IKARUS security software

NOZOMI NETWORKS MSSP of the Year 2024 IKARUS security software

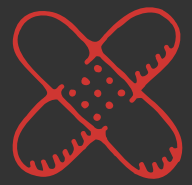
NOZOMI NETWORKS

OT-Security

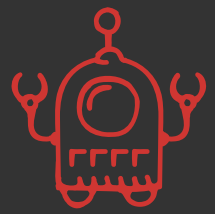
Warum unser Denken gefährlicher ist als jede Schwachstelle?

Herbert Dirnberger

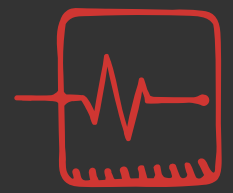
In 30 Minuten: 6 Erkenntnisse für Ihre Sicherheit



Warum Denkfehler gefährlicher sind als fehlende Patches



Warum OT ≠ IT ist – gleiche Ziele, aber andere Spielregeln



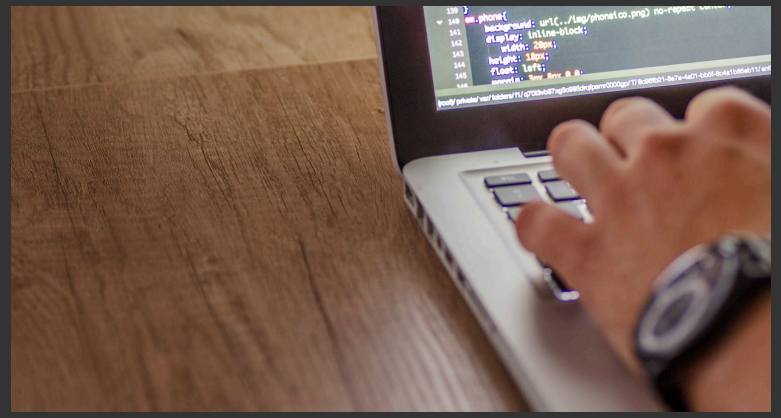
Warum Legacy ein Risiko ist, aber kein Schicksal

Welche Metriken wirklich zählen – und nicht lügen

Warum Segmentierung & Monitoring den Tool-Zoo schlagen

Wie Resilienz durch geübte Wiederanläufe entsteht

IT, IoT, OT – Drei Welten. Drei Risiken. Ein Ziel.



💻 IT – Die Welt der Daten

- Entwickelt für **Vertraulichkeit und Geschwindigkeit**
- Nutzt KI, Cloud, Edge Skalierbar, innovationsgetrieben
- **Aber:** keine Rolle für Safety, keine physische Resilienz
- 🎯 IT schützt Daten. Nicht Maschinen.

🌐 IoT – Die Welt der Verbindung

- Verbindet IT und OT mit Echtzeitdaten
- Optimiert Prozesse, erhöht Effizienz
- Brücke – aber auch **Einfallstor für Angriffe** Anfällig, weil oft **ungeschützt & breit verteilt**
- 🎯 IoT verbindet – und öffnet zugleich neue Angriffsflächen.

⚙️ OT – Die Welt der physischen Kontrolle

- Steuert Maschinen, Prozesse, Anlagen – **in Echtzeit**
- Fokus: **Safety, Resilienz, Verfügbarkeit**
- Basierend auf **Legacy-Systemen** – schwer patchbar, aber unverzichtbar
- Kritisch für Strom, Wasser, Verkehr
- 🎯 OT hält die Welt am Laufen – auch dann, wenn alles andere offline ist.


Ist die Anlage von folgenden bekannten Schwachstellen betroffen?
URGENT-11
RIPPLE20
BadAlloc
CVE-2024-21762
...
Koan Stress – unsre Ånlog is so oid, de Schwachstöhn gibt’s bei uns eh ned.
DENK-

#1 Air-Gap

Nicht glauben – verifizieren: isolieren, kontrolliert koppeln, dauerhaft überwachen.

"Air-Gap = sicher"

- Verdeckte Brücken (VPN/USB/WLAN/Cloud) bleiben unbemerkt
- Vermeintliche Isolation wird durch Engineering-Laptops und externe Modems aufgehoben.
- "Air-Gap" selten verifiziert

"IT/OT zusammen + Endpoint + NDR genügt"

