DATA GOVERNANCE
MANAGING UNSTRUCTURED DATA

NextGen DSPM

Data Security Posture Management

Georg Bommer – Consultant
Benjamin Kern – Software & Data Engineer

Agenda

- Was ist DSPM
- DSPM und KI
- NextGen DSPM
- Zusammenfassung
- Datagovernance Plattform

DATA GOVERNANCE

Hype um «DSPM»

- ist die am schnellsten wachsende Sicherheitskategorie (Cyera)
- ermöglicht Echtzeit-Einblicke und Sicherheitsbewertungen (Netskope)
- deckt Schatten-IT und unstrukturierte Daten auf (Proofpoint)
- bildet die Grundlage für den sicheren Einsatz von KI (Security ai)
- wird als Schlüssel zur datenzentrierten Sicherheitsstrategie gesehen (Microsoft)
- gilt als Game Changer für datengesteuerte Risikoentscheidungen (Forcepoint)
- ist ein zentraler Baustein für Zero Trust in der Cloud (IBM)

Bis 2026 werden 20 % der Unternehmen DSPM Technologie einsetzen

(Prognose Gartner)

DATA GOVERNANCE

DSP und DSPM

Das Data Security Posture Management (DSPM) bietet Transparenz darüber, wo sich sensible Daten befinden, wer Zugriff auf diese Daten hat, wie sie verwendet wurden und wie die Sicherheitslage der gespeicherten Daten oder Anwendungen ist.

Dazu wird der aktuelle Stand der Datensicherheit bewertet, potenzielle Risiken und Schwachstellen identifiziert und klassifiziert, Sicherheitskontrollen zur Minderung dieser Risiken implementiert und die Sicherheitslage regelmäßig überwacht und aktualisiert, um ihre Wirksamkeit sicherzustellen.

Dadurch können Unternehmen die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Daten gewährleisten.

Zu den typischen Anwendern von DSPM gehören IT-Abteilungen, Sicherheitsteams, Compliance-Teams und die Geschäftsleitung.

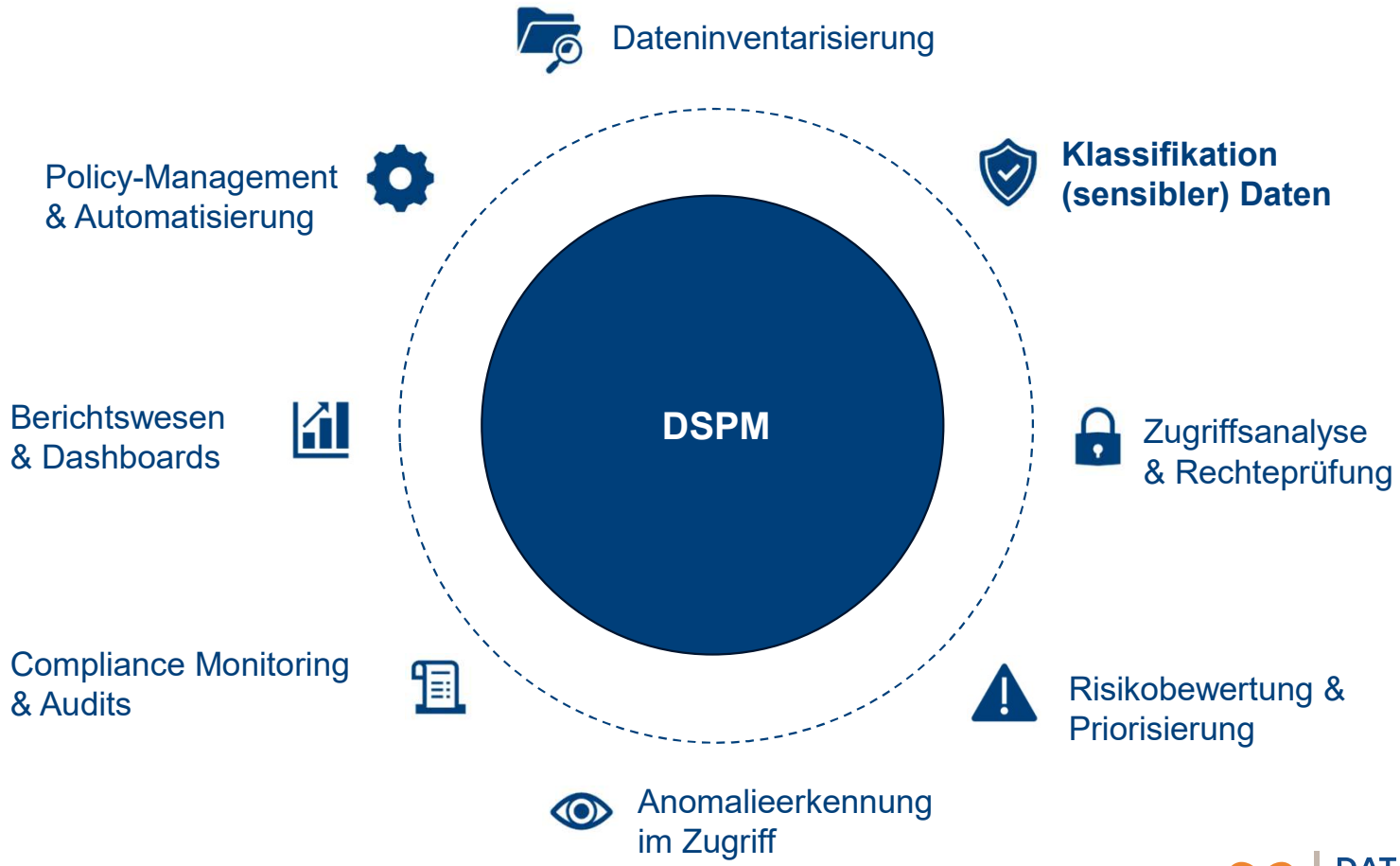
(Quelle Gartner)

