Dataminr®

Introducing Dataminr Pulse for

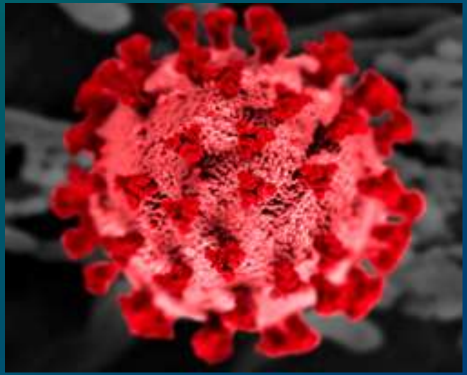
Cyber Risk

Amelie Renken | Account Executive DACH, Public Sector
amelie.renken@dataminr.com

Marion Dupuy | Director, Customer Success
mdupuy@dataminr.com

ITSA | October 2024 | Stand # 7A-620

Erkennt digitale Muster von Ereignissen aus täglich Milliarden von Datensignalen



Cluster von Augenzeugen Berichten

Coronavirus-Ausbruch in Wuhan, China

30. Dezember 2019

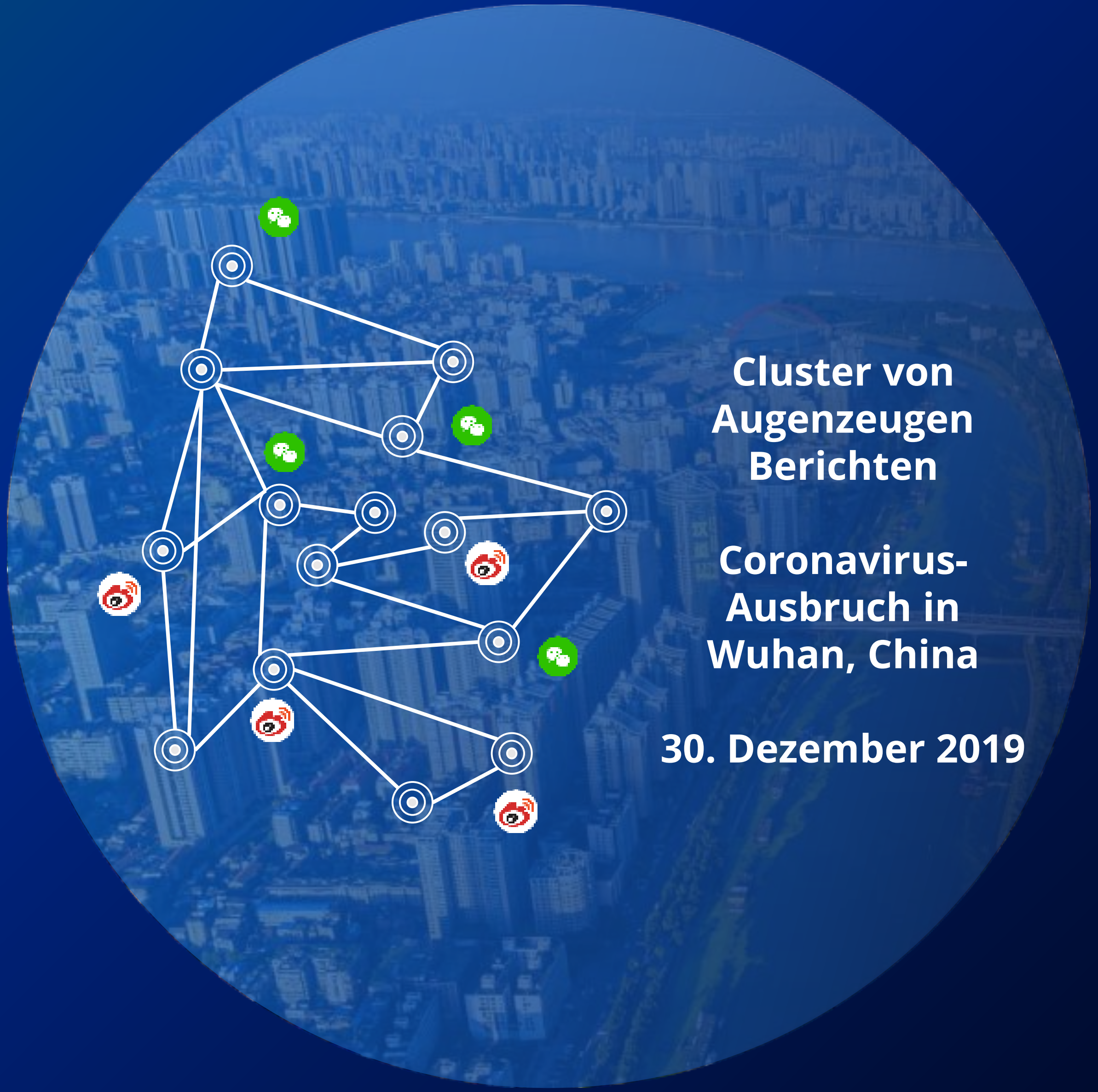
Dataminr

Erkennt digitale Muster von Ereignissen aus täglich Milliarden von Datensignalen

Multi-Modale KI:
Korreliert Datenformate: Text in über 150 Sprachen, Bild, Video, Ton und Sensordaten

