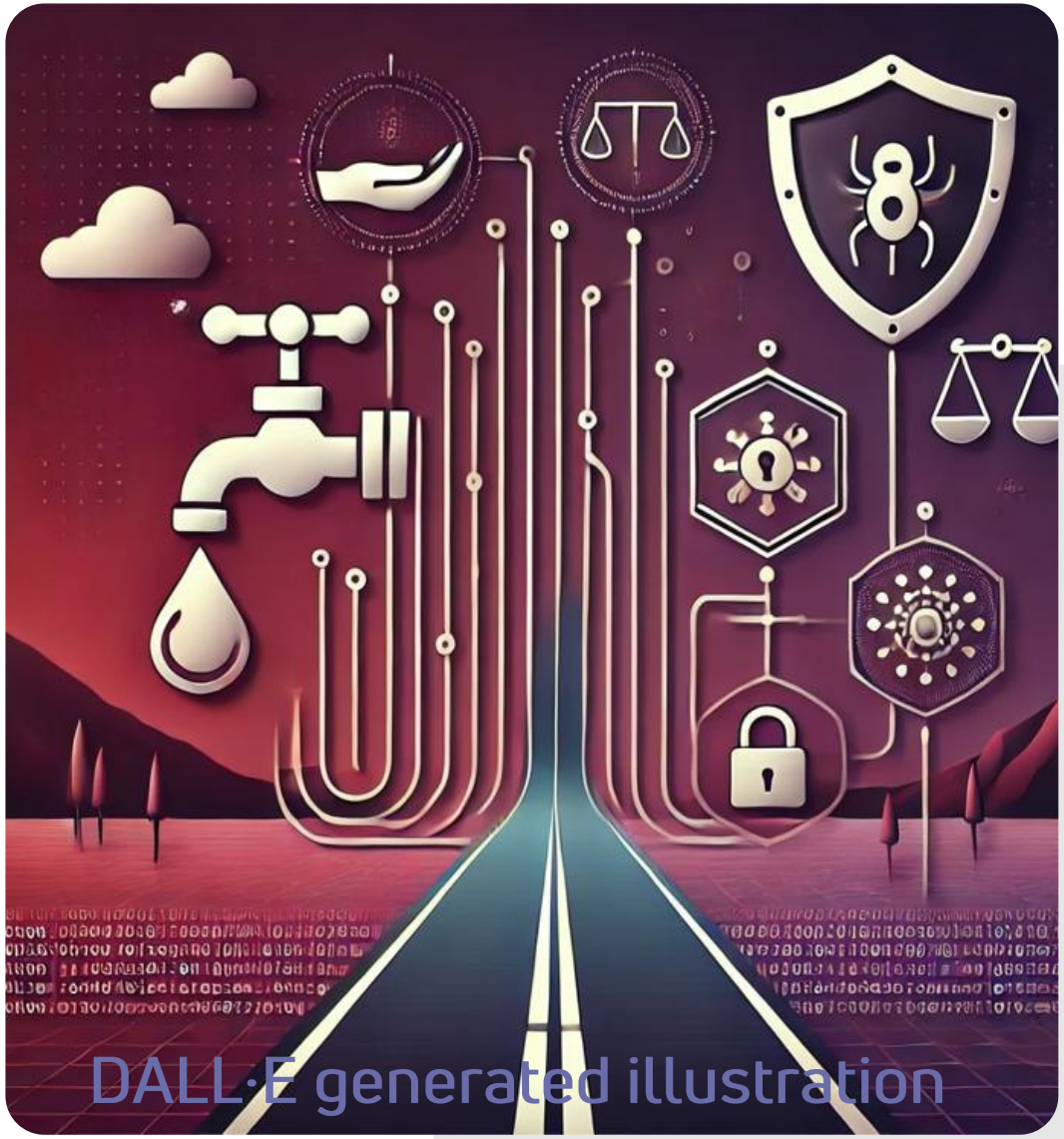
infodas
connect more. be secure.

AI-Driven Discovery of PII and Classified Information

Christopher Coppess
Regional Manager CEE & North America



DALL·E generated illustration

SECURITY DAY '26

Santa Monica Networks

Agenda

01

Opening



02

Data Protection and Privacy with Evidence



03

DCS/ZT: Enhanced Data Labeling



04

Closing and FAQ



infodas at a glance.

50+

50 Years Cybersecurity Excellence

2024

An Airbus subsidiary specialized in Cyber & IT

~310

~ 310 experts in IT, AI & Cybersecurity

~66

65.8m € turnover / 9.7m € EBIT (FY 2025)

Sectors

Defence, Public / CI, Security

Portfolio

Cross Domain Solutions	Cybersecurity Consulting & Security Testing	Applied Technology

Badges & Certifications.

COMING SOON

ITA SECRET

Zertifizierter IT-Sicherheitsdienstleister

DEU SECRET

EU SECRET

NATO SECRET

BUREAU VERITAS

COMMON CRITERIA

Trust Seal www.teletrust.de/itsmie

ITAR free products and services

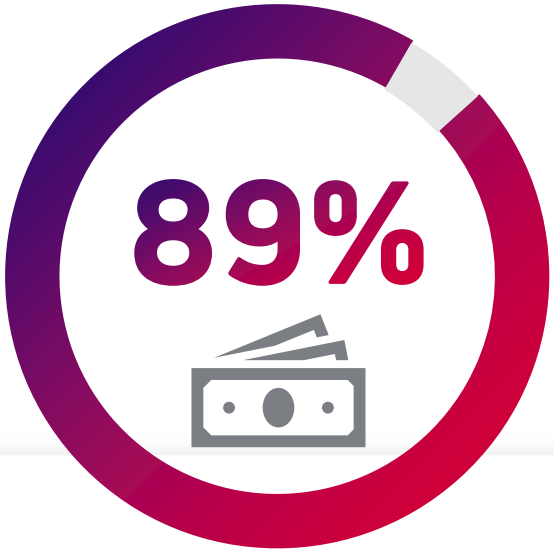
Agenda

02

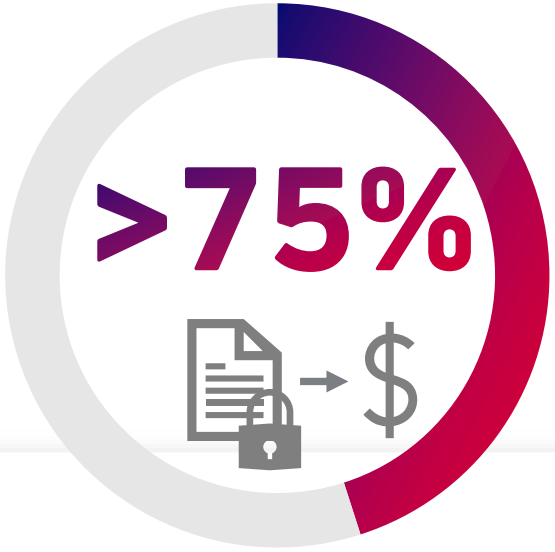
Data Protection and Privacy with Evidence



