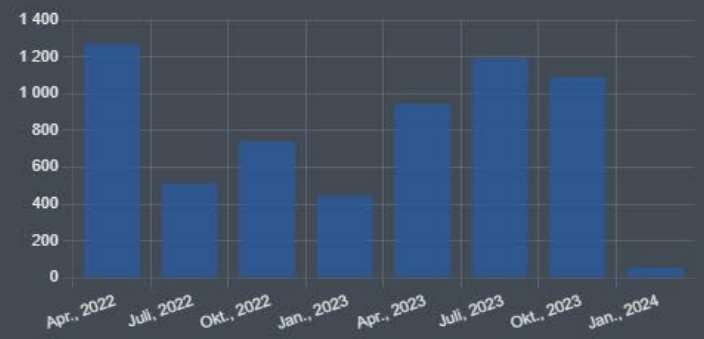
Security Rating | Title

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

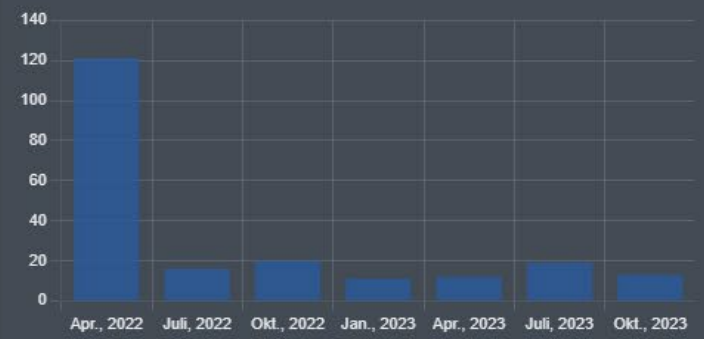
Risks Discovered



Risks Solved

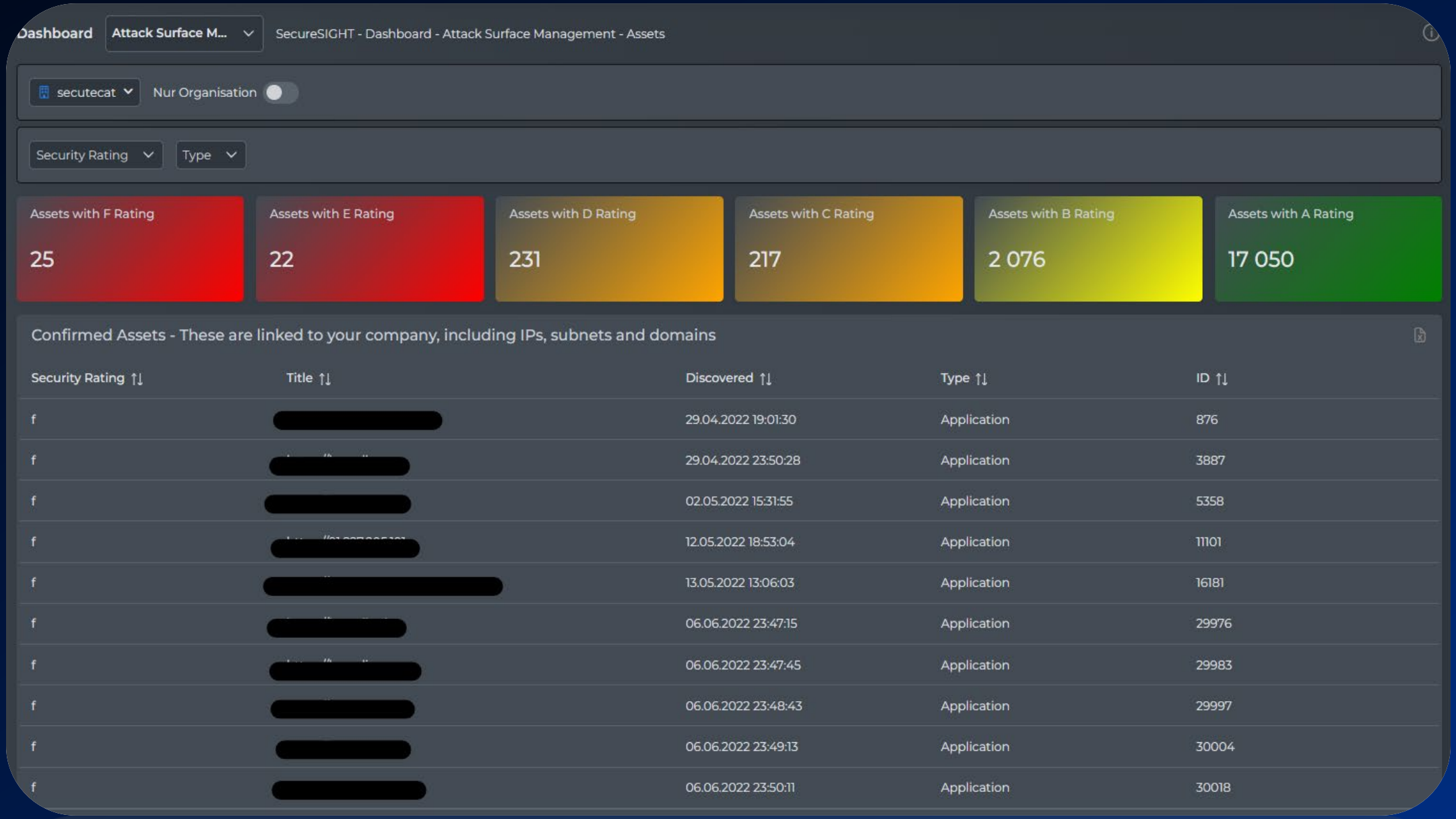


Risks Mitigated



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


Dashboard
Attack Surface M...
SecureSIGHT - Dashboard - Attack Surface Management - Assets
secutecat
Nur Organisation
Security Rating
Type
Assets with F Rating
25
Assets with E Rating
22
Assets with D Rating
231
Assets with C Rating
217
Assets with B Rating
2 076
Assets with A Rating
17 050
Confirmed Assets - These are linked to your company, including IPs, subnets and domains
Security Rating
Title
Discovered
Type
ID
f
29.04.2022 19:01:30
Application
876
f
29.04.2022 23:50:28
Application
3887
f
02.05.2022 15:31:55
Application
5358
f
12.05.2022 18:53:04
Application
11101
f
13.05.2022 13:06:03
Application
16181
f
06.06.2022 23:47:15
Application
29976
f
06.06.2022 23:47:45
Application
29983
f
06.06.2022 23:48:43
Application
29997
f
06.06.2022 23:49:13
Application
30004
f
06.06.2022 23:50:11
Application
30018

