THREAT INTELLIGENCE SUR LE DARK WEB

DarknetSearch

by Kaduu AG

Surveillance continue du dark web, du deep web et du web ouvert pour détecter
fuites, actifs exposés et usurpations avant que les attaquants ne les exploitent.

PRÉSENTATION CLIENT · DÉMONSTRATION DU PRODUIT



darknetsearch.com

PROGRAMME

Ce que nous verrons

1 **Le défi**

Pourquoi l'exposition sur le dark web est un risque croissant pour toute organisation

2 **Aperçu de la plateforme**

Un tableau de bord pour une visibilité continue sur les menaces

3 **Fonctionnalités clés**

Recherche, exposition des identifiants, discussions du darknet, surface d'attaque, protection de la marque

4 **Alertes et rapports**

Surveillance automatisée, incidents et rapports de direction

5 **Conçu pour votre équipe**

Cas d'usage pour RSSI, analystes threat intelligence, SOC et MSSP

6 **Pour démarrer**

Essai gratuit, rapport sur le darknet et prochaines étapes

LE DÉFI

Vos données sont déjà échangées là où vous ne les voyez pas

Identifiants volés, logs de malwares et domaines similaires circulent sur les places de marché du dark web, les canaux Telegram, les sites de paste et les forums criminels, bien avant d'apparaître dans un gros titre sur une fuite de données.

24/7

Surveillance continue de sources du dark web, du deep web et du web ouvert

2 200+

Canaux Telegram et forums cybercriminels suivis

10+

Facteurs de risque évalués par organisation, automatiquement

24 h

Délai pour un rapport complet d'exposition sur le darknet

PRÉSENTATION DE DARKNETSEARCH

Une plateforme pour la visibilité sur les menaces externes.

DarknetSearch analyse en continu le dark web, le deep web et le web ouvert : vous savez toujours quand vos identifiants, votre infrastructure ou votre marque sont exposés, et pouvez agir avant les attaquants.

01

Détection des fuites

Identifiez en temps réel identifiants volés, appareils compromis et expositions de la chaîne d'approvisionnement.

02

Découverte de la surface d'attaque

Voyez votre réseau comme le voit un attaquant : CVE, ports ouverts et shadow IT.

03

Protection des domaines et de la marque

Bloquez le phishing et le typosquatting avant la mise en ligne des domaines similaires.

LA PLATEFORME EN BREF

Votre score de risque, dans un seul tableau de bord

Chaque organisation obtient un score de risque global en direct, calculé à partir de l'historique des fuites, de l'hygiène des identifiants, des ports exposés et de l'exposition dans les moteurs de recherche, avec une chronologie sur 12 mois pour suivre les progrès.

— **Score de risque global** : une note unique de 0 à 100, comparée à votre secteur et à vos concurrents.

— **Principaux facteurs de risque** : fuites récentes et anciennes, mots de passe faibles, ports ouverts inhabituels, exposition dans les moteurs de recherche.

— **Chronologie du risque** : suivez l'évolution du risque de votre organisation et de votre infrastructure sur l'année écoulée.

— **Statistiques sur les identifiants et utilisateurs divulgués** : total des enregistrements divulgués, stealer logs, combo lists et utilisateurs les plus à risque.



Score de risque | Comparaison | Chronologie des tendances | Statistiques d'identifiants

FONCTIONNALITÉ CLÉ · 01

Recherchez dans le dark web et le deep web en quelques secondes

Quick search interroge toutes les sources de données à la fois ; Expert search permet aux analystes de formuler des requêtes booléennes précises sur une source donnée, idéal pour la première réponse comme pour l'investigation approfondie.

— **Recherche sur tout** : domaine, e-mail, nom, IP, marque, mot de passe, nom de fichier ou nom d'hôte.

— **14 sources spécialisées** : fuites brutes, identifiants filtrés et bruts, Telegram, Discord, pastes et plus encore.

— **Générateur de requêtes personnalisé** : combinez les opérateurs AND / OR / NOT, plages de dates et types de fichiers pour plus de précision.

— **Résultats instantanés et dédupliqués** : identifiants, brokers, pastes et cas de phishing classés par pertinence.



