DATASHEET

SpyCloud

INVESTIGATIONS PORTAL

DRAMATICALLY INCREASE THE ACCURACY AND SPEED OF INVESTIGATIONS

THE PROBLEM

The volume and complexity of data available to analysts and investigators makes it hard to find the right information in a short enough time to support the right decisions. On top of that, finding the right team with the perfect skill set is an expensive and consuming process.

Getting what an organization needs from traditional threat intelligence tools often requires knowledge and experience that looks more like data science. The tools are often painful to use, and take a lot of time to properly craft a query to get the information the team needs, if it even exists.

SpyCloud makes it fast and simple to get the most impactful information in a format that is easy for analysts to use and even easier for decision makers to interpret. SpyCloud is the ultimate force multiplier for analysts – providing a wealth of quality analytics to profile threat actors, opening up new angles to investigate, and illuminating connections that make it faster and more efficient to achieve desired outcomes.

PRODUCT OVERVIEW

SpyCloud Investigations Portal delivers a powerful SaaS-based solution that enables analysts and investigators to quickly piece together decades-worth of criminals' digital breadcrumbs to reveal the identities of specific adversaries engaging in corporate compromise, online fraud, and other illegal activities. Simply put, SpyCloud Investigations makes it faster and more efficient to prevent adversary activity, protect employees, understand tactics, techniques, and procedures (TTPs), and make informed decisions.

BENEFITS AT A GLANCE

RAPID RESULTS

Robust query results deliver a full picture of adversaries and enable analysts to swiftly assess internal and external risks to the organization.

DEEPER CONTEXT

Easily correlate previously unknown information, selectors, and other digital exhaust for a contextualized view of your research subject.

SHORTEN THE INVESTIGATION TIMELINE

Get deep results based on even limited information or selectors, including email address, domain, IP address, password, and more.

GAIN SPEED & EFFICIENCY

Streamline workflows and visualize connections without needing to manage a third-party integration tool or install any software.

UNCOVER THE UNKNOWN

Easily connect potentially problematic activity to the broader context of historical actions, digging deep into the patterns of life of adversaries to illuminate hidden connections and infrastructure entry points.

KEY USE CASES

- RANSOMWARE PREVENTION
- FINANCIAL CRIMES RESEARCH
- THREAT ACTOR ATTRIBUTION
- INSIDER RISK ANALYSIS
- CREDENTIAL STUFFING ANALYSIS
- INFECTED HOST IDENTIFICATION

CYBERCRIME INVESTIGATIONS POWERED BY RECAPTURED DATA

KEY CAPABILITIES

SpyCloud Investigations Portal offers an easy to use SaaS-based user interface that makes it faster and more efficient to take down those attempting to harm your organization.

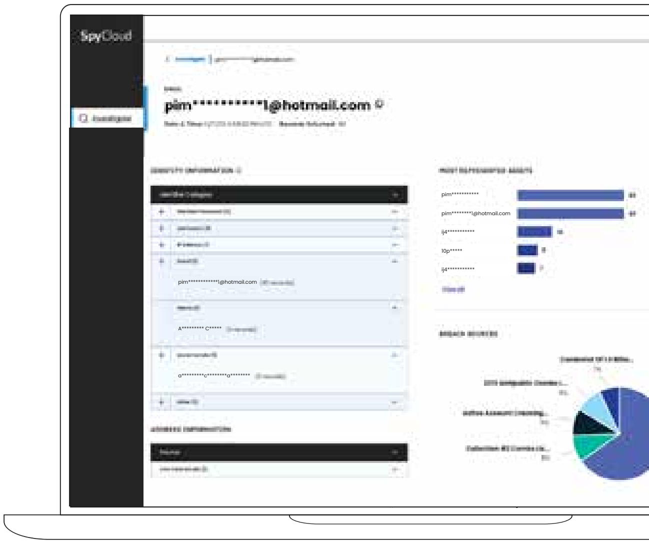
▣ ACTIONABLE DATA, FASTER RESULTS, CONFIDENT DECISIONS

No other provider offers this scale of high-quality data that is de-duplicated and normalized – enabling teams to take action with confidence without having to dig through mountains of noise

- Get unlimited queries with robust analytics
- Access SpyCloud's rich dataset of billions of assets from tens of thousands of third-party breaches and millions of malware-infected devices, with over 200 data types
- Leverage the world's largest and deepest collection of recaptured data, with 12+ billion assets analyzed and ingested monthly

▣ INTUITIVE VISUALIZATION, ROBUST DATA METRICS

- No endpoint or advanced querying skills required
- Statistics and visual reporting overviews based on the search type
- Powerful link analysis graph that supports "pivot" searches to quickly build a picture of the search target with "previously unknowable" connections
- Perform "follow up"searches in the same graph and tables so analysts don't lose their place
- Insightful widgets answer analyst questions without needing to sort through raw data to find needles in the haystack
- Easily see relationships between entities and pull threads to understand connections
- Guided analytic workflows and tradecraft based on best practices from world class analysts and investigators


SpyCloud
pim***********1@hotmail.com
pim***********
pim*********1@hotmail.com
ij4***********
10p*****
ij4***********
pim*************1@hotmail.com
A********* C*****
a*********c*********a*********

Looking to perform larger scale queries or need more customization? **Explore SpyCloud Investigations API >**

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.