IT/OT SOC für Spitäler – ein ganzheitlicher Ansatz

Mathias Bücherl, Axians Cyber Security & BI AG

Mathias Bücherl (M. Sc.)
Chief Technology Officer
Axians Cyber Security & BI AG

+41 79 746 10 98
mathias.buecherl@axians.com

Professional

- **Axians Cyber Security & BI AG** (Zurich)
  - since 04/2021 — Chief Technology Officer
  - 11/2020 – 03/2021 — Head of Consulting & PreSales
- **Hochschule Luzern**
  - since 04/2021 — (Guest) Lecturer SOC & OT Security
- **Cooperative State University Stuttgart**
  - since 09/2019 — Lecturer Cyber Security
- **T-Systems International GmbH** (Munich, Singapore, Mexico-City)
  - 09/2019 – 10/2020 — Senior Security Bid Manager International
  - 01/2019 – 08/2019 — Senior Security Solution Designer International
  - 10/2013 – 12/2018 — Security Architect Managed Cyber Defense

Education

- **Master of Science in IT-Management**
  Hochschule für Ökonomie & Management Nuremberg
- **Bachlor of Science in Business Computer Science**
  Cooperative State University Stuttgart
- **IT specialist in System Integration**
  IHK Regensburg

Axians Cyber Security

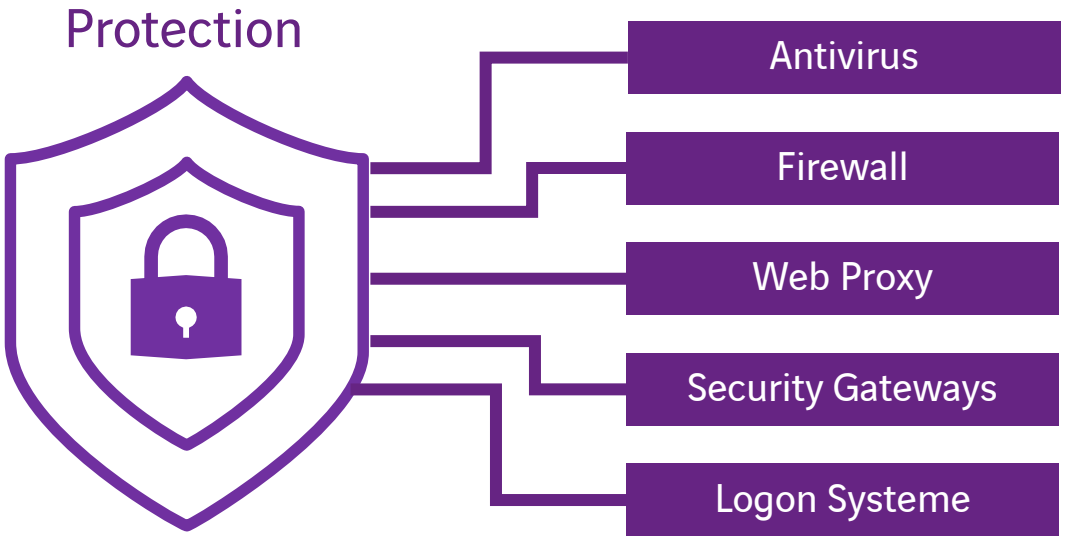
- End-to-end Managed Security Service Provider (MSSP)
- Mehr als 300 Cyber Security Experten in Europa
- Unsere fünf Kernwerte:
  - Vertrauensvoll
  - Unabhängig
  - Verantwortungsbewusst
  - Unternehmerisch
  - Solidarisch

"Axians Cyber Security ist der Cyber Security Dienstleiter, der die individuellen Bedürfnisse seiner Kunden versteht."


Dem BSI zufolge bleiben Hacker durchschnittlich
243 Tage
in einem Unternehmen unentdeckt.

Ist unser bestehende Schutz nicht ausreichend?

«Wir setzen bereits unterschiedliche Technologien ein, um Cyber Angriffe abzuwehren. Wir sind genügend ausgerüstet!»

