
Secutec
Cyber security intelligence

Secutec
Cyber security intelligence

Geert Baudewijns
CEO & Founder

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

Wir arbeiten für Behörden und Organisationen weltweit und haben Erfahrung aus über 500 Attacken und 300 Verhandlungen mit professionellen Hacker Organisationen.

- ✓ Führender europäischer Cybercrime Negotiater
- ✓ Organisationen wie Europol, Secret Services, diverse CERTs
- ✓ Cyber-SOC / Forensiker, Analysten, Fraud Spezialisten

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

Cyber Security = Multi-Vendor-Strategie

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 Professional Darknet Monitoring

24/7 Attack Surface Management

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 Komminkation

-Betreiber und Besucher möchten anonym bleiben

-Illegaler Inhalt, politischer Protest, geheime Kommunikation

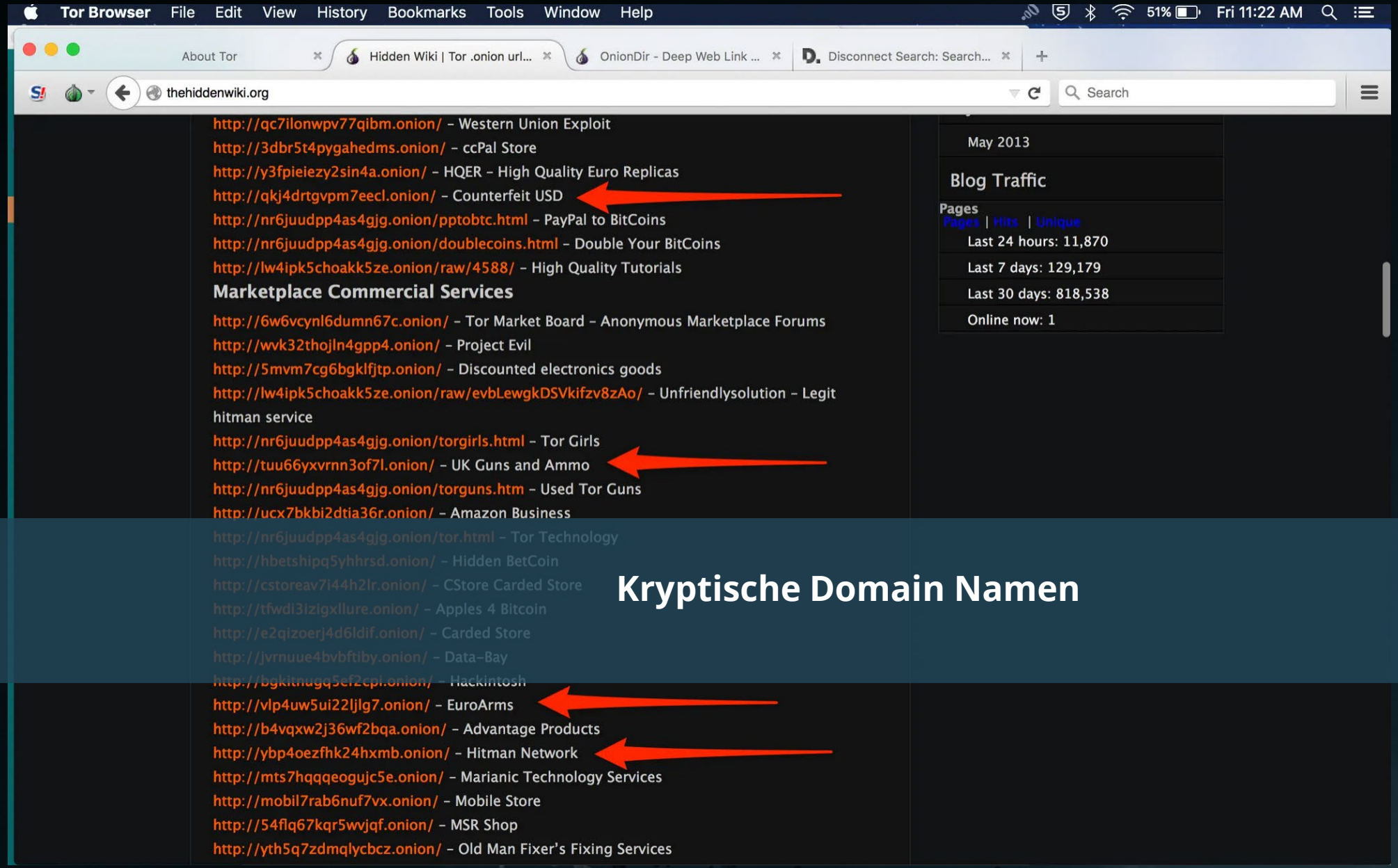
Russisches Darknet

Persisches Darknet

Englisches Darknet

Chinesisches Darknet

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



Kryptische Domain Namen

Tor Browser File Edit View History Bookmarks Tools Window Help 58% Fri 10:57 AM

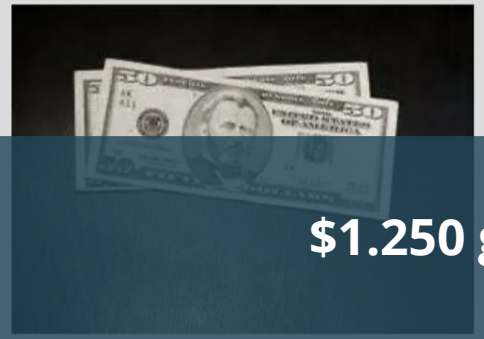
About Tor | Hidden Wiki | Tor .onion url... | Problem loading page | Counterfeit USD - High qua... | Disconnect Search: Search...

Search

Counterfeit USD

Login Register FAQs Products

50 USD BILLS



Our notes are produced of cotton based paper. They pass the pen test without problems. UVI is incorporated, so they pass the UV test as well. They have all necessery security features to be spent at most retailers. Free shipping in the US.

$1.250 gefälschte USD für $600 – 50% Rabatt

Product	Price	Quantity
25 x 50 USD BILLS	600 USD = 1.652 ฿	1 X Buy now
100 x 50 USD BILLS	2000 USD = 5.506 ฿	1 X Buy now

Counterfeit USD

Tor Browser File Edit View History Bookmarks Tools Window Help 45% Fri 11:35 AM

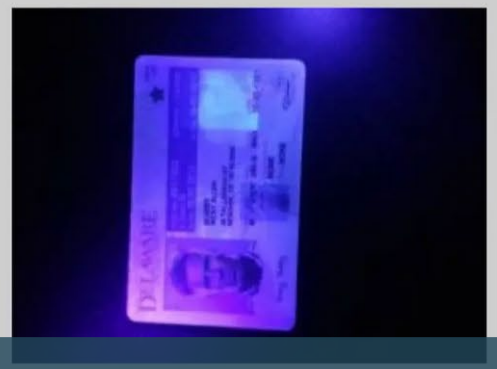
The-Hidden-Wiki.com - Hidden... | Disconnect Search: Search... | US Fake ID Store - Drivers ...

Search

USfakeIDs

Products FAQs Register Login

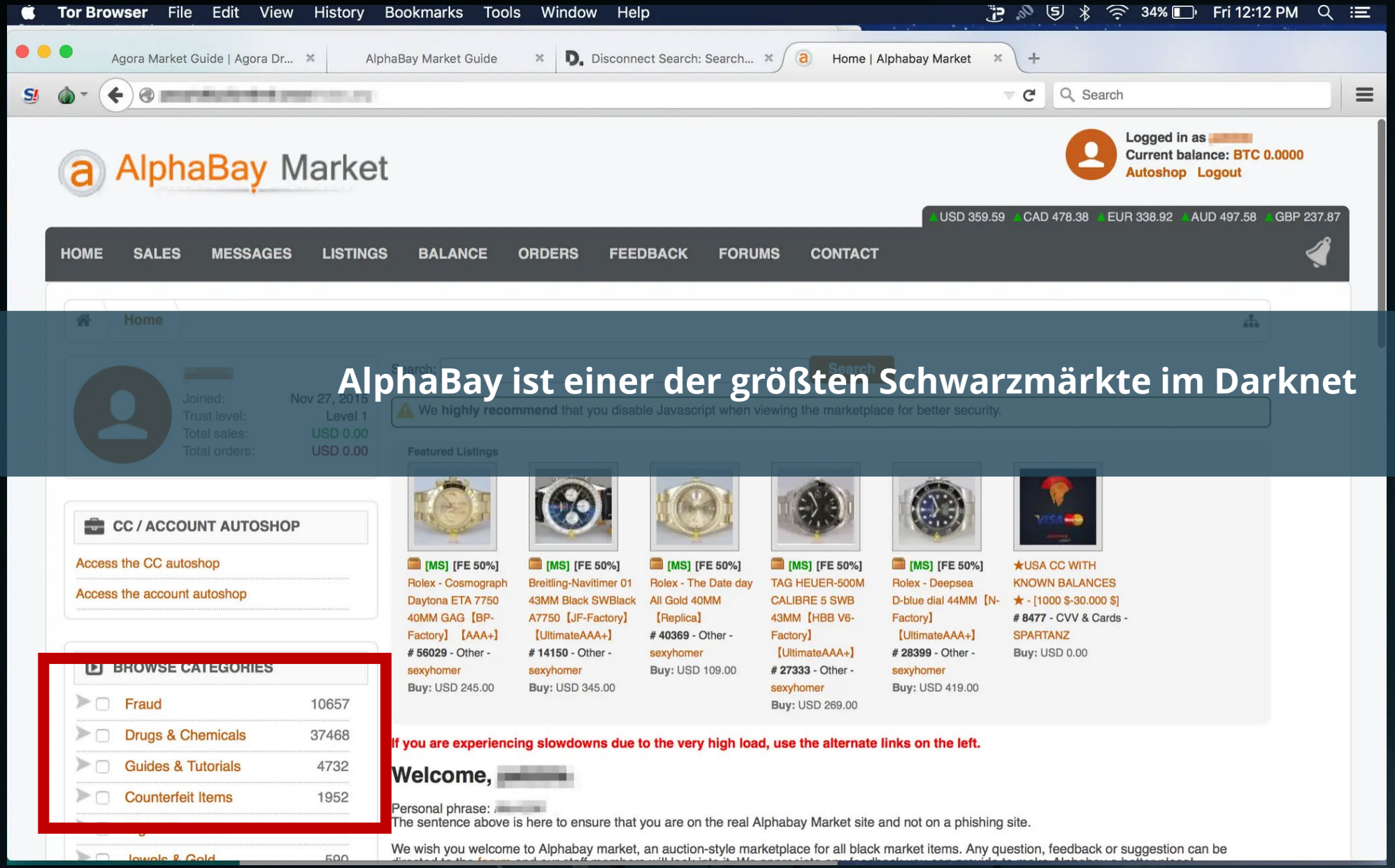
US Fake Drivers Licenses - Scannable, Holograms, UV etc