Secutec

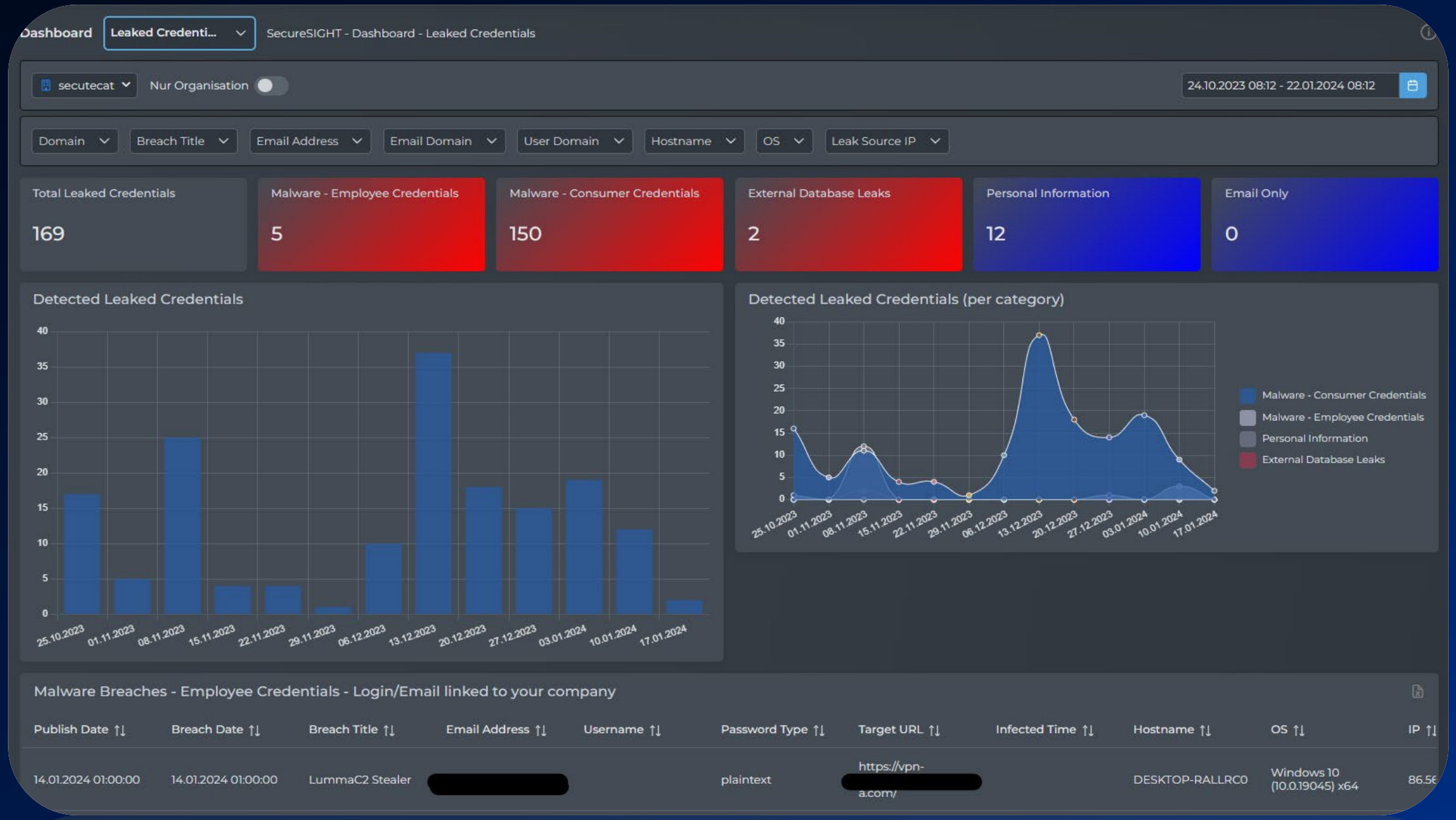
Darknet Monitoring

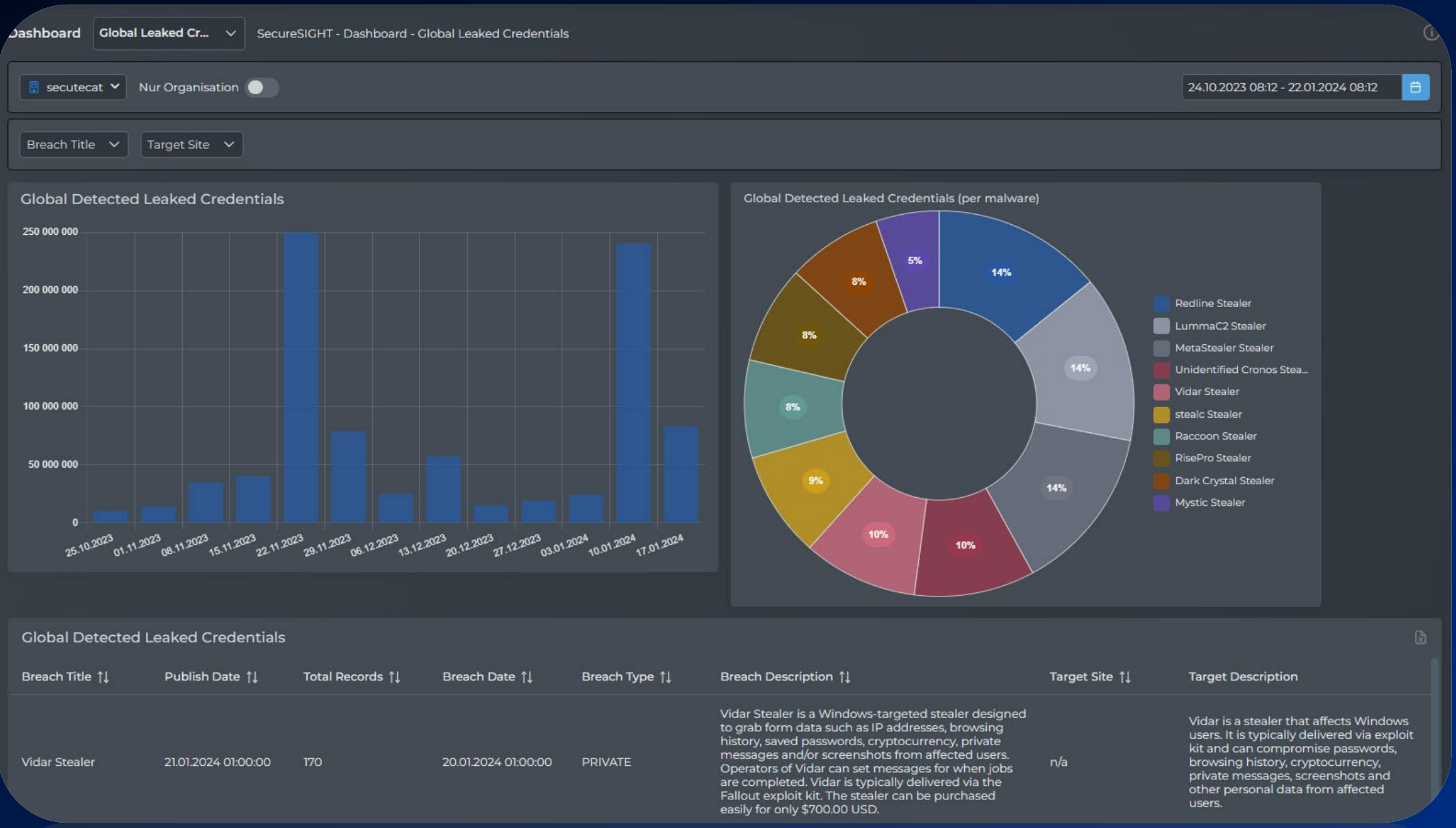
- Aktives Darknet Monitoring im Bereich Darknetseiten, Foren, Chats, Marktplätze

- 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
169
Malware - Employee Credentials
5
Malware - Consumer Credentials
150
External Database Leaks
2
Personal Information
12
Email Only
0
Detected Leaked Credentials
40
35
30
25
20
15
10
5
0
25.10.2023
01.11.2023
08.11.2023
15.11.2023
22.11.2023
29.11.2023
06.12.2023
13.12.2023
20.12.2023
27.12.2023
03.01.2024
10.01.2024
17.01.2024
Detected Leaked Credentials (per category)
Malware - Consumer Credentials
Malware - Employee Credentials
Personal Information
External Database Leaks
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
plaintext
https://vpn-
a.com/
DESKTOP-RALLRC0
Windows 10
(10.0.19045) x64


Dashboard
Global Leaked Cr...
SecureSIGHT - Dashboard - Global Leaked Credentials
secutecat
Nur Organisation
24.10.2023 08:12 - 22.01.2024 08:12
Breach Title
Target Site
Global Detected Leaked Credentials
250 000 000
200 000 000
150 000 000
100 000 000
50 000 000
0
25.10.2023
01.11.2023
08.11.2023
15.11.2023
22.11.2023
29.11.2023
06.12.2023
13.12.2023
20.12.2023
27.12.2023
03.01.2024
10.01.2024
17.01.2024
Global Detected Leaked Credentials (per malware)
14%
14%
14%
10%
10%
9%
8%
8%
8%
5%
Redline Stealer
LummaC2 Stealer
MetaStealer Stealer
Unidentified Cronos Stea...
Vidar Stealer
stealc Stealer
Raccoon Stealer
RisePro Stealer
Dark Crystal Stealer
Mystic Stealer
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.

