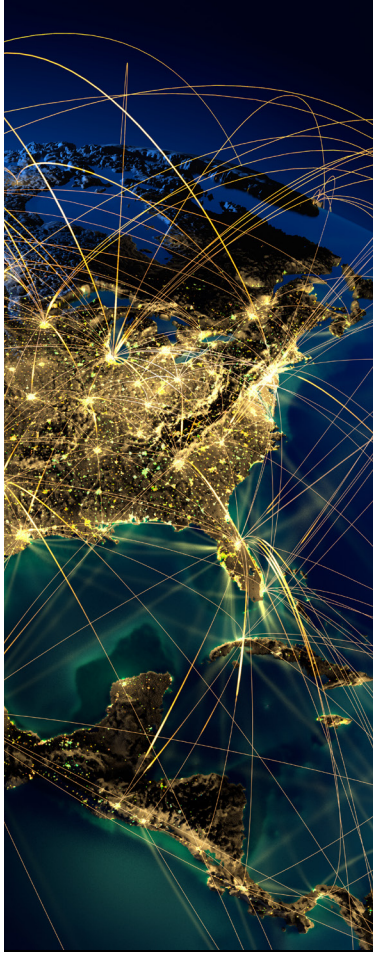
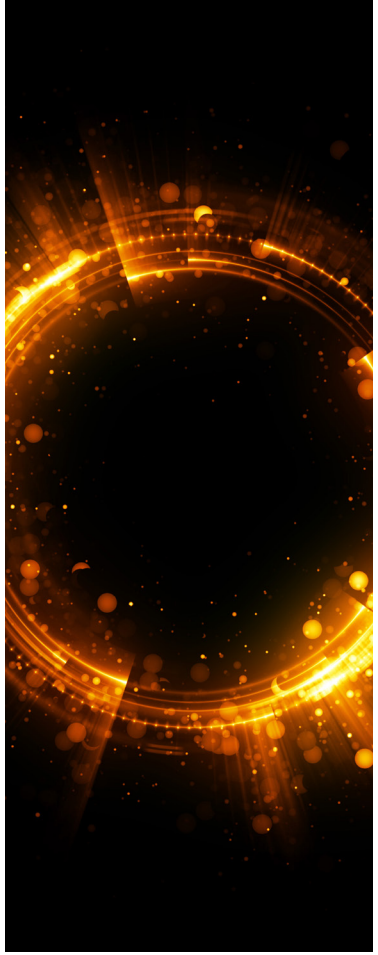
Dataminr

Dataminr Checklist

Optimizing Data Collection for Actionable Threat Intelligence

Analyze your current data collection to ensure you're getting the most expansive, precise, and clearest picture of the external threat landscape pertinent to your organization.





More Data Doesn't Correlate to Stronger Defenses

The cybersecurity landscape is evolving quickly, with threat actors employing sophisticated tactics not only targeting companies, but their subsidiaries and third-party vendors as well. Facing 600 million attacks daily from both cybercriminals and nation-state actors, cyber intelligence teams are facing the daunting task of safeguarding their organizations while plagued by:

1. INFORMATION OVERLOAD:

The sheer volume of data generated by various sources, such as logs, alerts and threat feeds, has become overwhelming. Analysts receive around 500 security alerts daily—this number can get up to 3,000 for larger enterprises. In a recent survey by Vectra AI, more than 50% of SOC practitioners said they cannot keep pace with the fast-growing number of cyber threats.

2. FALSE POSITIVES:

It's difficult for threat intelligence analysts to distinguish genuine threats from false alarms due to massive amounts of data, which lead to wasted time and resources. Out of the threat alerts addressed by analysts, only 16% are real attacks, according to Vectra AI.

3. LACK OF STANDARDIZATION:

Organizations with multiple security tools are more prone to having non-standardized formats for sharing threat intelligence, causing inefficiencies that hinder mean times to detect, acknowledge, contain, resolve and recover from an incident.

The Need for Dynamic Tools With Robust, Contextual Data Sourcing

Analysts require seamlessly integrated applications that offer optimized, dynamic tools and robust, contextual data sourcing within their existing workflows for effective management of today's constantly evolving risk landscape and attack intelligence, allowing them to focus on taking action.

