ITSENSE

SWISS MADE IAM

# Willkommen im IAM-Circle!

abraxas

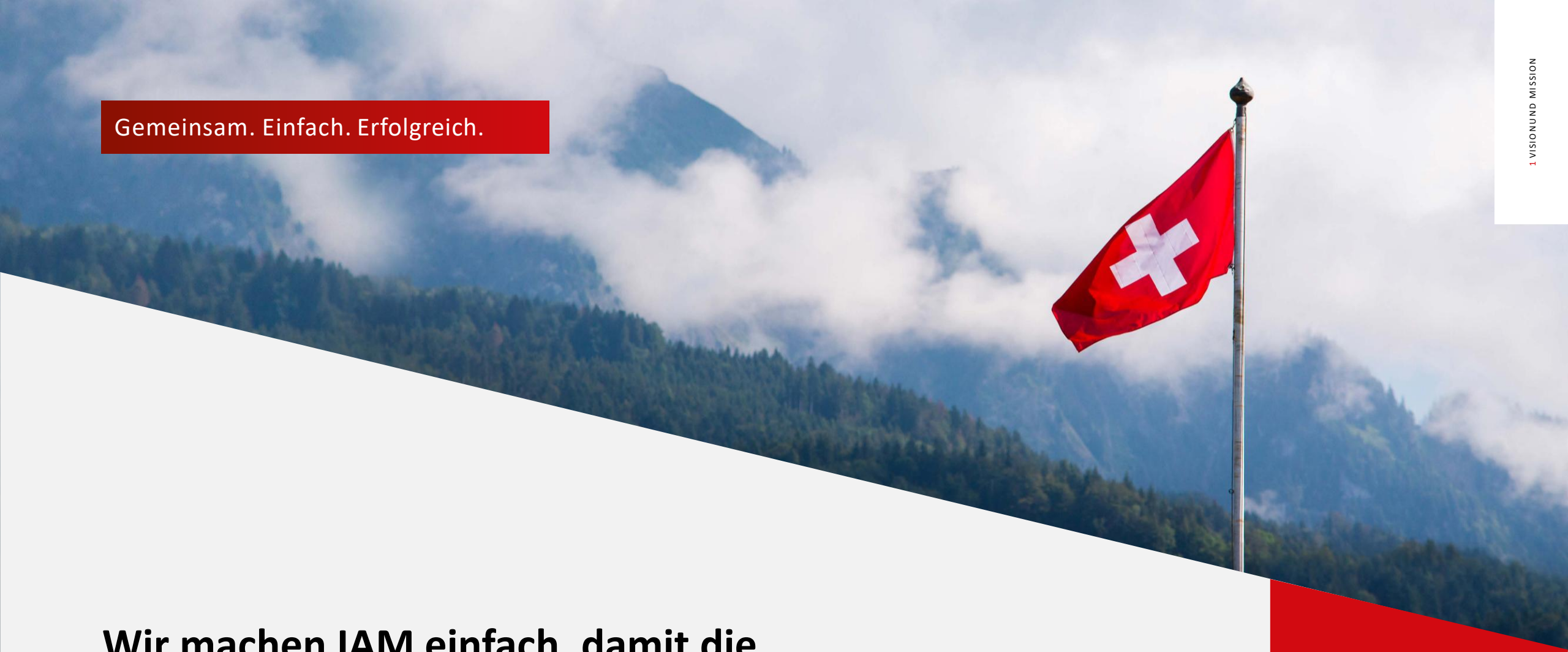
ti&m

COPEBIT

white rabbit Communications

netzmedien

#10

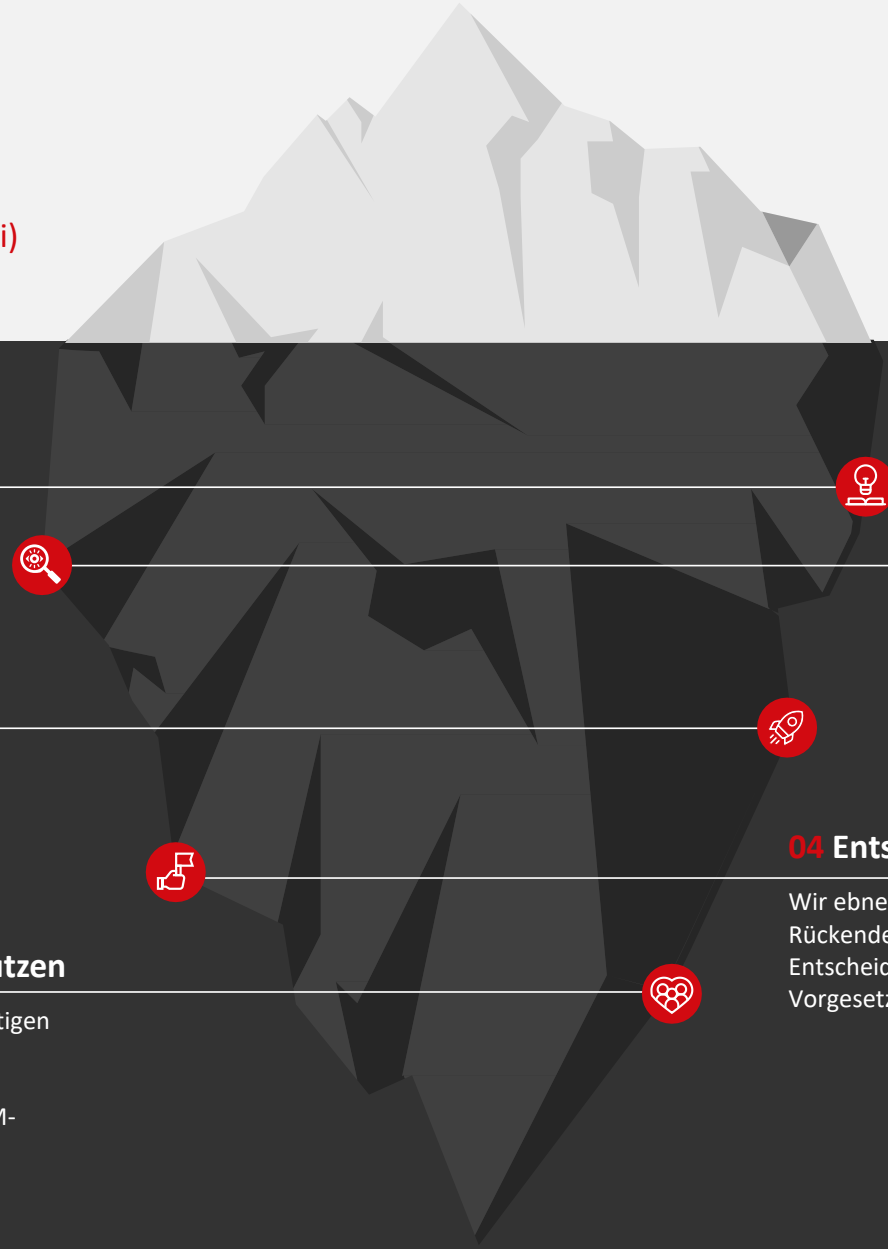


Gemeinsam. Einfach. Erfolgreich.

**Wir machen IAM einfach, damit die Schweiz sicher wird:** für dich, für uns und für den Rest der Welt!

ITSENSE

# 5 überzeugende Gründe für eine #Mitgliedschaft (kostenfrei)



## 01 Fachwissen vertiefen

Im IAM-Circle vertiefen wir gemeinsam mit Gleichgesinnten aktuelles Wissen zu IAM und IT-Security.

## 02 Projekte erfolgreich realisieren

Mit dem Wissen kannst du IAM-Projekte erfolgreich und wirtschaftlich in Unternehmen initiieren und umsetzen.

## 03 Community-Support nutzen

Unsere Community schafft den richtigen Klick, wenn du ihn brauchst. Mit relevantem Wissen und passender Kommunikation führst du deine IAM-Projekte zum Erfolg.

