Vom digitalen Nachzügler zum Cyber-Leader

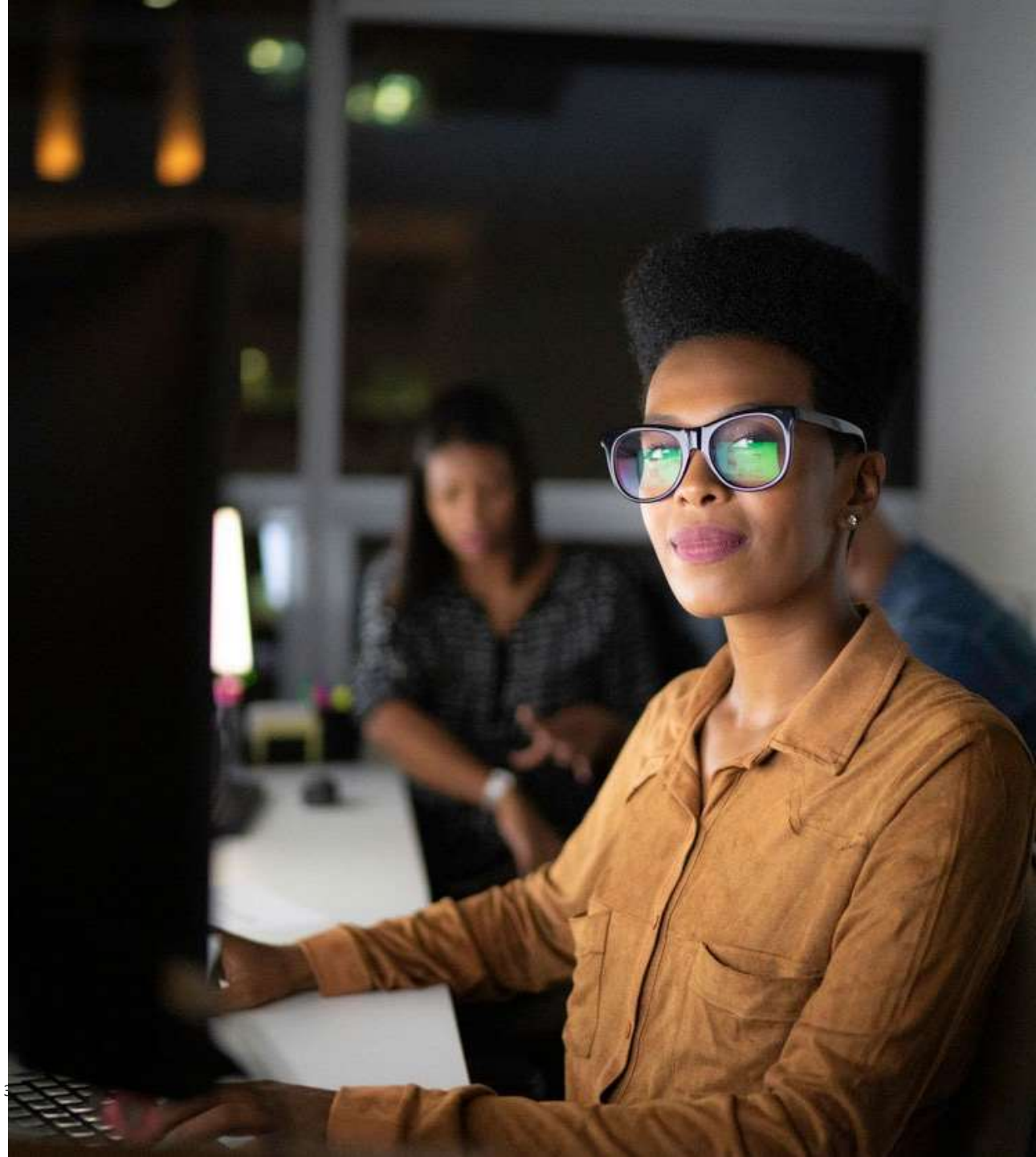
Paul Bauer
Regional Sales Director DE/EE

ILLUMIO CONFIDENTIAL

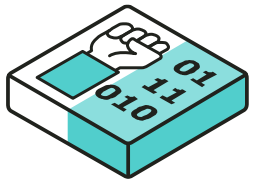
Der Schutz kritischer Güter ist schwieriger denn je!