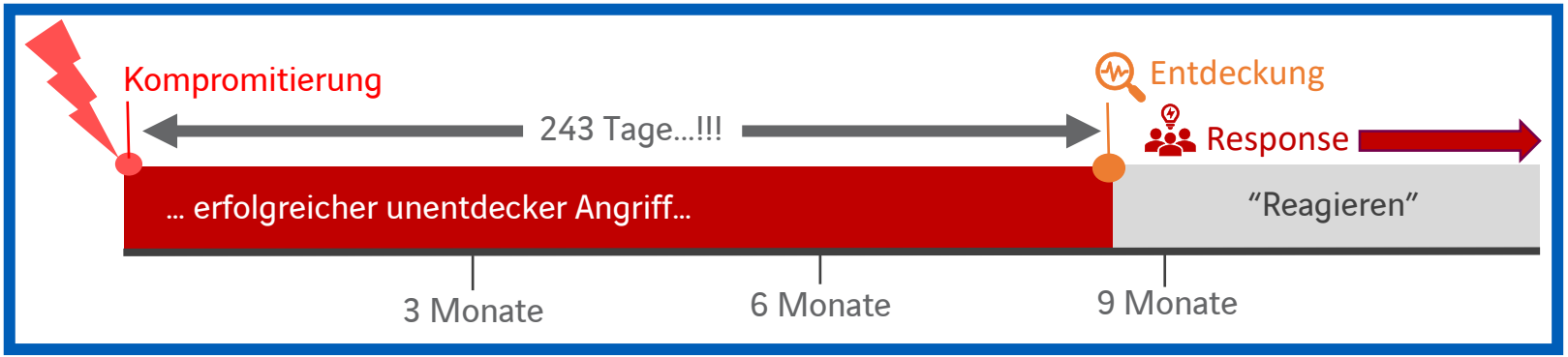


Der Realitäts-Check für Spitäler

Viele Spitäler erfahren von dritter Stelle über erfolgreiche Angriffe auf die eigene Einrichtung

Die meisten Opfer hatten aktuelle (up-to-date) Präventivmassnahmen bzw. Schutzvorrichtungen

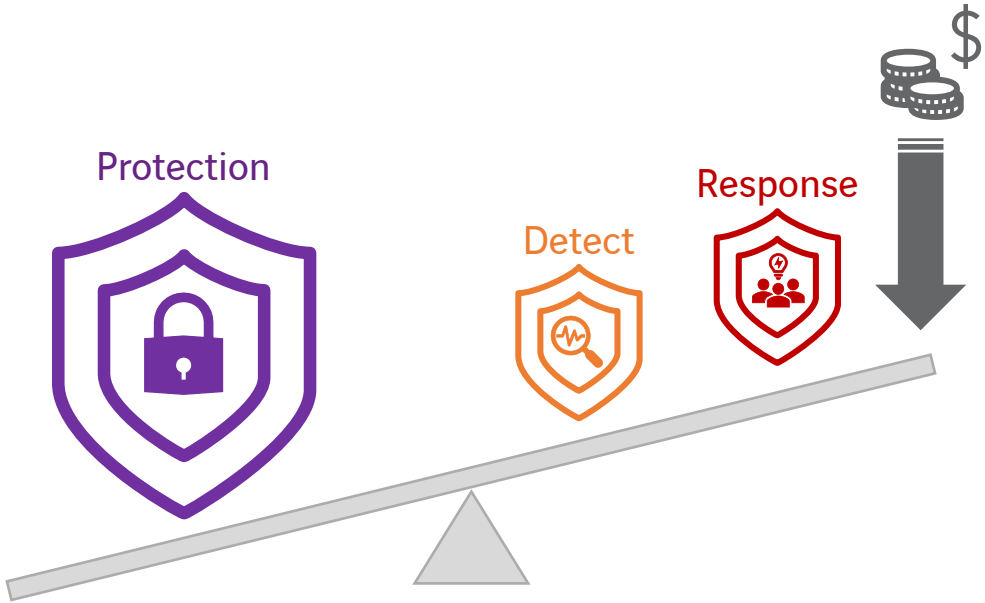
Es gibt keinen 100% Schutz. Die Frage ist nicht ob, sondern wann ein Angriff erfolgreich sein wird.



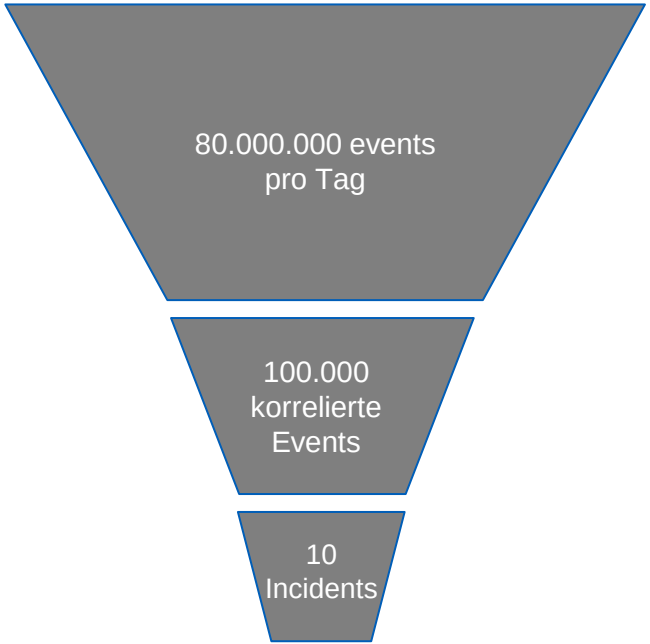
Protection alleine ist nicht ausreichend!

