Dataminr | splunk> a CISCO company

Close Gaps Across Digital, Physical, and Third-Party Risk with Real-Time, AI-Powered Alerts

Without External Context, Even the Best Security Teams Fall Behind

Security teams today face critical blind spots:

- **Limited real-time third-party risk monitoring:** Delayed incident notifications and point-in-time vendor assessments leave you exposed
- **Reactive cybersecurity:** Alerts arrive too late, and the context needed to understand true risk is missing
- **Alert overload:** Staff are stretched thin and can't prioritize response
- **Lack of immediate situational context:** Legacy threat data is too slow to match the pace of attacks
- **Disconnected cyber and physical security:** Siloed tools and teams miss cross-domain threats

40% of compliance leaders

say that between 11% and 40% of their third parties are high-risk[1]

50% of organizations

50% of organizations lack the skilled staff to perform threat hunting[2]

70% of organizations

plan to deploy cyber-physical security platforms as the first step in their security journey[3]

Detect Threats Earlier and Act Faster

Dataminr amplifies Splunk's powerful data analytics and automation platform by adding AI-powered external threat detection from over one million public sources that enriches your security telemetry with relevant context for faster response. Key components include:

- Pre-built dashboards
- Rich metadata
- IoC dashboard
- Splunk CIM integration
- Security Threat Intelligence framework alignment

Increase the Value of Your Splunk Investment

Enhance security operations efficiency

Accelerate response with contextualized threats, prioritization, and automated workflows by integrating Dataminr alerts with Splunk security telemetry

Amplify third-party and cyber-physical risk detection

Continuously monitor vendors, supply chains, and critical infrastructure to mitigate cyber and operational vulnerabilities

Enable proactive security

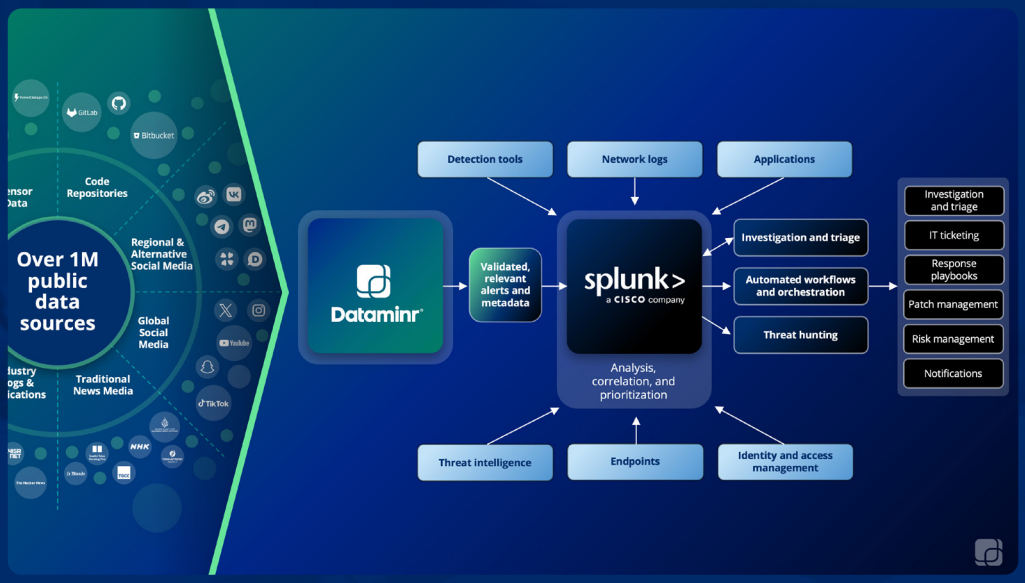
Mitigate threats faster and maintain business continuity with real-time alerts on cyber, physical, and third-party risks

Increase enterprise resilience

Automate threat detection and response workflows, reducing manual efforts, MTTR, and costs due to fines or downtime

From Alert to Action: Security Use Cases Across Your Enterprise

Mitigate Third-Party Risk	Proactively add third-party accounts to Splunk watchlists to increase monitoring sensitivity
Adopt Continuous Threat Exposure Management	Establish a preemptive security approach that continuously scans for emerging threats and vulnerabilities, enabling prioritized response
Converge Cyber and Physical Security	Unify security across cyber and physical domains to identify threats, facilitate coordination between teams, and improve security posture



Dataminr and Splunk: A Unified Approach to Threat Detection and Response

Better Together

Dataminr and Splunk deliver comprehensive security, visibility, and proactive action. The integration empowers you to identify emerging threats faster, understand how they impact your organization, and respond automatically through orchestrated workflows—all within your existing Splunk environment.

Recognized as a global leader in AI and trusted by over half of the Fortune 100, Dataminr supports public and private sector organizations across more than 100 countries. Its powerful AI platform monitors more than one million public data sources in over 150 languages.

Learn more about Dataminr Pulse for Cyber Risk at www.dataminr.com/products/pulse/cyber-risk

Sources

1. Gartner, Third-Party Risk Management Best Practices, Oct 2024
2. SANS Institute, SANS 2024 Threat Hunting Survey: Hunting for Normal Within Chaos, Mar 2024
3. Accenture, Operational technology and product security, accessed Mar 2025

Start building your real-time, location-aware response.