



Secutec

Cybersecurity Intelligence

Prevent now, secure tomorrow

Präventiv schützen!

Entwicklung und Expertise in
Cyber Threat Intelligence
Technologie in Europa seit 2005.

Hilfe leisten!

Erfahrungen aus hunderten
Incident Response Fällen,
Verhandlungen und
Lösegeldzahlungen.

Secutec wins exclusive €35 million contract with CCB for delivery of cyber threat intelligence feeds.



„Secutec weiß, was CTI-Feeds sind
und wie man sie effizient einsetzt.“

Miguel De Bruycker, Generaldirektor CCB



CENTRE FOR
CYBERSECURITY
BELGIUM

Secutec wurde 2005 gegründet mit der Vision, weltweites Wissen über Bedrohungen in einer Technologie zu bündeln.

Cyber Security = Multi-Vendor-Strategie

Datenquelle 1:
Antiviren- 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

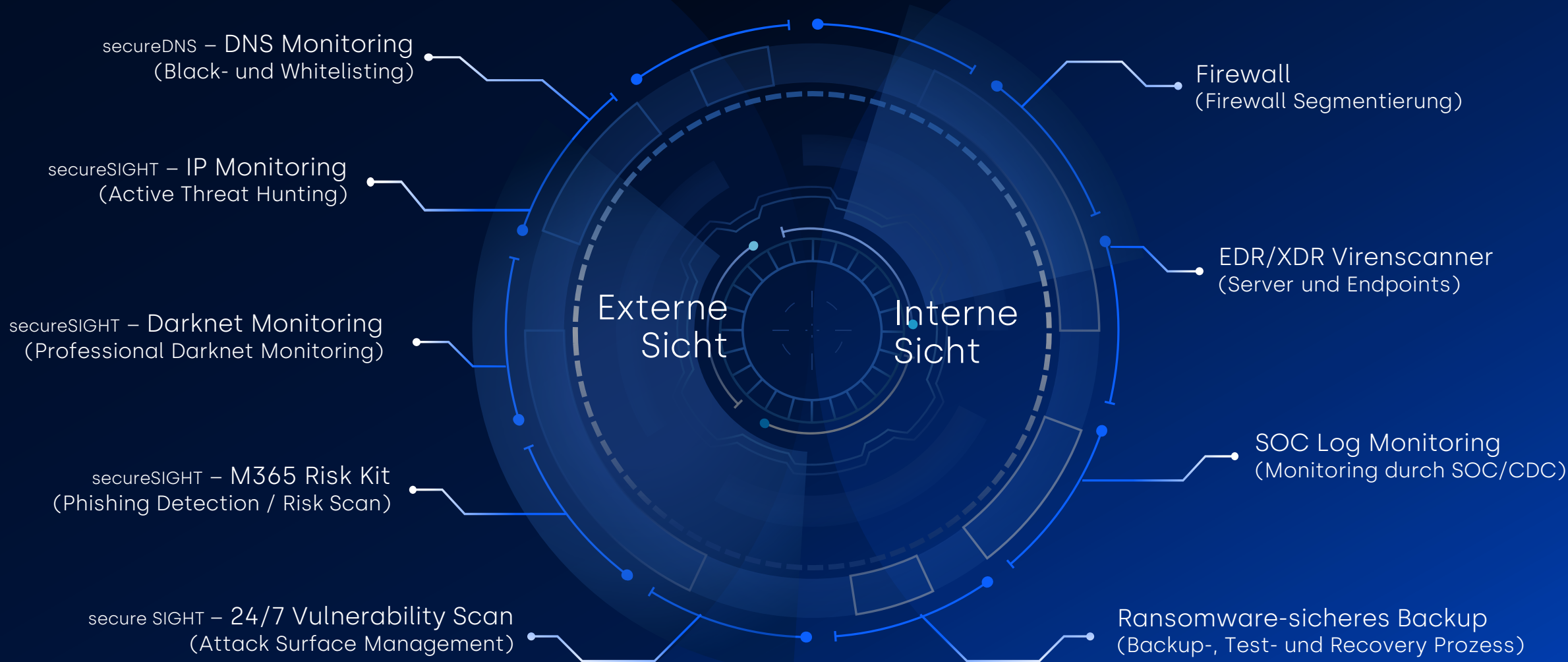
Cyber Bedrohungen, die
durch Checks von Secutec
erkannt und an Behörden und
Partner weitergegeben
werden



Secutec Integrated Advanced Malware Database (SIAM)

SECUTEC Layer (externe Sicht)

Kunde / SOC (interne Sicht)



SECUTECH 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.“

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

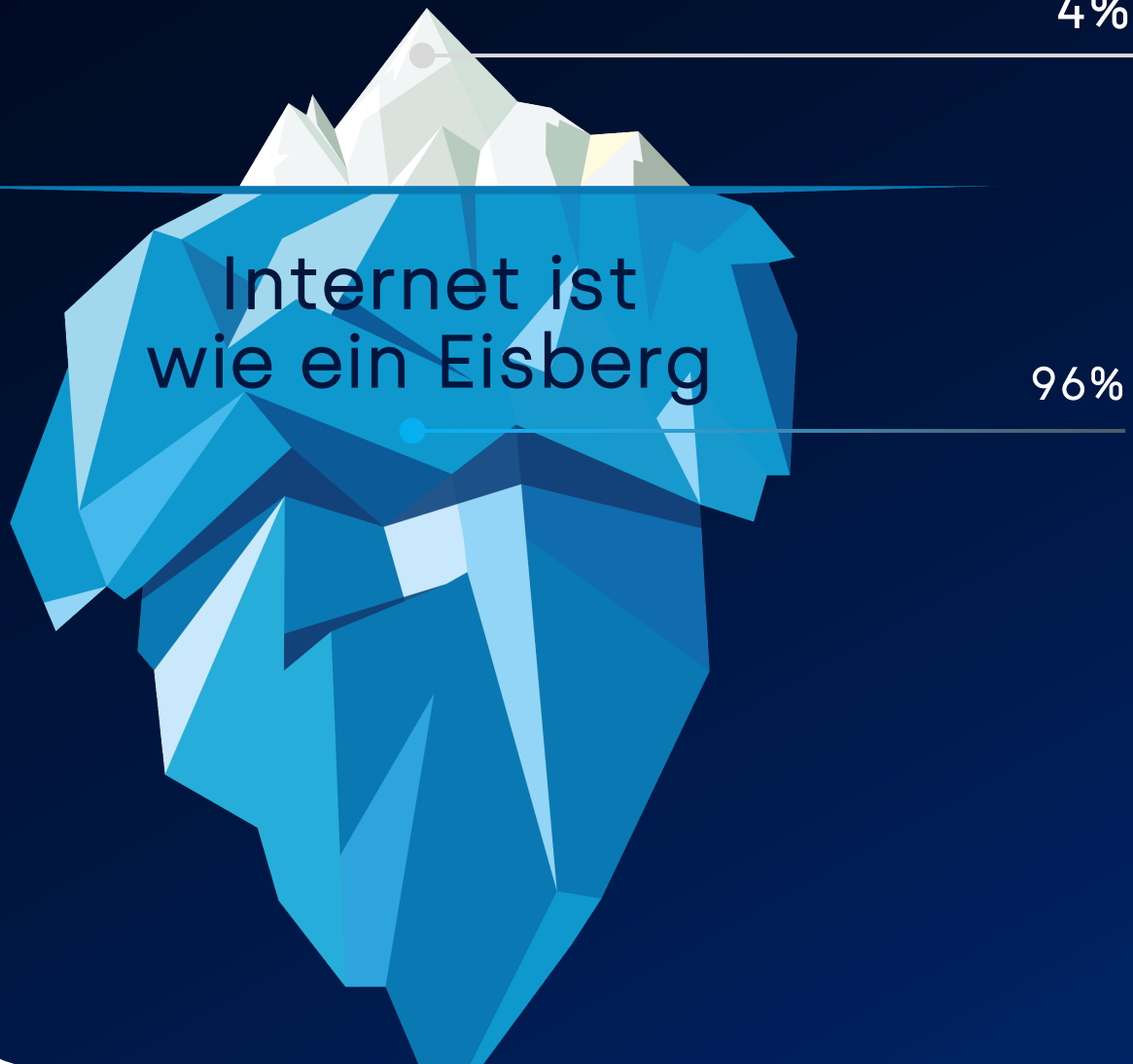
Secutec Webinar W06.2 - 26.06.2025 / Einblicke ins Darknet, Hacker Organisationen und Cyber Security Intelligence

Das Darknet



ClearWeb, DeepWeb, Darknet ...