- Präventivmassnahmen alleine, durch Ausbau von weiteren Elementen im Bereich **Protection genügen nicht**, um die Einrichtung langfristig vor Schaden durch Cyber Angriffe zu bewahren.

- Spitäler müssen Ihre Cyber Security Investitionen in den Bereichen **Detect** und **Response** erhöhen um Angriffe schneller **entdecken** und darauf **zeitgerecht reagieren** zu können.



Big Security Data – eine Herausforderung



- Hohe Anzahl an Events
- Fachkräftemangel im Bereich Cyber Security
- Steigende regulatorische Anforderungen
- Viele wiederkehrende Tätigkeiten
- Export von Logs aus OT-Geräten nicht “out-of-the box”

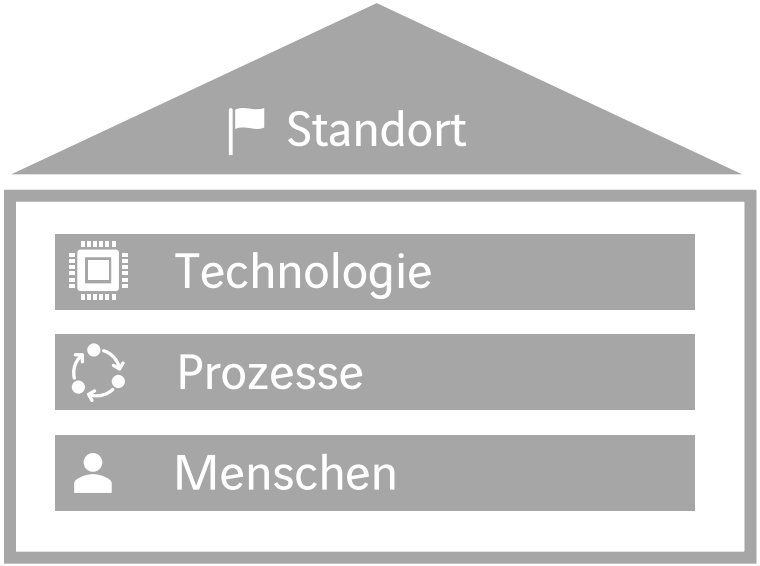
SOC vs. SIEM

Besuche ein Restaurant und geniesse die Speisen die serviert werden.

Hier ist die Pfanne, viel Spass beim Kochen bei Dir zu Hause!

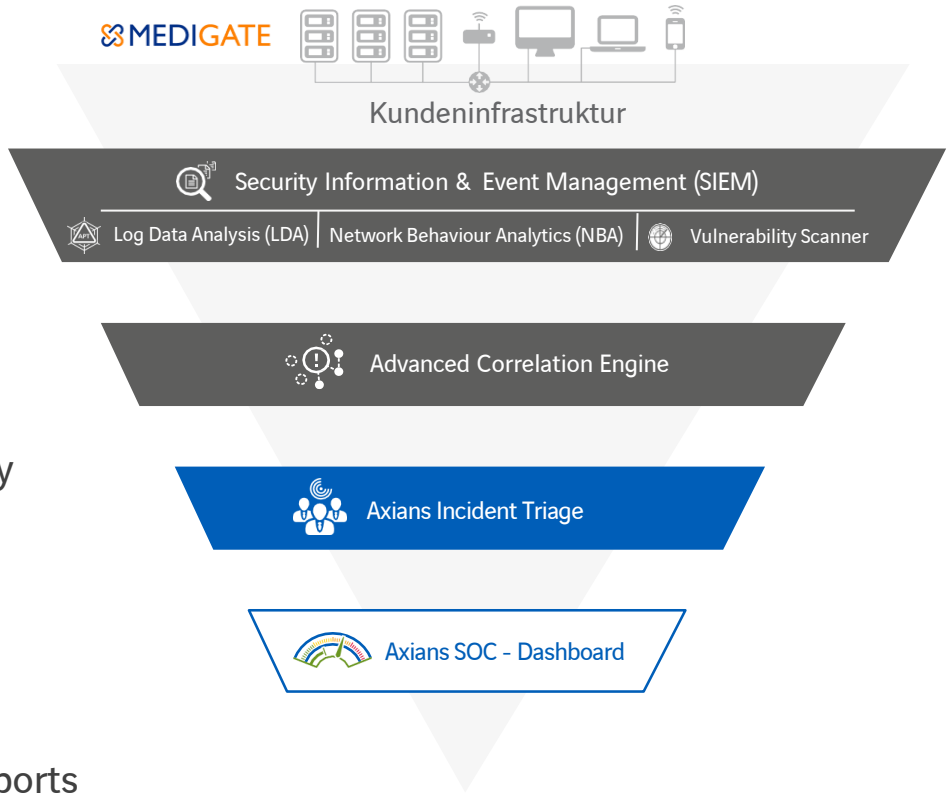
Was ist ein Security Operation Center?