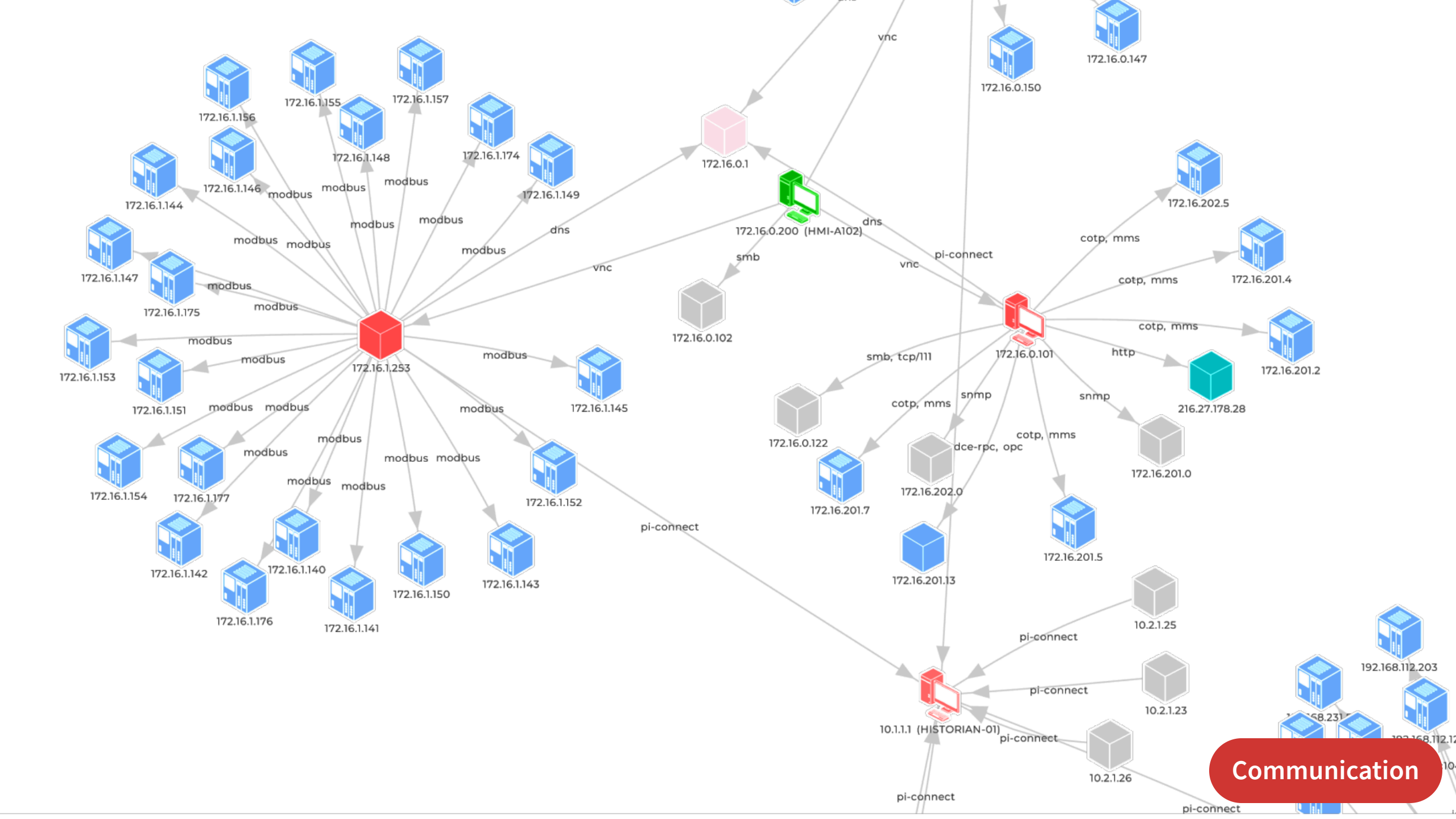
- OT != IT/IoT (Safety, Echtzeit, Legacy begrenzen Kontrollen)
- NDR/NTA sieht viel, stoppt aber nichts ohne harte Perimeter

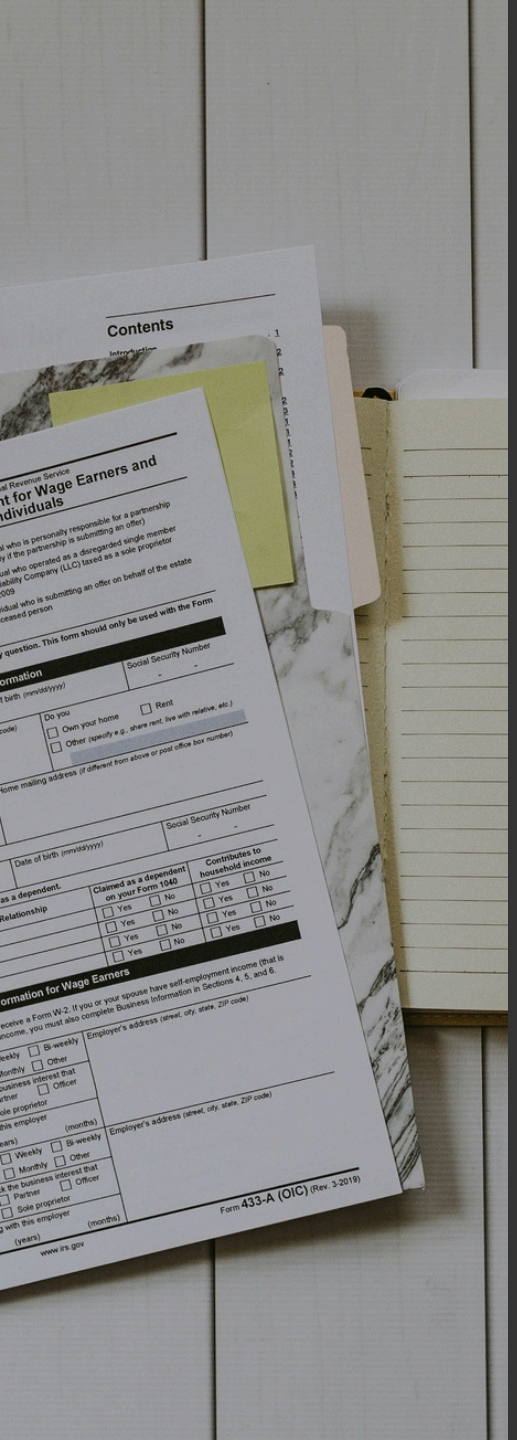
"DMZ = automatisch sicher"

- Falsche Trusts/Bypässe, Dual-Homing, unklare Datenfluesse
- Ohne Nachweise bleibt die DMZ nur "Checkbox"