Quellenumfang:
Integriert mehr als 1 Mio. öffentliche Datenquellen: Globale und regionale Social-Media-Plattformen, Blogs, Webforen, Deep- und Dark-Web, Audioübertragungen, Live-Kameraübertragungen, TV/Radio/Podcasts, Internet-Scanner, Wetterdaten und öffentliche IoT-Sensoren

Uneinholbarer KI Vorteil:
15 Jahre historisches Ereignis- und Datenarchiv, einschließlich Milliarden historischer Datensätze



*2009

Dataminr – Eilmeldungen in Echtzeit

KI-gestützte OSINT und Lageerfassung

Öffentlicher Sektor	Wirtschaft	Nachrichten & Medien
200+ Organisationen **150K+** Nutzer **100+** Länder	**550+** Global Security Teams **10K+** Nutzer **700K+** Standorte **14.4M+** Mitarbeiter	**30K+** Journalisten **1.5k+** Redaktionen **190+** Länder

Dataminr

A New Paradigm for Managing Third-Party Risk

Marion Dupuy |Director, Customer Success | Dataminr
IT SA
23.10.2024

Cyber Risk

Pulse for Cyber Risk

Risiko- und Bedrohungserkennung in Echtzeit.

Digital Risk

Third-Party Risk

Vulnerability Intelligence

Cyber-Physical Risk

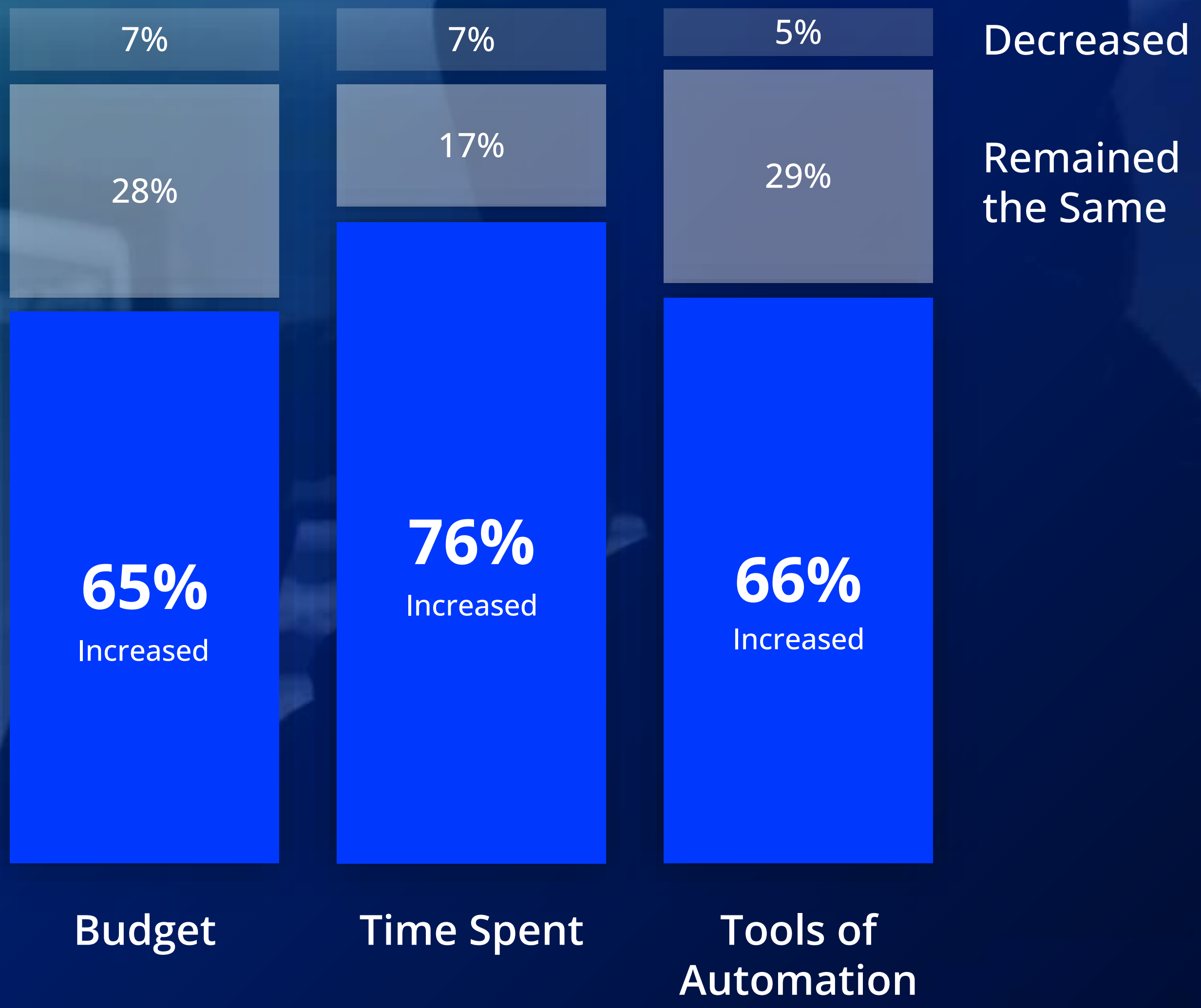
Dataminr

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 are fully satisfied with your Third-Party Risk Management capabilities?

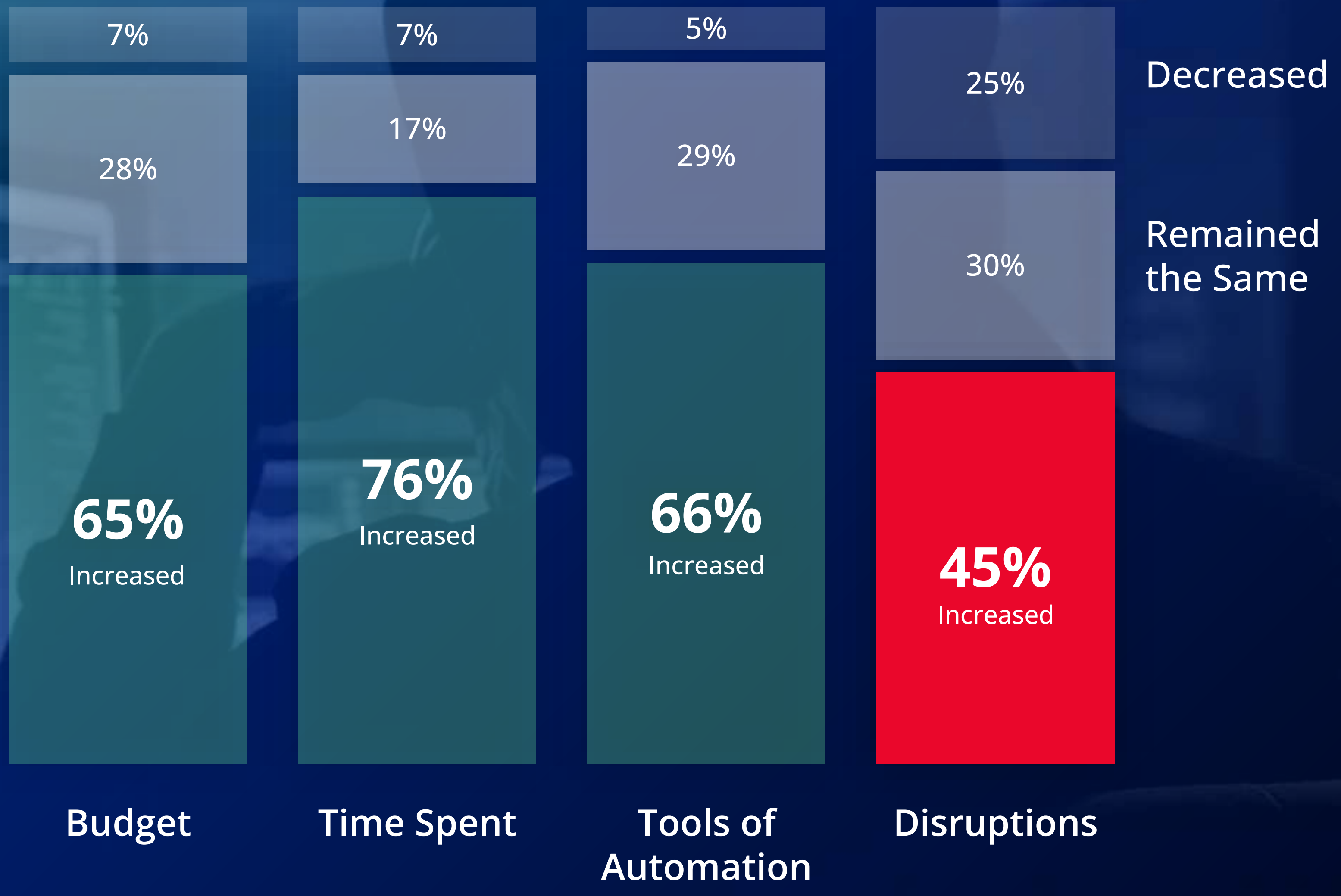
Third-Party Risk Management is a priority



Source: 2023 Gartner Reimagining Third Party Cybersecurity Risk Management Survey

Third-Party Risk Management is a priority

....but current approaches are insufficient



Source: 2023 Gartner Reimagining Third Party Cybersecurity Risk Management Survey

Why is Third-Party Risk Management so challenging?

