4iQ IDLake™

DELVE DEEP™

The traditional approach to building a virtual wall to protect data cannot be counted on.
That's why hundreds of "secure" networks are compromised every day.
By going where hackers buy, sell, trade and dump data,
4iQ provides a layer of protection never before available.

4iQ continuously scans deep and dark web sources for stolen, leaked or lost login credentials and other personal identifiable information (PII). With **team and technology,** 4iQ indexes billions of identity records exposed in hacked and dumped breach corpuses across the world.

As breach hunting pioneers, the 4iQ intelligence team has spent over eight years developing tools and techniques to both automatically and continuously crawl and manually access:

- **Very restricted forums.** These can be joined after a vetting process or by special invitation. These forums are transient - they often close, reopen, disappear and are re-constituted. Some are global while others are regional, using a specific language and local slang.
- **Semi-restricted forums**. These are also transient and found both in Tor networks and the surface web.
- **Tor and I2P networks**. The Tor Network fluctuates between 25k-60k sites, many of which come and go.
- **Dumped/leaked text -> file storage sites** (e.g. Pastebins).
- **P2P networks** containing millions of live torrents or files.
- **Surface web directories** leaking identity data.

4iQ automatically scans open and exposed data repositories daily:

- Open **MongoDB** with no authentication or access controls.
- Live **Cloud Sharing** sites like Mega, Google Drive.

98+Billion
Breach Attributes

11+Billion
Curated Records

4.6Billion
Validated Passwords

16Million
Malicious Actors

54,000+
Breaches

24x7Service

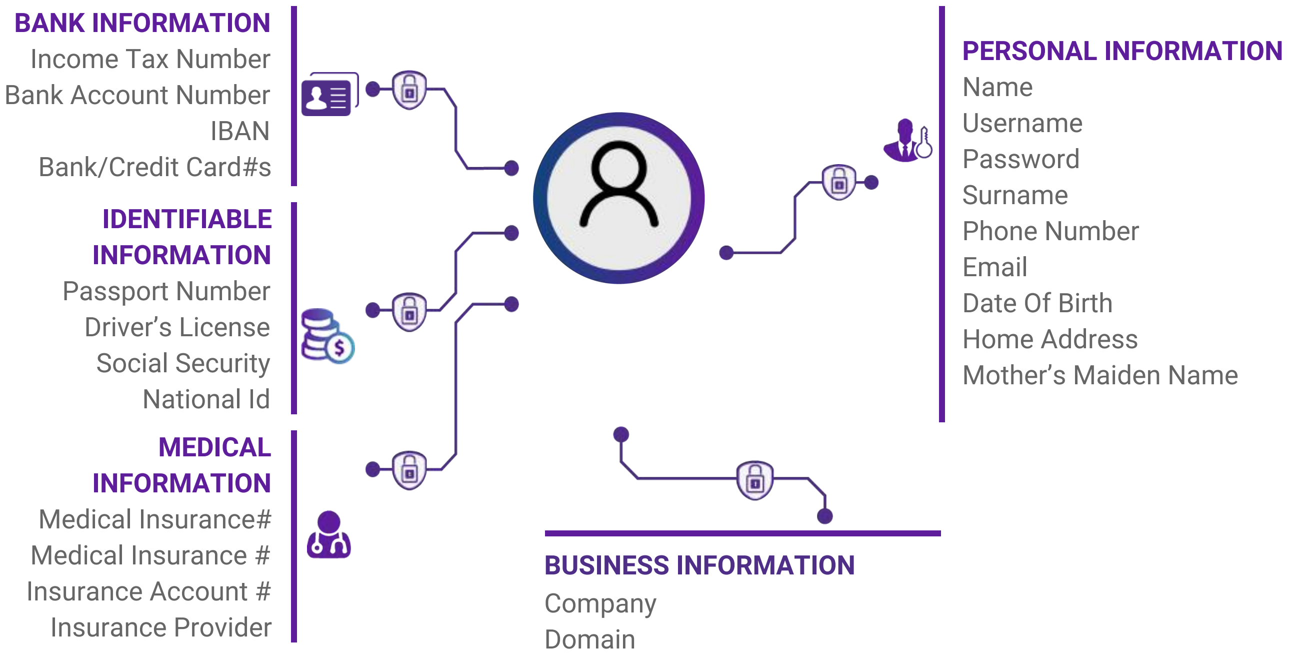
The 4iQ breach team also monitors hundreds of actors on **Twitter, Discord, Live Torrents,** and other **social media, chat rooms / (IRC / Jabber)** who are actively engaged in chatter about breaches and exposed PII.