Die Exekutiv-Charta

Cyber-Resilienz ist jetzt eine Priorität für die Unternehmensleitung

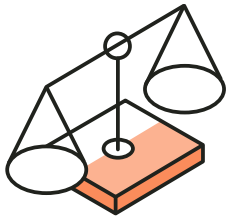


Die Aufgaben des CISO



Das Unternehmen schützen

Sicherstellen, dass ein Cybervorfall den Geschäftsbetrieb nicht gefährdet



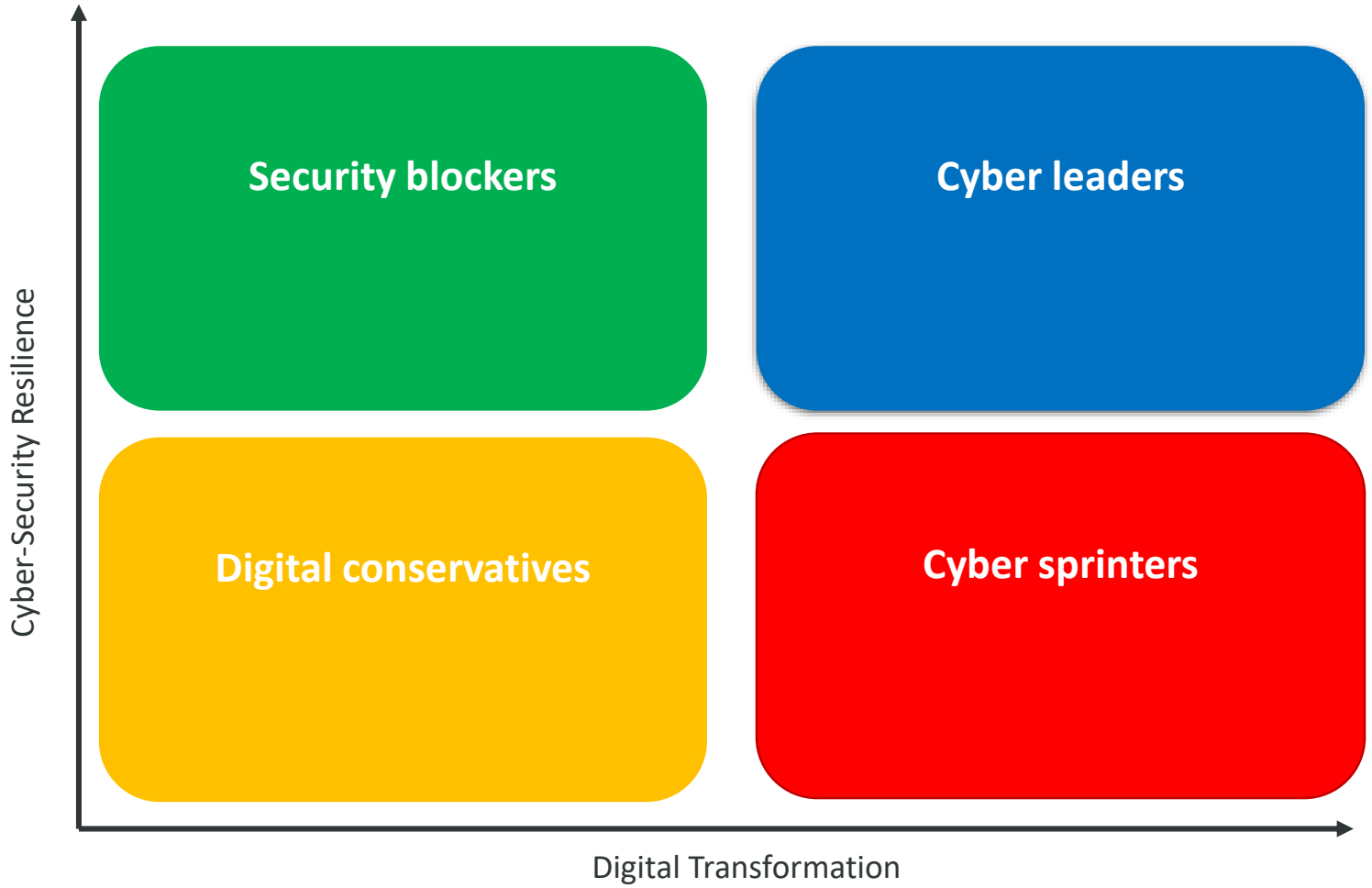
Abstimmung der Prioritäten

Balance zwischen Sicherheitsprioritäten und Unternehmenszielen

Management von Risiken

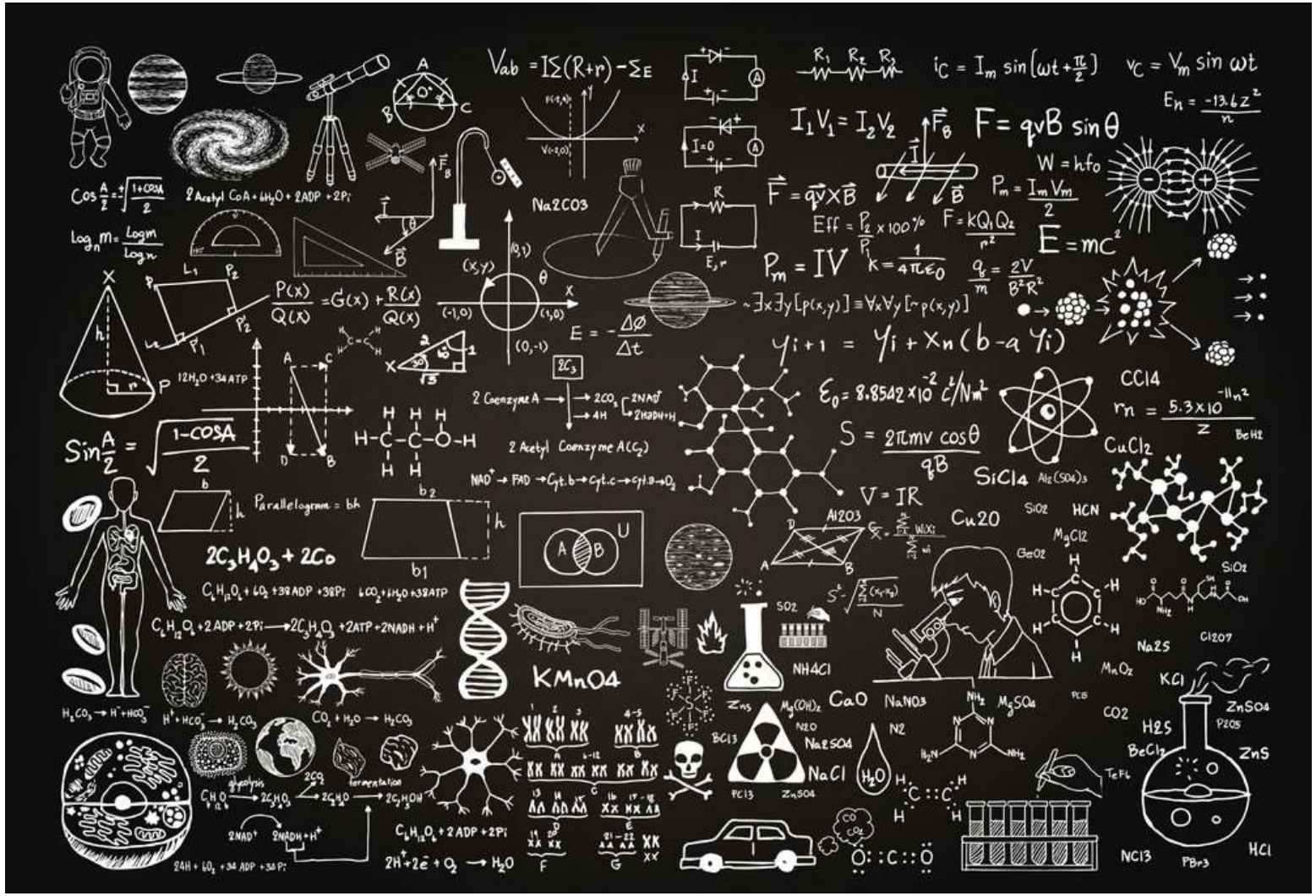
Risiken angemessen managen

Transformierung des Unternehmens



Ransomware hat sich von einem Problem der Cybersicherheit, zu einem Problem der Geschäftsstabilität entwickelt

Wo und wie soll man mit Zero Trust anfangen?



illumio

Zwei wesentliche Zero-Trust-Prinzipien

Gehen Sie von einer Breach aus & planen Sie diese Zugriff nur mit “least privilege access”

NIST Zero Trust Prämissen

- Das gesamte Unternehmensnetz wird nicht als Vertrauenszone betrachtet.
- Geräte im Netzwerk sind nicht unbedingt Eigentum des Unternehmens.
- Keine Ressource ist von vornherein vertrauenswürdig
- Nicht alle Unternehmensressourcen befinden sich in der unternehmenseigenen Infrastruktur
- Remote-Unternehmensanlagen können ihrem lokalen Netzwerk nicht vertrauen
- Anlagen und Arbeitsabläufe, die zwischen Unternehmens- und Nicht-Unternehmensinfrastrukturen verschoben werden, sollten eine einheitliche Security Policy und Sicherheitsstrategie haben.

