



A New Paradigm for Managing Third-Party Risk

Tess Smichenko
06.22.2025

Dataminr

Leading AI company for real-time event, risk, and threat detection



220+

Countries &
Territories

700K+

Facilities

500

Corporate Security
Teams

Public Sector

150K+ Government Users



United
Nations



Department
for Transport



News Media

1500+ Newsrooms



Enterprise

10K+ Corporate Security Users



Goldman
Sachs



DAIMLER



MERCK



FedEx



Walmart

dyson



HSBC

L'ORÉAL

How Dataminr Pulse for Cyber Risk Works

DATA INGESTION + EXTRACTION

Real-time sourcing from 1M+ global, public data sources

 Deep + Dark Web

 Code Repositories

 Sensors

 Regional & Alt Social Media

 Global Social Media


 News Media

 Industry Blogs

 Audio Transmissions


REAL-TIME THREAT DETECTION


AI processing of trillions of computations daily


 **Natural Language Processing** for text in 150+ languages


 **Computer Vision** for image & video

 **Audio Processing** for broadcast, recordings, & scanners

 **Anomaly Detection** across all public data sources

 **Multi-Modal Fusion AI** For fusing audio, video, text


 **Generative AI** for alert captions

 **Regenerative AI** for updating descriptions of unfolding events

ALERT FILTERING

Granular filtering and customization based on user-defined criteria

 **Company & Brand Names**

 **Topics + Keywords**

 **Location**

 **Priority levels**

COLLABORATION + COMMUNICATION

Integrate & automate preferred workflows

 **Out-of-the-Box Connectors (SIEM+)**

 **API**

 **Desktop, Mobile, Email**

Agenda

- The Challenge of Continuous Monitoring of Third Parties
- Current Process for Managing Third-Party Risk
- Applying AI Across Public Data to Detect Third-Party Risk
- Real World Example



How many of
you have been
impacted by
third-party risk
in the last 12
months?

How many of
you have been
impacted by
third-party risk
in the last 12
months?

How many of you
think your
Third-Party Risk
Management
program is
effective?

