Dataminr®

How to Extract Actionable Intelligence Using AI Across Public Data For Preemptive Third-Party Risk Management

Risks arising from third-parties are increasing precipitously, making third-party risk management a top priority for organizations today. The exponential rise in SaaS subscriptions, cloud storage, and the use of software with open-source code are radically expanding the attack surface.

Security magazine reports that third-party attacks account for fully **29%** of data breaches, and **nearly half of energy sector breaches.**

Organizations invest heavily in continuous monitoring inside their enterprise perimeter, but they are not able to continuously monitor their third parties.

Third-party risk is especially difficult to manage, primarily because:

- Organizations have no direct oversight, control, or management of their third parties
- Organizations have constrained resources and can't scale to match the ever-expanding attack surface
- Threat actors increasingly target third parties, as they are often softer targets and offer broader downstream impact

Organizations invest heavily in continuous monitoring inside their enterprise perimeter, but traditional tools are not designed to continuously monitor their third parties.

As such, they rely upon contractual obligations, manual and reactive risk scoring, attestations, and audits to manage third-party risk. While these are essential, they provide only a retroactive snapshot in time.

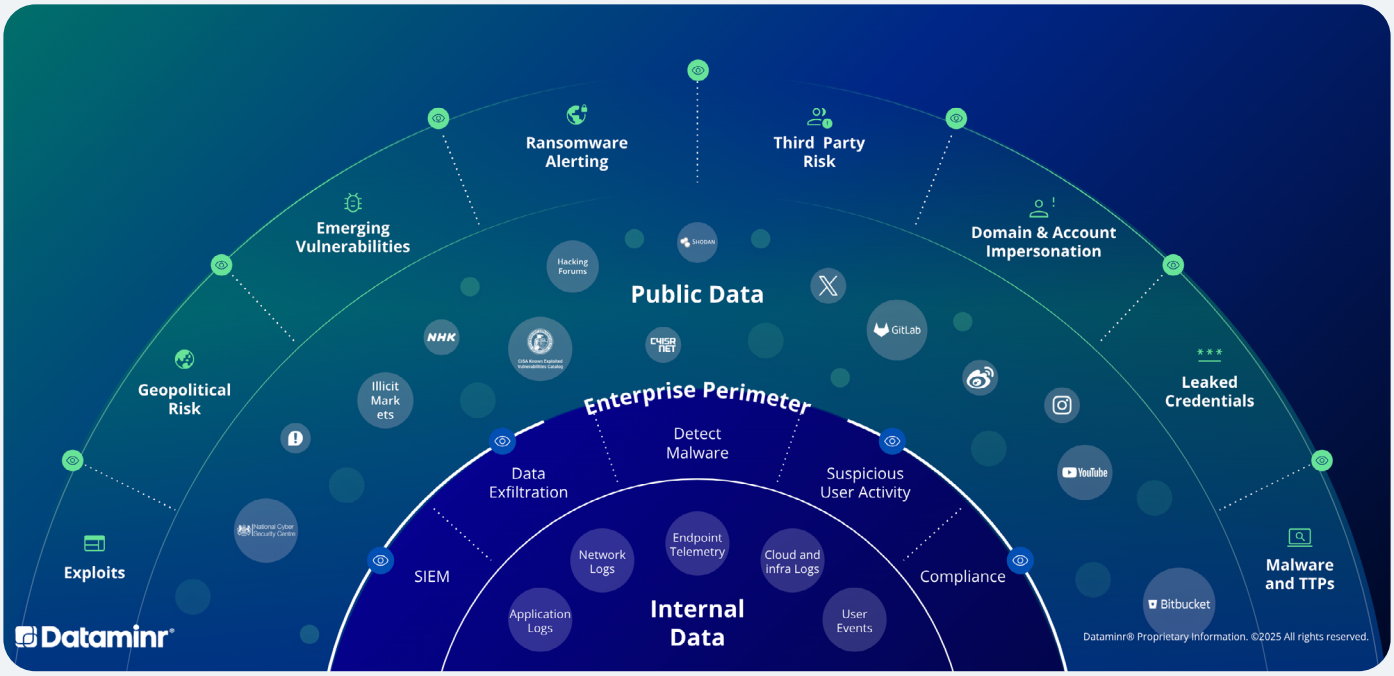

FIGURE 1: Digital transformation is continuously expanding the risk surface area

What if you could continuously monitor third parties for the first indication of risk? That would significantly reduce your mean time to detect and respond. But how?