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



Clear Web

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

Deep Web

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

Darknet

- Über "normale" Wege nicht auffindbare Webseiten
- Verschlüsselte Kommunikation
- Illegaler Inhalt, politischer Protest



- — Russisches Darknet
- — Persisches Darknet
- — Englischs Darknet
- — Chinesisches Darknet

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

tor Browser File Edit View History Bookmarks Tools Window Help

About Tor Hidden Wiki | Tor .onion url... OnionDir - Deep Web Link ... Disconnect Search: Search...

thehiddenwiki.org

<http://qc71lonwvpv77qibm.onion/> - Western Union Exploit
<http://3dbr5t4pygahedms.onion/> - ccPal Store
<http://y3fpieiezy2sin4a.onion/> - HQER - High Quality Euro Replicas
<http://qkj4drtgvpm7eecl.onion/> - Counterfeit USD
<http://nr6juudpp4as4gig.onion/pptobtc.html> - PayPal to BitCoins
<http://nr6juudpp4as4gig.onion/doublecoins.html> - Double Your BitCoins
<http://lw4ipk5choakk5ze.onion/raw/4588/> - High Quality Tutorials

Marketplace Commercial Services

<http://6w6vcynl6dumn67c.onion/> - Tor Market Board - Anonymous Marketplace Forums
<http://wvk32thojln4gpp4.onion/> - Project Evil
<http://5mvm7cg6bgklfjtp.onion/> - Discounted electronics goods
<http://lw4ipk5choakk5ze.onion/raw/evbLewgkDSVkfzv8zAo/> - Unfriendlysolution - Legit hitman service
<http://nr6juudpp4as4gig.onion/torgirls.html> - Tor Girls
<http://tuu66yxvrnn3of7l.onion/> - UK Guns and Ammo
<http://nr6juudpp4as4gig.onion/torguns.htm> - Used Tor Guns
<http://ucx7bkbi2dtia36r.onion/> - Amazon Business
<http://nr6juudpp4as4gig.onion/tor.html> - Tor Technology
<http://hbetshipq5yhhrsd.onion/> - Hidden BetCoin
<http://cstoreav7i44h2lr.onion/> - CStore Carded Store
<http://tfwdi3izigxlure.onion/> - Apples 4 Bitcoin
<http://e2qizoerj4d6ldif.onion/> - Carded Store
<http://jvrnuue4bvbftiby.onion/> - Data-Bay
<http://bgkitnugq5ef2cpi.onion/> - Hackintosh
<http://vlp4uw5ui22ljlg7.onion/> - EuroArms
<http://b4vqxw2j36wf2bqa.onion/> - Advantage Products
<http://ybp4oezfkhk24hxmb.onion/> - Hitman Network
<http://mts7hqqeogujc5e.onion/> - Marianic Technology Services
<http://mobil7rab6nuf7vx.onion/> - Mobile Store
<http://54flq67kqr5wvjgf.onion/> - MSR Shop
<http://yth5q7zdmqlycbcz.onion/> - Old Man Fixer's Fixing Services

May 2013

Blog Traffic

Pages
Pages | Hits | Unique
Last 24 hours: 11,870
Last 7 days: 129,179
Last 30 days: 818,538
Online now: 1

Kryptische Domain Namen



SORTED BY CATEGORIES

CANNABIS & HASH

BENZOS

DISSOCIATIVES

ECSTASY

STIMULANTS

OPIOIDS

PSYCHEDELICS

SOFTWARE & MALWARE

COUNTERFEIT ITEMS

POISON

GOLD & JEWELS

DIGITAL PRODUCTS

STERIODS

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



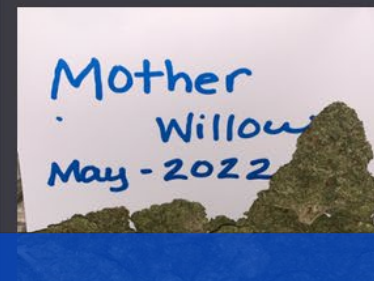
1000 GRAMS S-ISOMER NEEDLE-KETAMINE HIGHEST QUALITY DISSOCIATIVE

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



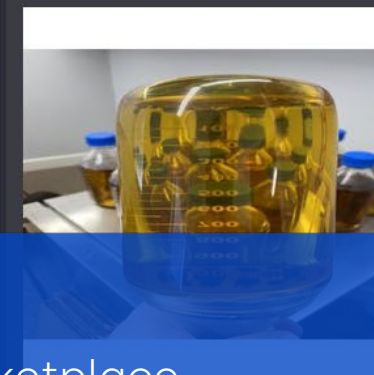
4 OZ OF WEDDIDNG CAKE!!! \$500 112 GRAMS

Motherwillow

4 oz

This is somesone 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

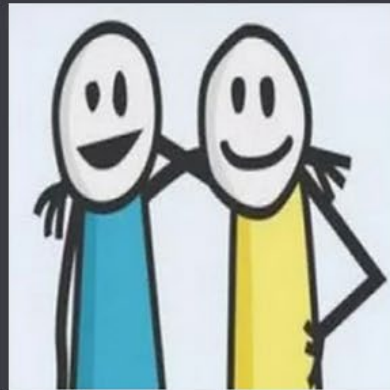
40 ml

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

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



crypto.com

FULLY VERIFIED USA, UK OR EU
CRYPTO.COM ACCOUNT

feggmann

Digital

You will be getting the fullz, and 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

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.

Hacker as a Service

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.

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 web servers, 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 additionally: Add this item if your target is a high profile VIP or large public company

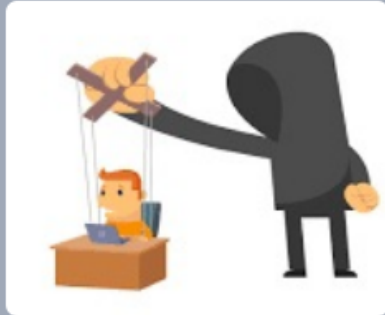
2500 USD =
0.12990 ₺

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 ₺	<input type="text" value="1"/> X Buy now
Spreading false information about someone on social media, not as life ruining but still nasty	450 USD = 0.02338 ₺	<input type="text" value="1"/> X Buy now
Social engineering to get secrets from a person, private or from some employee	450 USD = 0.02338 ₺	<input type="text" value="1"/> X Buy now

Social Engineering as a Service

Die Welt der Hackergruppen



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

100%

Schlecht gesicherte Unternehmen in 2 Minuten und 2 Jahre unerkant.

Sehr gut gesicherte Unternehmen in 2 Jahre und 2 Minuten unerkant.



