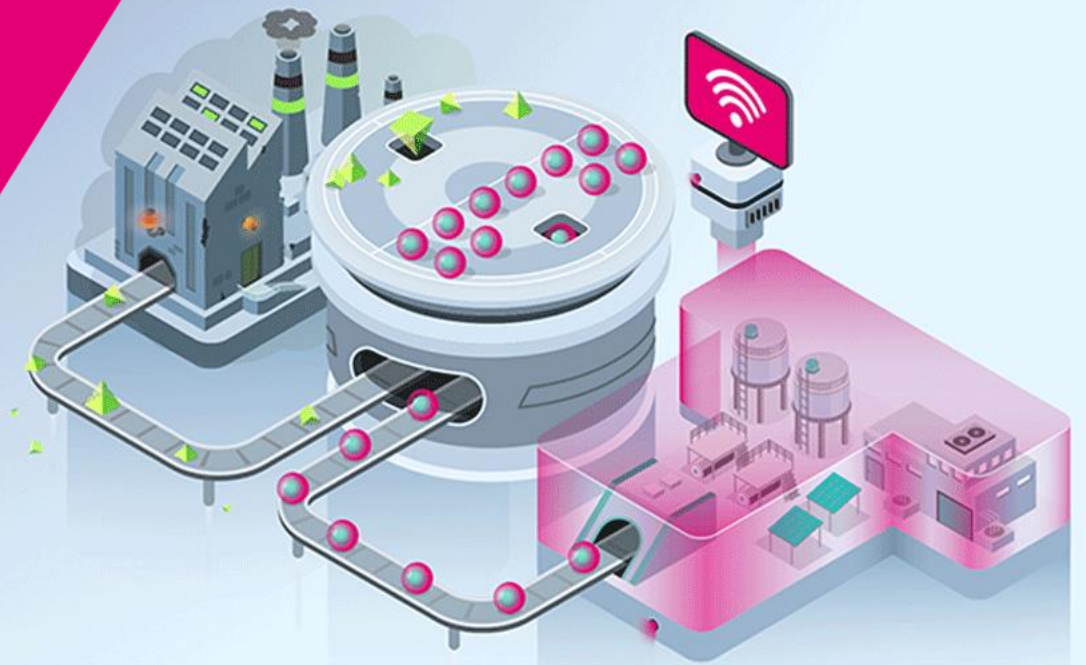
Die drei größten Bedrohungen für die IIoT effektiv und pragmatisch handhaben

(auch ohne AI ;-)

Bernd Jäger
bernd-jaeger@telekom.de
GRID, GCFA, GCIA, GREM, GWASP, CISSP
Practice Lead ICS/IoT Security

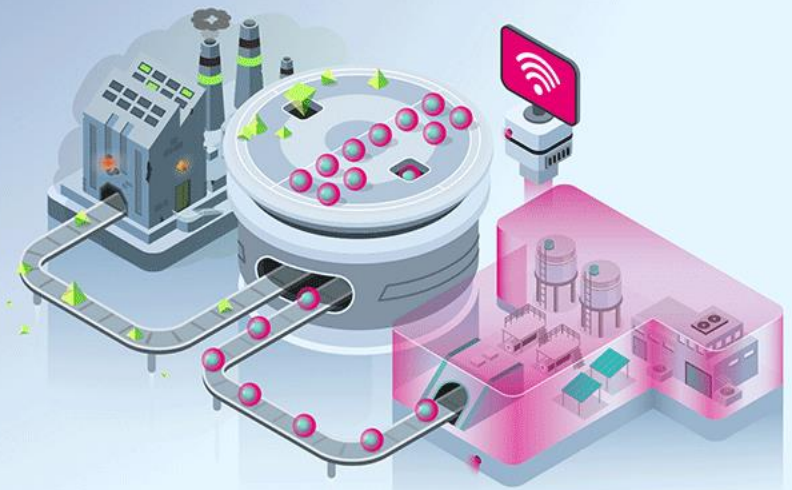


IoT Security

Top 3?

0. Your [redacted]
1. Ransomware
2. Remote Access
3. Suppy Chain

Quelle: Kunden- & Analyst Feedback, eigene Erfahrung (T-Sec. SOC/CERT)



1. Ransomware

Ransomware Business Case

Cybercrime Magazine: Global ransomware damage costs predicted to reach $250 billion USD by 2031.

https://cybersecurityventures.com/global-ransomware-damage

🌐 1. Tech-Giganten (Einzelunternehmen)

- **Apple**: Umsatz 2023 ca. **380 Mrd. USD**
  → Hauptumsätze aus iPhones, Services, Macs, iPads.
- **Amazon**: Umsatz 2023 ca. **570 Mrd. USD**
  → Kombination aus E-Commerce, Cloud (AWS), Werbung, Prime.
- **Microsoft**: Umsatz 2023 ca. **240 Mrd. USD**
  → Software (Windows, Office), Cloud (Azure), Gaming (Xbox).