Finally, a significant portion of data is provided by private sources or from breaches and leaks not commonly known or available from any other vendors or underground forums, discovered for the first time by the 4iQ breach hunting team, or shared by underground actors to only 4iQ. 4iQ does not buy data.

As a result, 4iQ has built the world's largest and most accurate datalake of exposed identities - the **4iQ IDLake™** - that includes cryptocurrency wallets and addresses, IP addresses, phone numbers, passwords, credit card numbers, csvs, social security numbers, birthdays, drivers licenses and other identity attributes.

MOST ATTRIBUTES TRACKED

Personal Data Attributes



BANK INFORMATION
Income Tax Number
Bank Account Number
IBAN
Bank/Credit Card#s

IDENTIFIABLE INFORMATION
Passport Number
Driver's License
Social Security
National Id

MEDICAL INFORMATION
Medical Insurance#
Medical Insurance #
Insurance Account #
Insurance Provider

PERSONAL INFORMATION
Name
Username
Password
Surname
Phone Number
Email
Date Of Birth
Home Address
Mother's Maiden Name

BUSINESS INFORMATION
Company
Domain

MOST ACCURATE DATA.
STRONG VERIFICATION METHODOLOGY.

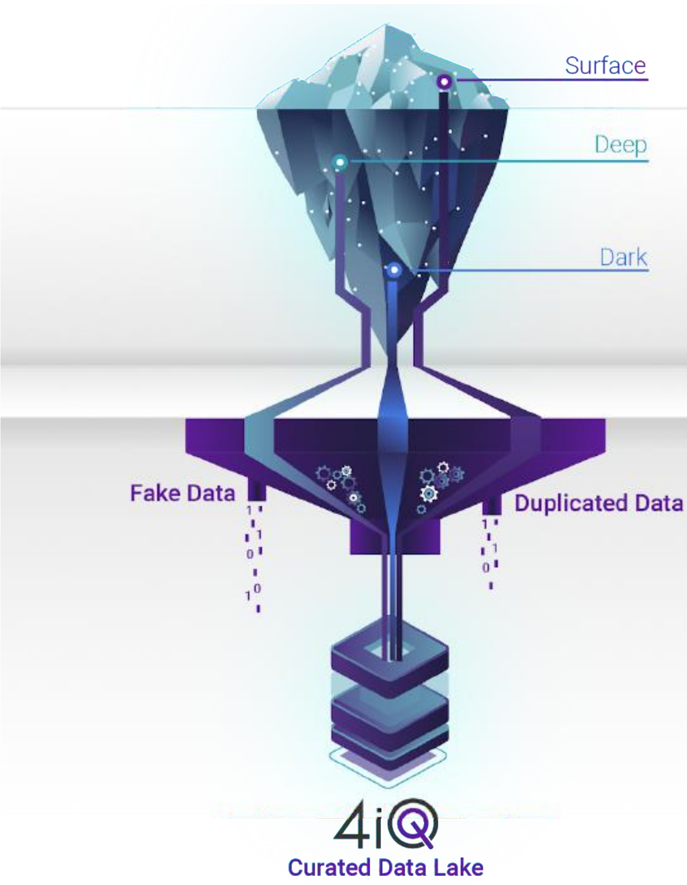
While the number of accumulated raw identity records provides insight into the sheer volume of data points out there, it is not the best indicator of overall risk. This is because not all of the data gathered is authentic or unique.

Circulating in the Darknet and mixed in with authentic breach corpuses, are fake breaches and “combo-lists” or mashups of different breach packages.

In addition, **attribution** is all too often not clear, so it may not be obvious where the data came from and which site was actually breached. Misattribution incidents – like the 2016 event, when a breach attributed to Dropbox was actually from Tumblr - create anxiety for consumers, costly loads on call centers, and potential legal liability for service providers.

The 4iQ breach team has established a strong data verification methodology and curation process and creates accurate, detailed reports that assess the **authenticity, freshness and risk** of every breach or leak.

After we gather the raw data, our next step is to **analyze** the details. 4iQ has machine learning algorithms that quickly identify real, sensitive data, removes duplicate records, and normalize the information for further analysis.



Then, the breaches undergo a **verification process** where our analysts and experts use numerous research and investigation methods to ensure that the domain data and other information are real and valid. Once a breach is verified, the 4iQ platform calculates a **risk score** based on a number of variables such as type of attributes, date, and strength of password.

Find out how 4iQ can strengthen your Intelligence Operations.

Learn: www.4iq.com | Connect: info@4iq.com | Connect: @4iQ