ZERO TRUST

ONLINE-SEMINAR #5: NETWORK

UNSERE PARTNER:

Extreme networks

ZERO TRUST

SCALTEL ZERO TRUST FRAMEWORK

SOC	Vulnerability Management	Event Management	Incident Response	Visibillity and Analytics Automation and Orchestration
Identity	Multi Faktor Authentification	Network Access	Cloud Access	Authentication Identity Stores
Device	Visibility	Classification	Endpoint Protection	Asset Management Data Access
Network / Environment	Network Topology	Macro Segmentation	Micro Segmentation	Network Segmentation Threat Protection
	Building Access Control	Building Segmentation	Physical Security Management	
Application	Secure Web Gateway	Secure Mail Gateway	Code Security	Threat Protection Application Security
Data	Graduierung	Encryption	Secure Backup	Encryption Access Determination
ISMS	Information Security	Privacy	Employee Awareness	Governance

ZERO TRUST

SCALTEL ZERO TRUST FRAMEWORK

Online-Seminar Network

SOC	Vulnerability Management	Event Management	Incident Response	Visibillity and Analytics Automation and Orchestration
Identity	Multi Faktor Authentification	Network Access	Cloud Access	Authentication Identity Stores
Device	Visibility	Classification	Endpoint Protection	Asset Management Data Access
Network / Environment	Network Topology	Macro Segmentation	Micro Segmentation	Network Segmentation Threat Protection
	Building Access Control	Building Segmentation	Physical Security Management	
Application	Secure Web Gateway	Secure Mail Communication	Code Security	Threat Protection Application Security
Data	Graduierung	Encryption	Secure Backup	Encryption Access Determination
ISMS	Information Security	Privacy	Employee Awareness	Governance

ZERO TRUST

EINE REVOLUTIONÄRE SICHERHEITSSTRATEGIE

Never Trust, always verify

Eliminierung des „Implicit Trust“
Kontinuierliche Prüfung von
Identität, Device und Applikation
Auswirkung auf die Definition des Perimeters?

Least privilege access

Zugriff nur auf benötigte Ressourcen
Umkehrung des Regelwerkes

Assume breach

Mehrere Verteidigungslinien
Schnelle Erkennung

ZERO TRUST

RÜCKBLICK

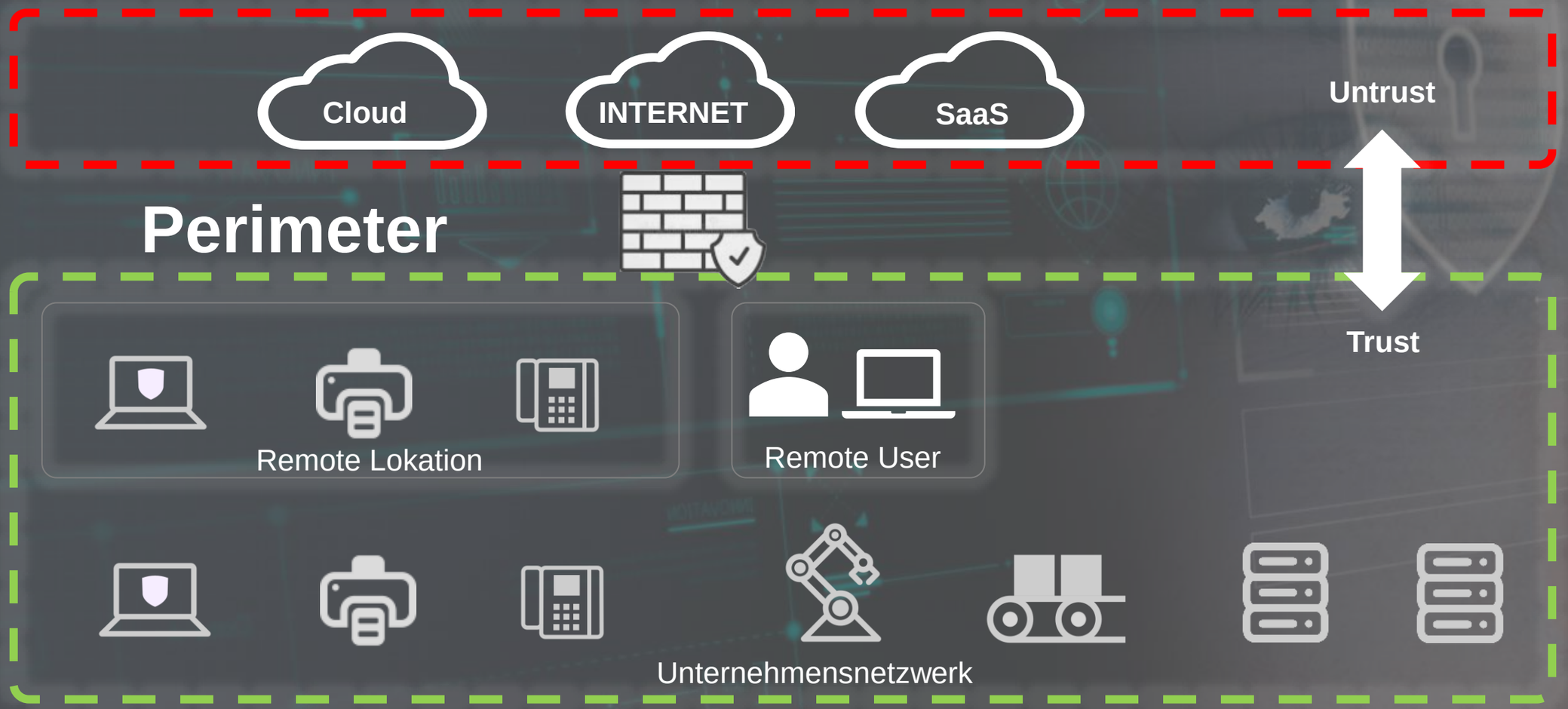
Online-Seminar Perimeter

SOC	Vulnerability Management	Event Management	Incident Response	Visibillity and Analytics Automation and Orchestration
Identity	Multi Faktor Authentification	Network Access	Cloud Access	Authentication Identity Stores
Device	Visibility	Classification	Endpoint Protection	Asset Management Data Access
Network / Environment	Network Topology	Macro Segmentation	Micro Segmentation	Network Segmentation Threat Protection
	Building Access Control	Building Segmentation	Physical Security Management	
Application	Secure Web Gateway	Secure Mail Communication	Code Security	Threat Protection Application Security
Data	Graduierung	Encryption	Secure Backup	Encryption Access Determination
ISMS	Information Security	Privacy	Employee Awareness	Governance