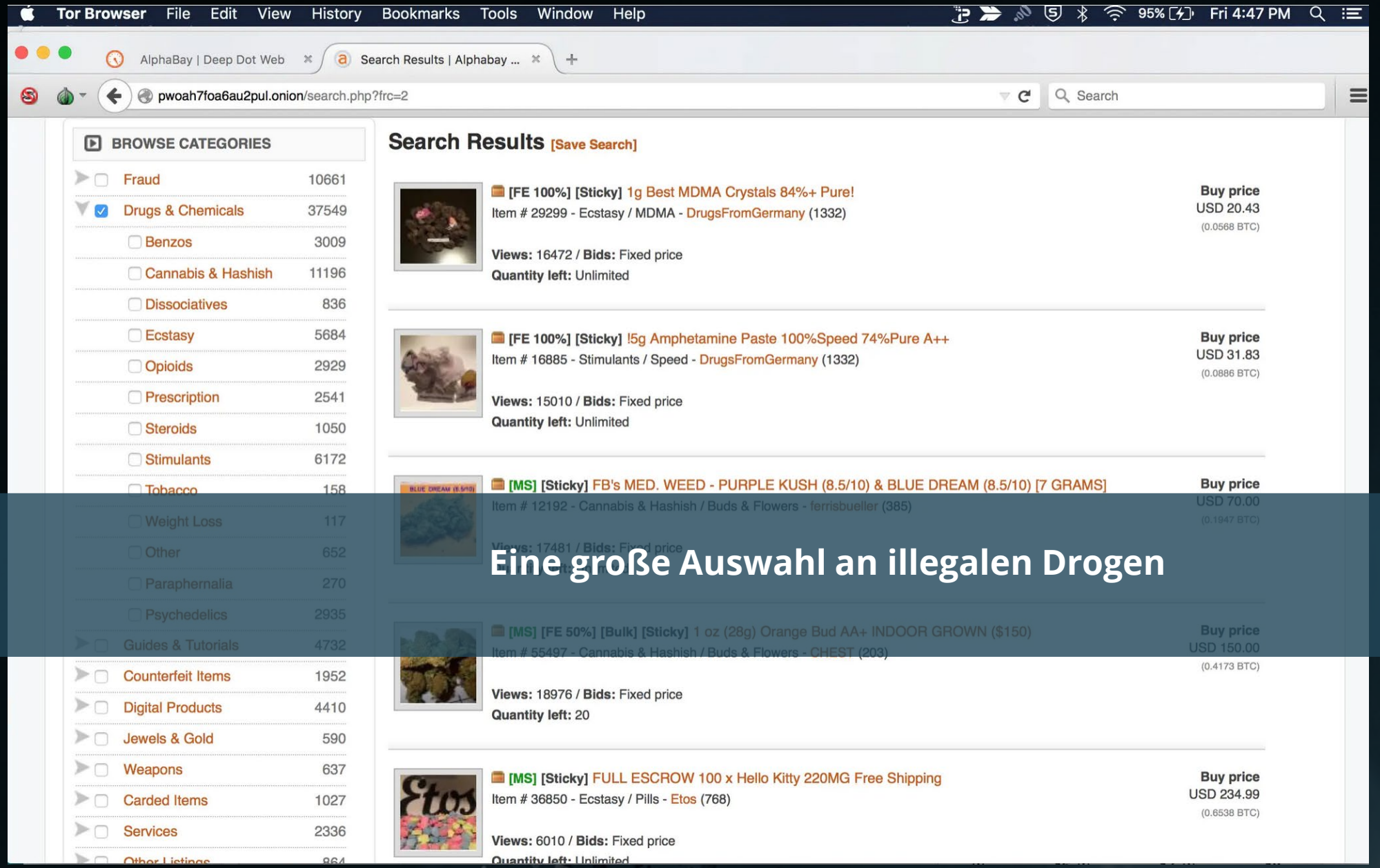
Our fake drivers licenses are all scannable, contain original hologram and UV, microprint, laser engraving etc.
Shipping from the US within 48 hours!
We only sell the best quality, you wont find any better on the net.

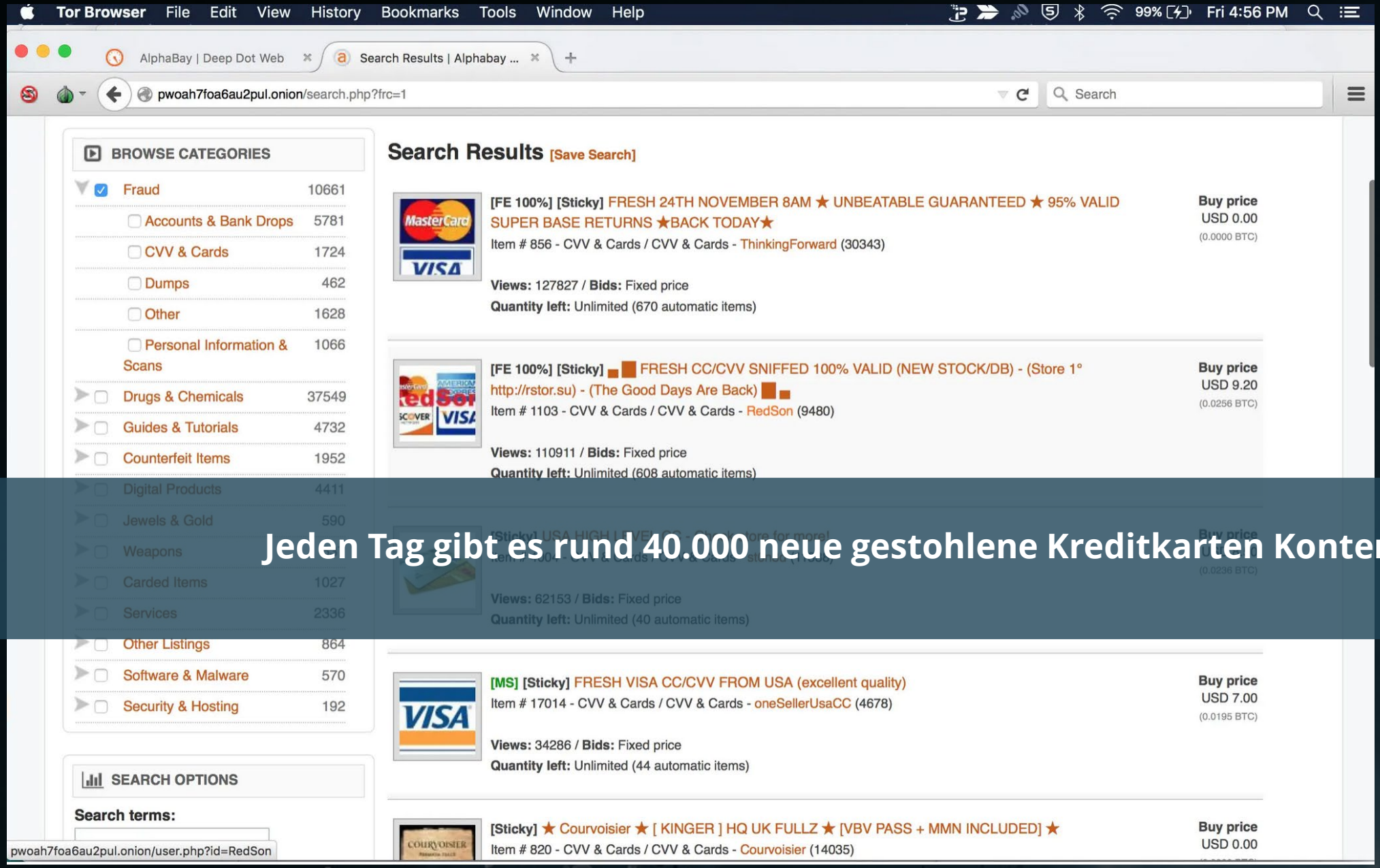
Gefälschter Führerschein für $200 USD

Product	Price	
Delaware	200 USD = 0.551 ฿	1 X Buy now
Illinois	200 USD = 0.551 ฿	1 X Buy now
South Carolina	200 USD = 0.551 ฿	1 X Buy now
New Jersey	200 USD = 0.551 ฿	1 X Buy now
Colorado	200 USD = 0.551 ฿	1 X Buy now