Ziel von DSPM

- Zentrale Kontrolle über die Daten erhalten
- Kontext der Daten verstehen und klassifizieren
- Anomalien und potenzielle Bedrohungen erkennen
- Risiken, und Schwachstellen identifizieren und bewerten
- Sicherheitsrichtlinien und Compliance-Anforderungen durchsetzen
- Berichtswesen und Audits automatisieren

DSPM schafft Transparenz, Kontrolle & Risikobewusstsein auf Datenebene

Hauptfunktionen



DATA GOVERNANCE

DSPM und KI

Einsatzmöglichkeiten von KI in DSPM

Automatische Datenklassifikation

- Analysiert Inhalte und Metadaten, um sensible Daten wie PII, PHI, Finanzdaten automatisch zu erkennen

Verhaltensbasierte Anomalieerkennung

- Analyse des Nutzerverhaltens (z. B. Zugriffsmuster, Zeit, Ort, Datenvolumen)
- Erkennung abweichender Aktivitäten, die auf Missbrauch, Fehler oder Angriffe hindeuten

Kontextuelle Risikobewertung

- Kombiniert Datenart, Zugriffshäufigkeit, Nutzerrolle und Speicherort zur dynamischen Risikoermittlung
- Risikostufen und Eskalationsempfehlungen werden automatisch generiert

Priorisierung und Entscheidungshilfe

- Identifikation der relevantesten Risiken für Security-Teams
- Automatisierte Empfehlungen zur Policy-Anpassung oder Rechteänderung

Schutz vor Shadow Data

- Erkennen von Datenquellen, die ausserhalb der bekannten und verwalteten Systeme liegen
- Hilfreich bei der Aufdeckung von Schatten-IT und unerkannten Speicherorten

Adaptive Access Control

- Einsatz von Reinforcement Learning zur dynamischen Anpassung von Sicherheitsrichtlinien an reale Zugriffsmuster

Kriterien für den Einsatz von KI und die Wahl vom geeigneten Modell

Technologie

- Funktionalität für spezifische Use Case
- Genauigkeit, Erklärbarkeit
- Ressourcenbedarf, Skalierbarkeit, Performance
- Integration in IT-Security Umgebung

Aufwand

- Technische Implementierung
- Datenaufbereitung, Training vom Modell
- Kontinuierliche Optimierung

