Kontakt

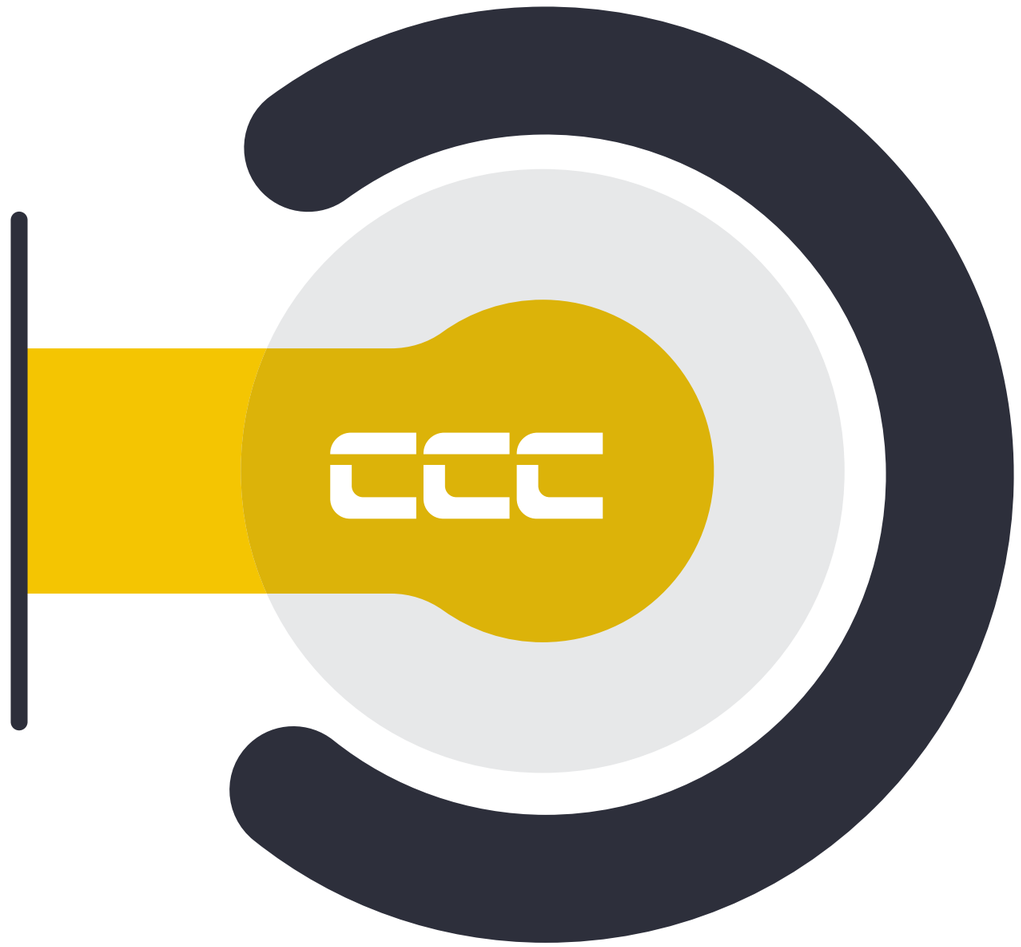
Weststraße 4
57392 Schmallenberg

P : 02972 96396-01

M : 0173 8253824

E : b.richter@cybercomplete.de

w : www.cybercomplete.de



Darknet Monitoring
durch Cyber Complete

Unser
Unternehmen

Das Team der Cyber Complete GmbH versteht die Informationssicherheit als ganzheitlichen Ansatz und eine der wichtigsten Säulen in heutigen Unternehmen. In der Industrie- und Wirtschaftswelt des 21. Jahrhunderts ist inzwischen eine Vernetzung und Globalisierung gegeben, die eine Cybersicherheit für Unternehmen, Konzerne und Privatpersonen unabdingbar macht und eine Grundvoraussetzung für ein erfolgreiches Wirken ist. Täglich erfolgen aus allen Winkeln des Globus unzählige Hackerangriffe und Versuche, in die Systeme von Firmen einzudringen – die Tendenz ist weiter steigend. Auch politische Institutionen und ganze Regierungen sind von diesen Entwicklungen betroffen, besonders wenn es dabei um sensible und besonders schützenswerte Inhalte und Daten geht.