🛢️ 2. Rohstoffe/Energie

- **Ölkonzerne wie Saudi Aramco, ExxonMobil, Shell**
  → Jahresumsätze oft über **250 Mrd. USD**, abhängig vom Ölpreis.

🚙 3. Automobilbranche (nach Unternehmen)

- **Volkswagen-Gruppe**: Umsatz 2023 ca. **330 Mrd. USD**
- **Toyota**: Umsatz 2023 ca. **275 Mrd. USD**
  → Hauptumsatz durch Fahrzeugverkauf, Teile & Finanzierung.

📱 2. Weltweiter Smartphone-Markt

Umsatz (2023): ca. 450–500 Mrd. USD

- Geräteverkauf, Zubehör, Reparaturdienste
- Apple und Samsung dominieren, aber viele weitere Anbieter beteiligt

💳 3. Kreditkarten- und Zahlungsdienstleistungen

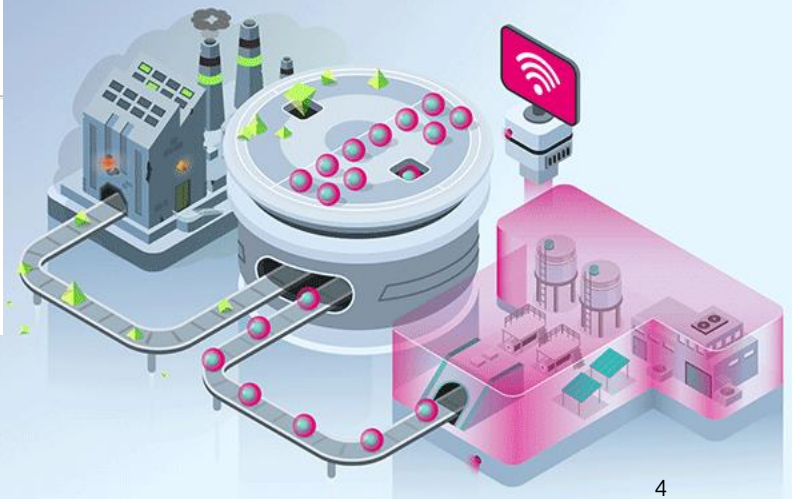
Globaler Umsatz (Kartenverarbeitung, Gebühren etc.): > 250 Mrd. USD

- Visa, Mastercard, American Express, Stripe, Adyen, PayPal
- Stark wachsend durch E-Commerce & Mobile Payments

🎮 4. Gaming-Industrie (inkl. Mobile & PC)

Weltweiter Umsatz (2023): ca. 250–300 Mrd. USD

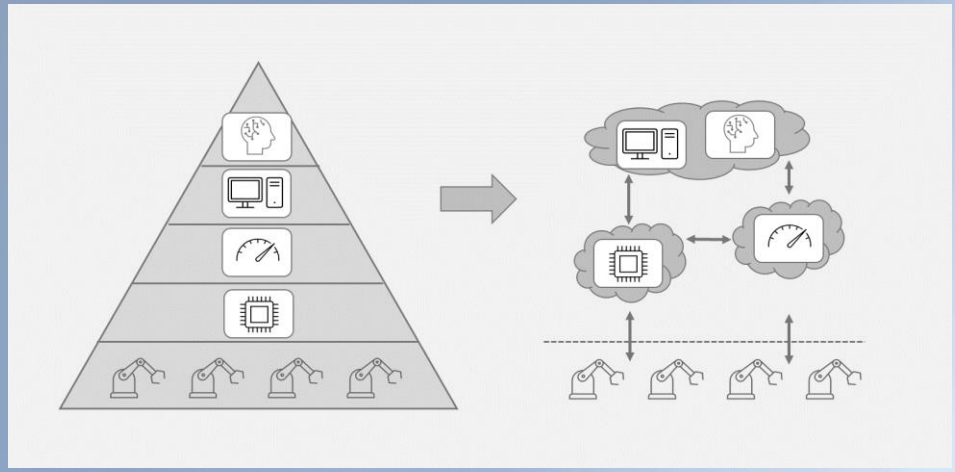
- Konsolen (Sony, Microsoft, Nintendo), PC, Mobile Games, In-Game-Käufe
- Große Publisher wie Activision Blizzard, Tencent, EA



