DARKNET THREAT INTELLIGENCE

DarknetSearch

by Kaduu AG

Kontinuierliches Monitoring von Darknet, Deep Web und offenem Web, das Ihnen hilft,
Leaks, offengelegte Assets und Identitätsmissbrauch zu finden, bevor Angreifer sie nutzen.

KUNDENÜBERSICHT · PRODUKTRUNDGANG



darknetsearch.com

AGENDA

Unsere Themen

1 **Die Herausforderung**

Warum Darknet-Exposition für jede Organisation ein wachsendes Risiko ist

2 **Plattformüberblick**

Ein Dashboard für dauerhafte Transparenz über Bedrohungen

3 **Kernfunktionen**

Suche, Zugangsdaten-Exposition, Darknet Chatter, Angriffsfläche, Markenschutz

4 **Alarme & Berichte**

Automatisiertes Monitoring, Vorfälle und Management-Berichte

5 **Für Ihr Team gebaut**

Anwendungsfälle für CISOs, Threat-Intel-Analysten, SOC & MSSP

6 **Erste Schritte**

Kostenlose Testphase, Darknet-Bericht und nächste Schritte

DIE HERAUSFORDERUNG

Ihre Daten werden bereits gehandelt, wo Sie nichts sehen

Gestohlene Zugangsdaten, Malware-Logs und Lookalike-Domains zirkulieren in Darknet-Marktplätzen, Telegram-Kanälen, Paste-Sites und kriminellen Foren, lange bevor sie in einer Datenleck-Schlagzeile auftauchen.

24/7

Kontinuierliches Monitoring von Quellen im Darknet, Deep Web und offenen Web

2.200+

Telegram- und Forenkanäle der Cyberkriminalität erfasst

10+

Risikofaktoren automatisch je Organisation bewertet

24 Std.

Bearbeitungszeit für einen kompletten Darknet-Expositionsbericht

DARKNETSEARCH IM ÜBERBLICK

Eine Plattform für externe Bedrohungstransparenz.

DarknetSearch durchsucht kontinuierlich Darknet, Deep Web und offenes Web, damit Sie immer wissen, wann Ihre Zugangsdaten, Infrastruktur oder Marke exponiert sind – und handeln können, bevor Angreifer es tun.

01

Leak-Erkennung

Erkennen Sie gestohlene Zugangsdaten, kompromittierte Geräte und Lieferketten-Exposition in Echtzeit.

02

Attack Surface Discovery

Sehen Sie Ihr Netzwerk mit den Augen eines Angreifers – CVEs, offene Ports und Schatten-IT.

03

Domänen- & Markenschutz

Stoppen Sie Phishing und Typosquatting, bevor Lookalike-Domains live gehen.

DIE PLATTFORM AUF EINEN BLICK

Ihr Risikowert in einem Dashboard

Jede Organisation erhält einen aktuellen Gesamt-Risikowert, berechnet aus Leak-Historie, Zugangsdaten-Hygiene, offenen Ports und Exposition in Suchmaschinen – mit einer 12-Monats-Zeitleiste zur Fortschrittskontrolle.

— **Gesamt-Risikowert** – eine einzige Zahl von 0–100, verglichen mit Ihrer Branche und Ihren Wettbewerbern.

— **Wichtigste Risikofaktoren** – aktuelle und ältere Leaks, schwache Passwörter, ungewöhnliche offene Ports, Exposition in Suchmaschinen.

— **Risiko-Zeitleiste** – Verlauf des Risikos Ihrer Organisation und Ihrer Infrastruktur im letzten Jahr.

— **Statistiken zu Zugangsdaten & geleakten Nutzern** – geleakte Datensätze gesamt, Stealer-Logs, Combo-Listen und riskanteste Nutzer.



Risikobewertung | Benchmarking | Trend-Zeitleiste | Zugangsdaten-Statistik

KERNFUNKTION · 01

Darknet und Deep Web in Sekunden durchsuchen

Quick search durchsucht alle Datenquellen gleichzeitig; mit Expert search erstellen Analysten präzise boolesche Abfragen für eine bestimmte Quelle – ideal für die erste Reaktion und die tiefe Untersuchung.

— **Suche nach allem** – Domäne, E-Mail, Name, IP, Marke, Passwort, Dateiname oder Hostname.

— **14 spezialisierte Quellen** – Raw Data, Filtered Credentials, Telegram, Discord, Pastes und mehr.

— **Eigener Query Builder** – kombinieren Sie AND / OR / NOT, Zeiträume und Dateitypen für mehr Präzision.