illumio

Die 3 Schritte zur Cyber-Resilienz

Identifizierung der gefährdetsten Bereiche

Entwicklung eines sofortigen Reaktionsplan

Entwicklung einer langfristigen Strategie

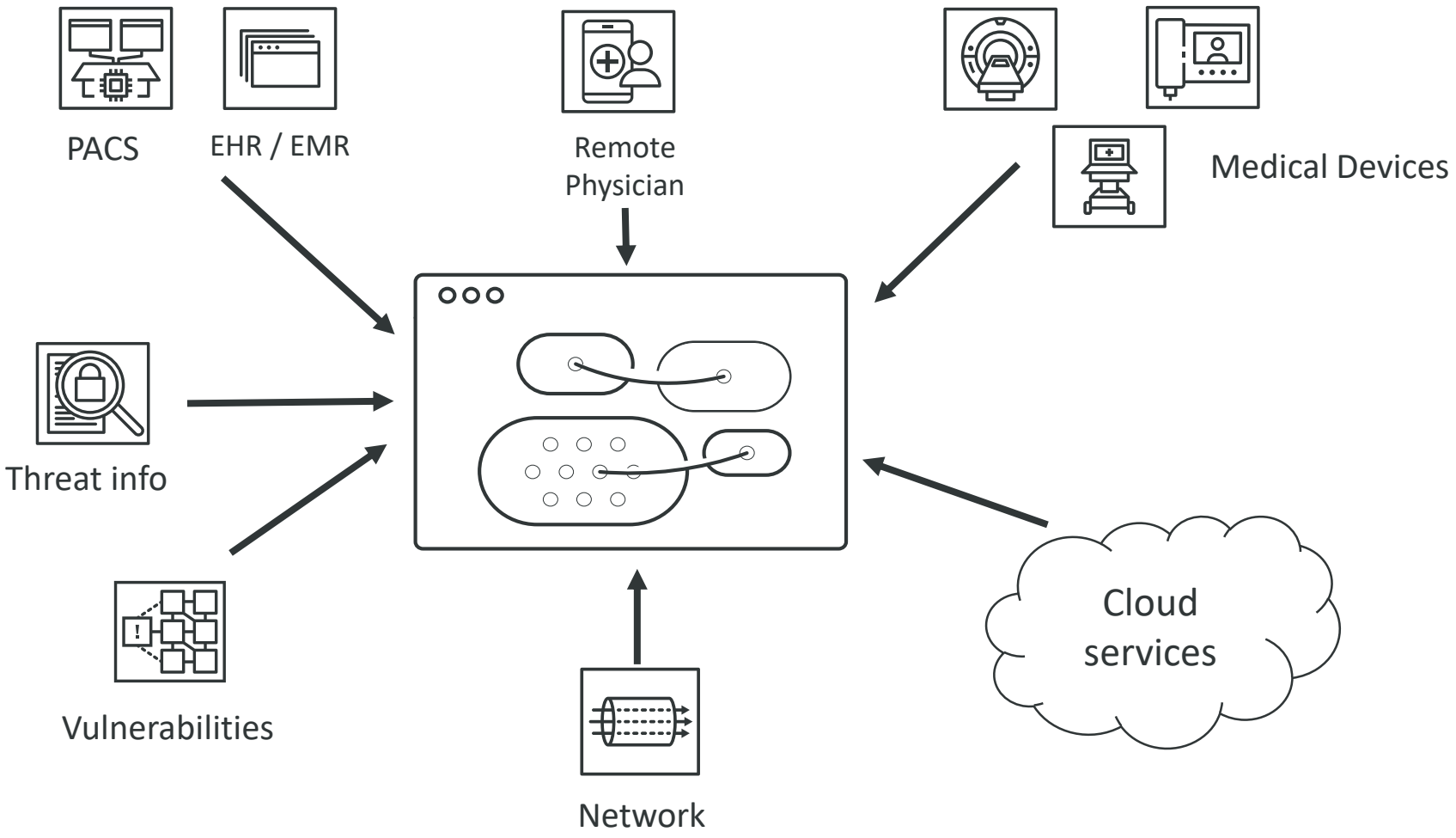
Die 3 Schritte zur Cyber-Resilienz

Identifizierung der gefährdetsten Bereiche

Risiko verstehen

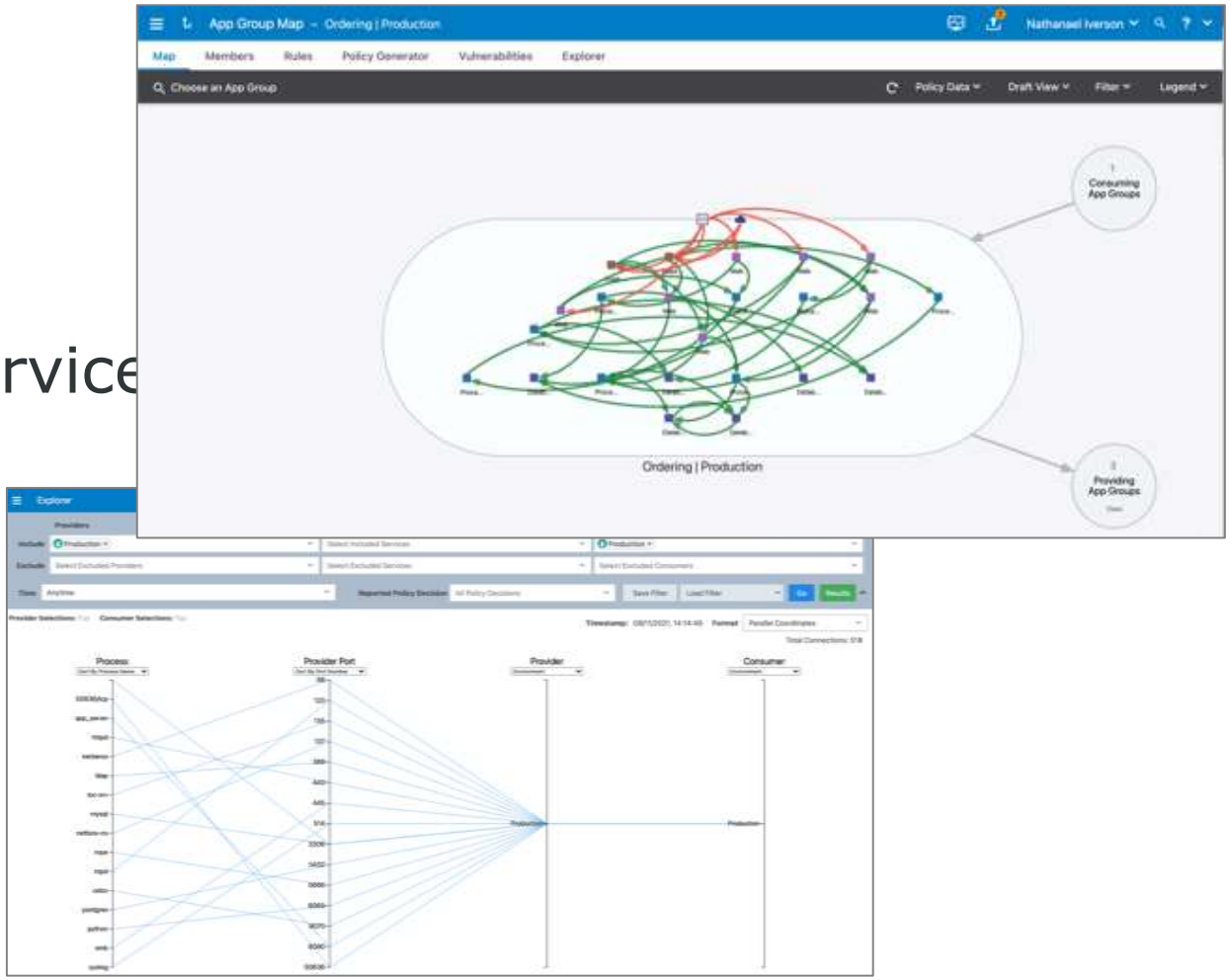
Likelihood of threat event initiation or occurrence	Likelihood Threat Event Results in Adverse Impacts				
	Very low	Low	Moderate	High	Very high
Very high					
High					
Moderate					
Low					
Very low					