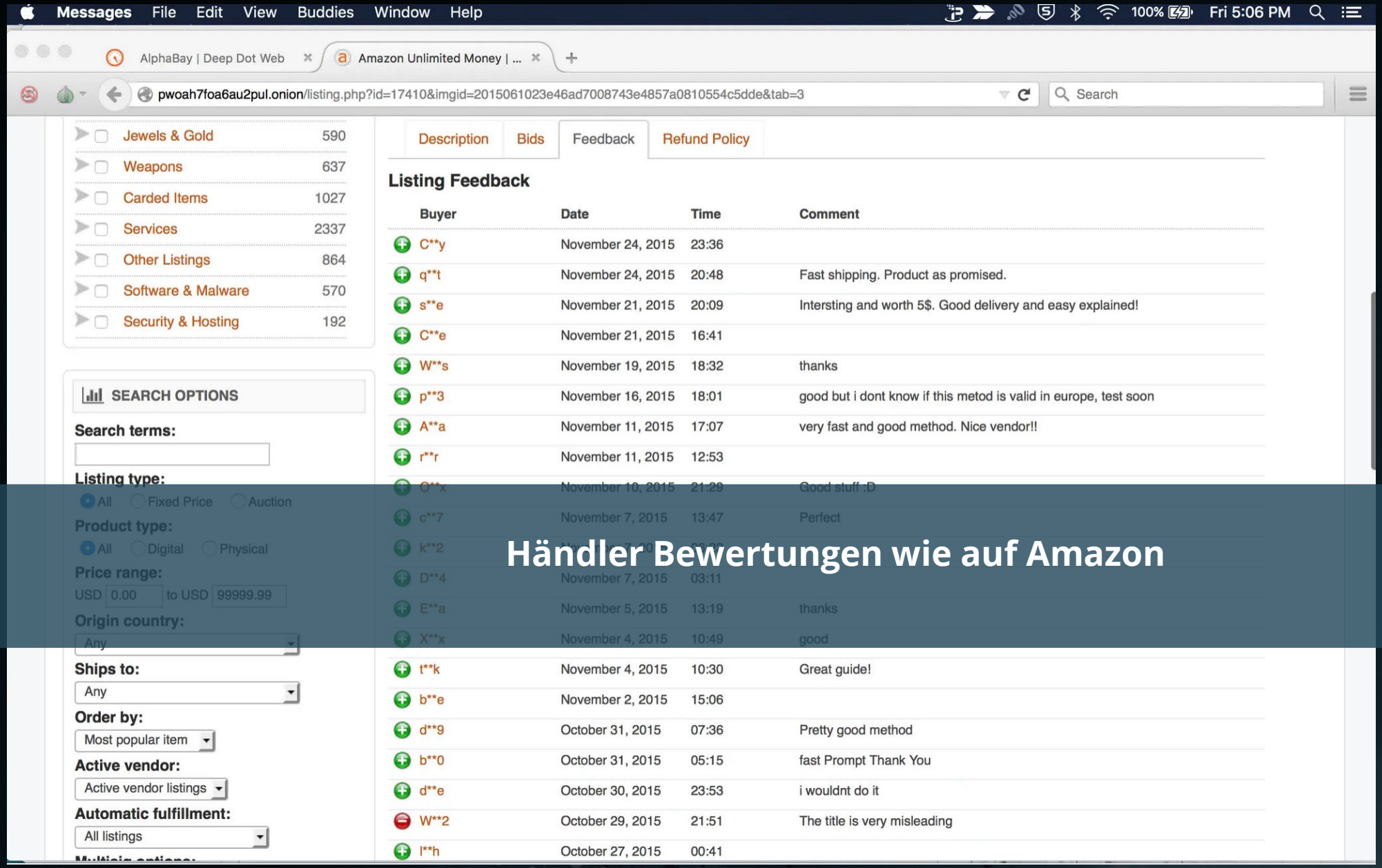
AlphaBay ist einer der größten Schwarzmärkte im Darknet


Tor Browser File Edit View History Bookmarks Tools Window Help
95% Fri 4:47 PM
AlphaBay | Deep Dot Web
Search Results | Alphabay ...
pwoah7foa6au2pul.onion/search.php?frc=2
Search
BROWSE CATEGORIES
Fraud 10661
Drugs & Chemicals 37549
Benzos 3009
Cannabis & Hashish 11196
Dissociatives 836
Ecstasy 5684
Opioids 2929
Prescription 2541
Steroids 1050
Stimulants 6172
Tobacco 158
Weight Loss 117
Other 652
Paraphernalia 270
Psychedelics 2935
Guides & Tutorials 4732
Counterfeit Items 1952
Digital Products 4410
Jewels & Gold 590
Weapons 637
Carded Items 1027
Services 2336
Search Results [Save Search]
[FE 100%] [Sticky] 1g Best MDMA Crystals 84%+ Pure!
Item # 29299 - Ecstasy / MDMA - DrugsFromGermany (1332)
Views: 16472 / Bids: Fixed price
Quantity left: Unlimited
Buy price
USD 20.43
(0.0568 BTC)
[FE 100%] [Sticky] !5g Amphetamine Paste 100%Speed 74%Pure A++
Item # 16885 - Stimulants / Speed - DrugsFromGermany (1332)
Views: 15010 / Bids: Fixed price
Quantity left: Unlimited
Buy price
USD 31.83
(0.0886 BTC)
[MS] [Sticky] FB's MED. WEED - PURPLE KUSH (8.5/10) & BLUE DREAM (8.5/10) [7 GRAMS]
Item # 12192 - Cannabis & Hashish / Buds & Flowers - ferrisbueller (385)
Buy price
USD 70.00
(0.1947 BTC)
[MS] [FE 50%] [Bulk] [Sticky] 1 oz (28g) Orange Bud AA+ INDOOR GROWN ($150)
Item # 55497 - Cannabis & Hashish / Buds & Flowers - CHEST (203)
Views: 18976 / Bids: Fixed price
Quantity left: 20
Buy price
USD 150.00
(0.4173 BTC)
[MS] [Sticky] FULL ESCROW 100 x Hello Kitty 220MG Free Shipping
Item # 36850 - Ecstasy / Pills - Etos (768)
Views: 6010 / Bids: Fixed price
Buy price
USD 234.99
(0.6538 BTC)
Eine große Auswahl an illegalen Drogen

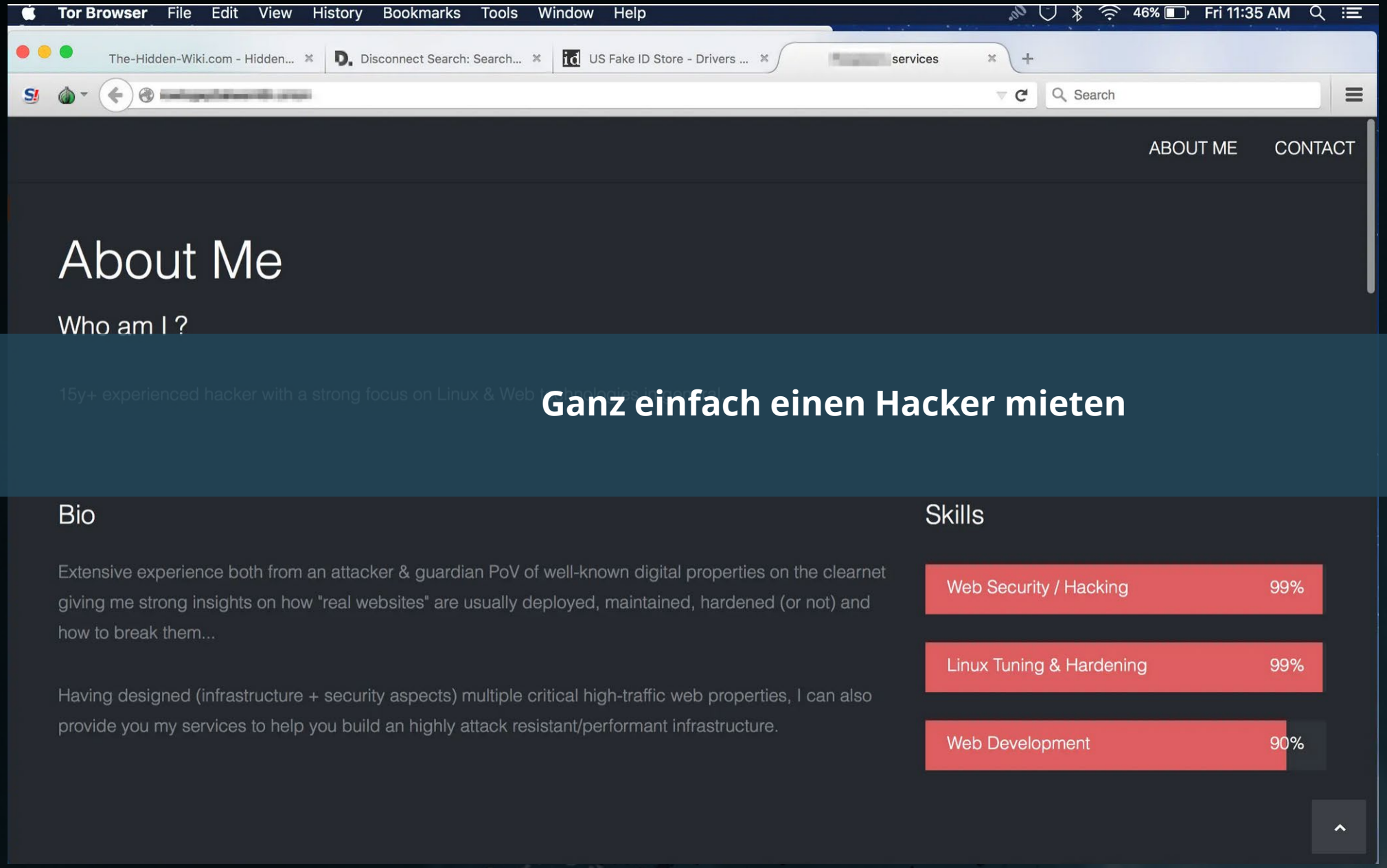


Jeden Tag gibt es rund 40.000 neue gestohlene Kreditkarten Konten

Secutec
Cyber security intelligence



Händler Bewertungen wie auf Amazon



Ganz einfach einen Hacker mieten

Secutec
Cyber security intelligence

Secutec
Cyber security intelligence

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!

Hacker as a Service

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.

Secutec
Cyber security intelligence

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

Secutec
Cyber security intelligence

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.

Hacker as a Service

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

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.

