Risiken durch Cyberangriffe

Herausforderungen bei der Umsetzung von Informationssicherheit in deutschen Krankenhäusern

xevIT
part of conscia

Aktuelle Gefährdungslage

Stuttgarter Zeitung

Hacker-Attacke am Bodensee: Cyberangriff auf Kliniken – was ...

Friedrichshafen - Nach dem Hackerangriff auf den Klinikverbund „Medizin ... hat rund 640 Betten - davon 370 im Krankenhaus Friedrichshafen.

14 Jan 2022

NDR

Wolfenbüttel: Vielversprechende Spuren nach Hackerangriff

Polizeibeamte hatten in der vergangenen Woche in dem Klinikum Spuren gesichert, wie der NDR in Niedersachsen von der Staatsanwaltschaft erfuhr.

19 Jul 2021

Badische Neueste Nachrichten

SRH-Klinikum Karlsbad kämpft 2021 mit Corona und einem ...

SRH-Klinikum Karlsbad kämpft im Jahr 2021 mit Corona und einem Hackerangriff. Im Januar wütete Corona, im September kam ein Cyberangriff, kurz...

30 Dec 2021

„Erhöhte Bedrohungslage für Deutschland" – Behörden warnen vor russischen Hackern

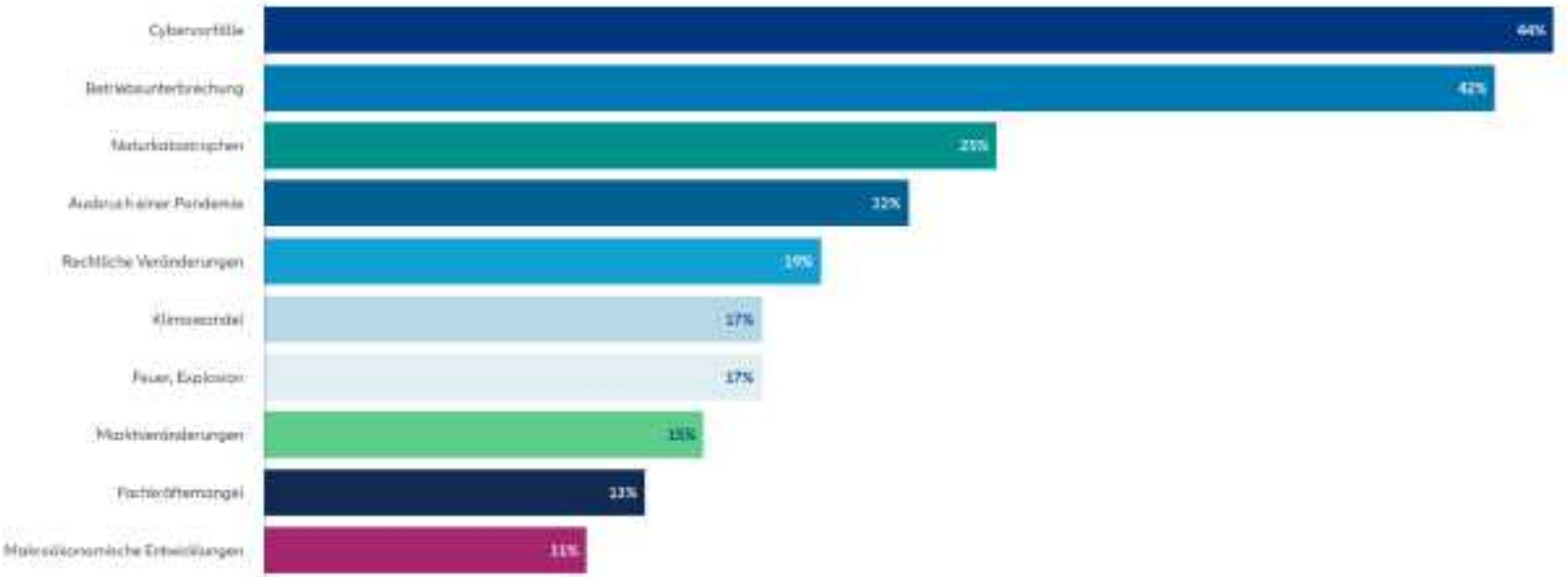
Es herrscht die zweithöchste Gefahrenstufe für deutsche Verwaltung und Unternehmen. Ein Cyber-Team der EU soll unterdessen der Ukraine helfen, kann aber nicht ins Land reisen.

