UNIVERSITÄTS-
KINDERSPITAL
ZÜRICH

Information Security in Healthcare vom 31.05.2022

Cédric Sieber, CISO im Universitäts-Kinderspital Zürich, berichtet wieso Cyber-Bedrohungen nicht zwingend zum Problem werden müssen

Universitäts-Kinderspital Zürich

UNIVERSITÄTS-
KINDERSPITAL
ZÜRICH

Über 100'000 Patienten pro Jahr

Rund 2'500 Mitarbeitende

220 Betten in 30 Abteilungen (ohne Reha)

Notfall: Bis zu 200 Patienten pro Tag

Über 6'000 Operationen pro Jahr

300 Forschende

80 klinische Studien

Verweildauer Akutspital ca. 6 Tage

Umsatz 2019: 336Mio CHF

Das Spital der Eleonorenstiftung

Informatik des Universitäts-Kinderspital Zürich

UNIVERSITÄTS-
KINDERSPITAL
ZÜRICH

Informatik

2810 Benutzer

37 Mitarbeiter

51 Tickets/Tag
Total: 18'615

7.0 Mio. CHF/Jahr

Infrastruktur

2200 Clients

750 Laptops

30 iPads

120 AP Drucker

680 Etagen & Netz-Drucker

4 Mio. Seiten

451 Server

2.53PB Storage & Archiv

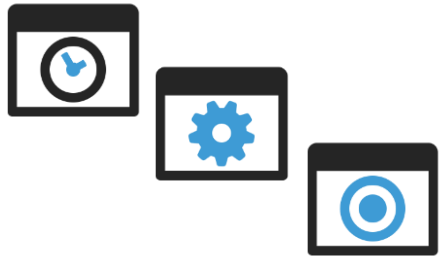
1'100 Telefone

8 WAN/ISP-Zugänge

6260 LAN-Ports

250 WLAN Hot-Spots

Applikationen



300 Haupt-Applikationen

Mit zu betrachten

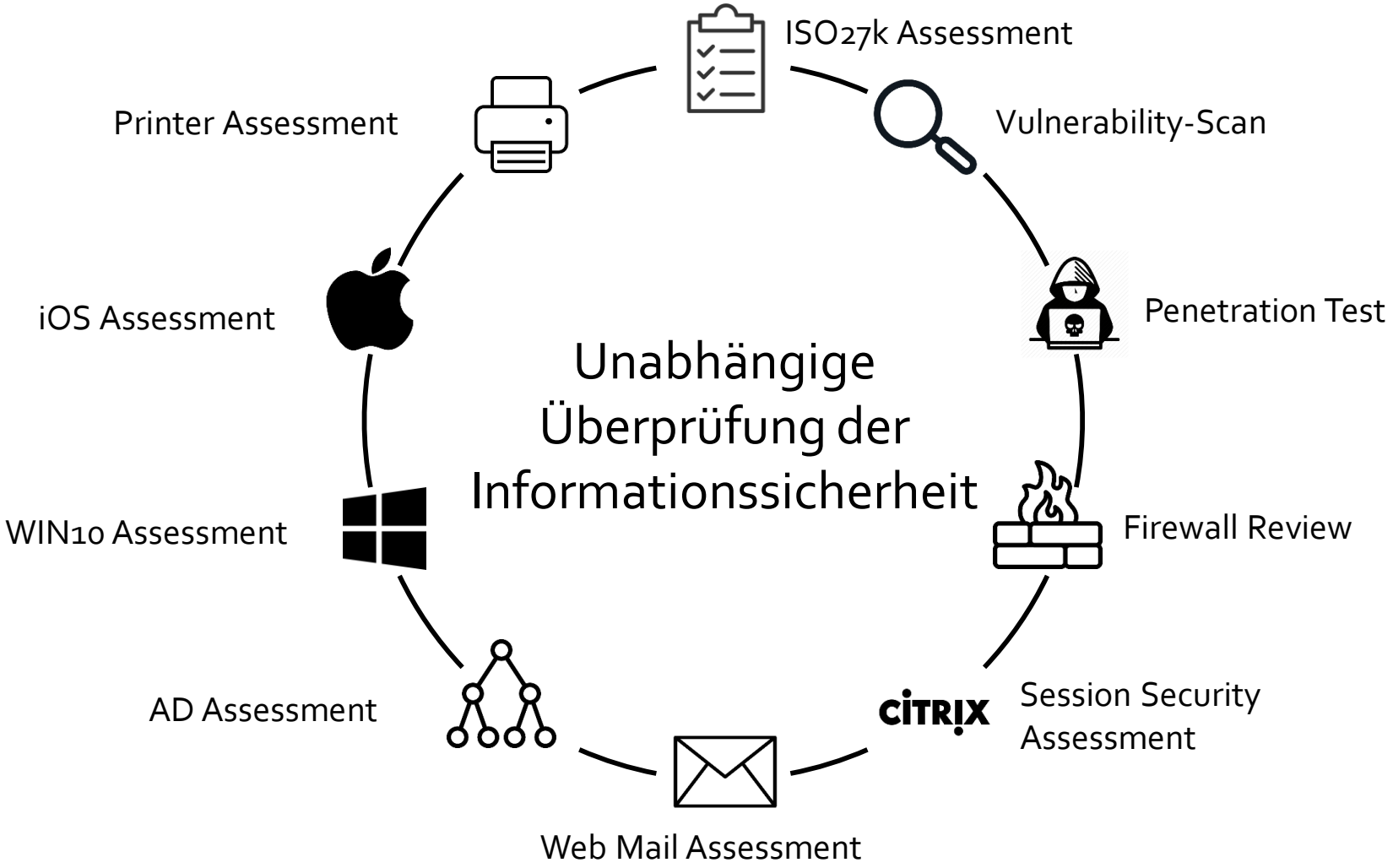
BYOD Geräte ca. 1500

Medizinische Geräte

Technischer Dienst
(Telefonie, Alarmierung, Patientenruf, Gebäudeverkabelung)

Stärkung des Informationssicherheits-Dispositivs

UNIVERSITÄTS-
KINDERSPITAL
ZÜRICH



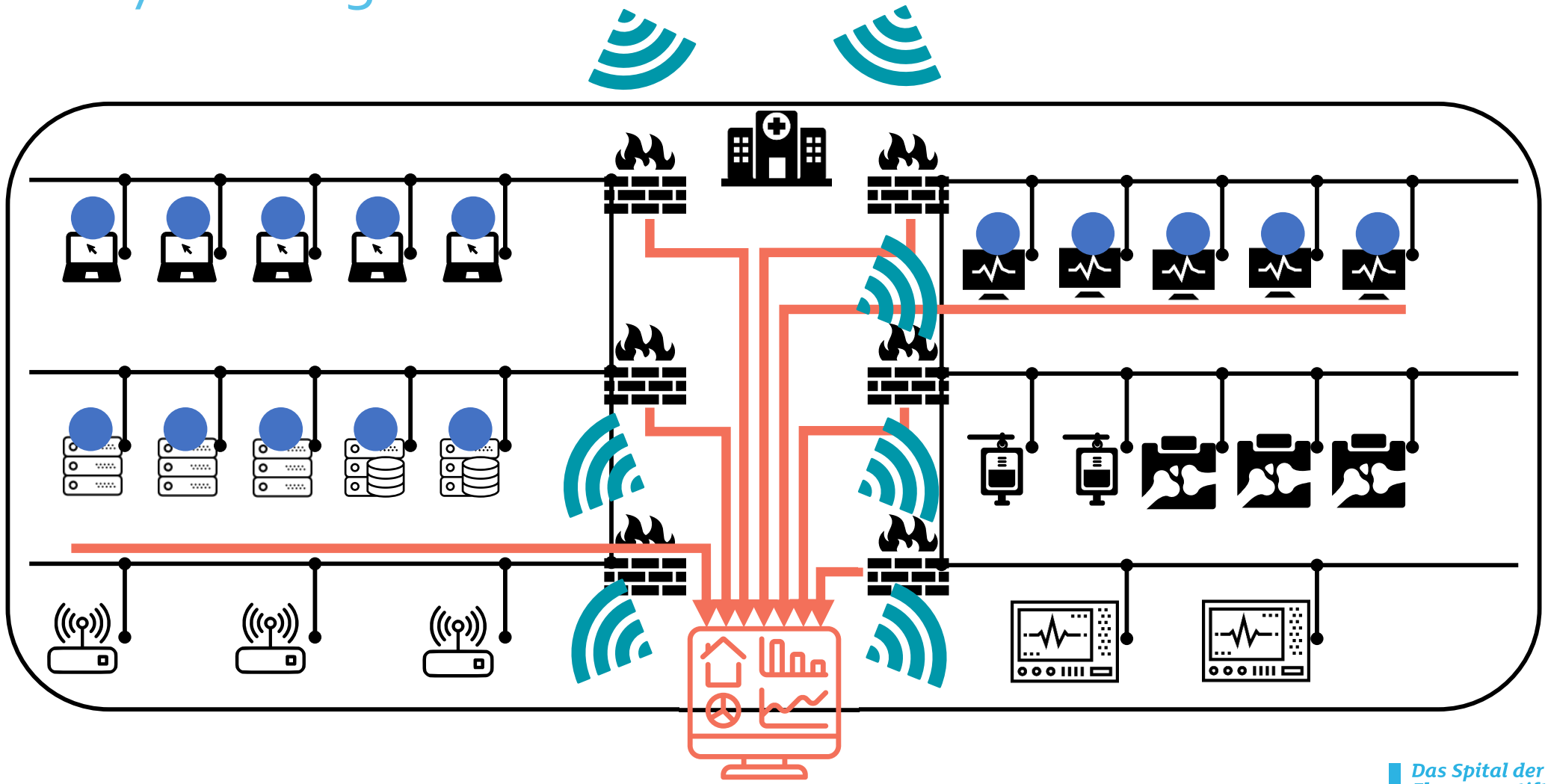
Identifikation von Risiken durch ein externes Assessment

