DARK WEB THREAT INTELLIGENCE

DarknetSearch

by Kaduu AG

Continuous dark, deep and open web monitoring that helps you find
leaks, exposed assets and impersonation before attackers use them.

CLIENT OVERVIEW · PRODUCT WALKTHROUGH



darknetsearch.com

AGENDA

What we'll cover

1 **The Challenge**

Why dark web exposure is a growing risk for every organization

2 **Platform Overview**

One dashboard for continuous threat visibility

3 **Core Capabilities**

Search, credential exposure, darknet chatter, attack surface, brand protection

4 **Alerts & Reporting**

Automated monitoring, incidents and executive reports

5 **Built For Your Team**

CISOs, threat intel analysts, SOC & MSSP use cases

6 **Getting Started**

Free trial, darknet report, and next steps

THE CHALLENGE

Your data is already being traded somewhere you can't see

Stolen credentials, malware logs and lookalike domains circulate across dark web markets, Telegram channels, paste sites and criminal forums long before they show up in a breach headline.

24/7

Continuous monitoring of dark, deep and open web sources

2,200+

Cybercrime Telegram & forum channels tracked

10+

Risk factors scored per organization, automatically

24h

Turnaround for a full darknet exposure report

INTRODUCING DARKNETSEARCH

One platform for external threat visibility.

DarknetSearch continuously scans the dark, deep and open web so you always know when your credentials, infrastructure or brand are exposed — and can act before attackers do.

01

Leak Detection

Identify stolen credentials, compromised devices and supply-chain exposure in real time.

02

Attack Surface Discovery

See your network the way an attacker does — CVEs, open ports, and shadow IT.

03

Domain & Brand Protection

Stop phishing and typo-squatting before lookalike domains go live.

PLATFORM AT A GLANCE

Your risk score, in one dashboard

Every organization gets a live Overall Risk Score, calculated from leak history, credential hygiene, exposed ports and search-engine exposure — with a 12-month timeline so you can track progress.

— **Overall Risk Score** — a single 0-100 number benchmarked against your industry and competitors.

— **Top risk factors** — recent vs. historical leaks, weak passwords, unusual open ports, search exposure.

— **Risk timeline** — trend your organization's risk and infrastructure risk over the past year.

— **Credential & leaked-user stats** — total leaked records, stealer logs, combo lists and riskiest users.



Risk scoring | Benchmarking | Trend timeline | Credential stats

CORE CAPABILITY · 01

Search the dark & deep web in seconds

Quick Search sweeps every data source at once; Expert Search lets analysts build precise, boolean queries against a specific source — ideal for both first response and deep investigation.

— **Search by anything** — domain, email, name, IP, brand, password, file name or host name.

— **14 specialised sources** — raw leaks, filtered & raw credentials, Telegram, Discord, pastes and more.

— **Custom query builder** — combine AND / OR / NOT operators, date ranges and file types for precision.

— **Instant, deduplicated results** — credentials, brokers, pastes and phishing hits ranked by relevance.



Raw Leaks | Telegram | Discord | Data Brokers | SSL Logs

CORE CAPABILITY · 02

Credential exposure, scored and prioritized

Every leaked username / password pair tied to your domain is deduplicated and scored, so your team can focus on the accounts that matter most — not thousands of raw rows.

— **Novelty, risk & reuse scores** — instantly see which credentials are new, high-risk, or reused elsewhere.

— **Own infrastructure vs. third party** — separate internal logins from partner and client-side exposure.

— **Stealer logs & combo lists** — catch malware-harvested credentials, not just old breach dumps.

— **Comparison reports** — benchmark credential exposure across subsidiaries, brands or peers.



Unique credentials | Password reuse | Stealer logs | Combo lists | Domain accounts