Cyber-Risiken Trends 2023

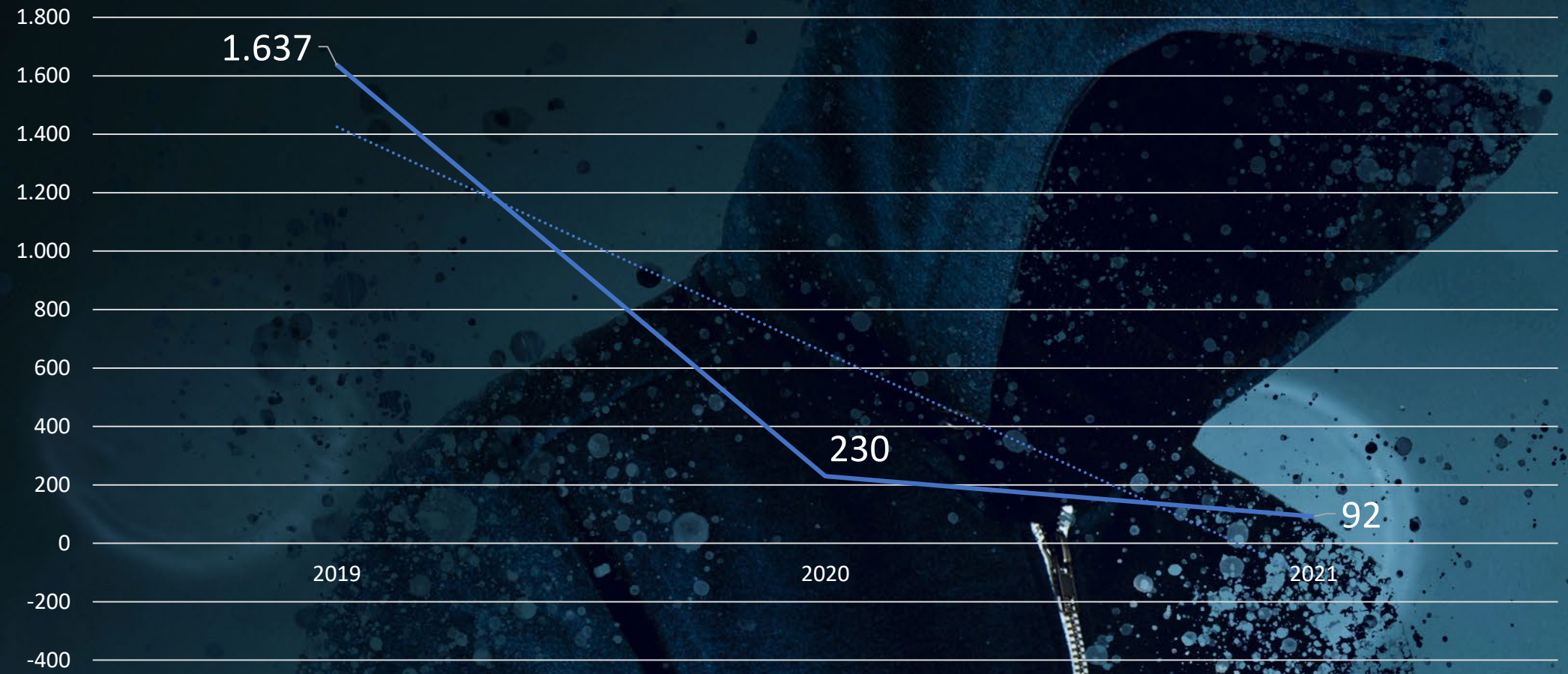
- Supply-Chain-Attacken
- Deep Fake (KI) / Deep Fake Audio-/Visuals
- Professionelle/Trendy Phishing Attacken
- Geopolitische Konflikte – Wiper Funktionalität
- Cyber-War-Klauseln in Versicherungsverträgen
  Bedarf einer professionellen Betreuung
- 3,5 Mio. fehlende Cybersecurity Spezialisten


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

Schwachstelle	Initial Access	Preparation	Impact

Phishing

Secure DNS

Password guessing Bruteforce

Secure SIGHT

Exploit Vulnerability

Secure SIGHT

Email

Secure DNS

Erlangen valider Zugangsdaten

Public Services / Internet

Dokumente mit schadhaftem Inhalt

Secure DNS

Malware

Secure SIGHT

Command & Control

Laterale Verbreitung

Privilege Escalation

Exfiltrieren von Daten

Secure SIGHT

Backups zerstören

Daten verschlüsseln

Wiper Funktionalität

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

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

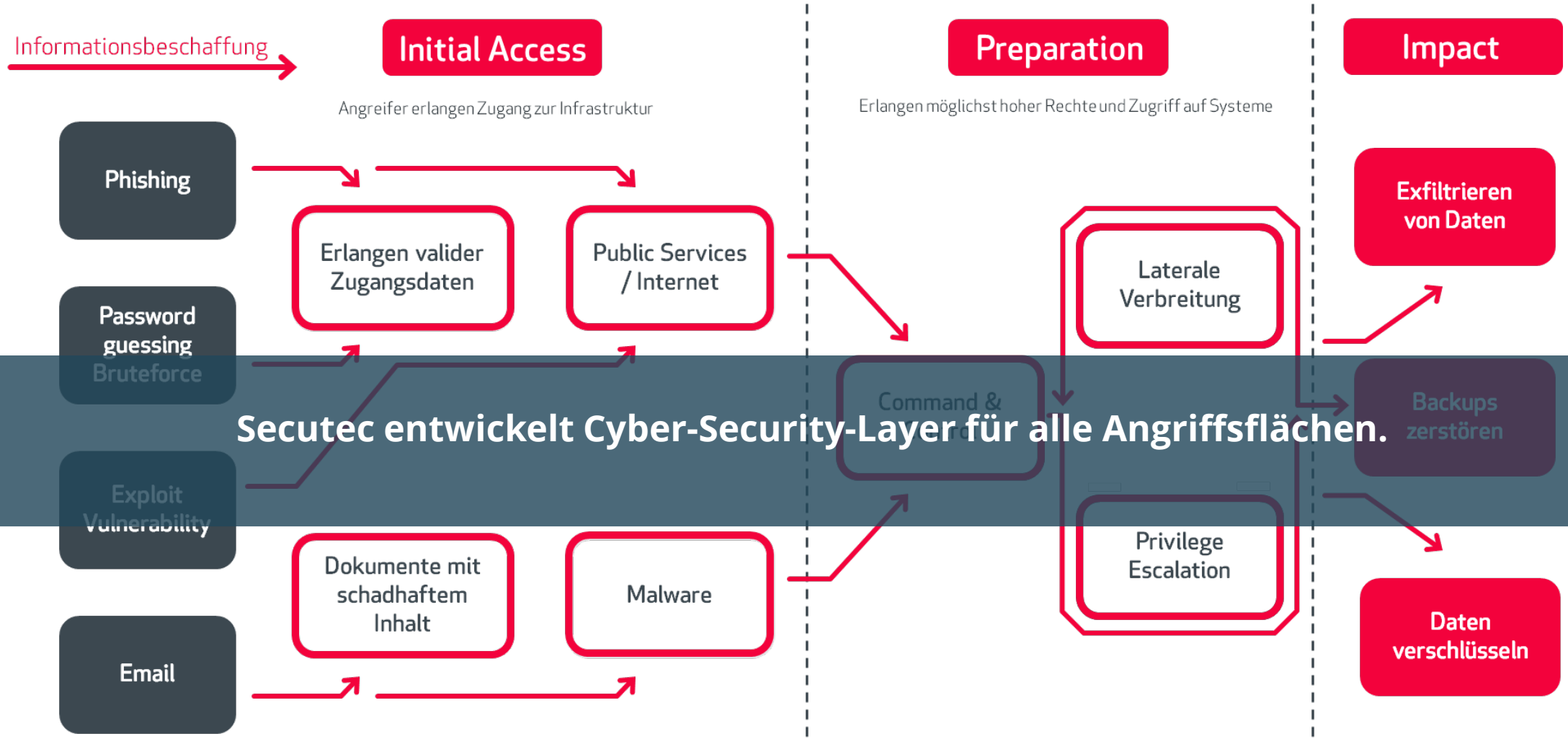
-Server Logs Backup
Je länger desto besser für die Forensik, min. 90 Tage