IUEG: isoliert, überwacht, getrennt, entkoppelt

- Internet-Entkopplung in OT
- Zonen/Conduits (IEC 62443), deny-all/permit-by-exception auf Zellenebene
- IT/OT-DMZ + Remote-Access-DMZ (Jump-Server, Proxy, Recording)
- Data Diodes OT->IT; Mikrosegmente fuer High-Criticality
- PAM/MFA/JIT; keine IT<->OT-Trusts; strikte Sprungserver-Pflicht
- **Passives OT-NDR/NTA + zentrales Logging**
- Pull-the-Plug-Drills & USB-Canary-Tests


172.16.1.156
172.16.1.155
172.16.1.157
172.16.1.148
172.16.1.174
172.16.1.146
172.16.1.144
172.16.1.149
172.16.1.147
172.16.1.175
172.16.1.153
172.16.1.151
172.16.1.253
172.16.1.145
172.16.1.154
172.16.1.177
172.16.1.152
172.16.1.142
172.16.1.140
172.16.1.150
172.16.1.143
172.16.1.176
172.16.1.141
172.16.0.1
172.16.0.200 (HMI-A102)
172.16.0.102
172.16.0.150
172.16.0.147
172.16.202.5
172.16.201.4
172.16.0.101
172.16.201.2
216.27.178.28
172.16.0.122
172.16.201.7
172.16.202.0
172.16.201.0
172.16.201.5
172.16.201.13
10.2.1.25
10.2.1.23
10.1.1.1 (HISTORIAN-01)
10.2.1.26
192.168.112.203
modbus
dns
vnc
smb
pi-connect
cotp, mms
smb, tcp/111
http
snmp
dce-rpc, opc
Communication



#2 Compliance ≠ Sicherheit

ISO 27001/NIS Audits bestanden – Risiko unverändert: fehlende Mitigations, Legacy, keine Wirksamkeitsnachweise

„Audit-grün = sicher“

- geprüft wurden vor allem **Dokumente/Momentaufnahmen**, nicht die **Wirksamkeit**.
- **Scope-Lücken & Stichproben** lassen kritische OT/Legacy-Themen unberührt.
- Legacy?

Red Flags

- **Ungepatchte** Systeme ohne **kompensierende Kontrollen** (Segmentierung/Allowlisting/IPS).
- **Remote-Zugänge** ohne MFA/Jump-Host/Session-Logs.

Audits unterstützt die **OT-Sicherheit** proaktiv

- **Sichtbarkeit schaffen:** Prüfen, ob **Asset-Inventar** und **Netz-Flows** vollständig sind (was ist wo, wer spricht mit wem?).
- **Governance klären:** Rollen, Freigaben, **Wartungsfenster** und Notfallprozesse verankern.
- **Risiken priorisieren:** Legacy/Unpatchbares, **Remote-Zugänge**, schwache Segmentierung werden sichtbar und gewichtet.
- **Evidenz einfordern:** Belege für **Segmentierungs-Tests**, **Restore-Drills** (RTO/RPO) und **Alarm-Response** (MTTD/MTTR).
- **Verbesserungen treiben: CAPA-Plan** (Maßnahmen, Verantwortliche, Fristen, Enddatum für Ausnahmen).
- **Lieferkette absichern:** Nachweise zu **MFA/Jump-Host/Logs** bei Dienstleistern und Wartungspartnern.

ACMEincHQ_SW1

IP	192.168.1.3	**MAC address (2)**	00:16:b9:49:b6:40, 00:16:b9:49:b6:7d
Roles:	other	**MAC vendor**	Hewlett Packard
Product name	ProCurve 2626 Switch	**Vendor**	Hewlett Packard
Type	Switch	**Firmware version**	h.10.38
Product lifecycle status	End of support		
End of sale:	2009-02-01		
End of support:	2014-02-01		

Overview | Sessions 193 active | Alerts 0 high · 0 med. | Software 0 installed | Vulnerabilities 0 high · 0 med. | Variables 0 entries

Focus on 00:16:b9:49:b6:40

Network Stats

Focused on: 00:16:b9:49:b6:40

		Retransmission	Links
Received	25.3 KB		
Sent	188.0 B	0.000%	1
First seen	2017-02-16 13:57		
Last seen	2017-02-16 13:57	0.0 B in last 30'	active

Network Location

Focused on: 00:16:b9:49:b6:40

Zone	Subnet	VLAN
Layer2	-	-

Properties

No properties to display

Protocols

Focused on: 00:16:b9:49:b6:40

Protocol	Last activity	Inbound	Outbound
other	2017-02-16 13:57	-	-

Learning status

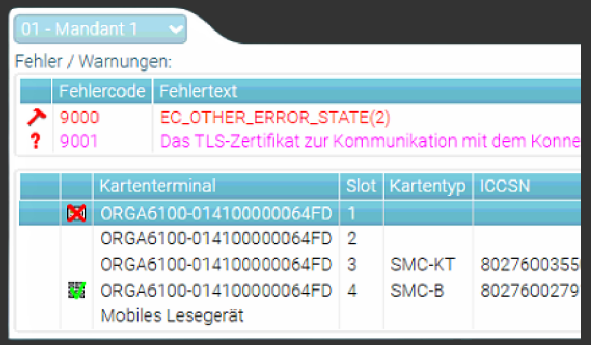
Node is fully

Asset intelligence

Legacy

#3 Kein Vorfall = kein Risiko

Vorfallsfreiheit beweist nichts, - **Risiko bleibt** (Hazard × Vulnerabilität × Exposition × Auswirkung).



