

## IS YOUR CLIENTS DATA IN THE DARK WEB?

Despite good technical protection measures, it frequently happens that **your customers data (accounts, credit cards, internal documents, etc.) may turn up on the darknet**. However, it is generally not known how much data has been leaked. With our solution, which is explicitly aimed at Service providers, we can answer this question.

### WHAT DO WE MONITOR IN KADUU?

Kaduu helps you understand when, where and how stolen or accidentally leaked information in dark web markets, forums, botnet logs, IRC, social media and other sources is exposed. Setup in minutes you will receive instant access to real-time reporting including:

- ✓ Infrastructure exposure: IOT, Git, AWS, Bitbucket & more
- ✓ People exposure: Social media monitoring
- ✓ Ransomware exposure: leak & credential monitoring
- ✓ Attack prevention: domain and certificate monitoring

### GROW YOUR BUSINESS

Cybersecurity is an important topic for CEOs and CISOs. But it is also an issue for every customer in every industry. Kaduu can be used as an entry-level tool for selling cybersecurity: You can give customers a live demonstration of the consequences of a lack of security infrastructure or security awareness. Telling organizations that they are at risk of having their credentials compromised is one thing, but if you can show that, then that has a different impact! Use Kaduu to show customers and prospects their risk in real time. This leads to quick sales and serves as a starting point for many other discussions on security topics with your customers.

### OPTIMIZED FOR MANAGED SERVICE PROVIDERS

- ✓ **No need for long commitments:** Our SaaS platform can be booked as a one-time access to analyze the exposure in the darknet or as a permanent dark web monitoring tool, which alerts the customer immediately in case of a data leakage.
- ✓ **Flexible clients data search:** Use any search term in Kaduu provided by your clients without any complicated registration and validation process
- ✓ **Flexible pricing:** Fixed, very favorable prices that are not dependent on the size of the company mean higher margins, but also the possibility to serve markets that do not have access to it due to the usually elevated prices. We offer Pay-As-You-Go models or as an alternative we can create a package at a fixed price for one year in advance - with the according discounts. You have no risk: If the planned budget is not used up, the license can be transferred in the following year without additional costs.
- ✓ **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! We assist you in the setup and analysis of the data. From security experts for security experts: Our experienced penetration testers and former hackers are at your disposal. Because you have better things to do than follow red herrings, go down rabbit holes and chase phantom threats.

### NEXT STEPS

**Step 1:** Book A live Demo: Pick any client of yours to see data that relates to your business. Identify which domains, email addresses or people you want to focus on (Golden Keyholders, C Suite, etc)

**Step 2:** Sign up with us! You like Kaduu? Sign up a partner contract and start onboarding:



#### Partner onboarding

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



#### Client Onboarding

For your first project, our team will again support you in creating the correct search queries and evaluations. If required, you can also create your own accounts on Kaduu for your clients.



#### Pay-as-you-go or fixed budget in advance

Payment can be made only after successful completion of the project: There are no financial risks for our partners due to high upfront investments.

## WHAT RISKS CAN BE MITIGATED WITH KADUU?

### **Prevent phishing**

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. With our certificate log monitoring service you will also detect scammers using the same name on a SSL certificate as your protected asset.

### **Detect exposed infrastructure**

We monitor server access, IOT (Shodan) or complete DB dumps in different formats (CSV, Memory Dumps, Office Files etc). We regularly also examine also S3 buckets for sensitive data. Kaduu also provides a search option to query regularly updated botnet logs for domain names, brands or IP addresses as 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 sum in order to regain access to their own data. In some cases, ransoms are not paid or, despite payment of ransom, the stolen data is uploaded to the Internet or darknet for every user to see. We monitor common ransomware groups and can inform the customer if stolen data is shared with the public.

### **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 leaked 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.

### **Detect spoofing and impersonation**

We monitor social media services such as Twitter, Reddit, Youtube, Telegram, etc. for posts that could be damaging to our 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, such attacks should already be detected in the preparation phase.

### **Understand employee exposure**

Employees who are heavily exposed to the Internet are at greater risk of social engineering attacks such as phishing. Therefore, in Kaduu we measure how exposed an employee is on the Internet and where indications of activities related to the specific email account can be found.

### **Detect stolen data**

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

### **And many more risk indicators**

Kaduu is constantly under development and we see ourselves as a one-stop-shop for various cyber threat intelligence indicators. We will be happy to show you a detailed list of all the data sources we monitor and are still developing in a personal meeting.

## Contact us

Europe (Switzerland)

[switzerland@kaduu.io](mailto:switzerland@kaduu.io)

+41 79 6959510

USA

[usa@kaduu.io](mailto:usa@kaduu.io)

512 696 1498

Website: <https://kaduu.io> | Twitter: <https://twitter.com/CtiKaduu>