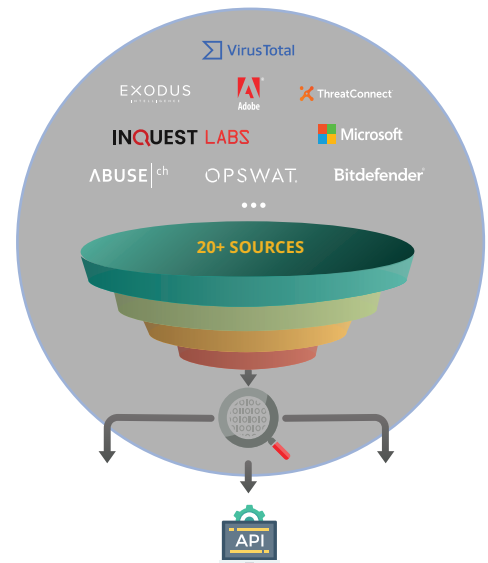


# INQUEST®

# InSights

InSights threat intelligence service is comprised of data extracted from billions of file samples and indicators of compromise with a specific focus on the identification of goodware and malware content as well as the activity associated with their execution.

The collection, processing, analysis, and normalization of raw threat intelligence information from disparate third-party open/closed sources, our customers' environments, and our own internal research is what differentiates us from the traditional threat intelligence providers.



## CORE COMPETENCIES

- Automated File Reverse Engineering
- Threat Prevention
- Threat Hunting via RetroHunt®
- Data Loss Prevention
- Actionable and Automated Threat Intelligence

## FEATURES & BENEFITS

- Real-time notifications of threats detected and/or prevented
- 24x7 access to a dedicated InQuest threat analyst
- Recurring threat reporting tailored to your environment and operational objectives

## DIFFERENTIATORS

- Proven early warning identification of threat actors' attack infrastructure prior to the launch of the threat campaign
- Unique insights captured from our customer IOC extraction, identification, and threat exchange network
- Unique insight and perspective into the attack chain given our experience and focus on malicious artifacts
- Support for customization and integrations into your existing SecOps infrastructure and operational environment
- Highly experienced Threat Intelligence analysts with a wide range of backgrounds and experiences to deliver actionable indicators and outcomes

## OUR OFFERINGS

### Threat Intelligence Feed

Aggregated, curated feed of IOCs delivered daily to your organization with a number of formats to choose from.

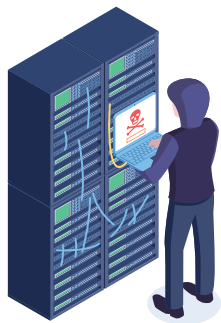


### Threat Intelligence Gateway

Natively capture and tag your network session and file data utilizing our aggregated threat intelligence feed coupled with your user-defined IOCs and disseminate the output to your analysts.

### Tailored Threat Intelligence

We tailor and deliver threat intelligence specific to your organization through brand monitoring and early warning indications of actor intentions to target your assets.



### Threat Actor Tracking

How would you detect or even identify a threat actor's tradecraft that has never been seen before and was developed with the sole purpose of infiltrating your organization? Proactively track threat actor groups targeting your vertical or even your organization through the identification and use of their tactics, techniques and procedures.

### Threat Intelligence Analyst Augmentation

Augment your staff with one of our threat analysts (dedicated or part-time), assess the state of your existing threat intelligence capabilities based on your requirements, address any of the gaps we may identify in how you are currently postured (people, processes, tools), define threat intelligence use cases specifically focused on your organizational objectives, and assign threat intelligence tasks.