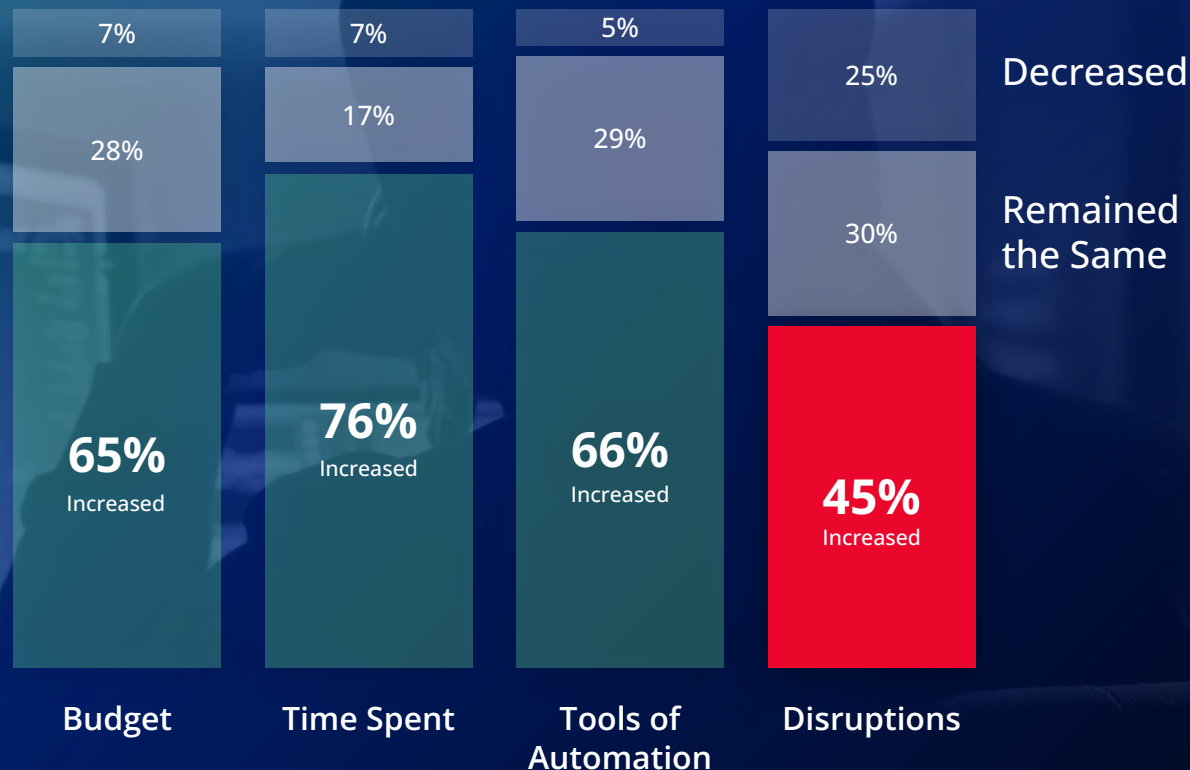
Expanding 3rd-Party Risk

Percent of breaches where a
third-party was involved
doubled from 15% in 2023 to
30% in 2024



Third-Party Risk Management is a priority

....but current approaches are insufficient



A large commercial airplane, likely a Boeing 737, is shown from a side profile, parked on a runway. The image is heavily overlaid with a semi-transparent blue filter. White text is superimposed on the image, listing various entities and events. The text is arranged in a grid-like fashion, with some words spanning multiple lines.

Change Healthcare

CDK Global

CrowdStrike Outage

Snowflake

Port of Seattle

How are we managing that Risk today?