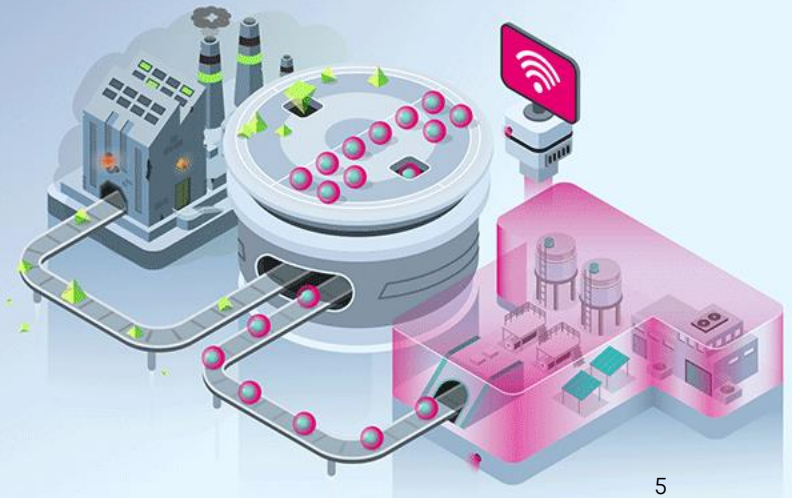
Trends

Rasomware Risiko im IIoT/OT Umfeld wächst überproportional
(~50% in 2024 *Quelle: Dragos*)

- IIoT attraktives Ziel:
  - ältere Netze, kaum Security,
  - IIoT stärker vernetzt,
  - hoher Verfügbarkeitsdruck = hohe Wahrscheinlichkeit für Ransom
- Politische motiviert – Kritische Infrastruktur – Kollateralschäden durch Malware-Kampagnen
- Awareness: Malware Scan wärend Integrationstests für gebrauchte Anlagenteile?



„Cloudifizierung“ = Mehr Angriffsfläche (Netz, Protokolle, APIs, Identities, Komplexität, …)



Beobachtungen (relevant für die Verteidigung)

Spezialisierung der Rollen innerhalb von Gruppen:

- Initial-Access-Broker -> Remote Access
- Ransomware Akteure

- Beim Handover entstehen oft lange Pausen (ToyMaker Example)
- Monitoring wichtig und wirksam

Was ist Ziel der Angriffe?

- „High-Level“ Planungs-, Management- und Monitorng-Systeme (HMI, Historian, ERP, MES, …) + Hypervisor (vCenter im IT-Netz)

Although ransomware attacks rarely compromise lower-level process systems such as programmable logic controllers (PLCs), they often disrupt higher-level systems essential for process visibility, control, management, and telemetry.

There is rarely a substantial effort made to impact lower-level systems directly, because that is currently not necessary or efficient for achieving their financial goals

… and hypervisors are a typical target for ransomware

SANS: A Simple Framework for OT Ransomware Preparation – Lesley Carhart

Day of activity	Type of malicious activity	Threat actor
Initial compromise	User enumeration Preliminary recon Fake user creation Credential extraction via Magnet RAM Capture	ToyMaker
+2 day(s)	Deploy LAGTOY implant	ToyMaker
	Lull in activity for 3 weeks	
+3 weeks aka Cactus day 0	Endpoint enumeration	Cactus
Cactus day 2	Server and file enumeration Indicator removal	Cactus
Cactus day 2 and 3	Proliferation through enterprise	Cactus
Cactus day 4	Archiving sensitive data for exfiltration - extortion	Cactus
Cactus day 8	Remote management tools deployment: eHorus, RMS, AnyDesk OpenSSH connections	Cactus
Cactus day 12	Malicious account creations for ransomware deployment	Cactus
Cactus day 12	Delete volume shadow copies Boot recovery modifications	Cactus

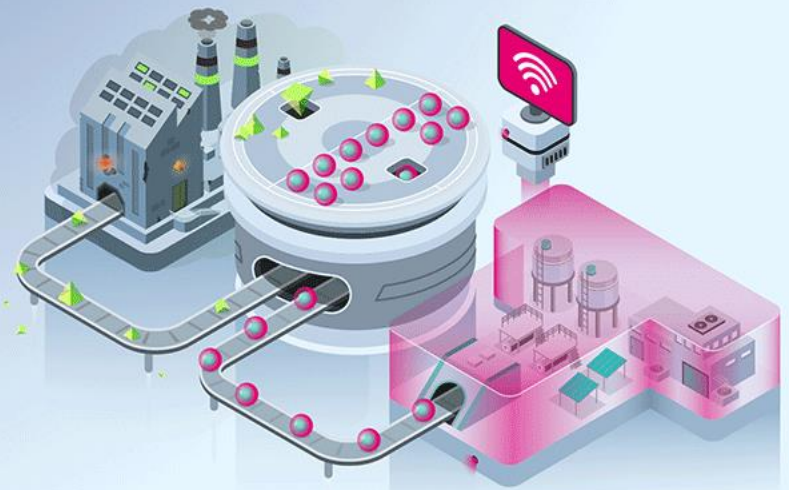
https://blog.talosintelligence.com/introducing-toymaker-an-initial-access-broker