ZERO TRUST

PERIMETER

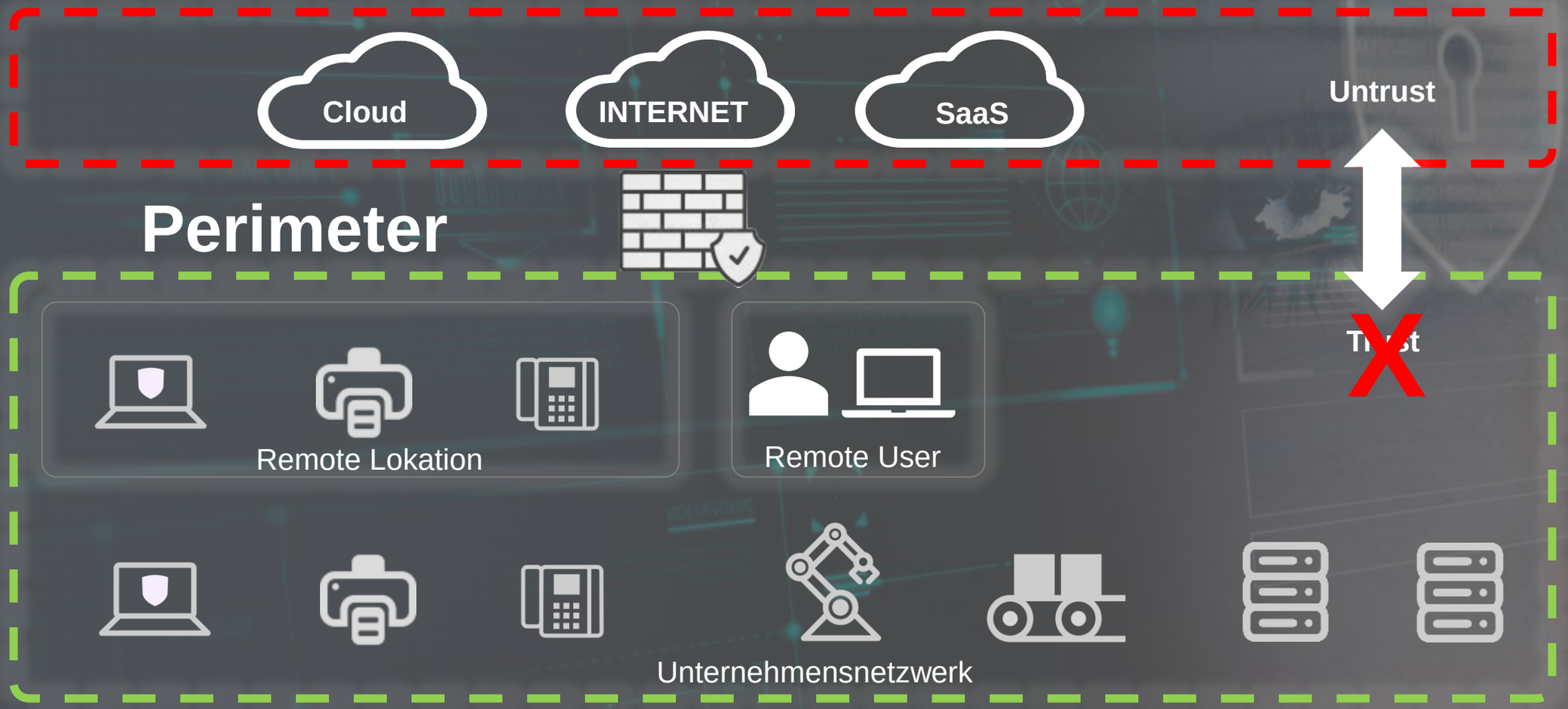
Never Trust, always verify



ZERO TRUST

PERIMETER

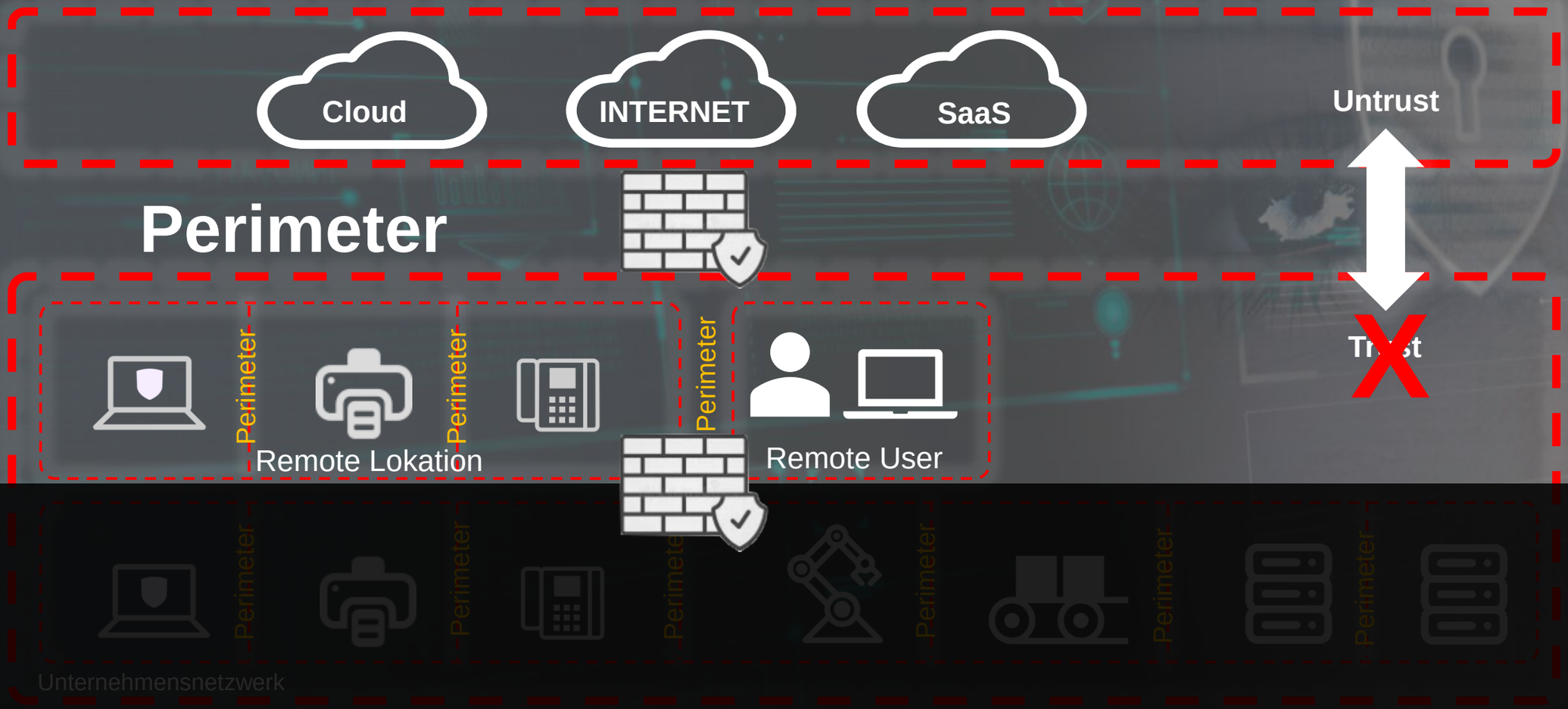
Never Trust, always verify



ZERO TRUST

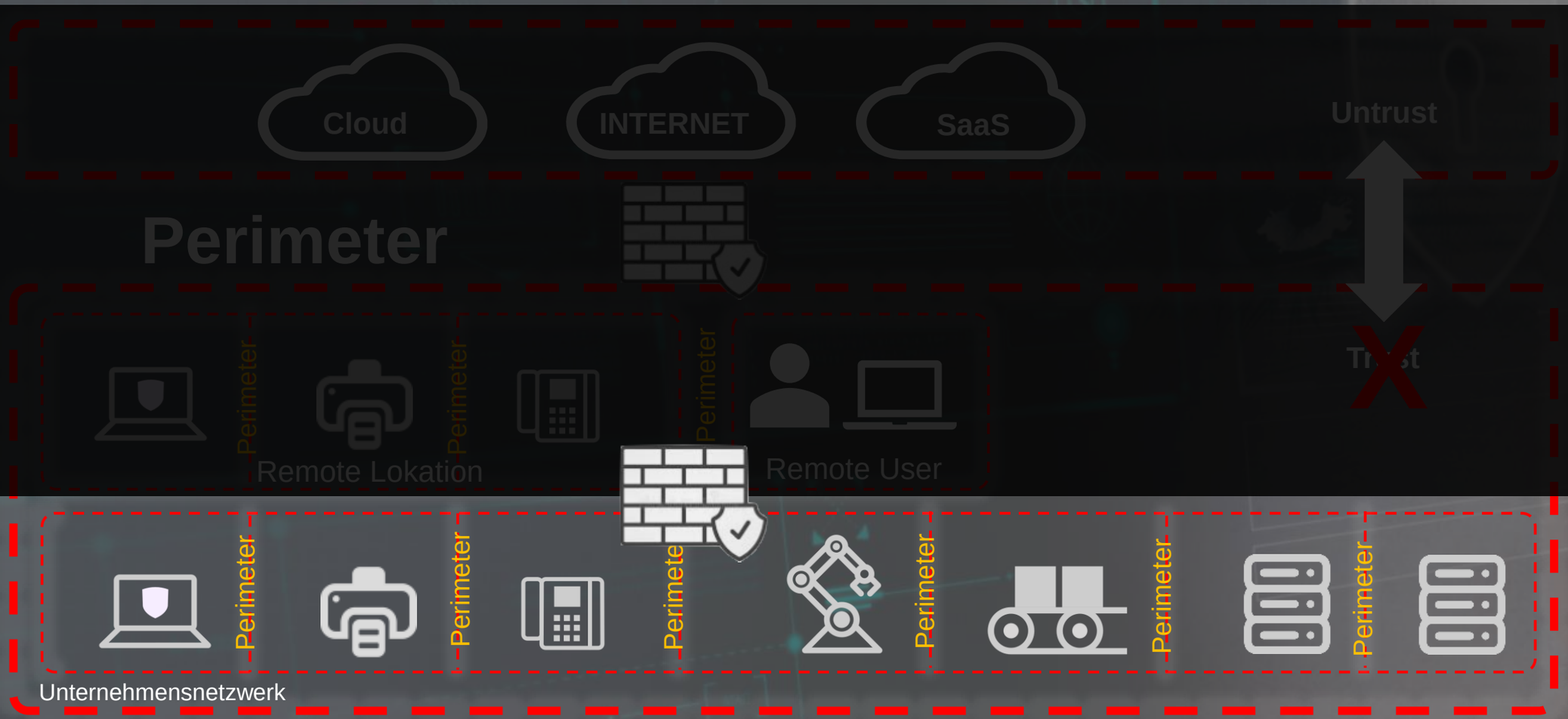
PERIMETER

SASE



ZERO TRUST

NETWORK



ZERO TRUST

SCALTEL ZERO TRUST FRAMEWORK

Online-Seminar Network

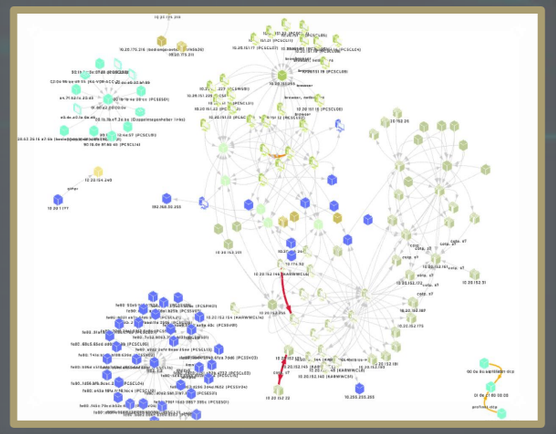
SOC	Vulnerability Management	Event Management	Incident Response	Visibillity and Analytics Automation and Orchestration
Identity	Multi Faktor Authentification	Network Access	Cloud Access	Authentication Identity Stores
Device	Visibility	Classification	Endpoint Protection	Asset Management Data Access
Network / Environment	Network Topology	Macro Segmentation	Micro Segmentation	Network Segmentation Threat Protection
	Building Access Control	Building Segmentation	Physical Security Management	
Application	Secure Web Gateway	Secure Mail Communication	Code Security	Threat Protection Application Security
Data	Graduierung	Encryption	Secure Backup	Encryption Access Determination
ISMS	Information Security	Privacy	Employee Awareness	Governance

ZERO TRUST

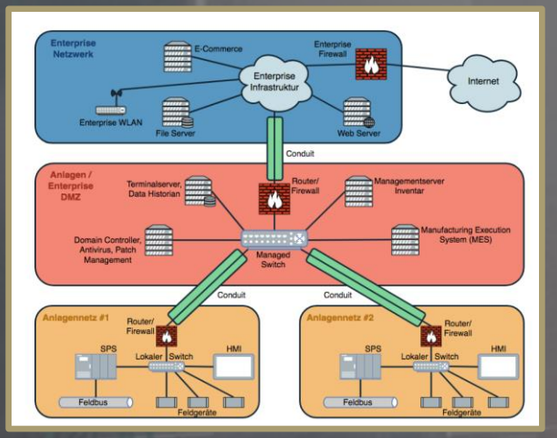
NETWORK

ZERO TRUST

NETWORK



DMZ			
Access	**Corporate**	**Industrial**	**Betriebsleitebene**
Workstations	Webserver	Filetransfer	MES
Drucker	Sec.-Gateways	Jump-Hosts	OPC Server
Gäste			Engineering Stationen
			Initial Access