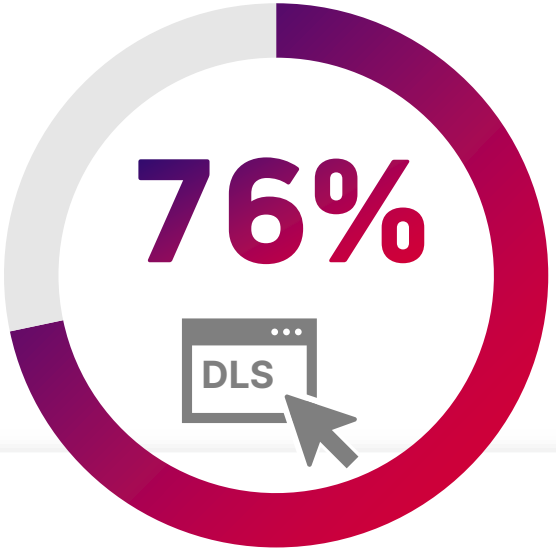
Recent Facts on Data Leakage



Primary motive for data leakage is financial gain*



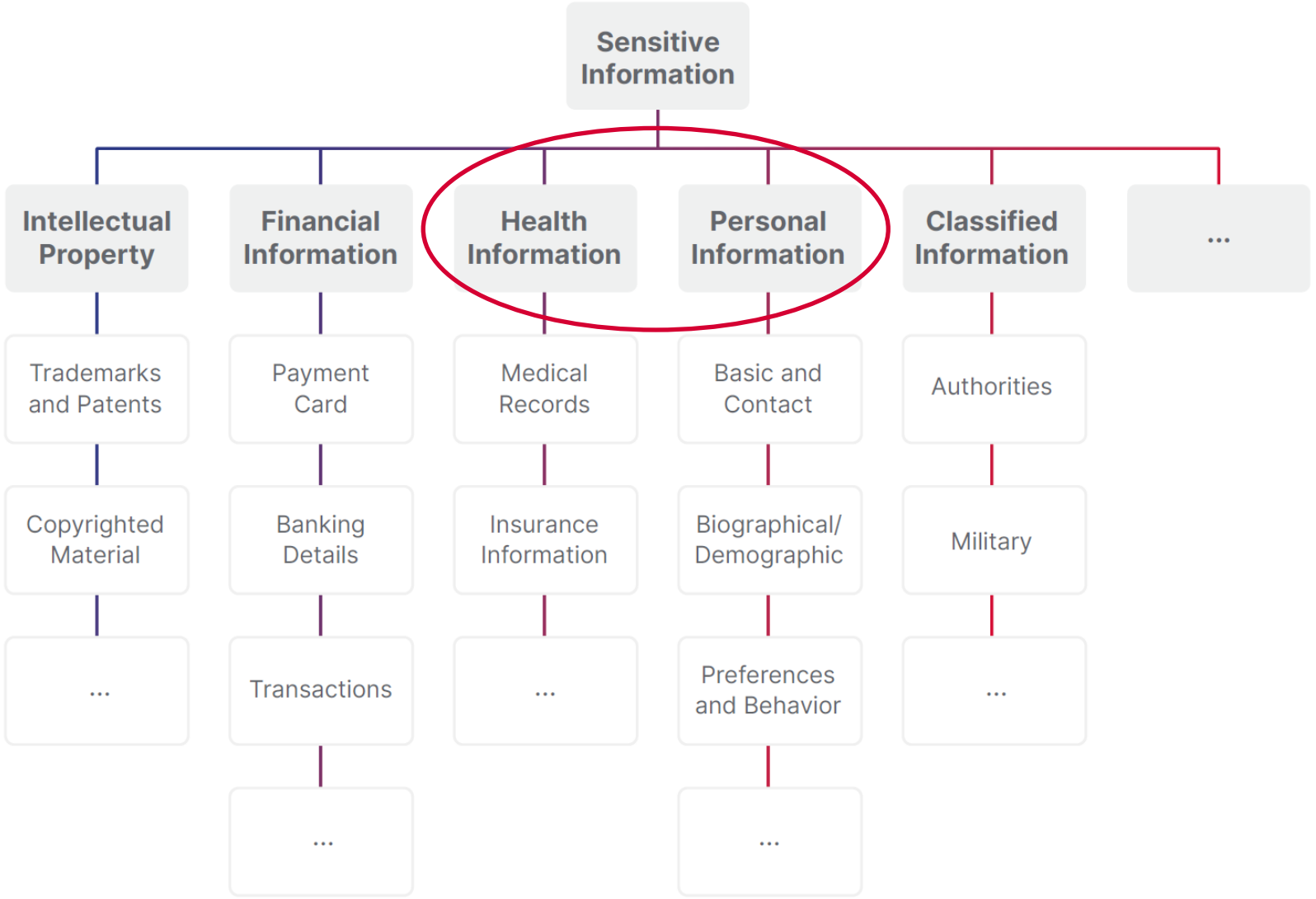
Three of four ransomware case involves exfiltration**

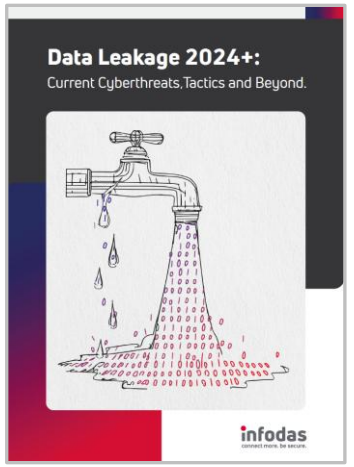


Number of dedicated leak sites rises***

* Verizon: "2025 Data Breach Investigations Report (DBIR)", Verizon Communications, 2025
** Mandiant: "Ransomware Tactics, Techniques, and Procedures in a Shifting Threat Landscape", Google Threat Intelligence, 2026
*** CrowdStrike, "CrowdStrike 2024 Global Threat Report", CrowdStrike, 2024