Allianz

Top 10 Geschäftsrisiken weltweit in 2022

Allianz Risk Barometer 2022

Basierend auf den Antworten von 2.650 Risikomanagement-Experten aus 89 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.

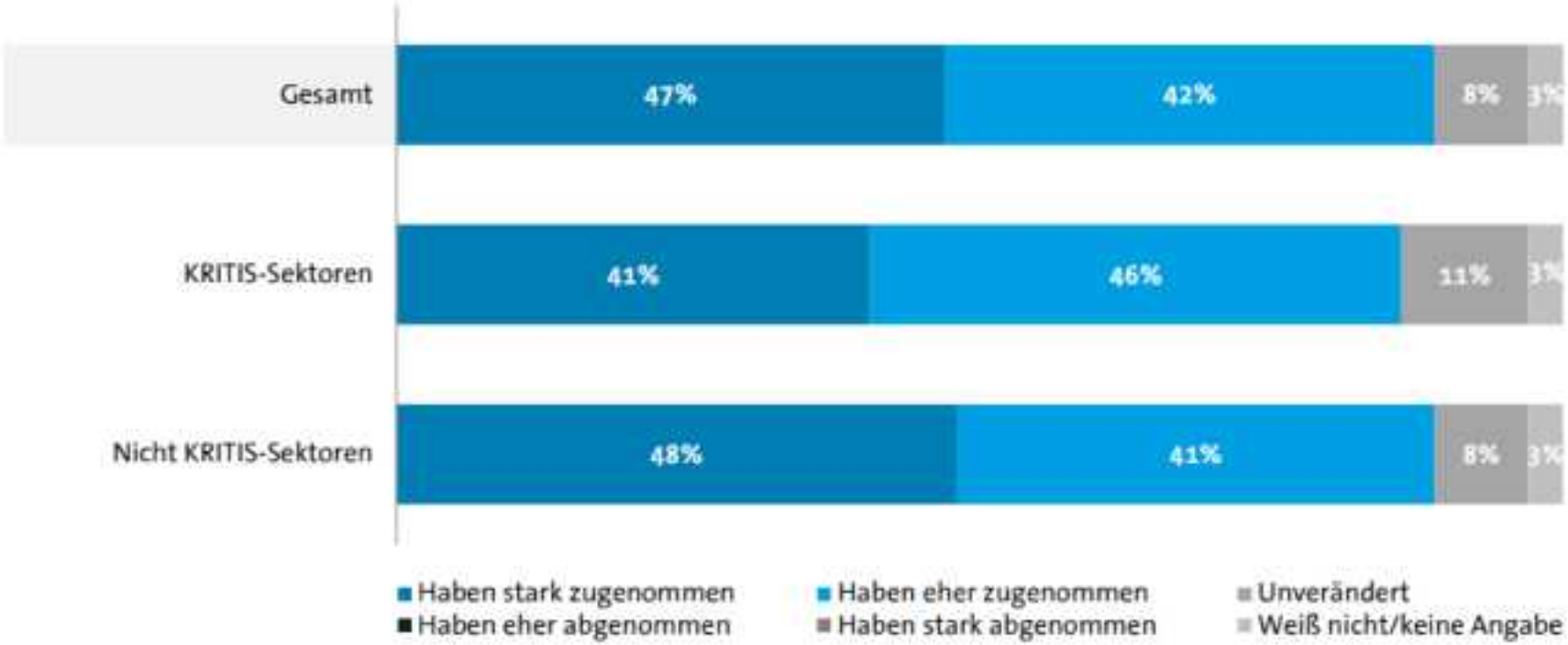


AGCS News & Insights

Source: Allianz Global Corporate & Specialty

Zahl der Cyberattacken nimmt stark zu

Wie hat sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den vergangenen 12 Monaten entwickelt?



5 Basis: Alle befragten Unternehmen (n=1.067); Werte ≤2 zur übersichtlicheren Darstellung ausgeblendet | Quelle: Bitkom Research 2021

bitkom

Cyberangriffe betreffen nahezu 9 von 10 Unternehmen

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?