Visibility

Wir können nur das schützen, was wir sehen

Ergebnis: Asset Inventory

Classification

Wir müssen Risiken bewerten und Schutzmaßnahmen definieren

Ergebnis: Workbook für Projekte

Segmentation

Eine Segmentierung reduziert die Angriffsfläche und ermöglicht eine schnelle Reaktion bei Angriffen

Ergebnis: Projektumsetzung in Reifegradmodellen

MÖGLICHE QUELLEN

VISIBILITY

Online Seminar:
Devices - 11.05.23

Endpoint-Security

NAC

Leitstand

VM-Scanner

OT-Monitoring

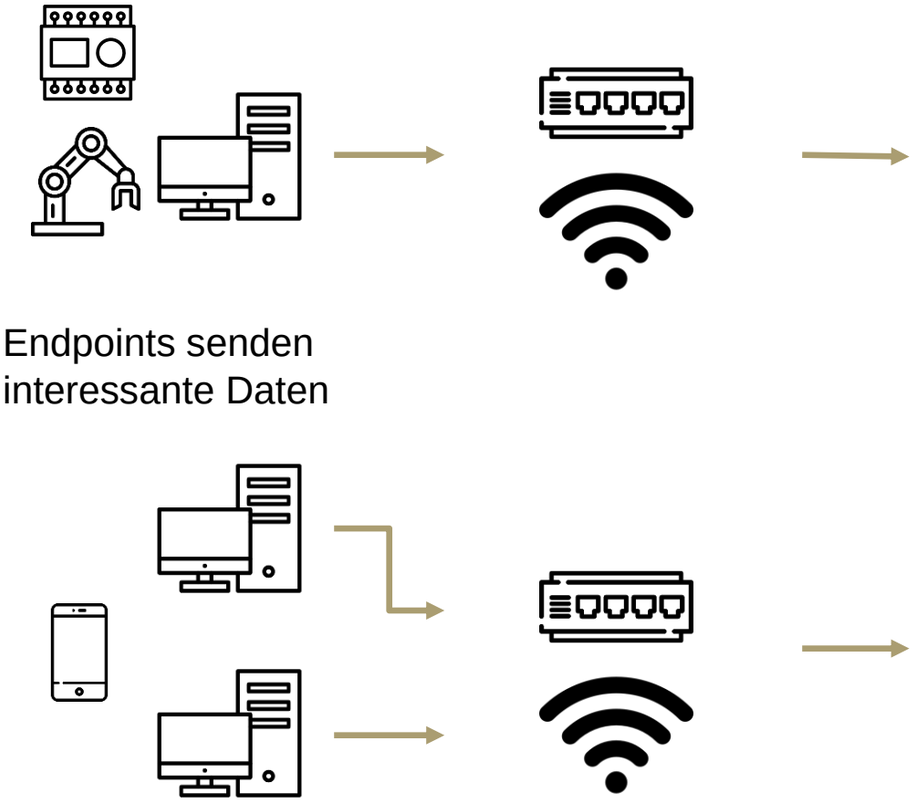
IP-Management

Netzwerk-Monitoring

ENDPOINT PROFILING

VISIBILITY

Data Collection	Visibility - autom. Erkennung



Endpoints senden
interessante Daten

NAC

OT-Monitoring

Network Access Control – Visibility:
Authentifizierung von Benutzer und/oder Geräten für einen sicheren Netzwerkzugriff

OT-Monitoring – Visibility:
Passive Detection:
Analyse des Netzwerkverkehrs ohne Beeinflussung des Endpoints, um Endpoints und Verkehrsmuster zu identifizieren.

NETWORK ACCESS CONTROL

VISIBILITY

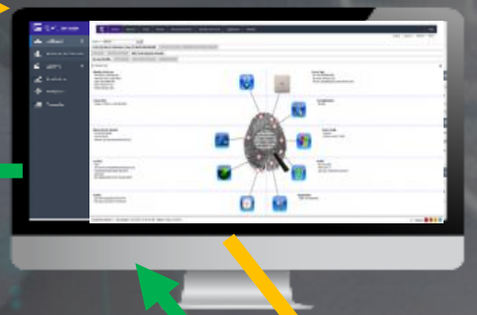
- Wer
- Was
- Wann
- Wo
- Wie
- Bedrohung

Authenticator
LAN/WLAN

EAPOL

Radius Anfrage

Authentication Server
(Radius, NAC-Server)



Success
USER VLAN

Accept

Firewall mit
IDS und IPS

Active Directory

NETWORK ACCESS CONTROL

VISIBILITY

Zentrale Sicherheitslösung für den Zugriff auf Netzwerkressourcen

Identität, Profil und Vorschriften

Wer	unbekannt
Was	unbekannt
Wann	unbekannt
Wo	unbekannt
Wie	unbekannt
Bedrohung	unbekannt

NETWORK ACCESS CONTROL

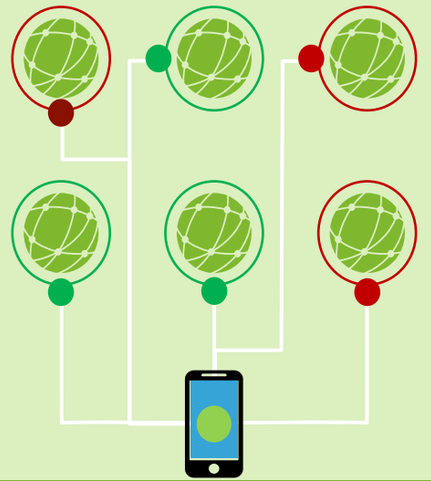
VISIBILITY

Zentrale Sicherheitslösung für den Zugriff auf Netzwerkressourcen

Identität, Profil und Vorschriften

Wer	Frau Mayer (Mitarbeiterin)
Was	iPhone X
Wann	8:00 Uhr
Wo	1.OG
Wie	WLAN
Bedrohung	Aktuelles OS