When evaluating current data collection, it is imperative cybersecurity leaders answer three questions at scale to ensure they are able to properly operationalize cyber threat intelligence tools:

1. Is the information provided relevant to my organization?
2. Does the information support our cybersecurity threat intelligence strategy?
3. Does the provided information warrant action?

A 'no' answer to any of these questions suggests it's time to evaluate current data collection strategies.

Checklist

Evaluate Your Current Data Collection

While comprehensive coverage, precision and interoperability are crucial for the effectiveness of your threat intelligence strategy, it can be challenging to strike a balance between all three. Use this checklist to help your team assess your data coverage and tools and identify any gaps.

Comprehensive Coverage

- [ ] Do I have aggregate data from diverse sources, including open source intelligence (OSINT), deep and dark web sources, and proprietary feeds?
- [ ] Is a wide range of data types monitored and alerted on, such as indicators of compromise (IoCs), tactics, techniques and procedures (TTPs), threat actor chatter, malware development and deployment?
- [ ] Do I have a truly global coverage of threats?
- [ ] Does my coverage include a focus on subsidiaries and third-party vendors?
- [ ] Is the data updated in real time with contextual insights to provide timely information about emerging threats and vulnerabilities?

Precision

- [ ] Does the data I'm ingesting improve my ability to respond to incidents?
- [ ] Is there any noticeable lag in retrieving and processing threat intelligence data?
- [ ] Do my tools produce a high volume of redundant alerts?
- [ ] Is the data reliable and valuable?
- [ ] Does the solution adhere to data privacy regulations and compliance standards applicable to my organization's industry, local requirements, etc.?
- [ ] Can the tool be customized to fit my organization's needs?

Interoperability

- [ ] Is my data integrated into a central security information and event management solution, security orchestration, automation and response tool, or threat intelligence platform?
- [ ] Can I import and export threat intelligence data in necessary formats?
- [ ] Is the solution scalable?
- [ ] Does my data collection properly accommodate the evolving needs of my organization in terms of necessary sources?

By systematically evaluating cybersecurity tools against this criteria, threat intelligence teams can enhance their capabilities and strengthen their security posture.

There's Value in Actionable Threat Intelligence

By implementing right-sized information tools and applications, cybersecurity threat intelligence teams can maintain comprehensive visibility into risks facing their company's digital assets. Take for example Dataminr Pulse for Cyber Risk.

In June 2025, the cybercriminal group Scattered Spider launched a coordinated attack targeting the aviation industry. The attack caused significant disruptions, including cybersecurity incidents at WestJet, Hawaiian Airlines, and Qantas, with millions of customer records potentially impacted. Dataminr Pulse for Cyber Risk—specifically its agentic AI capability, Intel Agents—provided the critical context necessary for organizations to understand and triage response to the attack.

Intel Agents delivered instant, enriched cyber threat intelligence with the right context for businesses to understand the scope of the attacks; the tactics, techniques, and procedures (TTPs) of Scattered Spider; and the group's background and motivation. Information about Scattered Spider's recent activities was also provided to help organizations decide whether they were at risk—directly or via third-party affiliation. Dataminr surfaced several real-time alerts over 19 days.

Dataminr Pulse for Cyber Risk Alerts on Scattered Spider Activity

ALERT **JUNE 14, 2025**

WestJet says internal systems and app access restricted for several users during cybersecurity incident: Business.

ALERT **JUNE 27, 2025**

Palo Alto Networks's Unit 42 researchers observe Scattered Spider hacking group targeting aviation industry: Business via Social Media.

ALERT **JUNE 14, 2025**

WestJet says customers and employees should exercise caution when sharing personal details due to "cybersecurity incident": Business.

ALERT **JUNE 27, 2025**

Scattered Spider hacking group reportedly gained access to WestJet by performing self-service password reset for employee, whose account was then used to gain access to Citrix: Blog

ALERT **JUNE 26, 2025**

Hawaiian Airlines investigates cybersecurity event impacting some IT systems, says flights operating safely: Social Media.