While you don't have direct visibility into your third parties, you do have access to public data that has essential information for cybersecurity teams—in blogs, social media, code repositories, corporate disclosures, sensor data, and the deep and dark web, etc. (see **FIGURE 1**). And yet, it can be difficult to extract actionable signals from public sources, because:

How can you cut through the noise of public information to find early and actionable third-party risk signals? Through well-trained and carefully-tuned domain-specific AI models.

- There are millions of sources and billions of metadata produced every day
- Sources exist in multiple modes (audio, video, text, images) and in hundreds of different languages
- Signals contain a lot of inaccurate, irrelevant, and noisy information
- It's hard to find and stay up-to-date on the most recent information

So, how can you cut through the noise of public information to find early and actionable third-party risk signals? Through well-trained and carefully-tuned domain-specific AI models.

Dataminr Pulse for Cyber Risk ingests information from over 1 million publicly-available data sources in over 150 languages across more than 220 countries and territories to detect external cyber risks, events, and threats in real time (see **FIGURE 2**).

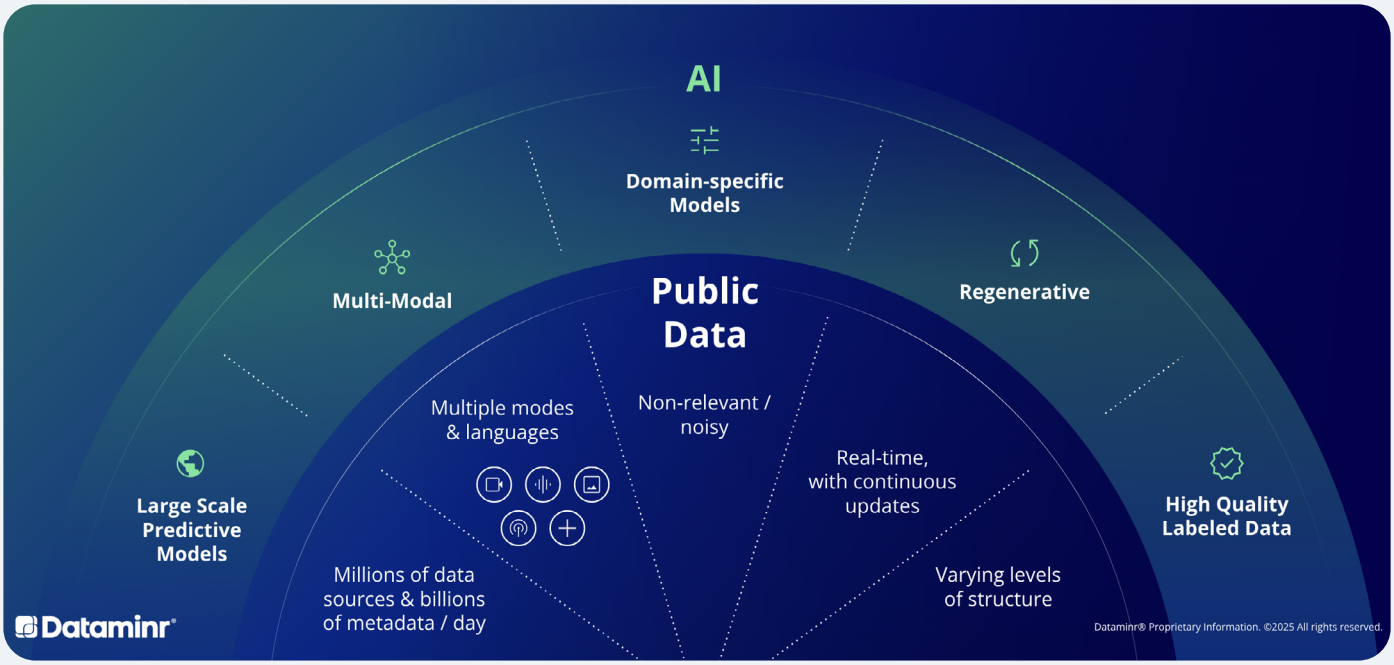

FIGURE 2: Spot the earliest indicators of external threats and vulnerabilities with Dataminr Pulse for Cyber Risk

