Dataminr

Checklist

How to Leverage Real-Time Intelligence to Eliminate Risk Blind Spots

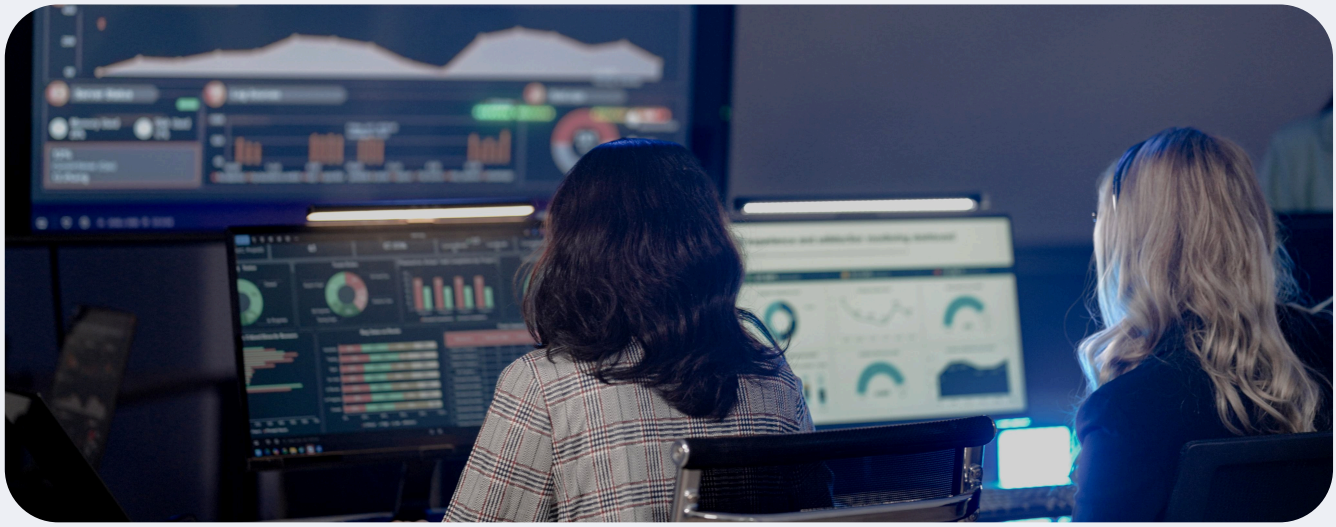
Go from chaos to clarity with
AI-powered real-time intelligence

Today's public and private sector organizations face increasingly complex, diverse, and domain-agnostic threats with far-reaching impacts. In the face of those threats, many security teams are still operating in an environment of fragmented data and organizational silos. Traditional security strategies must evolve beyond functional priorities to focus on events and threats with the potential for risk across the entire organization.

This will be achieved using AI-powered, real-time intelligence to provide a proactive, holistic view of events, threats, and risks across the entire organization. A re-imagination of the role security plays in the broader organizational strategy will be required, as well as how internal security teams operate and collaborate with each other and vendors.

Evaluate your own organization's readiness for the expanding risk landscape with Dataminr's Risk Readiness Checklist

- [ ] Educate the executive team on the expanding risk landscape and potential business impacts to establish a baseline understanding of broader security trends and goals.
- [ ] Design security operations through a holistic lens which accounts for the organization's risk appetite and incorporates all potential areas of threat: cyber, physical, reputation, operations, legal, human resources, etc.
- [ ] Establish strategic risk committees to facilitate strong collaboration between teams to account for cross-domain threats. These teams must agree to a response plan when risks in one domain impact other domains.
- [ ] Develop risk and security activities that align with business priorities (identified in company 10k and other places) and organizational needs versus team-level needs and priorities.
- [ ] Establish standardized risk calculations and a standard risk framework to be utilized across the organization. Avoid team-by-team risk scores.
- [ ] Confirm all security and risk teams have access to the same threat data regardless of domain or business unit.
- [ ] Verify all security tools are integrated and streamlined to deliver a comprehensive, single pane of glass view of event, threat, and risk intelligence across the organization. Avoid fragmented, multi-platform security strategies.
- [ ] Ensure all third-party vendors meet standardized cross-domain security practices and needs for each security and risk team.
- [ ] Integrate a platform that utilizes AI-powered, real-time intelligence to share critical event, threat, and risk data and delivers actionable, evolving insights.



Dataminr Guide to the Expanding Risk Landscape

For any organization aiming to thrive—or even simply ensure continuity—the ability to act on real-time intelligence is no longer an advantage; it is the bedrock of resilience. The days of siloed, reactive risk management are over. Today's leaders require a proactive, holistic view to effectively govern in an uncertain world. Learn how in this eBook.

READ THE eBOOK