Definition von Massnahmen und Erstellung eines Roadmaps basierend auf den identifizierten Risiken

Budgetierung basierend des erstellten Roadmaps

Management Attention & Commitment

Erhöhung Visibilität und Handlungsfähigkeit auf Cyber-Angriffe

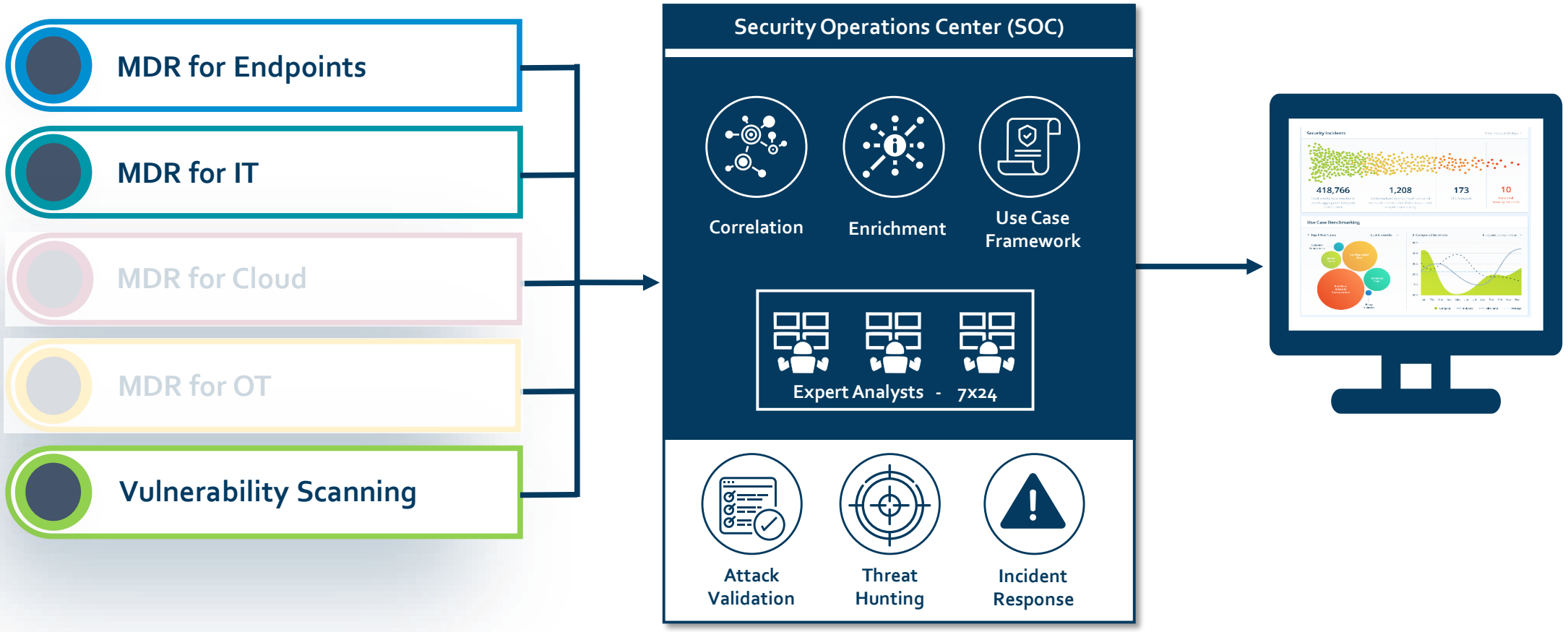


UNIVERSITÄTS-
KINDERSPITAL
ZÜRICH

Das Spital der
Eleonorenstiftung

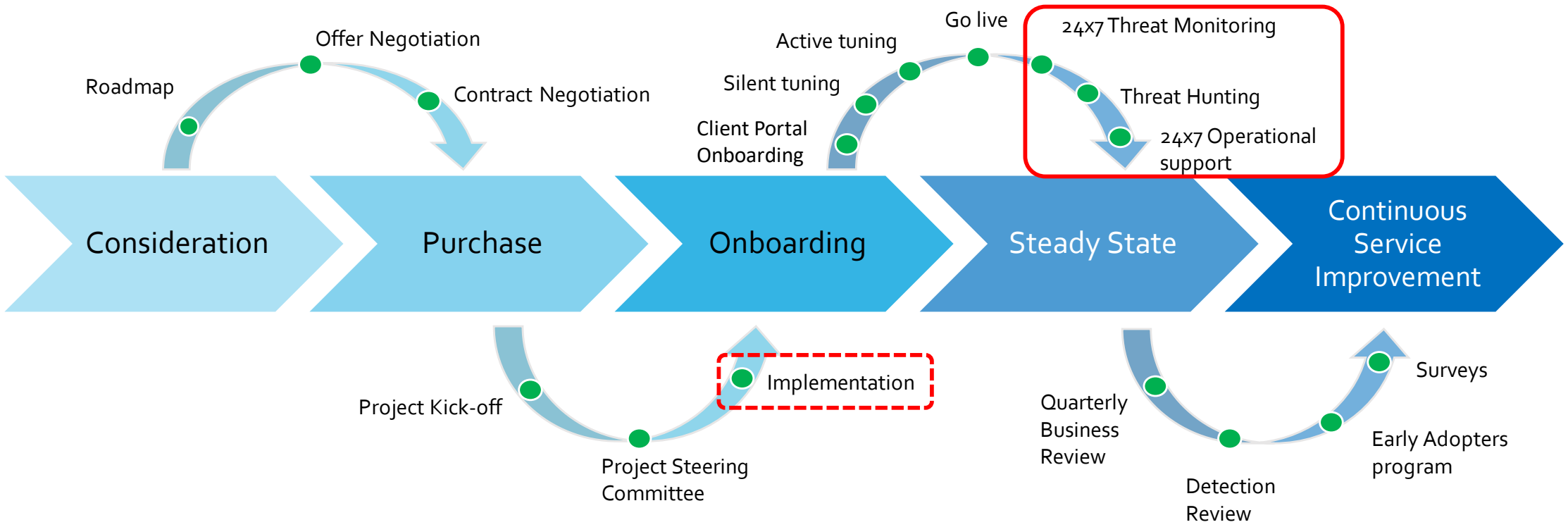
Security Operations Center (SOC)