Dataminr overcomes the public data challenges by:

- Leveraging a suite of domain-specific AI models (including large scale predictive models)
- Employing a comprehensive and highly-detailed knowledge graph
- Building upon over 12 years of training on domain-specific results

Dataminr Pulse for Cyber Risk provides continuous monitoring outside of your enterprise perimeter to identify and alert you to relevant cyber threats that you can filter and frame according to your specific needs—and integrate and automate into your preferred workflows, such as your SIEM, SOAR, or TIP solutions (see **FIGURE 3**). Dataminr delivers unmatched value in terms of:

- **Speed.** Proactively manage risk by knowing at the earliest possible time and acting quickly.
- **Scope.** Avoid missed threats with broad and granular visibility across public data sources and formats.
- **Relevance.** Focus teams on prioritizing and managing risk, not searching for it.

CASE STUDY

Global Payments Reduces Third-Party Risk with Dataminr Pulse for Cyber Risk

Global Payments is a Fortune 500 worldwide financial and payments technology company working with 4.6 million merchant accounts, 4,000 technology partners, and 1,500 financial institutions in more than 100 industries.

Challenge

As a global commerce platform that serves and partners with numerous organizations and industries, Global Payments is especially

FIGURE 3: How Dataminr Pulse for Cyber Risk works

susceptible to third-party cyber risk. It's imperative that "our third-party suppliers tell us when they have a problem before we find out that they have a problem," said Mike Kane, vice president of Cyber Security Operations at Global Payments. "It's a scary thing. It's what keeps us up at night." In particular, zero-day vulnerabilities and leaked credentials on the dark web—whether they pertain to Global Payments, its third-party vendors, or one of its 25-plus subsidiaries—are of the biggest concerns for Kane and his team. They needed to build a robust threat intelligence system that would notify them as soon as a risk emerges.

Solution

Once Kane and his team integrated Dataminr into their cyber threat intelligence platform, they were better able to identify vulnerabilities as they occurred—giving them the lead time needed to, as Kane puts it, "prevent a catastrophic event." "Dataminr is very centric to [our threat intelligence] in which we're monitoring our third-party supply chain and looking for anything that's hitting social media, news cycles, whatever it happens to be," said Kane. "We're notifying third-party suppliers that they've got a problem before they know that they have a problem."

Additionally, Kane has found Dataminr's ReGenAI—a new combination of predictive and generative AI—highly valuable and effective in helping his team maintain situational awareness and an understanding of cyber risks. This is due to ReGenAI's ability to distill multidimensional events into concise briefs that dynamically update in real time, enabling Kane and his team to gain rapid understanding of risks and events as they unfold.

"[Dataminr's ReGenAI] makes Dataminr Pulse for Cyber Risk more of an asset to us because we're able to say, 'I just saw this in three different places.

Let me give you a briefing of that. Also, we saw this a couple of months ago and here's what we did about that, or here's what was said about that,'" said Kane. "Bringing all of that together gives us a truer picture."

Outcome

Now that Kane and his team have more comprehensive visibility into their third-party cyber risk exposure, they can swiftly take the right course of action when a critical incident occurs. This includes notifying key stakeholders within and outside of the organization so that each team can activate its response plans in a timely manner.

"It's the speed at which we're able to identify and say, yes, this is relevant, or no, this is not relevant. And notify the people that need to know," said Kane.

Dataminr Pulse for Cyber Risk strengthens your cyber resilience with early and actionable intelligence for adopting a preemptive defense strategy, so you can:

- **Identify Digital Risk.** Respond quickly to early warning of risks to your organization's digital assets.
- **Expose Third-Party Risk.** Mitigate risks to your organization with increased visibility into threats to your subsidiaries and third parties.
- **Receive Vulnerability Intelligence.** Prioritize patching with visibility to the entire lifecycle of a vulnerability.
- **Respond to Cyber-Physical Risk.** Respond to real-time intelligence on cyber threats affecting physical assets, and vice versa.

Learn More

Dataminr's mission is to help security teams take faster actions against emerging risks and threats using publicly-available information. Detecting security events in the public domain, recognizing their relevance, and delivering them to the appropriate organization with the appropriate context so that cyber professionals can take the appropriate mitigation is the key to Dataminr's advantage.

For more information, visit **dataminr.com**