- Eine Kombination aus **Experten, Werkzeugen** und **Prozessen** mit dem Ziel **Cyber Security Risiken** zu **entdecken**, zu **verhindern**, zu **analysieren** und zu **bewerten.**
- **Unterstützung** bei der Umsetzung von **Massnahmen zur Behebung** von Cyber Security Risiken
- Es liefert **forensische Daten** zur **Beweissicherung** und **Dokumentation** bei IT-Security Vorfällen



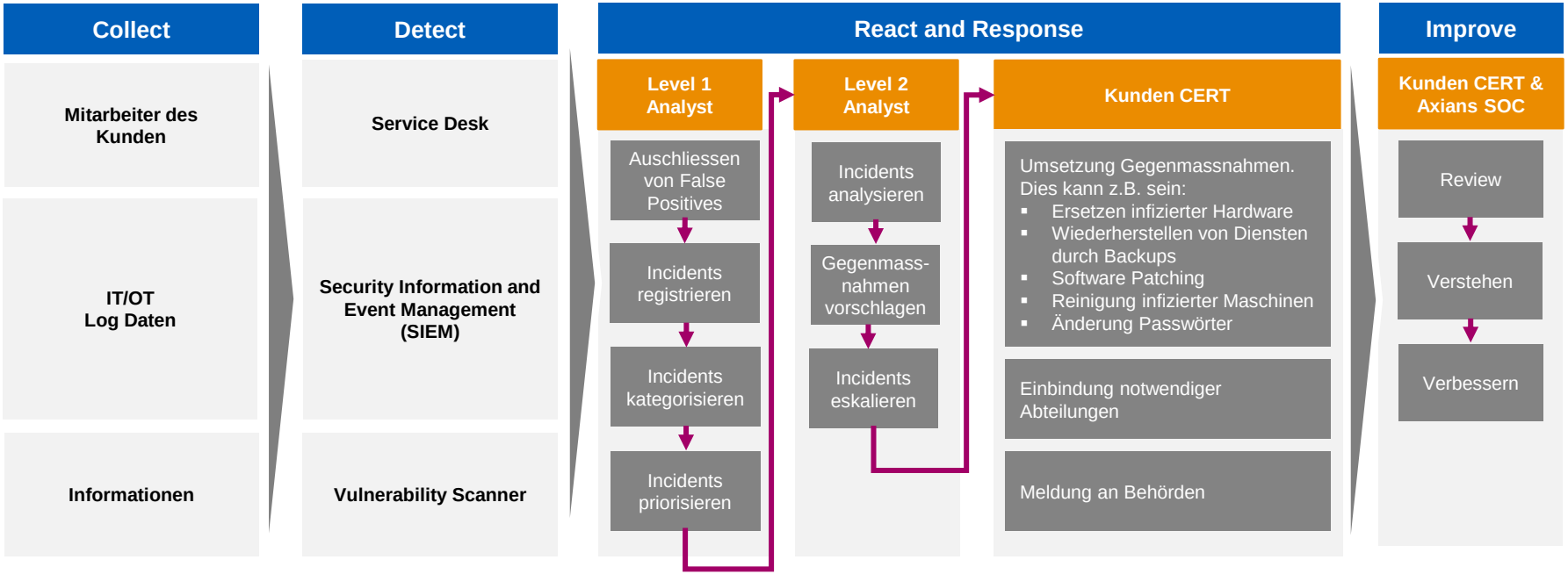
Technologie – Axians IT/OT SOC

- Komplette SOC Plattform → nicht nur SIEM
  - SIEM
  - Vulnerability Scanner
  - Log Data Analytics
  - Network Bevhaviour Analytics
  - Ticketsystem
  - Dashboard & Reporting
- Vereinheitlichtes und zentralisiertes Security Event Management
- Schnelle und präzise Erkennung von echten Bedrohungen
- Hochentwickelte Korrelationsfähigkeit
- Individuelle Use-Cases, Dashboards und Reports



Security Incident Management bei Axians

Die Reaktion auf Sicherheitsvorfälle wird durch zwei Faktoren erschwert. Erstens sind keine zwei Vorfälle gleich. Zweitens erfordert jede Reaktion auf einen Sicherheitsvorfall das enge Zusammenspiel von Personen, Technologien und Prozessen. Daher ist es wichtig die Reaktion auf Security Incidents im Voraus planen. Der Security Incident Management Prozess unseres Security Operation Centers orientiert sich an ITIL v4.



Wie bietet die Axians einen ganzheitlichen Ansatz für Spitäler?

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?

Axians Cyber Security & BI AG
Riedstrasse 1
CH-6343 Rotkreuz
info-ch.security@axians.com