— **Sofortige, deduplizierte Ergebnisse** – Zugangsdaten, Broker, Pastes und Phishing-Treffer nach Relevanz sortiert.



Raw Leaks | Telegram | Discord | Datenhändler | SSL-Logs

KERNFUNKTION · 02

Zugangsdaten-Exposition, bewertet und priorisiert

Jedes geleakte Paar aus Benutzername und Passwort zu Ihrer Domäne wird dedupliziert und bewertet. So konzentriert sich Ihr Team auf die wichtigsten Konten – nicht auf Tausende Rohzeilen.

— **Neuheits-, Risiko- und Wiederverwendungswerte** – sehen Sie sofort, welche Zugangsdaten neu, hochriskant oder anderswo wiederverwendet sind.

— **Eigene Infrastruktur vs. Dritte** – trennen Sie interne Logins von Exposition bei Partnern und Kunden.

— **Stealer-Logs & Combo-Listen** – erfassen Sie per Malware abgegriffene Zugangsdaten, nicht nur alte Leak-Dumps.

— **Vergleichsberichte** – vergleichen Sie die Zugangsdaten-Exposition von Tochterfirmen, Marken oder Wettbewerbern.



Eindeutige Zugangsdaten | Passwort-Wiederverwendung | Stealer-Logs | Combo lists | Domänen-Konten

KERNFUNKTION · 03

Darknet-Chatter-Monitoring in Echtzeit

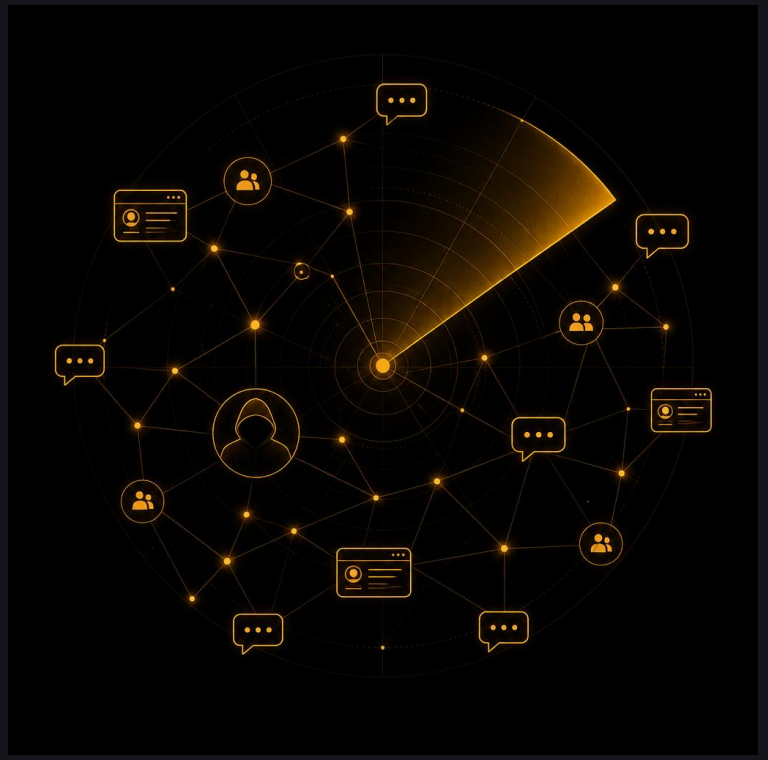
Verfolgen Sie Beiträge in Cybercrime-Foren, Marktplatz-Angebote und Aktivitäten von Threat Actors, sobald sie erscheinen – in Tausenden Telegram-Kanälen, Foren und carding-Seiten.

— **Über 2.200 überwachte Kanäle** – Telegram, Discord und Dark-Foren, durchsuchbar mit booleschen Operatoren.

— **Threat-Actor-Tracking** – ordnen Sie Chatter bekannten Aliasen zu und überwachen Sie ransomware-Gruppen direkt.

— **Kategorisierte Ergebnisse** – Marktplätze, Leaks & Daten, carding/Betrug, Hacking, Dienste, Diskussion.

— **Live-Recherchen** – fragen Sie Tor / I2P und geschlossene Kanäle diskret über unser Proxy-Netzwerk ab.



Marktplätze | Leaks & Daten | Carding / Betrug | Threat Actors | Live-Suche

KERNFUNKTION · 04

Angriffsflächen- & Code-Exposure-Scans

Sehen Sie Ihr Unternehmen mit den Augen eines Angreifers. Entdecken Sie vergessene Assets, riskante Konfigurationen und in öffentlichem Code geleakte Secrets, bevor andere sie finden.