Ransomware – Risiko Management

Kundenaussage: *„Wenn einem Mitarbeiter was merkwürdig vorkommt, geht der rüber zum Sicherungsraum und schaltet den Strom aus …“*

Basics

- Full, tested Backups,
- Segmentation,
- Risiko basiertes Schwachstellen Management (Hypervisor)
- Monitoring (Verhaltensmuster, weniger Endpoint – mehr Netzwerk basiert)
- Virtualisierung für schnelles DR



Ransomware – Incident Respose

Tested Playbooks – Erfolgsfaktoren

Close Valves before hunting IPs

- Zusammenarbeit zwischen IT und OT schon bei der Erstellung der Playbooks
- Gemeinsame Tabletop Übungen (TTX)
- Gemeinsames Verständnis des Betriebs (Assets und Funktion, Topology, Software …)
  - Kann ich IT und OT trennen? Für wie lange? Wie (Firewall Notfall Regel)?
  - Welche Werkzeuge stehen mir zur Verfügung?
  - Welche Systeme kann ich ggf. manuell fahren? Für wie lange?
- Eine zentraler „Cyber-Security“ Ansprechpartner für die Betriebsmannschaft
- Klärung der Verantwortlichkeiten: Wer entscheidet unter Zeitdruck ob bezahlt wird?
- Was sind die Kriterien für eine solche Entscheidung (Decryptor vorhaden, tolerierbare Ausfallzeiten, betroffene Systeme und alternative Betriebsszenarien, finanzieller Impact, rechtliche Bestimmungen, …)

Start simple: Wer informiert wen? Bezahlen? Verhandlungsführer…

Die Identifikation und das Verständnis von Abhängigkeiten von IT-Systemen kann entscheidend und nicht immer offensichtlich sein

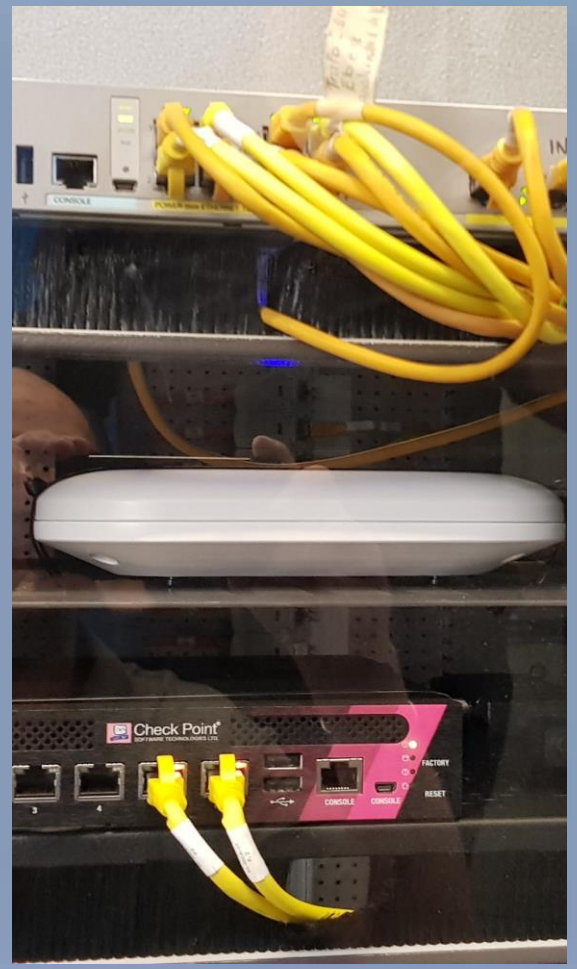
DNS, AD, NTP, …

2. Remote Access

IoT Security

Remote Access – Warum ist das (immer noch) ein Problem?

1. Weil Ich nicht weiß, dass er da ist …



Remote Access – Warum ist das (immer noch) ein Problem?