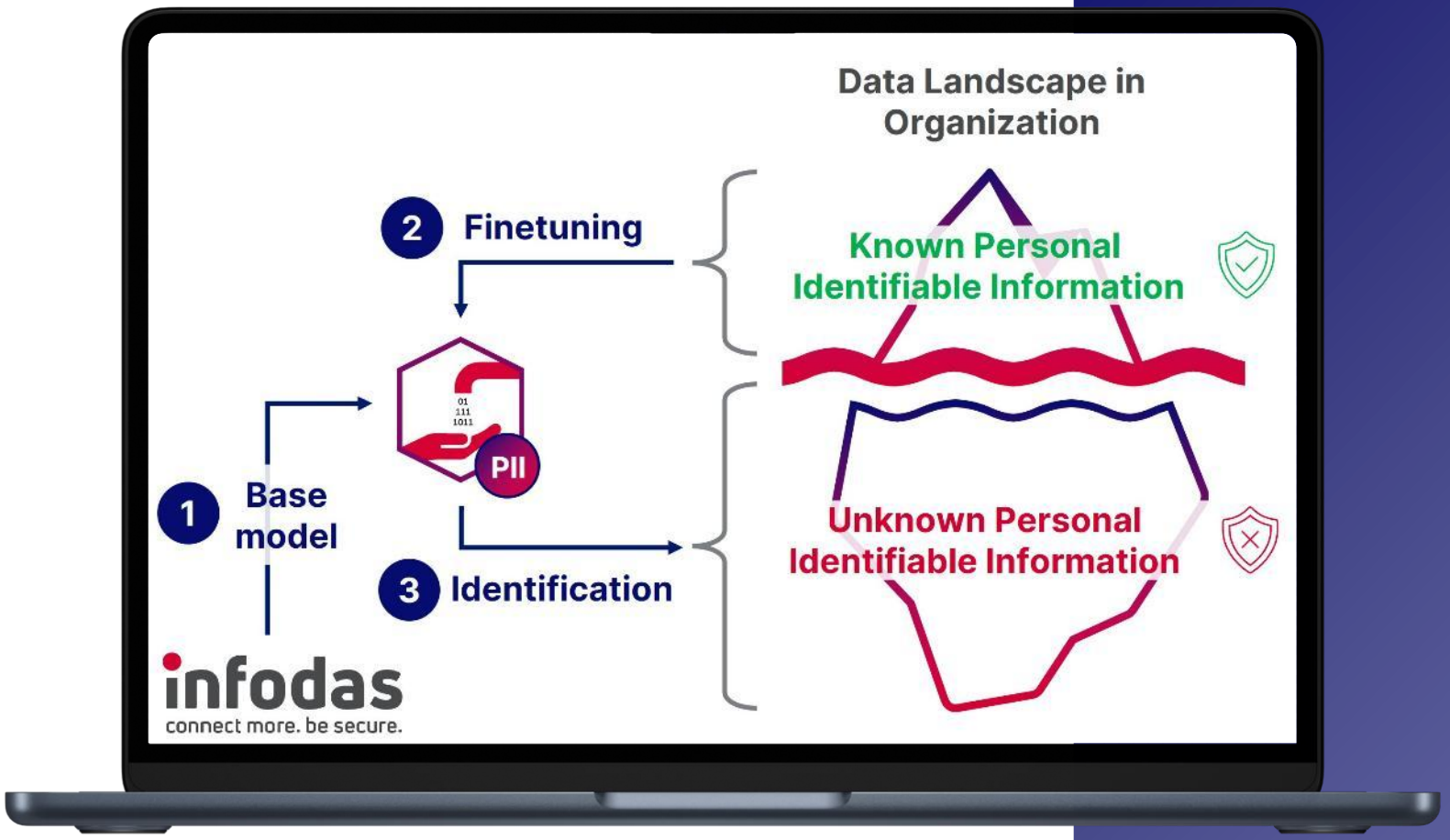
Which Data is Leaked Most ...





The Data-driven Approach

Consulting supported by evidence

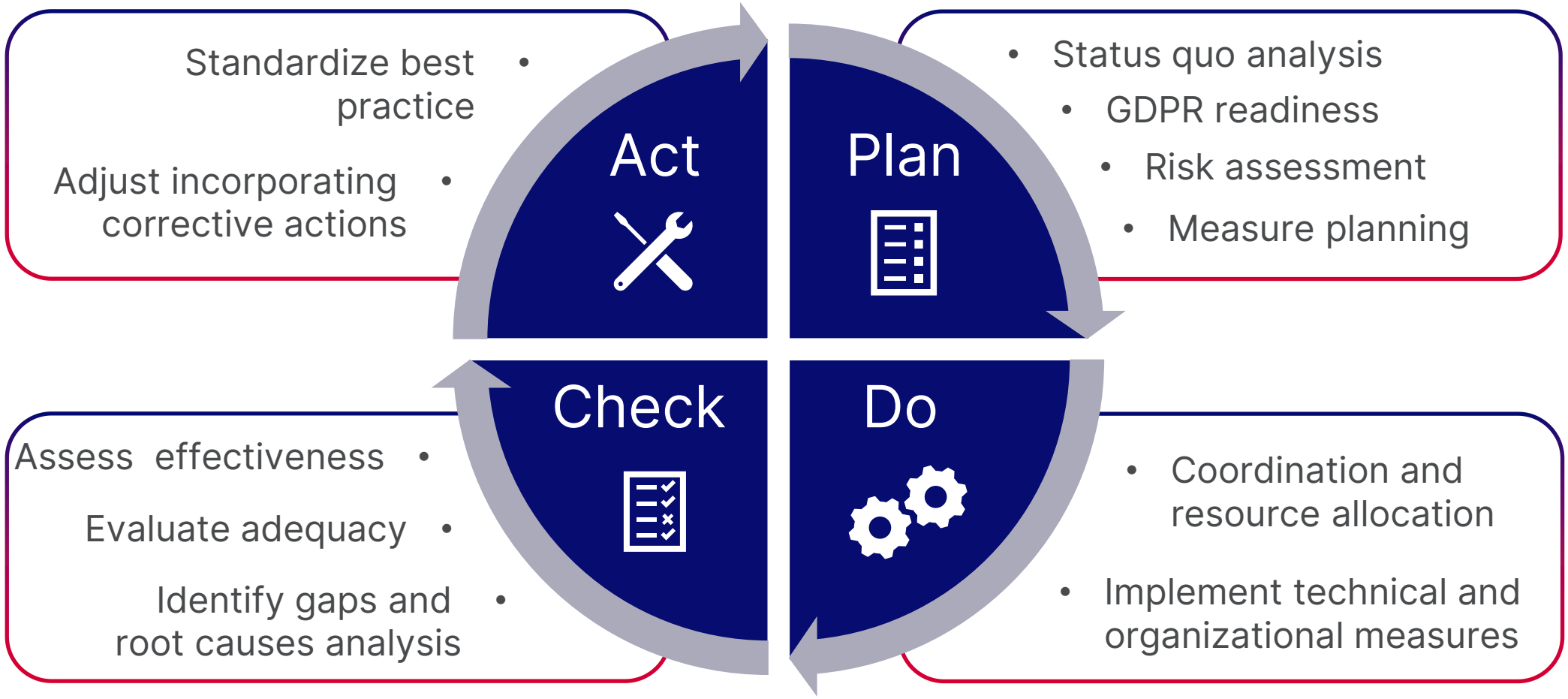


Benefits:

- Automated data inventory and transparency across the data landscape
- Cost reduction through
  - Less manual effort for data gathering
  - More efficient data protection consultancy
- Reducing the risk of shadow IT and uncontrolled data flows