Darstellung ALLER Kommunikationen zum Risiko Verständnis



Karte der gesamten Kommunikation

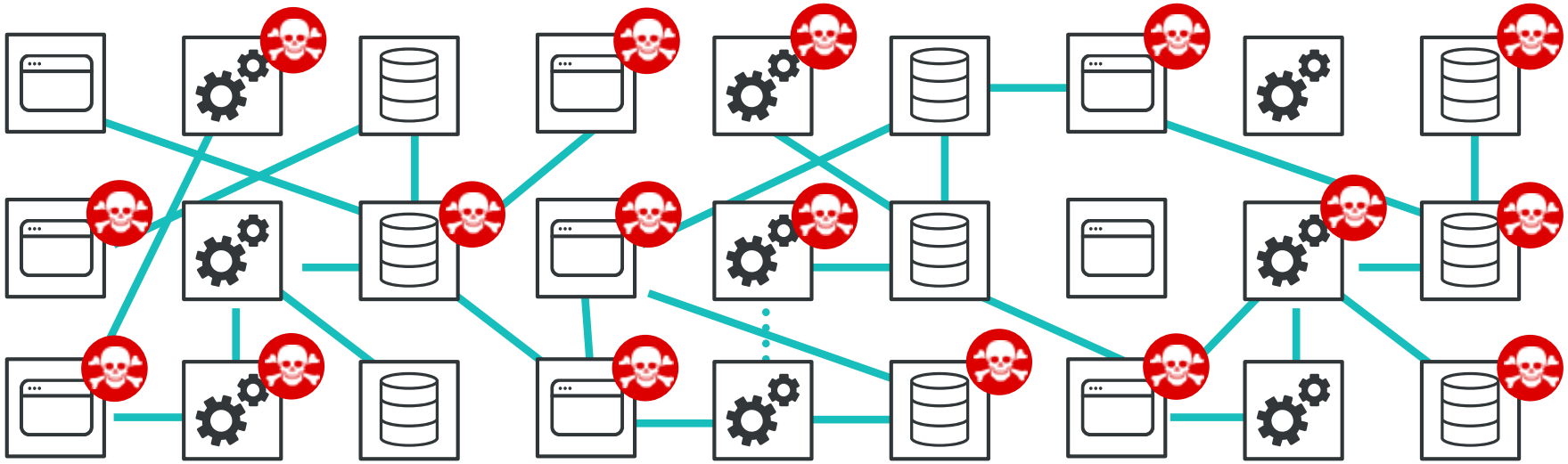
- Workload zu workload
- Anwendung zum Device
- System zum externen Bereich
- Application zum cloud service
- IT zu OT



