DATASHEET

SpyCloud

INVESTIGATIONS MODULE

ACCELERATE INVESTIGATIONS. STRENGTHEN ATTRIBUTION. SHIFT THE ADVANTAGE.

THE PROBLEM

Analysts are drowning in data and starved for clarity. The sheer volume of compromised identity assets and OSINT data makes it nearly impossible to correlate digital breadcrumbs, attribute threats, or spot insider risks – before damage is done. Most tools demand deep expertise, limiting success to only the most seasoned investigators. SpyCloud Investigations changes that. It gives teams a faster, smarter path from raw exposure to finished intel – helping organizations act before cybercriminals do.

PRODUCT OVERVIEW

SpyCloud Investigations is a SaaS-based module that lets cyber threat intel, security operations, and fraud and risk teams uncover, analyze, and act on identity exposures with speed and confidence.

Designed as the ultimate force multiplier for analysts, delivering deep identity intelligence by transforming malware, phished, and breached data into deep identity intelligence – revealing holistic views of exposed users and infrastructure.

Powered by **IDLink™** analytics, SpyCloud Investigations automatically connects the dots across exposed assets to build holistic digital identities. Analysts can explore these relationships in an interactive graph and pivot across exposures correlated to their environment and supply chain.

SpyCloud Investigations accelerates the path from raw data to finished intelligence. Embedded **AI Insights** – built on decades of SpyCloud's investigative tradecraft and methodologies – detect insider threats, surface hidden connections, and close investigative gaps, faster than ever.

BENEFITS AT A GLANCE

See The Full Picture, Instantly
Query SpyCloud's vast collection of recaptured data to rapidly construct digital identities and uncover sophisticated insider and external threats

Accelerate Investigations
Find answers faster with AI that detects suspicious identity patterns and relationships often missed by other solutions, significantly reducing discovery time from hours to seconds

Deliver Finished Intel
AI Insights transforms complex exposure patterns into actionable threat signals and clean, exportable reports with the click of a button

Amplify Analyst Impact
Empower analysts of any expertise level to focus on the most critical threats and maximize their investigative impact regardless of case complexity

SPYCLOUD COVERS THE *FULL SPECTRUM* OF IDENTITY THREATS AND INVESTIGATION USE CASES

- THREAT ACTOR ATTRIBUTION
- INFECTED HOST IDENTIFICATION
- VIP EXPOSURES
- SUPPLY CHAIN EXPOSURES
- INSIDER THREATS (MALICIOUS & UNWITTING)
- PATTERN OF LIFE ANALYSIS
- IDENTITY RESOLUTION
- REMOTE WORKER & CONTRACTOR FRAUD
- PLATFORM ABUSE
- HARD-TO-DETECT FRAUD
- KNOW YOUR CUSTOMER (KYC)
- TRUST & SAFETY ESCALATIONS

SPYCLOUD GIVES TEAMS ***EXPOSED IDENTITY DATA AND AI-DRIVEN CONTEXT*** TO INVESTIGATE WITH SPEED AND PRECISION.

BUILT FOR EVERY TEAM

CYBER THREAT INTEL

Attribute adversaries and map digital identities across campaigns and infrastructure

SOC & IR

Accelerate investigations and pivot faster from detection to decisive action

FRAUD & RISK

Uncover compromised identities and stop fraud tied to phishing and malware exposures

TRUST & SAFETY

Protect users and platforms by identifying identity abuse and account compromise early

SpyCloud

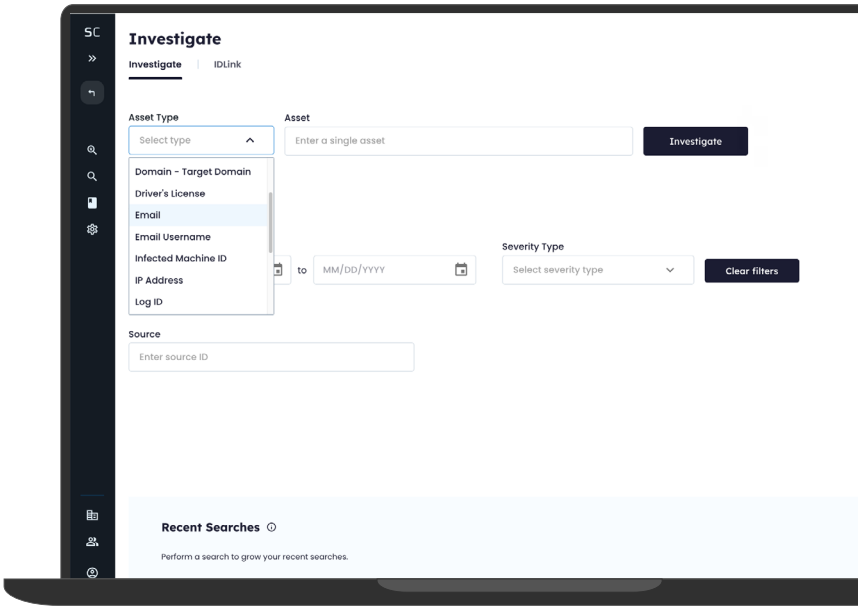
HOW SPYCLOUD INVESTIGATIONS WORKS

SpyCloud Investigations combines deep recaptured data from the criminal underground with automated correlation and intuitive visualizations. Queries begin with any of the most common selectors analysts rely on – like an email, phone number, or IP address – and automatically expands through **IDLink** analytics, which maps connected identity elements to reveal a holistic digital profile. These relationships are visualized in an interactive graph, allowing analysts to pivot through connections and uncover hidden exposures quickly.