Current State

Vendor Surveys

Attestations

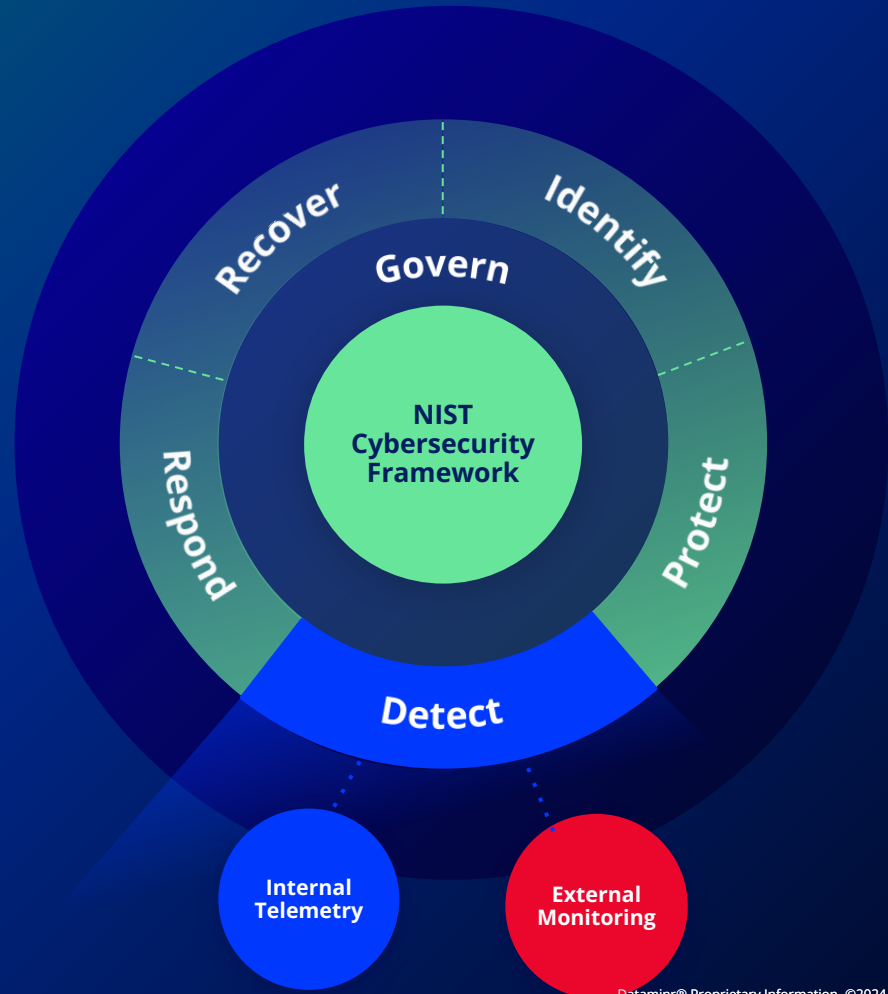
Security Ratings

Example		
c) Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimizes security risk;	4e(i)(C)	PO.5.1, PO.5.2
d) Taking consistent and reasonable steps to document, as well as minimize use or inclusion of software products that create undue risk, within the environments used to develop and build software;	4e(i)(D)	PO.5.1
e) Encrypting sensitive data, such as credentials, to the extent practicable and based on risk;	4e(i)(E)	PO.5.2
f) Implementing defensive cyber security practices, including continuous monitoring of operations and alerts and, as necessary, responding to suspected and confirmed cyber incidents;	4e(i)(F)	PO.3.2, PO.3.3, PO.5.1, PO.5.2
2) The software producer has made a good-faith effort to maintain trusted source code supply chains by: a) Employing automated tools or comparable processes; and b) Establishing a process that includes reasonable steps to address the security of third-party components and manage related vulnerabilities;	4e(iii)	PO.1.1, PO.3.1, PO.3.2, PO.5.1, PO.5.2, PS.1.1, PS.2.1, PS.3.1, PW.4.1, PW.4.4, PW.7.1, PW.8.1, RV.1.1
3) The software producer maintains provenance data for internal and third-party code incorporated into the software;	4e(vi)	PO.1.3, PO.3.2, PO.5.1, PO.5.2, PS.3.1, PS.3.2, PW.4.1, PW.4.4, RV.1.1, RV.1.2
4) The software producer employed automated tools or comparable processes that check for security vulnerabilities. In addition:	4e(iv)	PO.4.1, PO.4.2, PS.1.1, PW.2.1, PW.4.4, PW.5.1, PW.6.1, PW.6.2, PW.7.1, PW.7.2, PW.8.2, PW.9.1, PW.9.2,