— **Attack Surface Discovery** – automatische Sicht auf aus dem Internet erreichbare Hosts, CVEs und offene Ports.

— **Shadow-IT-Erkennung** – finden Sie Assets, die Entwickler, Agenturen oder Freelancer ohne Ihr Wissen angelegt haben.

— **Code-Exposure-Scans** – Stichwortsuche in GitHub, Gist, GitLab, Postman und per Google dorking.

— **Eingrenzung über Contributors** – öffentliche Repos und Contributors einer Organisation abbilden, um Scans gezielt zu fokussieren.



CVEs | Offene Ports | GitHub | Gist | Postman

KERNFUNKTION · 05

Domänen- & Markenschutz

Verhindern Sie, dass Threat Actors Ihre Marke fälschen, bevor eine phishing-Seite online geht – bei Lookalike-Domains, App Stores und sozialen Plattformen.

— **typosquatting-Erkennung** – tägliche Überwachung neuer Domänen-Registrierungen und SSL-Transparency-Logs.

— **Visuelle Analyse von Logo-Fälschungen** – WHOIS, Geolokalisierung, Screenshots und Web-Risikowert für jede gefundene Domäne.

— **App-Store- & Social-Monitoring** – gefälschte Apps bei iTunes / Google Play und falsche Markenprofile.

— **Eigene Risikoberichte** – Berichte zu Domain-Spoofing, VIP Executive, Social Media und Application Security.



typosquatting | SSL Transparency | App Stores | VIP-Executive-Bericht

KERNFUNKTION · 06

Automatische Alarme & Incident Response

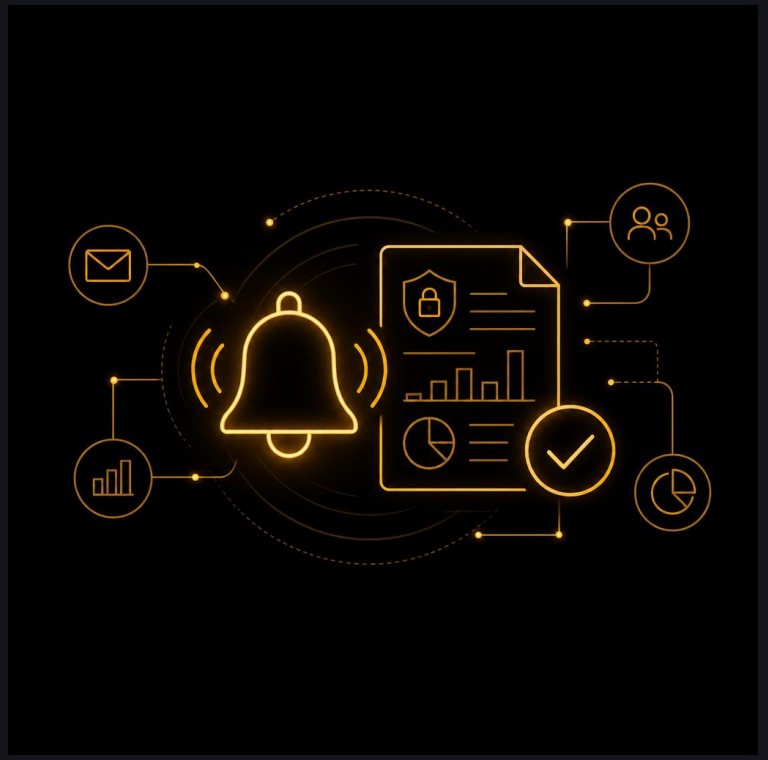
Machen Sie aus kontinuierlichem Monitoring Handlung. Legen Sie Regeln einmal an und werden Sie sofort benachrichtigt, wenn etwas wichtig wird – mit vollem Kontext für die sofortige Untersuchung.

— **Eigene Alarmregeln** – Abfragen für jede Datenquelle erstellen und die Benachrichtigungshäufigkeit wählen.

— **Incident-Feed** – jeder Auslöser mit Status und Quelle protokolliert, per Klick bis in die Raw Data.

— **Extrahierte Entitäten** – Domänen, Benutzernamen und Passwörter werden aus jedem Treffer automatisch extrahiert.

— **Intelligente Ausschlüsse** – False Positives und wiederkehrende Treffer mit wiederverwendbaren Ausschlussregeln stummschalten.



Alarmregeln | Incidents | Ausschlüsse | Webhooks

KERNFUNKTION · 07

Management-Berichte & Branchenvergleich

Machen Sie aus Raw Data Berichte für die Geschäftsleitung – automatisch geplant oder auf Abruf erstellt und mit Ihrer Branche und Ihren Wettbewerbern verglichen.