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

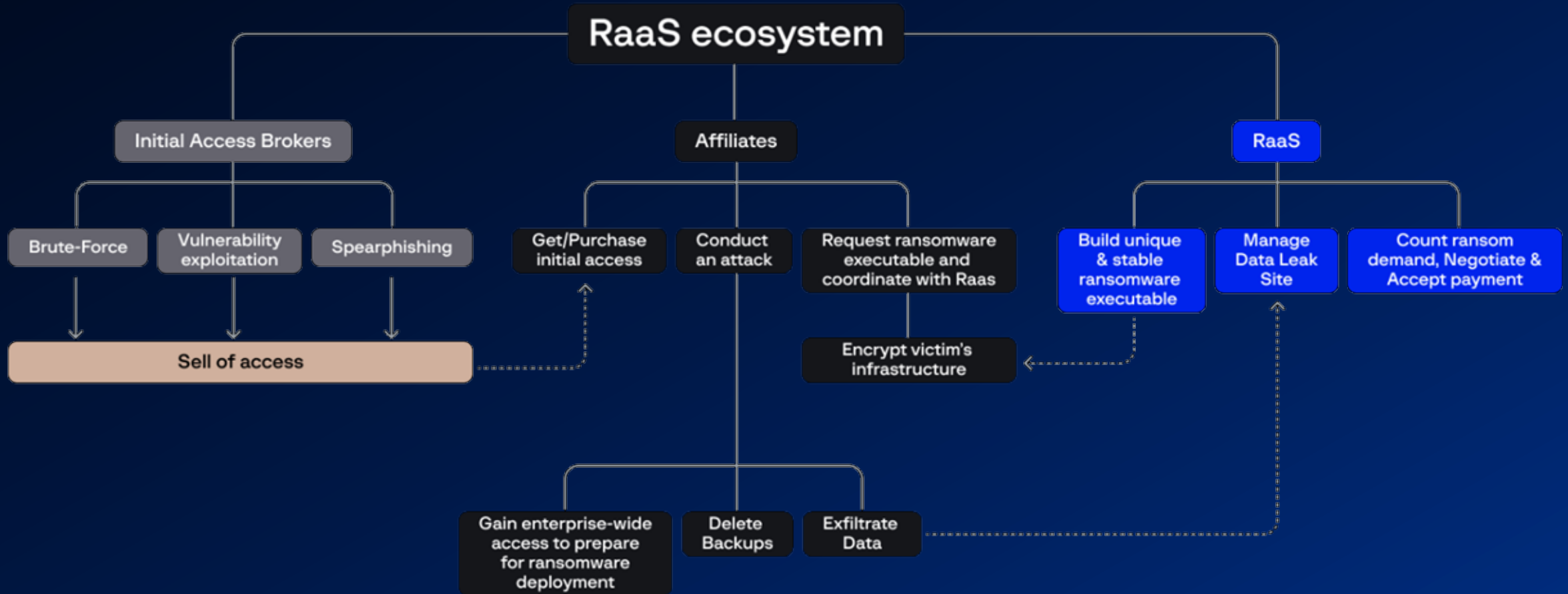
Anonymous

Hacktivismus - als Protestmittel, für politische und ideologische Ziele.

NoName057, Killnet

Pro russische Hackergruppen, die gezielt den Westen angreifen.

ZIELE: Politische und Ideologische Ziele erreichen, Privatpersonen



lafondasantafe.com

12D 09h 10m 39s

Each year, La Fonda proves itself of being among the top Santa Fe luxury hotels

Updated: 06 Sep, 2022, 01:51 UTC 38

gavresorts.com.br

14D 11h 11m 23s

GAV Resorts is a company specializing in high-end resorts.

Updated: 06 Sep, 2022, 01:52 UTC 35

pdh.com.tw

11D 22h 57m 35s

Rottley Tile has more than 35 years of experience and professional service team, all kinds of tile questions are happy to answer for you, your inquiries are our honor.

Updated: 05 Sep, 2022, 15:38 UTC 143

monnensenpartners.be

11D 22h 54m 39s

Your partner in accounting, taxation and advice Our accountants and advisors help you with personal and professional growth and work on the well-being and future goals of

Updated: 05 Sep, 2022, 15:39 UTC 168

sbr-zwiesel.de

9D 20h 45m 56s

The company SBR - Stahlbau Regenhütte GmbH - based in Zwiesel is a future-oriented and high-performing medium-sized family company, which manufactures complete

Updated: 05 Sep, 2022, 15:26 UTC 129

finnco.eu

9D 20h 06m 25s

Finnco-altec is a company that operates in the Packaging and Containers industry. It employs 21-50 people.

Updated: 05 Sep, 2022, 14:47 UTC 158

sportscity.com.tw

11D 02h 03m 45s

As a clothing manufacturer for over 30 years, SCI has witnessed the development of the garment industry in Taiwan. We are fully aware that talent is the key to a company's

Updated: 05 Sep, 2022, 14:44 UTC 143

kamut.com

7D 15h 33m 28s

We have three main activities at KEE. We have the production of the KAMUT(R) tradename in the European Union. We also coordinate a research program

Updated: 05 Sep, 2022, 12:14 UTC 173

divultec.pt

11D 19h 20m 55s

Divultec's offering is focused on Systems integration offering solutions for backup

www3.comune.gorizia.it

9D 07h 01m 08s

Gorizia is an Italian town and the capital of the Province of Gorizia in its inhabitants are

eneva.com.br

13D 19h 37m 32s

1223 GB. finance, plans for the future, legal information accounting marketing insurance

floresfunza.com

13D 22h 45m 54s

floresfunza.com FLORES FUNZA is one of the leading companies in the flower industry in