## 04 Entscheidungen erleichtern

Wir ebnen den Weg, damit du Rückendeckung von oben bekommst, die Entscheidungsprozesse leicht sind und Vorgesetzte sie verstehen.

## 05 Sicherheit & Klarheit gewinnen

Als Teil des IAM-Circle gewinnst du Sicherheit. Du erhältst Klarheit über die nächsten Schritte und Zugang zu geballtem Fachwissen.

ITSENSE


# #Fokusthema heute

## SIEM & IAM: Hand in Hand für eine starke Cybersicherheit!

ITSENSE

# SIEM und IAM

## für eine robuste Sicherheitsarchitektur

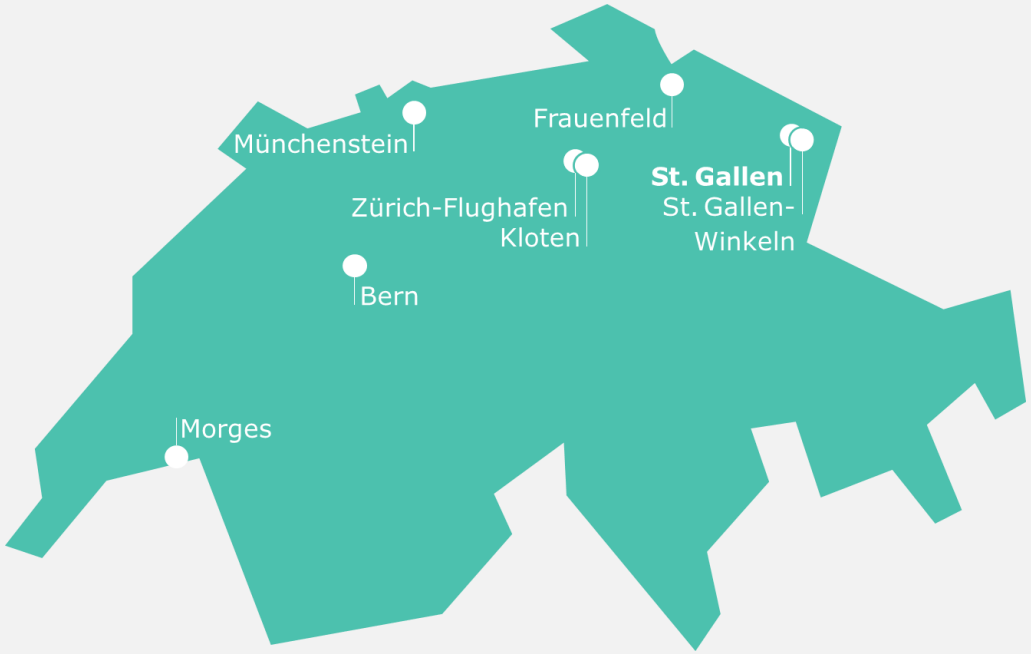
Silvano Fari | 16.06.25 | intern

# Ablauf

| | | |
|---|---|---|
| 1. | Einführung ins Nachmittagsprogramm | 10 Min. |
| 2. | Präsentation: Was ist ein Security Information und Event Management (SIEM) | 30 Min. |
| 3. | Workshop 1 | 30 Min. |
| | Pause | 20 Min. |
| 4. | Präsentation: Robuste Sicherheitsarchitektur dank dem Zusammenspiel von SIEM und IAM / Demo | 30 Min. |
| 5. | Workshop 2 – Diskussion | 30 Min. |

