KADUU

THE DARK WEB OWNS YOUR CLIENTS’ DATA

Despite applying the best IT defense techniques, your clients’ data (passwords, accounts, credit cards, internal documents, codes, etc.) will inevitably appear on the Dark Net. The question is, “**How much data?**” Kaduu, a SaaS solution for Service Providers, will give you the answer to this question and more.

WHAT WE WILL MONITOR IN KADUU:

Kaduu helps you investigate when, where and how stolen or accidentally leaked information is exposed on Dark Web markets, forums, botnet logs, IRC, social media and other sources. Go Live to receive instant access to realtime custom reporting tailored to meet your client-servicing needs

- ☑ **Infrastructure exposure: IOT, Git, AWS, Bitbucket & more**
- ☑ **People exposure: Social Media Monitoring**
- ☑ **Ransomware exposure: Leak & Credential Monitoring**
- ☑ **Attack prevention: Domain & Certificate Monitoring**

GROW YOUR BUSINESS

Cybersecurity is the fastest growing IT Services sector. Kaduu offers a way to expand your business with all your clients. You can show your customers the consequences of poor security infrastructure and “click-happy” staff.

TELLING ISN’T SELLING!

Telling someone they are at risk of a Ransomware or Email Compromise Attack is one thing, but showing them will grow your sales exponentially! Use Kaduu to show your current and prospective clients the risks they face in real time.

Accelerate sales conversion rates and initiate new customer conversations on Cybersecurity with Kaduu.

OPTIMIZED FOR MANAGED SERVICE PROVIDERS

☑ NO LONG-TERM COMMITMENTS. NO RENEWAL LOCK-IN

Kaduu’s SaaS platform can be licensed for one-time access to analyze Dark Net exposure or as a subscription Cybersecurity Risk Monitoring tool. The latter option provides 24/7 monitoring and sends immediate alerts to you and your clients when data leakage or a Cyberthreat is detected.

☑ FLEXIBLE DATA SEARCH CRITERIA

Performing a data search in Kaduu doesn’t require any registration or validation.

☑ HIGH MARGINS AND LOW, FLEXIBLE PRICING

Fixed, aggressive, per-client pricing, regardless of the client’s size, allows for higher margins, plus the possibility to reach under-served markets usually excluded by the more expensive but lower quality solutions. Choose between Pay-As-You-Go pricing, custom packages and fixed “all-you-can-eat” annual subscriptions, paid monthly or up-front. Choose the option that fits your budget and needs

☑ NO-RISK ROLL-OVER

If a client’s budget is paused, or they have a couple of months down time at the year’s end, the unexpired license can be rolled over to the following year at no additional cost.

☑ QUICK SETUP

No installation. No agents. Just Real-Time, Actionable Intel.

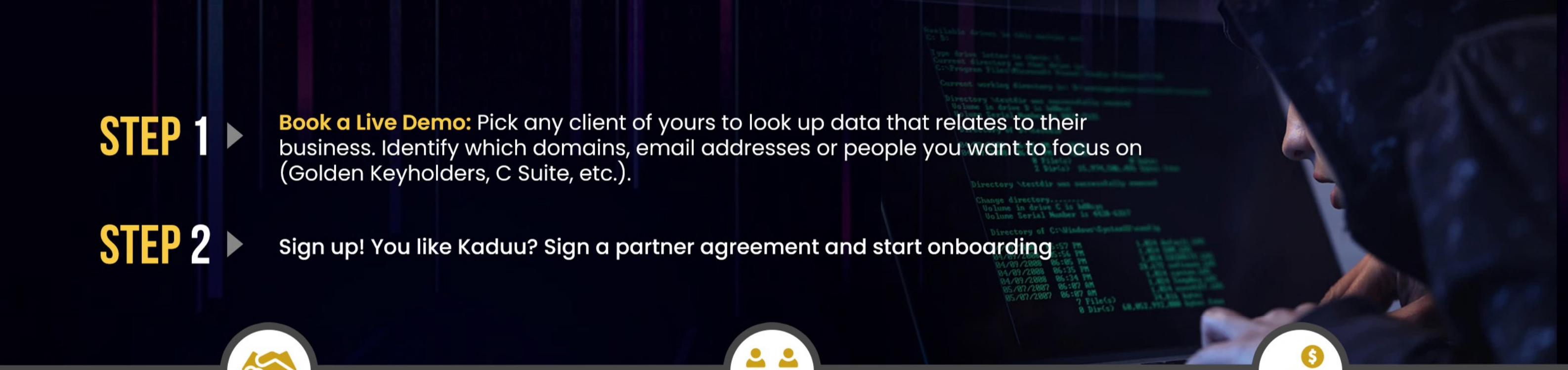
☑ KNOW-HOW TRANSFER

Not sure what to query and how to interpret the data? No worries! Kaduu’s experienced Penetration Testers and White Hat hackers will train and support you. Created by security experts for security experts. Because you have better things to do than chase red herrings, go down rabbit holes and uncover phantom threats.