Wall of Shame – Lockbit 3.0



Supply Chain
Attacken

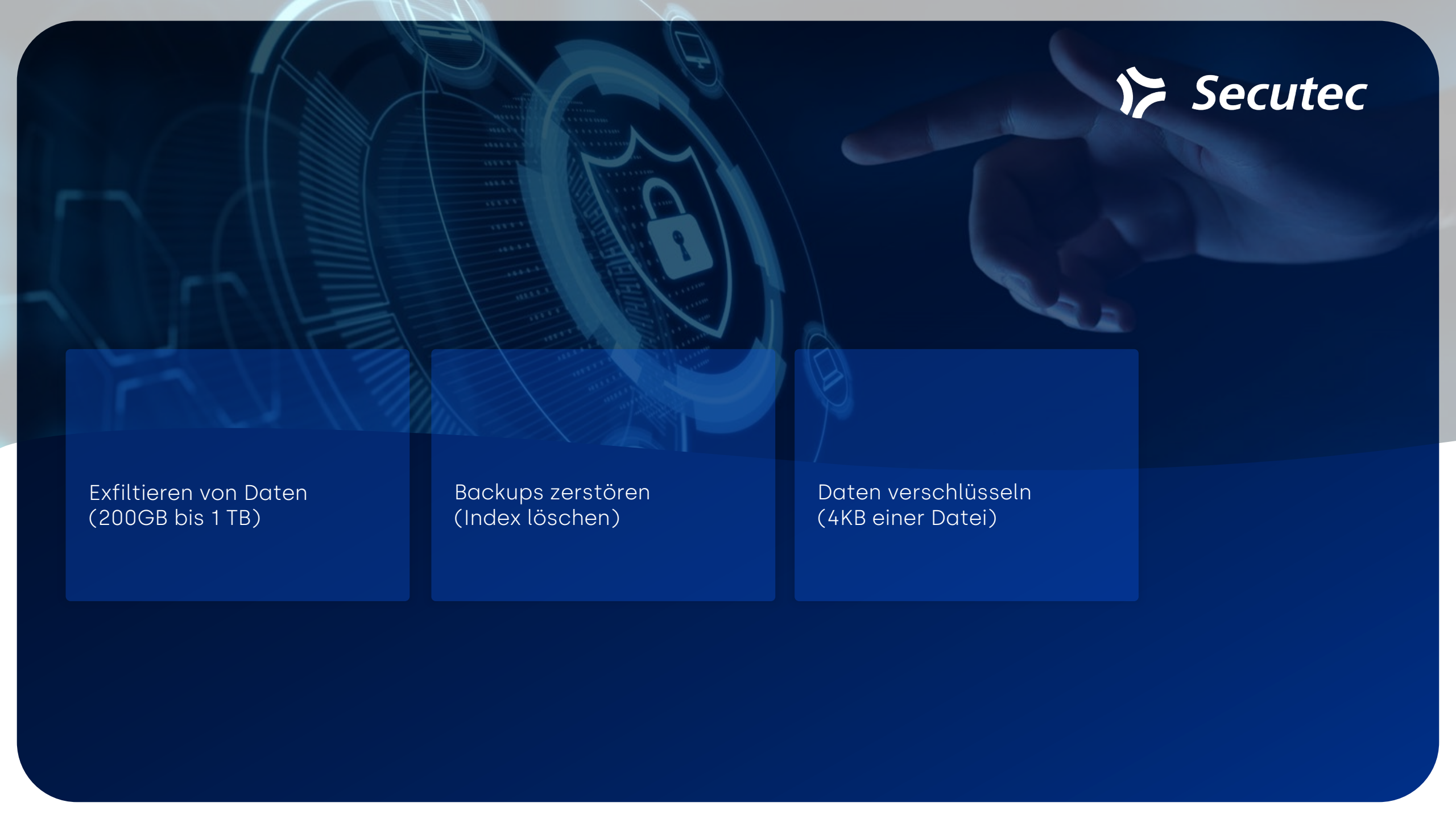
Deep Fake
Audio und Video

KI unterstützte
Attacken

Wiper Malware
Kriege

Cyber
Versicherung

Die Ransomware Attacke



Exfiltrieren von Daten
(200GB bis 1 TB)

Backups zerstören
(Index löschen)

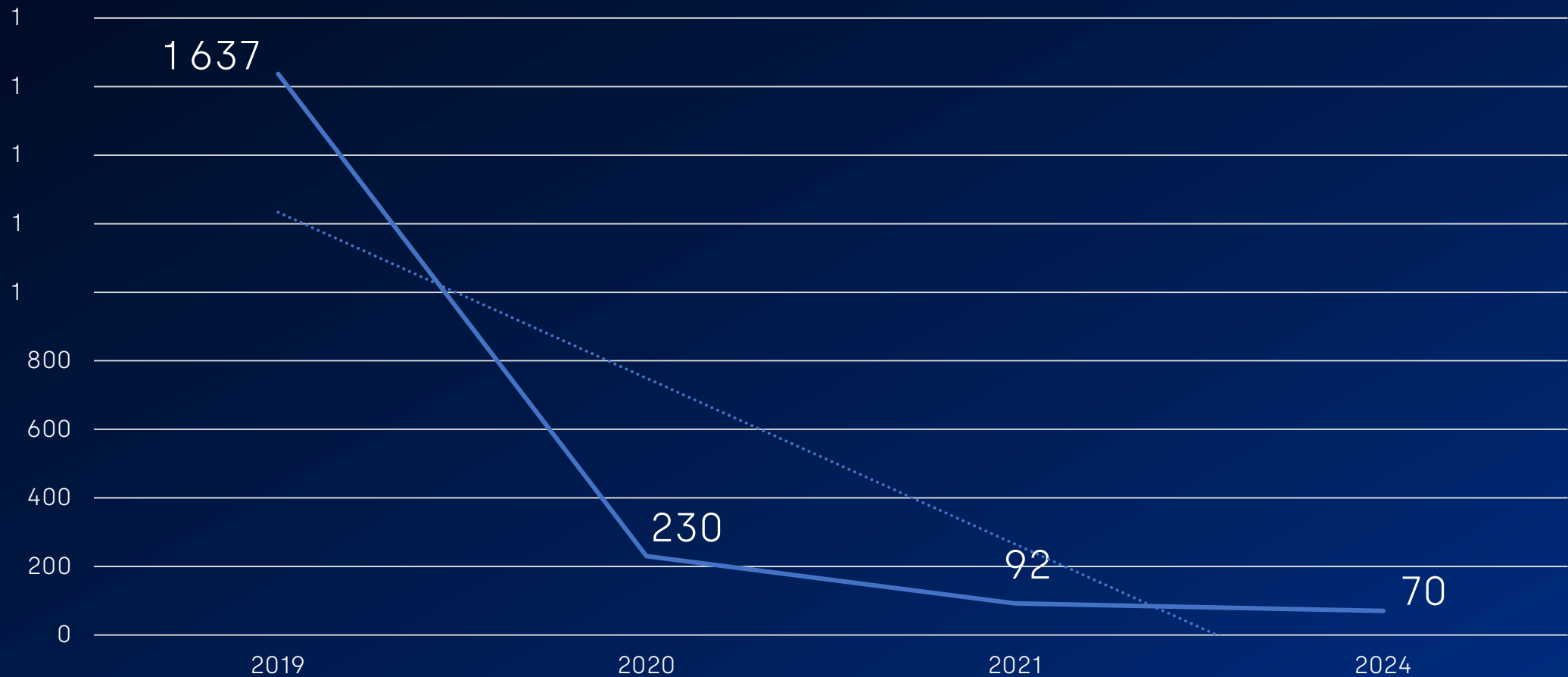
Daten verschlüsseln
(4KB einer Datei)



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

The diagram features a central hub with the text 'Angriffsvektoren'. Eight lines radiate from this hub to eight different attack vectors arranged in a circle. Each vector is accompanied by a specific solution. The background consists of concentric circles and a gear-like pattern, all in shades of blue.

Phishing
(Fokus New Domains)

Lösung: SecureDNS

Supply Chain Attacken
(Lieferketten und Kunden)

Lösung: ASM und Darknet Monitoring

Brute-Force Attacken
(Wellen bei größeren Leaks)

Lösung: Darknet Monitoring

Man in the Middle
(Fokus Rechnungsbelege)

Lösung: SecureDNS, Threat Hunting, M365 Kit

Passwort Stealer/Keylogger
(Private- und Firmengeräte)

Lösung: Darknet Monitoring

Deep Fake
(Audio und Video)

Exploit Vulnerability
(Platzierung von Backdoors)

Lösung: Attack Surface Management

O365 Phishing
(Proxy/Cache - Logindaten/MFA)

Lösung: M365 Security Kit

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

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 werden 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 GDPR 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://an2ce4pppf2ipvba2djurxi5pnxxhu3uo7ackul6eafcundqtl7bhid.onion/>
- Log in using the Client ID:

Empfehlungen



DNS Monitoring

Auch IoT Devices beachten!

Externe Scans Schwachstellen

Aus Sicht eines Cyberkriminellen

Darknet Monitoring

User, Keylogger, VIPs, Keywords

Incident Vorbereitung

Geschäftsleitung nicht vergessen!

Playbook Notfallhandbuch

Hacker Attacke
Blackout, usw.

Multifaktor Authentifizierung

Nicht nur mit Bestätigung!