# Abraxas ein Schweizer Unternehmen

## In der ganzen Schweiz vor Ort.




Dienstleistungsertrag 2024
In Mio. CHF

**214.5**

Mitarbeitende
Per 31.12.2024

**984**

## Unsere Aktionäre

**7** Kantone

**141** Gemeinden

## ISO-Zertifizierungen

**ISO 9001**
Quality Management

**ISO 14001**
Bereich Umwelt-management

**ISO 27001**
Security Management

**ISO 20000**
IT Service Management

## Cloud-Zertifizierungen

**+60**

## Unsere Kunden im Fokus

- Bund
- Kantone
- Gemeinden
- Bildung
- Polizei & Justiz
- Versicherungen
- Unternehmen

# Unsere IT-Lösungen und Dienstleistungen für alle Anforderungen.

**Beratung**
Von IT-Strategien bis zu komplexen Prozessberatungen.

**Fachanwendungen**
Von Polizei-Anwendungen bis zu Software für Berufsbildungsämter.

**IAM & SOC**

**Digital Government**
Von Fachanwendungen bis zu voll digitalisierten Verwaltungen.

**IT Services**
Von Workplace bis zu Cloud Services

# Wer sind wir?


Christoph Müller
Leiter Security Solutions
christoph.mueller@abraxas.ch


Silvano Fari
Leiter Cloud Platform Services
silvano.fari@abraxas.ch

# Was ist ein Security Information und Event Management (SIEM)?

## Agenda

- Was ist ein SOC?
- Rollen in einem SOC
- Bausteine eines SOC (SIEM, SOAR)
- Daten- resp. Logeinlieferung in ein SIEM
- Standard- oder Custom-Rules
- Custom-Rule Lifecycle (Logs, Events, Threshold)

# Was ist ein Security Operation Center (SOC)?

- Ein **Security Operations Center (SOC)** ist eine zentrale Einheit innerhalb einer Organisation, die sich rund um die Uhr mit der **Überwachung, Erkennung, Analyse und Reaktion auf IT-Sicherheitsvorfälle** beschäftigt.

- Ziel des SOC ist es, die IT-Infrastruktur vor Bedrohungen zu schützen und Sicherheitsvorfälle möglichst frühzeitig zu erkennen und zu beheben.

# Rollen in einem SOC:

- **SOC Analyst (Tier 1–3)**
  - **Tier 1 Analyst (T1):** Erste Anlaufstelle – überwacht Alarme, filtert False Positives, leitet echte Vorfälle weiter.
  - **Tier 2 Analyst (T2):** Führt tiefere Analysen durch, untersucht Ursachen, bewertet Risiken.
  - **Tier 3 Analyst (T3):** Experte für komplexe Angriffe, Malware-Analyse, Bedrohungsjagd (Threat Hunting).
- **Incident Responder**
  Reagiert auf Sicherheitsvorfälle und leitet Massnahmen zur Eindämmung, Behebung und Wiederherstellung ein.
- **SOC Manager**
  Verantwortlich für das Team, Koordination, Berichterstattung, Strategie und Kommunikation mit anderen Abteilungen.
- **Threat Hunter**
  Proaktiv auf der Suche nach bislang unentdeckten Bedrohungen im Netzwerk.
- **Security Engineer**
  Baut und wartet die technische Infrastruktur des SOC, z. B. SIEM-Systeme und Sensoren.

# Bausteine eines SOC:

- **SIEM (Security Information and Event Management)**
  - Zentraler Baustein für Logsammlung, -korrelation und Alarmierung.
    *Beispiele: Palo Alto Networks Cortex XSIAM, Splunk, IBM QRadar, Microsoft Sentinel, Elastic SIEM*

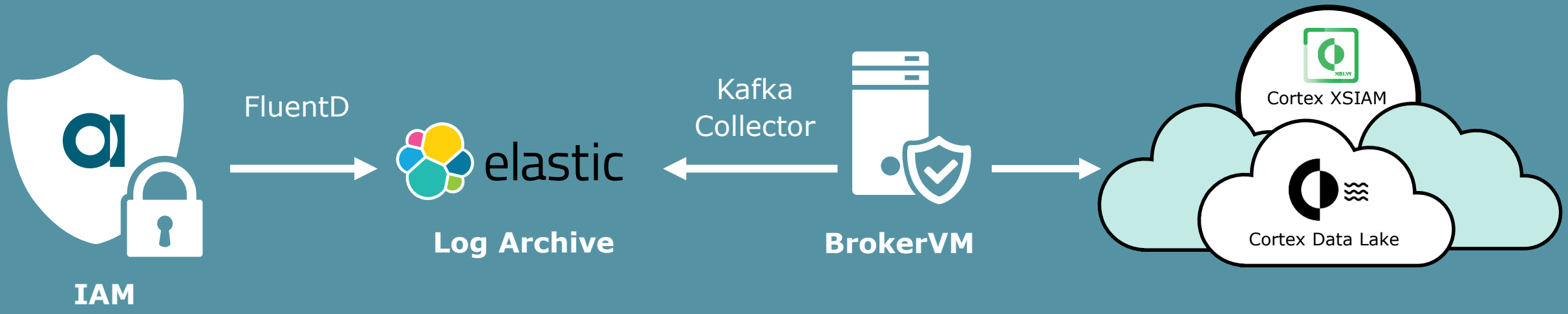
- **EDR/XDR (Endpoint/Extended Detection and Response)**
  - Schutz und Überwachung von Endgeräten (PCs, Server, Mobile Devices).
    *Beispiele: Palo Alto Networks Cortex XSIAM, CrowdStrike, SentinelOne, Microsoft Defender for EP*