Cyberangriffe haben bei

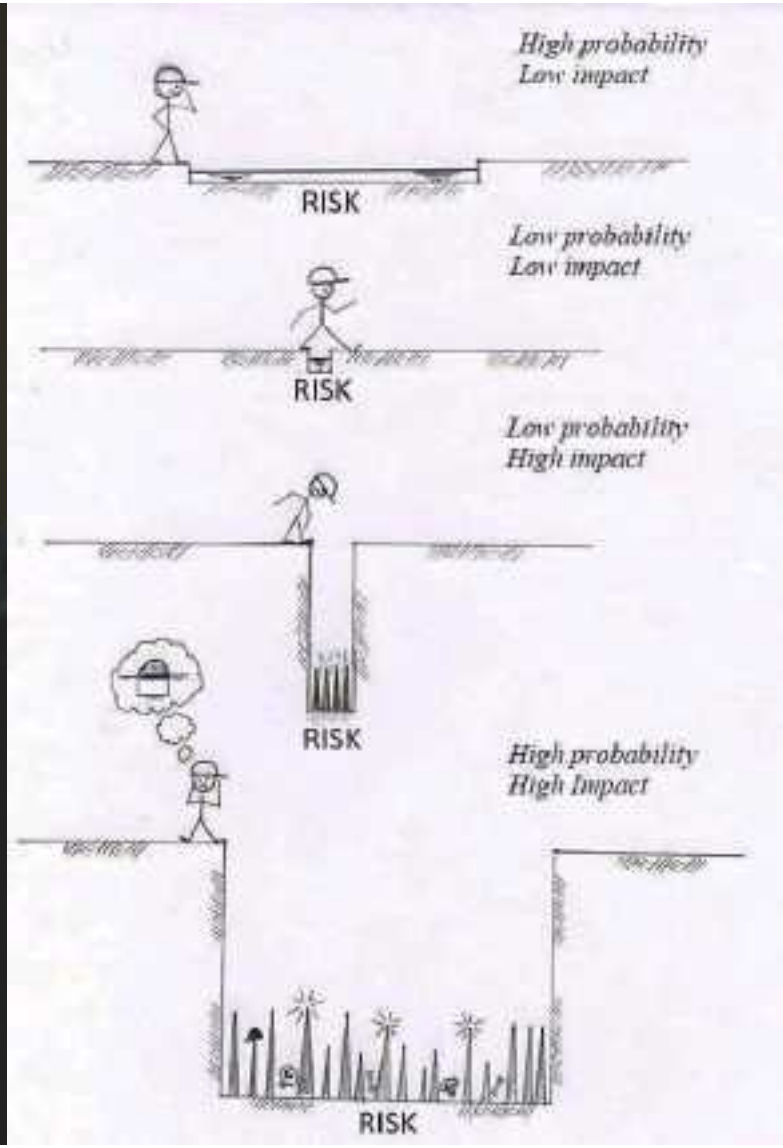
86%

der Unternehmen einen Schaden verursacht – **2019** waren es erst **70%**.

Basis: Alle befragten Unternehmen (2021: n=1.067; 2019: n=1.070); Mehrfachnennungen in Prozent, 2019: innerhalb der letzten zwei Jahre |
Quelle: Bitkom Research 2021

bitkom

Risikobehandlung



Akzeptanz

Transfer

Vermeidung
Reduzierung

Risiken durch
Cyberangriffe

Maßnahmen aus Sicht der Krankenhäuser

Cyberrisiken erkennen und bewerten
- ISMS
- Risikobewertung
- Einbindung GF
- *„Business Case“*

Wiederherstellung Normalbetrieb nach Angriff
- Geschützte Backups
- Notfall Plan
- Disaster Recovery
- Regelmäßige Tests

Erweiterte Schutzmaßnahmen
- Sicherheit vernetzte Medizintechnik
- Netzwerksegmentierung
- Identity & Access Management

Angriffserkennung 24x7
- Endpunkte (Server, PC, Mobile)
- Medizingeräte
- IoT

Reaktion auf Angriffe 24x7
- Reaktionsplanung
- Abwehrmaßnahmen
- Kommunikation & Koordination