Netzwerk Ressourcen



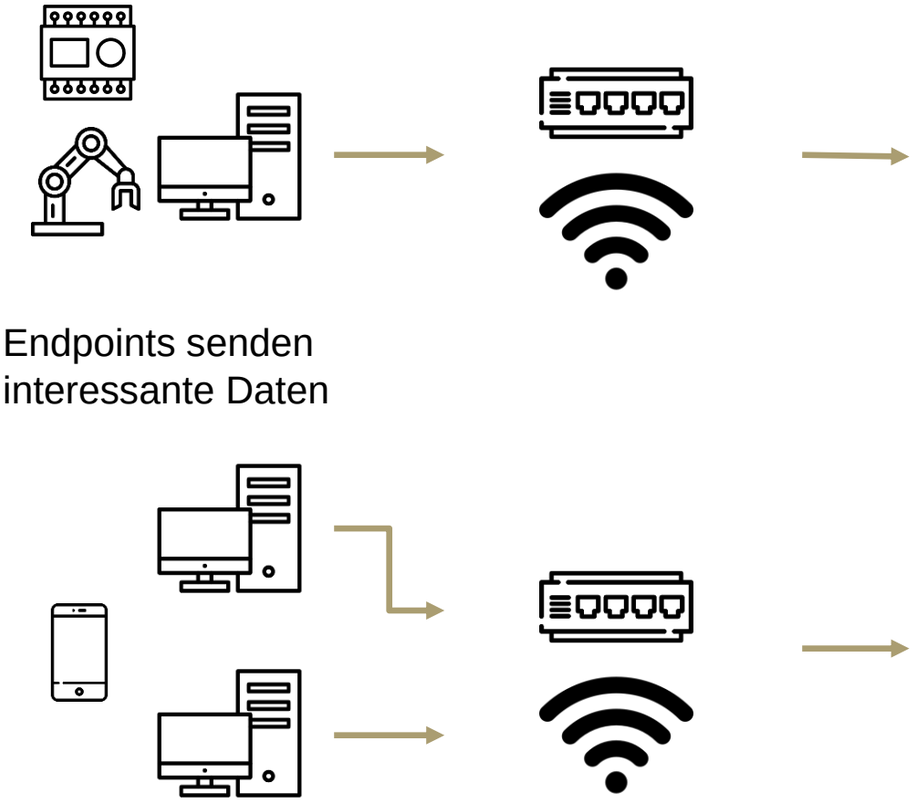
Rollenbasierter Zugriff

Bedingungen erfüllt

ENDPOINT PROFILING

VISIBILITY

Data Collection	Visibility - autom. Erkennung



NAC

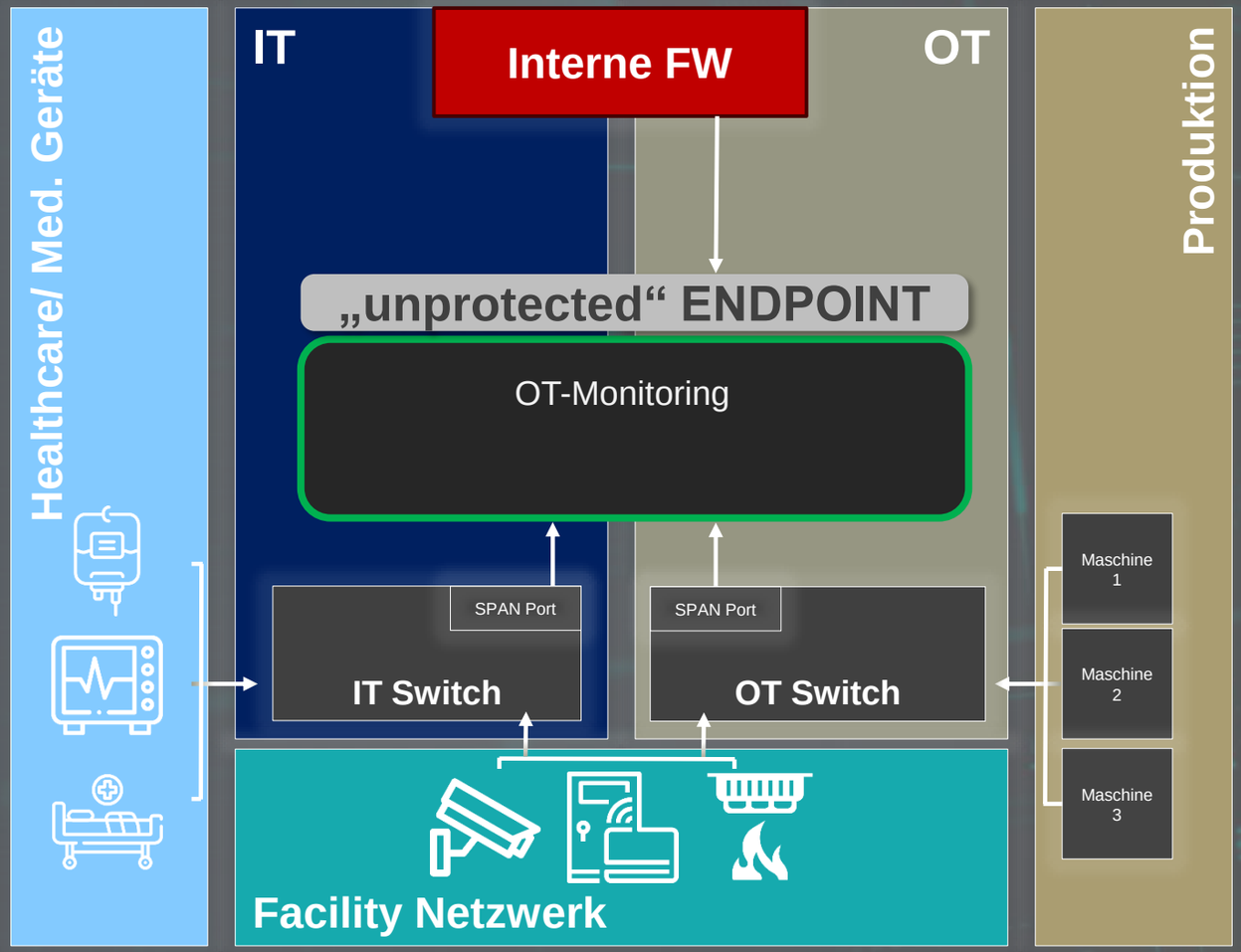
OT-Monitoring

<u>Network Access Control – Visibility:</u>
Authentifizierung von Benutzer und/oder Geräten für einen sicheren Netzwerkzugriff

<u>OT-Monitoring – Visibility:</u>
Passive Detection:
Analyse des Netzwerkverkehrs ohne Beeinflussung des Endpoints, um Endpoints und Verkehrsmuster zu identifizieren.

OT-MONITORING

VISIBILITY



Security Scan
„unprotected“ Endpoint

- **Passiv (Vermeidung von Betriebsstörungen kritischer Umgebungen)**

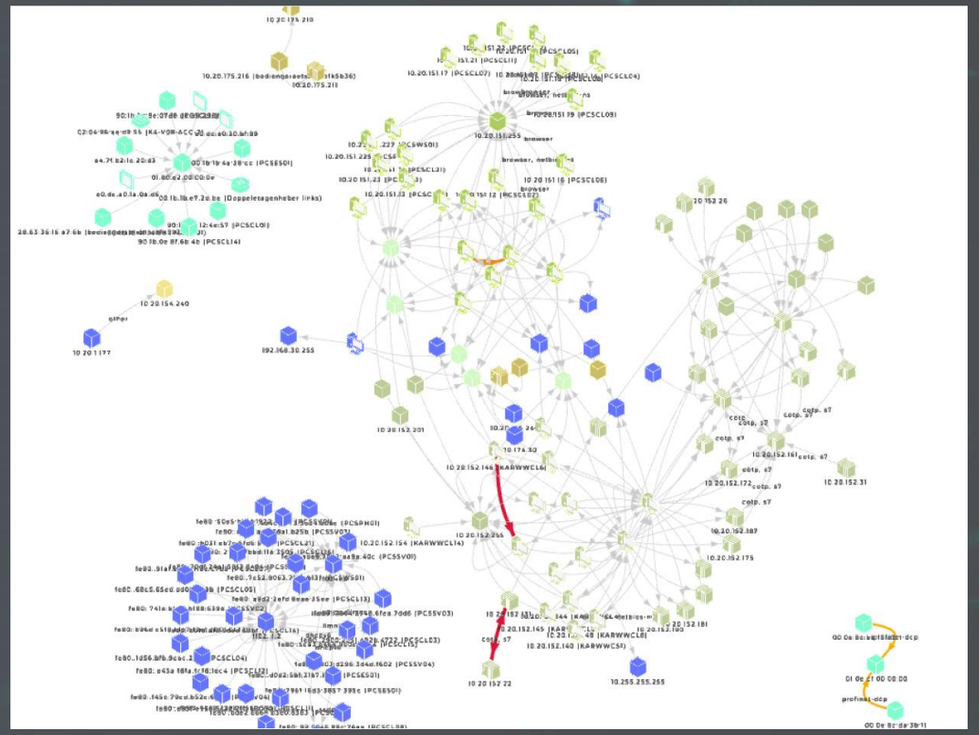
Analyse des Netzwerkverkehrs ohne Beeinflussung des Endpoints, um Endpoints und Verkehrsmuster zu identifizieren.

ERGEBNISSE EINES PASSIVEN SCANS

VISIBILITY

Transparente Netzwerkdarstellung

Netzwerkteilnehmer und Kommunikationsbeziehungen



Ergebnisse des passiven Scans

Asset- und Kommunikations Inventory

Asset view

Page 1 of 1, 7 entries / filtered by **name: pn-io** / sorted by **name: desc**

ACTIONS	NAME	TYPE	OS/FIRMWARE	
•••	pn-io			
	pn-io	OT_device	Firmware: V2.5.0	10.1.4.38
	pn-io	OT_device		
	pn-io	OT_device	Firmware: V3.0.23	10.1.4.43
	pn-io	OT_device	Firmware: V2.6.0	10.1.4.29
	pn-io	OT_device	Firmware: V2.3.2	10.1.4.33
	pn-io	OT_device	Firmware: V2.5.0	10.1.4.36
	pn-io	OT_device		10.1.4.32

From	To	Protocol	Transport protocols	First activity time	Is broadcast	Is to public
						true
10.31.249.31	34.102.140.103	https	tcp	16:14:07	false	true
10.31.11.30	34.102.140.103	https	tcp	16:14:20	false	true
10.31.246.202	34.102.140.103	https	tcp	16:14:23	false	true
10.30.14.34	80.154.223.99	ssh	tcp	16:19:01	false	true
10.30.13.208	9.9.9.9	dns	udp	16:07:41	false	true
10.30.13.208	8.8.8.8	dns	udp	16:24:23	false	true
10.30.13.208	1.1.1.1	dns	udp	16:02:27	false	true
10.30.13.208	116.202.229.59	other	tcp	2023-03-24 14:42:49	false	true

ASSET IDENTITY

VISIBILITY

NAC

OT-Monitoring

Asset Identity:

- User
- Lokation
- Asset OS
- Asset Mac Address
- Asset IP Address
- Asset Device Type
- Asset Name
- Asset Protocol
- Asset Group

Asset Identity:

Rockwell Automation/Allen-Bradley 5069-L330ERM/A Series

Technology category	OT
Type	Controller
Vendor	Rockwell Automation/Allen-Bradley
Product name	5069-L330ERM/A

Os or firmware	Firmware: 33.015
Ip	10.10.75.11
Mac address	5c:88:16:98:b9:d9
Mac vendor	Rockwell Automation

ASSET IDENTITY

VISIBILITY

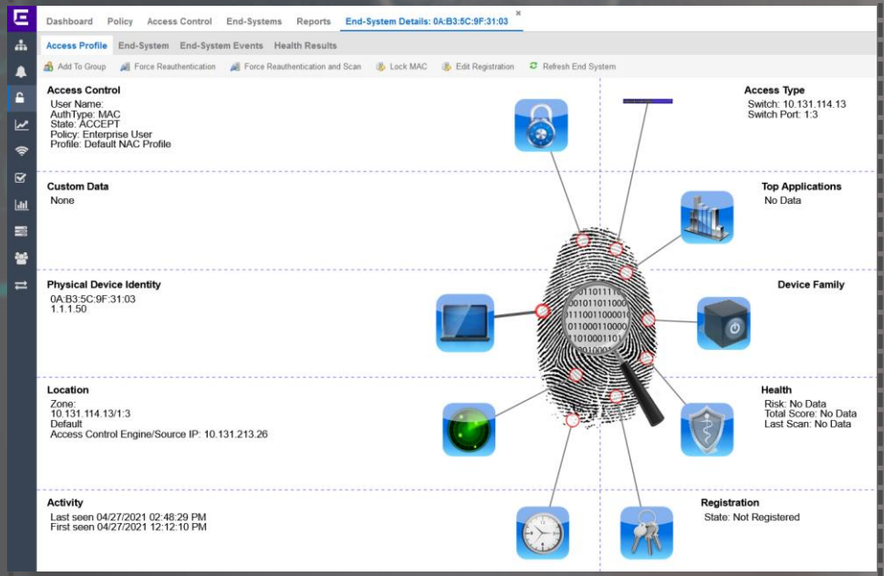
NAC

OT-Monitoring

Asset Identity:

- User
- Lokation
- Asset OS
- Asset Mac Address
- Asset IP Address
- Asset Device Type
- Asset Name
- Asset Protocol
- Asset Group

Asset Identity:



CLASSIFICATION

RISIKOBEWERTUNG

GRUNDLAGEN CLASSIFICATION

Asset Name	CVE	Score ↓	Category	Asset Technology category
5069-L330ERM/A	CVE-2021-22681		Insufficiently Protected Credentials	OT
5069-L330ERM/A	CVE-2022-1161		Inclusion of Functionality from Untrusted Con...	OT
5069-L330ERM/A	CVE-2022-1159		Improper Control of Generation of Code ('Cod...	OT
5069-L330ERM/A	CVE-2021-3011		Observable Discrepancy	OT

Risikobewertung
Entwicklung einer Übersicht zur Klassifizierung

INITIAL ACCESS

- Internetzugang
- E-Mail
- Aus dem Internet erreichbar

LATERAL MOVEMENT

- Managed/unmanaged
- Potenzielles Ziel für Berechtigungserweiterung
- Bekannte Sicherheitslücken