- **SOAR (Security Orchestration, Automation and Response)**
  - Automatisiert Reaktionen auf Vorfälle.
    *Beispiele: Palo Alto Networks Cortex XSOAR (und XSIAM), Swimlane, Splunk SOAR*

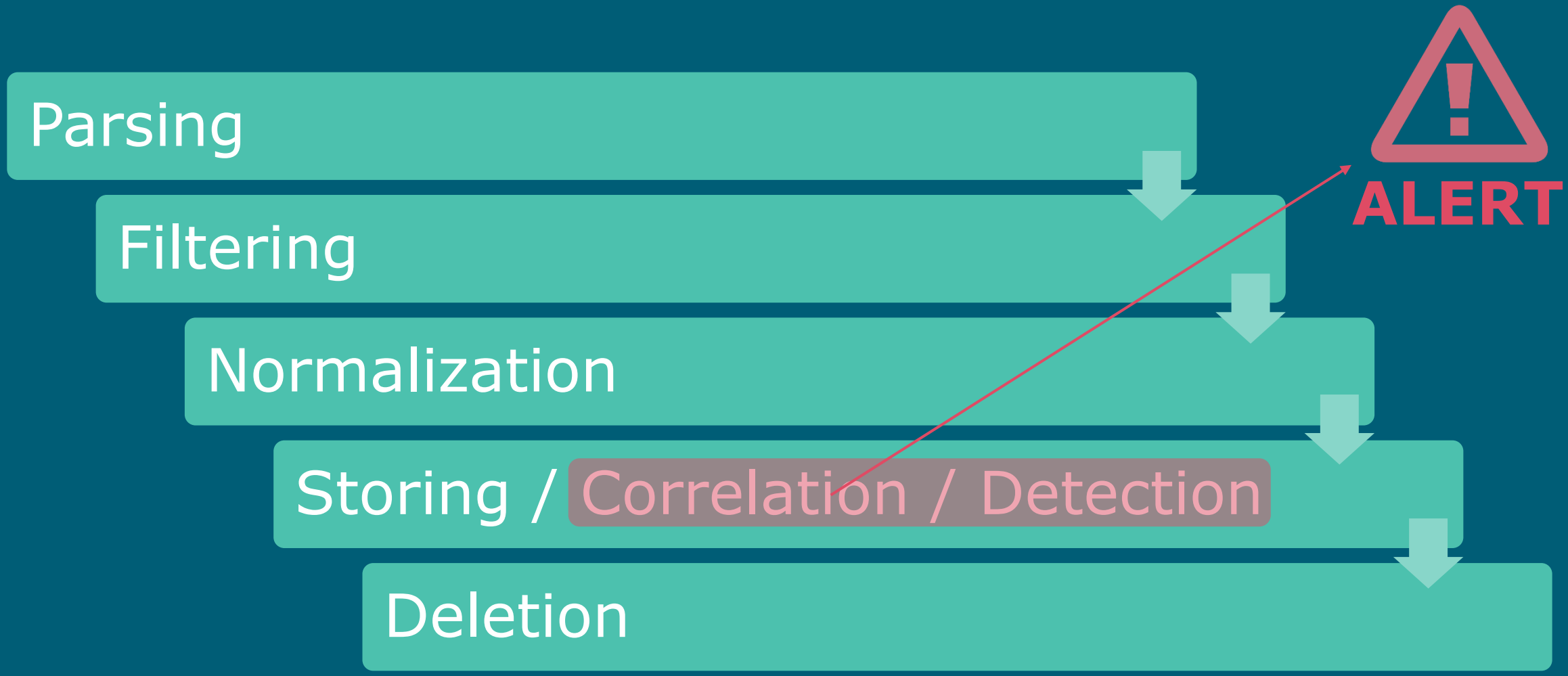
- **Threat Intelligence Plattformen**
  - Informationen über aktuelle Bedrohungen und Angreifer.
    *Beispiele: Palo Alto Networks Cortex XSIAM, MISP, Recorded Future, Anomali*

- **Netzwerküberwachung (NDR – Network Detection and Response)**
  - Analyse von Netzwerkverkehr zur Erkennung verdächtiger Aktivitäten.
    *Beispiele: Palo Alto Networks Cortex XSIAM, Exeon Analytics, Darktrace, Vectra AI*

