

# IDLINK API

EMPOWERING ANALYSTS WITH DARKNET INTELLIGENCE  
TO **SPEED UP THREAT ACTOR ATTRIBUTION**

## THE PROBLEM

Valuable OSINT data gives analysts and investigators the ability to follow new threads to identify cybercriminals and disrupt criminal activity. However, with traditional OSINT feeds, investigators face the time-consuming challenge of piecing together fragmented identities from a growing volume of darknet data. Queries often throw false positives with too many identifiers and analysts are left to dig through results and manually clean the data. Chasing connections between data assets and removing irrelevant records slows down response times and complicates the detection of critical relationships between identities.

Give your analysts a shortcut to the answers they seek with identity-centric intelligence from SpyCloud.

## UNDERSTAND THE SCOPE OF AN IDENTITY, FASTER

**SpyCloud's IDLink API** supports querying by emails, usernames, or phone numbers, and then automatically pivots through additional fields to link high confidence assets to an identity, while dropping low confidence ones. IDLink API dramatically shortens the time to uncover linked identities and aggregates comprehensive digital identities, enhancing overall decision-making.

### USE CASES



IDENTITY RESOLUTION



ADVERSARY RESEARCH



VIP EXPOSURE VERIFICATION

### BENEFITS AT A GLANCE

#### ENHANCED RELEVANCY AND PRECISION

Automatically analyze and filter out irrelevant data to only receive the most pertinent information, reducing noise

#### STREAMLINED IDENTITY RESOLUTION

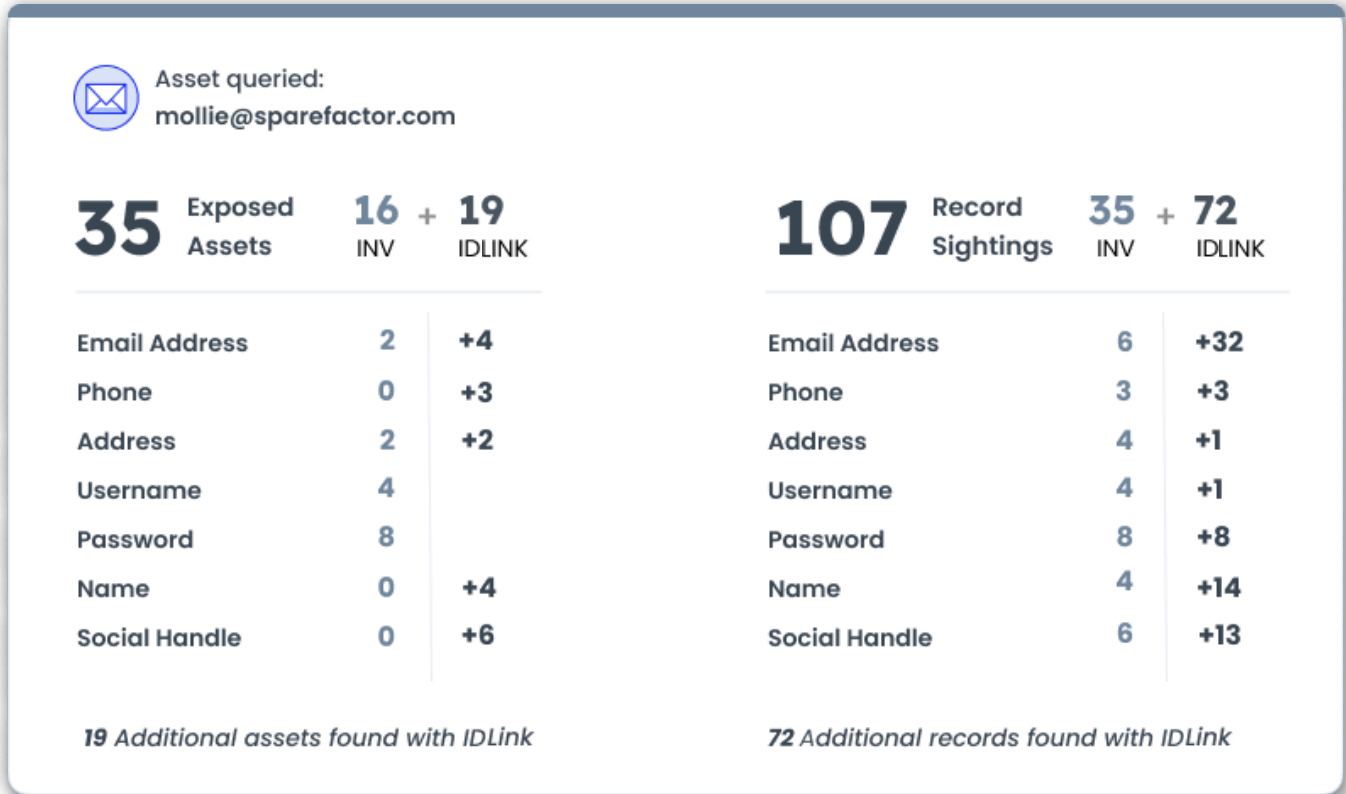
Quick and easy identity aggregation responds to new information to build comprehensive identity profiles and synthesize data from diverse sources

#### RESOURCE OPTIMIZATION

Elevate value from analysts - of all experience levels and data access - and free up time to maximize existing resources

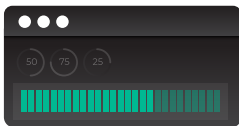
SpyCloud's IDLink API enhances investigations and individual identity resolution by streamlining the process of linking disparate identity-based data.

## QUERY IDLINK API TO FIND HIDDEN IDENTIFIERS



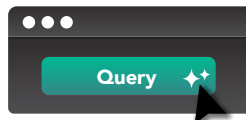
IDLink helps to automate common identity resolution workflows for analysts to find all the digital elements of a person.

## COMPREHENSIVE INVESTIGATIVE CAPABILITIES AT THE INDIVIDUAL LEVEL



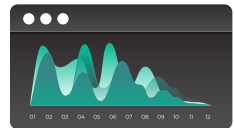
### RAPID ANALYSIS AND PIVOTING

Query on a targeted set of selectors to quickly find correlations with linked identifiers matching their connectors.



### HIDDEN CORRELATIONS

Query targeted set of selectors to aggregate linked identifiers hidden, removing dead ends from searches.



### REMOVE NOISE

Automatically sift and drop unrelated records — reducing noise from low confidence linked identities.

## KEY CAPABILITIES

**MULTI-LAYERED IDENTITY SEARCHES** | Conducts extensive searches across various identifiers like email, username, and phone number.

**AUTOMATED PIVOTING** | Reduce noise by automatically focusing only on relevantly-linked identity data when pivoting beyond the top layer of results.

**RELEVANCE SCORING** | Automatically evaluates the relevance of connected assets using a confidence score, focusing on the most pertinent connections.

**DATA ENRICHMENT** | Enhances raw data with additional context to provide a fuller picture of identities and their associated threats.



“Manually pivoting between selectors costs time and resources, as many investigations may lead to dead-ends and require a restart. IDLink automates the manual data pivots through an advanced algorithm, drastically **reducing our workflow time by 50%.**”

**CHRIS WINGFIELD** | MANAGING DIRECTOR – CYBER THREAT INTELLIGENCE  
**360 PRIVACY**

## ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to protect businesses from cyberattacks. Its products operationalize Cybercrime Analytics (C2A) to produce actionable insights that allow enterprises to proactively prevent ransomware and account takeover, safeguard employee and consumer identities, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, successful phishes, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include more than half of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to make the internet safer with automated solutions that help organizations combat cybercrime.