Fuites brutes | Telegram | Discord | Data brokers | Logs SSL

FONCTIONNALITÉ CLÉ · 02

Exposition des identifiants, évaluée et priorisée

Chaque paire nom d'utilisateur / mot de passe divulguée et liée à votre domaine est dédupliquée et évaluée : votre équipe se concentre sur les comptes les plus importants, pas sur des milliers de lignes brutes.

— **Scores de nouveauté, de risque et de réutilisation** : repérez d'un coup d'œil les identifiants nouveaux, à haut risque ou réutilisés ailleurs.

— **Infrastructure propre ou tiers** : distinguez les connexions internes de l'exposition des partenaires et des clients.

— **Stealer logs et combo lists** : détectez les identifiants récoltés par des malwares, pas seulement les anciennes fuites.

— **Rapports comparatifs** : comparez l'exposition des identifiants entre filiales, marques ou pairs.



Identifiants uniques | Réutilisation de mots de passe | Stealer logs | Combo lists | Comptes de domaine

FONCTION CLÉ · 03

Surveillance en temps réel des discussions du darknet

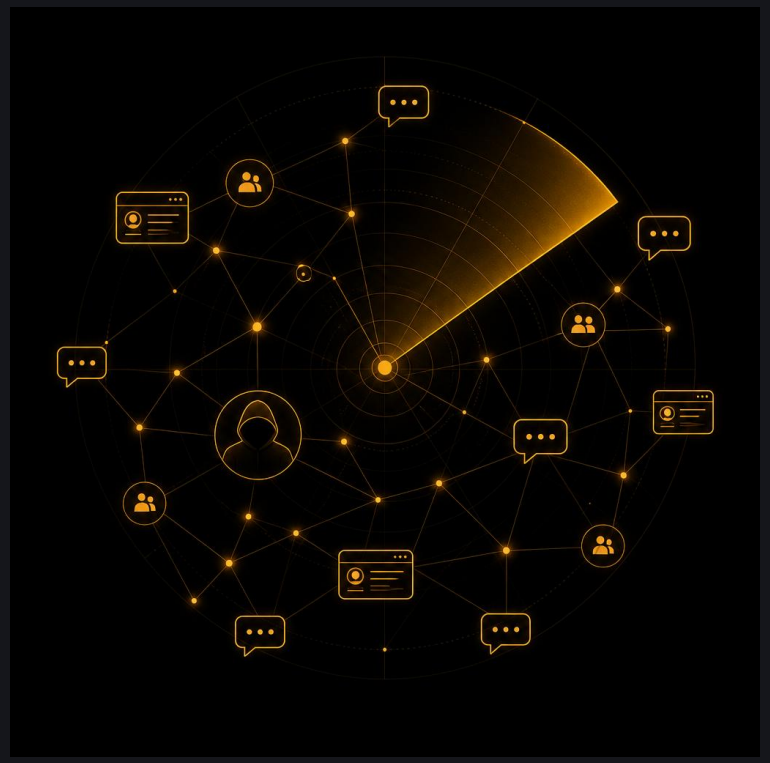
Suivez les publications des forums de cybercriminalité, les annonces des places de marché et l'activité des acteurs de la menace dès leur apparition, sur des milliers de canaux Telegram, forums et sites de carding.

— **Plus de 2 200 canaux surveillés** – Telegram, Discord et forums du dark web, interrogés avec des opérateurs booléens.

— **Suivi des acteurs de la menace** – attribuez les discussions à des alias connus et surveillez directement les groupes de ransomware.

— **Résultats catégorisés** – places de marché, fuites et données, carding/fraude, piratage, services, discussions.

— **Investigations en direct** – interrogez Tor / I2P et les canaux fermés en toute discrétion via notre réseau de proxys.



Places de marché | Fuites et données | Carding / Fraude | Acteurs de la menace | Recherche en direct

FONCTION CLÉ · 04

Analyse de la surface d’attaque et de l’exposition du code

Voyez votre organisation comme la voit un attaquant. Découvrez les actifs oubliés, les configurations à risque et les secrets divulgués dans du code public avant que d’autres ne les trouvent.

— **Attack Surface Discovery** – visibilité automatique sur les hôtes exposés à Internet, les CVE et les ports ouverts.