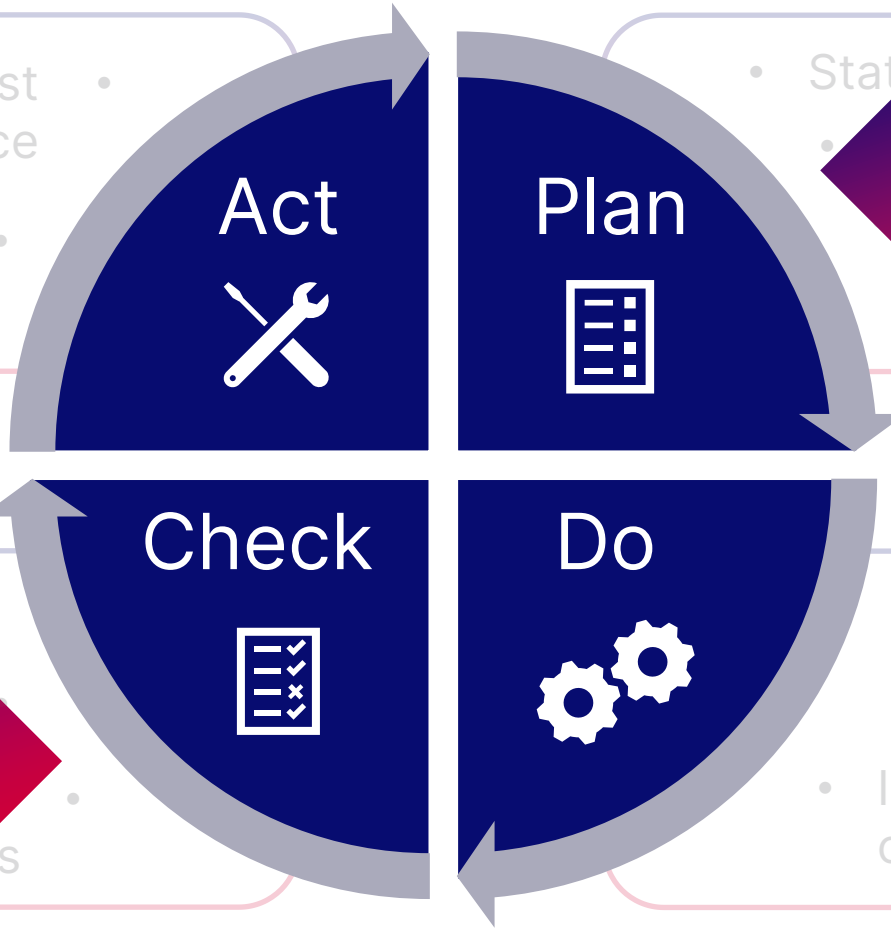
Accelerating the PDCA Cycles

Classic GDPR Consulting in Data Protection Projects



Accelerating the PDCA Cycles

With Data-driven Consulting



Data-driven Approach

- **Higher coverage of data inventory at-rest and in-motion**
- **Targeted priorization through risk scoring**

Improved cost/benefit analysis through real-time monitoring
Automated reporting of findings

Data-driven Approach

State-of-the-Art on Detecting GDPR-related Content

Product Line/ Solution	Forcepoint DLP	Nightfall AI DLP	Spirion DSPM	BigID Next	Private AI	infodas data-driven Consulting
Cloud	✓	✓	✓	✓	✓	✓
On-prem	✓		✓		✓	✓
Consulting	(✓)	(✓)	(✓)	(✓)		✓
Low Hardware Demands	(✓)				(✓)	✓
TAI/Explainability		✓	(✓)	(✓)		✓
Entity Distinction	(✓)	(✓)	(✓)	✓	(✓)	✓

Illustrative example:

„Frank was very [...]. He was born in Bonn.“

✓ :PERS

Birth place? :LOC

Most solutions today:

- Target cloud environments
- Provide technical support rather than consulting
- Have strong hardware demands or limited explainability
- Do not distinguish between personal and non-personal entities

Illustrative Analyse: Business letter (I)



Nordlicht Logistik OHG
Abteilung Vertrieb & Auftragsabwicklung
An der Hafenmole 12b
D-25761 Büsum
Fon: +49 4834 9127-00
E-Mail: vertrieb@nordlicht-logistik.de

BrightCore Solutions Ltd.
12 Bishopsgate
London EC2N 4BQ
United Kingdom

17 February 2024

Subject: Claim regarding damaged delivery – Reference No. BL-ORD-59384

Dear Sir or Madam,

We refer to our order dated February 12, 2024 (Reference No. BL-ORD-59384) and the subsequent delivery received on April 18, 2024.

Upon inspection of the delivered electronic components, we regret to inform you that a portion of the shipment was found to be damaged. Specifically, 37 units of the HTX-440 control modules exhibit visible casing fractures and are not operational. The damage appears to have occurred prior to or during transit, as the external packaging showed signs of compression.

We kindly request that you review this matter and advise on the appropriate next steps. We propose either a replacement delivery or a credit note for the affected items. Supporting photographic documentation and the delivery note (No. DN-77821) are available upon request.

We would appreciate your prompt response so that we may proceed without delay and minimize disruption to our operations.

Yours faithfully,

Nordlicht Logistik OHG

Actual models from october 2026

Presidio

spaCy

Hugging Face

- **Supporting up to 26 languages**
- **> 95% global F1-Score**
- **42 PII-Typs (Personal, Contact, Health ...)**
- **GDPRA Compliance (!)**

Illustrative Analyse: Business letter (II)

Nordlicht Logistik OHG
Abteilung Vertrieb & Auftragsabwicklung
An der Hafenmole 12b
D-25761 Büsum
Fon: +49 4834 9127-00
E-Mail: vertrieb@nordlicht-logistik.de

BrightCore Solutions Ltd.
12 Bishopsgate
London EC2N 4BQ
United Kingdom

17 February 2024

Subject: Claim regarding damaged delivery – Reference No. BL-ORD-59384

Dear Sir or Madam,

We refer to our order dated February 12, 2024 (Reference No. BL-ORD-59384) and the subsequent delivery received on April 18, 2024.

Upon inspection of the delivered electronic components, we regret to inform you that a portion of the shipment was found to be damaged. Specifically, 37 units of the HTX-440 control modules exhibit visible casing fractures and are not operational. The damage appears to have occurred prior to or during transit, as the external packaging showed signs of compression.

We kindly request that you review this matter and advise on the appropriate next steps. We propose either a replacement delivery or a credit note for the affected items. Supporting photographic documentation and the delivery note (No. DN-77821) are available upon request.

We would appreciate your prompt response so that we may proceed without delay and minimize disruption to our operations.

Yours faithfully,

Nordlicht Logistik OHG

Nordlicht Logistik OHG
Abteilung Vertrieb & Auftragsabwicklung
An der Hafenmole 12b
D-25761 Büsum
Fon: +49 4834 9127-00
E-Mail: vertrieb@nordlicht-logistik.de

BrightCore Solutions Ltd.
12 Bishopsgate
London EC2N 4BQ
United Kingdom

17 February 2024

Subject: Claim regarding damaged delivery – Reference No. BL-ORD-59384

Dear Sir or Madam,

We refer to our order dated February 12, 2024 (Reference No. BL-ORD-59384) and the subsequent delivery received on April 18, 2024.

Upon inspection of the delivered electronic components, we regret to inform you that a portion of the shipment was found to be damaged. Specifically, 37 units of the HTX-440 control modules exhibit visible casing fractures and are not operational. The damage appears to have occurred prior to or during transit, as the external packaging showed signs of compression.

We kindly request that you review this matter and advise on the appropriate next steps. We propose either a replacement delivery or a credit note for the affected items. Supporting photographic documentation and the delivery note (No. DN-77821) are available upon request.

We would appreciate your prompt response so that we may proceed without delay and minimize disruption to our operations.

Yours faithfully,

Nordlicht Logistik OHG

Nordlicht Logistik OHG
Abteilung Vertrieb & Auftragsabwicklung
An der Hafenmole 12b
D-25761 Büsum
Fon: +49 4834 9127-00
E-Mail: vertrieb@nordlicht-logistik.de

BrightCore Solutions Ltd.
12 Bishopsgate
London EC2N 4BQ
United Kingdom

17 February 2024

Subject: Claim regarding damaged delivery – Reference No. BL-ORD-59384

Dear Sir or Madam,

We refer to our order dated February 12, 2024 (Reference No. BL-ORD-59384) and the subsequent delivery received on April 18, 2024.