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

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


Secutec
Cyber security intelligence

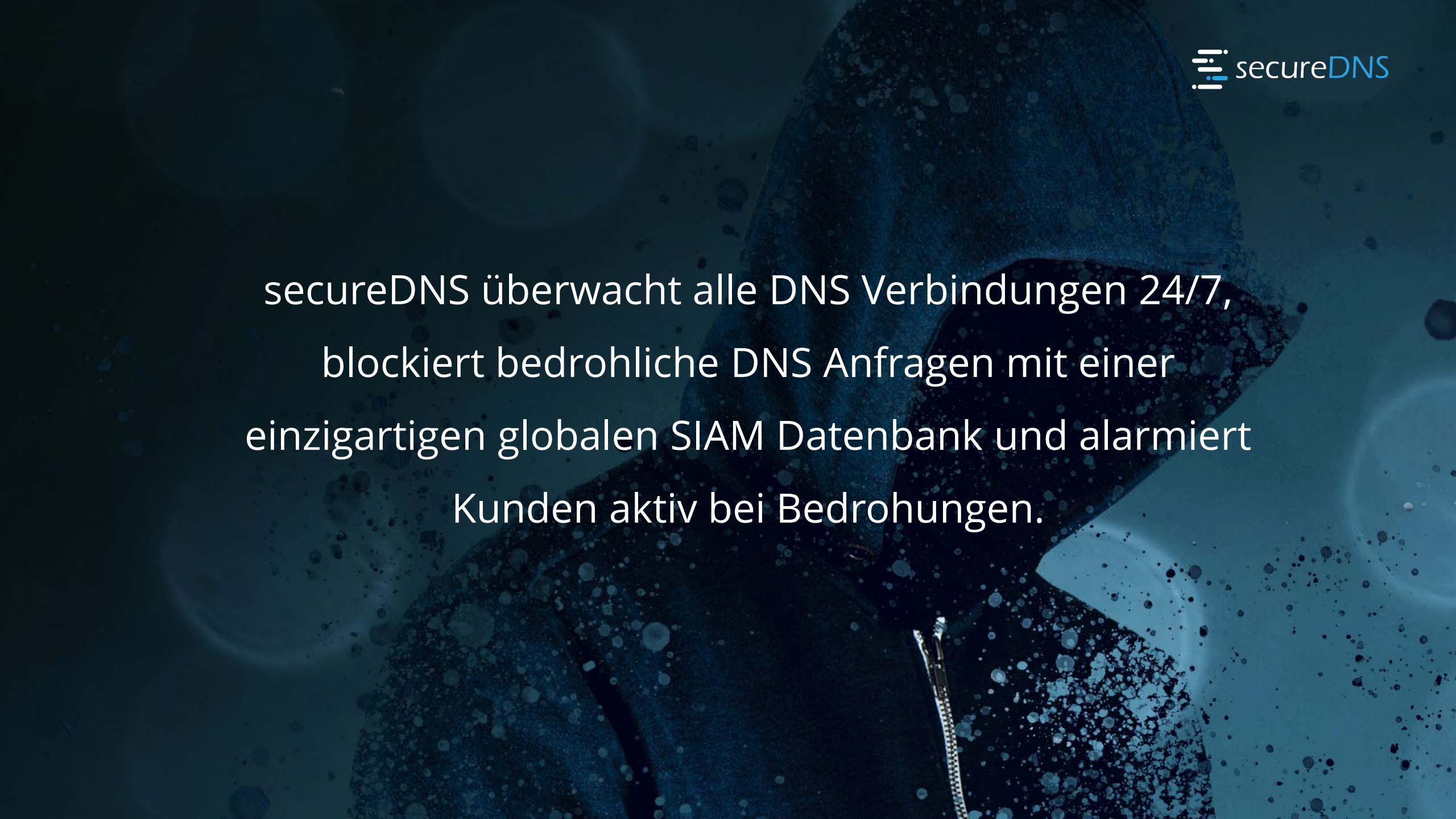
Lifecycle einer Ransomware Attacke



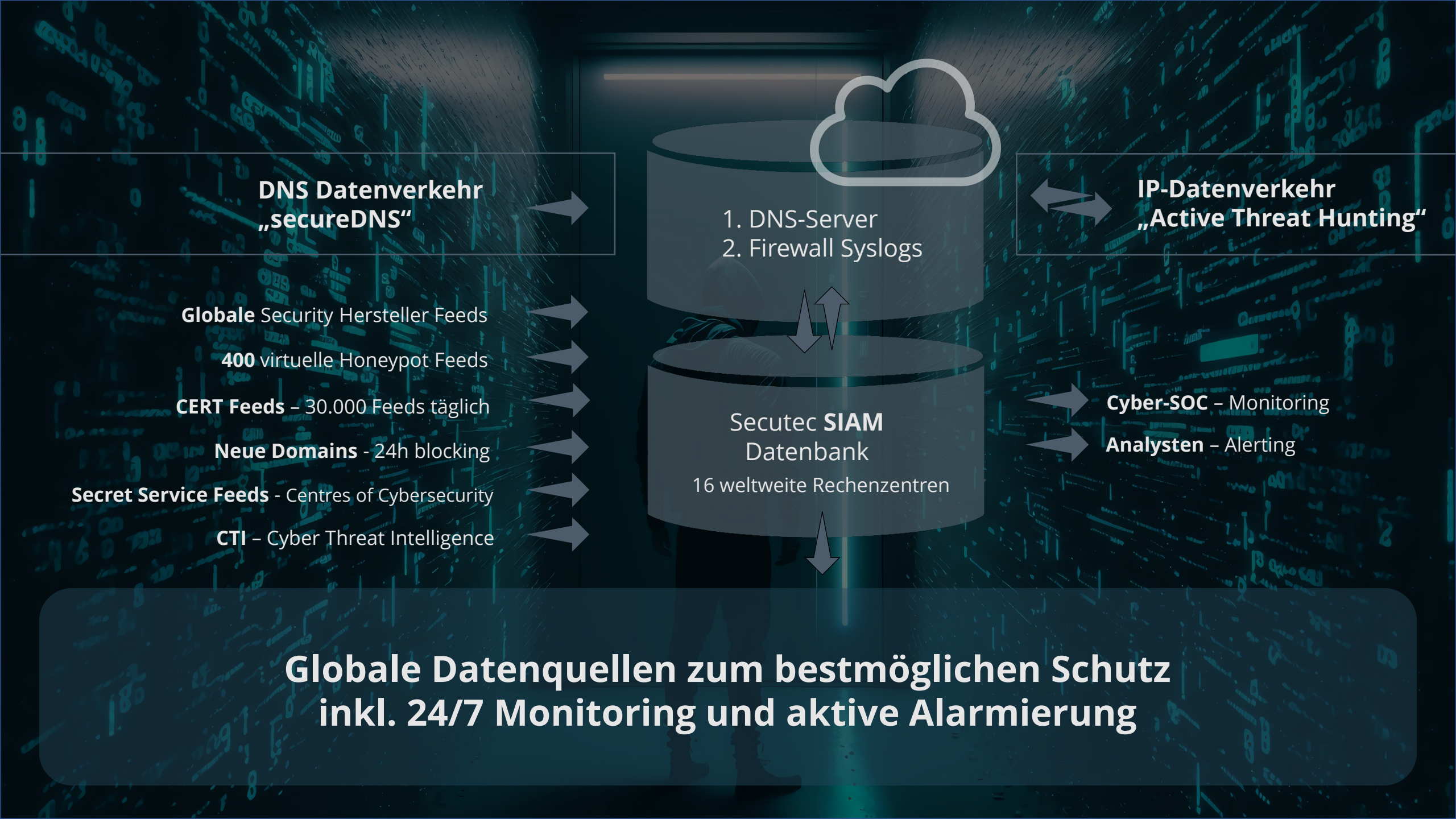
Secutec entwickelt Cyber-Security-Layer für alle Angriffsflächen.

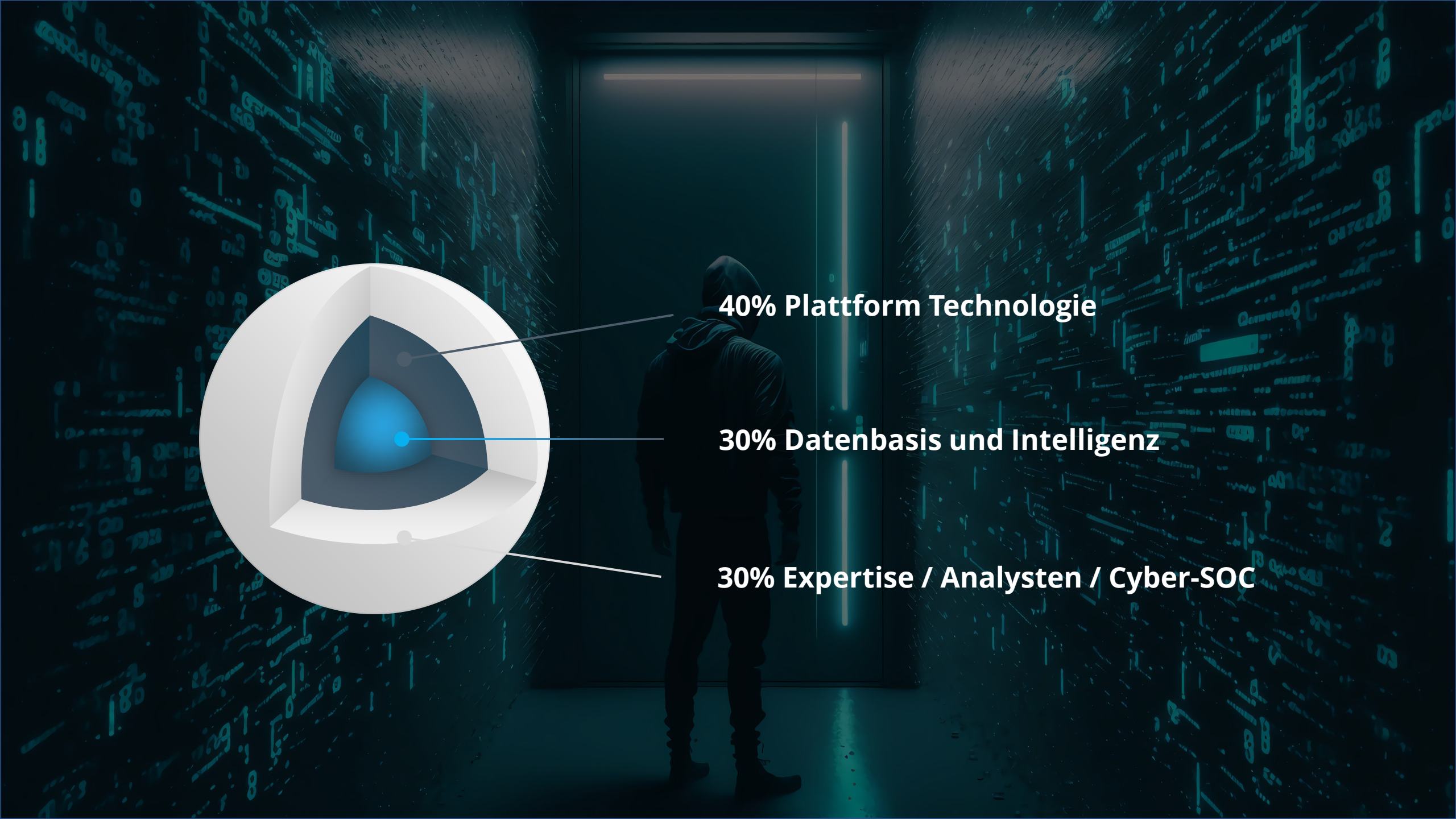
secureDNS

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“
IP-Datenverkehr
„Active Threat Hunting“
1. DNS-Server
2. Firewall Syslogs
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

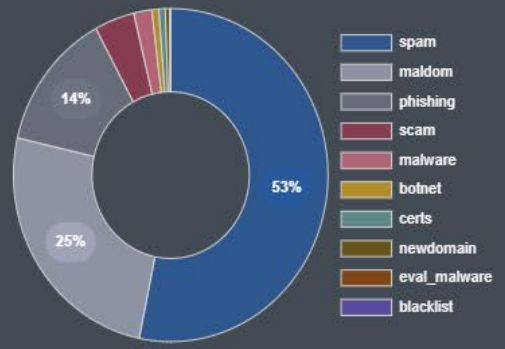
Unser Expertenteam aus dem SOC- und Incident Response Team kann bei Bedarf jederzeit mit Praxiserfahrung und Know-how unterstützen