— **Détection du shadow IT** – repérez les actifs ajoutés par des développeurs, agences ou freelances dont vous ignoriez l’existence.

— **Analyse de l’exposition du code** – recherches par mots-clés sur GitHub, Gist, GitLab, Postman et par Google dorking.

— **Ciblage par contributeurs** – cartographiez les dépôts publics et les contributeurs d’une organisation pour cibler précisément les analyses.



CVE | Ports ouverts | GitHub | Gist | Postman

FONCTION CLÉ · 05

Protection des domaines et de la marque

Empêchez les acteurs de la menace d'usurper votre marque avant la mise en ligne d'un site de phishing, sur les domaines similaires, les boutiques d'applications et les réseaux sociaux.

— **Détection du typosquatting** – surveillance quotidienne des nouveaux enregistrements de domaines et des journaux de transparence SSL.

— **Analyse visuelle des logos usurpés** – WHOIS, géolocalisation, captures d'écran et score de risque web pour chaque domaine trouvé.

— **Surveillance des boutiques d'applications et des réseaux sociaux** – applis usurpées sur iTunes / Google Play et faux profils de marque.

— **Rapports de risque dédiés** – rapports Domain Spoofing, VIP Executive, Social Media et Application Security.



Typosquatting | Transparence SSL | Boutiques d'applis | Rapport VIP Executive

FONCTION CLÉ · 06

Alertes automatisées et réponse aux incidents

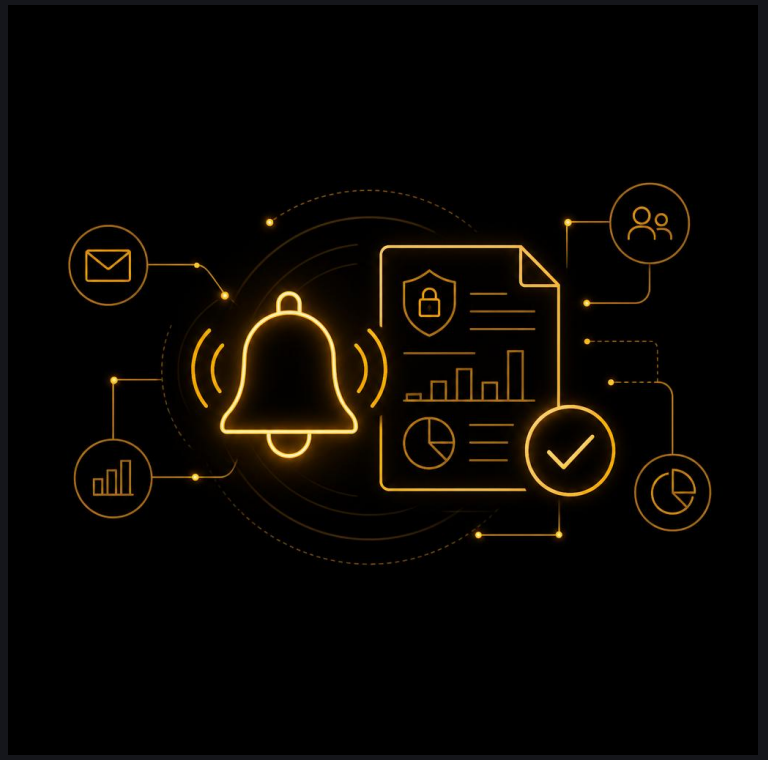
Transformez la surveillance continue en action. Créez des règles une fois et soyez averti dès que quelque chose compte, avec tout le contexte pour enquêter immédiatement.

— **Règles d'alerte personnalisées** – créez des requêtes sur n'importe quelle source de données et choisissez la fréquence des notifications.

— **Flux d'incidents** – chaque déclenchement est consigné avec statut, source et accès en un clic aux Raw Data.

— **Entités extraites** – domaines, noms d'utilisateur et mots de passe extraits automatiquement de chaque correspondance.

— **Exclusions intelligentes** – réduisez au silence les faux positifs et les correspondances récurrentes grâce à des règles d'exclusion réutilisables.