Ressourcen

- Technisches Know-How, Business Know-How
- Mitwirkung vom verschiedenen Stellen

Kosten

- Lizenz und Service Modell
- Betriebskosten

Sicherheit und Datenschutz

- Interner oder externer Betrieb

DATA GOVERNANCE

Paradigmen und Modelle - Teil 1

Supervised Learning - Klassifikation sensibler Daten (z. B. PII, IP)

- Vorteile: Hohe Genauigkeit bei guter Datenbasis, leicht prüfbar
- Nachteile: Hoher Aufwand für gelabelte Trainingsdaten

Unsupervised Learning - Erkennung unbekannter Muster oder Shadow Data

- Vorteile: Erkennt neue Risiken, ohne Vorwissen
- Nachteile: Geringere Präzision, schwer erklärbar

Reinforcement Learning - Adaptive Access Control Steuerung und Zugriffsentscheidungen

- Vorteile: Lernfähig, anpassbar an Veränderungen
- Nachteile: Komplex in Entwicklung, schwer vorhersagbares Verhalten

Paradigmen und Modelle – Teil 2

Neuronale Netze > Deep Learning - Analyse komplexer unstrukturierter Daten (Texte, E-Mails)

- Vorteile: Hohe Leistung bei grossen Datenmengen
- Nachteile: Erklärbarkeit und Trainingsaufwand hoch, ressourcenintensiv

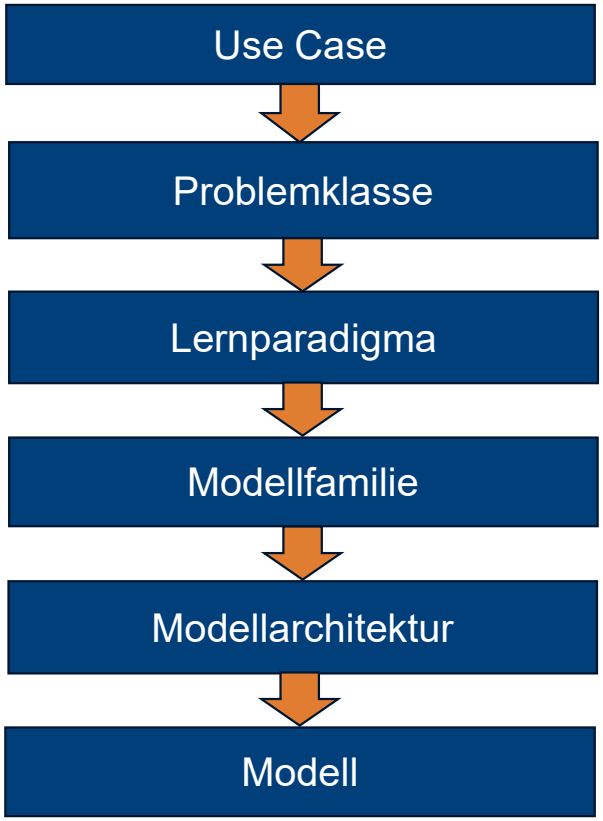
Statistical Machine Learning - Anomalie-Erkennung bei Datenzugriffen

- Vorteile: Hohe Erklärbarkeit (White-Box-Modelle), Geringer Rechen- und Datenaufwand
- Nachteile: Begrenzte Leistung bei komplexen, hochdimensionalen Daten, Schlechtere Skalierbarkeit bei sehr grossen Datenmengen

Ensemble Learning - Kombinierte Klassifikation und Risikobewertung

- Vorteile: Geringeres Fehlerpotenzial durch Modellkombination
- Nachteile: Erhöhter Rechen- und Verwaltungsaufwand