Wahrnehmung

- **Normalcy Bias:** Lange Ruhe = „Normalzustand“
- **Availability Heuristic:** Schwer vorstellbar = „unwahrscheinlich“
- **Confirmation Bias:** Nur bestätigende Hinweise zählen
- **Outcome Bias:** Gutes Ergebnis = „gute Entscheidung“
- **Risk Homeostasis:** Gefühlte Sicherheit → riskanteres Verhalten

Datenlücken

- **Sampling-/Messlücken:** Keine Erkennung/Logs → falsche Null
- **Unterreporting:** „Niemand meldet“ ≠ „nichts passiert“

Denkfehler

- **Abwesenheit von Evidenz ≠ Evidenz der Abwesenheit**
- **Survivorship Bias:** Nur die „überlebten“ Tage sichtbar
- **Basisraten-Ignoranz:** Grundwahrscheinlichkeiten ignoriert
- **Regressionsirrtum / Lucky Streak:** Glück als Trend gedeutet

„**Keine Vorfälle** zeigen nur, dass wir **Glück oder wirksame Kontrollen** hatten – **nicht**, dass kein Risiko existiert.“

3

Alert Process time issue [812429bd-ff82-41c7-9da3-63a8975d7d3e]

...

What happened

The time notified in the ASDU (2001/01/06-22:06:02) is inconsistent with the packet time.

Possible cause

The time stamp specified in process data is not aligned with current time. There could be a time sync issue with the source device, a malfunctioning or a packet injection.

Suggested solution

Verify the device configuration and status.

Source

Zone	Undefined
Label	n.a.
IP	192.168.1.11
MAC	18:66:da:00:01:11
Port	36037
Roles	consumer, web_server
Types	computer
Users	0

Communication

Protocol	iec104
Transport protocol	tcp

Destination

Zone	Undefined
Label	plc098.ACME0.corporationnet.com
IP	192.168.168.140
MAC	00:00:23:a8:a8:8c
Port	2404
Roles	producer
Types	OT_device
Users	0

Environment | Audit alert operations

Nodes currently involved

?

Selection info

192.168.1.11

› appliance host: guardian04

Alerts

#4 Der „Unsere-Leute“ (Irrtum)

Vertrauen mit System, nicht aus Gewohnheit

People (Menschen & Können)

- **Denkfehler:** „Unsere Leute schaffen das allein.“
- **Was passiert:** Man fragt zu spät um Hilfe, hält an Gewohnheiten fest, übersieht Risiken.
- **Beispiele:** Gemeinsame Passwörter, Alarme stumm schalten „nur kurz“, Änderungen ohne Zweitsicht.
- unreflektierte Betreibsroutine

System (Abläufe & Regeln)

- **Denkfehler:** „Prozesse bremsen nur.“
- **Was passiert:** Änderungen ad hoc, schlechte Doku, Ausnahmen ohne Enddatum, unsichere Fernzugriffe.
- **Beispiele:** Keine vollständige Geräteliste, flaches Netzwerk, Backups nie getestet.

besser

- Mentoring
- 4-Augen-Prinzip
- externe Zweitmeinung bei heiklen Aufgaben
- Checkliste + Rollback-Plan
- „Stop-the-Line“ bei Bypässen
- Segmentierung (IT/DMZ/OT)
- Rollen statt Shared-Accounts, Sprungserver mit Aufzeichnung
- regelmäßige **Restore-Tests** mit Protokoll
- Ausnahmen max. 90 Tage.

9

Incident Eng operations [55f0cb29-b8fc-47a0-b07b-659fd82f0a2b]

...

What happened

Eng operations made on device 192.168.10.17 issued by host 192.168.20.12

Possible cause

Various operations to modify the configuration, the program, or the status of a device have been detected.

Suggested solution

Validate the engineering operations.

Source

Zone	192.168.20.0/24
Label	EWS.ics.lab
IP	192.168.20.12
MAC	18:a9:05:24:d8:b5
Port	n.a.
Roles	consumer, engineering_station
Types	-
Users	0

Communication

Protocol	ethernetip
Transport protocol	unknown

Destination

Zone	Undefined
Label	n.a.
IP	192.168.10.17
MAC	00:00:bc:5e:ec:e4
Port	n.a.
Roles	producer
Types	controller
Users	0

Alerts

Page 1 of 1, 3 entries

Show all alerts | Export | Live

Actions	Risk	Time	ID	Type ID	Description	Proto...			
...	6	13:51:29.210	e3518532	SIGN:OT_DEVICE-START	OT device START issued to device 192.168.1...	ethe...			
...	6	13:51:29.200	68e8d82d..	SIGN:PROGRAM:TRANSFER	Program transfer from device 192.168.20.12...	etherne...			
...	9	13:51:29.197	6f3cb5f9	SIGN:OT_DEVICE-STOP	OT device STOP issued to device 192.168.10...	ethernet...	192.168.20.12	192.168.10.17	2927

Echtzeit-Warnungen zu verdächtigen Aktivitäten und Bedrohungen in OT-Netzwerken

#5 (No) Patch-as-Religion

vom No-Patch zur Über-Patch-Panik

No-Patch / Paralyse

- Air-gap/Proprietär schützt uns
- OEM verbietet Patch = Hände gebunden
- Ausnahme ersetzt Patch

Riskwashing

- Excel statt Umsetzung
- Virtual Patch reicht dauerhaft
- Exposure = nur Internet
- Kein Testbed ⇒ keine Changes

Patch-Reflex

- **CVSS = Priorität**
- Alles sofort patchen
- Patch = Security
- Zero-Day-Panik
- IT=OT
- Patch Tuesday & Scanner 1:1 in OT

Asset Illusion, One-Policy-fits-all, Big Bang Patchen, Rollbäck Märchen, Versions-Tunnelblick, Scan-Unbedenklichkeit, Agent-überall

...