- Zugang oft über Lagecy Geräte
- Veraltete, embedded SSH, Telnet und Web-Server

95.143.49.217
Hostettler Tamara
Switzerland, Schaffhausen

MikroTik v6.25
Login:

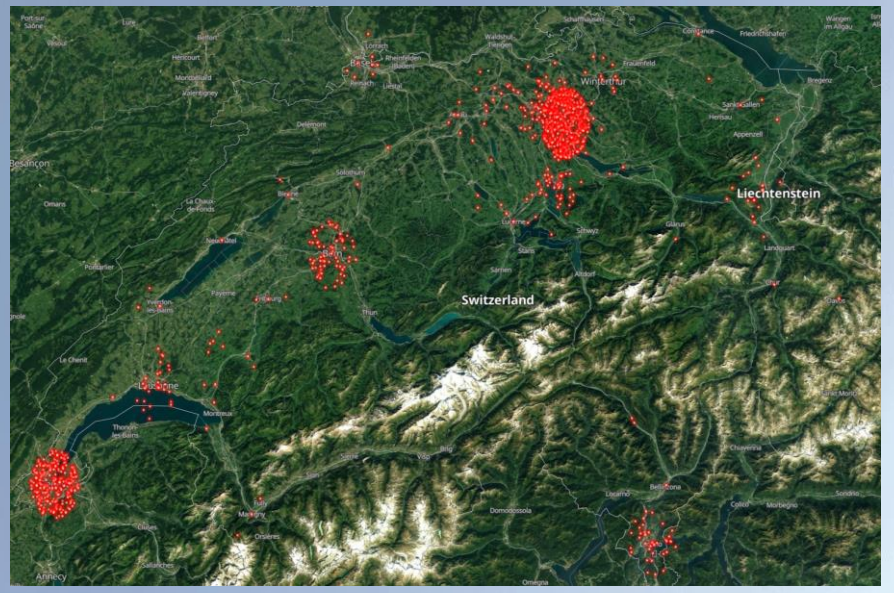
FrostyGoop
ICS Malware

- **MikroTik** ist ein lettischer Hersteller von Netzwerk-Hardware und -Software.
- **RouterOS** ist deren eigenes, Linux-basiertes Betriebssystem, das auf ihren Routern und Geräten wie dem **RouterBOARD** läuft.
- **v6.25** bezeichnet eine ältere Version (erschienen ca. 2015) – mittlerweile gibt es deutlich neuere Versionen (v7.x+).
- Solche Geräte werden oft eingesetzt als:
  - Router
  - Firewall
  - VPN-Gateway
  - Wireless Access Point

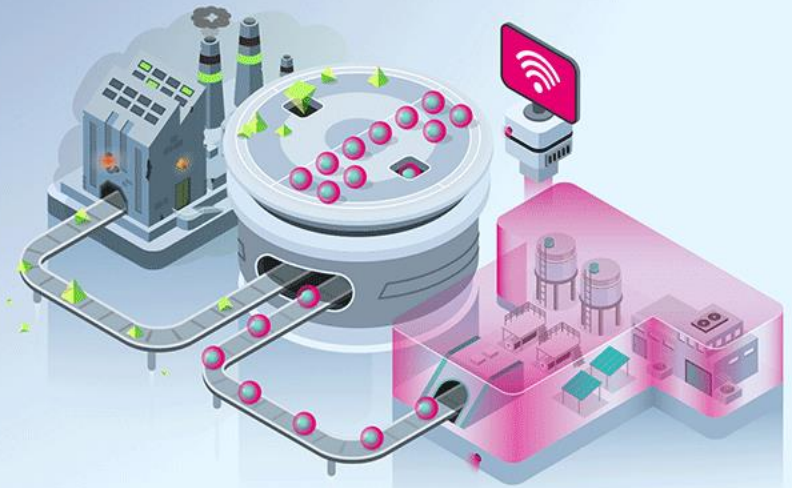
⚠ **Sicherheitshinweis:**

Geräte mit **veralteter Firmware (wie v6.25)** sind **anfällig für bekannte Sicherheitslücken**, z. B.:

- Fernzugriff ohne Authentifizierung
- Schwachstellen im Winbox-Dienst (Port 8291)
- Exploits für VPN, FTP, Telnet, SSH bei Standardkonfiguration



Shodan.io map: Modbus, SSH, RDP (Mai 2025)