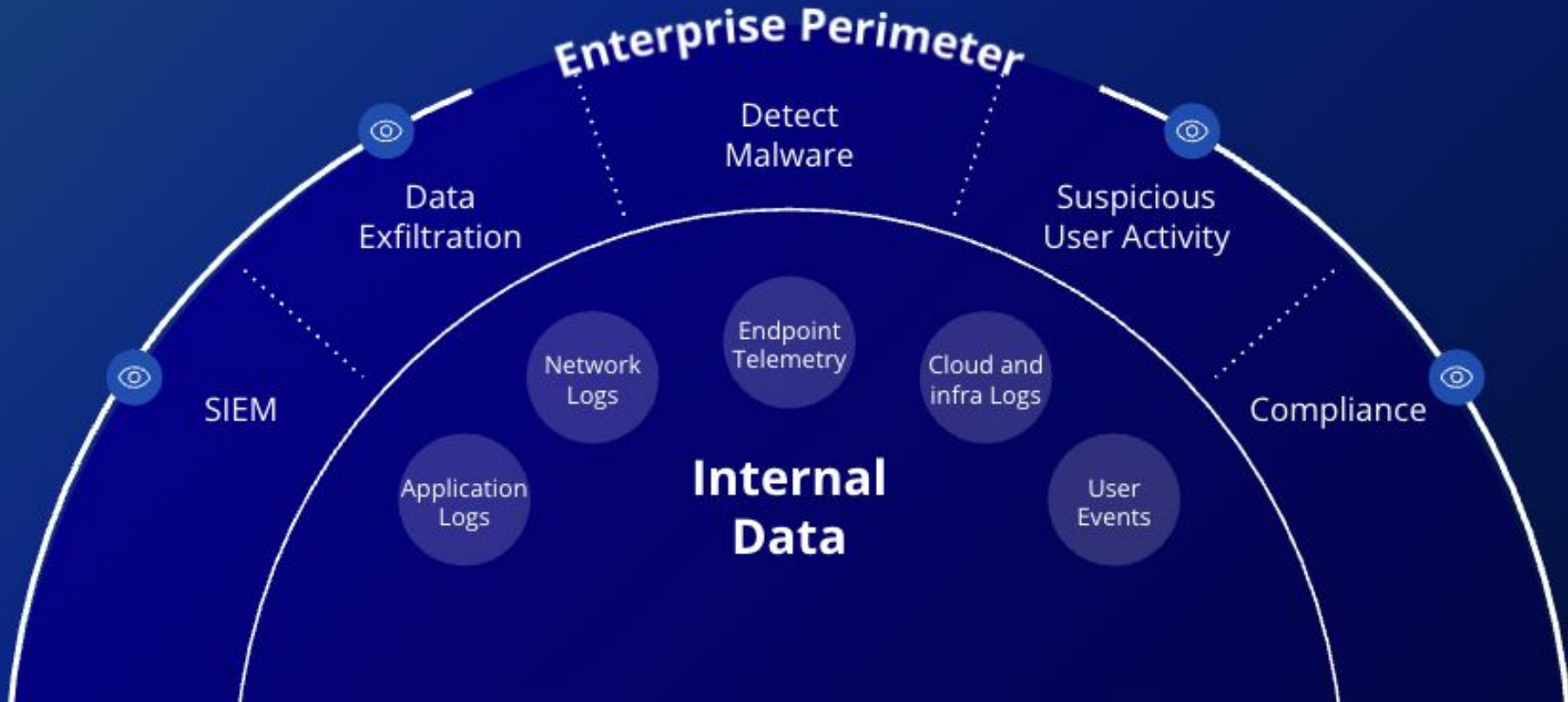
CISA Secure Software Self-Attestation Common Form (Draft)

What's Missing?