Contact us ▸

@CtiKaduu
www.kaduu.io

Europe (Switzerland) ▸	switzerland@kaduu.io	+41 79 6959510
USA ▸	usa@kaduu.io	+1 512 696 1498



STEP 1 **Book a Live Demo:** Pick any client of yours to look up data that relates to their business. Identify which domains, email addresses or people you want to focus on (Golden Keyholders, C Suite, etc.).

STEP 2 Sign up! You like Kaduu? Sign a partner agreement and start onboarding

PARTNER ONBOARDING

After your free registration with Kaduu, we will give your team a short introduction to the tool and show you how to retrieve data from the different sources and filter it for relevant risks

CLIENT ONBOARDING

For your first project, our team will provide support in creating the correct search queries and evaluations. You will also have the opportunity to create your own client sub-accounts on Kaduu.

PAY-AS-YOU-GO OR FIXED BUDGET – HOW DO YOU WANT TO PAY?

Pay when you have signed up your first client. There is no high up-front investment to make

WHAT RISKS CAN BE MITIGATED **WITH KADUU?**

✓ PREVENT PHISHING

Via Kaduu, we monitor all new domain registrations (ccTLDs, gTLDs, uTLD, sTLD). In doing so, we also record typical typosquatting techniques. Kaduu automatically analyzes domains that appear suspicious, capturing key properties such as WHOIS, geolocation, open web services, screenshots, similarity to the original site (AI analysis), etc. Our certificate log monitoring service will allow you to detect scammers that are using the same name on an SSL certificate as your protected asset.

✓ DETECT EXPOSED INFRASTRUCTURE

Kaduu monitors server access, IOT (Shodan) or complete DB dumps in different formats (CSV, Memory Dumps, Office Files, etc). Additionally, we regularly examine the S3 buckets for sensitive data. Kaduu also provides a search option to query regularly updated botnet logs for domain names, brands or IP addresses, a useful feature because malicious actors have built vast networks of hacked computers that can be rented or purchased and used for cyberattacks such as distributed denial of service, fraud, spam or phishing.

✓ DETECT LEAKS FROM RANSOMWARE

In ransomware attacks, victims are blackmailed into paying a ransom in order to regain access to their own data. In some cases, ransoms are left unpaid, or, despite payment, the stolen data is uploaded to the Internet or Dark Net for every interested user to see. We monitor common ransomware groups and can inform the customer for publicly shared stolen data.

✓ FIND EXPOSED DATA IN THE DARKNET

Monitoring whether your organisation's name appears in Dark Web forums, Onion-, I2P and paste sites can help you detect potential insider threats, enabling you to prevent data leaks and other incidents that may damage your organisation. Access to leacked accounts and passwords is also a popular darknet commodity. Passwords are valuable because attackers know that people tend to reuse their passwords for multiple accounts.

✓ FIND EXPOSED DATA ON THE DARK NET

Monitoring whether an organization's name appears in Dark Web forums, Onion-, I2P and paste sites can help you detect potential insider threats, enabling you to prevent data leaks and other incidents that may damage the organization. Access to leaked accounts and passwords is also a popular Dark Net commodity. Passwords are valuable because attackers know that people tend to reuse them for multiple accounts

✓ DETECT SPOOFING AND IMPERSONATION

Kaduu monitors social media services such as Twitter, Reddit, Youtube, Telegram, etc. for posts that could be damaging to a client's reputation. We also detect attempts to create fake user profiles of key executives. Especially in the case of phishing and spoofing attacks, in which a false identity is simulated, detection should happen in the preparation phase.

✓ UNDERSTAND EMPLOYEE EXPOSURE

Employees who are heavily exposed to the Internet are at greater risk of getting targeted for social engineering attacks such as phishing. Kaduu can be used to measure an employee's Internet exposure and identify possible warning signs of activities related to the specific email account.

✓ DETECT STOLEN DATA

In Kaduu, we offer the possibility to monitor the Dark Net for specific credit card information (cardholder's name, part of the number, etc.). If such data is offered for sale on relevant forums as part of a phishing or malware attack, we can inform the card owner promptly

✓ AND MANY MORE RISK INDICATORS

Kaduu is in continuous development, and we see ourselves as a one-stop-shop for various cyberthreat intelligence indicators. We will be happy to conduct a meeting to show you a detailed list of all the data sources we monitor and the features we are developing.

Contact us

@CtiKaduu
www.kaduu.io

Europe (Switzerland)	switzerland@kaduu.io	+41 79 6959510
USA	usa@kaduu.io	+1 512 696 1498