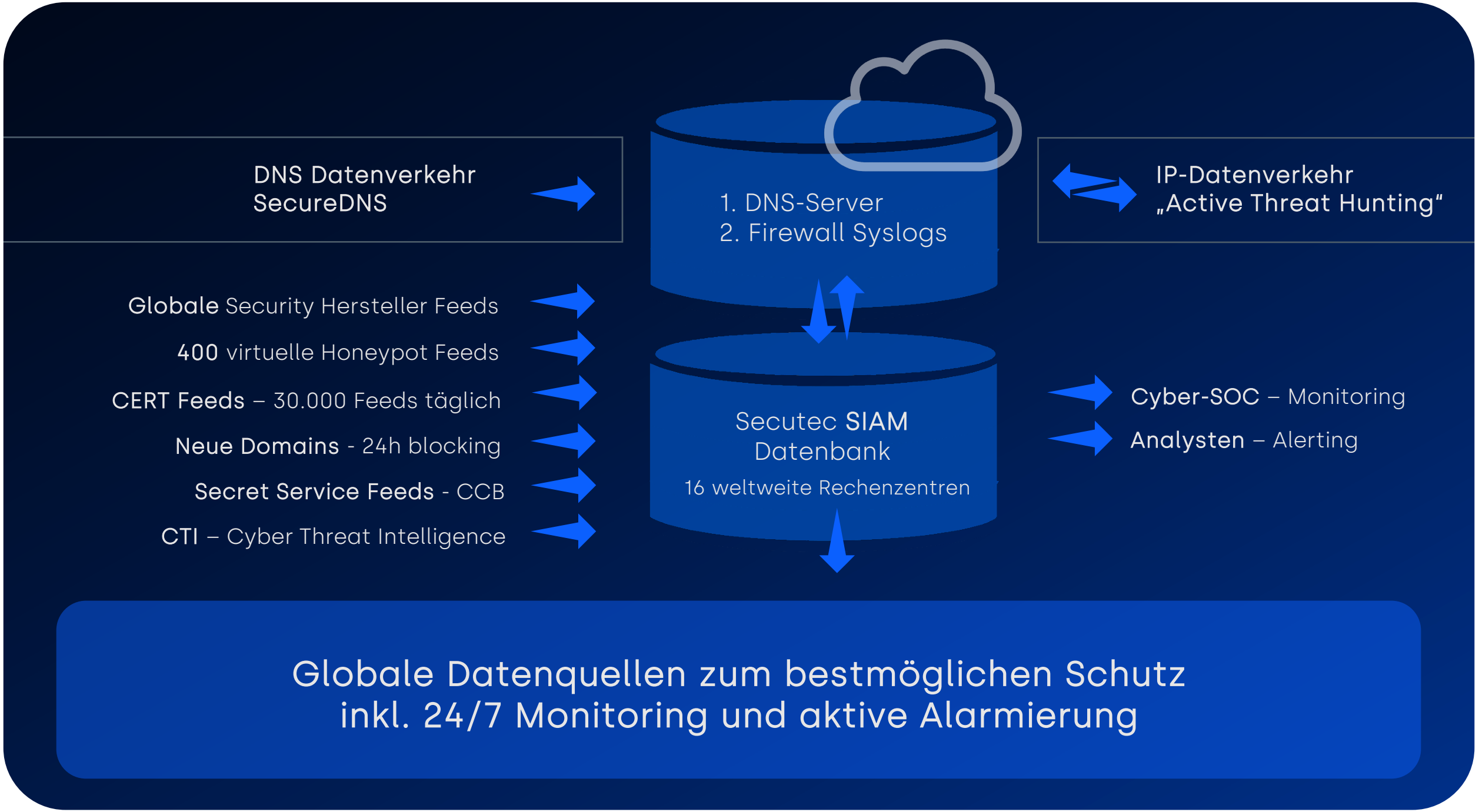
Secutec

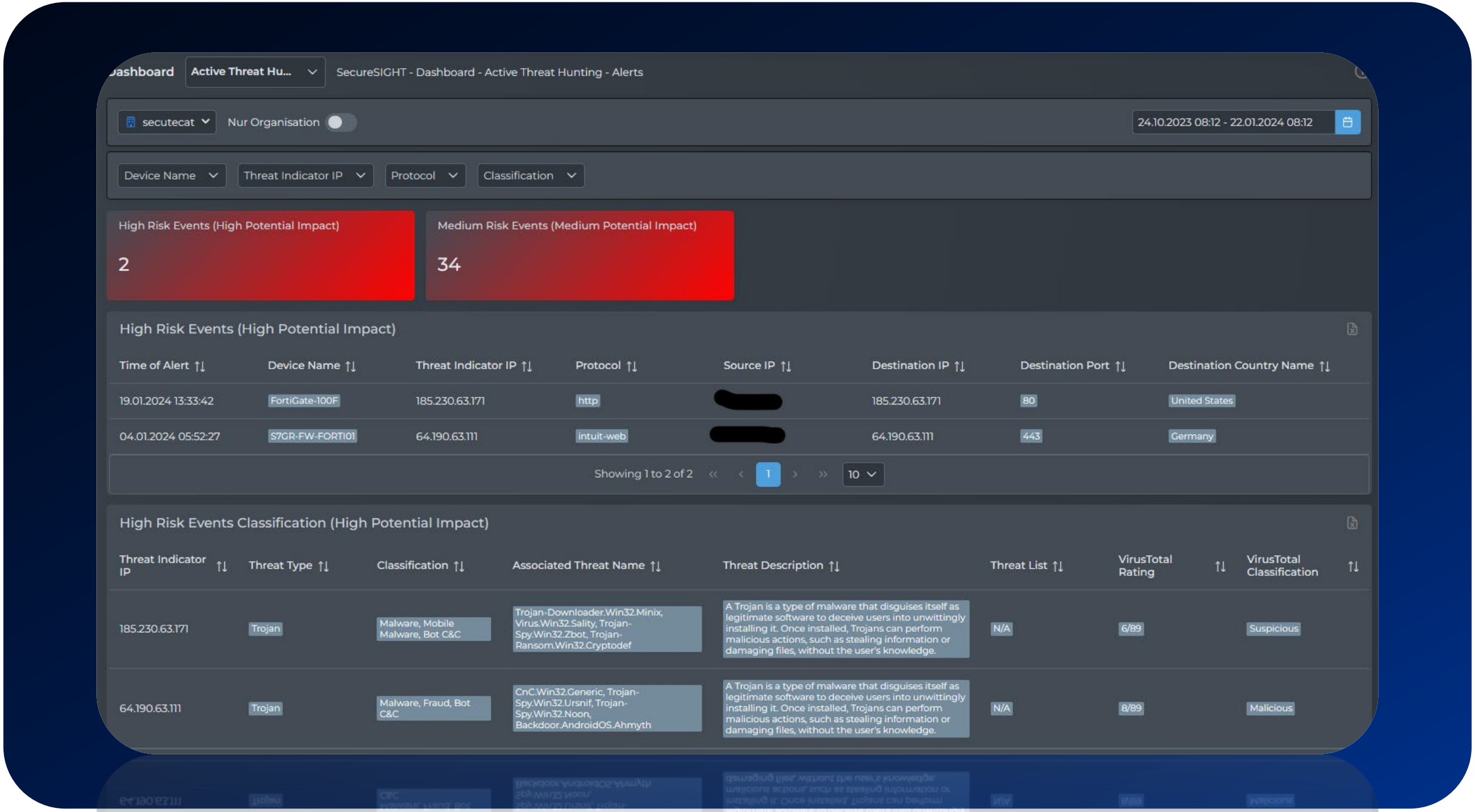
Active Managed Threat Hunting

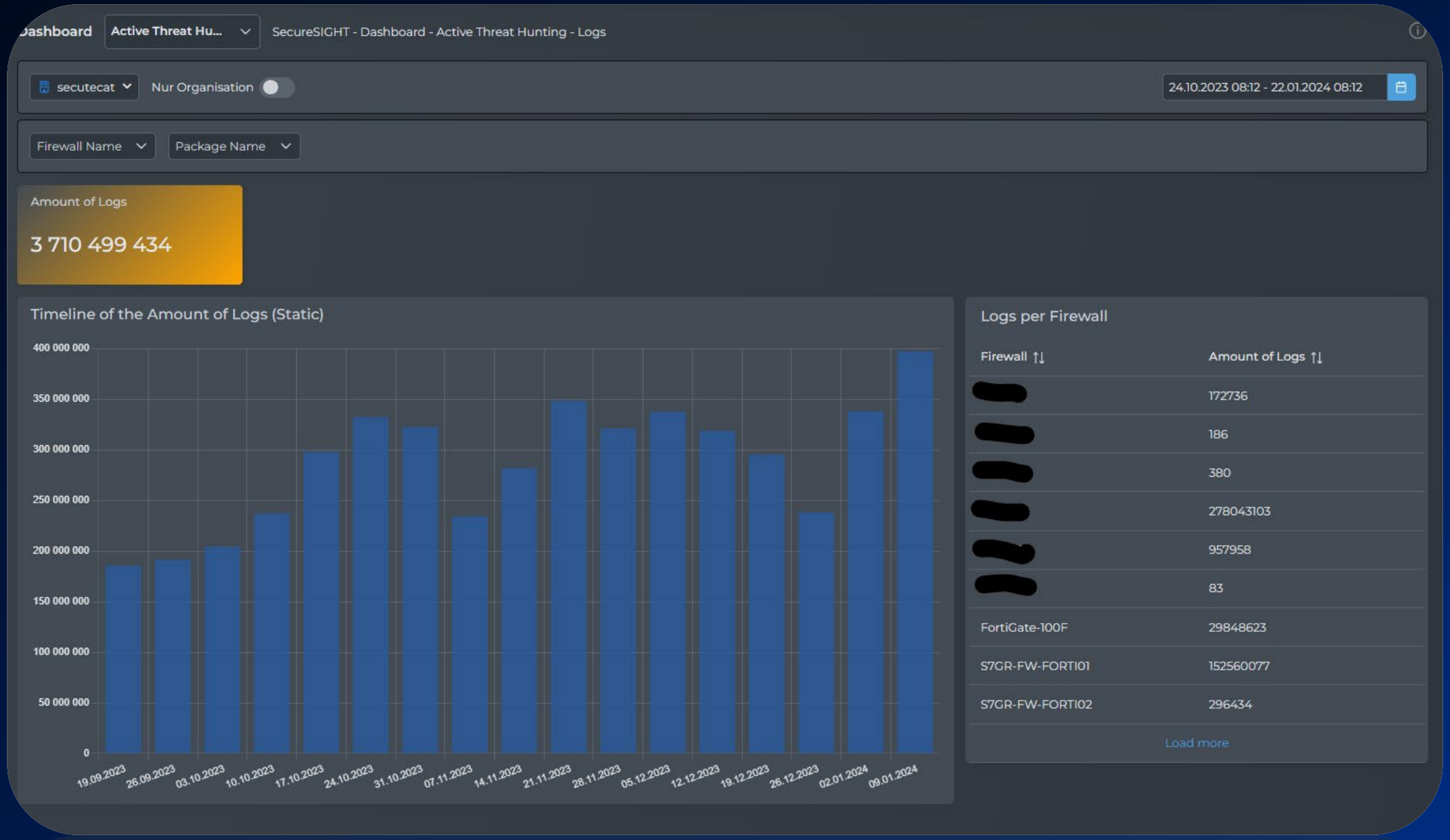
- 24/7 Überwachung aller IP-Datenverbindungen, die von der Firewall nicht blockiert wurden.

- 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 - CCB
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


Dashboard
Active Threat Hu...
SecureSIGHT - Dashboard - Active Threat Hunting - Alerts
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
185.230.63.171
80
United States
04.01.2024 05:52:27
S7GR-FW-FORTI01
64.190.63.111
intuit-web
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


Dashboard
Active Threat Hu...
SecureSIGHT - Dashboard - Active Threat Hunting - Logs
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)
400 000 000
350 000 000
300 000 000
250 000 000
200 000 000
150 000 000
100 000 000
50 000 000
0
19.09.2023
26.09.2023
03.10.2023
10.10.2023
17.10.2023
24.10.2023
31.10.2023
07.11.2023
14.11.2023
21.11.2023
28.11.2023
05.12.2023
12.12.2023
19.12.2023
26.12.2023
02.01.2024
09.01.2024
Logs per Firewall
Firewall
Amount of Logs
172736
186
380
278043103
957958
83
FortiGate-100F
29848623
S7GR-FW-FORTI01
152560077
S7GR-FW-FORTI02
296434
Load more


Secutec
Secutec SecureRESPONSE

Secutec

Incident Response Service

- 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

Cybersecurity Intelligence

Prevent now, secure tomorrow