1 **No direct oversight, control and management over third parties**

2 **Constrained cyber resources for continuous monitoring**

3 **Third parties are deemed more lucrative and softer targets by threat actors**

How are we managing that Risk?

Vendor surveys, attestations, & security ratings are the norm

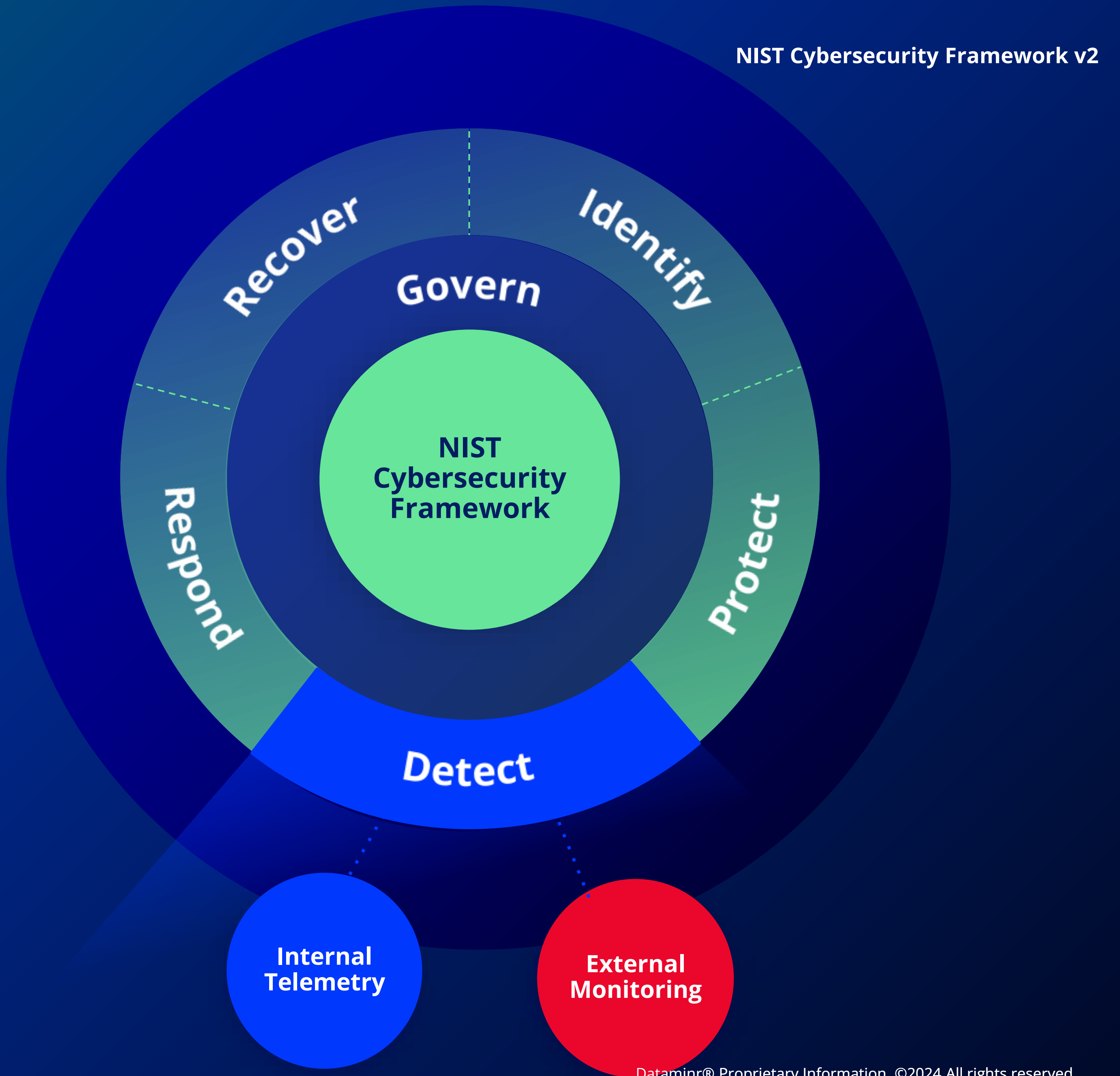
c) Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimizes security risk;	4e(i)(C)	PO.5.1, PO.5.2
d) Taking consistent and reasonable steps to document, as well as minimize use or inclusion of software 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?