Inhaltsverzeichnis

Darknet-Monitoring
für die digitale Sicherheit

Das Darknet, ein Bereich des Internets, der für seine Anonymität und Undurchsichtigkeit bekannt ist, hat in den letzten Jahren zunehmend an Aufmerksamkeit gewonnen. Während es als Ort für illegale Aktivitäten wie den Handel mit gestohlenen Daten, Drogen und Waffen bekannt ist, spielt das Darknet auch eine Rolle in der globalen digitalen Sicherheitslandschaft.

Darknet-Monitoring bezieht sich auf den Prozess der Überwachung von Aktivitäten im Darknet, um potenzielle Bedrohungen zu identifizieren und darauf zu reagieren. Diese Überwachung kann auf verschiedene Weisen durchgeführt werden, darunter die Verfolgung von Foren und Marktplätzen, das Durchsuchen von Chatrooms und die Analyse von Transaktionsmustern.

Insgesamt ist das Monitoring des Darknets ein wichtiger Bestandteil der digitalen Sicherheitsstrategie von Organisationen und Regierungen weltweit. Durch die Überwachung des Darknets können potenzielle Bedrohungen frühzeitig erkannt und Gegenmaßnahmen ergriffen werden, um die Sicherheit von Daten und Systemen zu gewährleisten. Gleichzeitig ist es wichtig, sicherzustellen, dass diese Überwachungsaktivitäten im Einklang mit ethischen Grundsätzen und rechtlichen Rahmenbedingungen durchgeführt werden.

Deep Web Check
durch Cyber Complete

Verschaffen Sie sich einen frühzeitigen Durchblick zu Ihrer externen Bedrohungslandschaft!

deep web • check

94% der weltweiten Informationen liegen im Deep- und Darkweb!
Wir von Cyber Complete greifen auf diese Informationen zu, um Ihr Unternehmen proaktiv vor Cyberangriffen zu schützen.

- ✓ Erkennen der Angriffsoberfläche
- ✓ Schutz vor digitalen Risiken
- ✓ Vorausschauende Cyber-Intelligenz
- ✓ Stabile Cyber-Sicherheitskultur etablieren

Überwachte Kanäle

Cyber-Interferenz-Risiko-Score: ist eine Kennzahl zur Bewertung des Risikos von Cyber-Interferenzen auf täglicher Basis

Überwachung von Hacker-Diskussionen: umfasst das Scannen von Foren, sozialen Medien und anderen Plattformen nach Diskussionen über Hackeraktivitäten.

Benutzerrisikoprofilierung mit KI: Künstliche Intelligenz wird verwendet, um das Verhalten und die Merkmale von Benutzern zu analysieren und Risikoprofile zu erstellen.

User Risk Profiling: Unser Prozess der Korrelation von Daten aus 100 E-Mail-Adressen, um Muster oder Verbindungen zu identifizieren, die auf eine Sicherheitsbedrohung hinweisen könnten.

Customer Data Breach: Kundendatenverletzung: Dies tritt auf, wenn unbefugte Parteien Zugang zu sensiblen Kundeninformationen erhalten, was zu einem möglichen Missbrauch dieser Daten führen kann.

Cyber-Risiko-Bewertung: Dies ist unser Prozess der Zuweisung eines numerischen Werts zur potenziellen Auswirkung einer Cyber-Bedrohung auf eine Organisation.

Active Monitoring: bezeichnet aktive Tests. Softwareroboter simulieren das Verhalten des Endanwenders.