Upon inspection of the delivered electronic components, we regret to inform you that a portion of the shipment was found to be damaged. Specifically, 37 units of the HTX-440 control modules exhibit visible casing fractures and are not operational. The damage appears to have occurred prior to or during transit, as the external packaging showed signs of compression.

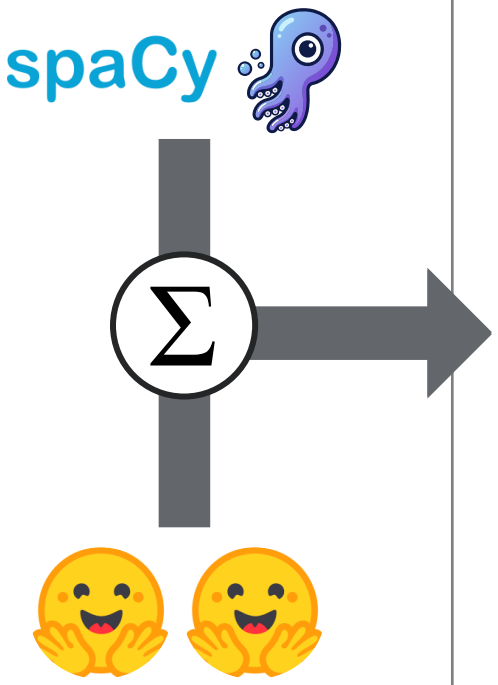
We kindly request that you review this matter and advise on the appropriate next steps. We propose either a replacement delivery or a credit note for the affected items. Supporting photographic documentation and the delivery note (No. DN-77821) are available upon request.

We would appreciate your prompt response so that we may proceed without delay and minimize disruption to our operations.

Yours faithfully,

Nordlicht Logistik OHG

Illustrative Analyse: Business letter (III)



Nordlicht Logistik OHG
Abteilung Vertrieb & Auftragsabwicklung
An der Hafenmole 12b
D-25761 Büsum
Fon: +49 4834 9127-00
E-Mail: vertrieb@nordlicht-logistik.de

BrightCore Solutions Ltd.
12 Bishopsgate
London EC2N 4BQ
United Kingdom

17 February 2024

Subject: Claim regarding damaged delivery – Reference No. BL-ORD-59384

Dear Sir or Madam,

We refer to our order dated February 12, 2024 (Reference No. BL-ORD-59384) and the subsequent delivery received on April 18, 2024.

Upon inspection of the delivered electronic components, we regret to inform you that a portion of the shipment was found to be damaged. Specifically, 37 units of the HTX-440 control modules exhibit visible casing fractures and are not operational. The damage appears to have occurred prior to or during transit, as the external packaging showed signs of compression.

We kindly request that you review this matter and advise on the appropriate next steps. We propose either a replacement delivery or a credit note for the affected items. Supporting photographic documentation and the delivery note (No. DN-77821) are available upon request.

We would appreciate your prompt response so that we may proceed without delay and minimize disruption to our operations.

Yours faithfully,

Nordlicht Logistik OHG

Company address ✓

Company address ✓

ID number ✗

Company address ✓

Illustrative Analy

Nordlicht Logistik OHG
Abteilung Vertrieb & Auftragsabwicklung
An der Hafenmole 12b
D-25761 Büsum
Fon: +49 4834 9127-00
E-Mail: vertrieb@nordlicht-logistik.de

BrightCore Solutions Ltd.
12 Bishopsgate
London EC2N 4BQ
United Kingdom

17 February 2024

Subject: Claim regarding damaged delivery – Reference No. BL-ORD-59384

Dear Ms. Bennett,

We refer to our order dated February 12, 202 (Reference No. BL-ORD-59384) and the subsequent delivery received on April 18, 2024.

Upon inspection of the delivered electronic components, we regret to inform you that a portion of the shipment was found to be damaged. Specifically, 37 units of the HTX-440 control modules exhibit visible casing fractures and are not operational. The damage appears to have occurred prior to or during transit, as the external packaging showed signs of compression.

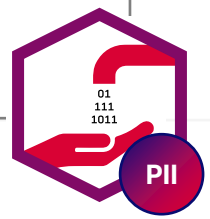
We kindly request that you review this matter and advise on the appropriate next steps. We propose either a replacement delivery or a credit note for the affected items. Supporting photographic documentation and the delivery note (No. DN-77821) are available upon request.

We would appreciate your prompt response so that we may proceed without delay and minimize disruption to our operations.