The **Detect** Function –

Continuous Monitoring for Third-Party Risk Management



Johnson Controls Cyber Incident Timeline

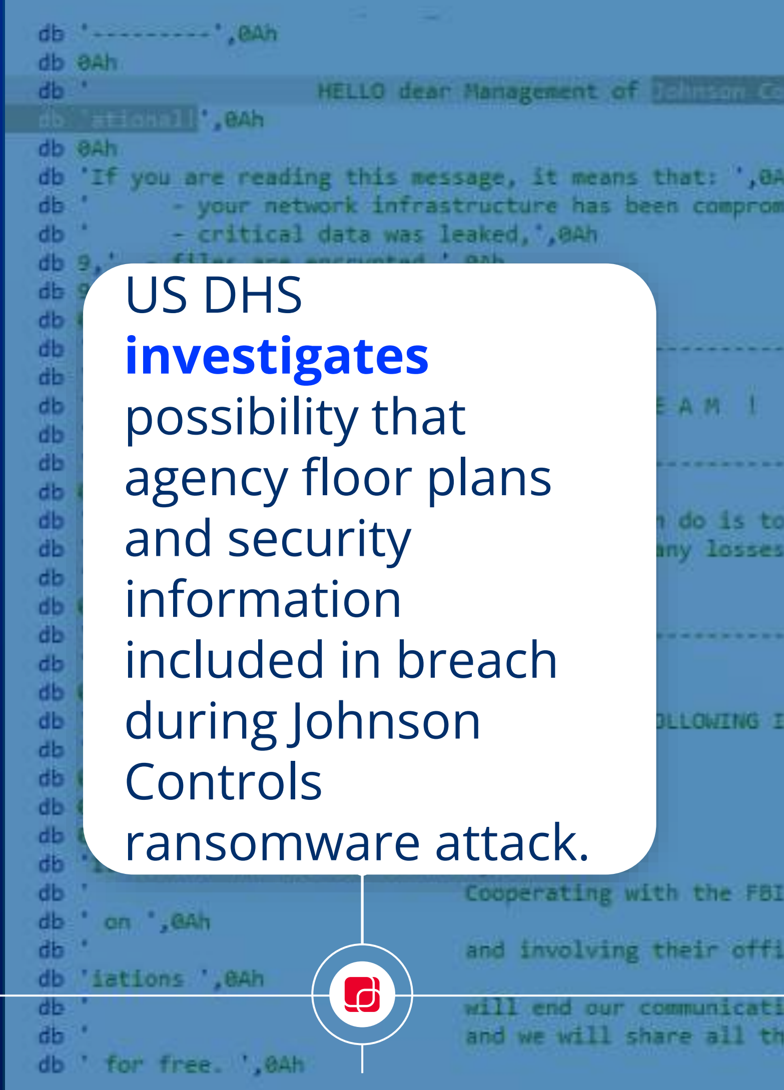
SEP 28, 2023

10:46AM

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

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

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 D A R K A N G E L S T E A M !