OT-„Mega-GAUs

Das Einfallstor ist selten eine einzelne, nicht gepatchte OT-CVE, sondern ..... Entscheidungen, Annahmen

Stuxnet 2010

- „Air-Gap ist sicher“
- USB/Wechselmedien ignoriert.

Deutsches Stahlwerk 2014

- IT ↔ OT nicht strikt getrennt
- Phishing auf IT sei „kein OT-Risiko“

BlackEnergy/KillDisk 2015

- Vertrauen in legitimen Remote-Zugang
- Air Gap im Kopf

CrashOverride/Industroyer 2016

- IT/OT-Trennung und Protokoll-Sicht unterschätzt

TRITON/TRISIS 2017

- Safety-System ist unantastbar
- unzureichende Segmentierung/Engineering-Zugriffe

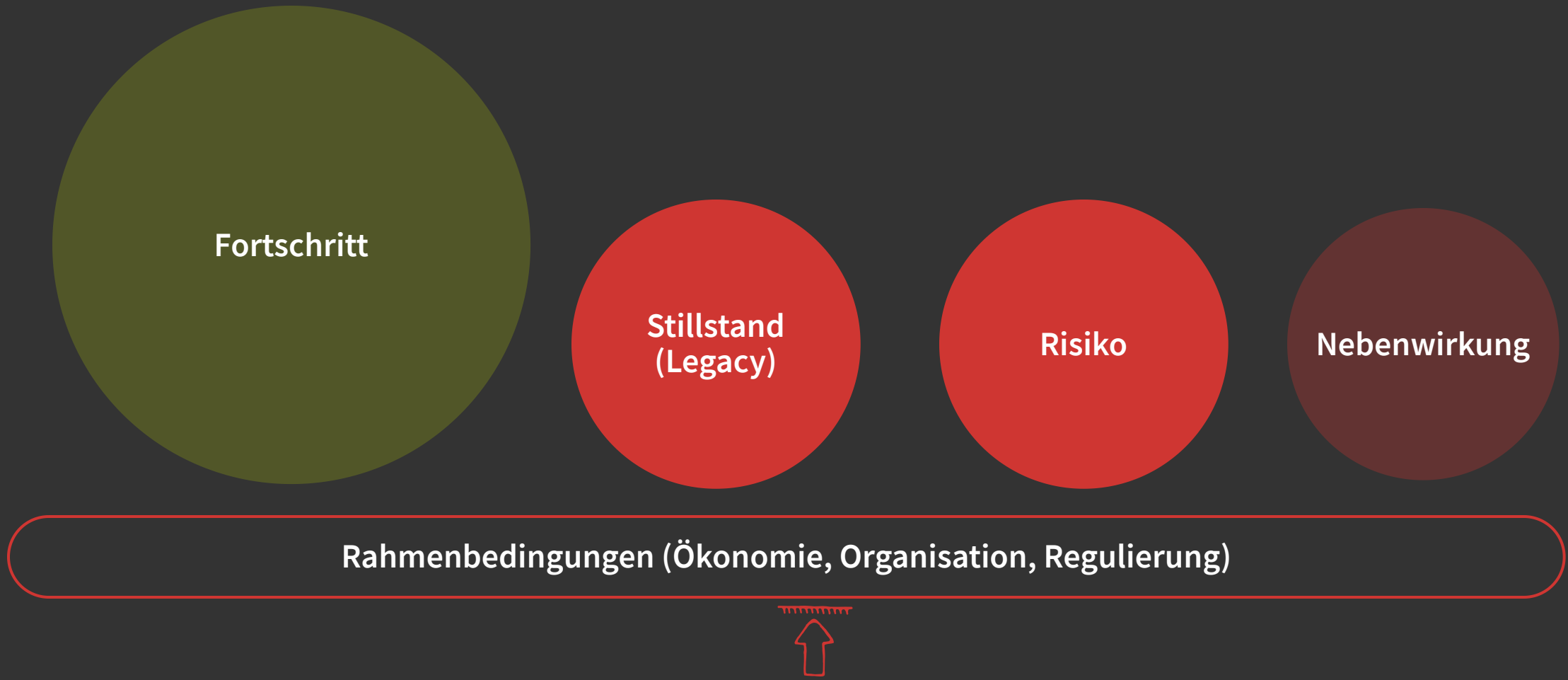
Oldsmar 2021
Colonial Pipeline 2021

- Fernzugriff mit gemeinsamem Passwort ohne MFA ist praktisch

Direkter IT-OT Zugriff ohne DMZ,Jumphosts/MFA, flache Netze, Any-Any, xxxViewer !!!