SCHUTZMECHANISMEN

- Mit Endpoint Security
- Ohne Endpoint Security

Asset Identity:

WIN10 Workstation:
- Internetzugang: **Ja**
- E-Mail: **Ja**
- Bekannte Sicherheitslücken: **keine**
- Endpoint Security: **vorhanden**

Asset Identity:
Controller 5069-L330ERM/A
Beispiel Asset OT:
- Internetzugang: **Nein**
- E-Mail: **Nein**
- Bekannte Sicherheitslücken: **Ja**
- Endpoint Security: **Nein**

KLASSIFIZIERUNGS-ÜBERSICHT

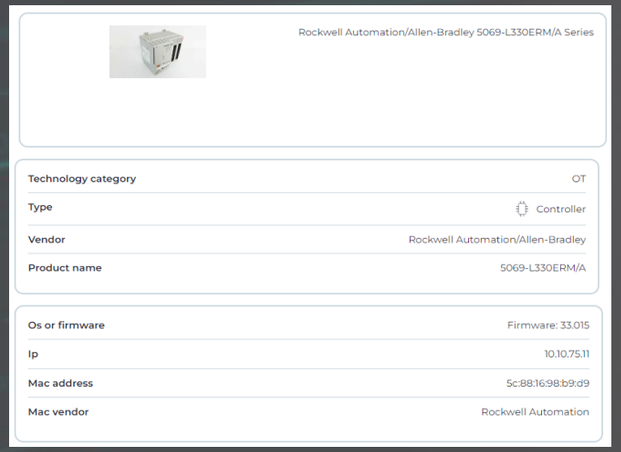
CLASSIFICATION

Unternehmensebene				DMZ		OT/ Industrial Control Systems			
Tier 0	**Tier 1**	**Tier 2**	**Access**	**Corporate**	**Industrial**	**Betriebsleitebene**	**Prozessleitebene**	**Steuerungsebene**	**Feldebene**
Domaincontroller	Appl.-Server	Terminalserver	Workstations	Webserver	Filetransfer	MES	SCADA	SPS	Sensoren
Exchange	Jump-Hosts		Drucker	Sec.-Gateways	Jump-Hosts	OPC Server	Local HMI	RTUs	Aktoren
	Management		Gäste			Engineering Stationen		IPCs	
Lateral Movement			**Initial Access**				**Lateral Movement**		

Asset Identity:

Beispiel WIN10 Workstation:
Internet Access: ja
Email Client: ja
→ Risiko: Initial Access
Maßnahmen: Endpoint Security
Client-Internet-Policy
Patch-MGMT
Software-Verteilung
Support: Nur über Client Admin Account

Asset Identity:



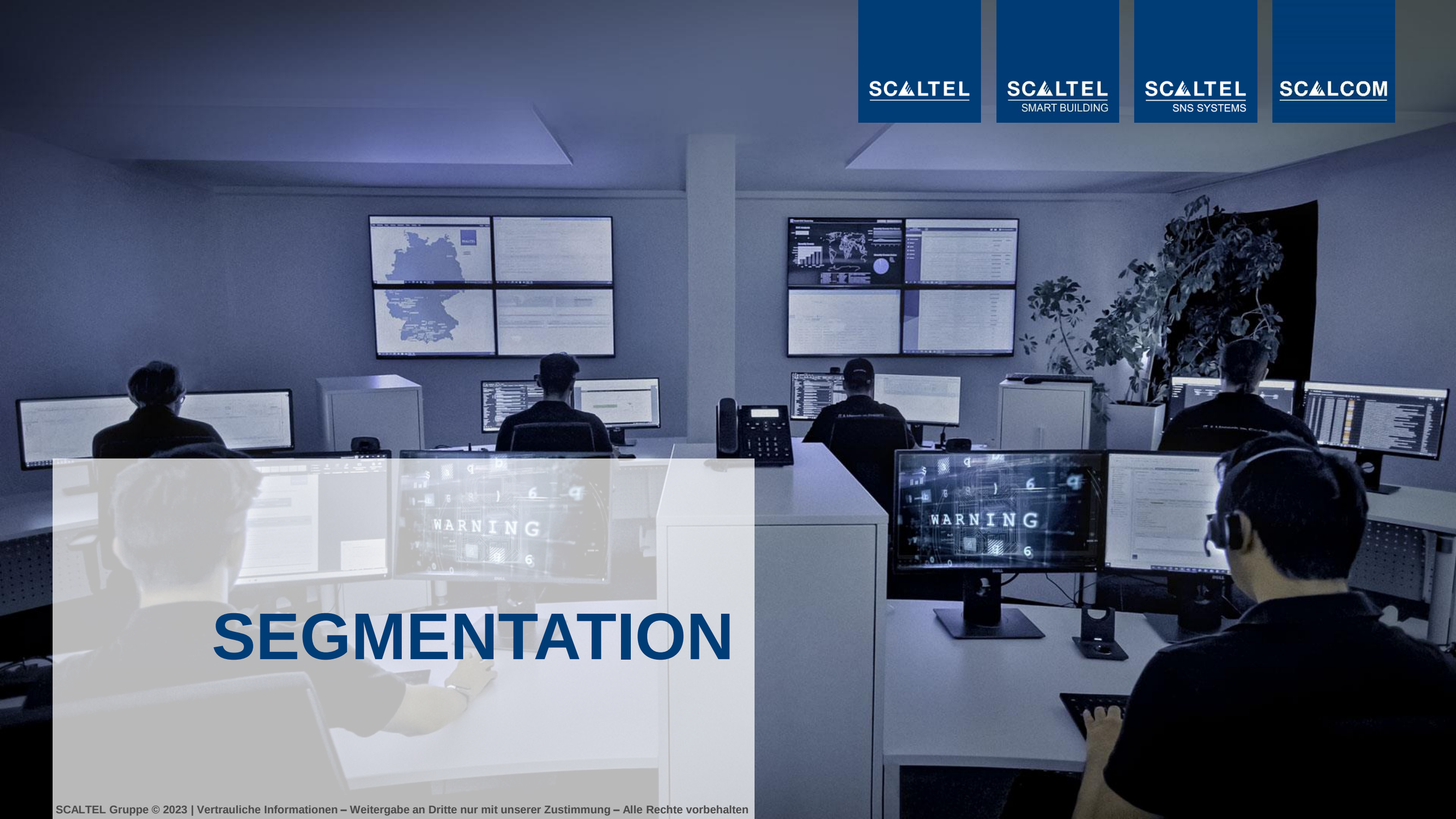
Gruppe: Steuerungsebene
Internet Access: nein
Email Client: nein
Schwachstellen OS: ja
→ Risiko: Lateral Movement
Maßnahmen: Micro Segmentierung
Policy: Zugriff nur auf Prozessleit- und Feldebene

KOMMUNIKATIONSMATRIX

CLASSIFICATION → SEGMENTATION

	Internet access	Internet restricted	Corporate access	Filetransfer/Jump-Host	Betriebsleitebene	Prozessleitebene	Steuerungsebene	Feldebene
Sensoren							x	
Aktoren							x	
SPS						x		x
RTU						x		x
IPC						x		x
SCADA					x		x	
HMI					x		x	
MES		x		x		x		
OPC Server		x		x		x		
Engineering Stationen		x	x	x		x		
Filetransfer			x					
Jump-Hosts			x					

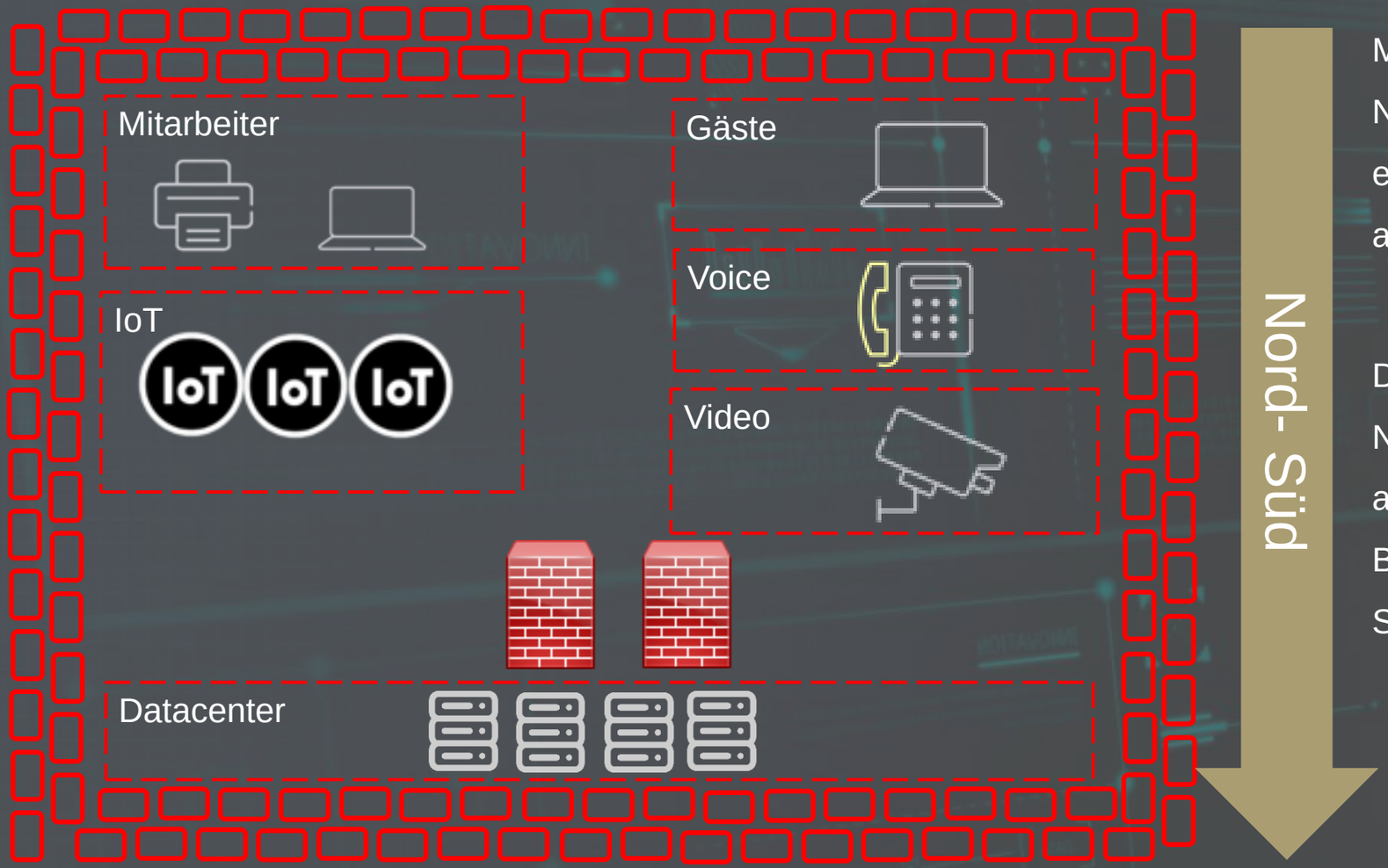
	Internet access	Internet restricted	E-Mail access	Access to Application Servers/Services (Zero Trust)	RDP to Admin-Jumphost	Management Access (RDP, SSH, HTTPS)	Access to special Admin-Fileserver
Workstations mit EDR	x		x	x			
Admin-WS mit EDR	x		x	x	x		x
Terminalserver	x		x	x			
Workstations ohne EDR		x		x			
Smartphones / Tablets	x		x	x			
Drucker				x			
IoT		x		x			
Gäste	x		x	x			
Admin Jump-Host						x	x
		x		x			
DMZ							
Server Tier 0 / Tier 1		x		x			