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

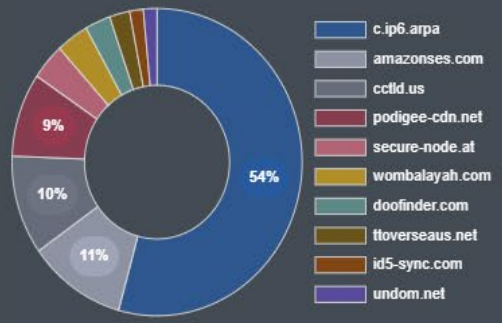
Domain | Query | Category | Public IP | Processes | Users | Computers | Private IP

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

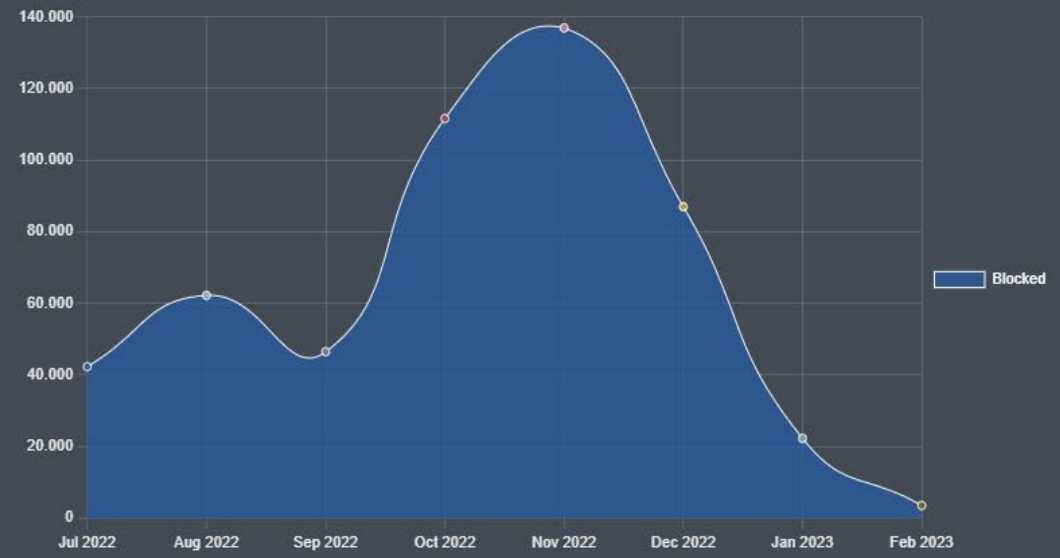
Top 10 categories



Top 10 domains

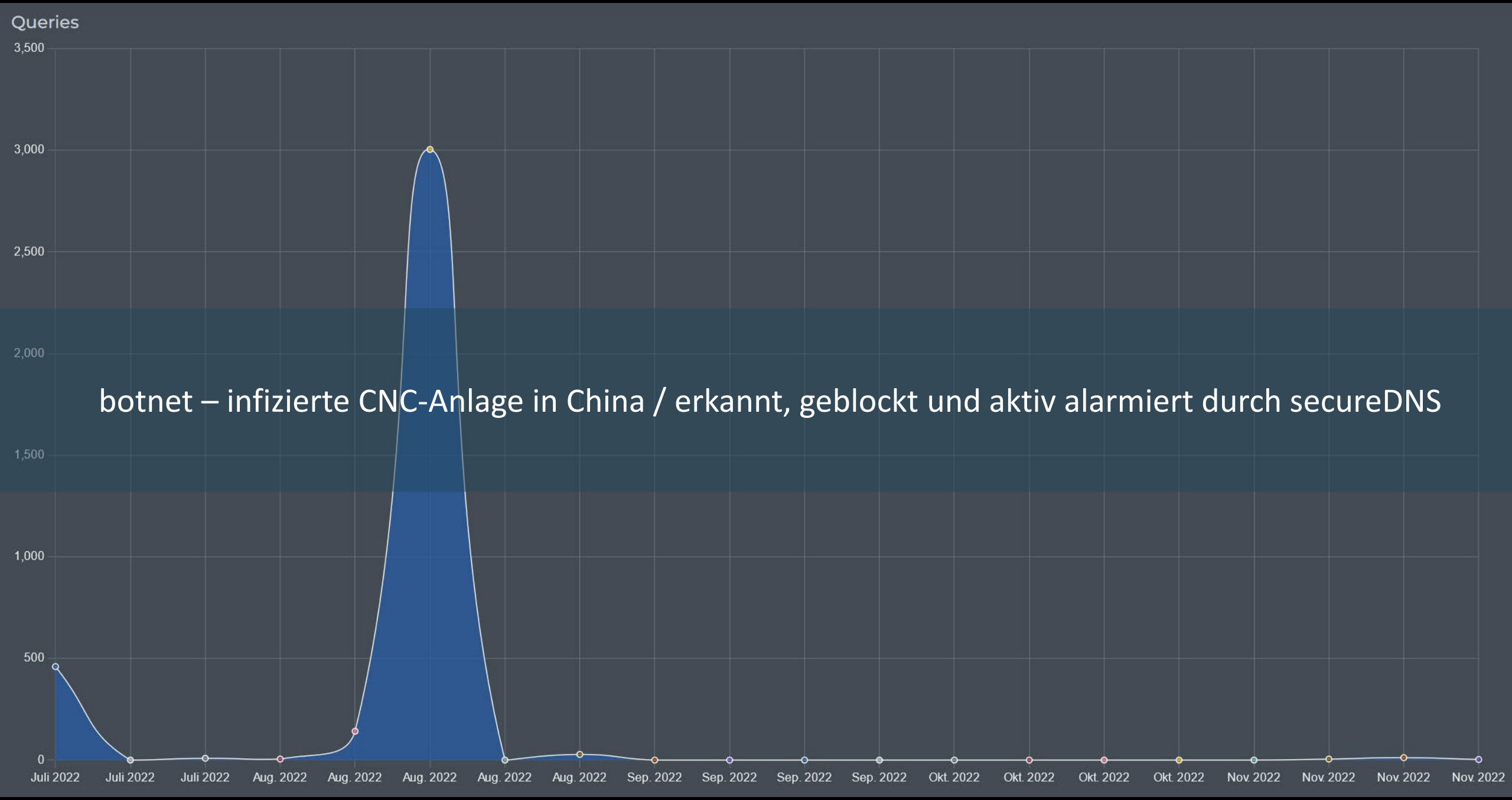


Queries

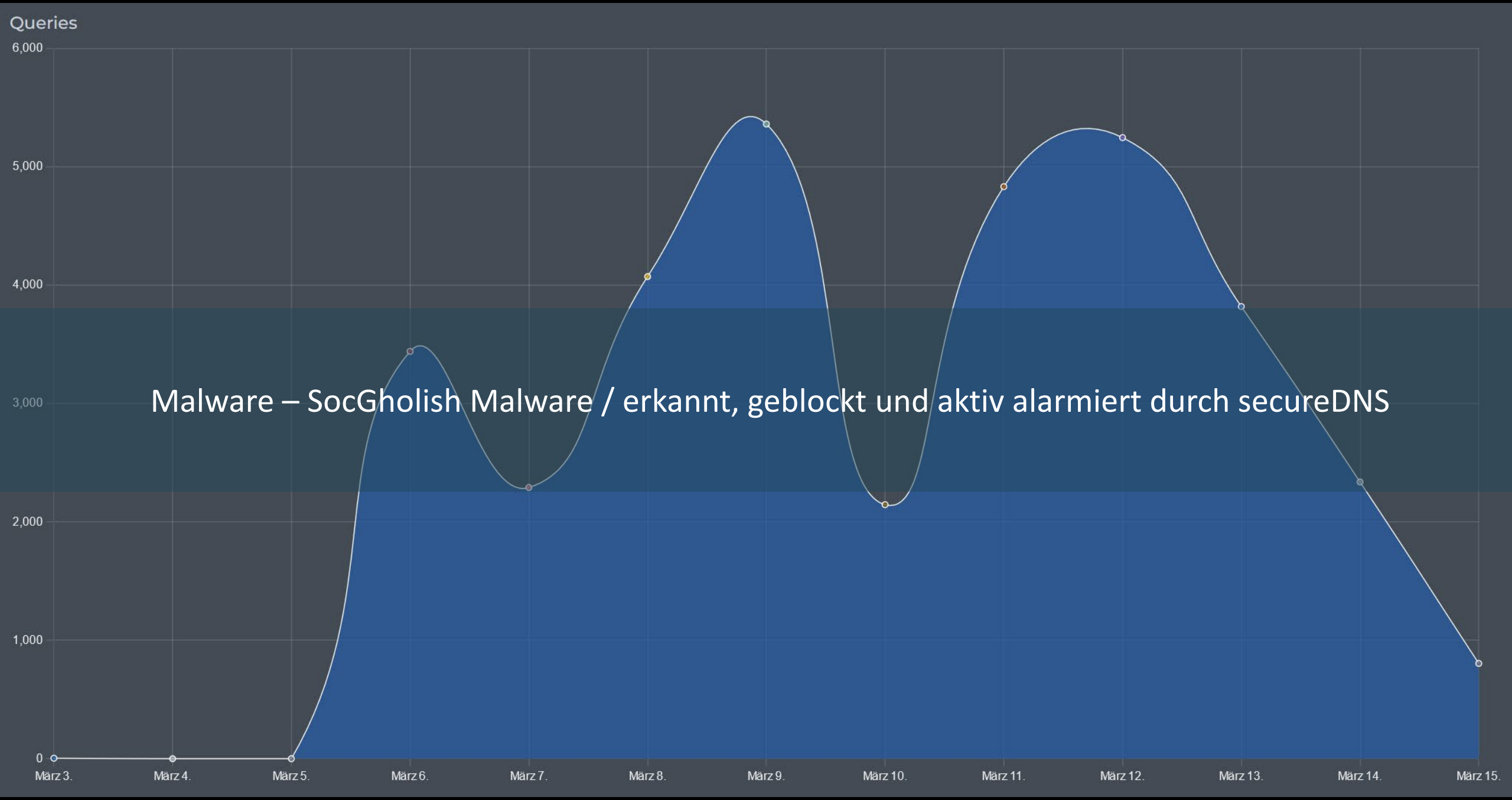


Queries

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



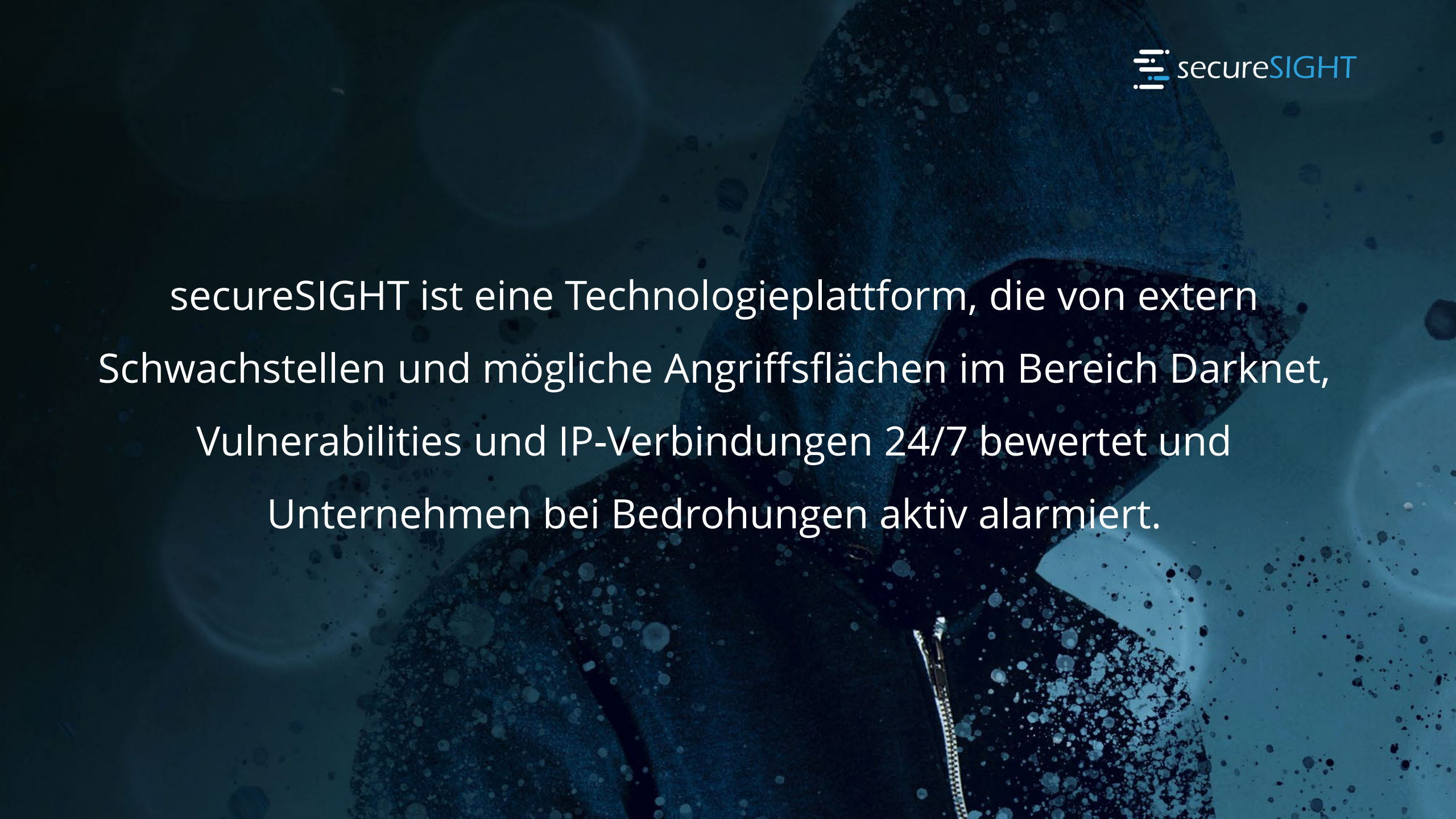
Malware – SocGholish Malware / erkannt, geblockt und aktiv alarmiert durch secureDNS