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

SEP 27, 2023

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

SEP 27, 2023

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

SEP 28, 2023

10:46AM

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

7:18PM

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

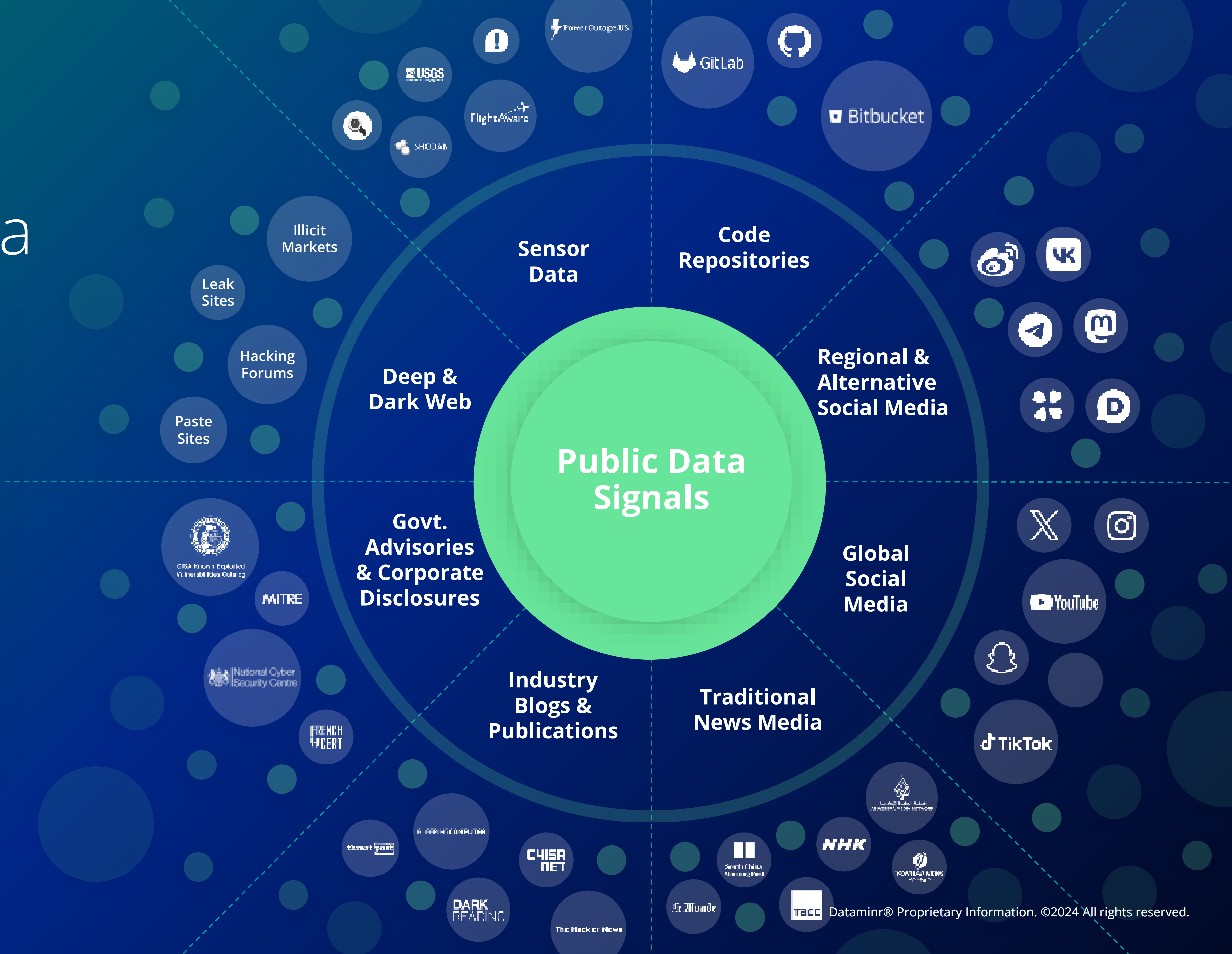
Dataminr

The Diverse Universe of Public Data

Millions
of data sources and

Billions
of metadata per day

6909
Distinct languages



Dataminr

Public data can be useful, but difficult to extract actionable signals in real-time

Public Data

Multiple modes & languages

Non-relevant / noisy

Real-time, with continuous updates

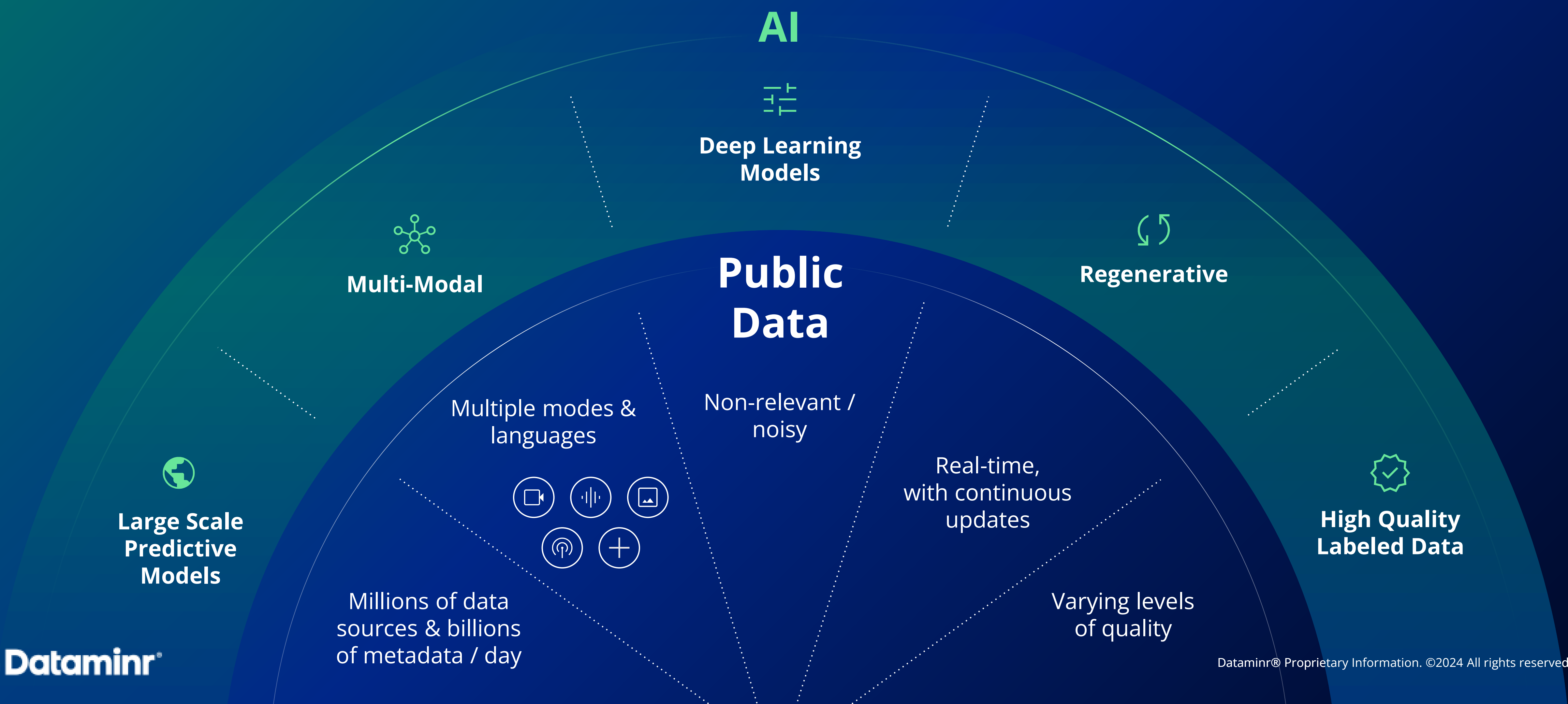
Millions of data sources & billions of metadata / day