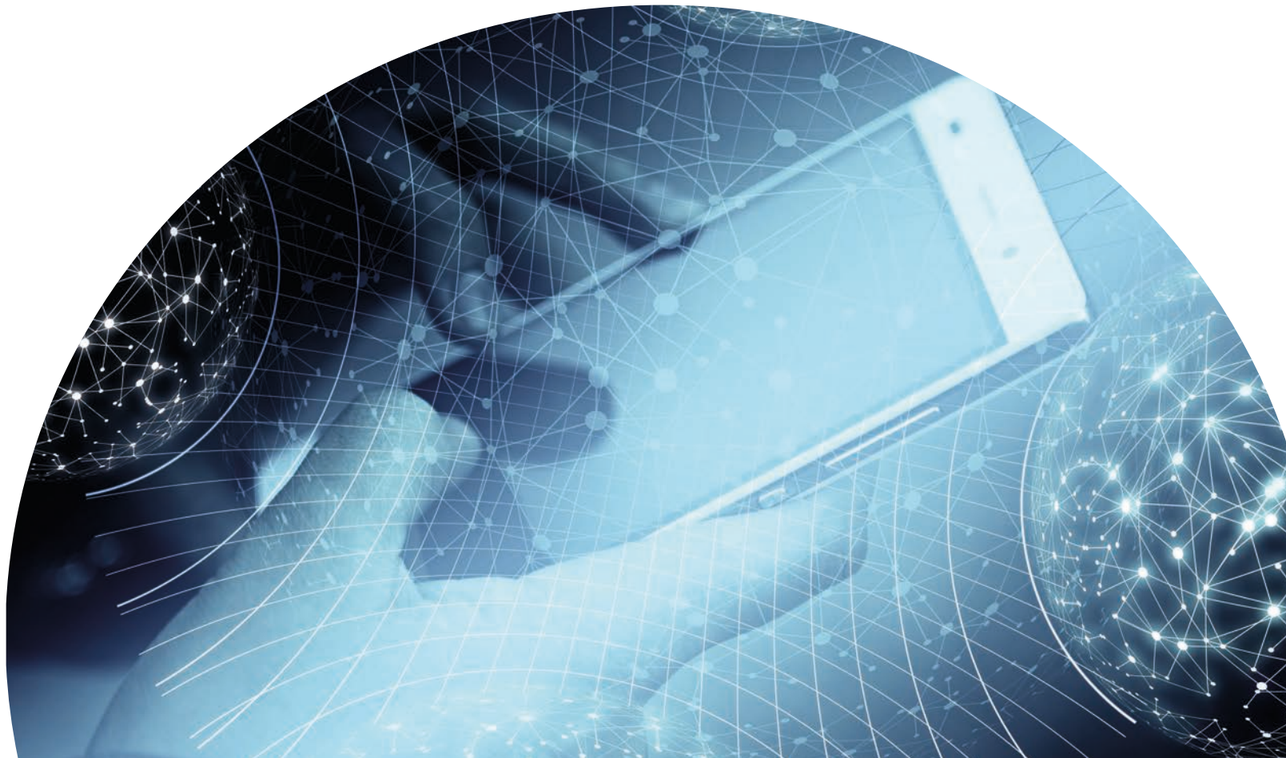
TOR (The Onion Router) ist ein Webbrowser, der den Zugang zu einem Netzwerk bietet, das den Internetverkehr anonymisiert und so ein wirklich privates Surfen ermöglicht.

ZeroNet: ist ein Peer-to-Peer-Netzwerk zur Bereitstellung von Webinhalten. Anstatt über IP-Adressen werden die im Netzwerk veröffentlichten Portale und Webseiten über einen öffentlichen Schlüssel identifiziert

Überwachte Kanäle

- **Black markets**
- **Paste Sites**
- **Telegram**
- **Discord**
- **IRC**
- **Dark Web Forums**
- **Private Hacker Forums**
- **Stealer Malware & Botnet Tracking**
- **Surface Web**
- **Social Media**
- **E-Mail & Chat Support**

Diese Konzepte der Überwachung sind entscheidend für die Aufrechterhaltung robuster Cybersicherheitsmaßnahmen und den Schutz sensibler Informationen vor potenziellen Bedrohungen.



Domainwatch
Upgrade

Proaktives Domain-Monitoring: **bezieht sich auf die aktive Überwachung von fünf Domains, um potenzielle Bedrohungen frühzeitig zu erkennen und darauf zu reagieren.**

Dynamische Profilierung: **umfasst die kontinuierliche Analyse und Anpassung von Benutzerprofilen basierend auf deren Verhalten und Aktivitäten, um Sicherheitsrisiken zu minimieren.**

Web-Überprüfungen (14 Überprüfungen): **beinhaltet versch. Prüfungen von Webseiten, um deren Sicherheit und Integrität zu gewährleisten.**

DNS- und E-Mail-Überprüfungen (24 Überprüfungen): **Diese Überprüfungen stellen sicher, dass die DNS- und E-Mail-Systeme sicher und frei von Bedrohungen sind.**

Infrastrukturüberprüfungen einschließlich Botnet- und Reputationsüberprüfungen (12 Überprüfungen): **umfasst die Überwachung der gesamten IT-Infrastruktur, einschließlich der Erkennung und Verfolgung von Botnets sowie der Überprüfung der Reputation von IP-Adressen und Domains.**

Echtzeit-Alarmbenachrichtigung: **bezieht sich auf die sofortige Benachrichtigung über sicherheitsrelevante Ereignisse oder Bedrohungen, sobald sie erkannt werden. Diese Benachrichtigungen sind entscheidend, um schnell auf potenzielle Sicherheitsvorfälle reagieren zu können und Schäden zu minimieren. Echtzeit-Alarmbenachrichtigungen können über versch. Kanäle wie E-Mail, SMS oder Sicherheits-Dashboards erfolgen und sind ein wesentlicher Bestandteil eines proaktiven Sicherheitsmanagements.**

