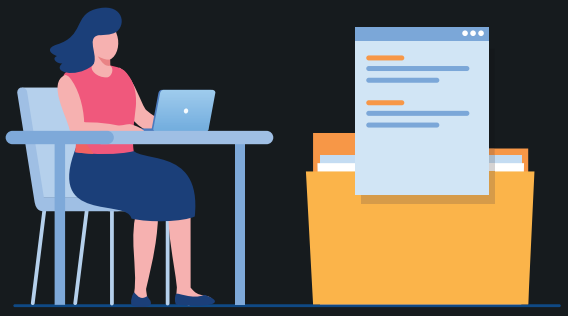
INQUEST

OVERVIEW

FILE DETECTION AND RESPONSE (FDR) SOLUTIONS



Problem

Some of today's biggest biggest security threats are malware, ransomware, phishing campaigns, impersonation, scams, fraud, and data loss violations. These threats typically have two things in common: an end-user and a file. One is easily tricked. The other is easily laced with hidden risk. This creates the end-user security gap.

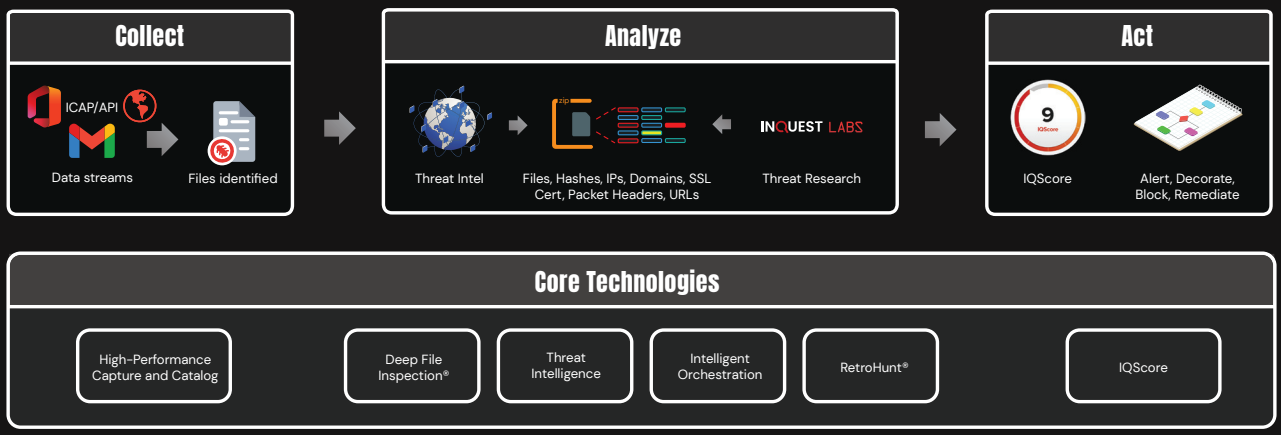
Solution

InQuest's File Detection and Response (FDR) solutions close the end-user security gap by stopping file-borne breaches and incidents with technology that takes the file interaction risk out of end-users' hands. Our FDR solutions operate against files in any state - files at rest, files in motion, and files in use. They can be deployed to inspect files that are delivered via email, downloaded over the web, or in transit on your network.

Other detection and response solutions (XDR, NDR, EDR) are ineffective against file-borne attacks. InQuest® File Triage, Analysis, and Control (FileTAC) is purpose-built for file analysis at scale. No other solution analyzes files - in more depth, faster, or across time - better than InQuest.

> *Prior to having InQuest, file decompression, decoding and post-processing were all manual steps that were very time consuming for us. Now that we're using InQuest, all of those steps are automated and it has given us the ability to apply these steps to not only files we think are suspicious, but all files received by our users.*
>
> Malware Analyst, US Intelligence Community

FileTAC In Action



FileTAC is a turnkey solution that begins with high-performance data collection from email, web, and network traffic sources. Raw, native data streams are ingested and files within are automatically extruded - making what was previously complex, time-consuming, and expensive work into a fast, easy, and scalable process.

Next, our patented Deep File Inspection® (DFI®) automates human, analyst-grade file dissection - exposing 4x more content in an average of three seconds. These outputs are then analyzed through a combination of proprietary systems and threat intelligence, both third-party and internally-curated. This results in the rapid identification of files with sensitive, suspicious, or malicious characteristics. Supported indicators of compromise (IOCs) include fuzzy hashes, IPs, domains, URLs, SSL certificates, web/email headers, and more. DFI relieves staff from countless hours of work required to find the proverbial needle in the haystack.

