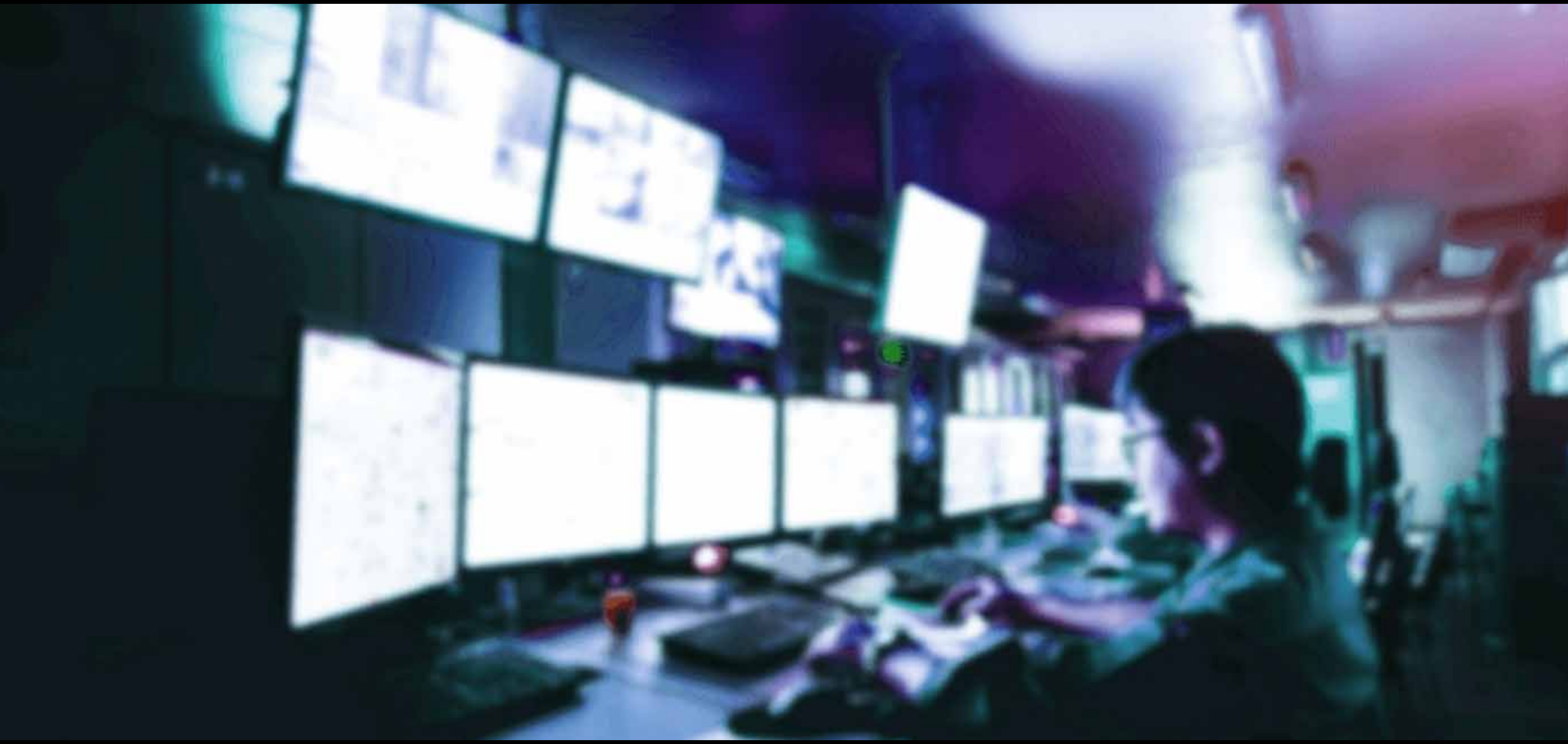
SpyCloud



Case Study

Enabling a Global Managed Services Provider to Expand the Value of Their Offering

Overview

This case study examines an anonymous SpyCloud customer that acts as a managed services provider for IT teams, supporting a set of Fortune 100 organizations. Their comprehensive security offering includes a whole suite of services such as security operations, threat intelligence, hunting, red teaming, and incident response.

Challenge

As a managed security provider, this customer needed an efficient way to keep up with newly-exposed breach data, both to identify clients' account takeover risks and expand their visibility into threat actor activity.

Solution

With SpyCloud, the customer now alerts clients when employee credentials have been exposed on the criminal underground and uses SpyCloud Investigations to help identify, track, and profile specific threat actors to guide recommendations to clients.