35 Jahre OT-Security?
"Früher? Do hot’s koane Security gebn.
Maschin muaß lafn, Punkt.
Alles war abg’schottet – des hot passt."
"Heute: Sichoheit muaß sei, sunst laft goa nix"
Werksleiter

Die Gleichung der Wahrheit (OT-Security)



OTSec(t) = Fortschritt (t) - Stillstand (t) - Risiko(t) - Nebenwirkung(t)
| Rahmenbedingungen

OT Security in Epochen

Wie sich Fortschritt, Stillstand, Risiko und Nebenwirkungen im Lauf der Zeit verschoben

Zeitraum	Fortschritt	Stillstand	Risiko	Nebenwirkung	Rahmenbedingungen (Öko/Reg/Org)
bis ~1975	•	•	•	•	Safety/Org stark, Cyber irrelevant
1975–1995	↑ (Automatisierung)	•	↑	•	Org: Security nicht vorgesehen
1995–2009	↑↑ (IT in OT)	↑ (Schulden)	↑↑	↑	Öko kostentreibend, Reg gering
2010–2014	↑ (ICS-Controls)	↑	↑↑	↑	Erste KRITIS-Regeln, Org erwacht
2015–2019	↑↑ (Architektur, 62443)	↑	↑	↑ (Tool-Zoo)	Reg/Standards zunehmen
2020–2022	↑ (Zero Trust, MFA)	↑	↑↑↑	↑↑	Öko volatil, Org unter Druck
2023–heute	↑↑↑ (Resilienz, All-Hazards)	↘️ (kompensiert)	hoch, **beherrschbar**	**balanciert**	Reg stark (NIS2), Org reift, Business-Alignment

Legacy

Journey

Legacy

Alt, kritisch, verwundbar – warum Legacy-OT uns alle betrifft

🔐 Cyber-Security

Diese Systeme wurden nie fürs Internet gebaut.

Sie sind offen – weil niemand je eine Firewall geplant hat.

🔄 Verfügbarkeit

Stillstand ist keine Option.
Aber: Patches können genauso gefährlich sein wie Angriffe.

⚙️ Resilienz

Ein Fehler kann in Sekunden ganze Prozesse kippen.

Es gibt keinen zweiten Versuch. Kein Zurück

💰 Ökonomie & Regulierung

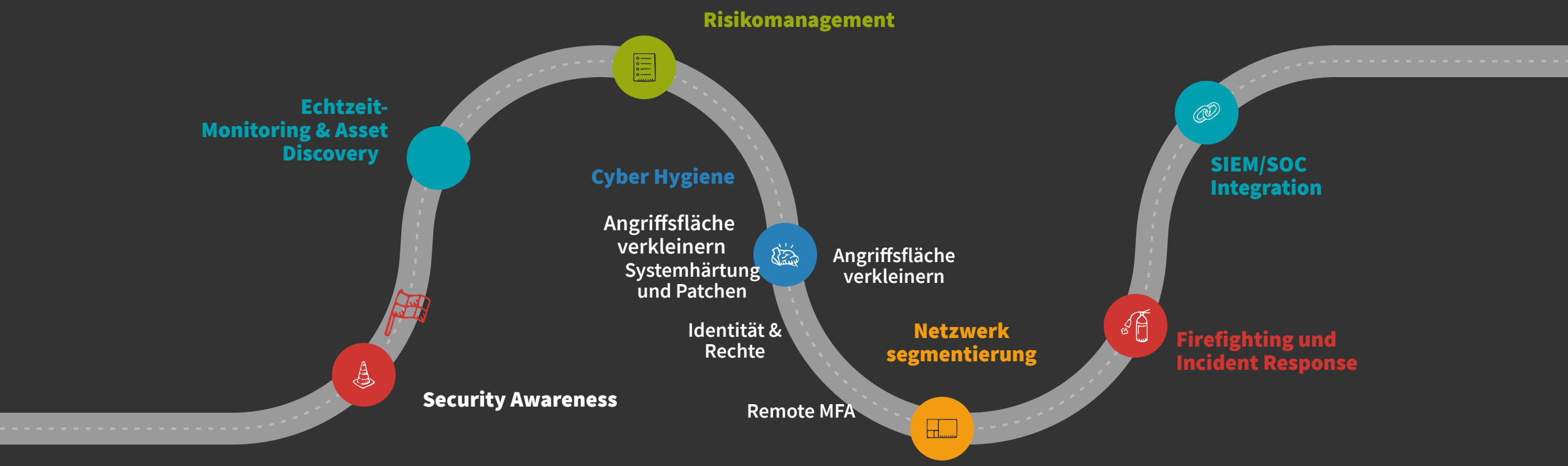
Ersetzen? Kaum leistbar.
Absichern? Pflicht – aber mit alten Mitteln gegen neue Bedrohungen.

„Legacy-OT ist das Rückgrat der Industrie.
Aber ohne Schutz wird genau dieses Rückgrat zum Schwachpunkt.“

Journey

IKARUS OT Security Journey

IT→OT-Angriffe stoppen wir nicht mit Technik allein – sondern mit einem strukturierten Sicherheitsweg.