Yours faithfully,

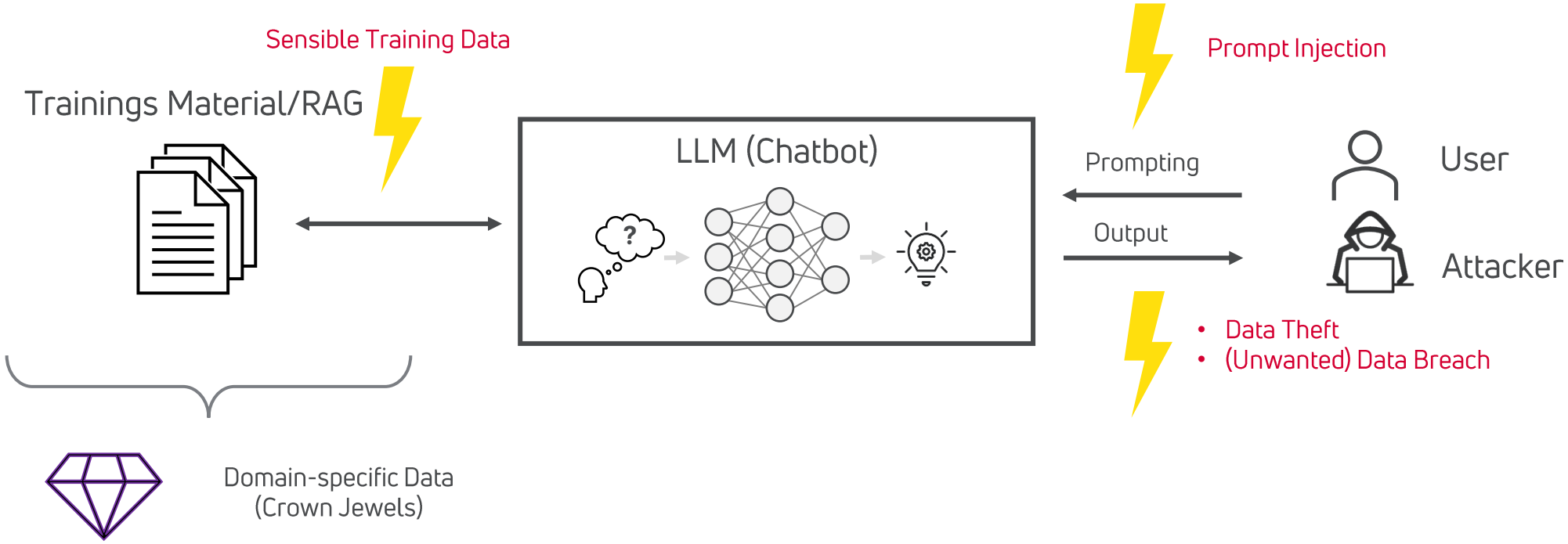
Markus Feldman

Nordlicht Logistik OHG



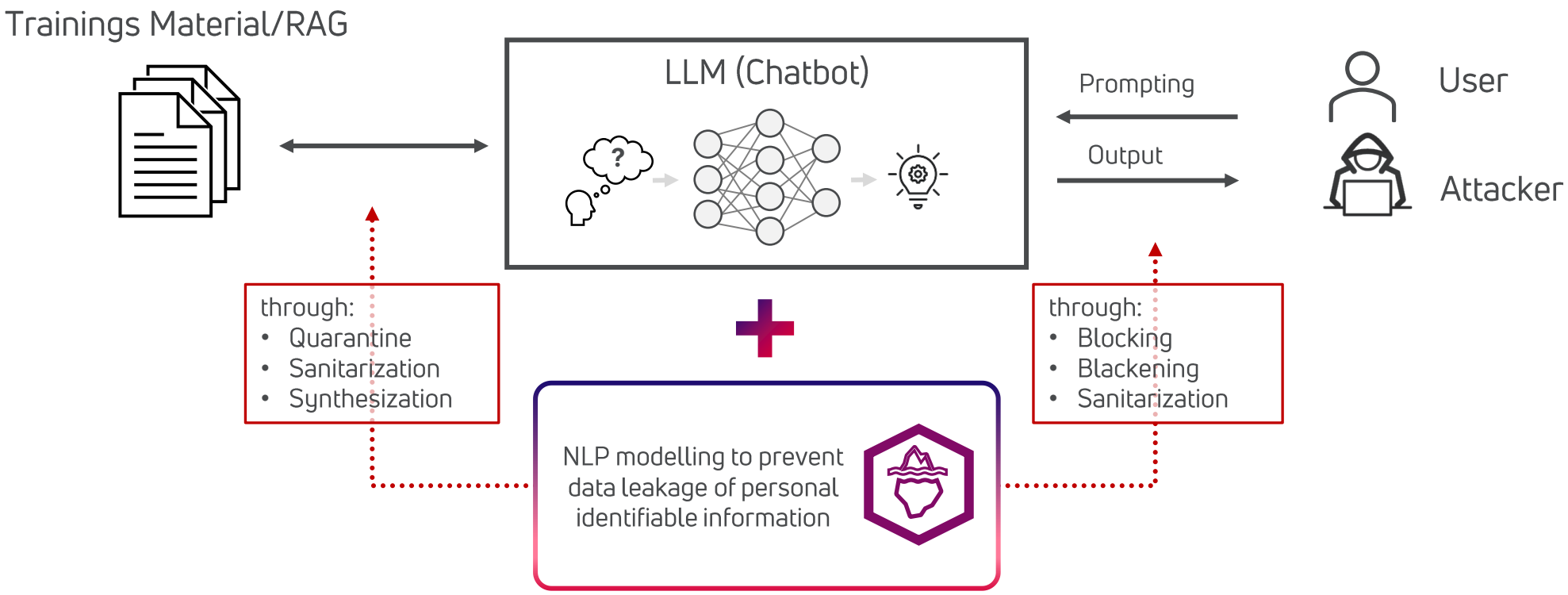
Further Use Cases (I)

Proactive Approach Protecting LLMs Against Data Leaks



Further Use Cases (I)

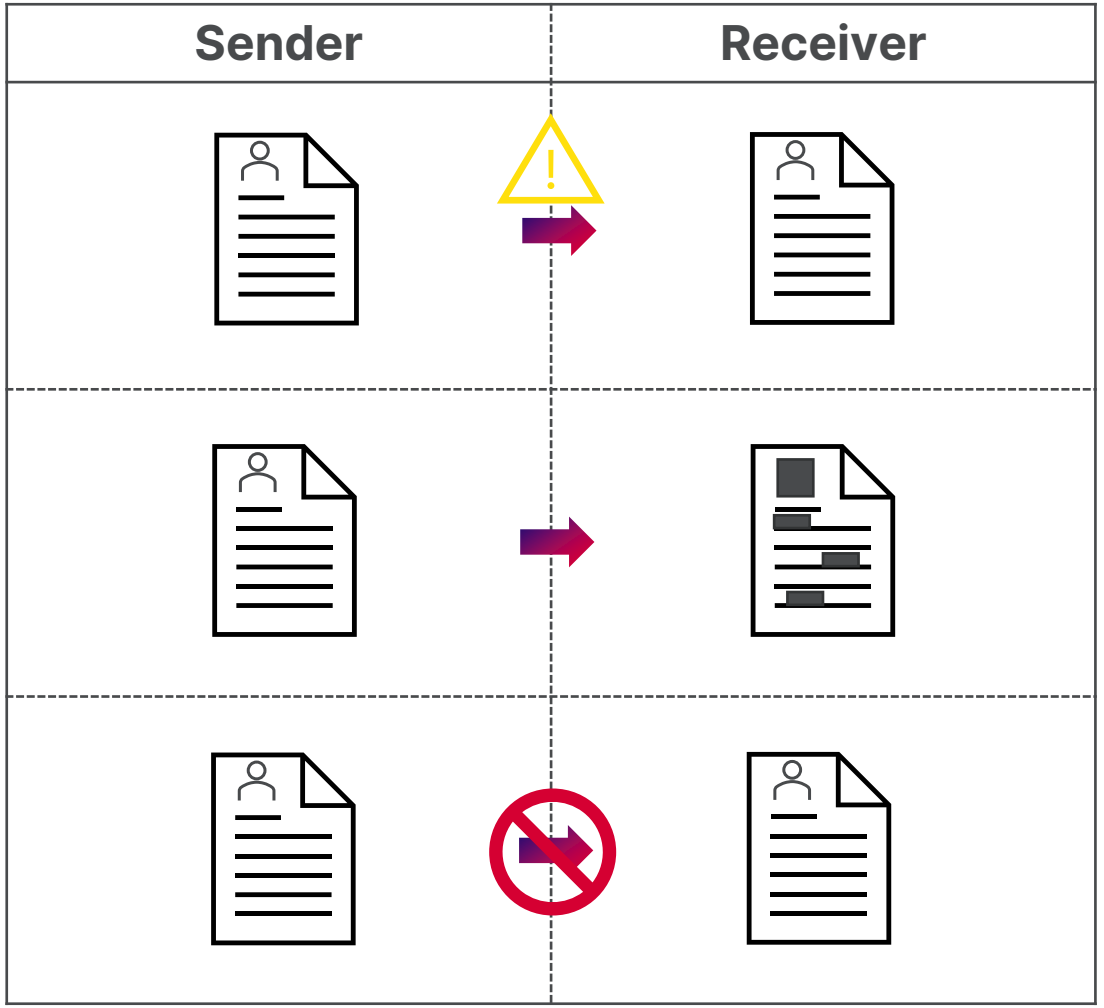
Proactive Approach Protecting LLMs Against Data Leaks



Further Use Cases (II)

... When Integrated in Operational Pipeline

- Endpoint integration
  - Warning on file upload/manipulation or while sending email
  - Recommendation on data anonymization/masking
- DLP at domain transition by blocking content
  - Unintended data breach
  - Insider threat detection