Real-time
detection & monitoring for
Third-Party Risk

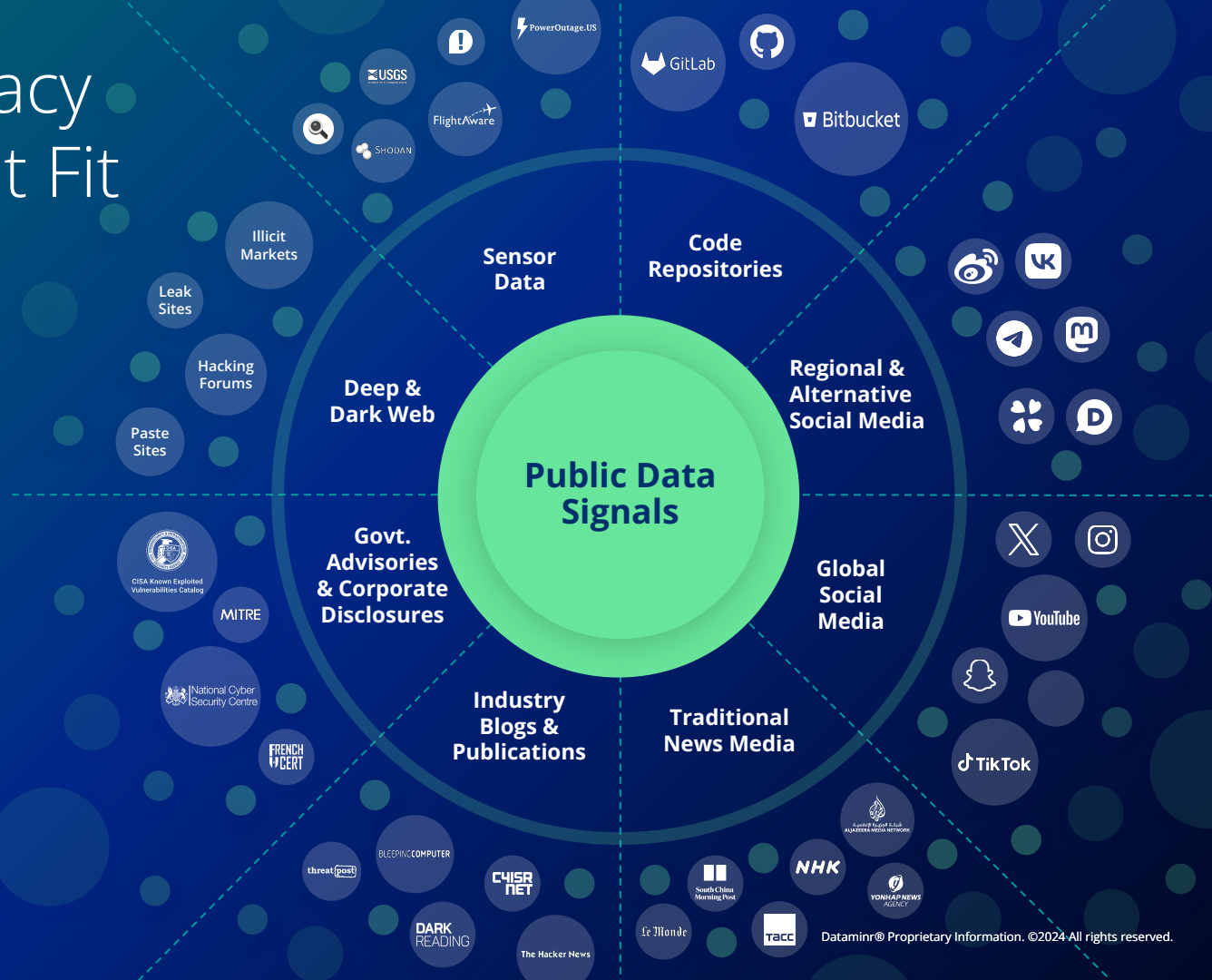


Challenge: No Direct Oversight, Control and Management Over Third Parties



Challenge: Legacy Threat Intel Not Fit For Purpose

- ✗ **Blind spots**
Missing sources, modalities, languages
- ✗ **Noisy**
Overwhelming alerts, false positives
- ✗ **Not real-time**
Lagging updates and context
- ✗ **Costly**
Manual and inefficient





A New Paradigm: AI & Public Data



Digital Risk Real-World Examples

CYBER ATTACK ON HEALTHCARE COMPANY

6:59 PM Feb 21, 2024

US healthcare technology company Change Healthcare confirms cyberattack on systems cause of ongoing network interruption, with disruptions expected to last into business hours on Thursday

“

Dataminr was **very timely** with this situation. We **sent alerts to our CISO** who was unaware of the attack which **impacted 12% of our business**”

MAJOR US HEALTH SERVICES COMPANY

THREAT ACTOR SELLING INFO ON ENERGY COMPANY

8:47 AM Apr 20, 2023

Database of US petroleum company advertised for sale, reportedly contains employee emails, names, departments, vehicle information, and more, with sample available

“

Dataminr was the **first to provide visibility** as [our] team had not seen this DDW discussion until Dataminr sent it to us”

MAJOR OIL & GAS COMPANY

CYBER ATTACK ON AEROSPACE COMPANY

1:59 PM Oct 27, 2023

Aerospace company impacted by LockBit 3.0 ransomware, group says "tremendous" amount of sensitive data exfiltrated and ready to be published if company does not make contact by November 2

“

Big win for us!!...the CIRT (Critical Incident Response Team) confirmed that **Dataminr was the first to alert us** of this attack”

GLOBAL AEROSPACE COMPANY



Johnson Controls Cyber Incident Timeline

Johnson Controls **confirms** cybersecurity incident impacting internal IT infrastructure & applications, says company largely unaffected and remains operational.

