Speed to Results: Discover, Uncover, and Disrupt Adversaries

If you are conducting complex cyber-crime investigations, you know how difficult it can be to identify threat actors due to multiple layers of purposeful misdirection. Pseudo names, anonymity tools, cryptocurrencies, and other evasive tactics make attribution of real identities difficult and time consuming.

4iQ IDHunt™ Core is an easy-to-use SaaS application that enables Intel analysts and investigators to quickly piece together exposed open source data from the **4iQ IDLake™** (a proprietary datalake with 20+ billion identity records from transient, historical and newly surfaced breach corpuses), correlate and enrich findings with **Pastebin documents,** historical **DomainWhoIs data, cryptocurrency addresses, social profiles and standard search engines, reverse IP lookups** and other data sources**.**

4iQ IDHunt™ Core provides context to threat actors, revealing their real identities, cohort and criminal rings. By unmasking cybercriminals attacking your organization, you can take action to **know your adversary and *prevent future attacks*.**

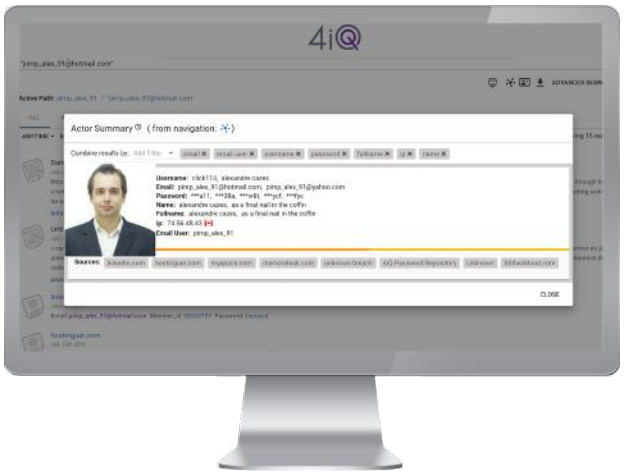
Provide Actionable Intelligence leading to Attribution. How it Works:

1) START YOUR SEARCH

Enter a digital asset (email, moniker) or term into the **IDHunt Core™** search bar. Just like any search engine, all results will be immediately returned with exposed identity attributes (26+ available, such as emails, usernames, passwords, IP addresses, phone numbers, BTC wallets, along with date of breach).

Depending on the use case, filter results by **identity, document leaks, domains, cryptocurrency, or *malicious sites.** *malicious sites are tagged based on the nature of and activity observed on the exposed site.

Exact, partial or "fuzzy" searches allow you to control the types of results returned.



2) PIVOT AND ENRICH TO FIND THE REAL IDENTITY

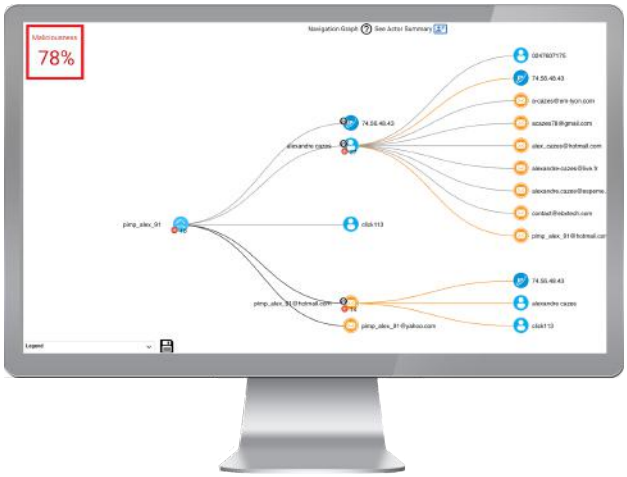
Delve deeper into your results. Simply right click on an attribute to geolocate and enrich findings with results from **standard search engines, Pastebin documents, DomainWhoIs data, social profiles,** and click to **Pipl** and **reverse IP lookups.**

Correlate passwords to reveal additional accounts that may be related. **Investigate domains** to see which breaches they have been exposed in. View identity attributes aggregated and displayed in your Active Path in your investigation. View automatically generated actor profiles containing all attributes associated with the individual.