Partner & Suppliers
Upgrade

Partner- und Lieferantenüberwachung (5 Überprüfungen)

Aktive Angriffsflächenüberwachung

Cyber-Risikobewertung **(täglich)**

Geplante, wiederkehrende Cyber Risk Reportings

(CIQ360) 15 Berichte **(können aufgestockt werden)**

Echtzeit-Alarmbenachrichtigung

Service-Pauschalen

Monatliche Service-Pauschale(n)

DarkNet Monitoring	*ab 499,00 € (netto)*
Domainwatch	*ab 399,00 € (netto)*
Partner & Supplier	*ab 499,00 € (netto)*

Welche Daten benötigt Cyber Complete vom Kunden?

**Wir benötigen Ihren Firmennamen,
die zu prüfenden Domains, die E-Mailadresse
und die Namen der User mit ihren Login-Daten
am besten in einer verschlüsselten Excel-Tabelle.**

B	C	D	E
Firmenname	Domains	E-Mail Adresse	Name der User (Login)

Cyber Security ist nicht länger eine Option, sondern eine Notwendigkeit, um unsere digitale Zukunft zu schützen.

Ein Fallbeispiel

Sehr geehrter Kunde,
unser Watchtower hat in einer neuen Liste in einer Telegram-Gruppe gefunden. Diese Liste beinhaltet auch Daten vom [redacted].

Details:
Quelle: Master Data - Russland
Daten: Firmenadresse, E-Mail-Adressen, Telefonnummer, Webseiten

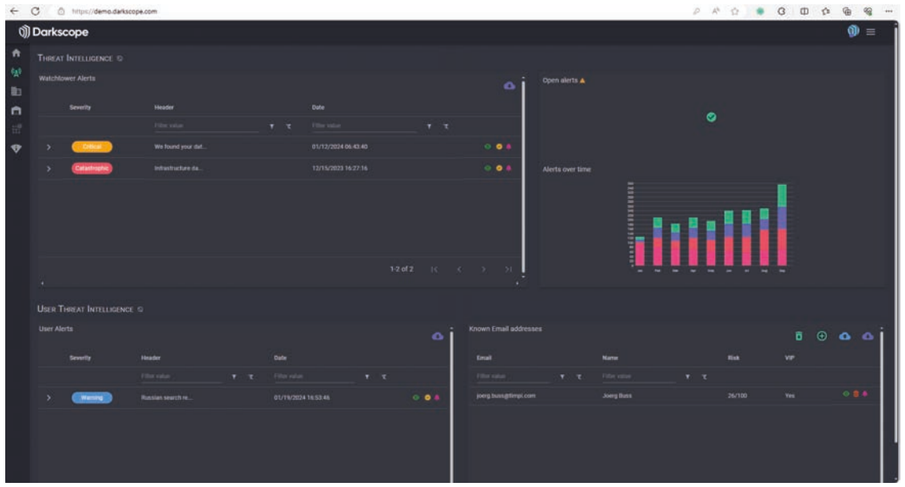
Die Liste wird als neu eingeschätzt und ist seit heute im Umlauf.

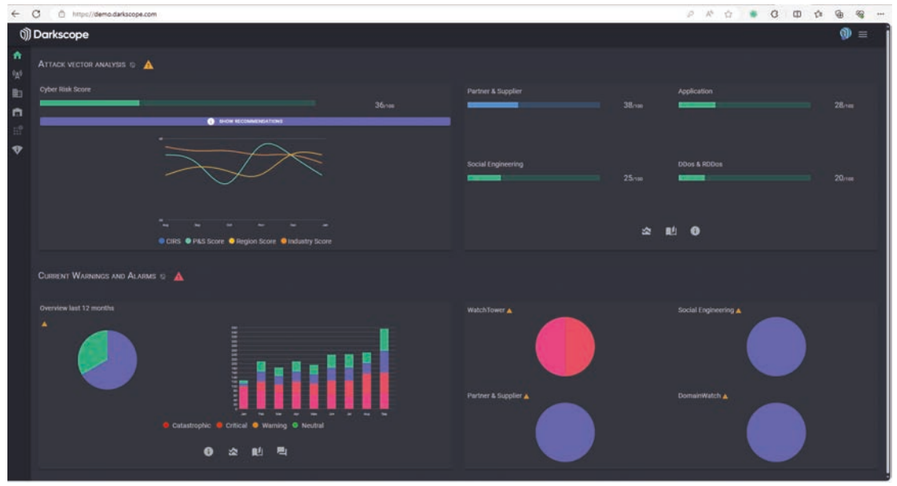
Empfehlung: Wir erwarten um Weihnachten und Neujahr herum einen Anstieg an Attacken gegen Firmen in Deutschland. Bitte weisen Sie Ihre Mitarbeiter auf die neue Gefahrenlage hin.

