Dataminr

Dataminr for Cyber Defense & Spur

Counter Attacks and Fraud with High-Fidelity IP Address Context

The Challenge

Threat intel analysts, threat detection engineers, SOC analysts, hunters, and incident responders can spend a lot of effort manually collecting context on IP address indicators, which takes away from doing the critical parts of their job - analyzing intel and threats, and responding to attacks.

Why Dataminr for Cyber Defense & Spur

The Spur Playbook App for Dataminr for Cyber Defense makes gaining rich context on IP addresses fast and easy. Spur enables organizations to gain advanced detection of anonymization and threats to counter fraud and other malicious activity. Using Dataminr for Cyber Defense's drag and drop, low-code Playbook automation, it's easy to quickly integrate Spur's IP address insights into any automated process or task. Every time context on an Address Indicator in Dataminr for Cyber Defense is needed, it saves analysts time and effort.

Get Results with Dataminr for Cyber Defense & Spur

Spur Context-API is a REST API service providing detailed IP context. It offers rapid IP search with actionable data, including client behaviors, geographical concentration, and associated risks. Spur integrates with Playbook automation in Dataminr for Cyber Defense through the Context-API Playbook App making it easy to incorporate Spur into your new and existing tasks and processes.

Spur provides the following context about an IP address:

- Autonomous System Details
- Client Behaviors
- Geographic Concentration
- Risks and Threats
- Infrastructure Classification
- Organization Details
- Services Running
- VPN/Proxy details

Key Benefits

Reduce manual effort collecting IP address context

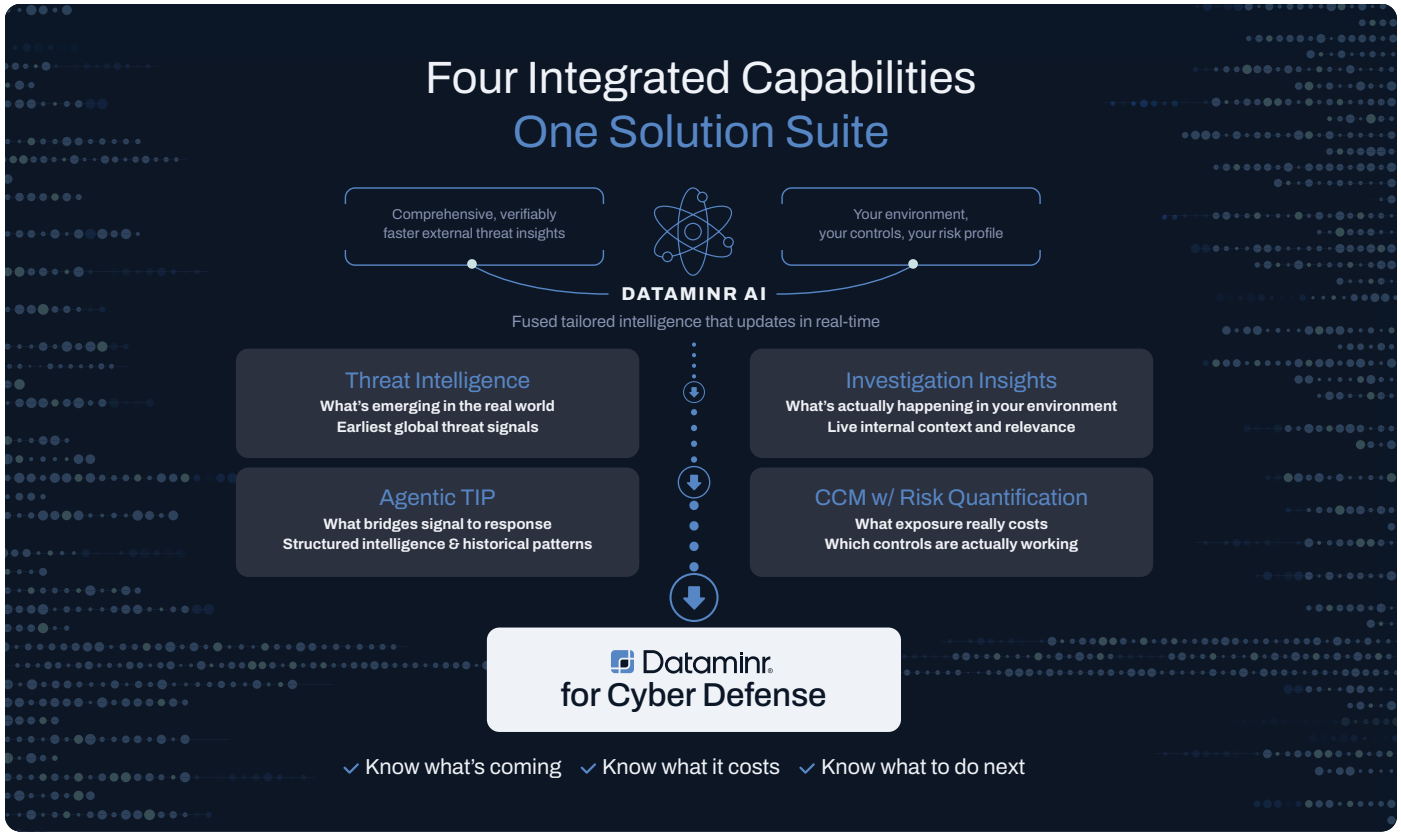
Enhance threat detections for malicious and fraudrelated activities

Speed up threat intel and detection analyses, and response

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.

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