AI Insights takes this a step further, detecting behavioral patterns and digital habits that signal insider and external threats. It turns raw identity exposures into finished intelligence, surfacing actionable leads and accelerating path to attribution.

INVESTIGATE USING THESE ASSET TYPES, AND MORE

- Domain
- Email address
- Password (hashed)
- Phone number
- Infected machine ID
- Social media handle
- Username
- SSN
- Drivers license number

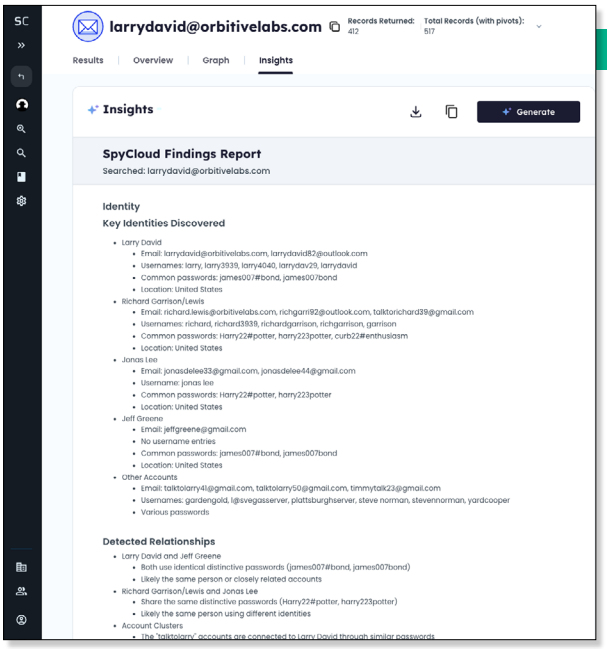


Findings in SpyCloud Investigations are based on continuously delivered recaptured identity assets from malware-infected devices, successful phishes, and third-party breaches, often accessible within minutes of discovery in criminal communities.

SpyCloud

AI INSIGHTS CLOSES GAPS *FASTER*

Detect threats uncovering patterns in identity misuse no human would spot. In seconds, analysts can produce reports ready for escalation, briefing, or compliance – leaning on the tradecraft and expertise of SpyCloud's elite team of cyber investigators. **AI Insights** is built on real-world investigative workflows and powered by **IDLink** – leveraging SpyCloud's robust repository of recaptured identity data.



*In seconds, **AI Insights** applies curated logic and correlation to identify the research subject, surfaces key exposures, and builds a comprehensive report that would take hours to compile manually.*

HOW AI INSIGHTS WORKS

From subtle patterns to finished intelligence – **AI Insights** uncovers the threats others miss. **AI Insights** automates the final step of the investigation process by turning complex identity exposures into actionable summaries without requiring manual analysis.

Built on SpyCloud's investigative tradecraft, it synthesizes relationships and risk indicators across malware, phished, and breached data to generate finished intelligence in seconds.

1. After pivoting across your dataset, **AI Insights** analyzes all exposed assets in context – flagging suspicious patterns such as identity reuse, credential overlap, and suspicious browser activity.
2. SpyCloud's AI model identifies unique patterns and signals commonly tied to insider threats, synthetic identities, and coordinated fraud by evaluating every data point returned in your queries.
3. **AI Insights** generates a streamlined PDF that summarizes the investigation's scope, key risks, and notable associations. Analysts can export the exec-ready report for escalations, incident response, or stakeholder briefings.

SpyCloud

GET ANSWERS FASTER WITH IDLINK POWERED INVESTIGATIONS

Unlocking and unblocking investigations is now easier than ever. SpyCloud Investigations includes our proprietary **IDLink** advanced analytics – which automatically builds holistic identities to give you the speed and resources you need to drive analysis to attribution.

HOW IDLINK WORKS

IDLink speeds up the process of investigating exposed identities, and reduces the manual effort to filter out irrelevant records that bog down analysis:

- After searching exact matches on an email, username, or phone number, **IDLink** automatically runs pivots in the background, looking for connections on everything that makes up a digital identity – from matching emails and backup emails, to shared and exposed PII, usernames, passwords, and over a dozen other asset types
- SpyCloud Investigations with **IDLink** only returns new, highly-relevant results, removing any out-of-scope identity asset that slows down analysis
- SpyCloud Investigations enhances raw data with additional context to give you a broader view of exposed identities and threats