Wir werden die Situation weiterverfolgen und Sie informieren, sollten wir neue Erkenntnisse erhalten.

Gruß

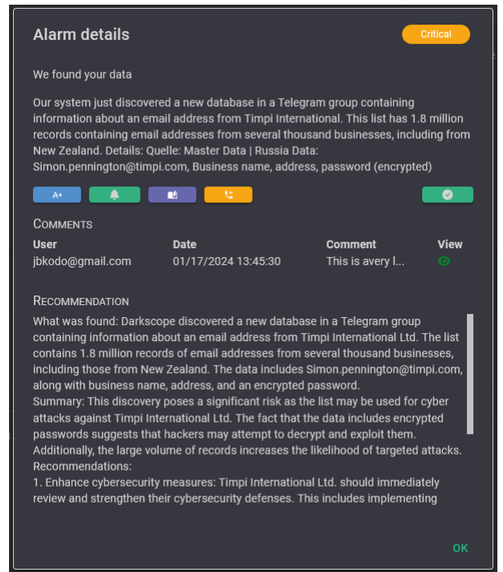
- Dark Web Forums
- TOR
- Zero Net
- Black markets
- Paste Sites
- Telegram
- Discord
- ICQ
- IRC
- Private Hacker Forums
- Private Hacker Channel Market
- Surface Web
- Social media





Kontinuierliche Aktualisierung:

Darknet-Monitoring bezieht sich auf den Prozess der Überwachung von Aktivitäten im Darknet, um potenzielle Bedrohungen zu identifizieren und darauf zu reagieren. Diese Überwachung kann auf verschiedene Weisen durchgeführt werden, darunter die Verfolgung von Foren und Marktplätzen, das Durchsuchen von Chatrooms und die Analyse von Transaktionsmustern.



Blick
in die Zukunft

Die Zukunft der Cybersicherheit wird von einer Reihe von Trends und Entwicklungen geprägt sein, die auf die ständig wachsenden und sich verändernden Bedrohungen im digitalen Raum reagieren. Hier sind einige Schlüsselaspekte der zukünftigen Cybersicherheit.

Künstliche Intelligenz und maschinelles Lernen

Diese Technologien werden immer mehr in Sicherheitslösungen integriert, um Anomalien zu erkennen, Bedrohungen vorherzusagen und automatisierte Reaktionen auf Vorfälle zu ermöglichen.

IoT-Sicherheit

Mit der zunehmenden Verbreitung von Internet of Things (IoT)-Geräten werden Sicherheitslösungen notwendig, die diese Geräte absichern und sie vor Missbrauch schützen.

Zero-Trust-Modell

Dieses Modell geht davon aus, dass niemandem, weder innerhalb noch außerhalb des Netzwerks, uneingeschränktes Vertrauen geschenkt werden sollte. Jede Aktivität und jeder Zugriff wird permanent überprüft und validiert.

Cloud-Sicherheit

Da immer mehr Unternehmen auf Cloud-Dienste umsteigen, wird die Sicherheit dieser Dienste eine kritische Rolle spielen. Cloud-orientierte Sicherheitslösungen und -praktiken werden weiterentwickelt, um Daten und Anwendungen zu schützen.

Sicherheit für kritische Infrastrukturen

Die Sicherheit von kritischen Infrastrukturen wie Energieversorgung, Verkehrssystemen und Gesundheitswesen wird eine wachsende Priorität darstellen, da Angriffe auf diese Systeme erhebliche Auswirkungen auf die Gesellschaft haben könnten.

Menschliche Faktoren

Der Faktor Mensch bleibt eine der größten Schwachstellen in der Cybersicherheit. Schulungen und Sensibilisierungsmaßnahmen werden wichtiger denn je sein, um Mitarbeiter vor sozialen Engineering-Angriffen zu schützen.

> ***Die Zukunft der Cybersicherheit wird von einer Mischung aus fortschrittlichen Technologien, neuen Sicherheitsansätzen und erhöhtem Bewusstsein für die Bedeutung der Sicherheit im digitalen Zeitalter geprägt sein.***