Dataminr

Dataminr for Cyber Defense & Recorded Future

Enhance Attacker Insights and Defenses

The Challenges

Over 25,000 new vulnerabilities emerge monthly, on average. Cybersecurity analysts need a better way to prioritize the new vulnerabilities that matter for defending their organization, and monitor existing vulnerabilities for being weaponized with an exploit. This process requires significant effort to monitor, review, and determine which vulnerabilities are applicable, and then prioritize the ones for remediation that create the greatest risk to the business. This leads to wasted resources, gaps between disclosure, exploitation and remediation, friction between the cybersecurity and IT teams, and ultimately, analyst burnout.

Why Dataminr for Cyber Defense & VulnCheck?

VulnCheck's unprecedented visibility into the vulnerability ecosystem enables organizations to get ahead of threat actors and reduce an organization's attack surface before an attack occurs. The VulnCheck App for Dataminr for Cyber Defense integrates VulnCheck's vulnerability and exploit intelligence, with its insights pushed directly into Dataminr for Cyber Defense.

Combining the power of VulnCheck's vulnerability intel with Dataminr for Cyber Defense enables cybersecurity teams to gain a broad-view of the threat landscape. This combined power enables analysts to achieve greater precision in determining which vulnerabilities are the most critical to address to protect the business data in Dataminr for Cyber Defense, along with associated context, enabling cybersecurity teams to know and take action when events are happening that could potentially threaten and impact their organization.

Get Results with Dataminr for Cyber Defense & VulnCheck

The VulnCheck integration with Dataminr for Cyber Defense ingests vulnerability and exploits details into TI Ops, bringing a richness of data for vulnerabilities, such as the description, CVSS scores and severity, CPE data, CISA KEV, exploit details and timelines, and threat actor usage and attribution. It also provides context on IP addresses with known vulnerabilities. The integration supports Vulncheck's Exploit and Vulnerability Intelligence and Initial Access Intelligence, as well as Community solutions like KEV, NVD++, and XDB, for use cases like Emerging Threat Monitoring and Vulnerability Prioritization.

Key Benefits

Get a unified view

via a singular source of vulnerability intelligence and analysis out-of-the-box, removing the need to collect and process data from disparate sources and for humans to perform manual analyses.

Gain novel insights

into vulnerabilities and exploits with in-depth details on vulnerabilities and threat actor activity.

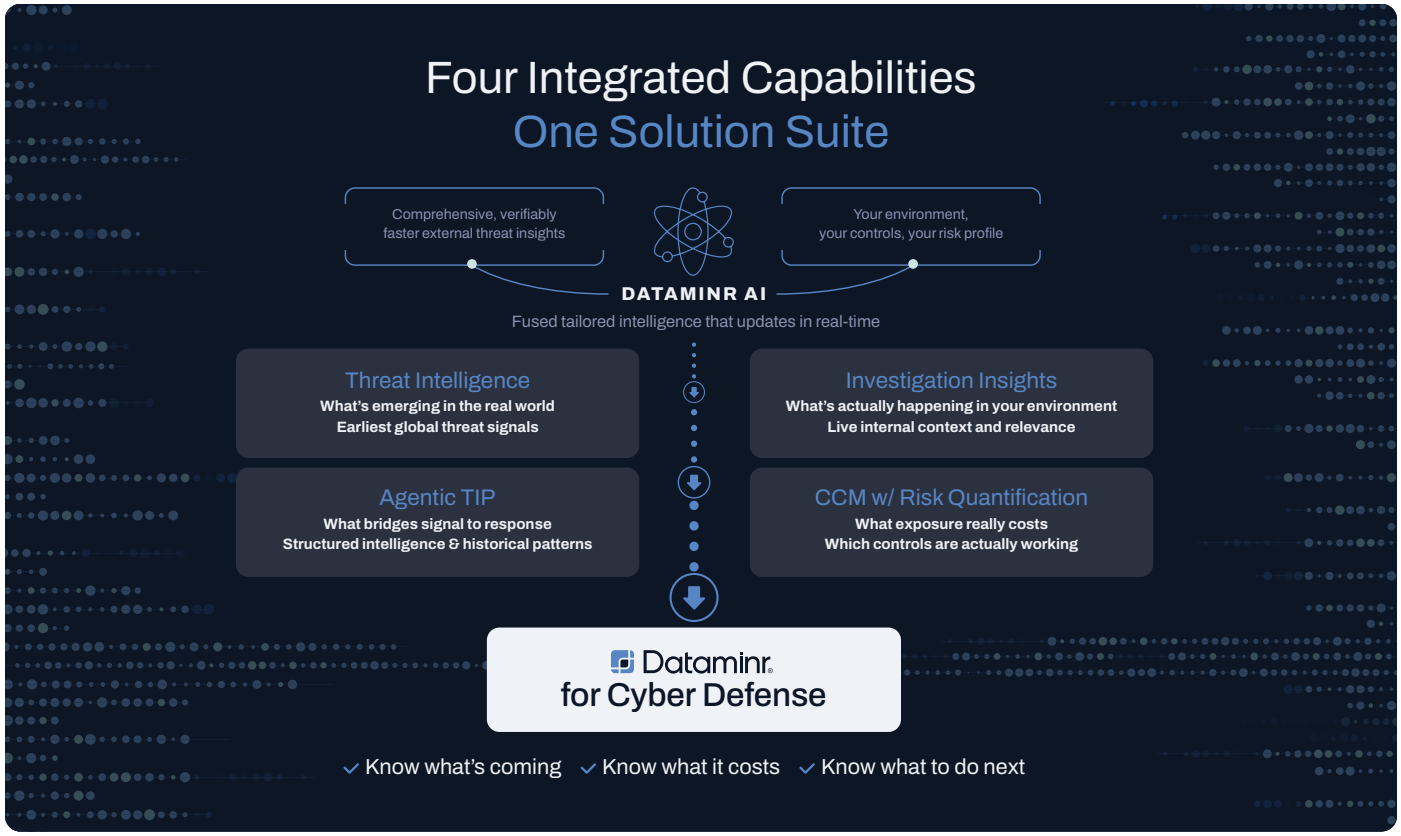
Automate monitoring

of emerging threats and exploits as "early warning indicators", and get specifics on the timeline of exploit development.

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