Règles d'alerte | Incidents | Exclusions | Webhooks

FONCTION CLÉ · 07

Rapports de direction et benchmarking sectoriel

Transformez les données brutes sur les menaces en rapports prêts pour le conseil d'administration, planifiés automatiquement ou générés à la demande, et comparés à votre secteur et à vos concurrents.

— **Évaluations complètes** – rapports en un clic couvrant le risque de fuite, l'infrastructure, l'usurpation et la sécurité des applications.

— **Rapport comparatif des identifiants divulgués** – comparez l'exposition entre divisions, filiales ou pairs.

— **Envoi planifié** – les rapports récurrents arrivent automatiquement dans votre boîte de réception, sans travail manuel.

— **Darknet Exposure Report** – une analyse approfondie ponctuelle de 24 heures, livrée en PDF + données CSV brutes.



Risque de fuite | Risque d'infrastructure | Domain Spoofing | VIP Executive | Rapports planifiés

CONÇU POUR VOTRE ÉQUIPE

Des analyses ciblées pour chaque rôle en cybersécurité

RSSI

Visibilité stratégique et priorisation des risques

Visibilité continue sur les identifiants divulgués, les accès exposés et les fuites chez des tiers, traduite en analyses claires, prêtes pour le conseil d'administration, pour la gouvernance et la conformité.

Analystes threat intelligence

Détecter, corréler, contextualiser

Réunissez recherche sur le dark web, surveillance des données volées, analyse des stealer logs et profilage des acteurs de la menace dans un seul flux de travail pour valider plus tôt les menaces émergentes.

Analystes SOC

Une réponse plus rapide et plus précise

Enrichissez le SIEM et les investigations d'incidents avec des signaux externes du dark web pour confirmer les incidents plus vite, réduire les faux positifs et raccourcir le délai moyen de réponse.

PRÊT POUR LES ENTREPRISES ET LES MSSP

Conçu pour passer à l'échelle entre équipes, marques et clients

Gérez chaque filiale, marque ou client depuis un seul compte – avec des rôles granulaires, la visibilité sur l'usage et un accès complet à l'API pour l'automatisation.

— **Gestion d'organisations multi-tenant –** passez d'un compte client à l'autre instantanément

— **Contrôle d'accès basé sur les rôles avec 2FA –** administrateurs système, utilisateurs d'organisation et plus

— **Tableaux de bord d'usage –** suivez le quota par service (recherches, alertes, rapports, appels API)

— **REST API complète —** envoyez alertes et données de fuite directement dans votre SIEM ou SOAR



POURQUOI NOS CLIENTS NOUS FONT CONFIANCE

La confiance d'équipes de sécurité de tous secteurs

"

Utilise DarknetSearch pour détecter en temps réel les fuites de données de ses clients, les actifs exposés et l'usurpation de domaine. Les alertes et le reporting par API aident son SOC à réagir plus vite.

Cloud y Olé

Fournisseur de sécurité managée

"

Détecte les identifiants divulgués et les fuites de données sur le dark web et envoie les alertes directement dans son SIEM pour renouveler les identifiants de manière proactive à l'échelle de l'entreprise.

Bühler

Fabricant industriel mondial

"

Surveille le dark web pour détecter les fuites et les données exposées touchant les ONG qu'il soutient – apprécié pour sa facilité d'utilisation et la pertinence des renseignements malgré des ressources limitées.

CyberPeace Institute

ONG suisse de cybersécurité

Évalué sur G2 · g2.com/products/kaduu/reviews

PREMIERS PAS

Voyez votre exposition. Commencez aujourd'hui.

Essai gratuit de 7 jours

Explorez toute la plateforme DarknetSearch – sans engagement, sans carte bancaire.

DÉMARRER L'ESSAI GRATUIT

Darknet Exposure Report

Analyse approfondie unique : identifiants exposés, tendances des fuites, utilisateurs à risque et domaines usurpés. Livrée en PDF + CSV sous 24 heures.

COMMANDER LE RAPPORT

Devis sur mesure

Obtenez une offre entreprise ou MSSP adaptée à la taille et au profil de risque de votre organisation.

DEMANDER UN DEVIS



Trouvons ce qui est déjà exposé.

Merci – nous avons hâte de vous montrer le score de risque en direct de votre organisation.

---

darknetsearch.com

Kaduu AG · Suisse

