# Anomalien in Schwachstellen-Behebungsprozessen

Florian Stertz

# Über uns

## Facts condignum:

- 2019 in Wien gegründet
- in Österreich und Deutschland vertreten
- integrierte Security Management Software
- Professional Services

## Mich

- Florian Stertz
- Ausbildung:
  - Masterstudium Medizinische Informatik an Med. Universität Wien, 2016
  - Doktoratsstudium Wirtschaftsinformatik an Universität Wien, 2022
- Wissenschaftliches Profil: https://scholar.google.com/citations?user=eKjsMEkAAAAJ&hl=en
- Wissenschaftlicher Mitarbeiter 2013-2022, Lektor 2016-
- Software Developer 2022 -

# Agenda

- Was sind Prozesse?
- Wie kann ich Prozesse erkennen?
- Welche Anomalien können auftreten?
- Wie kann ich diese automatisch finden?
- Conclusio

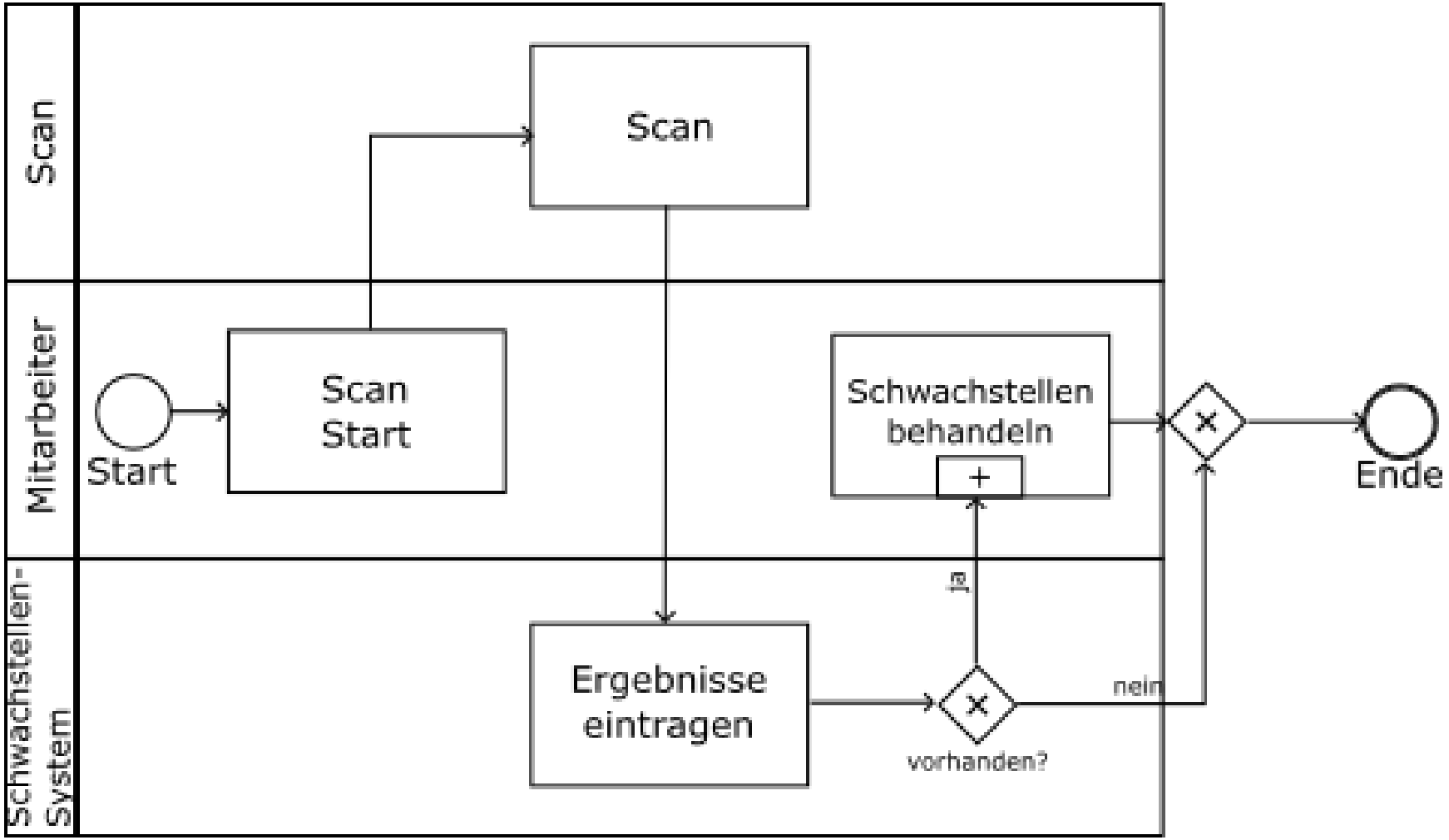
# Was sind Prozesse?