Demonstration

OneDrive

SharePoint

Confluence

Exchange

File Share

Google Drive



Filename	Filesize	Status	OCR	Risk Score
MED_Arbeitsunfähigkeit.pdf	210.25 KB	Completed	Only Images	4.7 / 5.0
WEB_AuszugMitgliederTippspiel.pdf	116.26 KB	Completed	Only Images	4.4 / 5.0
HR_Arbeitszeugnis.pdf	137.44 KB	Completed	Only Images	4.1 / 5.0
PPT_HABITUS_Next-Steps_02192026.pdf	1534.19 KB	Completed	Only Images	3.9 / 5.0
HR_Immatrikulation.pdf	179.35 KB	Completed	Only Images	3.5 / 5.0
EMAIL_BUSINESS_Rechnungskorrektur.pdf	145.41 KB	Completed	Only Images	2.8 / 5.0
EMAIL_PRIVAT_Zahnarzt.pdf	136.17 KB	Completed	Only Images	2.7 / 5.0
EMAIL_BUSINESS_Schulungsbestaetigung.pdf	437.04 KB	Completed	Only Images	2.7 / 5.0
AMTLICH_Kirchenaustritt.pdf	233.52 KB	Completed	Only Images	2.5 / 5.0
HR_CV_Deutsch.pdf	323.24 KB	Completed	Only Images	2.3 / 5.0
INVOICE_OpenAI.pdf	86.77 KB	Completed	Only Images	2.1 / 5.0
HR_Studienbescheinigung.pdf	369.79 KB	Completed	Only Images	1.9 / 5.0
RnD_Paper_TUM_woRef.pdf	681.64 KB	Completed	Only Images	1.2 / 5.0
HR_CV_Englisch.pdf	15.69 KB	Completed	Only Images	1.2 / 5

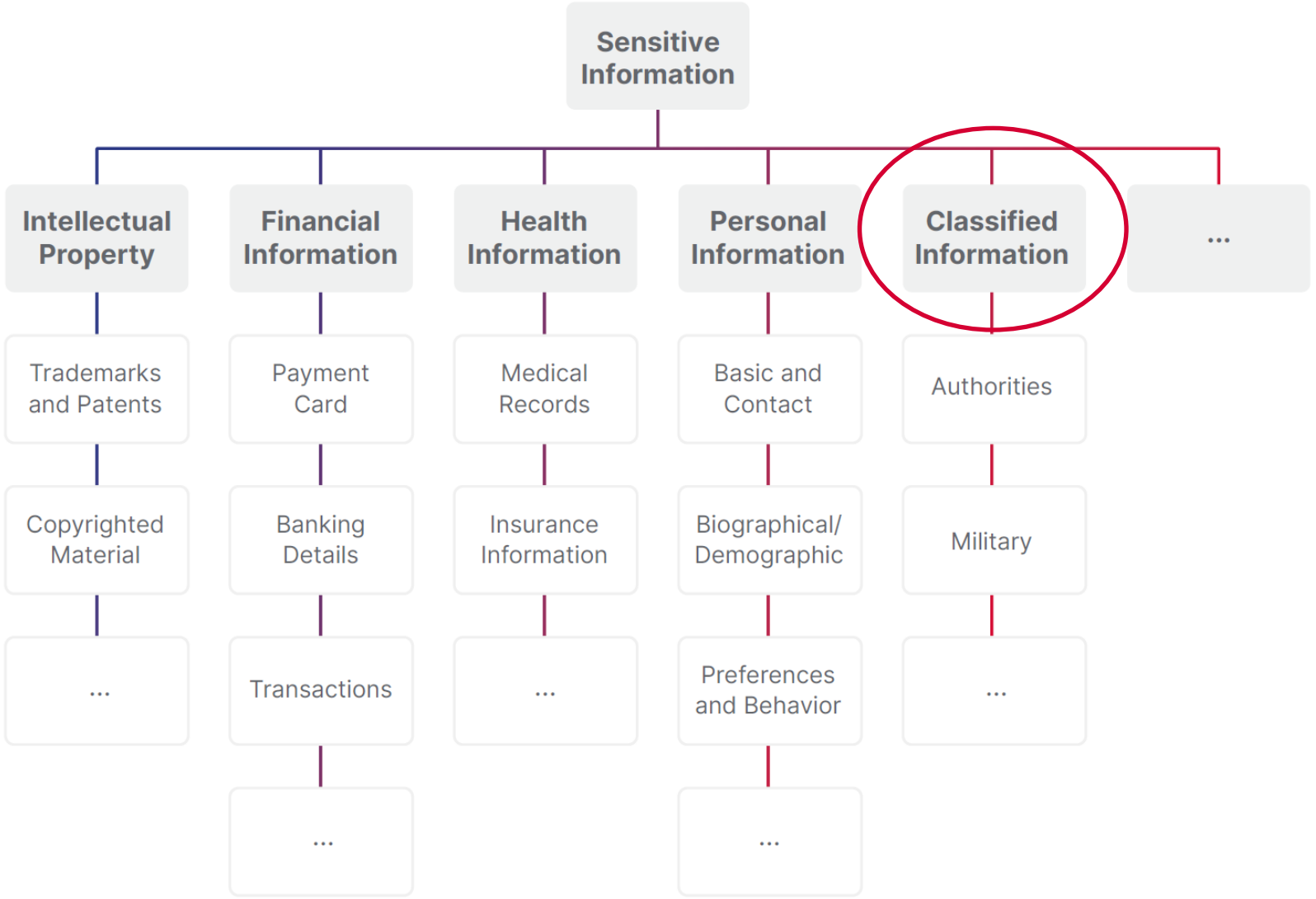
Agenda

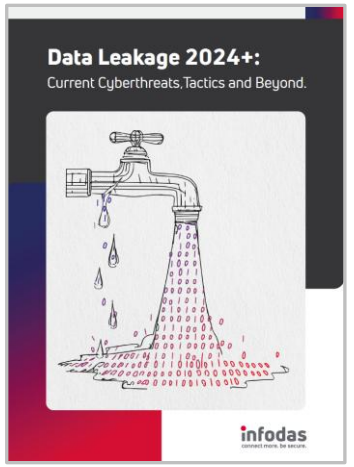
03

DCS/ZT: Enhanced Data Labeling



Which Data is Leaked Most ...

