Dataminr

Dataminr for Cyber Defense & Inquest

Proactive Protection for Organizations: Integrating Dataminr for Cyber Defense with InQuest InSights for Enhanced Cybersecurity

The Challenges

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 Dataminr for Cyber Defense & 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 Dataminr for Cyber Defense 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 Dataminr for Cyber Defense.

How to Get Started

Request a demo on our website. To learn more about this particular integration, contact sales@dataminr.com. If you're an existing customer, please reach out to your customer success manager.

Get Results with Dataminr for Cyber Defense & Inquest

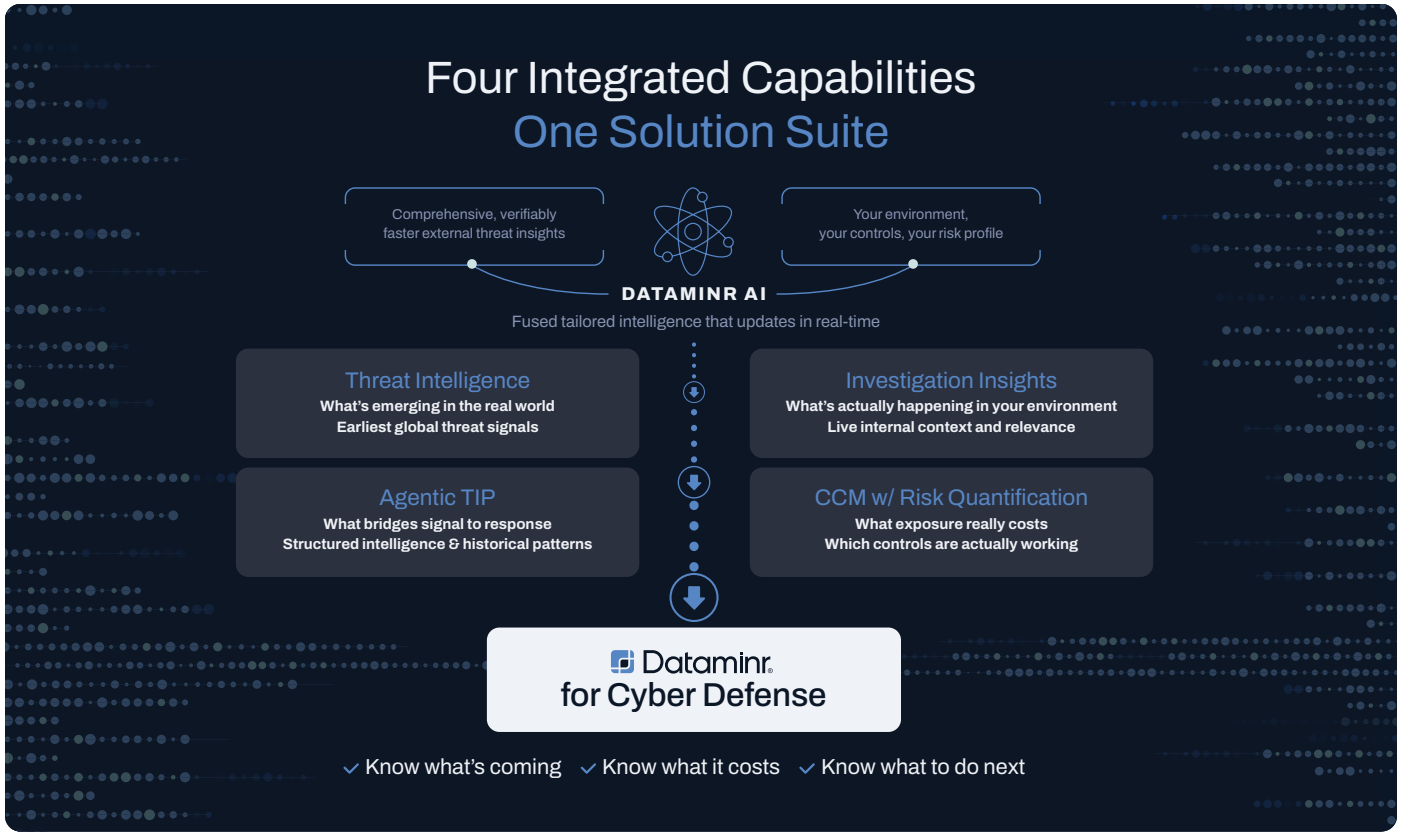
Incorporating InQuest InSights threat intel in Dataminr for Cyber Defense gives CTI and Security Operations teams a powerful way to use that intelligence across the range of technologies that integrate with Dataminr for Cyber Defense, for a variety of use cases, like:

- **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.

Four Integrated Capabilities
One Solution Suite



Client-Tailored
Threat Intelligence (CTTI)

Real-Time Threat Insights, Full-Stack Context

Detect emerging threats and exploits from the earliest signal with Dataminr Client-Tailored Threat Intelligence (CTTI), and instantly search across your security stack without pivoting.

Early-Signal Threat Detection
Agentic AI Adversary Intel
Cross-Stack Security Search
No Syntax, No Context Switching

Agentic TI Ops

From First Signal to Finished Intelligence — Automatically

Instantly discover emerging vulnerabilities, exploits, and zero-day attacks with detailed context on trending CVEs, CVSS/EPSS scores, and threat actor TTPs.

Embedded Dataminr CTTI Tooling
Intel-First Playbooks & Automation
Unified Threat Library & Reporting
Intel Hub with 125+ Integrations

Predictive Threat
Exposure Management (PTEM)

Exposure Prioritized by Risk, Quantified by Impact

Proactively prioritize vulnerabilities with continuous rationalization of high-efficacy exploit signals, attack surface context, compensating controls, and financially quantified risk.

Intel-Driven Risk Prioritization
Automated Attack Path Modeling
MITRE-Level Financial Modeling
Continuous Control Monitoring (CCM)

Dataminr for Cyber Defense

Activate a Unified, Multi-Modal Cyber Defense Fabric

Extend, tailor, and fuse cyber risk insights and context across Dataminr solutions for a shared, continuously adapting view of security, threat, and exposure priorities to drive agentic, threat-informed defense.

Threat Intelligence | Investigation Insights | Agentic TIP | CCM w/ Risk Quantification

Power the Future of Cyber Defense with Dataminr

dataminr.com