Die 3 Schritte zur Cyber-Resilienz

Entwicklung eines sofortigen Reaktionsplan

Ransomware verbreitet sich lateral



Schützen Sie die hochwertigen Assets

Potenzielle Risken

Highly Connected Ports

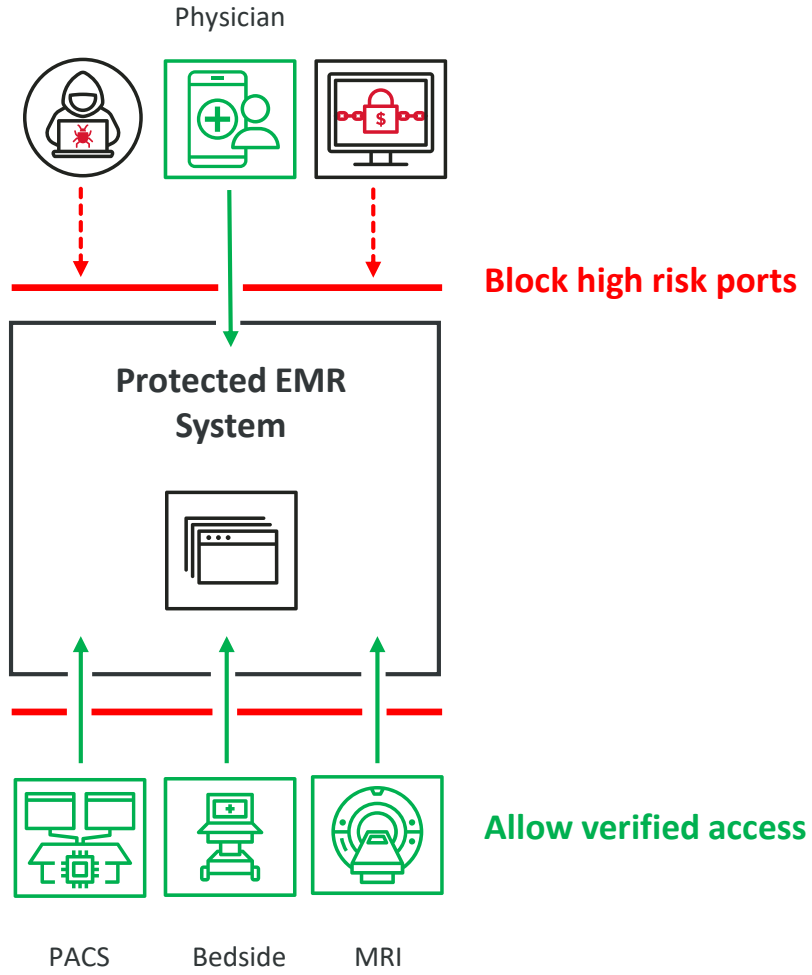
Core Services
Management ports
Polling/Reporting systems

Peer-to-Peer Ports

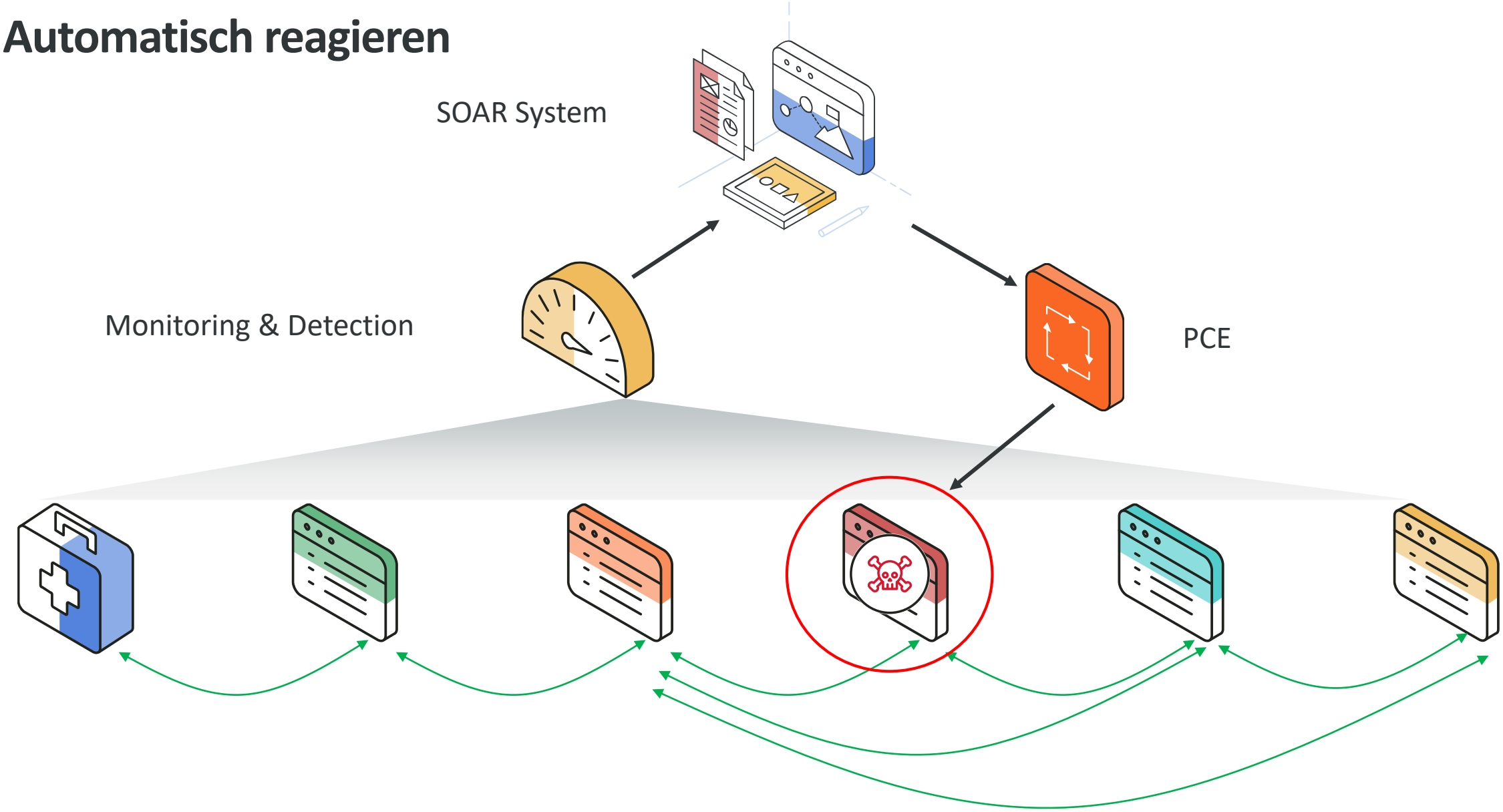
RDP, WinRM
SMB, RPC, WMI, DCOM
Social media