CORE CAPABILITY · 03

Real-time darknet chatter monitoring

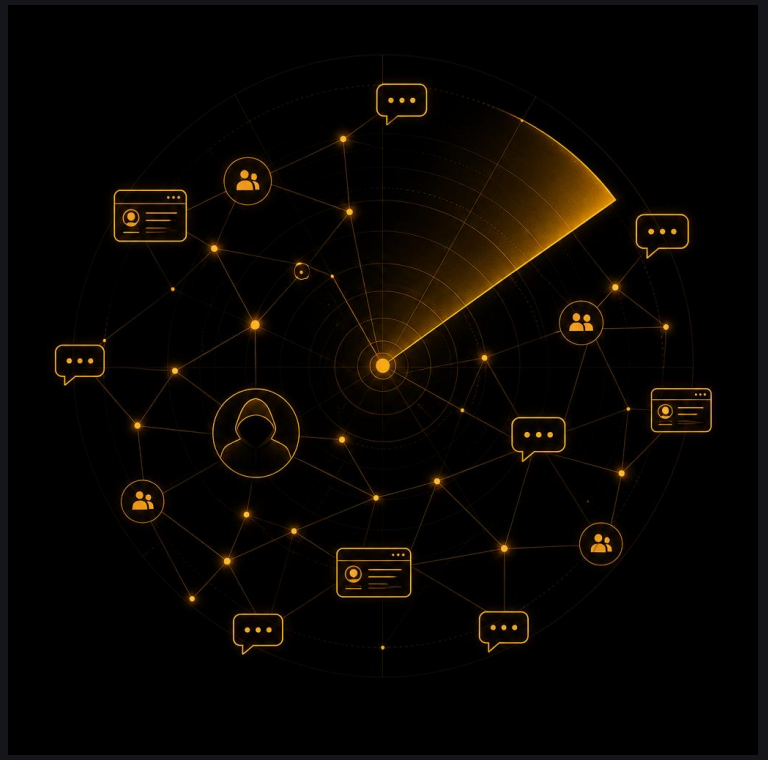
Track cybercrime forum posts, marketplace listings and threat-actor activity the moment they appear — across thousands of Telegram channels, forums and carding sites.

— **2,200+ monitored channels** — Telegram, Discord and dark forums searched with boolean operators.

— **Threat actor tracking** — attribute chatter to known aliases and monitor ransomware groups directly.

— **Categorised results** — marketplaces, leaks & data, carding/fraud, hacking, services, discussion.

— **Live investigations** — query Tor / I2P and closed channels discreetly through our proxy network.



Marketplaces | Leaks & Data | Carding / Fraud | Threat Actors | Live Search

CORE CAPABILITY · 04

Attack surface & code exposure scanning

See your organization the way an attacker does. Discover forgotten assets, risky configurations, and secrets leaked in public code before someone else finds them.

— **Attack Surface Discovery** — automatic visibility into internet-facing hosts, CVEs and open ports.

— **Shadow IT detection** — surface assets added by developers, agencies or freelancers you didn't know about.

— **Code Exposure scanning** — keyword scans across GitHub, Gist, GitLab, Postman and Google dorking.

— **Contributor-based scoping** — map an org's public repos and contributors to focus scans precisely.



CVEs | Open Ports | GitHub | Gist | Postman

CORE CAPABILITY · 05

Domain & brand protection

Stop threat actors from spoofing your brand before a phishing site goes live — across lookalike domains, app stores and social platforms.

— **Typo-squatting detection** — daily monitoring of new domain registrations and SSL transparency logs.

— **Visual logo-spoofing analysis** — WHOIS, geolocation, screenshots and web risk score for every domain found.

— **App store & social monitoring** — spoofed apps on iTunes / Google Play and fake brand profiles.

— **Dedicated risk reports** — Domain Spoofing, VIP Executive, Social Media and Application Security reports.



Typo-squatting | SSL Transparency | App Stores | VIP Executive Report

CORE CAPABILITY · 06

Automated alerts & incident response

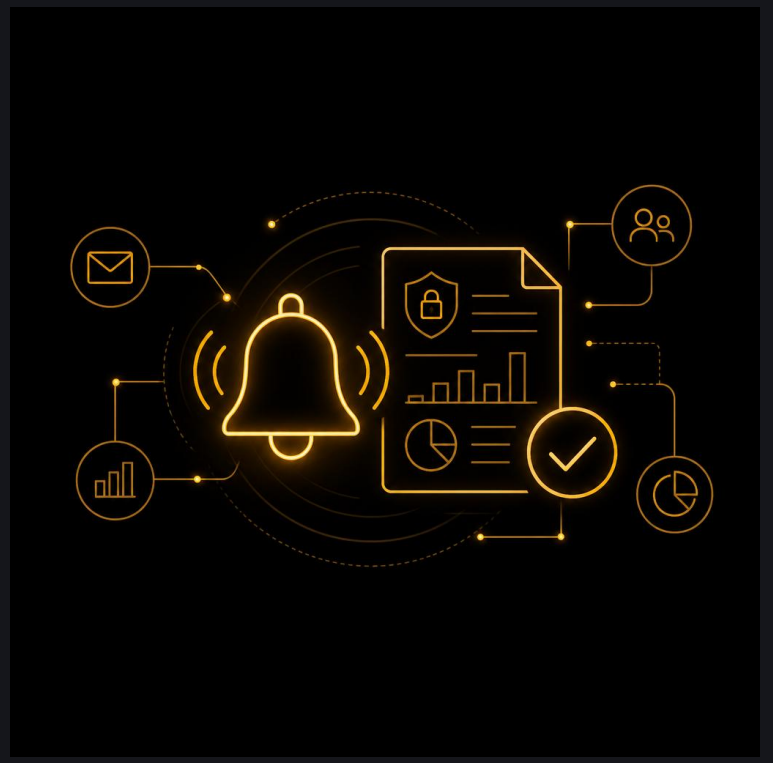
Turn continuous monitoring into action. Create rules once, and get notified the moment something matters — with full context to investigate immediately.