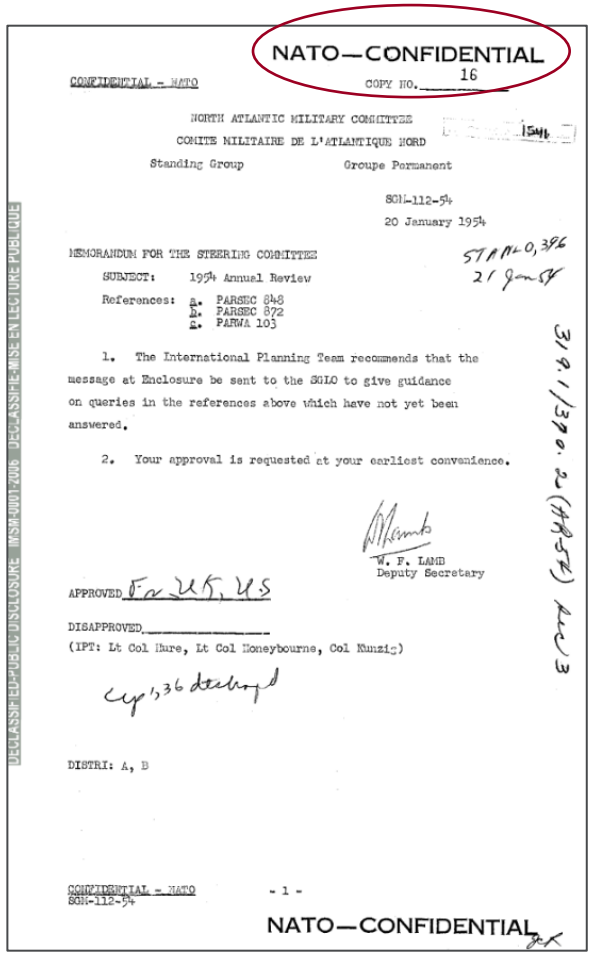




Is this Information Classified?



https://www.behoerden-spiegel.de



NATO—CONFIDENTIAL

CONFIDENTIAL - NATO COPY NO. 16

NORTH ATLANTIC MILITARY COMMITTEE
COMITE MILITAIRE DE L'ATLANTIQUE NORD
Standing Group Groupe Permanent

SGM-112-54
20 January 1954

MEMORANDUM FOR THE STEERING COMMITTEE

SUBJECT: 1954 Annual Review

References: a. PARSEC 848
b. PARSEC 872
c. PARWA 103

1. The International Planning Team recommends that the message at Enclosure be sent to the SGLO to give guidance on queries in the references above which have not yet been answered.

2. Your approval is requested at your earliest convenience.

W. F. LAND
Deputy Secretary

APPROVED

DISAPPROVED

(IPT: Lt Col Hare, Lt Col Honeybourne, Col Kunzig)

DISTRI: A, B

CONFIDENTIAL - NATO - 1 -
SGM-112-54

NATO—CONFIDENTIAL

DECLASSIFIED/PUBLIC DISCLOSURE MSM 0001-2006 DECLASSIFIE/MISE EN LECTURE PUBLIQUE

https://archives.nato.int



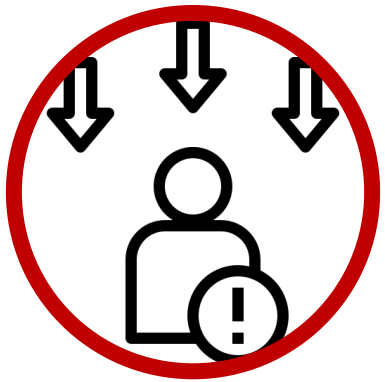
https://maps.google.com

Data-Centric Security Approach at Armed Forces

STANAG-conform Security Labels



Human Factors in the Classification Process



unintentional error

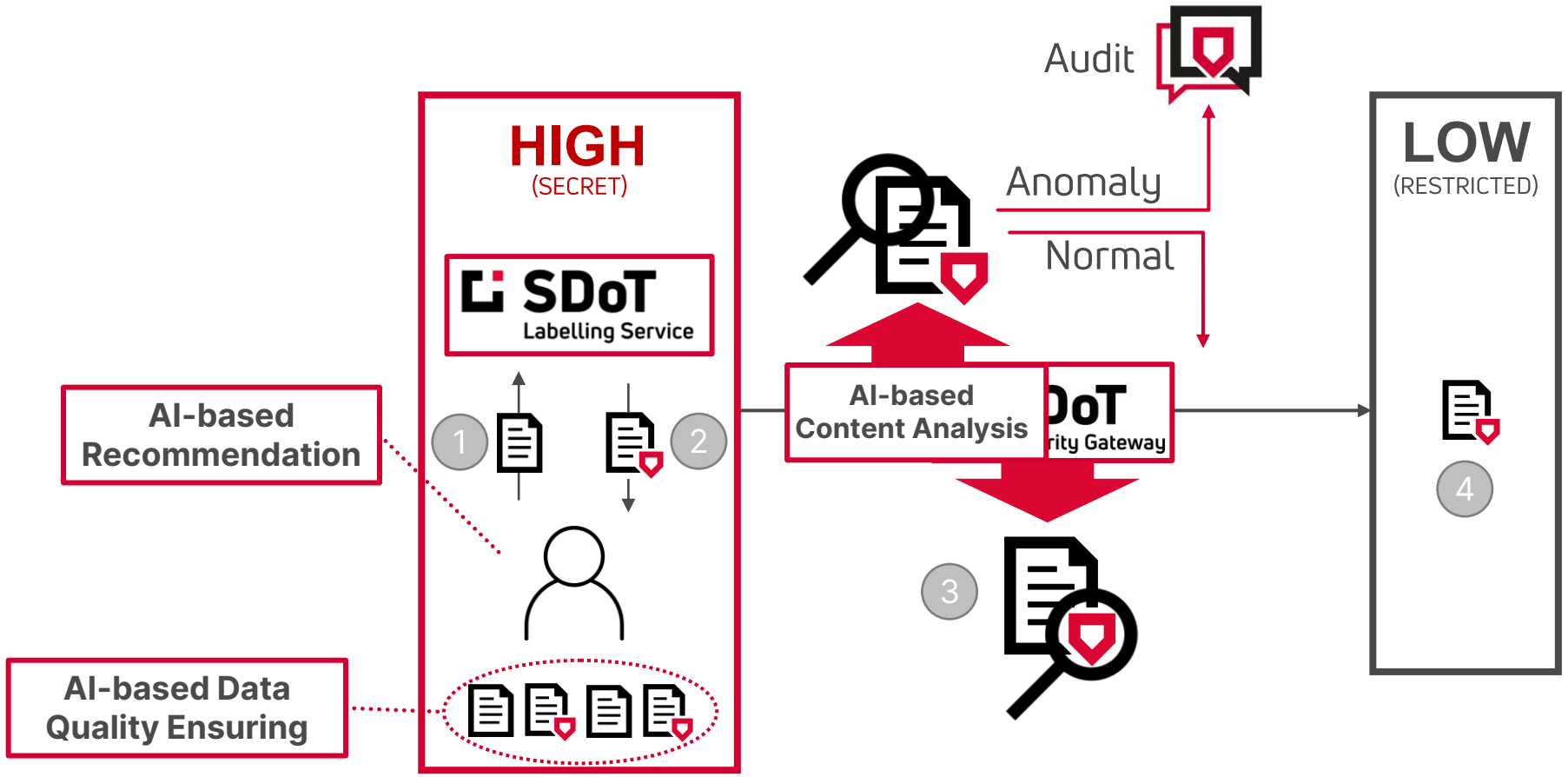
- Heavy load and new missions
- Digitization and complexity
- Uncertainty and misconception

intentional error

- Deliberate manipulation
- Insider attack

Technical measures against (un)intentional data leakage are limited because of a specific source of error, i.e. humans!

Enhancing Data Labeling using AI: Overview



Agenda

04

Closing and FAQ





Christopher Coppess

Regional Manager CEE & North America

M. : +49 151 58403261

c.coppess@infodas.de

Rhonestr. 2

50765 Cologne

Germany

www.infodas.com

infodas
connect more. be secure.

connect more.
be secure.