# Daten-, Logeinlieferung in ein SIEM



# Log Lifecycle



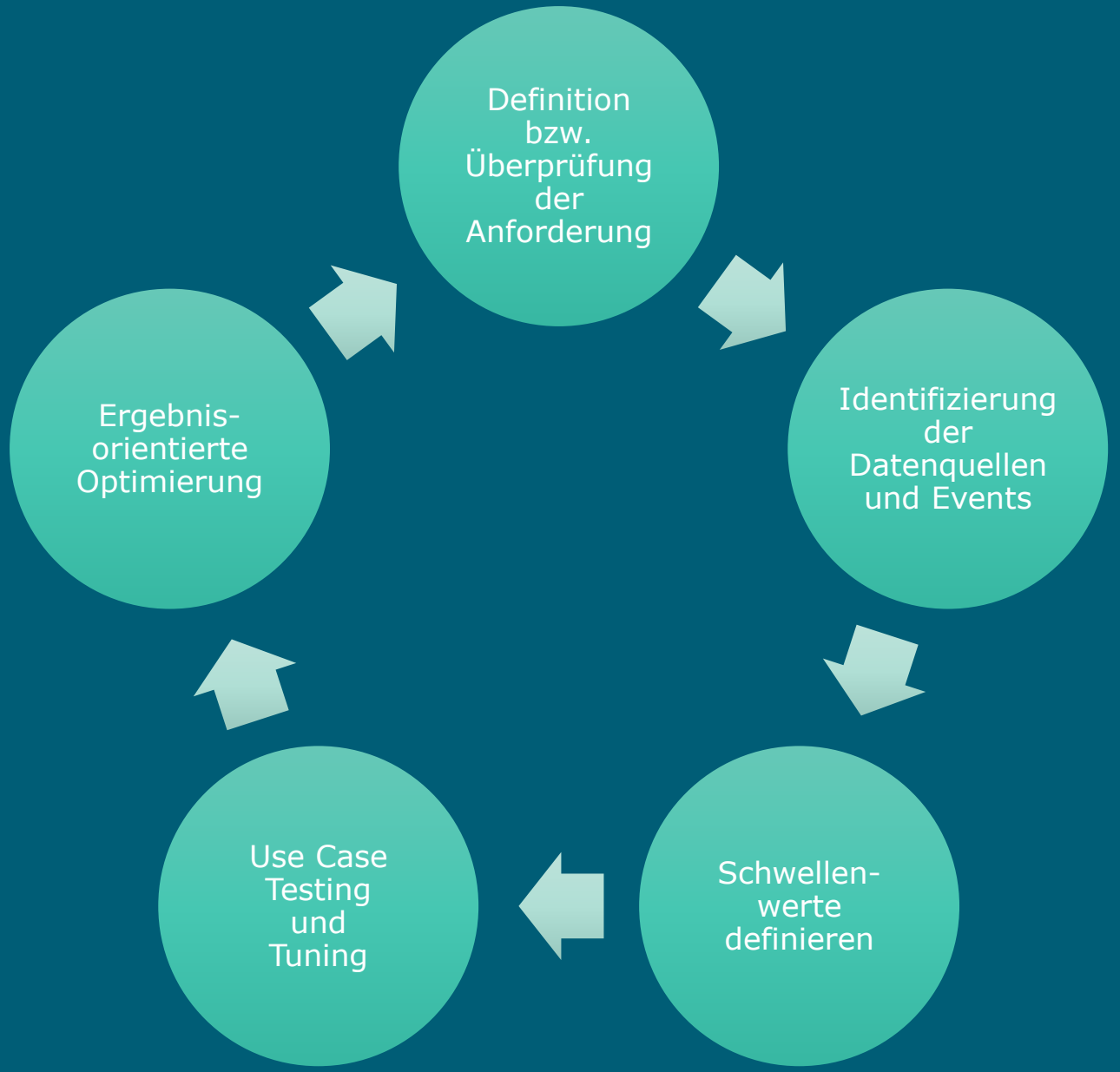
# Standard vs. Custom Rules:

**Standard Rules (vordefinierte Regeln)**
**Merkmale:**
› Werden vom SIEM-Anbieter mitgeliefert.
› Basieren auf **bekannten Angriffsmustern**, Compliance-Anforderungen oder Best Practices.
› Sofort einsatzbereit („Plug and Play“).
**Vorteile:**
› Schneller Start möglich.
› Gute Abdeckung häufiger Bedrohungen (z. B. Brute Force, Anomalien beim Anmelden).
› Oft regelmäßig aktualisiert (Threat Intelligence Feeds).
**Nachteile:**
› **Generisch**, daher mehr False Positives möglich.
› Nicht auf die individuelle IT-Umgebung oder Risiken der Organisation zugeschnitten.

# Standard vs. Custom Rules:

**Custom Rules (benutzerdefinierte Regeln)**
**Merkmale:**
› Werden vom SOC-Team speziell für die eigene Umgebung erstellt.
› Reagieren auf **unternehmensspezifische Bedrohungen oder Prozesse**.
**Vorteile:**
› **Gezielte Erkennung** von Vorfällen, die nur in der eigenen Umgebung relevant sind.
› Weniger Fehlalarme durch Anpassung an echte Risiken.
› Ermöglicht die Abbildung interner Sicherheitsrichtlinien und Geschäftsprozesse.
**Nachteile:**
› **Aufwändiger** in Entwicklung, Pflege und Test.
› Erfordert tieferes Verständnis der eigenen Systeme und Bedrohungen.

# Custom-Rule Lifecycle



# Workshop Teil 1

- Welche **Angriffe** könnt ihr euch auf ein IAM vorstellen?
- Welche Angriffe auf andere Systeme lassen sich dank Daten aus dem IAM erkennen?
- Wie könnten **Regeln** aussehen, um solche Angriffe zu detektieren?
- Was könnten mögliche **Reaktionen** auf einen Alarm aufgrund eines solchen Angriffs sein?

Threat → Rule → Response

- Gibt es Themen aus diesem Umfeld, auf die wir im zweiten Teil oder im zweiten Workshop noch gezielt eingehen sollten?