Result

SpyCloud enabled the customer to offer credential monitoring to their clients to prevent ATO, as well as increase the quality of their threat intelligence reports — all without hiring additional staff.

Collect Breach Data Efficiently at Scale

MSSPs accumulate their clients' challenges. When providing security services to thousands of subscribers around the world, agility and data quality are critical factors for remediating clients' vulnerabilities before they can be exploited, and providing recommendations on evolving threats so clients can set up proactive defenses.

According to the vice president of threat intelligence services at the company, the customer knew they needed access to the breach data available to cybercriminals in order to protect their clients effectively. They carefully considered the time and resources required to gather that type of data efficiently on their own.

"How much is a person capable of collecting? To be able to scale you need to be able to collect as much data as possible and make sure it's good quality. You need to have dedicated people to do that."

Before turning to SpyCloud, the customer considered building their own internal service that would collect breach databases and monitor for client data.

However, meeting their own needs for data volume and quality may have been prohibitively expensive and required additions to the team (or a whole new team). The customer understood that building this service themselves meant delaying a critical security service their clients needed.

"We knew how much and how long it would take to be able to do that and we wanted a solution that would help us hit the ground running right away."

Leverage SpyCloud Data for Faster, Better Visibility

The customer was not collecting breach data on their own before using SpyCloud, but did know what data they wanted and how they would make it valuable to clients.

When choosing a vendor to collect and operationalize this data for them, the customer says they considered several SpyCloud competitors but were impressed by the scale and quality of SpyCloud's data.

> “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.”

“SpyCloud gave us an easy and quick way to offer credential monitoring to clients that subscribe to our service. When a breach is made public, our clients worry about whether or not their information is included in the breach. Being able to collect data quickly to answer that question, then get it in the clients’ hands to remediate vulnerabilities before is crucial.”

SpyCloud has recovered over 100 billion breach assets from the cybercriminal underground, and as the company and its data resources have grown, the customer says they’re experiencing an increase in quality and availability of data.

“Knowing I have a dedicated system I can rely on to tell me if we have credentials exposed gives me peace of mind.”

The organization finds SpyCloud’s speed in recovering data after a breach particularly valuable.

“Every minute counts. Once a set of data is made available, we know there is a fast turnaround before bad guys get their hands on it and start attacking organizations using those accounts.”

In addition, the customer uses SpyCloud Investigations to help them identify, profile, and track threat actors in order to make security recommendations for their clients. This is another area where the quality and scale of SpyCloud’s data gave the customer an advantage: SpyCloud helps the team connect threat actor personas and TTPs into more comprehensive profiles.

“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.”

Results: Gain Critical Insights Without Increasing Team Size

SpyCloud’s ATO Prevention and Investigations solutions help this customer identify exposed credentials across their client organizations. This capability comes without the substantial investments of time and capital the customer would need to add dedicated staff who could collect, analyze, and operationalize breach data.

“I would need a bigger team without SpyCloud.”

Additionally, SpyCloud Investigations helps make the customer’s threat intelligence reports more valuable to their clients. And better data helps the customer build better profiles of threat actors. Their clients can use these profiles to more easily identify when certain TTPs are relevant to their organization and what changes are needed to close gaps in their security posture.

“SpyCloud really helps our research in connecting dots between a persona that we have and one that we don’t.”

Providing security services to support a set of Fortune 100 organizations requires agility.

With SpyCloud’s solutions, this customer and their team can move from research to action more quickly and provide insight on evolving threats at the crucial time before attacks begin.

“I really like to be able to connect dots between identities and personas and that’s only possible because we have SpyCloud. We can cover a lot of ground with it, and we can cover a whole set of third-party places that are exposed in a breach. That really helps, especially for certain actors that we track. The reach that we have in SpyCloud in terms of collection is really helpful.”

SpyCloud

"Because of the collection capabilities [SpyCloud has], we can do more at a bigger scale."

"I sleep well at night knowing that I have SpyCloud."

About SpyCloud

SpyCloud transforms recaptured data to protect businesses from cyberattacks. Its products leverage a proprietary engine that collects, curates, enriches and analyzes data from the criminal underground, driving action so enterprises can proactively prevent account takeover and ransomware, and protect their business and consumers from online fraud. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to over 150 cybersecurity experts who aim to make the internet a safer place.

Enterprise Protection

Prevent account takeover that can lead to ransomware.

Learn More

Consumer Protection

Combat account takeover and online fraud.

Learn More

Investigations

Unmask criminals attempting to harm your business.

Learn More

Data Partnerships

Enhance your solution with SpyCloud's data.

Learn More

Learn more at spycloud.com