EDR/XDR Virens Scanner

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)

Empfehlungen für den privaten Bereich



Passwort Manager

Sichere Passwörter
und Verwaltung

- NordPass,
- BitWarden,
- 1Password

Multifaktor Authentifizierung

Nicht nur mit
einfacher
Bestätigung

VPN Dienstleister nutzen

Anonymität
im Internet
(z.b. NordVPN)

Online Schutz für Kinder

Berechtigungen
und Schutz
(z.b. Salfeld.de)

Daten Sicherung

Regelmäßige
Sicherung der
wichtigsten Daten

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

- XDR Integration Sentinel One
- Integrierte Phishing Rootkits Detection

NEU



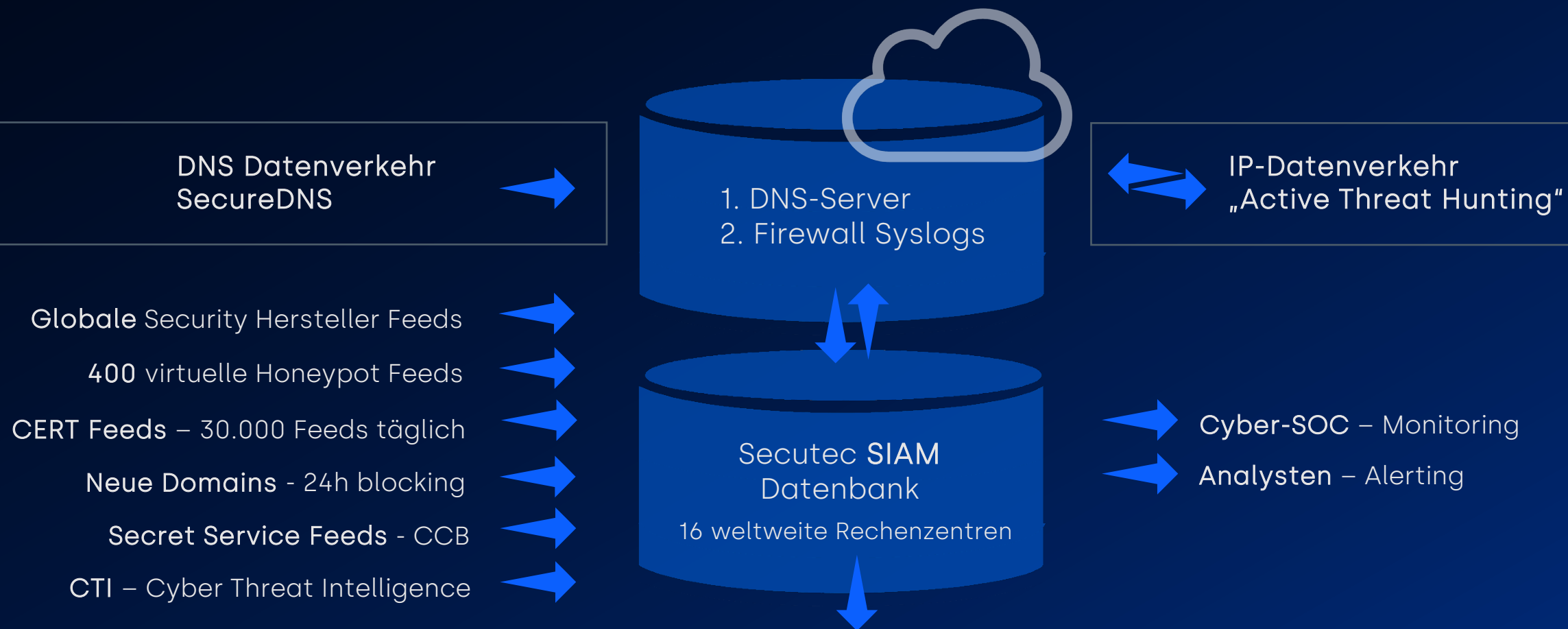
*Mag. Daniel Rossgatterer, MBA
CEO Secutec GmbH*

Let's connect!