SEP 28, 2023



10:46AM

US DHS **investigates** possibility that agency floor plans and security information included in breach during Johnson Controls ransomware attack.

7:18PM

US DHS **investigates** possibility that agency floor plans and security information included in breach during Johnson Controls ransomware attack.



Johnson Controls Cyber Incident Timeline

New Linux variant of Dark Angels Team ransomware **detected** targeting Multinational conglomerate company Johnson Controls.

SEP 27, 2023



7:36AM

Multinational conglomerate **Johnson Controls reportedly impacted** by Dunhill Leaks ransomware, group claims to have exfiltrated more than 27 TB of data, **affecting company and subsidiary systems.**

SEP 27, 2023



4:23PM

Johnson Controls **confirms** cybersecurity incident impacting internal IT infrastructure & applications, says company largely unaffected and remains operational.

SEP 28, 2023



10:46AM

US DHS investigates possibility that agency floor plans and security information included in breach during Johnson Controls ransomware attack.



7:18PM

HELLO dear Management of Johnson Controls International!!

If you are reading this message, it means that:

- your network infrastructure has been compromised,
- critical data was leaked,
- files are encrypted,
- backups are deleted

by DARK ANGELS TEAM !

The best and only thing you can do is to contact us to settle the matter before any losses occurs.

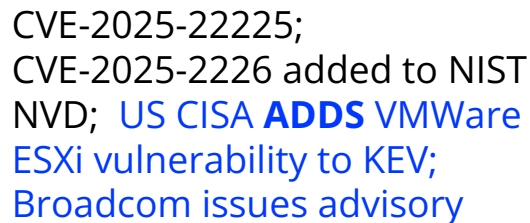


VMWare ESXi exploit timeline

CVE-2025-22225;
CVE-2025-2226 added to NIST
NVD;
US CISA **ADDS** vulnerability to
KEV;
Broadcom issues advisory

MAR 4





0-day being sold on
dark web forum

FEB 26



MAR 4





Public data has essential information, but difficult to extract actionable signals in real-time