Rechtlicher Rahmen

§

Gesetzliche Lage

B3S benennt die Anwendbarkeit der Normen ISO 27001 sowie DIN EN 80001-1

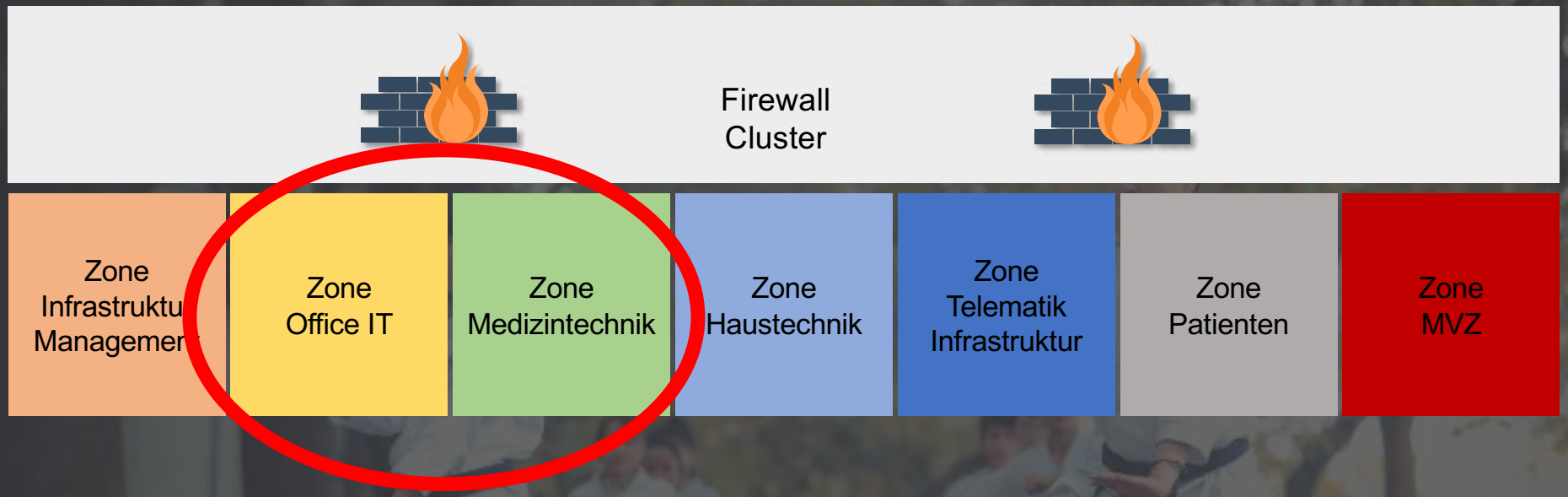
Betrachtung der Risiken aus der Vernetzung

MUSS-Kriterium B3S:
Risikomanagementmethode beim Einsatz von Medizinprodukten in einem IT-Netzwerk gemäß DIN EN 80001-1

Netzwerk Segmentierung

MUSS-Kriterium B3S:
Horizontale Segmentierung nach dem Muster Netzplan, Zonen, Zonenübergänge (Sicherheitszonen) als Mindestmaß