ALERT **JUNE 30, 2023**

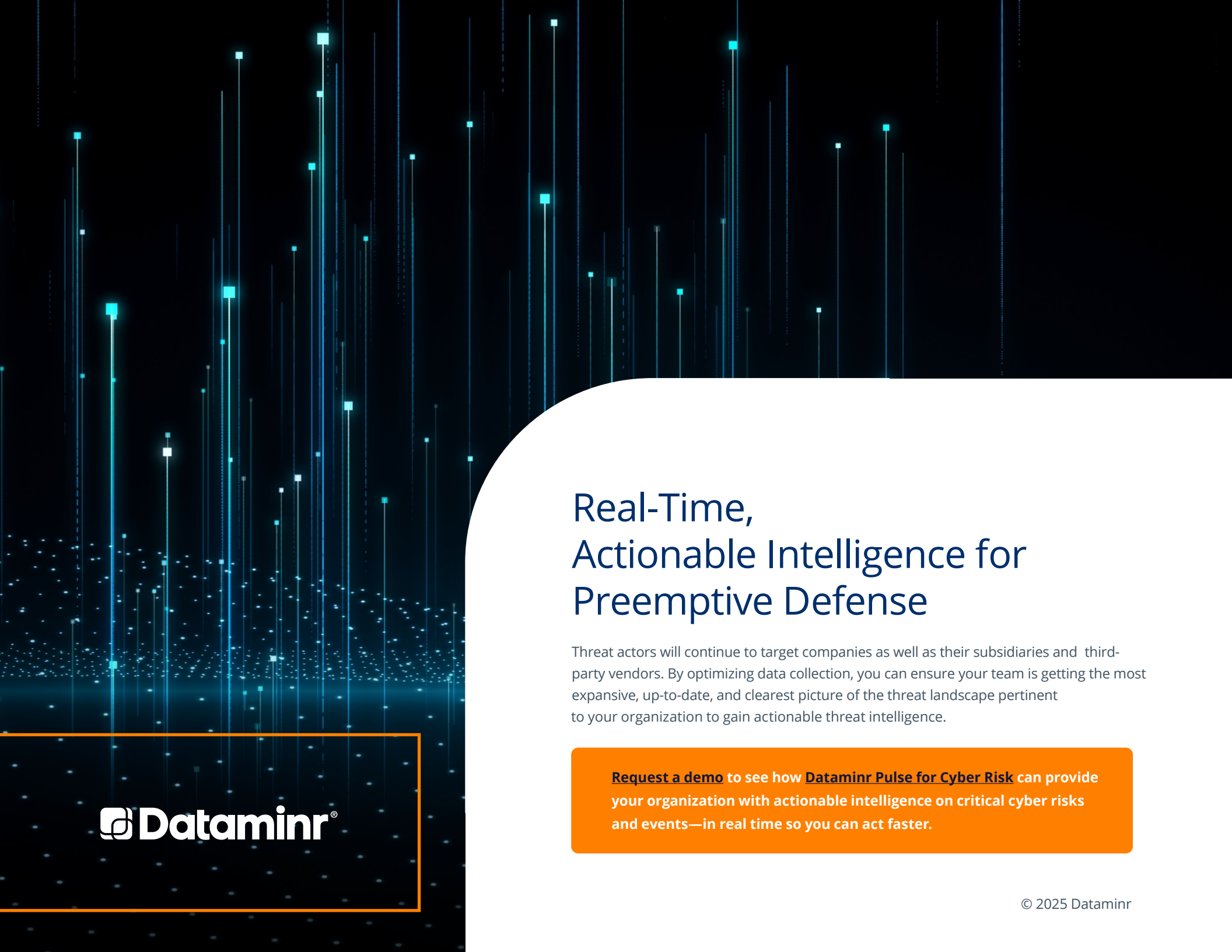
"FBI warns Scattered Spider hackers are now going after airlines": Blog.

ALERT **JUNE 27, 2025**

Mandiant says Scattered Spider hacking group actively targeting aviation and transportation sectors, with multiple incidents reported and group likely behind WestJet incident: News Outlet.

ALERT **JULY 1, 2025**

Qantas confirms cybersecurity incident impacting customer service platform, with data of 6M customers potentially impacted: Business.



Dataminr®

Real-Time, Actionable Intelligence for Preemptive Defense

Threat actors will continue to target companies as well as their subsidiaries and third-party vendors. By optimizing data collection, you can ensure your team is getting the most expansive, up-to-date, and clearest picture of the threat landscape pertinent to your organization to gain actionable threat intelligence.

Request a demo to see how Dataminr Pulse for Cyber Risk can provide your organization with actionable intelligence on critical cyber risks and events—in real time so you can act faster.