

ITHREAT IMPROVES INTERNET INVESTIGATION SERVICES WITH DATASTREAMER SUPPORT

Analysts increase speed of tracking online threats to protect clients



DATASTREAMER

ABOUT DATASTREAMER



Datastreamer's API-drive platform powers high quantity data filtering and aggregation products. Our solution enables clients to launch conversational text data products quickly, and continuously enhance existing features. Datastreamers' customers use real-world data and historical insights to answer research questions, ensure security, and deliver strategic intelligence. Through one API, you can leverage our data partner network, classifier technologies, and infrastructure delivering over 5 billion pieces of content a month.

ITHREAT COMPANY OVERVIEW



For over 20 years, iThreat has been at the forefront of threat signal monitoring for client organizations and their assets. Their solutions aim to detect, investigate, and find and mitigate threats to their customers, including investigative services. iThreat SignalAlert programs detect important human-driven dialogue and text representing real and implied threats to their customers, including information leaks, intellectual property theft and circumvention, brand disparagement and infringement, threats directed at key staff, threats of disruption, embargo agreement violations, counterfeiting, insider threats, and other security concerns.



INTRODUCTION

iThreat, an internet investigation service company, was looking to improve the speed, coverage, and accuracy of its reports for clients. To do this, they needed a technology partner behind the massive real-world data needs of their SignalAlert offerings, driven by their FusionCenter platform.

The company's goal is to include and monitor all relevant data sources via the FusionCenter platform. Analysts then use FusionCenter to review all data sources, allowing analysts to create and alter complex Boolean-based search rules in a single place and perform batch processing, filtering, and searching via the state-of-the-art intelligence product.

SOLUTION

iThreat chose Datastreamer as a solution for their SignalAlert service. We were able to provide them with the core data for their featured product. Our full streaming API handles 95 percent of data indexing requirements. Using the Datastreamer full-text search, analysts can run precise queries with a large amount of data from various sources. The results are not only quick and accurate but also specific to the needs of clients. Together with our data partner network, iThreat was able to expand their data coverage while investing their development resources into their FusionCenter and CleanDNS platforms.

BY THE NUMBERS

International Coverage

All primary European and American languages

3 Billion+ posts and articles.

Pieces of unique content sourced and analyzed monthly.

ACTION

iThreat was able to integrate the Datastreamer APIs into the FusionCenter platform, allowing iThreat analysts to set up a process for quickly gathering, sorting, investigating, and reporting key security threat signals.. Our support greatly expanded the reach and visibility of iThreat's detection programs and enhanced their analysts' ability to identify trends that signal risks to iThreat clients.

RESULTS

iThreat is building a reputation for wide coverage, speed, and accuracy. Detecting threats accurately and quickly are vital to assist analysts in the reporting process. Clients rely on their services to mitigate problems and minimize victimization.

To assist the internet investigation process, Datastreamer brought billions of pieces of data together to create a pipeline for iThreat analysts. Using this pipeline, they were able to filter and aggregate large data sets to uncover trends that indicate security risks to clients and identify additional information and activities associated with target threat actors.

With our help, iThreat's analysts quickly spot trends from the data collected, improve the accuracy and speed of risk identification, and more efficiently investigate the threat actors behind the threats.