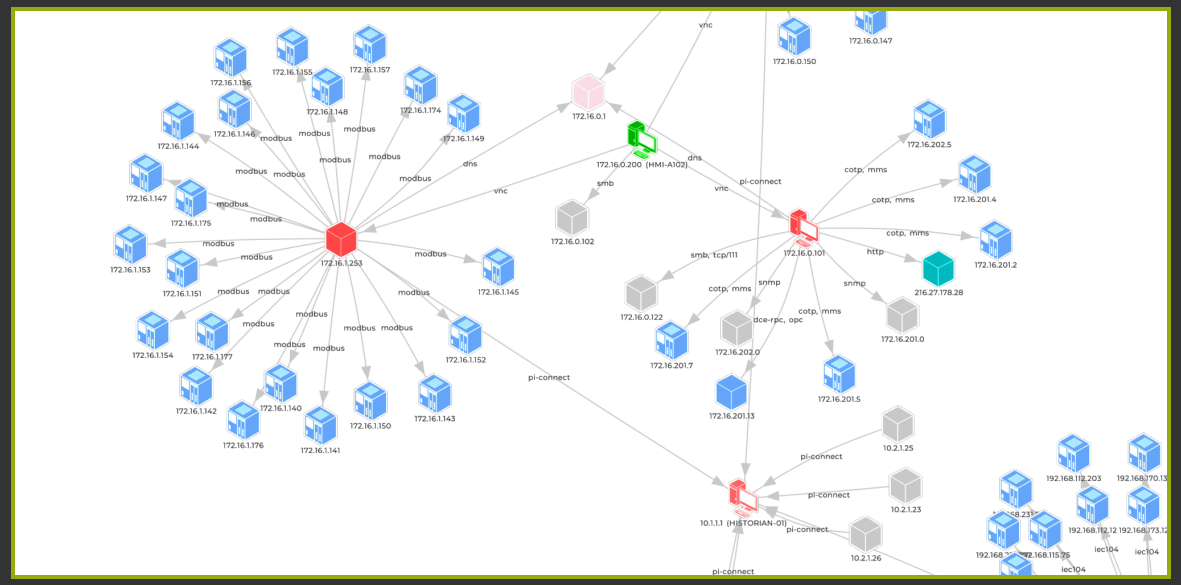


bei Greenfield + : **End-to-End Secure-by-Design**

Kontinuierliches, risikobasiertes Lifecycle-Management

Wohin geht die Reise bei IKARUS und Nozomi

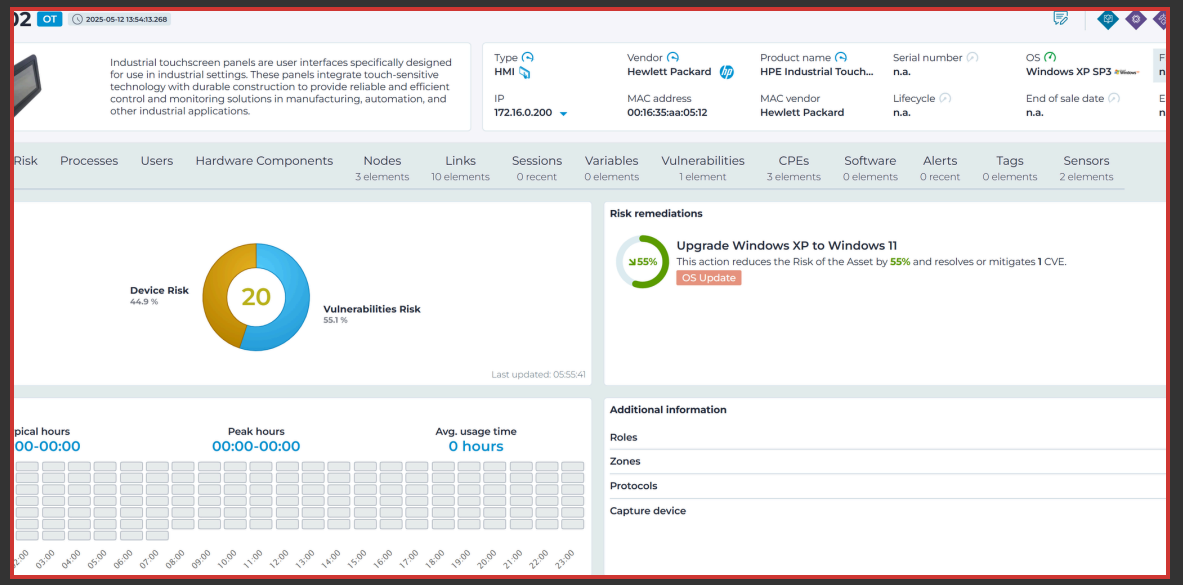
Risk Managment



Edge via Guardian

Läuft lokal. Erkennt Gefahren direkt vor Ort.
→ KI lernt mit Heuristik & unüberwachtem Lernen.
→ Erkennt Muster, die klassische Regeln übersehen

🔗 Beispiele: Cloud-trainierte Modelle liefern Bedrohungswissen.
Adaptive ML passt sich live an neue Angriffe an.



SaaS – ab Q1/2026

Egdge und Cloud-basierte Analyse, Priorisierung und Management.
→ KI bewertet Risiken, priorisiert Alarme automatisch.
→ Optional: Zeitreihen-Analysen, Asset Intelligence, Co-Pilot für Queries.
„Edge sichert lokal – Cloud sieht global."
Gemeinsam bilden sie ein lernendes, verteiltes Nervensystem.

Factsheet

Absicherung der Steuerungstechnik - OT Security 2025

Kleine digitale Ursachen erzeugen große physische Folgen.

Wir begrenzen **Eintritt**, **Ausbreitung** und **Erholungszeit**.

Warum jetzt? (All-Hazards nach NIS2)

- **Alle Ursachen zählen:** Fehler, Update, Lieferant, Manipulation, Angriffe, ...
- **Seitwärtseffekte aus Büro/Cloud-Systemen:** Identität/Namen/Zeit/Zertifikate als versteckte Single Points; Gebäude- & IoT-Systeme als Brücken.
- **Systemdynamik:** Enge Kopplung & Echtzeit ⇒ ein falsches Signal stoppt Linien oder verschiebt Grenzwerte.