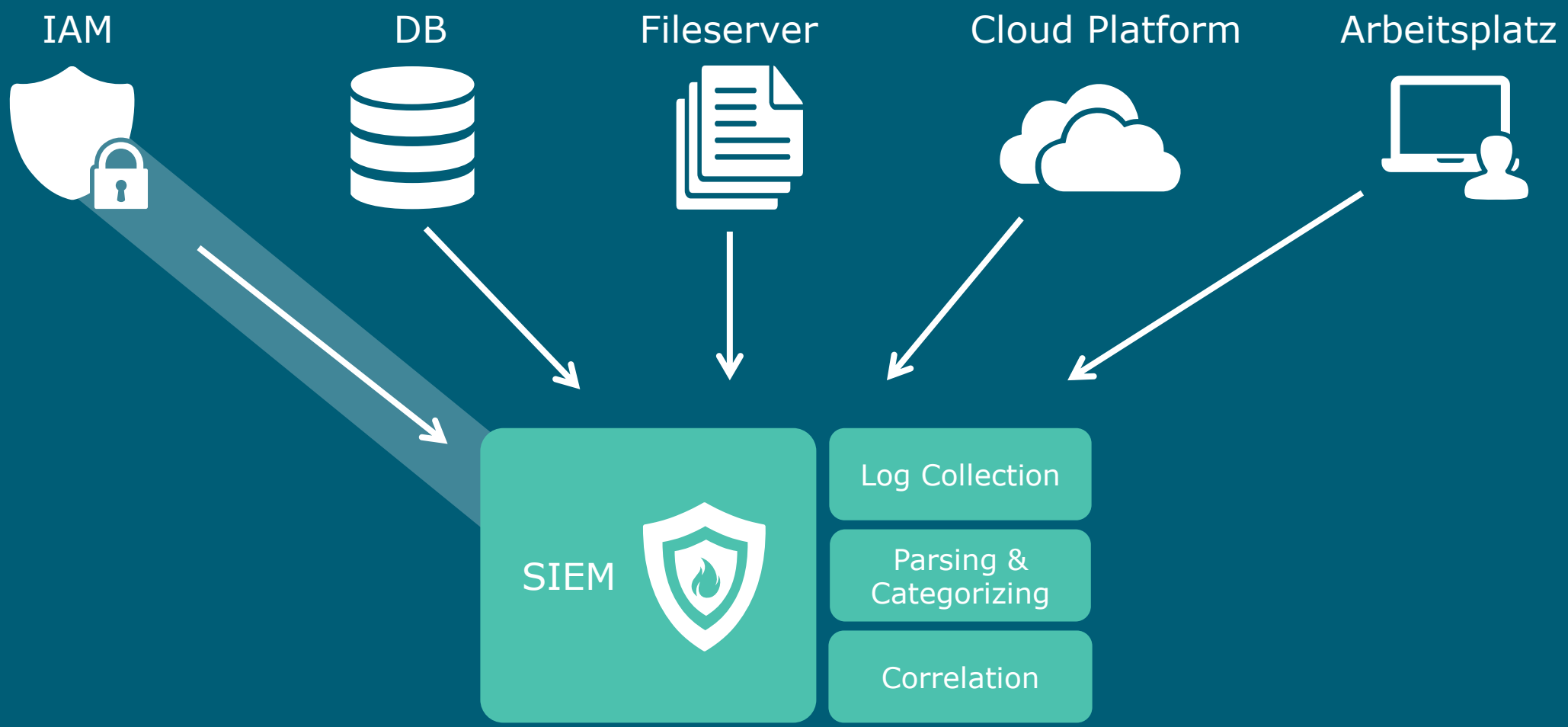
# Robuste Sicherheitsarchitektur dank dem Zusammenspiel von SIEM und IAM

## Agenda

- Integration SIEM - IAM
- Das IDR Triangle
- Anwendungsfälle
- Herausforderungen
- Zusammenfassung
- Live Demo

# Einordnung Integration SIEM – IAM

## Was ist der Kontext von heute?



# Integration SIEM – IAM

## Was sind die Grenzen in einen herkömmlichen IAM?

| | |
|---|---|
| **Kein aktives Monitoring** | sieht Berechtigungen, nicht deren Nutzung |
| **Keine Anomalieerkennung** | erkennt keinen Missbrauch korrekter Rechte |
| **Kein übergreifender Sicherheitskontext** | Kennt Identitäten, keine Events aus anderen Systemen oder Netzwerk |
| **Keine Echtzeit-Alarmierung** | reagiert nicht auf Bedrohungen |