Modellwahl – Beispiel 1



Klassifikation von Daten

Klassifikation

Unsupervised Learning

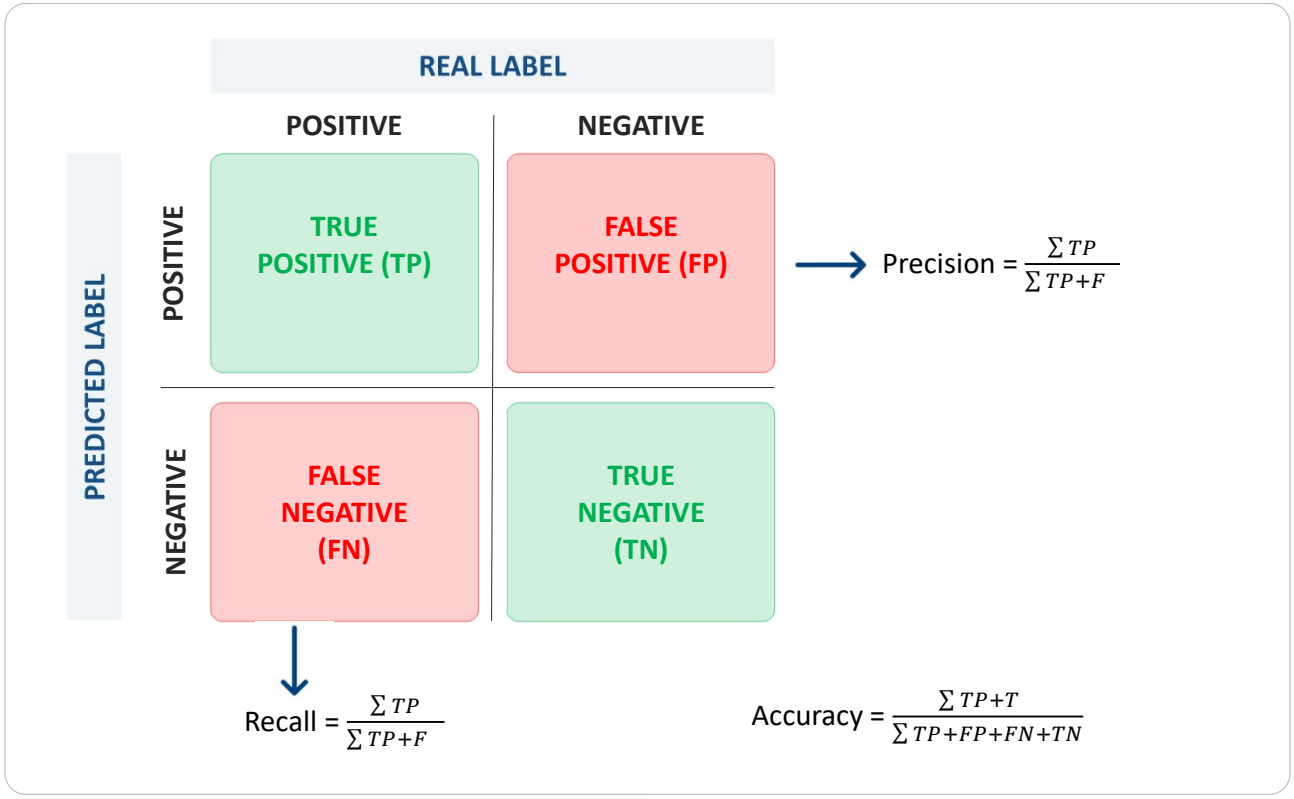
Clustering-Verfahren

Partitionierend (k-Means)

K-Means mit k=3 (nicht-sensibel, hoch-sensibel, unklar)