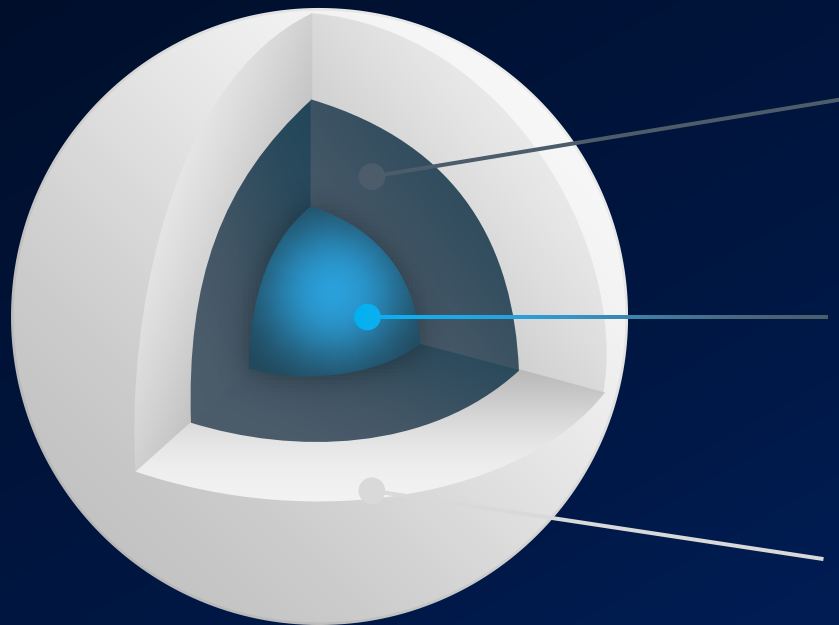
Cyber Security Intelligence

Secutec SecureDNS

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



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

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

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

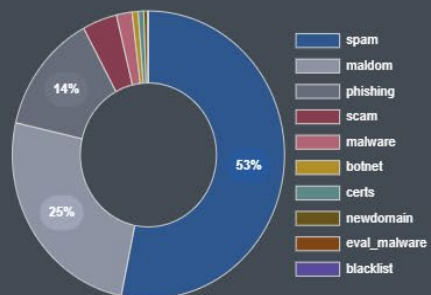
3 668



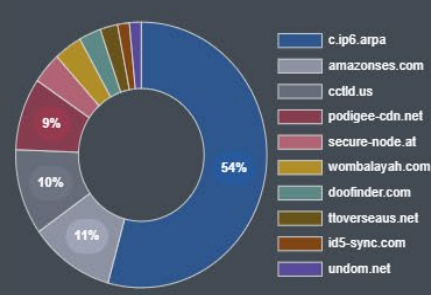
Blocked apt requests

0

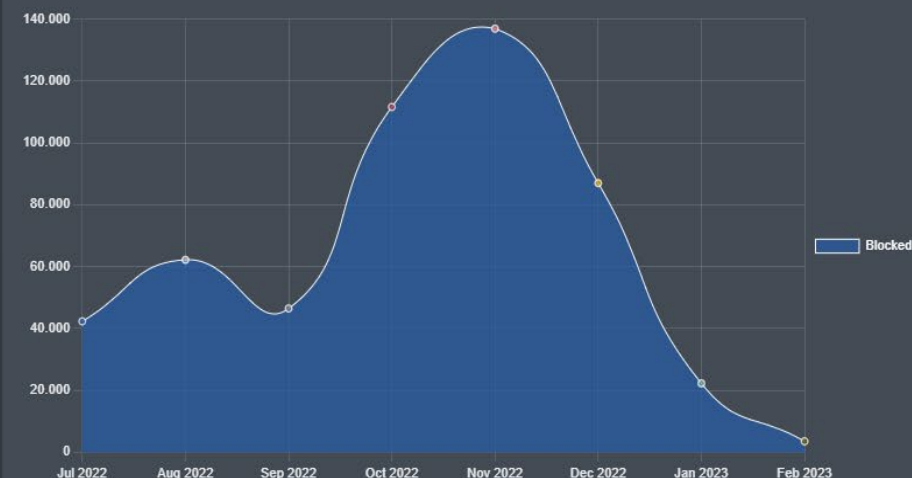
Top 10 categories



Top 10 domains



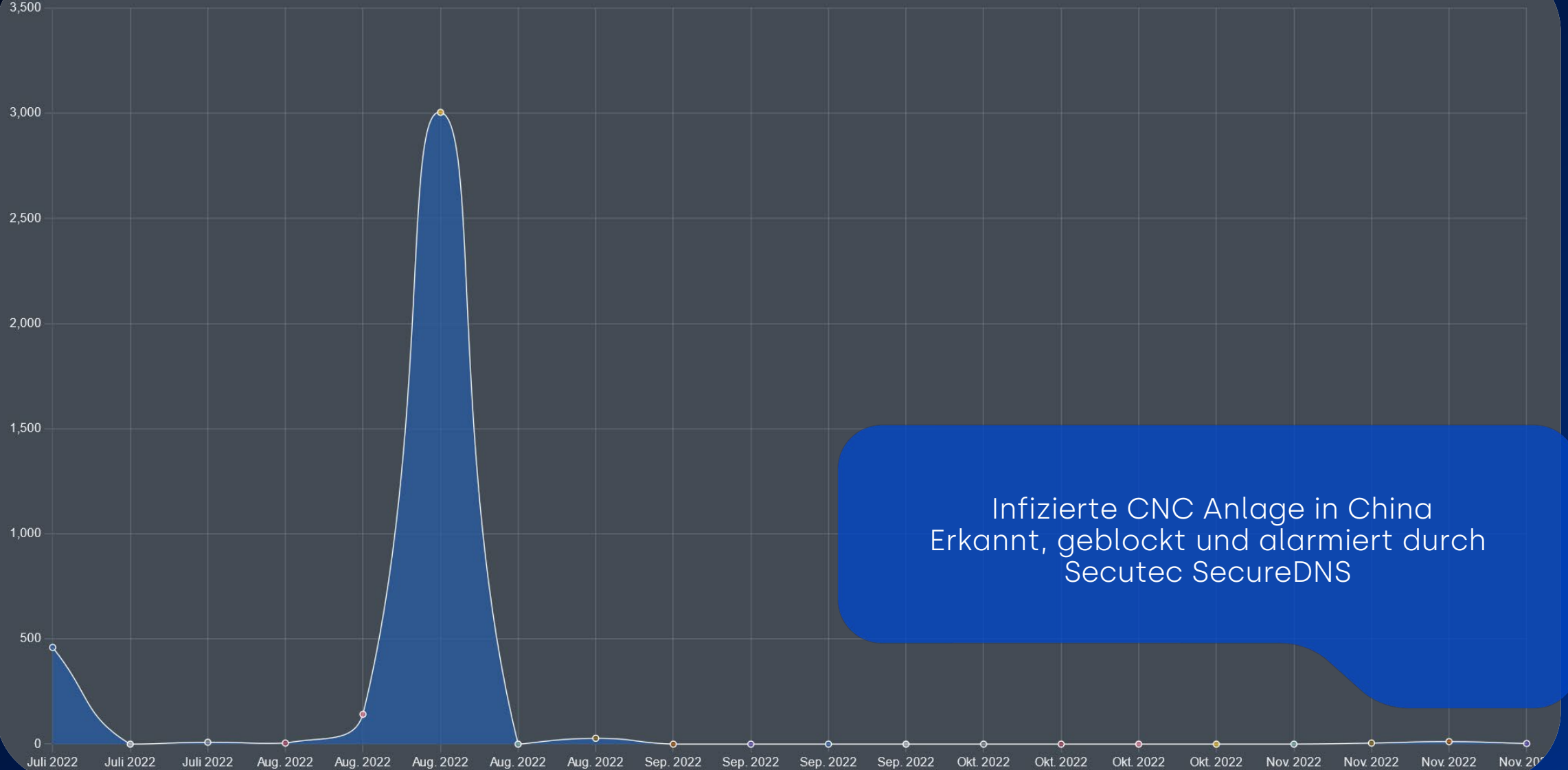
Queries



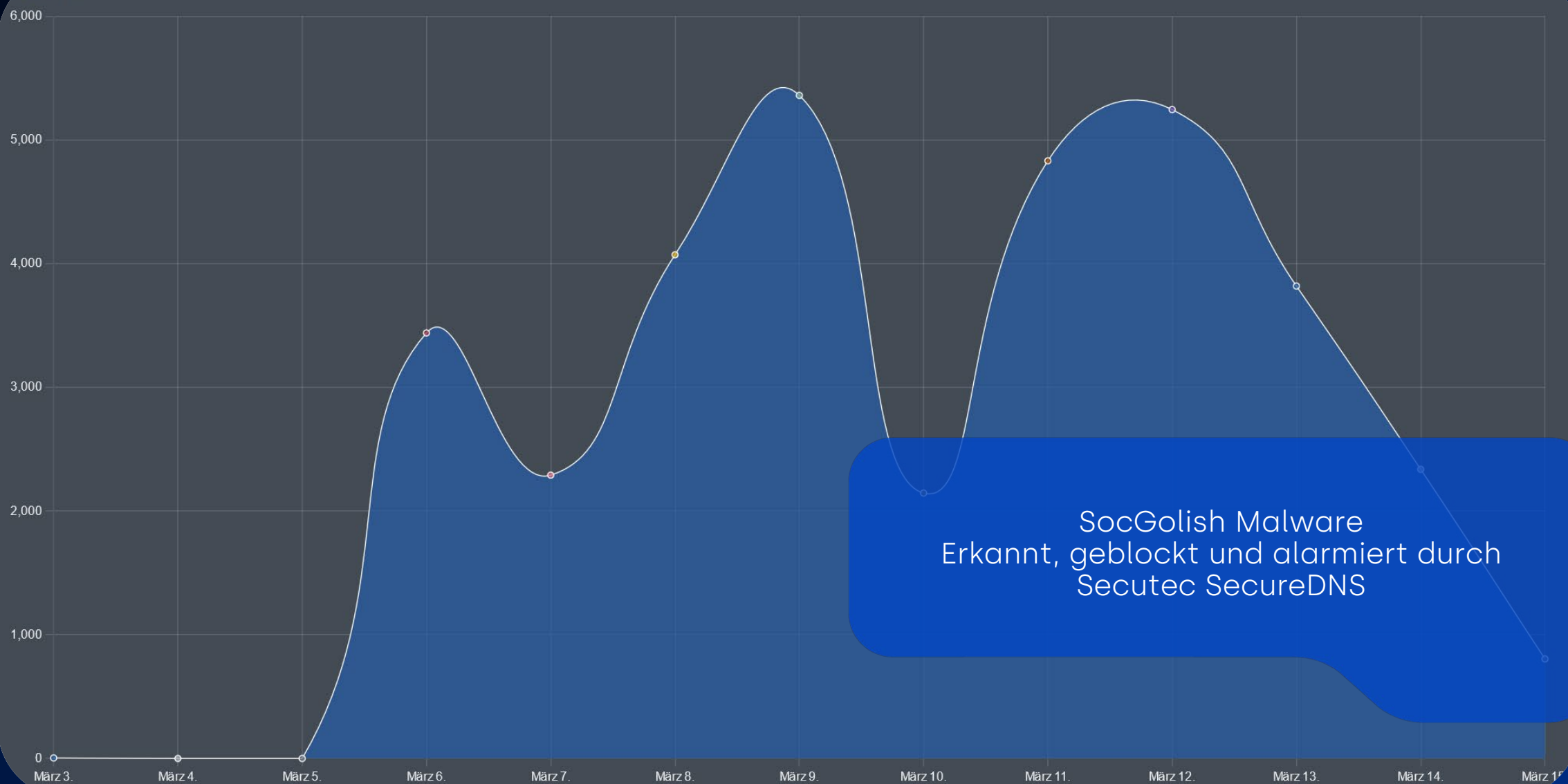
Queries

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

Queries



queries



SocGolish Malware
Erkannt, geblockt und alarmiert durch
Secutec SecureDNS

Secutec SecureSIGHT

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

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

secutecat Nur Organisation

Security Rating Title

F - Critical Risks

26

E - High Risks

29

D - Low Risks

249

C - Recommendations

366

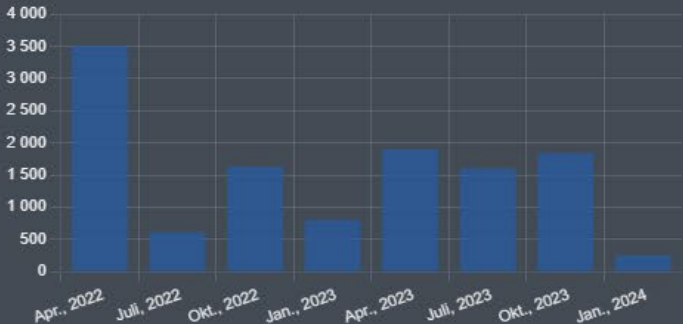
B - Improvements

4 964