# Integration SIEM – IAM

## Was sind die Vorteile?

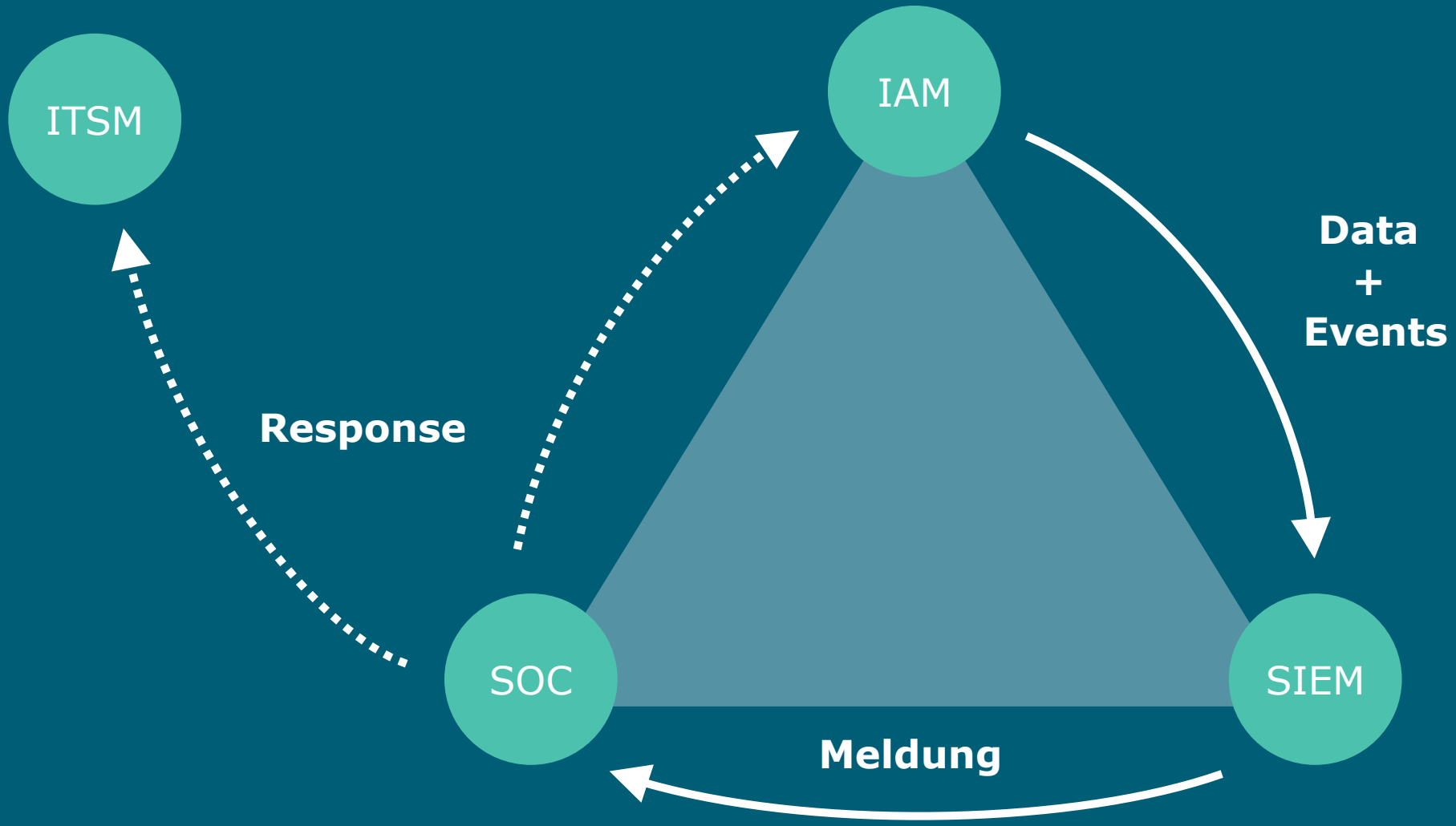
- **Bessere Bedrohungserkennung**
  Durch die Korrelation von Identitäts- und Berechtigungsdaten aus dem IAM mit Daten aus anderen Systemen
  -> **Reduzierung von Risiken bezüglich Zugriffskontrolle**

- **Höhere Visibilität und Nachvollziehbarkeit**
  Zugriffe und weitere sicherheitsrelevante Aktionen können in einem zentralen System (dem SIEM) nachvollzogen werden

- **Schnellere Incident-Response**
  Automatisierte Reaktionen oder durch Analysten, welche das SIEM als Hilfsmittel verwenden
  "Mean Time to Detect" (MTTD) und "Mean Time to Respond" (MTTR)

- **Effizientere Audits- und Compliance-Nachweise**
  Die kombinierte Datenbasis erleichtert den Nachweis von Regelkonformität

# Identity-Detection-Response Triangle



# Vorgehen um Anwendungsfälle zu definieren

1. Workshop mit Personen aus dem IAM- und SOC-Team organisieren.
2. Was sind die Angriffsszenarien, welche wir erkennen möchten?
3. Stehen Daten aus dem IAM zur Verfügung, in welchen man diese Angriffszenarien erkennen könnte?
4. Stehen für definierte Angriffsszenarien Standard-Rules im SIEM zur Verfügung? Oder braucht es Custom-Rules?
5. Umsetzung der Detektion der Angriffsszenarien priorisieren.

# IAM – SIEM Anwendungsfälle

Ein Service User holt sich mehr Tokens als üblich

Ein Service User greift von einer ungewohnten IP zu

Failed Logins eines Service Users

Failed Logins von User:
Password spraying, Credential suffing, Brute Force

Loginverhalten
Event kommt aus IAM

# IAM – SIEM Anwendungsfälle

Hochpriviligierte Berechtigung wird vergeben

Erstellung von sehr kurzlebenden Benutzern

Massenhafte Löschung von Benutzern

Adminverhalten
Event kommt aus IAM

# IAM – SIEM Anwendungsfälle

Security Monitoring suspendiert Benutzer oder erzwingt Passwortänderung

Benutzer meldet Phishing-Vorfall.
SOC-Team lost Action auf IAM aus.

SIEM lost Alarm zu einer Identität aus.
SOC verwendet IAM für Data Enrichment (bsp. Tel. Vorgesetzter).