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

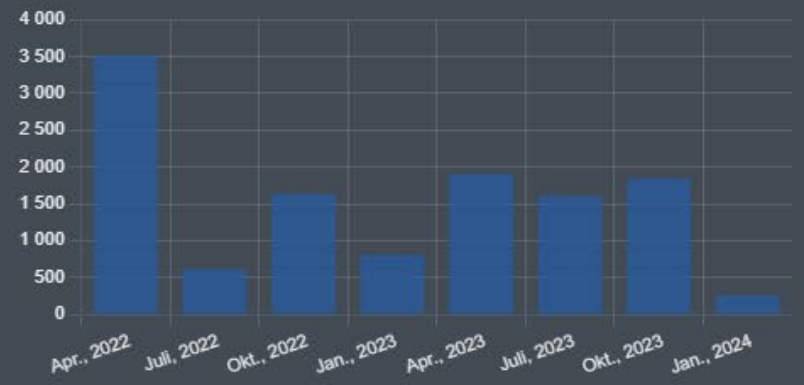
- Aktive Alarmierung bei Bedrohungen

secutecat | Nur Organisation

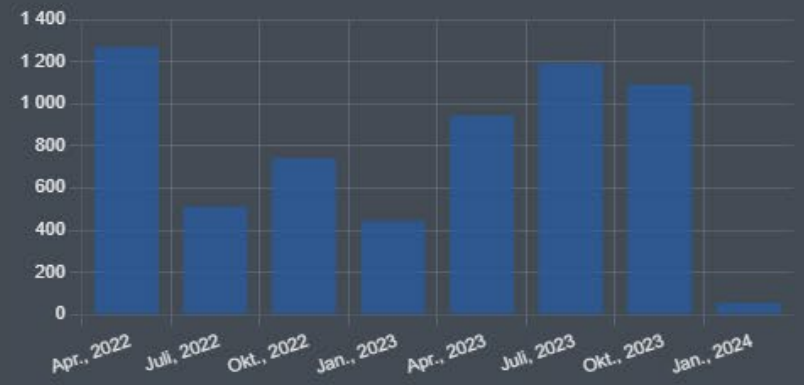
Security Rating | Title

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

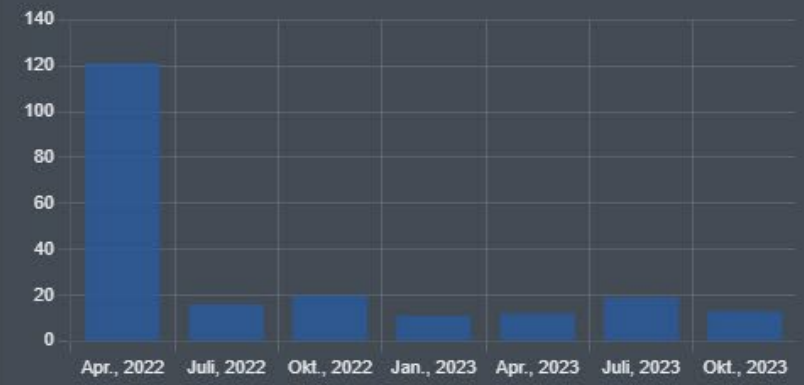
Risks Discovered



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

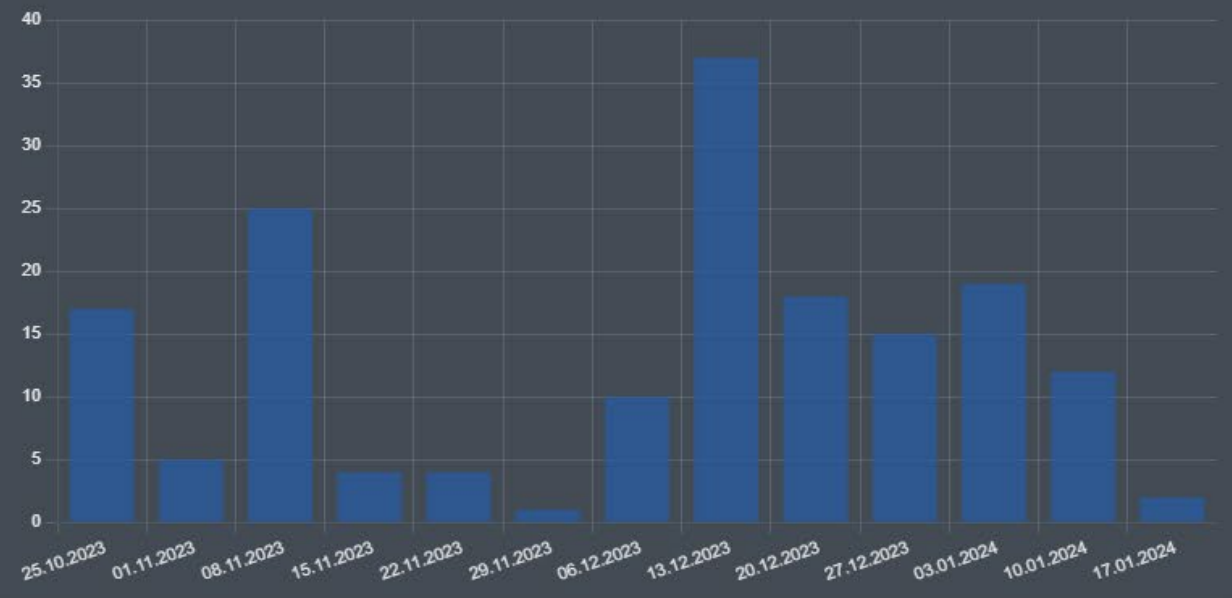
Dashboard | Leaked Credenti... | SecureSIGHT - Dashboard - Leaked Credentials