SEGMENTATION

MACRO SEGMENTATION

SEGMENTATION



Macro Segmentation bezieht sich auf die Teilung eines Netzwerks in **große**, logische Segmente, die jeweils mit eigenen Sicherheitsrichtlinien und Zugriffskontrollen ausgestattet sind.

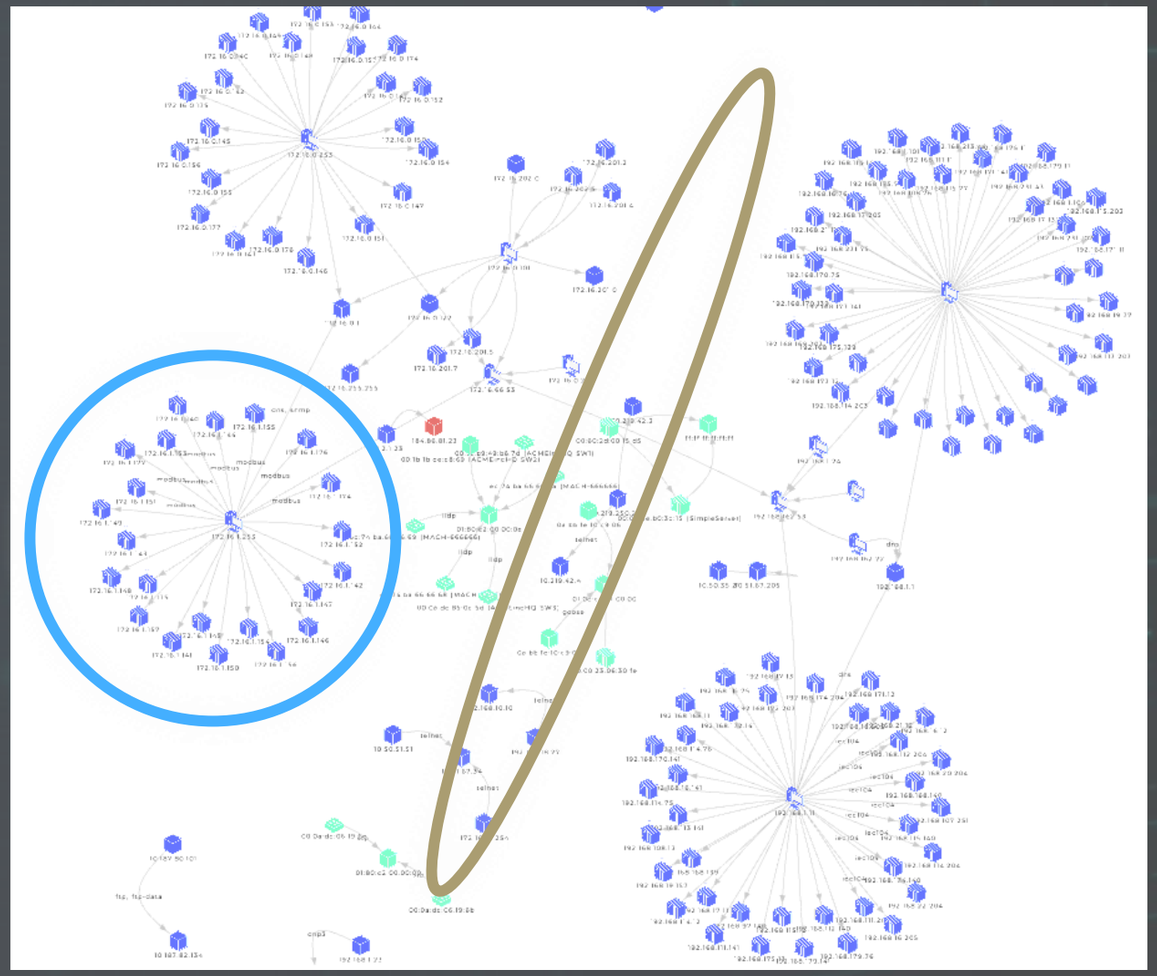
Das Ziel der Macro Segmentiation ist es, den Netzwerkzugriff mittels einer **Next Generation Firewall** auf ein Minimum zu beschränken, indem nur autorisierte Benutzer oder Anwendungen Zugang zu den jeweiligen Segmenten des Netzwerks haben.