Well-Known Ports

DB
Core Services
Microsoft applications
Common Linux utilities



Automatisch reagieren



Die 3 Schritte zur Cyber-Resilienz

Entwicklung einer langfristigen Strategie

Zero Trust Modell

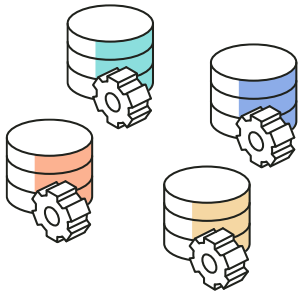
Zero Trust Network Access

Next generation perimeter, beschränken den Zugang auf verifizierte Benutzer

Zero Trust Segmentation

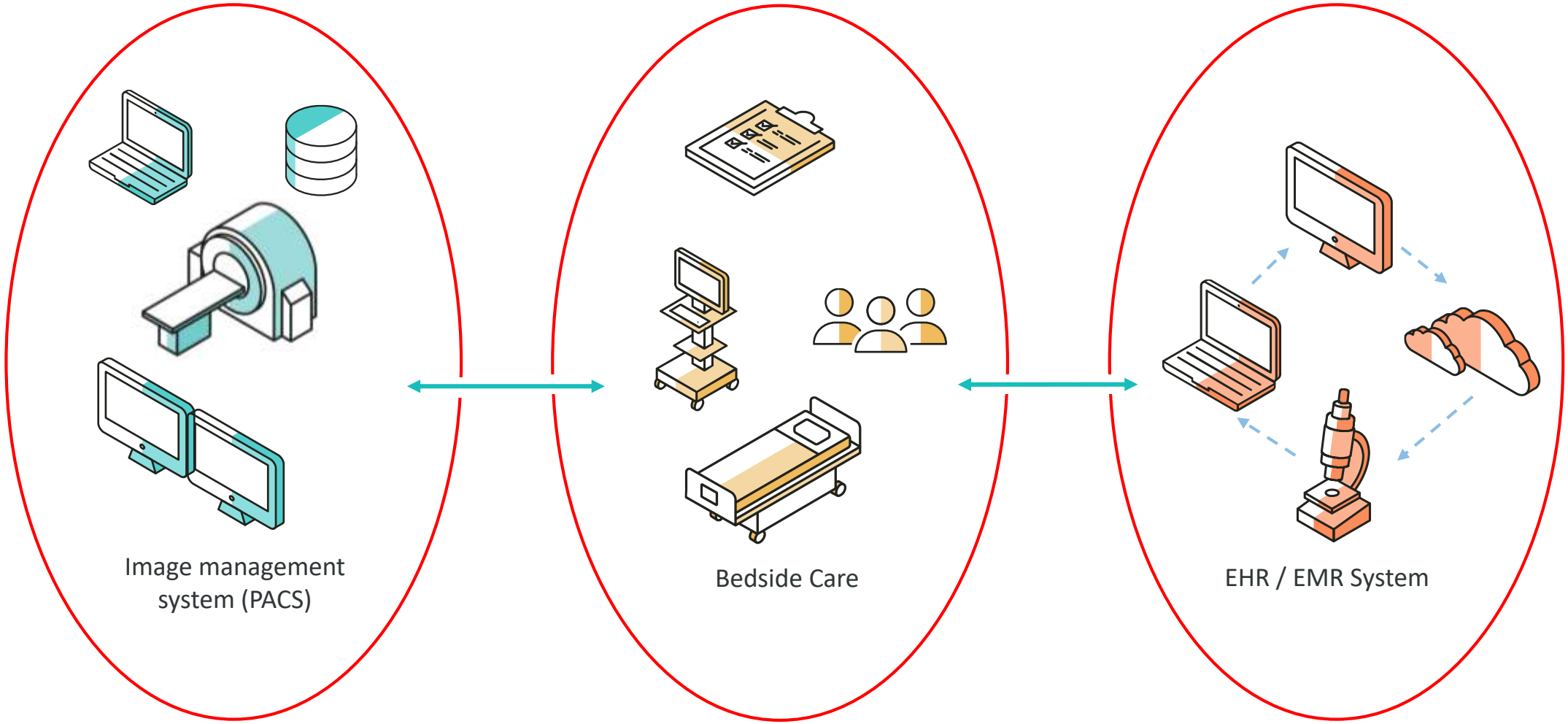
Kontrolle der Kommunikation zwischen geprüften Systemen und anderen Assets