Varying levels of quality

Dataminr

AI models are the only solution to the public data challenge:

Providing external threat detection with speed, scope, and relevance



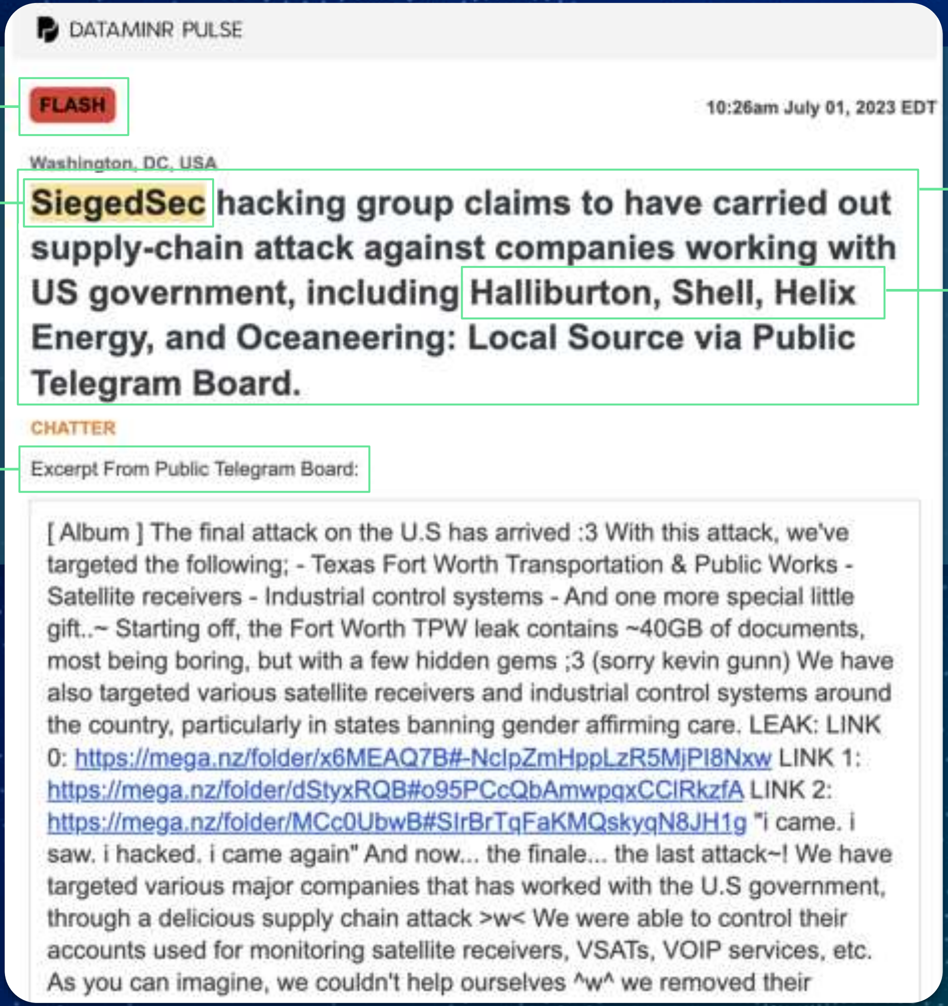
Dataminr

Metadata Extraction

Severity

Automated entity extraction - track 100+ groups

Sourced directly from Telegram



DATAMINR PULSE

FLASH

10:26am July 01, 2023 EDT

Washington, DC, USA

SiegedSec hacking group claims to have carried out supply-chain attack against companies working with US government, including Halliburton, Shell, Helix Energy, and Oceaneering: Local Source via Public Telegram Board.