DATA GOVERNANCE

Metriken zu Klassifikations-Modellen

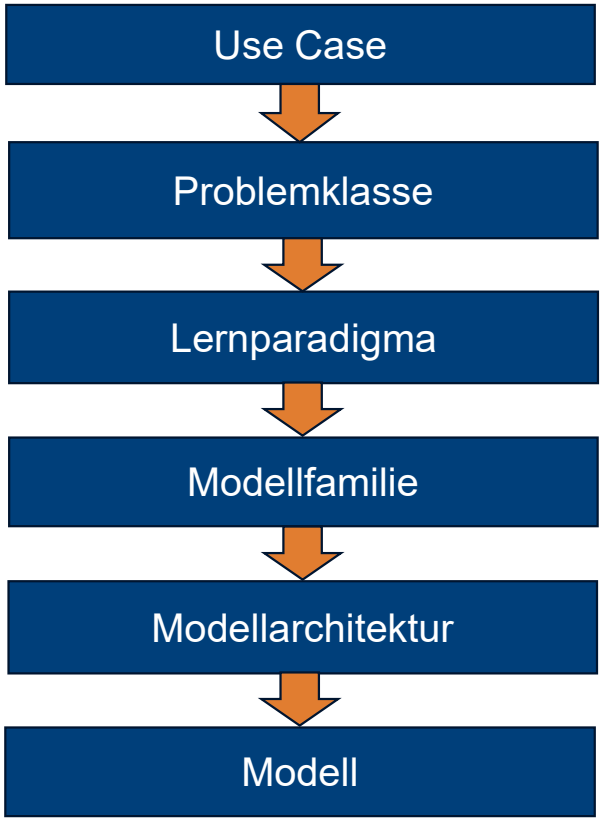


Sensible Daten

Nicht-Sensible Daten

DATA GOVERNANCE

Modellwahl – Beispiel 2



Adaptive Access Control

Optimierungsproblem

Reinforcement Learning

Agentenbasierte Entscheidungsmodelle

Q-Learning

Deep Q-Network

DATA GOVERNANCE

NextGen DSPM

Automatisierte Datenaufbereitung & Training
Vorverarbeitung und Modelltraining werden beschleunigt, der manuelle Aufwand reduziert

Erweiterte semantische Datenklassifikation
Kontextbasierte Erkennung sensibler Inhalte

Integration mit SOAR & Sicherheitsprozessen
DSPM-Ergebnisse fliessen direkt in Security-Orchestration und Reaktion ein.

Ganzheitliches Sicherheitsmanagement
DSPM interagiert aktiv mit Business, IT und Datenschutz.

Einbindung der Data Owner, Compliance Officer, Security Officer und Legal in den Prozess
Klare Rollen, Feedbackschleifen und nutzbare Werkzeuge für datenverantwortliche Personen.

DATA GOVERNANCE

Unsere aktuellen Projekte

Kontextbasierte Suche

- Zur Datenvorbereitung und Qualitätsoptimierung von Stammdaten (Personen, Firmen, Addressen aus CRM und ERP)

Chatbot

- Datenbankabfragen aus natürlicher Sprache generieren
- Technologie: RAG (Retrieval Augmented Generation)

Data Harmonizer

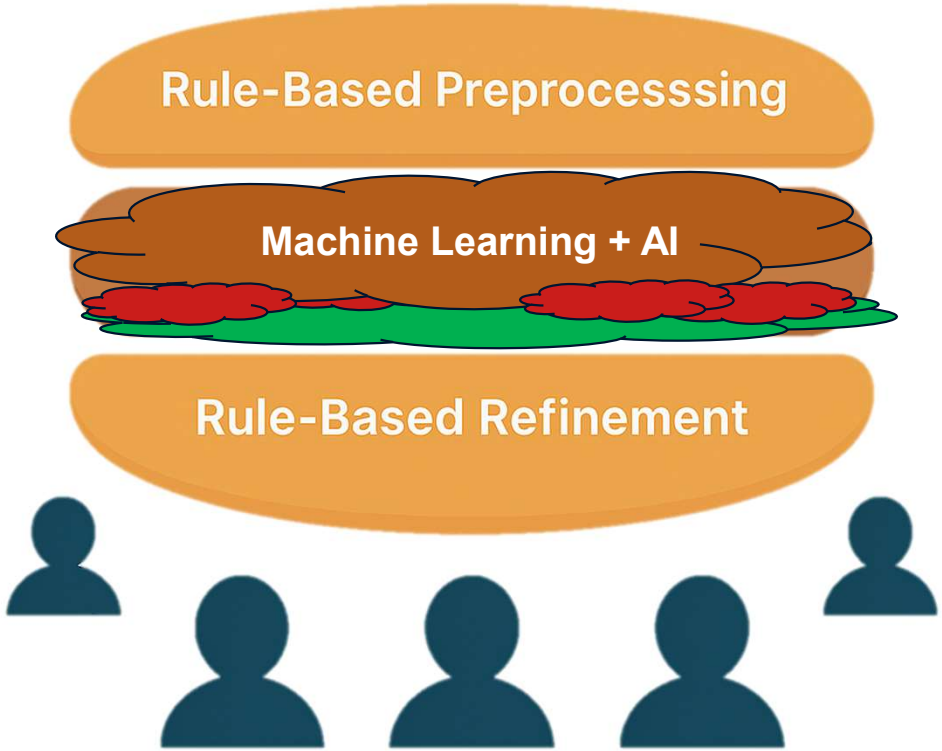
- Zur Datenvorbereitung und Qualitätsoptimierung von Stammdaten (Personen, Firmen, Addressen aus CRM und ERP)