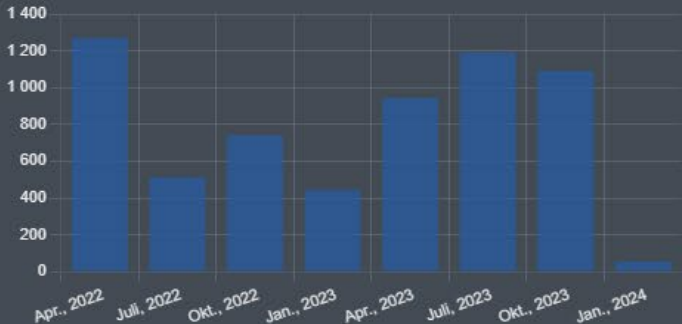
A - Informational

122

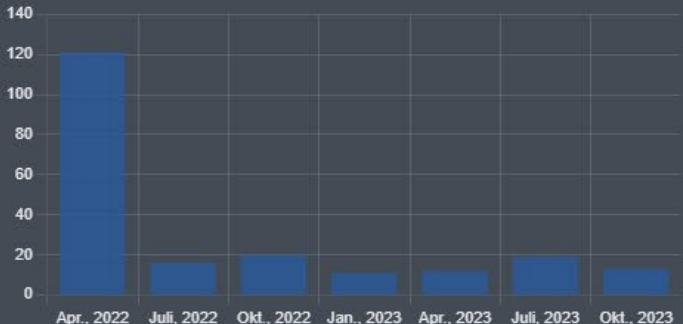
Risks Discovered



Risks Solved



Risks Mitigated



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

Security Rating ↑↓	Asset Title ↑↓	Discovered ↑↓	Title ↑↓	Description ↑↓	Proposed Action ↑↓	ID ↑↓
f		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		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

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

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

Total Leaked Credentials

169

Malware - Employee Credentials

5

Malware - Consumer Credentials

150

External Database Leaks

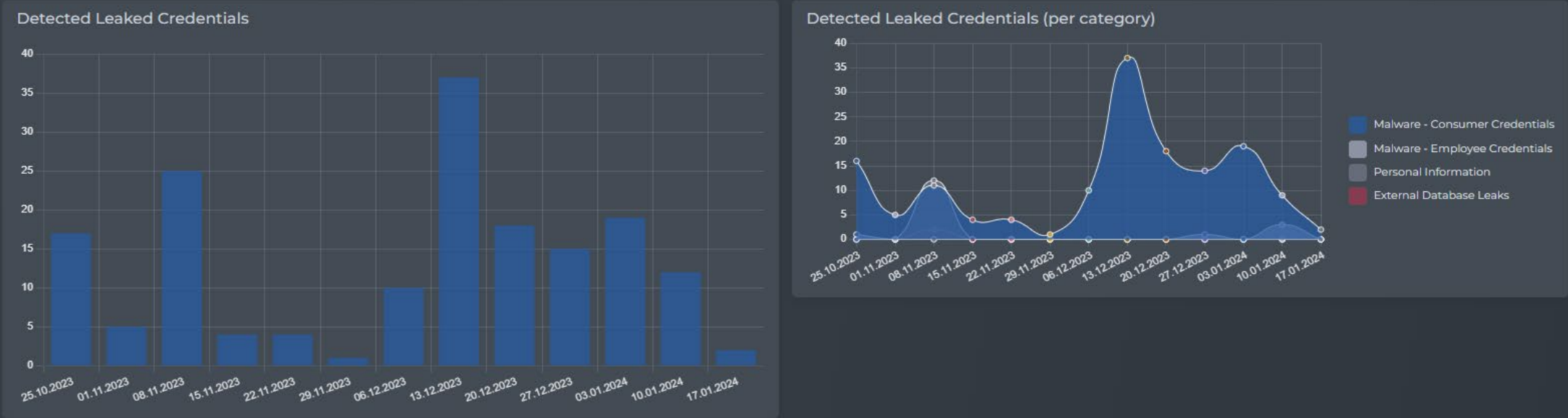
2

Personal Information

12

Email Only

0



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

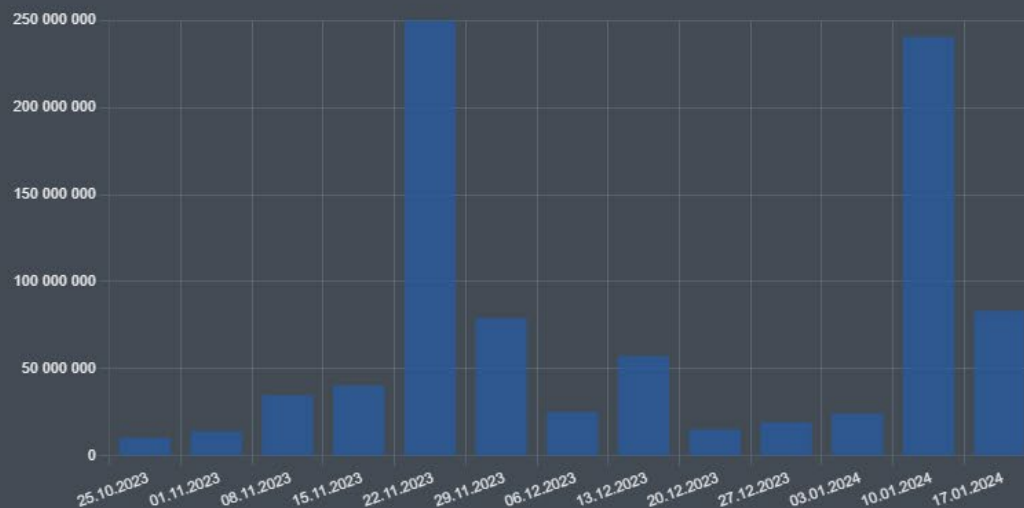
Publish Date ↑↓	Breach Date ↑↓	Breach Title ↑↓	Email Address ↑↓	Username ↑↓	Password Type ↑↓	Target URL ↑↓	Infected Time ↑↓	Hostname ↑↓	OS ↑↓	IP ↑↓
14.01.2024 01:00:00	14.01.2024 01:00:00	LummaC2 Stealer			plaintext	https://vpn-a.com/		DESKTOP-RALLRCO	Windows 10 (10.0.19045) x64	86.56

