Dataminr | splunk> a cisco company | AC3

Supercharge Security with Real-Time Threat Detection and Automation

Overview

Your attack surface is growing—so should your visibility. Dataminr enhances Splunk's powerful data analytics and automation capabilities with AI-driven external threat detection. It delivers actionable alerts combined with your security telemetry, enabling you to take swift, proactive action and automate responses within your existing Splunk environment.

Data Gaps Are Growing—And So Is the Risk

THIRD-PARTY VISIBILITY

40% of compliance leaders report a significant portion of third-party relationships are high risk[1]

SKILLED STAFF SHORTAGES

50% of organisations cite a shortage of skilled staff as the primary obstacle to effective threat hunting[2]

EXPANDING ATTACK SURFACES

30 billion IoT devices predicted by 2030 will vastly increase the cyber-physical attack surface[3]

Expand Your Visibility Externally

Inadequate third-party monitoring
Lack of visibility beyond organisational boundaries

Alert overload with poor prioritisation
Too many alerts and no idea what's important

Disconnected cyber and physical systems
Siloed systems miss threats that cross domains

Slow, manual remediation processes
Delayed responses give attackers more time to exploit

Vulnerabilities requiring urgent action
Teams can't keep pace with fast-moving risks

Delayed detection from outdated intelligence
Threats surface late due to outdated legacy intel

How Dataminr + Splunk Helps You Manage Risk

Real-time alerts from Dataminr integrate seamlessly with **Splunk Enterprise**, **Splunk Cloud**, and **Splunk SOAR**, helping you visualise threats, automate responses, and act faster—within tools your team already uses.

Rich metadata
Over 100 alert fields support precision and automation.

Automation
Trigger SOAR playbooks based on early warning indicators.

CIM integration
Use Dataminr alerts in default and custom dashboards.

Pre-built dashboards
Visualise alerts and events in Splunk instantly.

IoC correlation
Map alerts to internal telemetry to improve threat detection.

High-Value Gains You Can Measure

With **Dataminr + Splunk**, strengthen your security, resilience, and operational performance by proactively identifying, analysing, and responding to cyber, physical, operational, and reputational threats.

Operational efficiency
Cut through alert noise and focus on critical risks.

Continuous visibility
Reduce risk through real-time threat exposure management.

Faster response times
Quicken detection, prioritisation, and mitigation.

Stronger ROI
Maximise your Splunk investment.

Proactive defence
Detect threats early and intervene before escalation.

Examples Across Sectors

Organisations across industries are using integrated, AI-powered alerting to detect threats earlier, respond more quickly, and stay ahead of risk.

Financial Services
MITIGATING THIRD-PARTY RISK
A global bank receives an alert minutes after a vendor suffers a ransomware attack. Security teams act promptly, and automated workflows notify internal stakeholders—before the vendor communicates the incident.

Public Sector
CYBER & PHYSICAL SECURITY CONVERGENCE
A government agency receives real-time alerts of suspicious activity near a secure site. Simultaneously, login anomalies appear in Splunk. With unified insights, the agency escalates its response and prevents compromise.

Energy Sector
CONTINUOUS THREAT EXPOSURE
A power provider is alerted to a zero-day exploit affecting its OT infrastructure. Detected by Dataminr and correlated in Splunk, the team links it to internal assets and automatically patches the issue, avoiding major disruption.

Let's Make an Impact Together

Unlock greater value from your Splunk deployment with real-time, AI-powered external intelligence. Join other forward-thinking organisations who are boosting their visibility, speeding up threat detection, and automating their responses.

Talk to our team today to strengthen your cyber defence—together.

AC3
At AC3, we bring clarity to the cloud. If you are looking for experts in secure cloud, we can help. We have the people, expertise and the technology to deliver.

Learn more about real-time external context with Dataminr and Splunk by visiting www.ac3.com.au

Sources
1. Gartner, Third-Party Risk Management Best Practices, Oct 2024.
2. SANS Institute, 2024 Threat Hunting Survey: Hunting for Normal Within Chaos, Mar 2024.
3. Statista, IoT Connections Worldwide, Jun 2024.