Response auf IAM Event kommt nicht aus IAM

Data Enrichment mit IAM Event kommt evtl. aus IAM

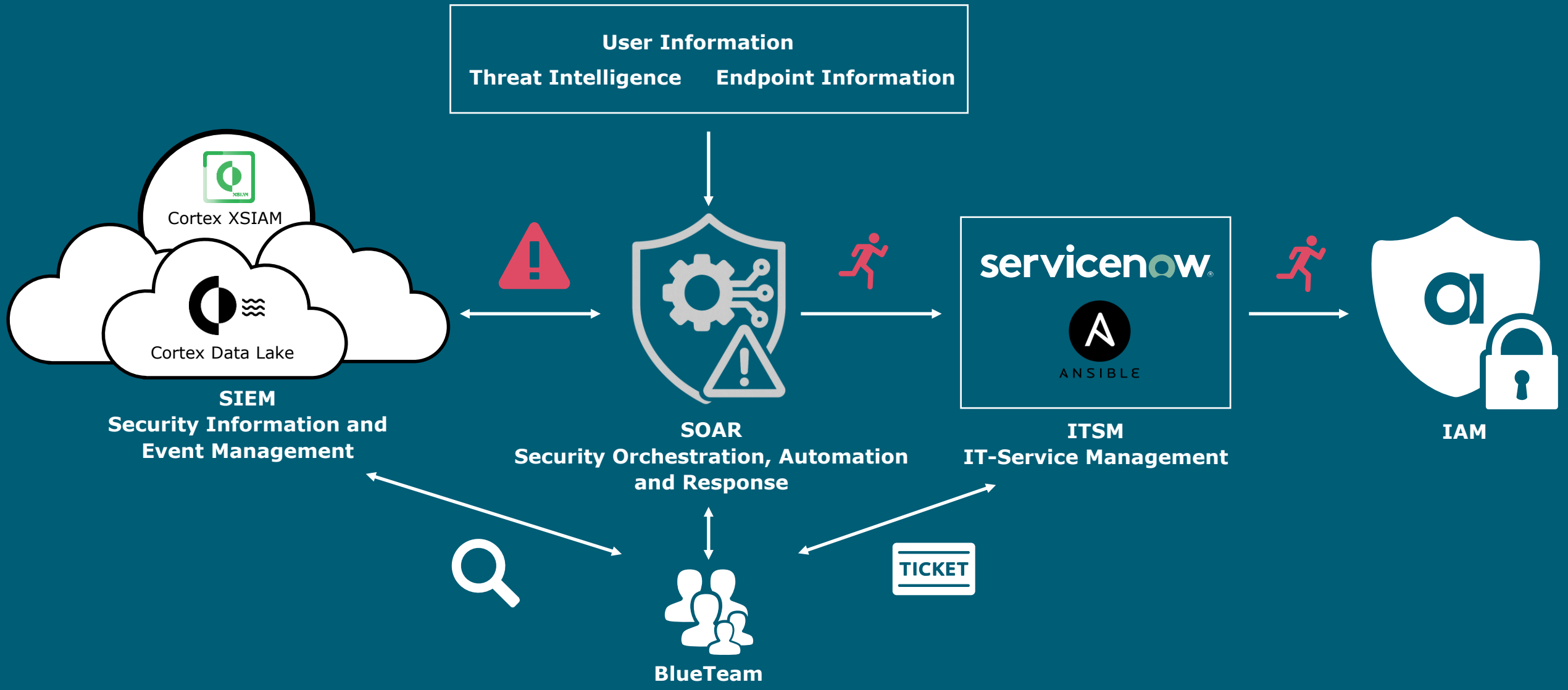
# Herausforderungen und Erkenntnisse


- Wie hoch sollen die Schwellwerte sein?
- Eventdaten für einen Anwendungsfall stehen nicht wie gewünscht zur Verfügung.
- Eventdaten eines Systems zeigen anderes Verhalten als erwartet.
- Teilweise braucht man recht viele Erfahrungswerte respektive Eventdaten, um sinnvolle Regeln definieren zu können

# Zusammenfassung IAM und SIEM

| | SIEM | IAM |
|---|---|---|
| **Frage** | Was passiert aktuell im System? | Wer darf was? |
| **Daten** | Events, Logs, Muster, Regeln | Identitäten, Rollen, Rechte |
| **Nutzen** | Angriffe erkennen | Zugriffskontrolle, Zugriff steuern |
| **Risiko ohne Integration** | Binde Flecken, viele False Positives | Fehlende Angriffserkennung |

# Cortex XSIAM – Response



# Demo

# Workshop Teil 2

- **Diskutiert und ergänzt** bitte die Punkte aus dem ersten Workshop.
- Sind Euch wichtige **neue Anwendungsfälle** eingefallen, die Ihr beim ersten Workshop noch nicht berücksichtigt habt?
  (Angriff – Rule – Response)


- Wo seht Ihr den **grössten Vorteil** eines gelungen Zusammenspiels von IAM und SIEM.

# Nächste Session IAM-Circle

**Die Rolle des IAM im modernen IT-Management und der digitalen Transformation**

📅 Donnerstag, 18. September 2025
🕐 14:30 bis 17:30 Uhr

📍 **MEMOX im The Circle Zürich**


ITSENSE

# Deine #Meinung ist wichtig – du machst den Unterschied!

Die Umfrage ist anonym. Keine deiner Antworten kann dir zugeordnet werden. Sie umfasst 10 Fragen und dauert gerade einmal 3 Minuten.

👇 **Jetzt scannen und Umfrage ausfüllen.** 👇

ITSENSE

ITSENSE

# Stay tuned, stay secure!

SWISS MADE IAM

abraxas

ti&m

COPEBIT

white rabbit Communications

netzmedien

#10