Adaptive Access Control

- Dynamische Profile generieren für den Zugriff auf Daten in Microsoft365 (Teams, SharePoint, Co-Pilot)

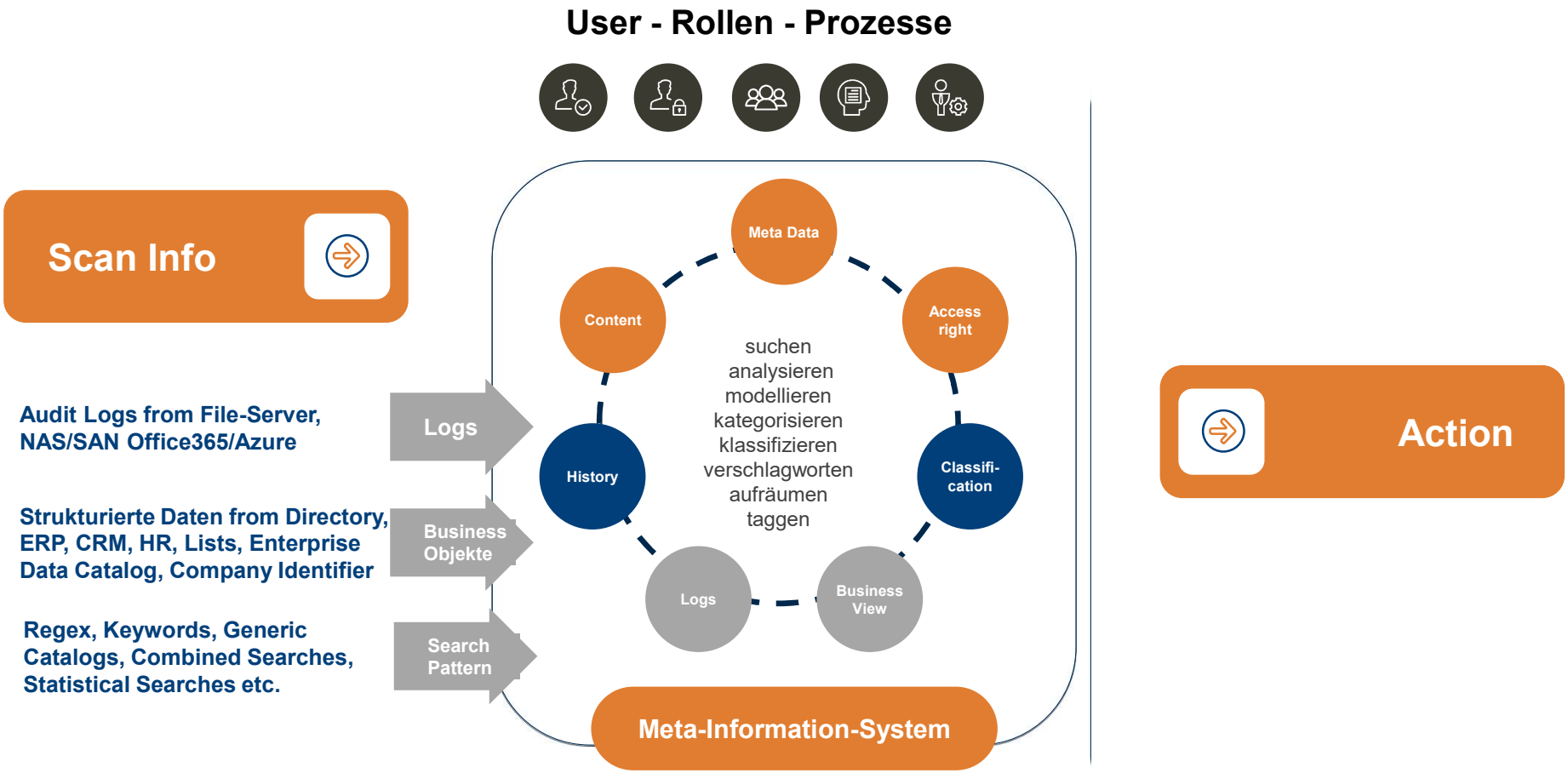
DATA GOVERNANCE

Zusammenfassung



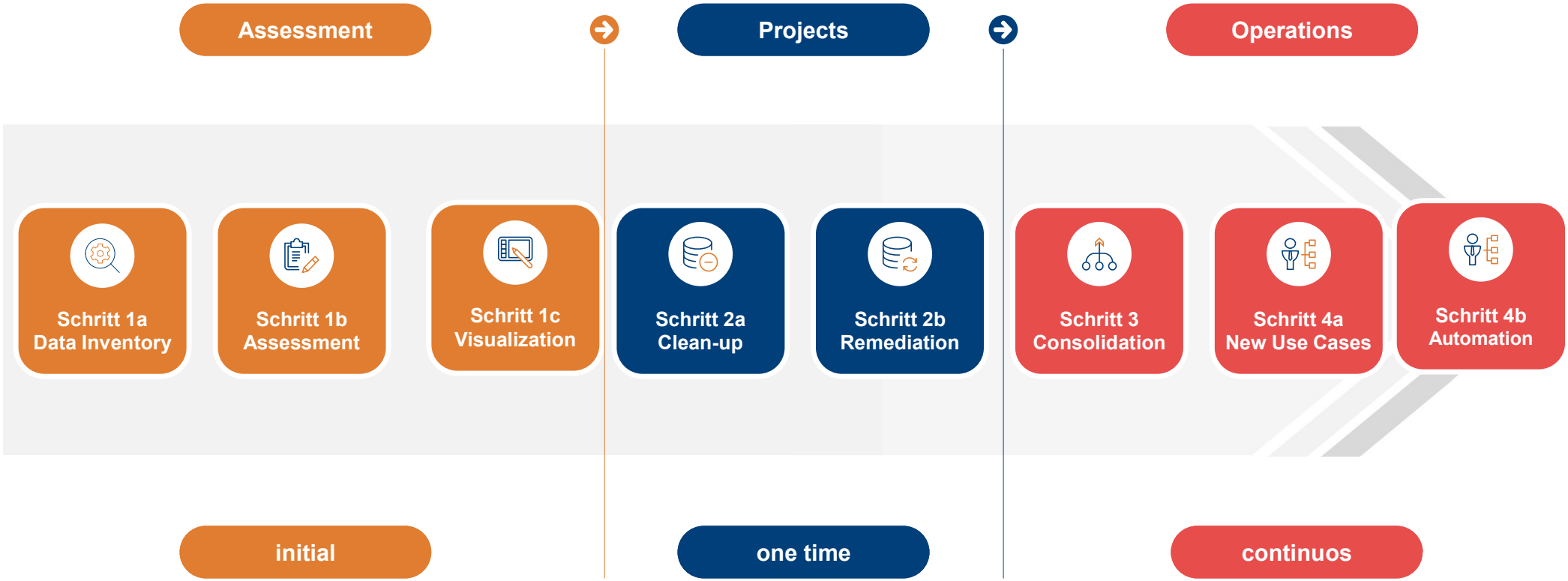
DATA GOVERNANCE

DGS – Data Governance Plattform



DATA GOVERNANCE

Vorgehensmodell



DATA GOVERNANCE

Georg Bommer
gbo@datagovernance.tech

Benjamin Kern
bke@datagovernance.tech

DATA GOVERNANCE

MANAGING UNSTRUCTURED DATA