Zero Trust Data Security



Zuverlässige Wiederherstellung von Daten

Was ist Zero Trust Segmentierung?

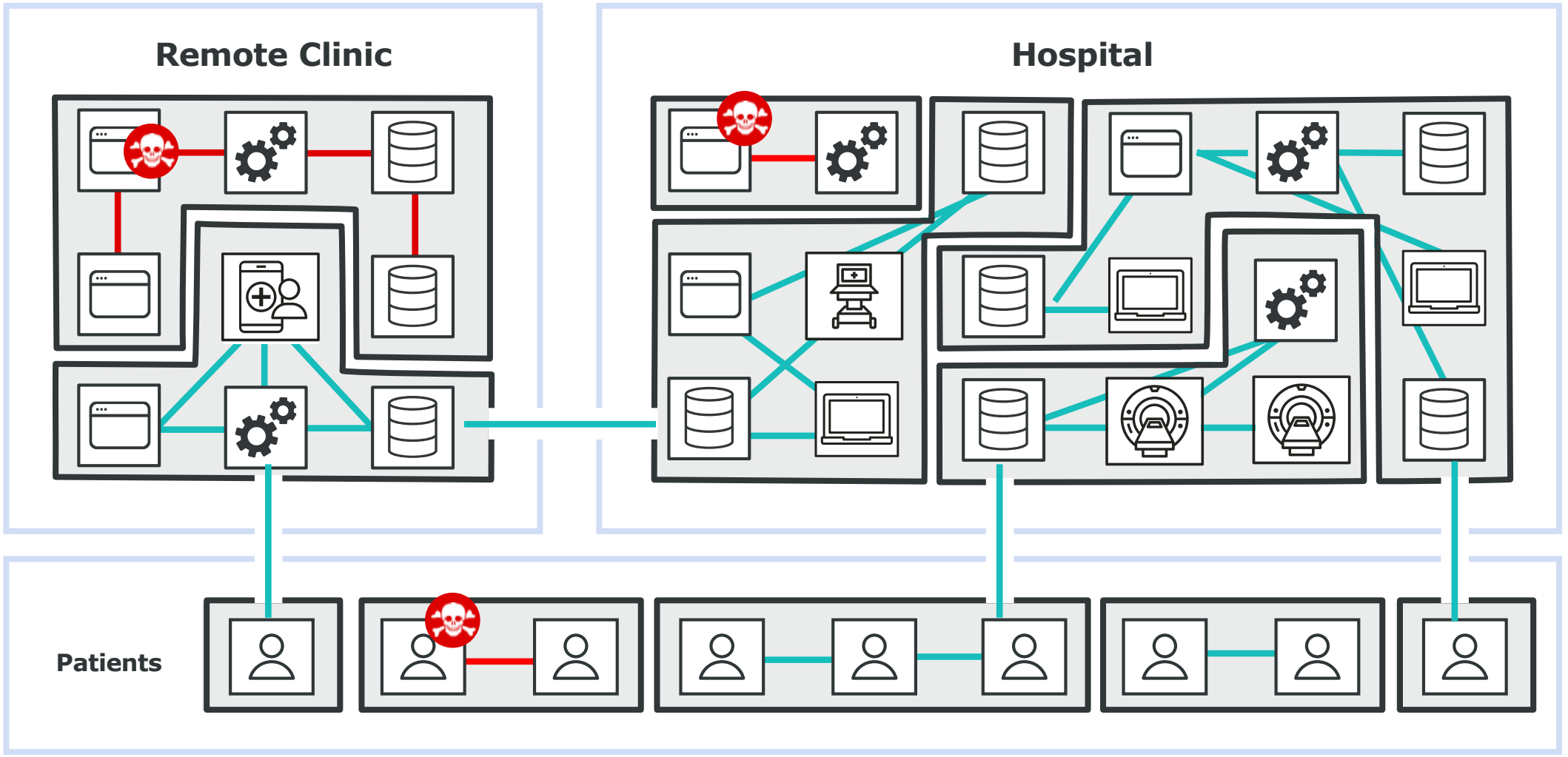


Least Privilege Access

Erstellen Sie einen Plan und testen Sie ihn!

Schutz kritischer Systeme

Verbreitung von Malware verhindern



Thank You

ILLUMIO CONFIDENTIAL