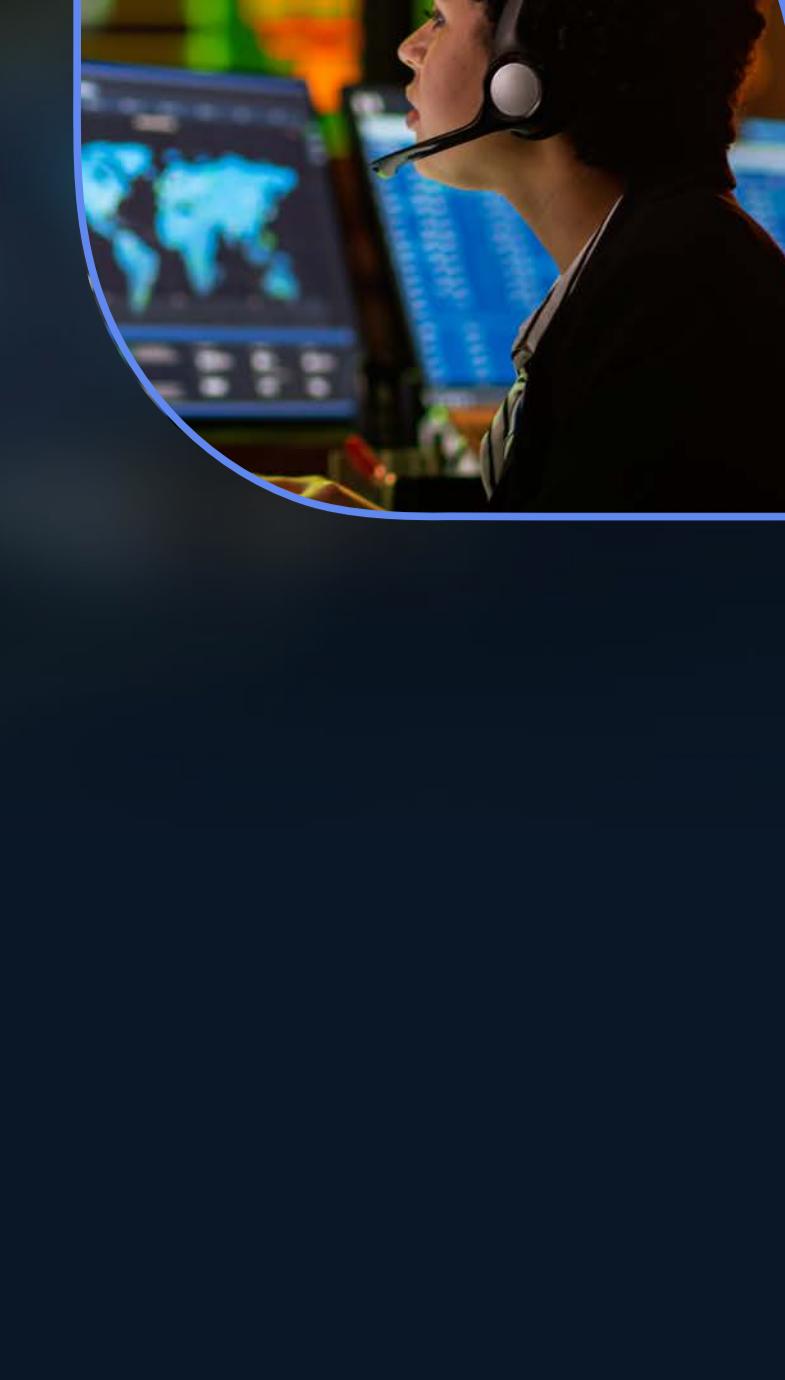


# Supercharge Security with Real-Time Threat Detection and Automation



Your attack surface is expanding—your visibility should too.

Dataminr amplifies Splunk's powerful data analytics and automation platform with AI-powered external threat detection, combining actionable alerts with your security telemetry. When risks emerge, receive instant alerts to take proactive action and automate response within your existing Splunk environment.