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

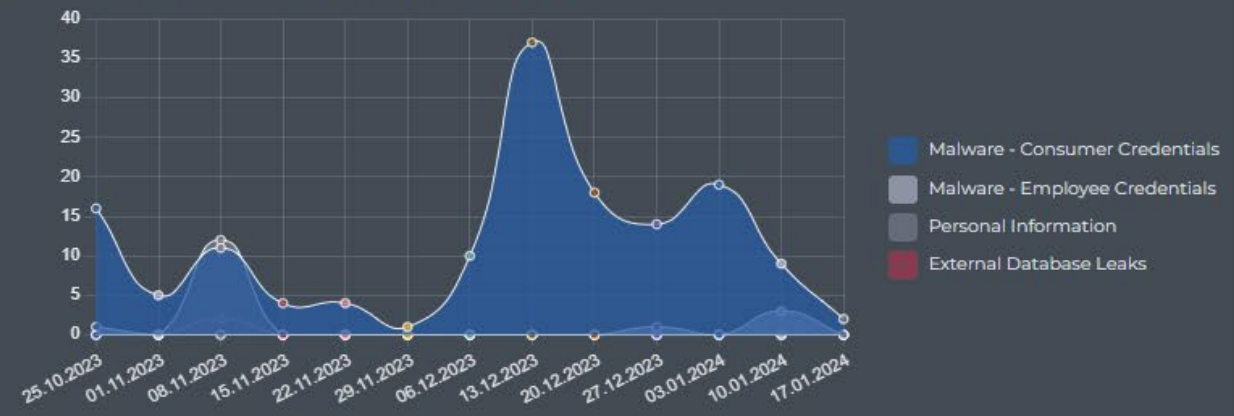
Domain | Breach Title | Email Address | Email Domain | User Domain | Hostname | OS | Leak Source IP

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)



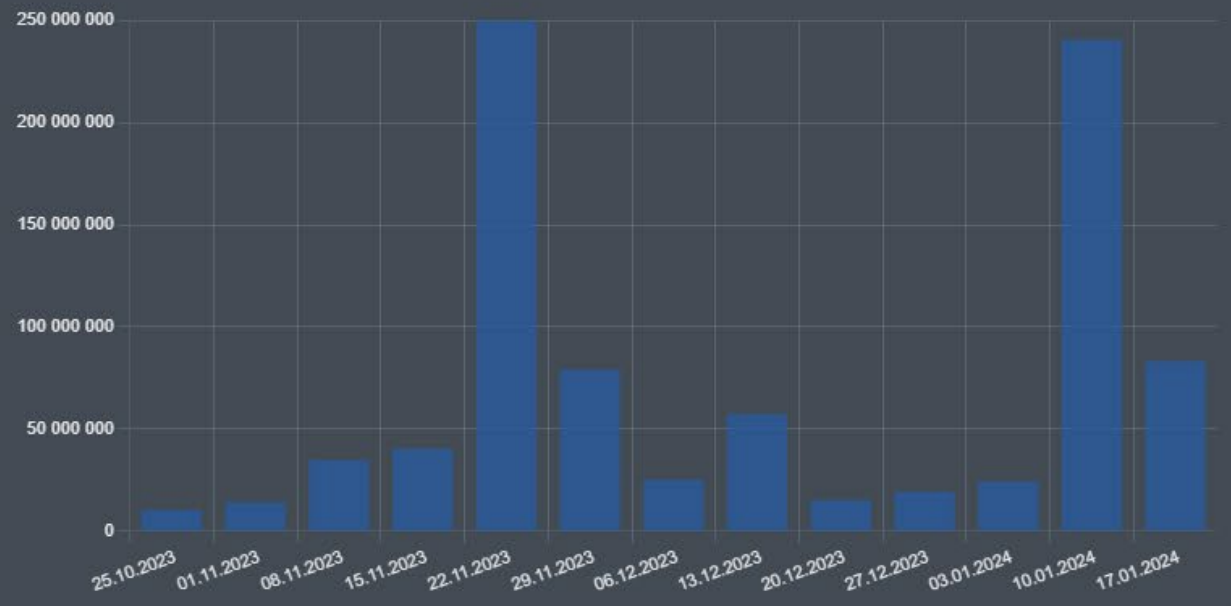
Malware Breaches - Employee Credentials - Login/Email linked to your company

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]

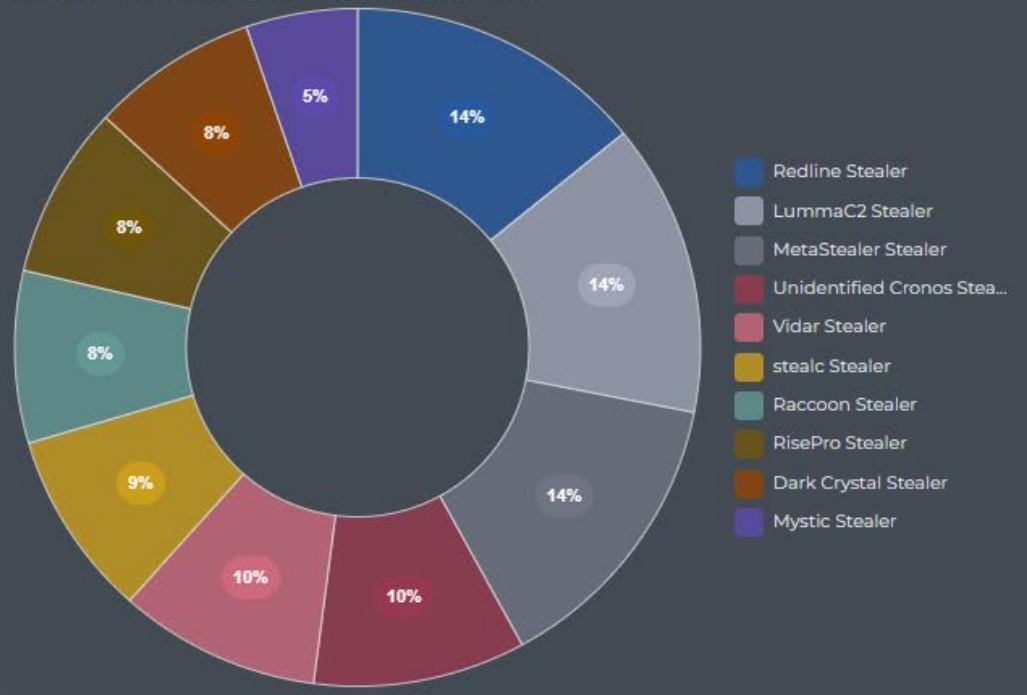
secutecat | Nur Organisation | 24.10.2023 08:12 - 22.01.2024 08:12

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.

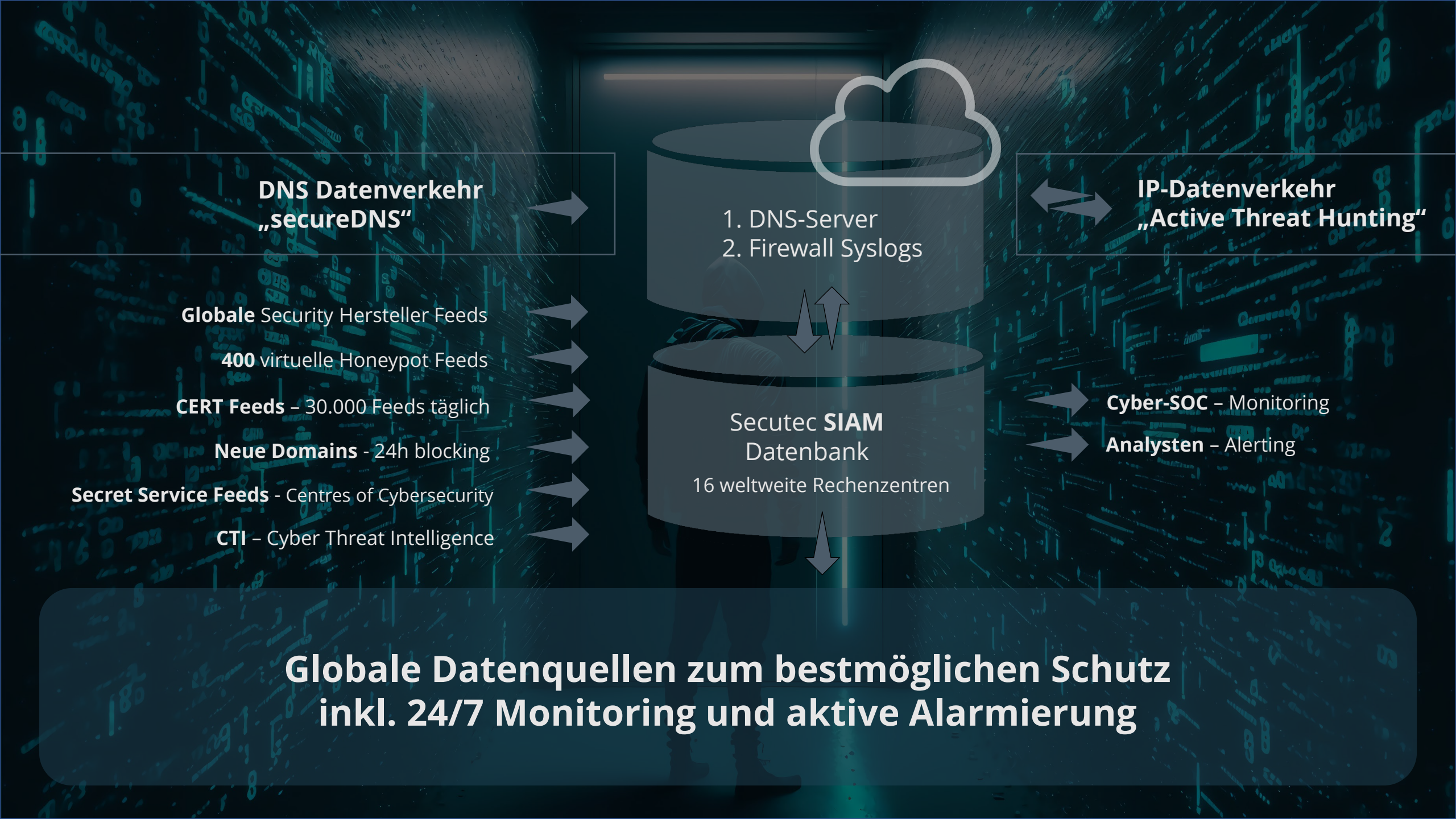
secureSIGHT

Active Manged 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“
IP-Datenverkehr
„Active Threat Hunting“
1. DNS-Server
2. Firewall Syslogs
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