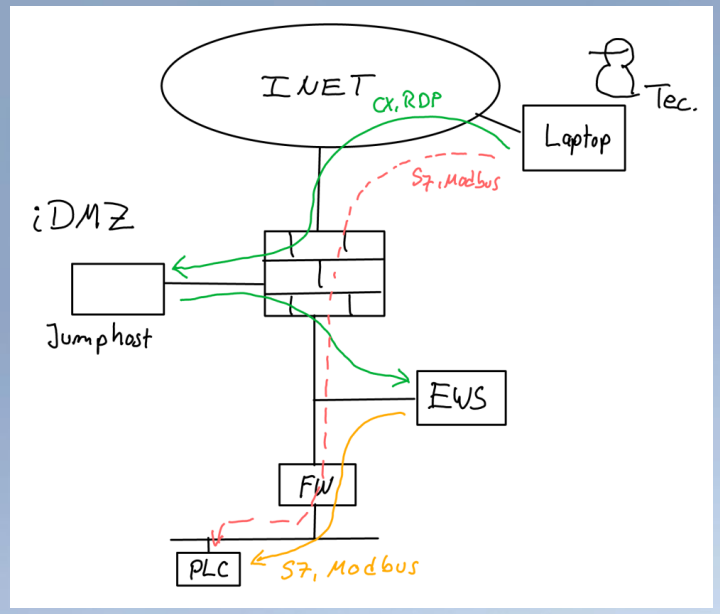
RAS - HowTo …

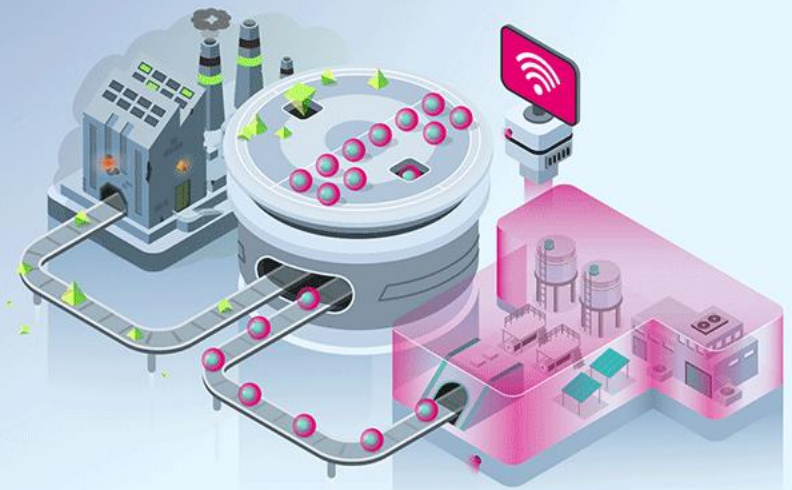
„Leckage-Warnung“

- Regelmäßige Assessments
- Kontinuierliches Monitoring (passiver Sniffer)
- Awareness & Policies

Architektur

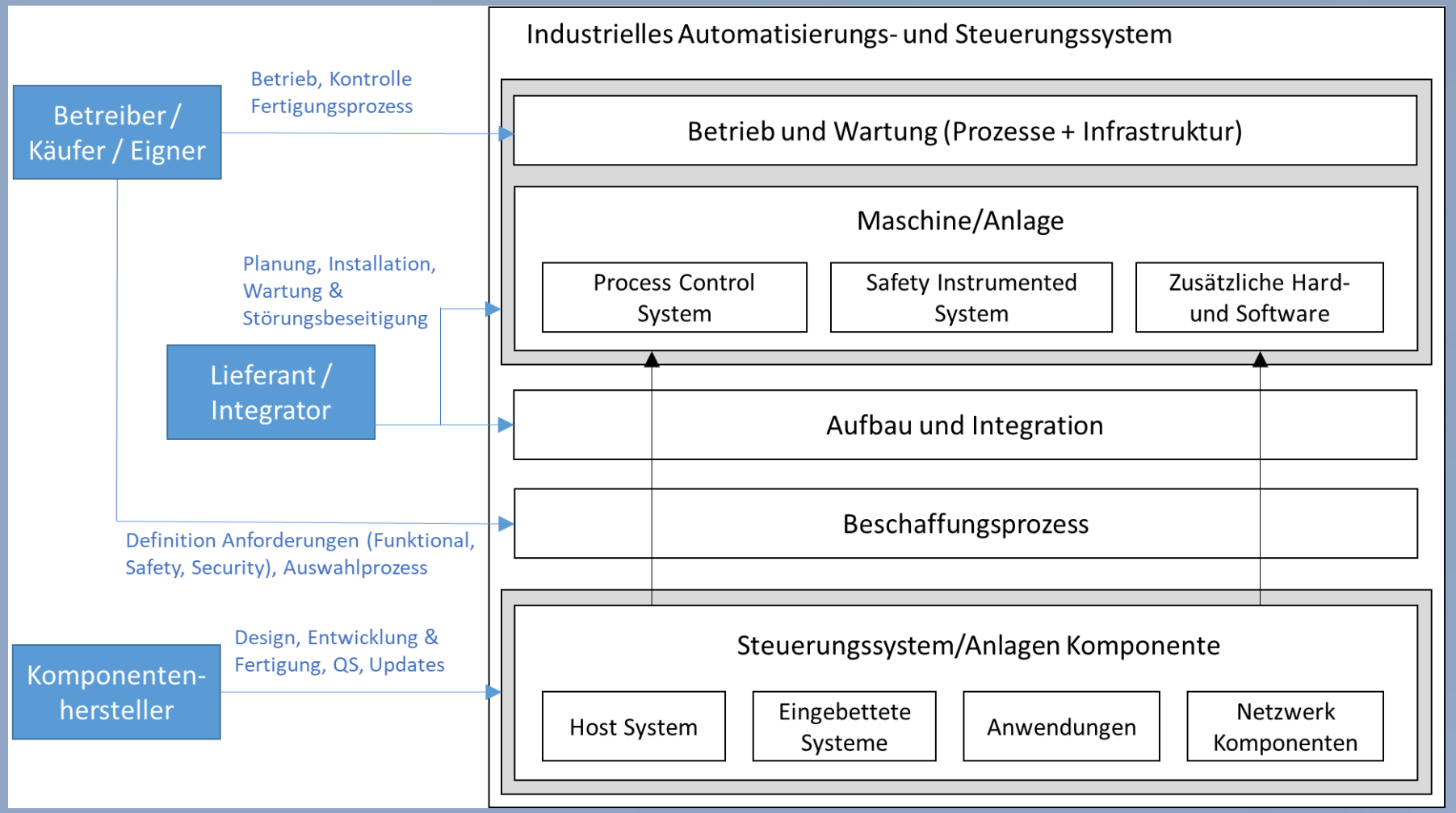
Move the user closer to the data vs. moving the data closer to the user ...