## Data Gaps Are Growing—And So Is the Risk

### THIRD-PARTY RISK

**23%**

of all incurred cyber insurance losses in 2024 were tied to vendors or suppliers<sup>1</sup>

### SKILLED STAFF SHORTAGES

**61%**

of organizations cite a shortage of skilled staff as the biggest barrier to effective threat hunting<sup>2</sup>

### SWIFT EXPLOITATION

**<48 mins**

is the avg. breakout time for adversaries, down from 62 mins the year prior<sup>3</sup>

## Limited Visibility and Overloaded Teams



### Limited third-party monitoring

Lack of visibility beyond organizational boundaries



### Reactive detection and delays

Threats surface late due to outdated legacy intel



### Vulnerabilities that demand urgent action

Teams can't keep pace with fast-moving risks



### Alert overload and prioritization gaps

Too many alerts and no idea what's important



### Slow, manual remediation processes

Delayed responses give attackers more time to exploit



### Analyst burnout

Manual process, too many tools taking a toll on teams

## How Dataminr + Splunk Help You Mitigate Risk

Dataminr real-time alerts connect directly with Splunk Enterprise, Splunk Cloud, or Splunk SOAR, making it easy to visualize threats, automate response, and take action faster—all within the tools your team already uses.



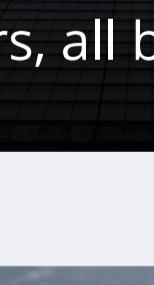
### Rich metadata

Dataminr alerts include 100+ fields to drive precision and automation



### Automation

Trigger SOAR playbooks automatically based on early warning signals



### CIM integration

Use external Dataminr alerts for both built-in and custom dashboards



### IoC correlation

Map alerts to internal telemetry to improve threat hunting

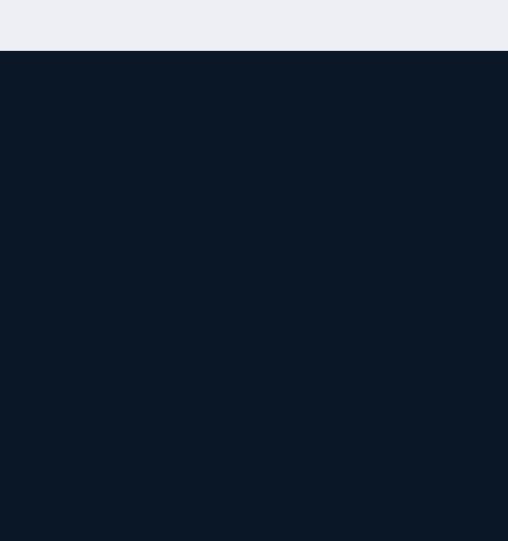


### Pre-built dashboards

Visualize alerts and events in Splunk with out-of-the-box dashboards

## High-Value Gains You Can Measure

With Dataminr + Splunk, you can enhance security, resilience, and operational efficiency by proactively identifying, analyzing, and responding to emerging, cyber, physical, operational, and reputational risks.



### Operational efficiency

Cut through noise and focus on the most important threats



### Faster response times

Accelerate detection, prioritization, and remediation



### Proactive defense

Identify threats early and act before they escalate



### Continuous visibility

Reduce risk with real-time threat exposure management



### Stronger ROI

Maximize the value of your existing Splunk investment

## Turning Data Into Action

### Mitigate Third-Party Risk

#### Financial services organization

A global bank receives an alert just minutes after a vendor is hit with ransomware. The security team takes action to prevent downstream impact while an automated workflow notifies internal stakeholders, all before they receive word from the vendor.



#### National energy provider

A power company is alerted to a zero-day exploit targeting its operational technology (OT) infrastructure. Flagged by Dataminr and correlated in Splunk, the team links it to internal assets and triggers automated patching—avoiding costly disruption.

## Let's Make an Impact Together

Make the most of your Splunk investment with AI-powered, real-time threat intelligence. Join the organizations transforming security with the Dataminr + Splunk joint solution to expand visibility, accelerate threat detection, automate response—and keep your organization ahead of emerging threats.

Talk to our team today and let's build a smarter cyber defense—together.

[Learn more](#) about Dataminr Pulse for Cyber Risk

### Sources

1. Resilience Cybersecurity's Biggest Blind Spot: Third-Party Risk, New Resilience Analysis Finds, Feb 2025.

2. SANS Institute, 2025 SANS Threat Hunting Survey, Mar 2025.

3. CrowdStrike, 2025 Global Threat Report: Beware the Enterprising Adversary, Feb 2025.