DATASHEET

SpyCloud

INVESTIGATIONS API

EMPOWERING ANALYSTS WITH DARKNET INTELLIGENCE

THE PROBLEM

Analysts and investigators increasingly recognize how OSINT data can support their work — that there is power in breached data made publicly available by bad actors. Often this underground data contains elements from attackers themselves. Those who perpetrate data breaches and online fraud or share stolen data with other criminals can be de-anonymized using this very data.

SpyCloud collects data circulating within criminal communities – not only breach data, but also malware logs and information from other underground sources. We make it actionable to protect organizations and their customers. Investigators can put it to use to protect users, discover information about adversaries, and shortcut their discovery of critical information.

BENEFITS AT A GLANCE

Gain Speed & Efficiency
Shorten the timeline of your investigations with deep results based on limited information, including email address, domain, IP address, password, and more

Correlate Multiple Data Sources
Connect SpyCloud with disparate data sources, including internal data and OSINT data sources such as VirusTotal, Passive DNS, and Whois to add even more context to your investigation or analysis

Discover the Undiscoverable
Unmask specific threat actors and their alternate personas, research criminal campaigns and their infrastructure, and open up new angles of investigation by pivoting on known and newly discovered data points

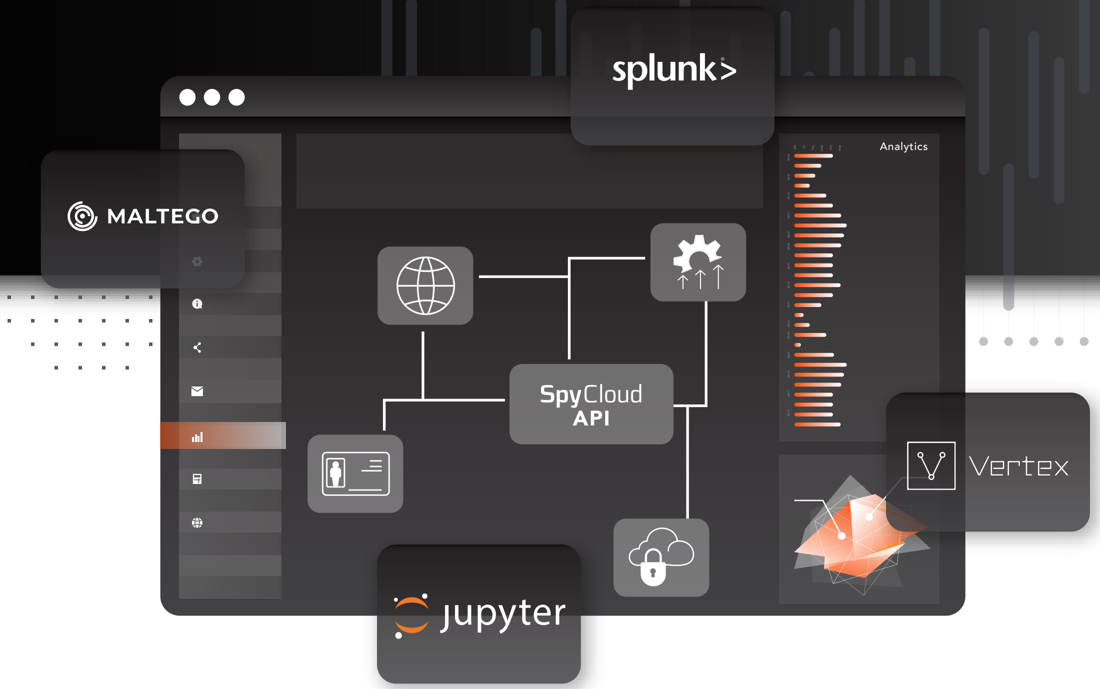
PRODUCT OVERVIEW

ACCELERATE ACCURACY OF INVESTIGATIONS WITH RECAPTURED DATA

SpyCloud Investigations API enables investigators to piece together decades-worth of criminals' digital breadcrumbs to reveal the identities of specific adversaries engaging in commercial 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.

USE CASES

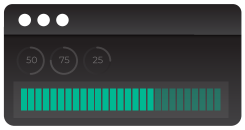
- THREAT ACTOR ATTRIBUTION
- INSIDER RISK ANALYSIS
- THIRD-PARTY EXPOSURE
- FINANCIAL CRIMES RESEARCH



HOW IT WORKS

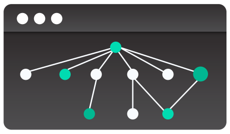
SpyCloud's REST-based Investigations API enables analysts and investigators to combine breach data with other internal and other OSINT data sources via link analysis tools such as Maltego and Jupyter Notebook. These interactive data mining tools render graphs for link analysis and are often used to find relationships between pieces of information collected from various sources located on the internet. With the SpyCloud Investigations API, investigators can pivot on data points like username, password, IP address, or email address and find a wealth of data.

COMPREHENSIVE INVESTIGATIVE CAPABILITIES FOR BROAD DATASETS



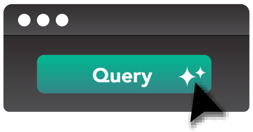
HIGH-VOLUME DATA ANALYSIS

Perform large queries on a range of identifiers (including domains, plaintext passwords, and infection records) with extensive result sets.



ASSOCIATING RESULTS

Query with a single data point or multiple pivots to narrow down relevant results to identify specific patterns or anomalies within large datasets.



LOOP & BATCH QUERY

For investigations that necessitate revisiting and refining parameters, loop and batch queries for specific selectors.

KEY CAPABILITIES

- **ATTRIBUTE CYBERCRIME |** Uncover the true identities of specific criminals and their personas.
- **EVALUATE THREAT ACTORS |** Profile criminal targets, identifying where they have had accounts and where they are operating.
- **ASSESS RISK |** Understand internal and external user risks, from reused credentials to malware infections.
- **UNDERSTAND ATTACKS |** Determine the origin of data used in credential stuffing attacks and identify the exposure of public applications to botnet credential stealers.
- **INVESTIGATE CAMPAIGNS |** Research criminal campaigns and infrastructure, including the breadth and nature of malicious campaigns.

SPYCLOUD API INTEGRATIONS

MALTEGO

Use link analysis to speed up your investigations

80+ Maltego Transforms to quickly leverage SpyCloud data

Easily investigate and identify relationships, or pivot on recaptured record details

jupyter

Prebuilt Notebooks deliver results in an easy-to-digest format that enables drill downs, data exports, and flexible graphs

Efficiently extract intelligence using a popular open-source tool

splunk>

Run ad hoc queries against SpyCloud's repository of recaptured assets

Use custom search commands for enrichment using SpyCloud data

Vertex

Provide custom Storm commands to access SpyCloud Investigations data within Synapse

Use SpyCloud Investigations data to enrich nodes

> “Having access to SpyCloud’s data lake related to PII supports a lot of research that we do. We can make connections between threat actors’ personas, the services they sell, malware they use, or specific attacks.”
>
> **GLOBAL MANAGED SERVICES PROVIDER**

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics to proactively prevent ransomware and account takeover, safeguard employee and consumer accounts, and accelerate cybercrime investigations. SpyCloud's data from breaches, malware-infected devices, and successful phishes also powers many popular dark web monitoring and identity theft protection offerings. Customers include seven of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies worldwide. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to protect businesses and consumers from the stolen identity data criminals are using to target them now.