UNIVERSITÄTS-
KINDERSPITAL
ZÜRICH



Das Spital der Eleonorenstiftung

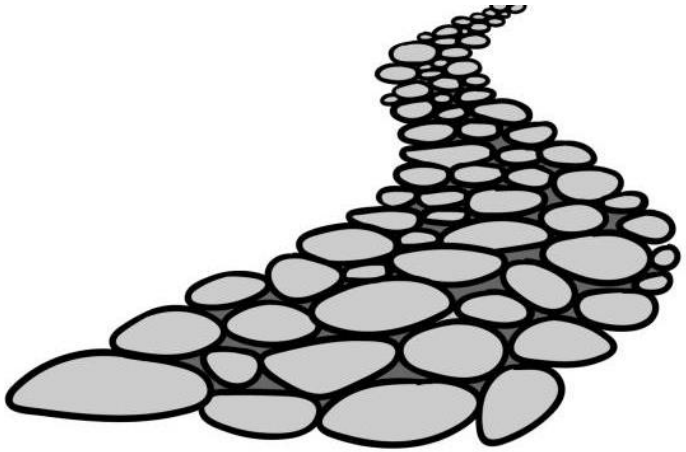
Aktueller Stand des SOC-Projektes



Erfahrungen und Herausforderungen

Positive Erfahrungen

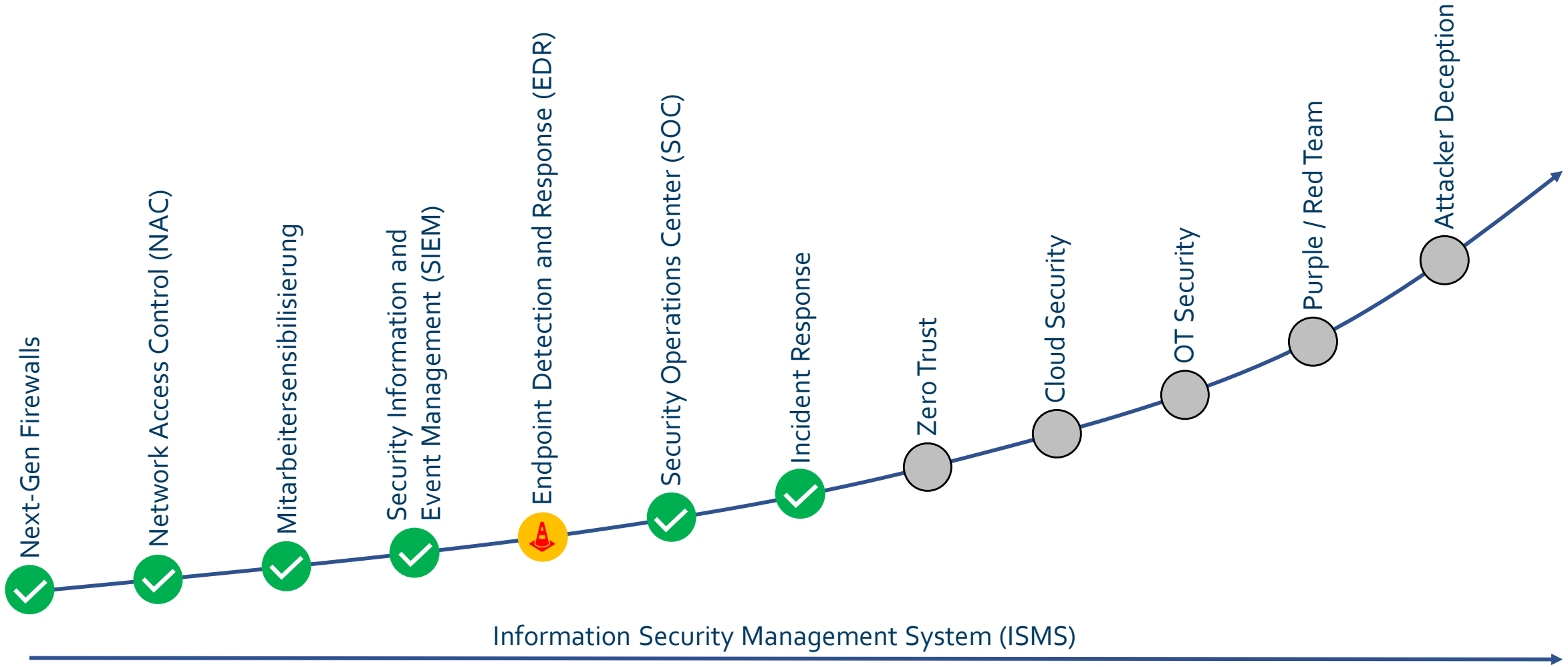
- Einfache Einführung vom Vulnerability Management
- Effizienter Aufbau des SIEM
- Gute Unterstützung durch strategische Partner



Herausforderungen

- Mangelhafte Grundlage für die Cloud-Integration
- Definition der Rollen und Verantwortlichkeiten
- Anpassung der Prozesse für die Behebung der Findings
- Minimale Integration ins Ticketing System
- Unzureichende Ressourcen für die Behebung von Findings

Nächste Schritte



UNIVERSITÄTS-
KINDERSPITAL
ZÜRICH

Vielen Dank für Ihre Aufmerksamkeit

Haben Sie noch Fragen?

Cédric Sieber (CISO)

cedric.sieber@kispi.uzh.ch