“Business processes represent a core asset of corporations”

-- Dumas, Fundamentals of Business Process Management

- Prozesse beschreiben Verbindungen und Interaktionen zwischen Resourcen
- Die Analyse des Verhalten von Prozessen ist definiert als “Business Process Management”

# Was sind Prozesse?



# Wie kann ich Prozesse erkennen?

# Process Mining Basis

- Process Mining ermöglich das Verhalten von Prozessen zu entdecken und analysieren auf Basis von Event Daten

- Ein Prozess besteht aus mehreren Instanzen, welche aus einer Reihenfolge von Events bestehen.
- …

```
<event>
  <string key="concept:name"> values="Scan"/>
  <string key="lifecycle:transition" value="start"/>
  <string key="org:resource" value="Open VAS Scan"/>
  <date key="time:timestamp" value="2024-01-01T09:22:51"/>
</event>
```

…

# Process Mining Basis

- Process Mining befasst sich mit 3 Bereichen:
  - Process Discovery
  - Conformance Checking
  - Process Enhancement

# Welche Anomalien können auftreten?

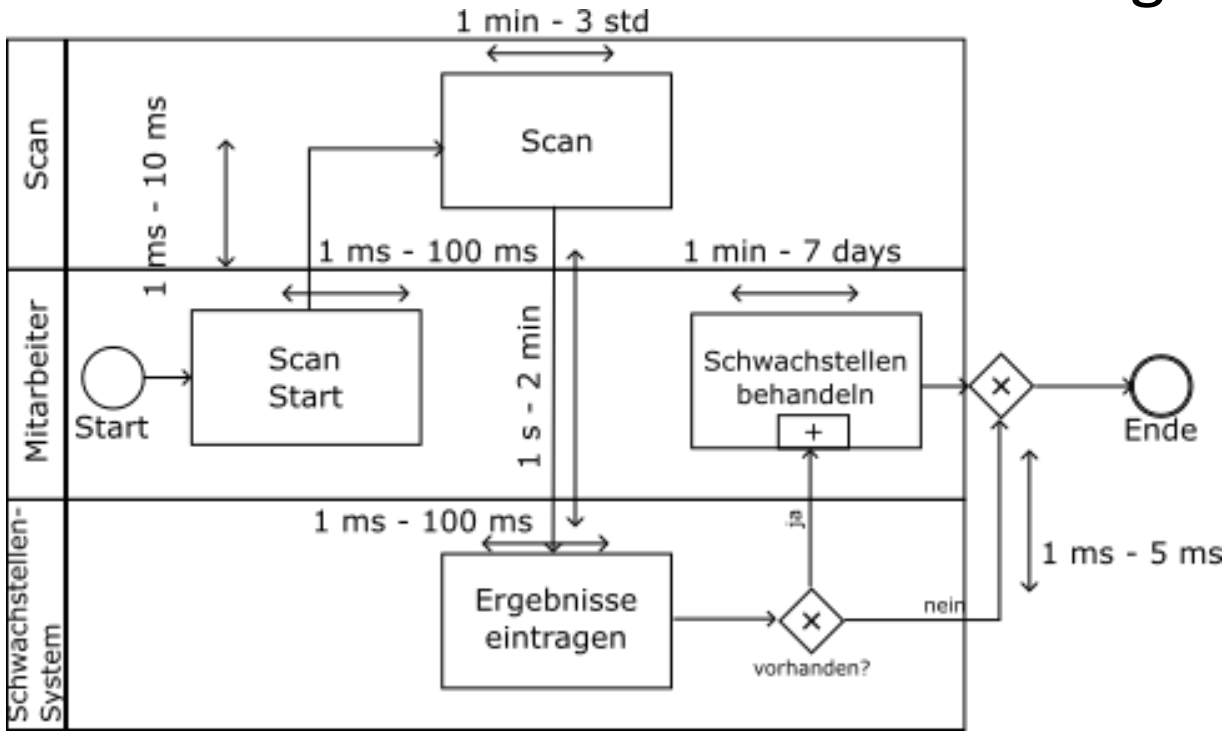
# Prozess Verhalten

- Conformance Checking fokusiert sich oft auf die Reihenfolge und Daten der Events → Es ist ein Fehler passiert, wenn die Ergebnisse des Scans bereits eingetragen wurden, obwohl Scan erst danach gestartet wurde.

- Doch auch die Events untereinander stehen in einer Beziehung zu einander

# Temporales Verhalten

- Ein Aktivität im Prozess kann über eine durschnittliche Dauer verfügen
- Die Dauer zwischen Aktivitäten kann hier ebenfalls weitere Information über das Verhalten von Prozessen bringen.



# Wie kann ich Anomalien automatisch entdecken?

# Intelligente Anpassungen des erwarteten Verhaltens

- Daten einer Prozessinstanz können das Verhalten eines Prozesses beeinflussen.
  - Ein Scan über eine IP-Range wird wahrscheinlich länger dauern als ein Scan über ein System
  - Verschiedene Schwachstellen können die Aktivität des Behandelns beeinflussen
  - Die Kennzahlen einer Firma können den Prozess beeinflussen.

# Clustering der entdeckten Verhalten

- Daten einer Prozessinstanz können das Verhalten eines Prozesses beeinflussen.
  - Ein Scan über eine IP-Range wird wahrscheinlich länger dauern als ein Scan über ein System
  - Verschiedene Schwachstellen können die Aktivität des Behandelns beeinflussen
  - Die Kennzahlen einer Firma können den Prozess beeinflussen.

# Profile erkennen und automatisch anwenden

- DBSCAN Algorithmus → Cluster ohne Anzahl zu Wissen
- Classifier anhand von Cluster → Zuordnen neuer Daten zu alten Clustern
- Process Mining Algorithmen → Anwendung auf spezialisiertes Profil

# Conclusio

# Conclusio

- Prozesse können als Arbeitsabläufe einer Organisation gesehen und analysiert werden
- Process Mining Algorithmen ermöglichen eine Darstellung unbekannter Prozesse auf Basis von Event-Daten sowie einer Überprüfung auf Compliance
- Methoden des Maschinellen Lernens können die Instanzen dieser Prozesse einem Profil zuordnen, welches eine detaillierte Analyse ermöglicht.

# Danke, für Ihre Aufmerksamkeit