80/20-Maßnahmen (betriebsschonend)

- **Trennen:** Zonen mit klaren Übergängen; nur Nötiges darf durch.
- **Zugänge steuern:** ein Einstiegspunkt, Mehrfaktor, zeitlich begrenzt, protokolliert.
- **Beobachten: passiv** und ereignisbezogen (z. B. Projekt-Downloads, neue Assets, Verbindungen, Warnungen etc.).
- **Schnell wieder anlaufen:** Offline-Backups, „Golden Images“, **regelmäßig testen**.
  (Resilienz = degradieren statt ausfallen • Betriebskontinuität = realistische RTO/RPO • Incident Response = klare Rollen & Übungen)

Geschäftlicher Nutzen

- **Weniger ungeplante Stopps & Ausschuss**
- **Sichere Betriebszustände** (Menschen/Umwelt)
- **Schnellere Erholung** nach Störungen
- **Prüfbare NIS2-Konformität & Versicherbarkeit**
- **Planbarkeit:** Ein Stillstandstag kostet meist mehr als ein Jahr Basis-Kontrollen

Management

- Verantwortliche & Budget bestätigen
- Lieferantenregeln mit Nachweisen (MFA, zentraler Einstieg, saubere Wartungsgeräte)
- **Üben & Messen** per KPI.

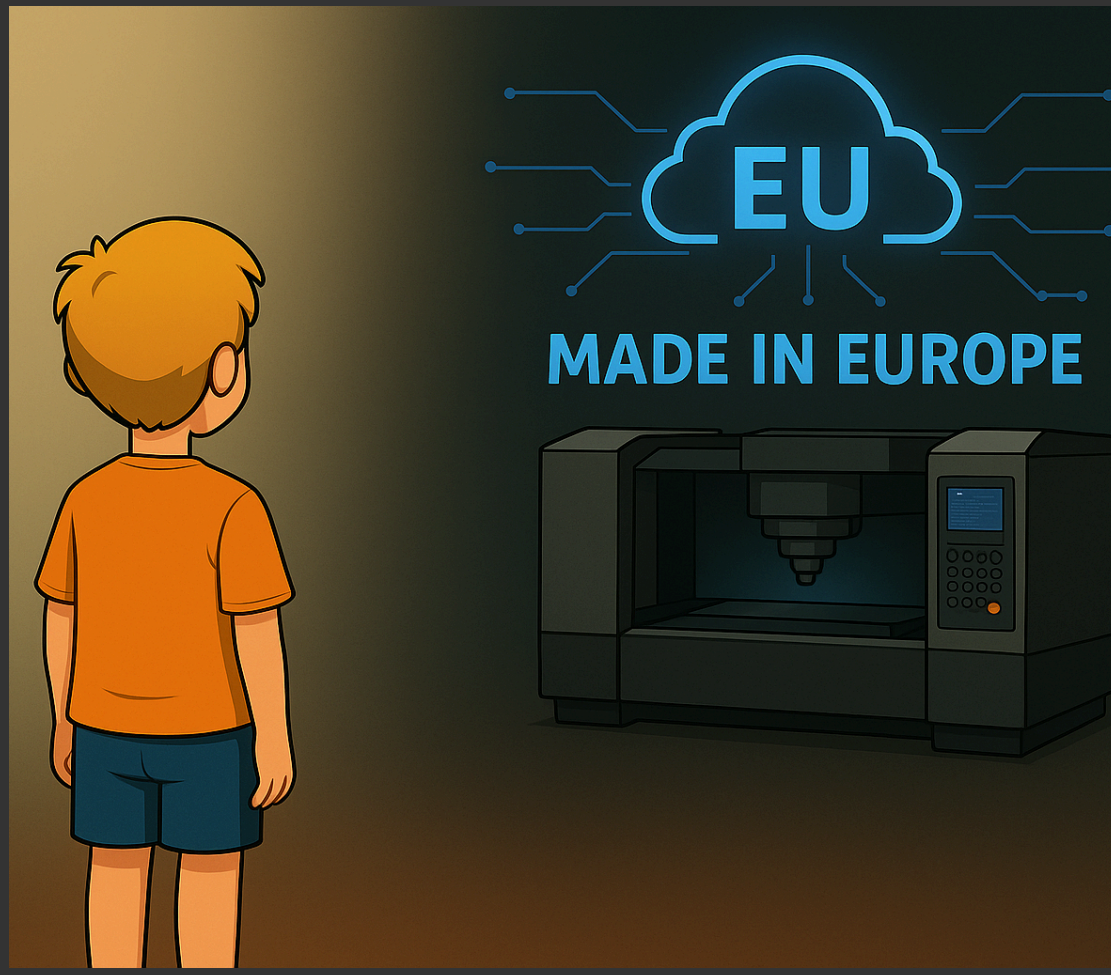
Fazit

+ Relativ leicht zu schützen weil sie statisch ist.

- Abhängigkeiten bleiben:, kein Null Risiko
- Umsetzung kostet Disziplin und Ressorucen
- Technische Schulden steigt mit den Alter der Anlagen

OT Security gelingt, wenn wir

- Denkfehler abbauen
- Risiken beherrschen
- Fortschritt messen und nutzen
- Nebenwirkungen balancieren
- Stillstand kompensieren
- Wirtschaft, Regulierung und Organisation einbeziehen




OT-Security!
Sicher ist, wer weiß wie’s geht.
„So pack ma’s o!“
DENK-