secutecat Nur Organisation

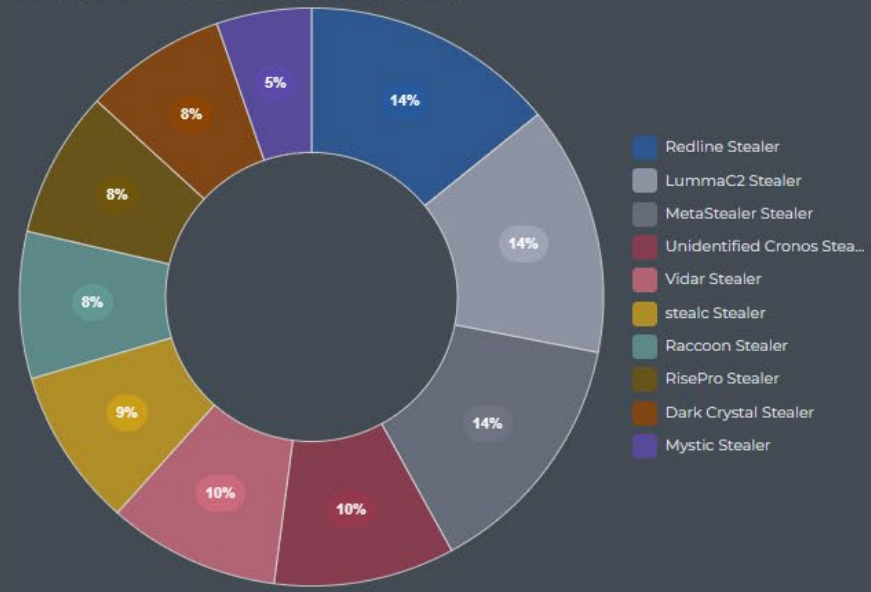
24.10.2023 08:12 - 22.01.2024 08:12

Breach Title Target Site

Global Detected Leaked Credentials



Global Detected Leaked Credentials (per malware)

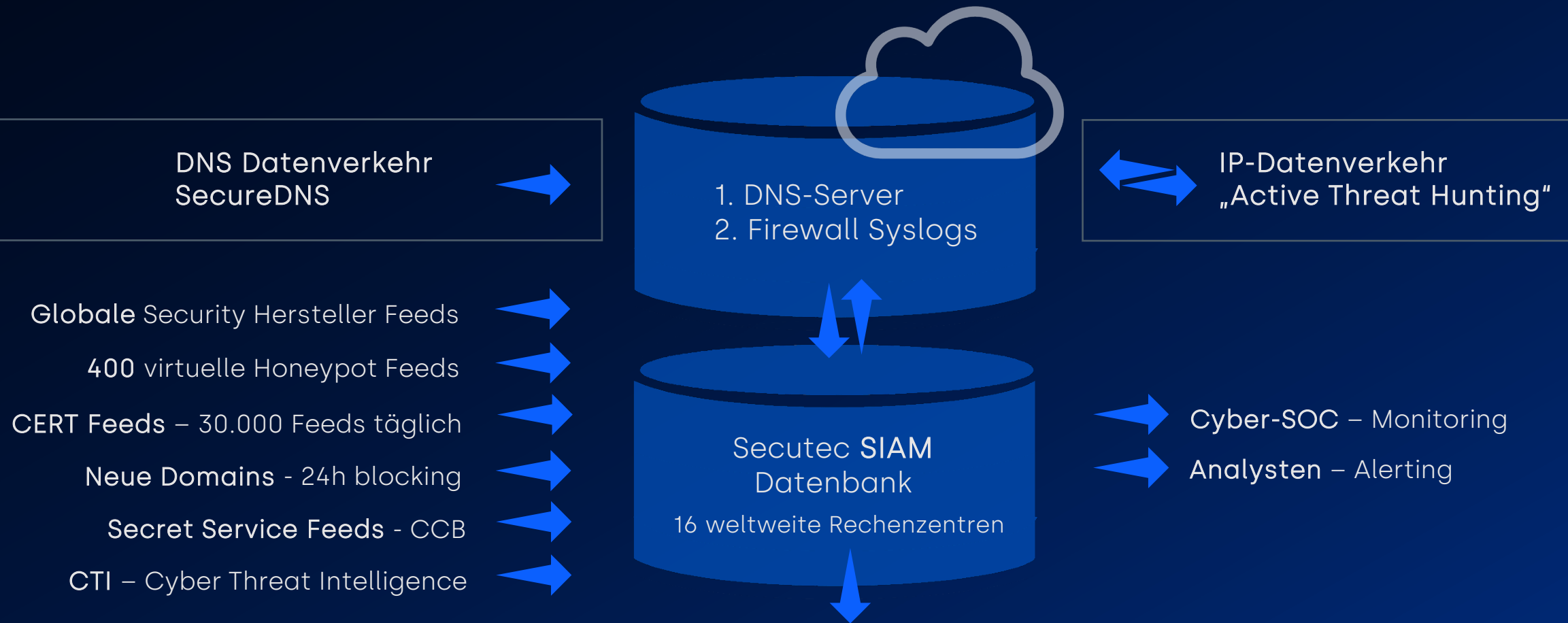


Global Detected Leaked Credentials

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.

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



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		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

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



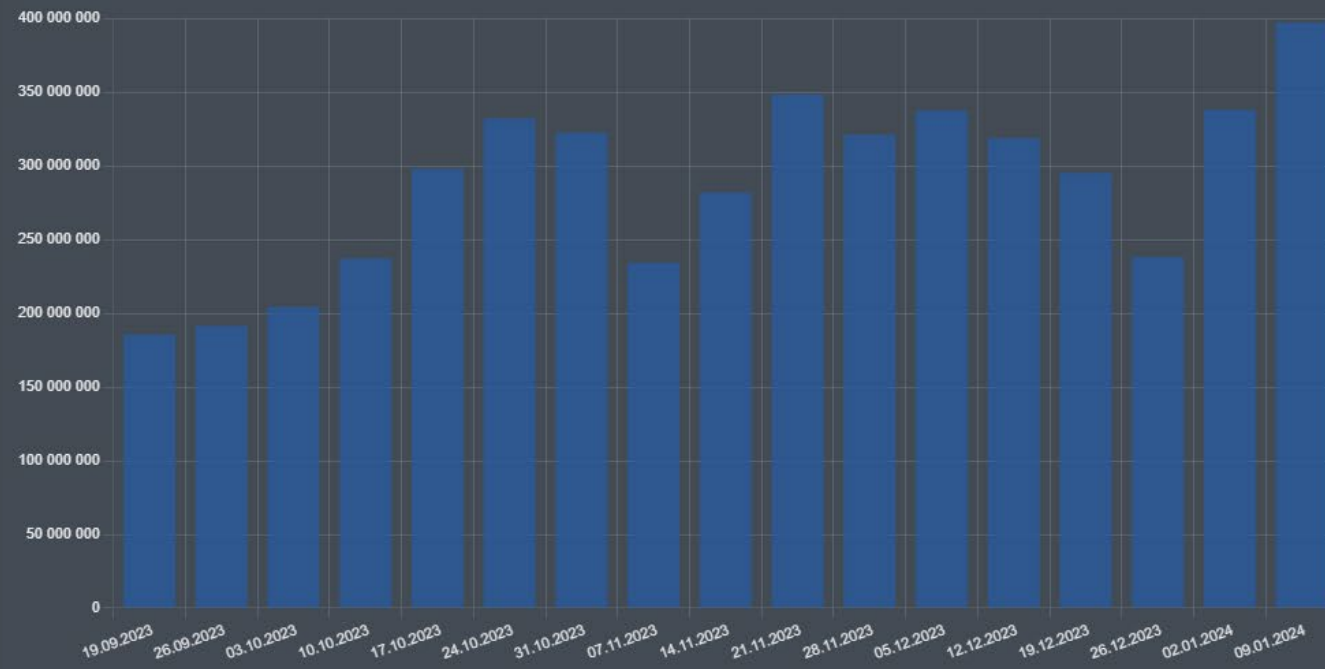
Firewall Name

Package Name

Amount of Logs

3 710 499 434

Timeline of the Amount of Logs (Static)



Logs per Firewall

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

Secutec SecureRESPONSE

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



Secutech

Cybersecurity Intelligence

Prevent now, secure tomorrow