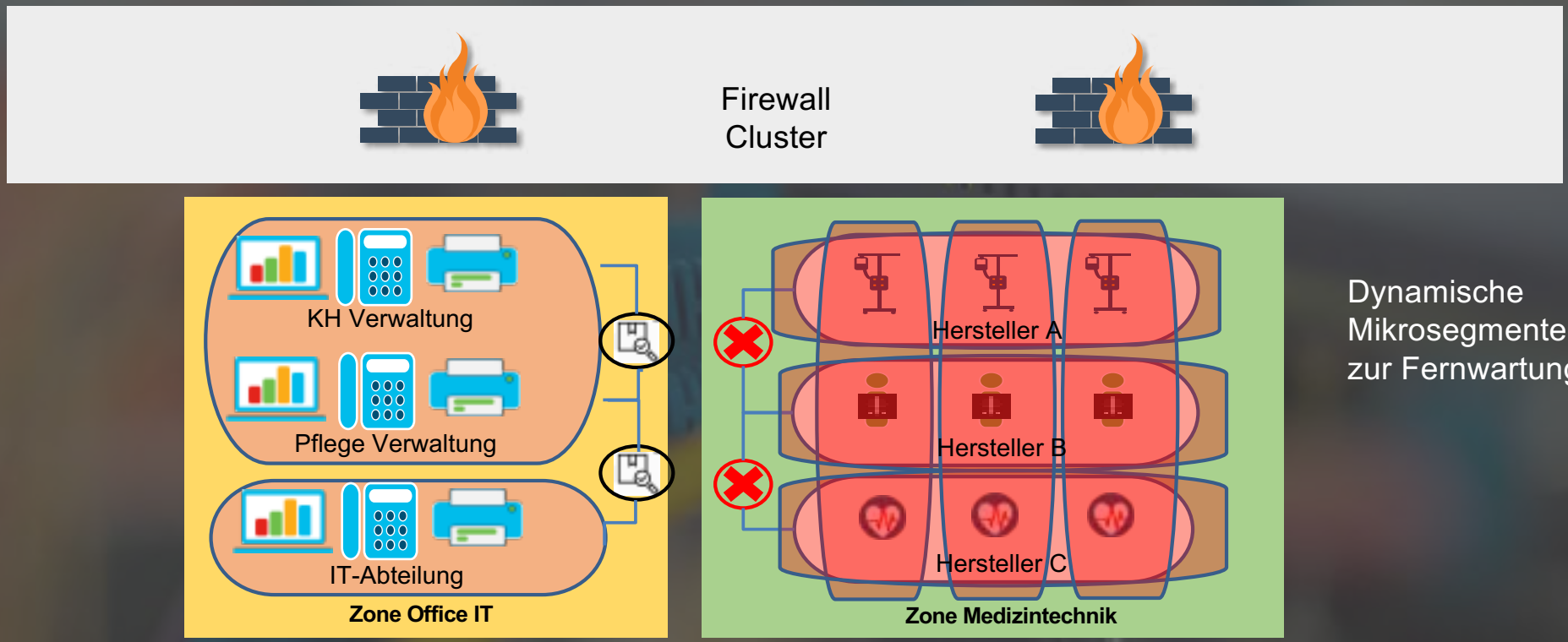
Netzwerksegmentierung – Minimalanforderung B3S



Horizontale Grobsegmentierung – Nutzen:

- Eventuelle laterale Propagierungen von Malware aus anderen Sicherheitszonen werden eingeschränkt
- Auch technisch veraltete oder unfähige Systeme können zumindest vor Außeneinflüssen geschützt werden
- Verwaltungs- und Zuständigkeitsgrenzen werden technisch manifestiert
- Grobfestlegung und eventuell -anpassung der tatsächlich gerechtfertigten Zugriffsnotwendigkeiten kann vorgenommen werden