MACRO SEGMENTATION

BEISPIEL

Netzwerk Graph SOLL

Darstellung eines optimalen Netzwerkaufbaus

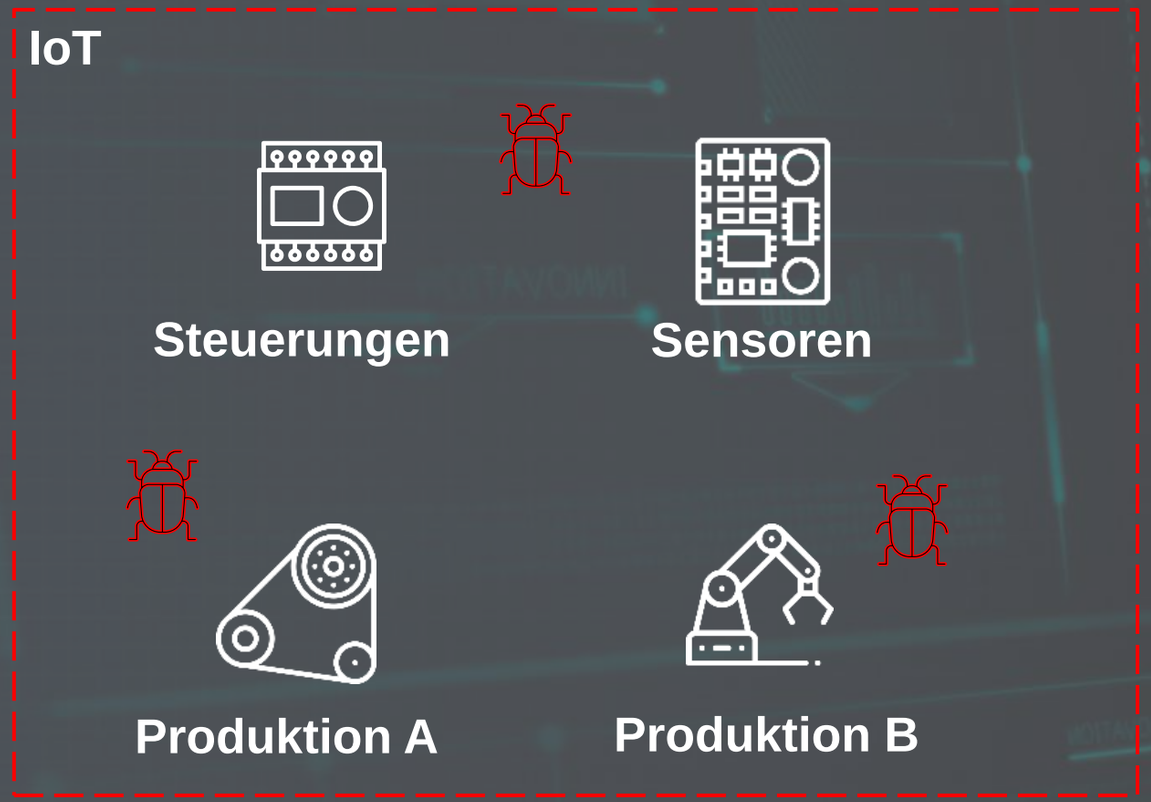


Definierte Übergänge zwischen IT und OT

Klar definierte Netzsegmente

GRENZEN DER MACRO SEGMENTATION

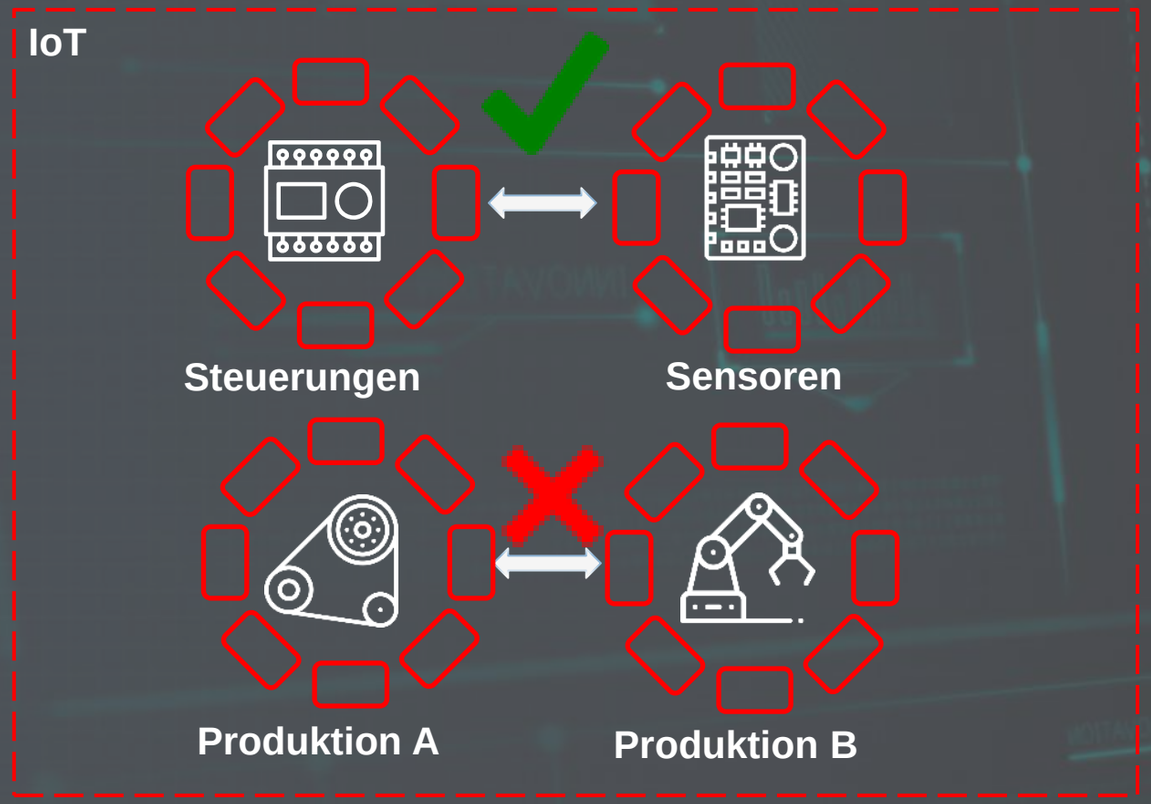
SEGMENTATION



- Kein Schutz innerhalb dem gleichen Segment
- Innerhalb von einem Segment können die Geräte frei kommunizieren
- Keine Unterscheidung von Zugriffsberechtigungen
- Wenn eine Malware ein System infiziert hat, breitet sich die Bedrohung im ganzen Segment aus
- Konfiguration am Switch um den Port in das richtige Segment zu hinterlegen
- Änderungen von Segmenten wirken sich auf die IP-Adresse von dem Gerät aus

MICRO SEGMENTATION

SEGMENTATION

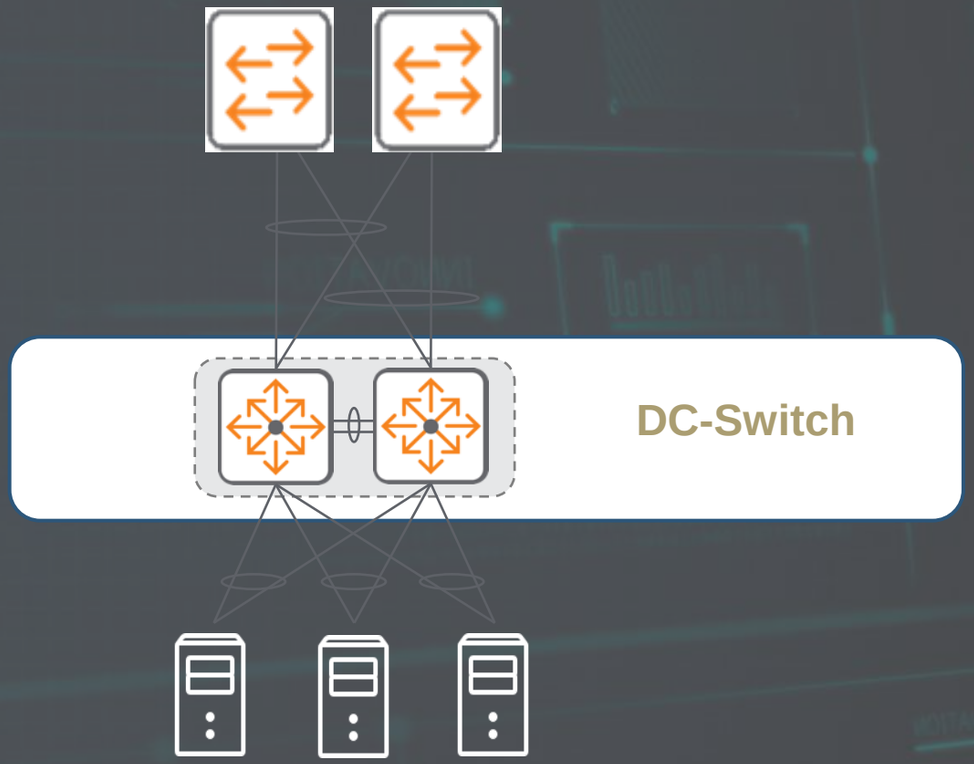


- Unterteilung in **kleine und isolierte** Segmente um die Angriffsfläche zu reduzieren
- Segment basiert auf ein Rollenkozept
- Kein „Implicit Trust“
- Ohne Genehmigung können Segmente nicht miteinander kommunizieren
- Jede Kommunikation zwischen den Segmenten wird durch eine Firewall mit IDS und IPS überwacht


BIS ZU 70 % DES DATENVERKEHRS IM NETZWERK BLEIBT IM DATACENTER (OST-WEST)

SECURITY IM DATACENTER

HERAUSFORDERUNGEN



Hoher Datendurchsatz im DC-Bereich

Statischer IP-Bereich
Änderungen nur mit hohem Aufwand möglich

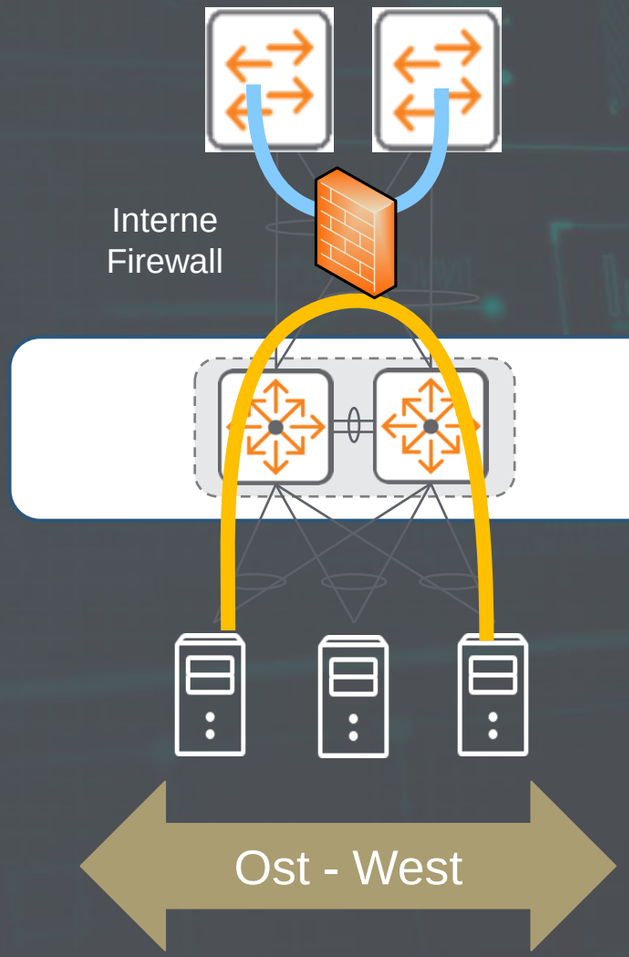
Einsatz von NAC nicht empfohlen

Visualisierung durch Endpoint-Security

Segmentierung ?

MICRO-SEGMENTIERUNG IM DATACENTER

BEISPIEL INTERNE FIREWALL



Campus Infrastruktur

Nord - Süd

- Traffic der Clients wird über die interne Firewall segmentiert
- Zugriffe von Client – Datacenter laufen über die interne Firewall
- Dedizierte Servernetze werden über die interne Firewall gerouted

Datacenter Infrastruktur

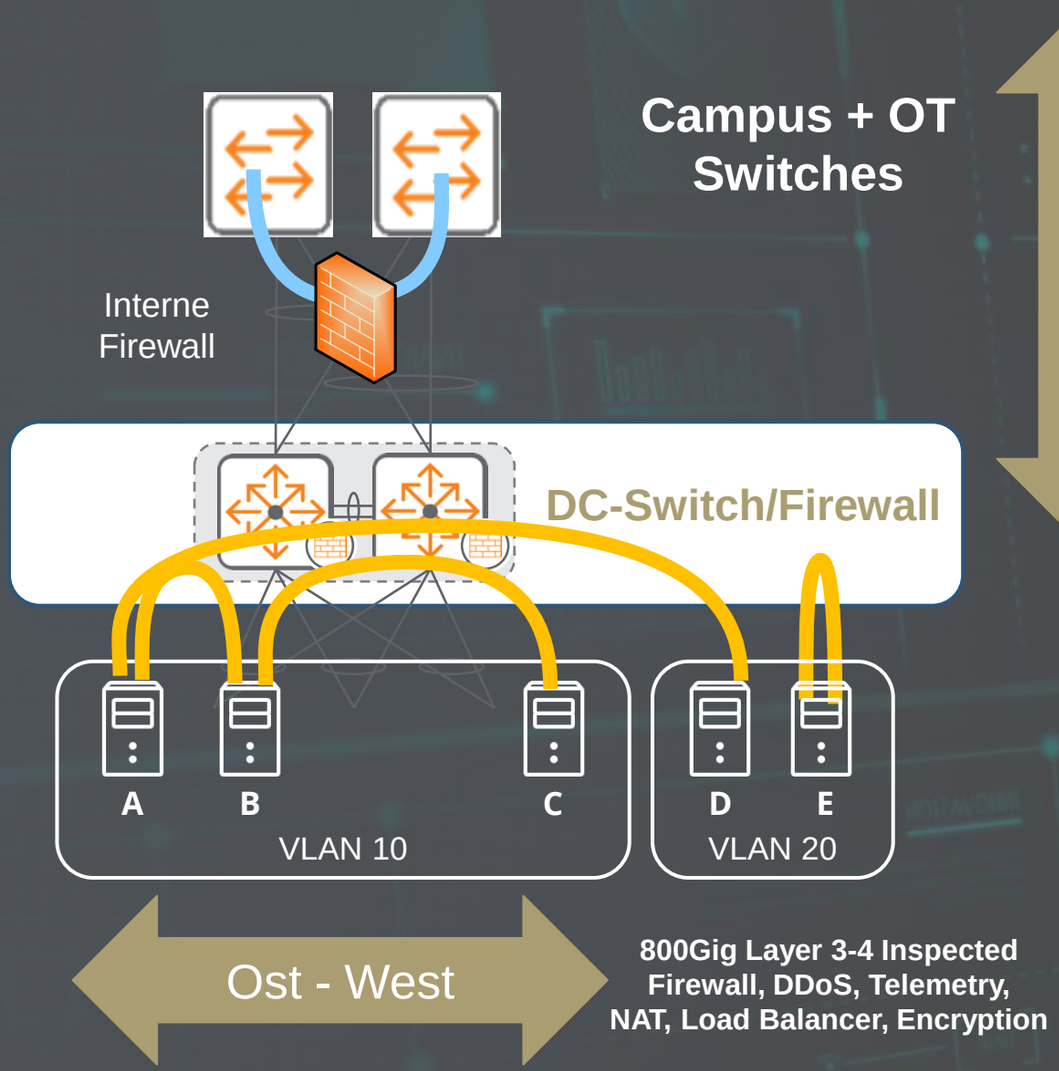
Tier 0	Tier 1
Domaincontroller	Appl.-Server
Exchange	Jump-Hosts
	Management
Lateral Movement	

