ThreatConnect and InQuest

Proactive Protection for Organizations: Integrating ThreatConnect's TI Ops Platform with InQuest InSights for Enhanced Cybersecurity

The Challenge

The cyber threat intelligence (CTI) data landscape is full of data, both commercial and open source, with varying levels of quality, and coverage. InQuest uses its Deep File Inspection® file analysis capabilities combined with a focus on the transport layer to provide novel insights and perspective into ongoing threat actor campaigns as they unfold. In many cases, InQuest releases indicators of compromise (IOCs) ahead of sources more focused on endpoint execution events.

Why ThreatConnect + InQuest

InQuest InSights combines advanced threat intelligence, derived from extensive malware file analysis and a mix of open-source and exclusive reputation data sources, augmented by the visibility of indicators extracted from file-based analysis across its customer base, partnerships, and its own analysis platform. The combination of ThreatConnect's TI Ops Platform and InQuest InSights enables CTI and security operations teams to benefit from InQuest's unique IOCs for CTI analysis, and threat detection and prevention to a wide range of SIEM and security analytics tools, as well as endpoint, network, and cloud security solutions. This enhances an organization's ability to detect threats and reduce false positives accurately. These IOCs, which are 92.9% unique compared to existing TI data shared with Quad9.net, provide security teams with a distinct perspective based on real attacks observed in the wild. These are typically from advanced threat actor groups targeting highly sensitive, strategic sectors. InQuest's IOCs are noteworthy for their timeliness and uniqueness, averaging 383 days ahead of public dissemination or recognition as a "new threat" by other major TI vendors.

Key Benefits

- Complete visibility of indicators extracted from InQuest's file-based analysis across their customer base, partnerships, and analysis platforms.
- Unique perspective based on real attacks seen in the wild, from threat actor groups targeting highly sensitive, strategic sectors and are typically more advanced in evasion capabilities.
- Quick time to value to apply InQuest's threat intel across a range of use cases with the ThreatConnect TI Ops Platform.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

Get Results with ThreatConnect + InQuest

Incorporating InQuest InSights threat intel in ThreatConnect's TI Ops Platform gives CTI and Security Operations teams a powerful way to use that intelligence across the range of technologies that integrate with ThreatConnect, for a variety of use cases, like:

Enhanced Threat Detection, Monitoring, and Alerting:

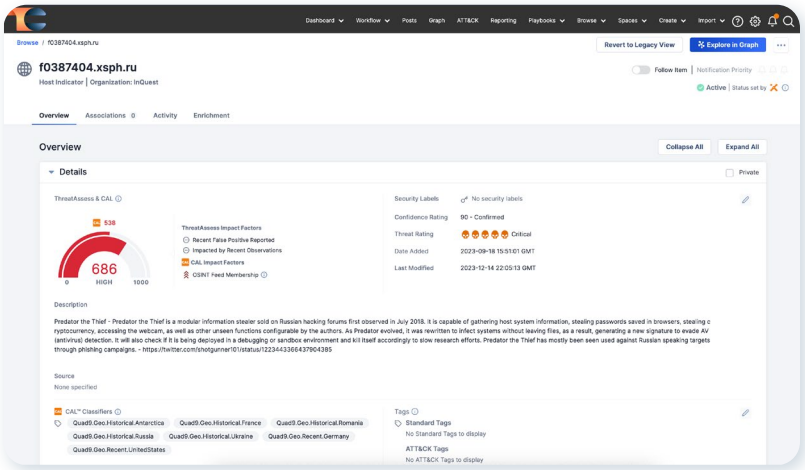
InQuest InSights is crucial for improving the detection capabilities of security solutions. By integrating IOCs like IP addresses, URLs, and malicious code signatures into security tools (such as EDR, NDR, XDR, firewalls) organizations can more effectively identify potential threats. This enhanced detection leads to timely alerts, allowing security teams to respond quickly to potential breaches or attacks.

Threat Hunting and Investigation:

InQuest InSights is invaluable for threat-hunting activities. By using known threat indicators, teams can comb through logs and other data to identify hidden threats. This proactive approach helps in uncovering sophisticated or advanced persistent threats (APTs) that can linger undetected in networks for long periods, causing significant damage.

Producing Strategic Intelligence:

InQuest InSights can play a pivotal role in assessing and managing cybersecurity risks. By analyzing these indicators, organizations can gauge their exposure to different types of cyber threats. This assessment helps in prioritizing security efforts, focusing on the most relevant and potentially damaging threats. It also aids in developing strategies for mitigating risks, such as applying necessary patches, enforcing security policies, or conducting targeted employee training to address specific vulnerabilities highlighted by the threat indicators.



How to Get Started

ThreatConnect users can get more details on the InQuest integration in the ThreatConnect Marketplace or reach out to Customer Success. To learn more about ThreatConnect's TI Ops Platform, visit threatconnect.com. To learn more about InQuest's solutions, visit inquest.net.

ThreatConnect.

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. Over 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

www.threatconnect.com
+1-703-229-4240
sales@threatconnect.com

INQUEST

InQuest empowers private and public sectors to identify, detect, and prevent advanced malware, ransomware, phishing, scam and fraud attacks, breaches, and data loss incidents. Its industry-leading File Detection and Response (FDR) solutions stop file-borne breaches and incidents, automate threat hunting with real-time intelligence, and force multiply SOC and SecOps across the globe. Learn more at inquest.net

inquest.net
+1-866-982-0561
sales@inquest.net