Mikrosegmentierung – Die nächste Stufe



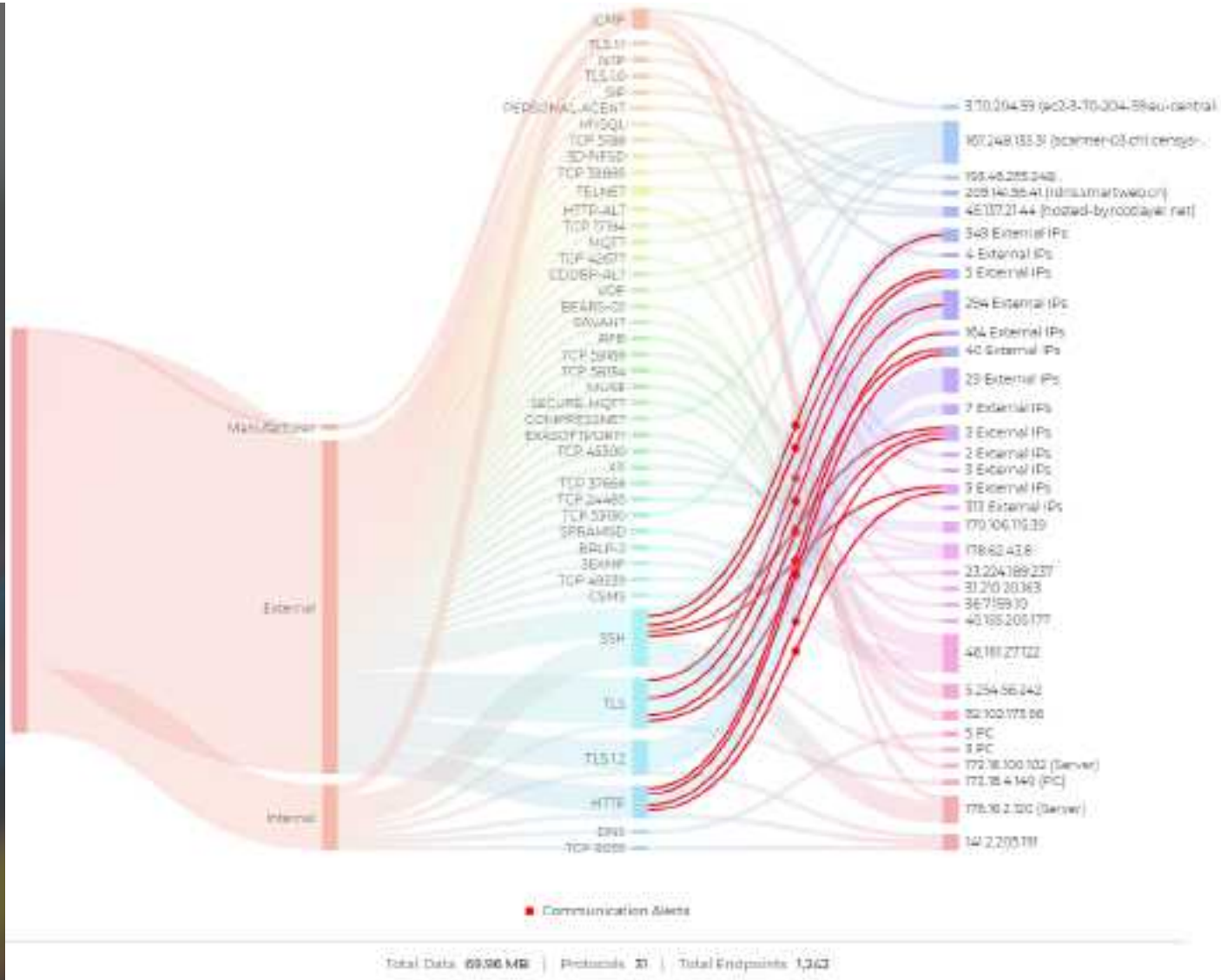
- Überwachung Endpunkte (EDR)
- Kommunikation offen halten
- Zusatznutzen granulare Segmentierung gering

Dynamische Mikrosegmente zur Fernwartung

Dynamische Mikrosegmente:
Funktionale Gruppen zur Sicherstellung Verfügbarkeit

Umsetzung Netzwerksicherheit

Praxisbeispiel – Kommunikation Imaging Server



IT- Sicherheitsgesetz 2.0 – Systeme zu Angriffserkennung

Die KRITIS-Regulierung fordert Maßnahmen nach Stand der Technik, Systeme zur Angriffserkennung und eine unverzügliche Meldung von Störungen, in § 8a (1), (1a) und § 8b (4) BSIG.

Bereich	BSI-ID	Anforderung
Governance	77-79, 81-82	Prozesse und Verantwortlichkeiten für Sicherheitsvorfälle
Systeme und Auswertung	80, 90-94	Systeme und Methoden zur systematischen Auswertung
Tests und Schwachstellen	95-96	Regelmäßige Penetrationstests und Umgang mit Schwachstellen