Then, FileTAC uses an expert system to produce a single, all-encompassing threat or data-loss score (IQScore) per artifact - pointing precious human decision-making energy exactly where it will be most effective.

Last, FileTAC takes this entire process one step further by not only performing the above against real-time traffic, but also against emails, files, etc. that may have bypassed defense-in-depth solutions that were operating on "yesterday's" threat intelligence. The moment new threat intelligence surfaces, RetroHunt® scavenges the network and file stores for active threats - rooting out attackers before dwell time turns into disaster.

Benefits

Stop file-borne breaches and incidents

First and foremost, FileTAC saves organizations from the costs associated with file-borne malware, ransomware, exploits, phishing campaigns, impersonation, scams, fraud, and data loss breaches and incidents. As examples, according to the Ponemon Institute in 2022:

Attack Type	**Average Total Cost in the U.S.** *(detection and escalation, notification, post breach response and lost business)*
Ransomware breach	$4.54M
Data breach	$4.35M
Business Email Compromise (BEC)	$4.89M
Phishing	$4.91M
Compromised Credentials	$4.50M

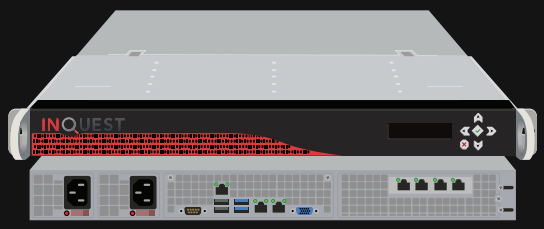
Automate threat hunting with real-time intelligence

There is no security silver bullet. Some adversaries will slip through even the very best defenses. This is where the human skill must be leveraged. But as we know, there is never enough human intel to combat a relentless and motivated world of attackers. And without question, SOC analysts and threat hunters are missing a full detection and response toolset if the average time to identify and contain a breach is nearly a year. FileTAC provides direct benefit to burned out and overloaded SecOps teams:

- Enables existing security personnel to find the real threats, attacks, breaches, and data exfils without wasting time on false positives or threats of low severity
- Saves massive amounts of analyst time stripping malware down to its very essence
- Decreases analysis time needed to understand/act
- Frees staff time for higher order work
- Reduces analyst alert fatigue
- Eliminates irrelevant, time-wasting work
- Enables a short learning curve for busy staff
- Simplifies analyst daily grind
- Operates in a clandestine manner - providing a distinct man-machine advantage over adversaries

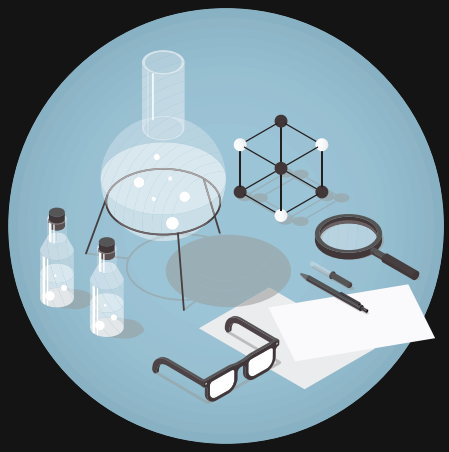
Force multiply your SOC ROI

FileTAC also provides substantial benefit by reducing cybersecurity capital spend, lowering operating costs, and driving up the efficacy and value of adjacent security solutions:



Collector and Manager appliances collect, process, and analyze network traffic at rates from 100 Mbps to 40 Gbps and beyond - in a single 1-RU appliance. Relative to other traffic capture and analysis appliances, this represents a substantial capital and operating cost savings in rack unit space, power, and cooling.

InQuest Labs' continuous harvesting, de-duping, parsing, augmenting, and scoring of internal/proprietary, public, and private 3rd party threat intel not only preserves human capital (time and energy), but also provides ultra-high fidelity threat intel back out to SIEMs and policy enforcement engines for immediate data enrichment - operational intelligence they are simply incapable of producing on their own.



Reducing the cost of two of the most expensive elements of cybersecurity - collecting big data cost-effectively and automatically distilling threat intelligence into the essence required by man and machine to take fast, corrective action - is a direct boost to any organization's overall return on the security dollar.

Contact us to see how InQuest can close your end-user security gap through an email security assessment, full product demonstration, or a 30-day free trial.

INQUEST

www.inquest.net @InQuest sales@inquest.net linkedin.com/company/inquest.net