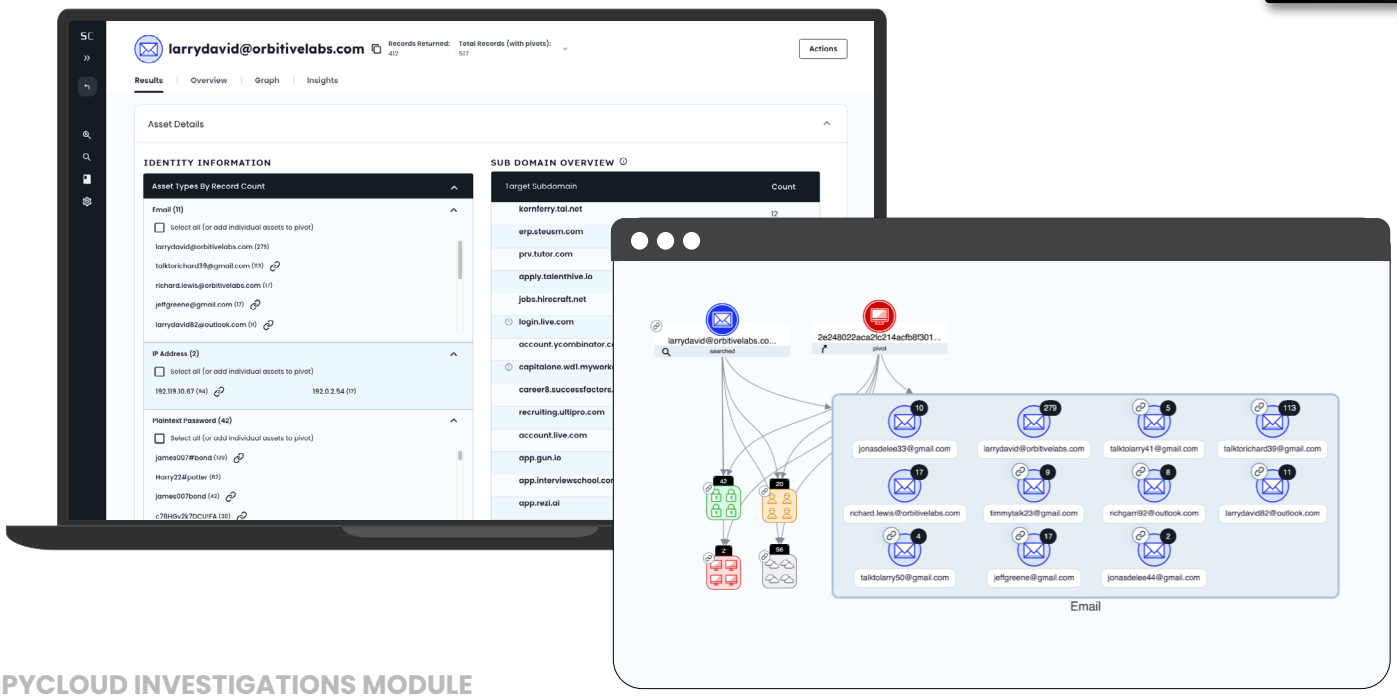
SEE MORE EXPOSURES WITH IDLINK

8x MORE IDENTITY RECORDS

2x MORE MALWARE RECORDS

14x MORE PLAINTEXT PASSWORDS

5x MORE EMAIL ADDRESSES



SPYCLOUD INVESTIGATIONS MODULE

SpyCloud

KEY CAPABILITIES

TURN EXPOSED IDENTITY DATA INTO FINISHED INTEL WITH SPYCLOUD INVESTIGATIONS

SpyCloud Investigations is a powerful, easy to use SaaS-based module that makes it faster and more efficient to analyze and remediate cybercrime and identity threats.

QUERY | Broaden your understanding of exposure risks across your organization and supply chain

- Perform unlimited queries against SpyCloud's rich dataset of identity assets from tens of thousands of third-party breaches, millions of malware-infected devices, and successful phishing attacks, with over 200 data types
- Start investigations for a direct match using 19 asset types, including email address, domain, IP address, password, and more, or reconstruct holistic identities faster by querying **IDLink** analytics on an email, username, or phone number

PIVOT | Pull in the most relevant identity data points for your investigation and analysis

- Pivot off query results for a full picture of exposures and identity compromise, and enable analysts to swiftly assess internal and external risks to the organization
- IDLink analysis to remove out-of-scope identity assets to focus investigations on relevant information, filtering out noise

GRAPH | Visualize holistic identities across employees, customers, and your supply chain

- Powerful link analysis graph to perform pivots and quickly build a picture of users with previously unknowable connections
- Perform follow up pivots in the same graph and tables so analysts don't lose their place, finding direct matches, wildcard searches with fuzzy pivots, or broader identity views with **IDLink** analysis

ACT | Get finished intel for attribution and analysis in a report ready for analysts to use

- Summarize exposed identities, digital habits, and key risk factors in seconds with **AI Insights**, without needing to sort through raw data or perform manual analysis
- Generate clean, consumable summaries for executives, IR teams, and external stakeholders

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics and AI to proactively prevent ransomware and account takeover, detect insider threats, safeguard employee and consumer identities, 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.

To learn more and see insights on your company's exposed data, visit **spycloud.com**.