Herausforderungen:

- Auflösen von Layer 3 Trennung Campus/Datacenter
- Mehr Performance auf Firewall durch OST → West traffic
- Anpassungen an IP-Konzept notwendig!
- Hoher Dienstleistungsanteil

MICRO-SEGMENTIERUNG IM DATACENTER

BEISPIEL INTERNE FIREWALL IM DATACENTER SWITCH INTEGRIERT



- Traffic der Clients wird über die interne Firewall segmentiert
- Zugriffe von Client – Datacenter laufen über die interne Firewall
- Alle Servernetze werden über die Datacenter-Firewall geroutet (PSM)

Mehrwerte:

- Ost → West Visibility
- Soft Migration
- Inter-VLAN und Intra-VLAN Segmentierung
- Deutlich geringerer Dienstleistungsanteil

ZERO TRUST

NETWORK ZUSAMMENFASSUNG

ZERO TRUST

ARCHITEKTUR GRUNDSÄTZE

Alle Datenquellen, Rechendienste und Geräte werden als Ressourcen betrachtet.

Kommunikation ist unabhängig vom Standort

Der Zugriff auf Ressourcen wird pro Sitzung gewährt

Der Zugriff auf Ressourcen wird durch eine dynamische Richtlinie bestimmt

Die Integrität und die Sicherheitslage aller eigenen und zugehörigen Ressourcen muss überwacht werden.

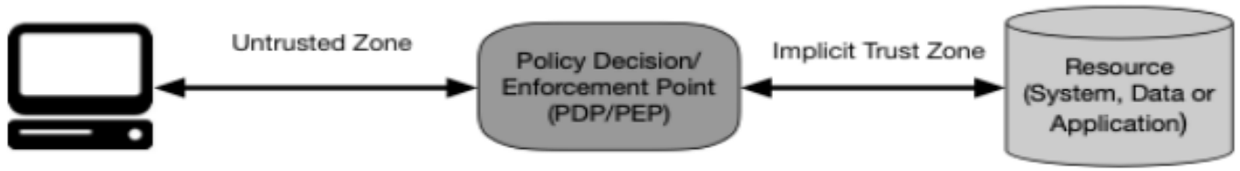


Figure 1: Zero Trust Access

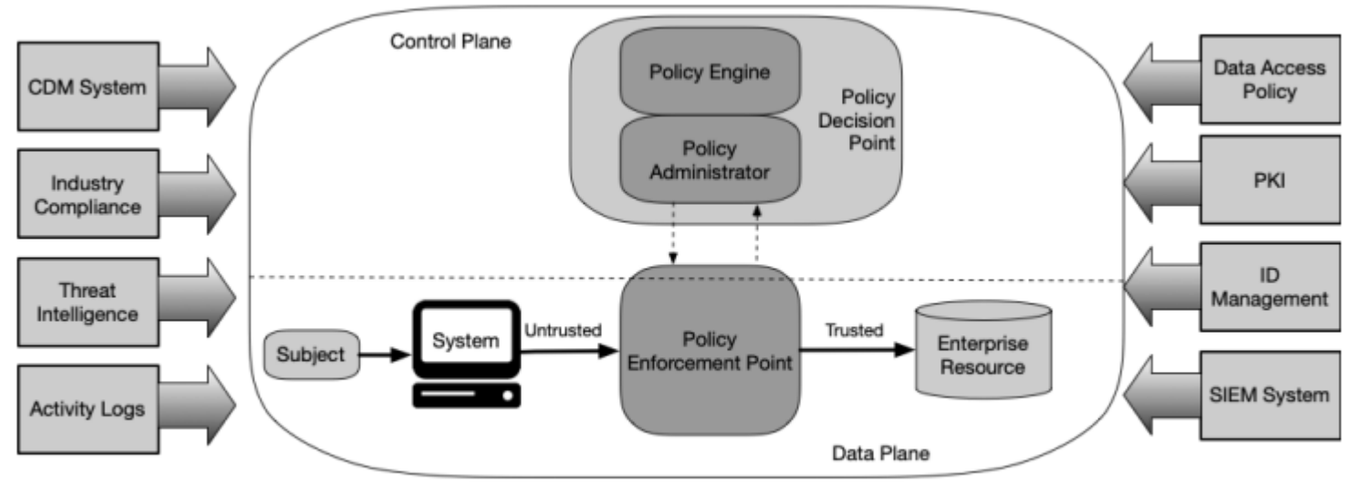


Figure 2: Core Zero Trust Logical Components

Authentifizierung und Autorisierung werden streng erzwungen, bevor der Zugriff erlaubt wird, und können Änderungen unterliegen.

Eine Organisation muss so viele Informationen wie möglich über den aktuellen Zustand ihrer Anlagen, Netzwerkinfrastruktur, Kommunikation, Endbenutzer und Geräte sammeln, um ihre Sicherheitslage zu verbessern. Nur mit diesen Erkenntnissen können Richtlinien erstellt, durchgesetzt und verbessert werden.

Quelle:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
https://www.csoonline.com/de/a/was-ist-eine-zero-trust-network-architecture

ZERO TRUST

ARCHITEKTUR UMSETZUNG

Identifizieren Sie die Ressourcen, die geschützt werden müssen

Zeichnen Sie die Transaktionsflüsse für diese Ressourcen auf

Bauen Sie die Architektur auf

Erstellen Sie eine Zero-Trust-Richtlinie, die Benutzerrollen, Berechtigungen und die Art der Authentifizierung festlegt

Überwachen und pflegen Sie das System und nehmen Sie bei Bedarf Änderungen und Verbesserungen vor.

Quelle:
https://www.csoonline.com/de/a/was-ist-eine-zero-trust-network-architecture

ZERO TRUST

NETWORK

NAC

OT-Monitoring

Endpoint-Security

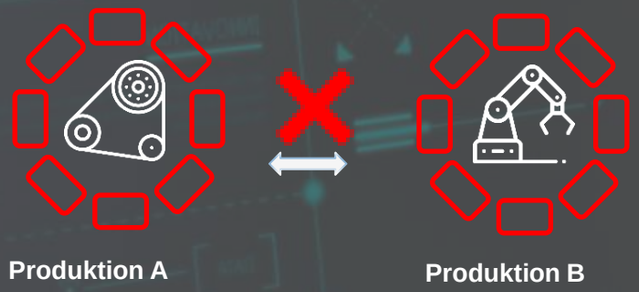
Risk

Initial Access
Lateral-Movement

Kommunikation
Macro Segmentation
Micro Segmentation

Visibility → **Classification** → **Segmentation**

Reifegrad 1	Reifegrad 2	Reifegrad 3
Netzwerk-Zugriff: Authentifizierung	Geregelte Kommunikation: Autorisierung	Monitoring/Anomalie Erkennung



ZERO TRUST

KEY TAKEAWAYS

Wir können nur schützen was wir sehen

Schutz und Risiko müssen in die Segmentierung einbezogen werden

Kommunikation nur unter Kontrolle → Macro Segmentation

Micro Segmentation schützt vor Ausbreitung…

…und ermöglicht eine schnelle Angriffserkennung

ZERO TRUST

AUSBLICK

Online-Seminar Devices

SOC	Vulnerability Management	Event Management	Incident Response	Visibillity and Analytics Automation and Orchestration
Identity	Multi Faktor Authentification	Network Access	Cloud Access	Authentication Identity Stores
Device	Visibility	Classification	Endpoint Protection	Asset Management Data Access
Network / Environment	Network Topology	Macro Segmentation	Micro Segmentation	Network Segmentation Threat Protection
	Building Access Control	Building Segmentation	Physical Security Management	
Application	Secure Web Gateway	Secure Mail Gateway	Code Security	Threat Protection Application Security
Data	Graduierung	Encryption	Secure Backup	Encryption Access Determination
ISMS	Information Security	Privacy	Employee Awareness	Governance

ZERO TRUST

UMFRAGE

Nutzen Sie ein NAC System?

Ja: 43% Nein: 16% keine Antwort: 41%

Nutzen Sie ein OT-Monitoring System?

Ja: Nein: keine Antwort:

Klassifizieren Sie Ihre Assets auf Basis einer Risikobewertung?

Ja: 15% Nein: 25% keine Antwort: 60%


SCALTEL
SCALTEL
SMART BUILDING
SCALTEL
SNS SYSTEMS
SCALCOM
ZUFRIEDENE
KUNDEN STEHEN
IM MITTELPUNKT