3) GRAPH RESULTS BY MALICIOUS IDENTITIES OR BREACHES

A single actor analysis can require hundreds of pivots. The application automatically generates very large graphs and a malicious score to help analysts assess profiles in seconds. Simply right click on an email or username to instantly generate graphs.

4iQ IDHunt™ Core provides two types of graphs:

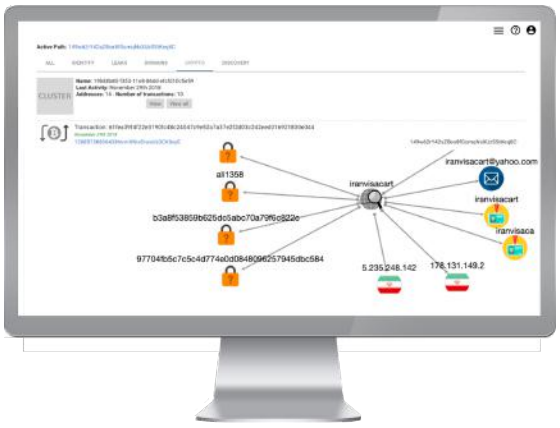


Malicious Graph (with score): provides automatic identity resolution and malicious scoring to help analyze very large graphs in seconds. The malicious score indicates the level of associated malicious activity (e..g hacking, money laundering) along with the confidence level that the associated entity is the same as the entity being investigated.

Identities Graph (with score): provides a view by breach and expands related nodes with a click of a button.

"It took two agents using 4iQ IDHunt™ Core one day to create a usable persona map versus 70 analysts about three months to build a comparable intel package for the same mission."

- Information Security Officer, Intel Agency



4) LINK CRYPTOCURRENCY TO THREAT ACTORS

Link Cryptocurrency addresses and wallets to identity attributes from data breach archived within the 4iQ IDLake™ and then uncover the real identity.

Currently, **4iQ IDHunt™ Core** has data from Bitcoin and Ethereum (including ICO).

Key Features

4iQ IDHunt Core™ enables investigators to analyze personas, enhance attribution analysis, and uncover the real identities behind criminal activities.

Targeted Threat Analysis

Instead of searching for a needle in a haystack, investigators start with what they already know - suspected bad actors - and search the 4iQ IDLake™ to begin making connections.

Accelerate Findings

4iQ has spent years curating and verifying billions of identity records, so that you can more efficiently unmask adversaries -- sometimes within a matter of hours.

AI/ML & Analytics

A single actor analysis can require hundreds of pivots. With 4iQ IDHunt Core™, you can automatically connect the dots, generate graphs and calculate maliciousness scores in seconds.

No Training Required

4iQ IDHunt Core™ application is simple. Using an intuitive interface, Investigators can search and immediately start seeing results with no prior training.

"It took us over 14 months to find this bad actor which with 4iQ iDHunt Core, took only 5 minutes."

- **Fraud Analyst, Top Tier Bank**

USE CASES

4iQ IDHunt™ Core uncovers adversaries and provides actionable intelligence leading to more cases solved efficiently and effectively. The application is easy to use, needs no training, and increases analyst productivity. It enables fraud and financial crime analysts and investigators to deliver timely Suspicious Transaction Reports (STR) and Suspicious Activity Reports (SAR) enriched with exactly the information law enforcement needs to disrupt and deter crime.

Anti-Money Laundering (AML) & Counter Terrorism Financing (CTF): Quickly unmask real identities and networks behind suspicious transactions (including cryptocurrency transactions), significantly reducing financial losses and operating costs.

Fraud: Gather insights and uncover the real identities of criminals stealing funds from your organization and your customers. Disrupt criminal activity and prevent future losses, while reducing the cost and complexity of investigating attacks.

Insider Threats: Identify and investigate suspicious personnel and uncover nefarious activities, including illicit activity and leaked proprietary documents through dark web sales and trades.

Cyber Crime Investigations: Build a persona map on adversaries attacking your organization in a fraction of the time it normally takes, with just one tool and fewer analysts.

There's always a real person behind an attack and organizations need to make a shift to catching the culprit and their cohorts rather than playing the unending game of defensive whack-a-mole. - **CISO, Global Bank**