Public Data

Multiple modes
& languages



Non-relevant /
noisy

Real-time,
with continuous
updates

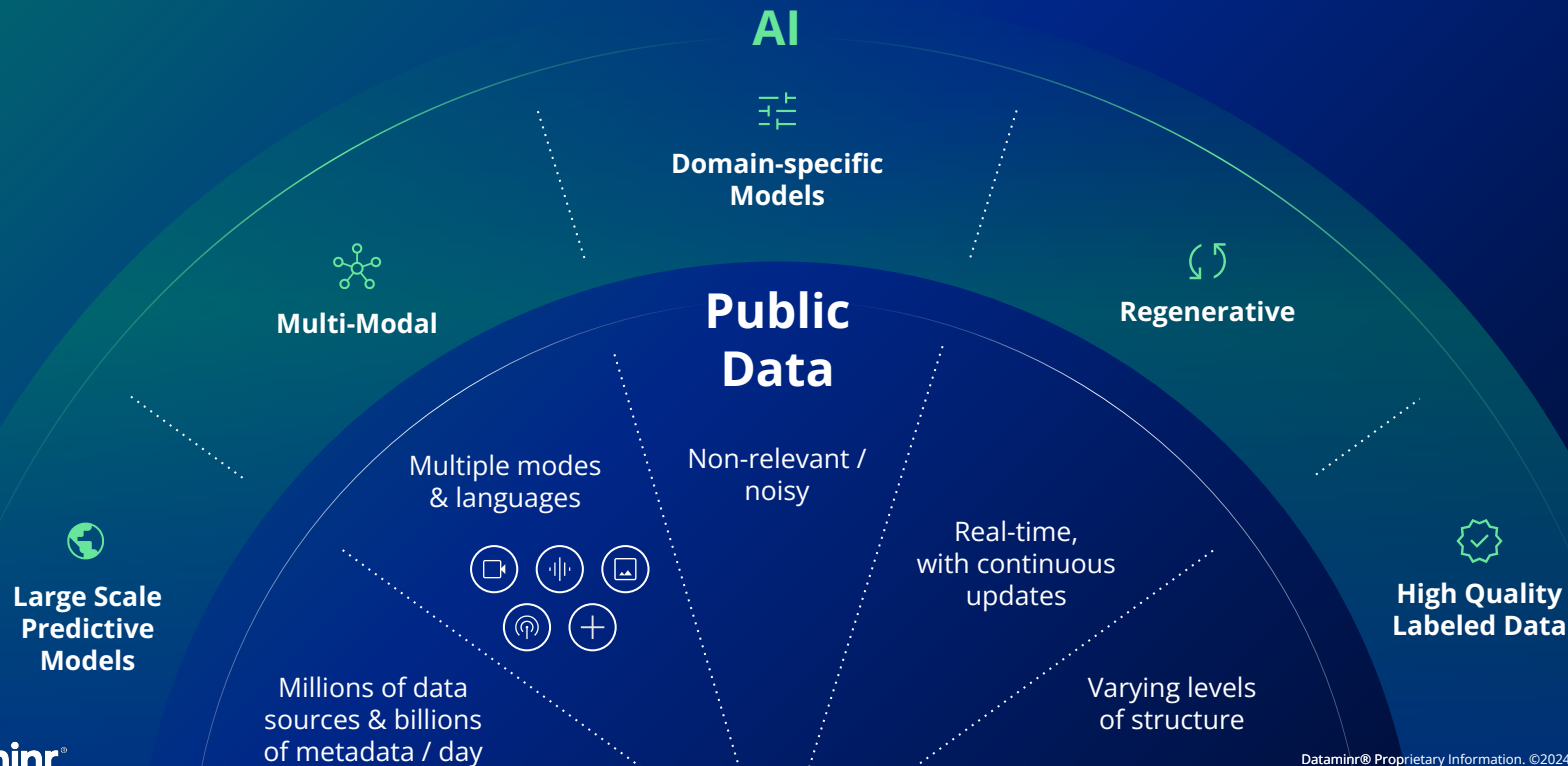
Varying levels
of structure

Millions of data
sources & billions
of metadata / day

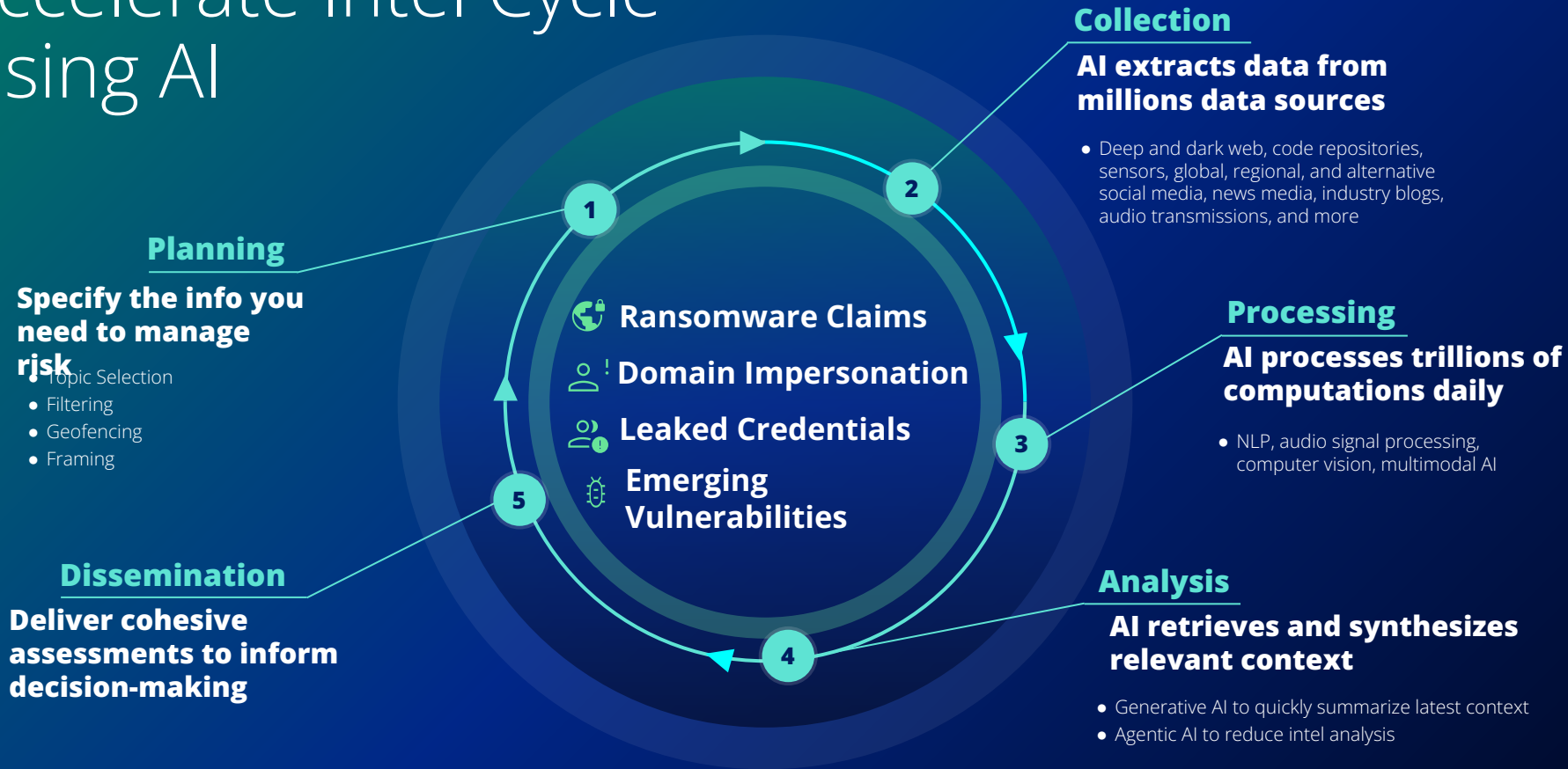


AI is the only solution to the public data challenge:

Providing third party monitoring with **speed, scope, and relevance**



Accelerate Intel Cycle Using AI





ALERT

1:03AM Jul 19, 2024

**User reports CrowdStrike
is triggering “blue screen
of death” on machines**

Jul 19



1:03AM

First reported
in major news



2:23AM



ALERT

1:03AM Jul 19, 2024

User reports CrowdStrike
is triggering “blue screen
of death” on machines

Jul 19



1:03AM

Third Party Risk Program

Create the Baseline

Develop, distribute, collect and analyze questionnaires

Risk Posture

Score Third Parties' risk posture

Continuous Monitoring & Threat Detection

- *Automated real time collection & extraction*
- *Domain-specific models*
- *Trained over time with high quality labeled data*
- *Deal with continuous updates to the risk event*

AWS Marketplace: Security Benefits



Deploy a comprehensive security architecture

From initial migration through ongoing day-to-day security platform management, leverage independent software vendors (ISVs) with proven success securing cloud adoption.

Reduce risk without losing speed

Minimize business disruptions by quickly procuring and deploying enterprise security software solutions that can manage identity and access, detect intrusions, and enable faster response times.

Integrate easily with AWS

Leverage security tools that are designed for AWS interoperability to follow security best practices.

AWS Marketplace: Customer Benefits

75%

less time
onboarding new
vendors

66%

less time
on procurement

25%

committed spend
recaptured using
AWS Marketplace

Source: “The Total Economic Impact™ Of AWS Marketplace” —a commissioned study by Forrester Consulting on behalf of AWS, May 2022.
Results are based on a composite organization comprised of interviewees with experience using AWS Marketplace.



Speak with us:

Ash D'Souza

ash.dsouza@dataminr.com

VP, Partner Ecosystems

dataminr.com