— **Vollständige Assessments** – Berichte per Klick zu Datenleck-Risiko, Infrastruktur, Spoofing und App-Sicherheit.

— **Vergleichsbericht geleakter Zugangsdaten** – Exposition über Bereiche, Tochtergesellschaften oder Vergleichsunternehmen hinweg messen.

— **Geplante Zustellung** – wiederkehrende Berichte landen automatisch in Ihrem Postfach, ganz ohne Handarbeit.

— **Darknet Exposure Report** – eine einmalige 24-Stunden-Tiefenanalyse als PDF + CSV-Rohdaten.



Datenleck-Risiko | Infrastrukturrisiko | Domain-Spoofing | VIP Executive | Geplante Berichte

FÜR IHR TEAM GEMACHT

Gezielte Einblicke für jede Rolle in der Cybersicherheit

CISOs

Strategischer Überblick & Risikopriorisierung

Laufende Sicht auf geleakte Zugangsdaten, offene Zugänge und Datenlecks bei Dritten – aufbereitet zu klaren Erkenntnissen für Geschäftsleitung, Governance und Compliance.

Threat-Intelligence-Analysten

Erkennen, korrelieren, einordnen

Vereinen Sie Darknet-Suche, Monitoring gestohlener Daten, Stealer-Log-Analyse und Profiling von Threat Actors in einem Workflow, um neue Bedrohungen früher zu bestätigen.

SOC-Analysten

Schnellere, präzisere Reaktion

Reichern Sie SIEM und Incident-Untersuchungen mit externen Darknet-Signalen an, um Vorfälle schneller zu bestätigen, Fehlalarme zu senken und die mittlere Reaktionszeit zu verkürzen.

BEREIT FÜR ENTERPRISE & MSSP

Gebaut für den Einsatz über Teams, Marken und Kunden hinweg

Verwalten Sie jede Tochtergesellschaft, Marke oder jeden Kunden in einem Konto – mit granularen Rollen, Transparenz über die Nutzung und vollem API-Zugriff für die Automatisierung.

— **Mandantenfähige Organisationsverwaltung –** sofort zwischen Kundenkonten wechseln

— **Rollenbasierte Zugriffskontrolle mit 2FA –** System Admins, Org Users und mehr

— **Nutzungs-Dashboards –** Kontingent je Dienst verfolgen (Suchen, Alarme, Berichte, API-Aufrufe)

— **Volle REST API –** Alarme und Leak-Daten direkt in Ihr SIEM oder SOAR übertragen



WARUM KUNDEN UNS VERTRAUEN

Im Einsatz bei Security-Teams in vielen Branchen

"

Nutzt DarknetSearch, um Datenlecks von Kunden, exponierte Assets und Domain-Spoofing in Echtzeit zu erkennen. Alarme und API-Reporting helfen dem SOC, schneller zu reagieren.

Cloud y Olé

Managed-Security-Anbieter

"

Erkennt geleakte Zugangsdaten und Datenlecks im Darknet und speist Alarme direkt in das SIEM ein, um Zugangsdaten im Enterprise-Maßstab proaktiv zu erneuern.

Bühler

Globaler Industriehersteller

"

Überwacht das Darknet auf Leaks und exponierte Daten, die von ihnen unterstützte NGOs betreffen – geschätzt für die einfache Bedienung und die Relevanz der Informationen trotz knapper Ressourcen.

CyberPeace Institute

Schweizer Cybersecurity-NGO

Bewertet auf G2 · g2.com/products/kaduu/reviews

JETZT STARTEN

Sehen Sie Ihre Exposition. Starten Sie heute.

7 Tage kostenlos testen

Testen Sie die gesamte DarknetSearch-Plattform – unverbindlich und ohne Kreditkarte.

KOSTENLOS TESTEN

Darknet Exposure Report

Einmalige Tiefenanalyse: exponierte Zugangsdaten, Leak-Trends, gefährdete Nutzer und gefälschte Domänen. Lieferung als PDF + CSV innerhalb von 24 Stunden.

BERICHT BESTELLEN

Individuelles Angebot

Erhalten Sie ein Enterprise- oder MSSP-Angebot, abgestimmt auf Größe und Risikoprofil Ihrer Organisation.

ANGEBOT ANFORDERN



Finden wir, was bereits exponiert ist.

Vielen Dank – wir freuen uns darauf, Ihnen den Live-Risikowert Ihrer Organisation zu zeigen.

---

darknetsearch.com

Kaduu AG · Schweiz

