Dataminr

Dataminr for Cyber Defense & Elastic Security

Amplify Threat Detection and Response in Elastic with the Power of Dataminr for Cyber Defense

The Challenges

Analysts monitoring, analyzing, and responding to threats are drowning in alerts, with limited means to determine which alerts and incidents are the most critical to address in order to protect the organization. Add to that all the false positives analysts have to contend with, and it creates an even more stressful situation. This leads to missed alerts, longer times to detect and respond to threats, and stressed-out staff.

Why Dataminr for Cyber Defense & Elastic Security

The combination of Elastic Security and the unified, highfidelity threat intelligence supplied by Dataminr for Cyber Defense enables SOC analysts, incident responders, and threat hunters to do their work faster, with greater effectiveness and efficiency, making their organizations more resilient to cyber attacks.

Get Results with Dataminr for Cyber Defense & Elastic Security

A native integration in Elastic along with Job and Service Apps in Dataminr for Cyber Defense allows the platforms to be connected in minutes. The integration enhances a range of use cases, like:

Threat detection, monitoring, and analysis: Leverage native threat scoring in Dataminr for Cyber Defense to optimize the Indicators sent to the Elastic Platform to improve threat detection and prioritization, while minimizing false positives.

Incident response: Reduce MTTD and MTTR through faster, more precise alert triage in Elastic leveraging relevant intel and rich context provided via Dataminr for Cyber Defense.

Threat hunting: Make threat hunting more robust and effective by leveraging relevant intel to define your hypotheses and starting points for hunts. Threat Graph in Dataminr for Cyber Defense augments the Elastic Platform for digging into threat intel and uncovering new relationships and threat actor insights.

Key Benefits

Strengthen threat detection, analysis, and response

Prioritize and respond to incidents with speed and accuracy

Make threat hunting more effective and productive

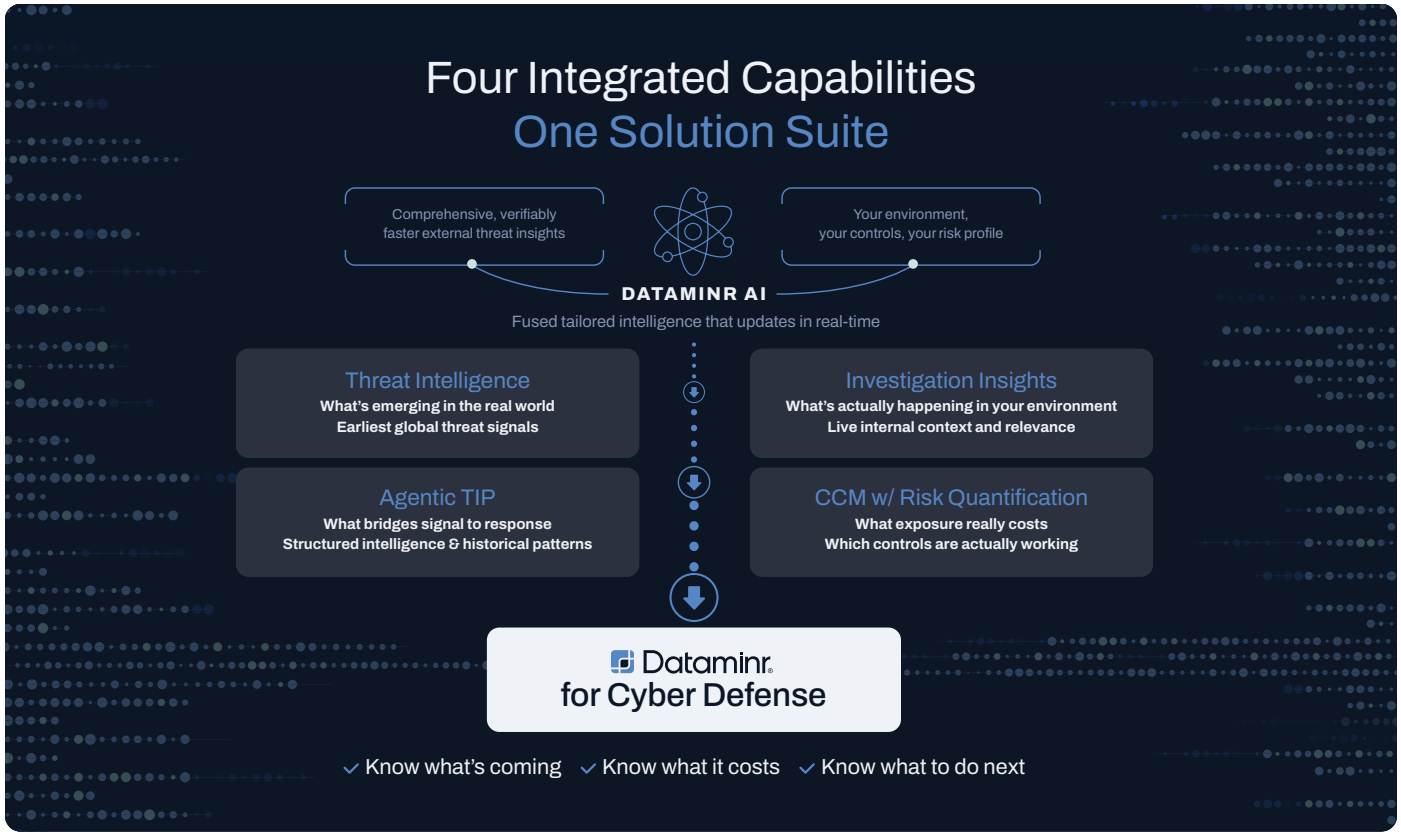
Highly customizable integration enables higher-fidelity intel use in Elastic

Not just a feed of raw indicators. Easily access additional intel context and relationship data in 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.

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