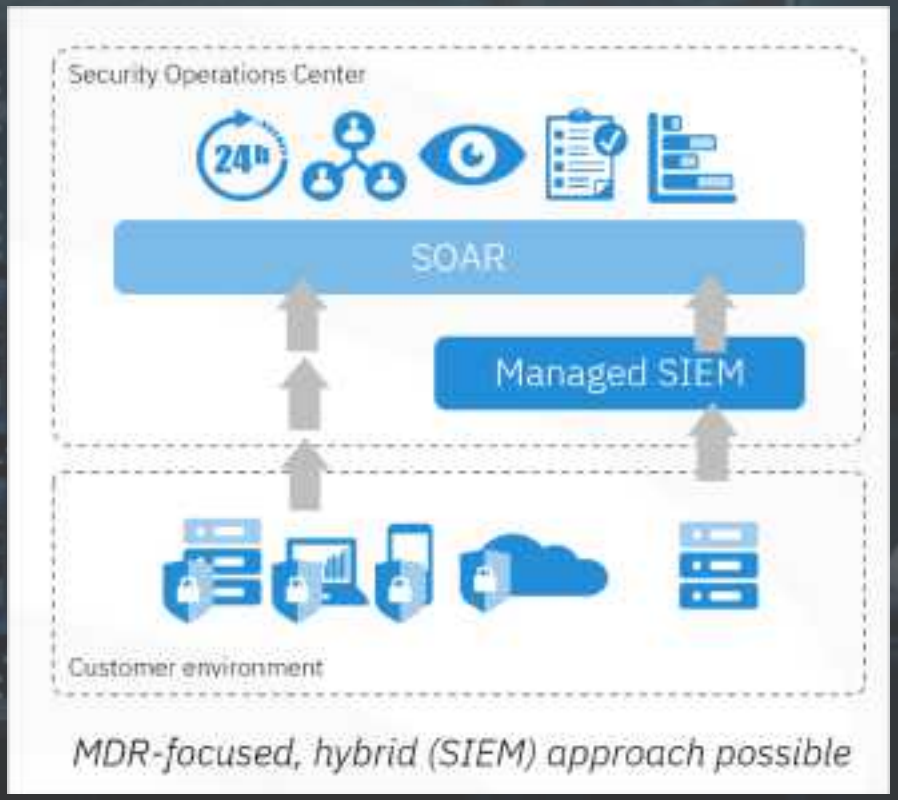
Klassischer SIEM Ansatz

- Sammlung von Unmengen von Rohdaten
- Noise-Anteil sehr hoch
- Suche nach der Nadel im Heuhaufen

- Datenanalyse äußerst komplex
- SIEM Spezialisten sind selten und teuer
- SIEM Infrastruktur in der Regel sehr kostenintensiv

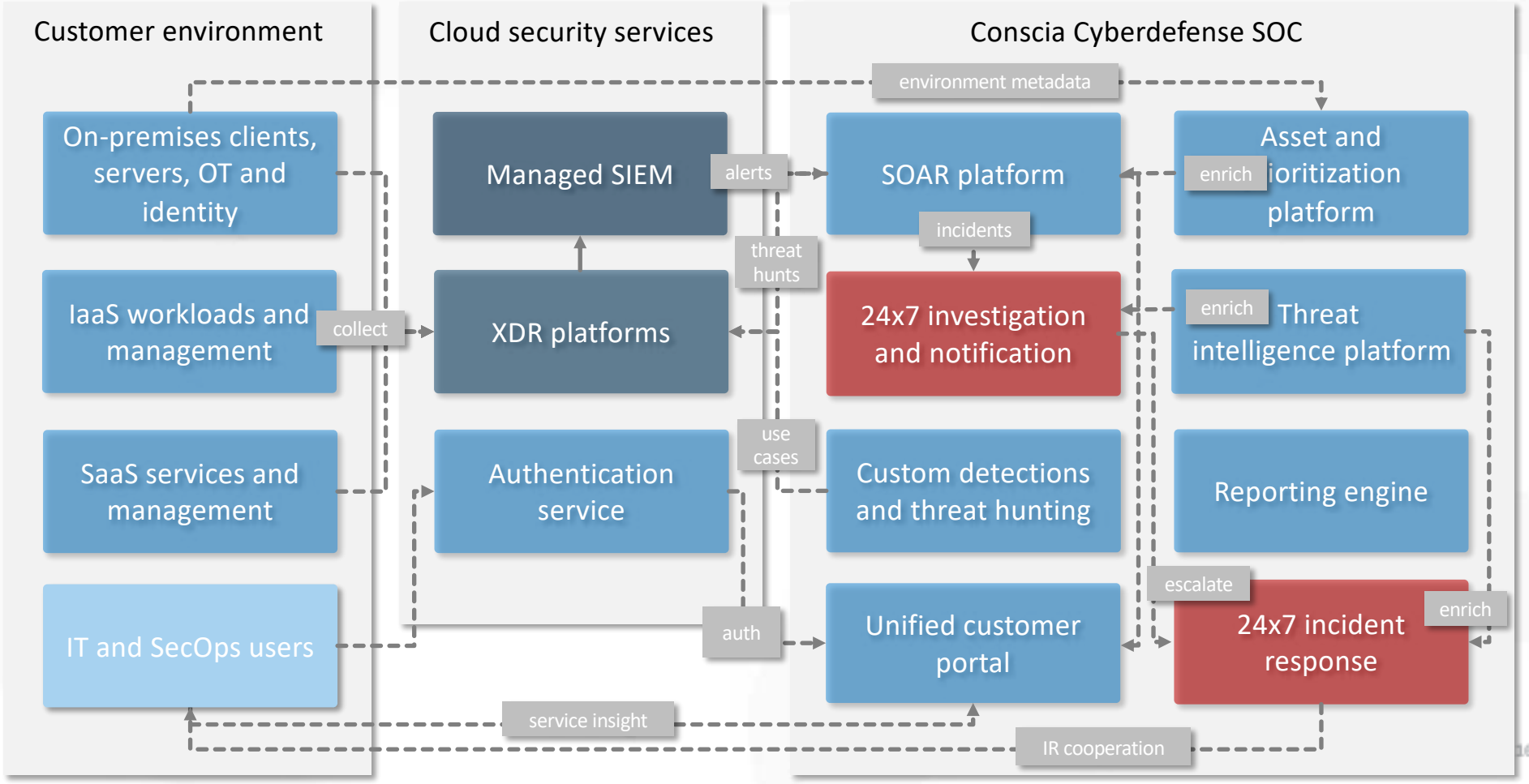
- Beschränkung des SOC auf Monitoring
- Wenig Interventions- und Handlungsmöglichkeiten für das SOC
- Komplexe und lange Einführungsprojekte
- Hohe Kundeneinbindung im Betrieb