CHATTER

Excerpt From Public Telegram Board:

[Album] The final attack on the U.S has arrived :3 With this attack, we've targeted the following; - Texas Fort Worth Transportation & Public Works - Satellite receivers - Industrial control systems - And one more special little gift..~ Starting off, the Fort Worth TPW leak contains ~40GB of documents, most being boring, but with a few hidden gems ;3 (sorry kevin gunn) We have also targeted various satellite receivers and industrial control systems around the country, particularly in states banning gender affirming care. LEAK: LINK 0: https://mega.nz/folder/x6MEAQ7B#-NclpZmHppLzR5MjPI8Nxw LINK 1: https://mega.nz/folder/dStyxRQB#o95PCcQbAmwpqxCClRkzfA LINK 2: https://mega.nz/folder/MCc0UbwB#SIrBrTqFaKMQskyqN8JH1g "i came. i saw. i hacked. i came again" And now... the finale... the last attack~! We have targeted various major companies that has worked with the U.S government, through a delicious supply chain attack >w< We were able to control their accounts used for monitoring satellite receivers, VSATs, VOIP services, etc. As you can imagine, we couldn't help ourselves ^w^ we removed their

Caption auto-generated using Dataminr LLM

Impacted companies identified using entity extraction

Key Points

CVE (with vendor and impacted product)

URL

Malware

IP address

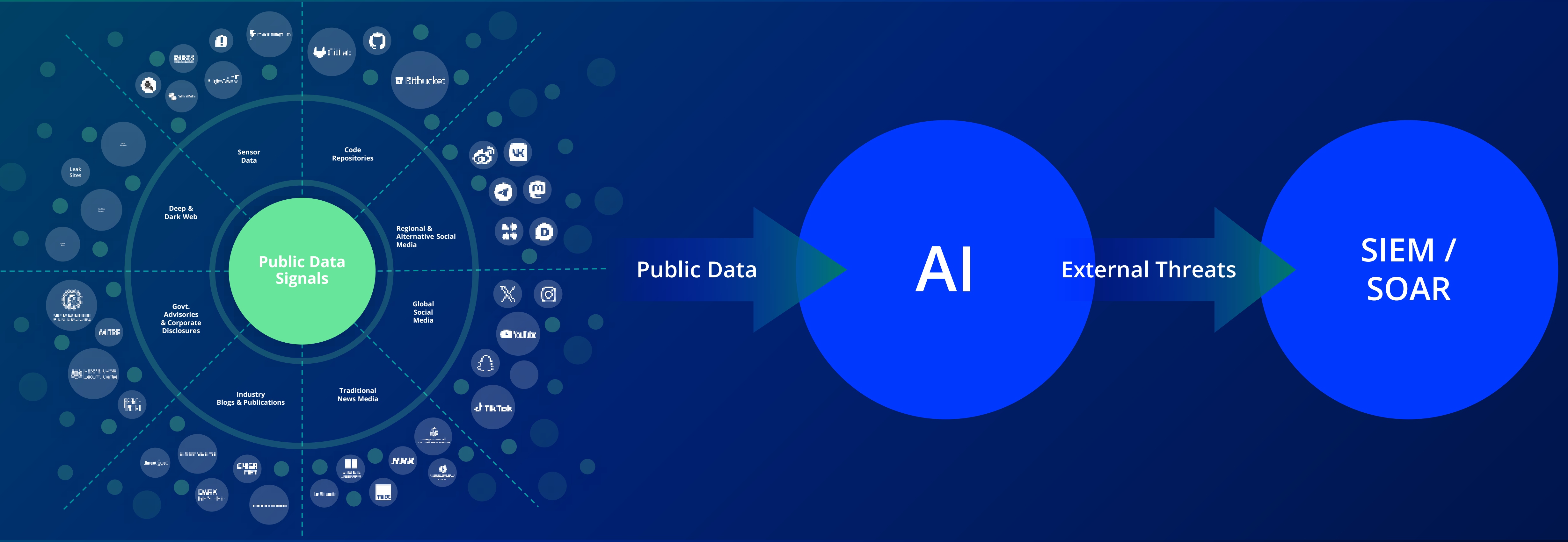
AS Org

Additional Details (as available)

CVSS	AS Host
Product Name / Version / Vendor	ASN
Exploit POC Link	Hash
Port	Hash Type
	Threat Actor

Dataminr

External Source Risk Alerting feeds into Existing Toolset



Dataminr

How multi-modal AI helps solve the public data problem

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 descriptions
- **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

Dataminr

Dataminr is your external threat detection platform using **AI** across **Public Data**

Speed
Real-time threat detection

Relevance
Actionable intelligence

Scope
Broad threat landscape coverage

Thank You!

Digital Risk

Third-Party Risk

Vulnerability Intelligence

Cyber-Physical Risk

Marion Dupuy
mdupuy@dataminr.com
dataminr.com

Stand # 7A-620

Dataminr