— **Custom alert rules** — build queries against any data source and choose your notification frequency.

— **Incident feed** — every trigger logged with status, source and one-click drill-down into raw data.

— **Extracted entities** — domains, usernames and passwords auto-extracted from every match.

— **Smart exclusions** — silence false positives and recurring matches with reusable exclusion rules.



Alert Rules | Incidents | Exclusions | Webhooks

CORE CAPABILITY · 07

Executive reporting & industry benchmarking

Translate raw threat data into board-ready reports — scheduled automatically or generated on demand, and benchmarked against your industry and competitors.

— **Full assessments** — one-click reports covering breach risk, infrastructure, spoofing and app security.

— **Leaked Credential Comparison Report** — benchmark exposure across divisions, subsidiaries or peers.

— **Scheduled delivery** — recurring reports land in your inbox automatically, no manual work required.

— **Darknet Exposure Report** — a one-time, 24-hour deep dive delivered as PDF + raw CSV data.



Breach Risk | Infrastructure Risk | Domain Spoofing | VIP Executive | Scheduled Reports

BUILT FOR YOUR TEAM

Targeted insights for every role in cybersecurity

CISOs

Strategic visibility & risk prioritization

Continuous visibility into leaked credentials, exposed access and third-party breaches — translated into clear, board-ready insights for governance and compliance.

Threat Intelligence Analysts

Detect, correlate, contextualize

Unify dark web search, stolen-data monitoring, stealer-log analysis and threat-actor profiling in a single workflow to validate emerging threats earlier.

SOC Analysts

Faster, more accurate response

Enrich SIEM and incident investigations with external dark web signals to confirm incidents faster, cut false positives, and reduce mean time to respond.

ENTERPRISE & MSSP READY

Built to scale across teams, brands and clients

Manage every subsidiary, brand or client from a single account — with granular roles, usage visibility and full API access for automation.

— **Multi-tenant organization management —** switch between client accounts instantly

— **Role-based access control with 2FA —** System Admins, Org Users and more

— **Usage dashboards —** track quota by service (searches, alerts, reports, API calls)

— **Full REST API —** push alerts and leak data directly into your SIEM or SOAR



WHY CLIENTS TRUST US

Trusted by security teams across industries

"

Uses DarknetSearch to detect client data leaks, exposed assets and domain spoofing in real time. Alerts and API reporting help their SOC respond faster.

Cloud y Olé

Managed Security Provider

"

Detects leaked credentials and breaches across the dark web, feeding alerts straight into their SIEM to proactively rotate credentials at enterprise scale.

Bühler

Global Industrial Manufacturer

"

Monitors the dark web for leaks and exposed data affecting the NGOs they support — valued for ease of use and relevance of intelligence despite limited resources.

CyberPeace Institute

Swiss Cybersecurity NGO

Rated on G2 · g2.com/products/kaduu/reviews

GETTING STARTED

See your exposure. Start today.

7-Day Free Trial

Explore the full DarknetSearch platform — no commitment, no credit card.

START FREE TRIAL

Darknet Exposure Report

One-time deep dive: exposed credentials, leak trends, risky users and spoofed domains. Delivered as PDF + CSV within 24 hours.

REQUEST YOUR REPORT

Tailored Quote

Get enterprise or MSSP pricing scoped to your organization's size and risk profile.

REQUEST A QUOTE



Let's find what's already exposed.

Thank you — we look forward to showing your organization's live risk score.

---

darknetsearch.com

Kaduu AG · Switzerland