Moderner Ansatz – Managed Detection & Response



- Einsatz von intelligenten Sensoren
- Endpoint Detection & Response (EDR)
  - Mehrzahl der Angriffe auf Endpoints ausgerichtet
  - Prävention, Angriffserkennung, Investigation, Threat Hunting und Response
- Weitere Quellen über XDR oder SIEM
  - NDR für OT, IoT, Medizintechnik
  - Next-Gen Firewall, Intrusion Detection Systeme
  - Mail, Web & Cloud Security
  - Identity & Access Management
- Definierte Interventions- und Handlungsmöglichkeiten für das SOC
- Kurze Einführungsprojekte mit geringer Komplexität im Vergleich zu SIEM
- Niedrige Kundeneinbindung und wirtschaftlicher Betrieb

Cyberdefense Platform Architecture



Informationssicherheit vs Datenschutz

EU-DSGVO
Erwägungsgrund 49

Risikobewertung von Informationssicherheits-maßnahmen in Datenschutzfolgeabschätzung

Erwägungsgrund 49

Netz- und Informationssicherheit als überwiegendes berechtigtes Interesse*

(49) Die Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams – CERT, beziehungsweise Computer Security Incident Response Teams – CSIRT), Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten stellt in dem Maße ein berechtigtes Interesse des jeweiligen Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service"-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.

In-house Detection and Response Fähigkeiten

Benötigt mindestens 2 (8x5) bis 5 (24x7) Vollzeitkräfte für eine Position, durchschn. Kosten SOC: 2,5M€ p.a.

Benötigt Expertenwissen für Threat investigation, Incident response, Digital forensics und Platform maintenance

TCO üblicherweise 7x höher als ausgelagertes SOC, mit hohem initialem Capex Investment

Outsourced Detection and Response Services

Gemeinsamer Pool von Experten um für mehrere Kunden SOC services zu liefern

Attraktiver Arbeitsplatz für Cybersecurity Spezialisten, Weiterbildungs- und Zertifizierungsprogramm, Partnerschaften mit Herstellern

Wirtschaftlicher Betrieb, laufende Kosten, geringe Anfangsinvestitionen

xevIT Cyber Resilience Programm – Portfolio

- Sicherheitsbewertung
- Security Check & Analyse
- Regelmäßige Penetrationstests
- Kontinuierliches Schwachstellenmanagement aaS

- Firewall aaS
- MFA aaS
- Email Security aaS
- Internet Security aaS
- Medizintechnik Sicherheit aaS
- OT Security aaS

- Wiederherstellung
- Nachbereitung
- Backup aaS
- Disaster Recovery aaS
- Archiving aaS
- Ransomware protection

- Cyberdefense Services
  - Endpoint
  - XDR
  - Enterprise

- Incident Response Service
  - IR Management
  - Eindämmung
  - Behebung


#cyberresilience
#gemeinsam
xevIT
part of conscia
www.xevit.com