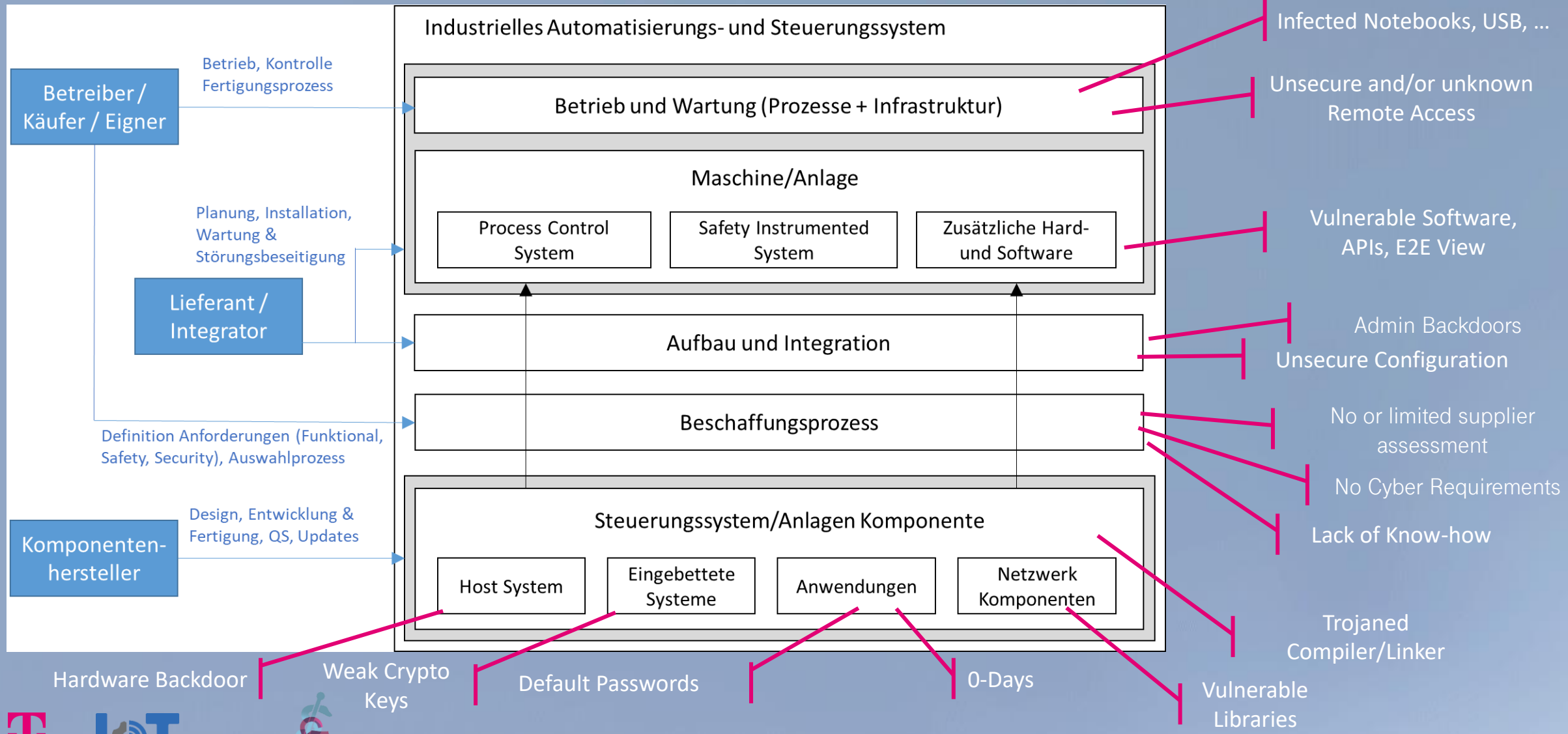


3. Lieferketten

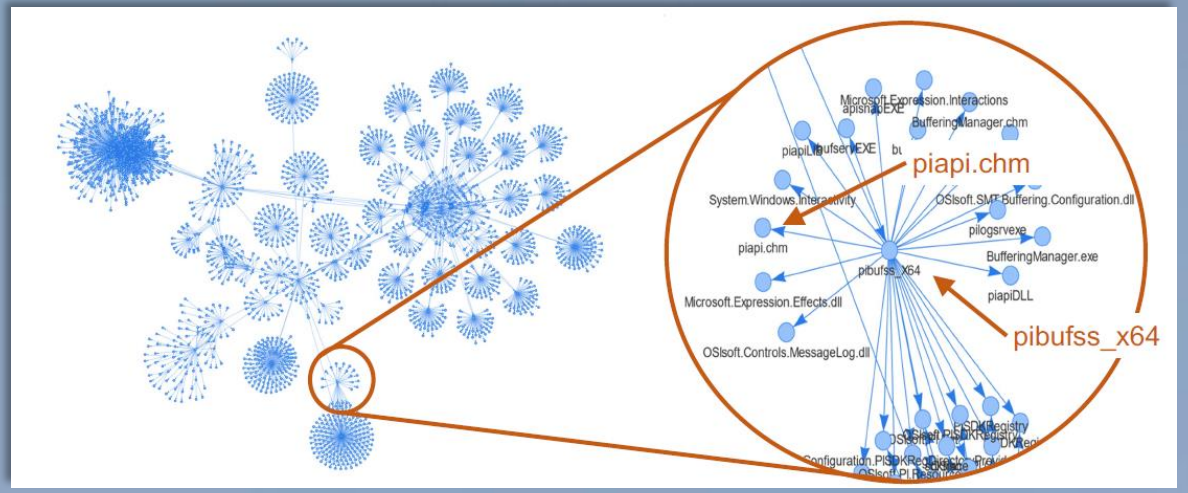
Lieferkettenmodelle und Risiken



Lieferkettenmodelle und Risiken



SBOM und “Attackers Return on Invest”



Attacker’s Return on Investment

Incident	Direct Targets	Indirect Victims	Time Undetected
SolarWinds	1	18,000 Infected ~250 Exploited	10 Months
Dragonfly	3	250-700	9 months
Kaseya	1	800-1500	N/A
Codecov	1	23,000 Possible 200 Likely?	2 months

- Softwareplatform Orion (NW Management)
- 33.000 Customer
- Discovered by FireEye
- Compromised update implements backdoor
- Installed by 18.000 customers
- Vulnerability exploited: Software Build-Process

Supply Chain - Riskmanagement

- Pentesting
- Verhaltensmuster Monitoring
- Analyst Threat-Hunting „Attitude“
- „Zero-Trust Light“ Ansätze
  - Rollenbasiertes User-/Rechte Management
  - (User-)Monitoring
  - „Micro-Segmentierung“ (Prozeß- und Aufgaben orientierte, logische Zonen)

4 SCHWACHSTELLEN IM PENETRATIONSTEST

Als Ergebnis des Tests wurden die folgenden Schwachstellen identifiziert.

Telekom Security weist darauf hin, dass alle empfohlenen Maßnahmen vor der Umsetzung auf der Produktionsumgebung auf Testsystemen auf Verträglichkeit überprüft werden sollten.

4.1 Serieller Port auf der Platine der Komponente

Auf der Platine der Komponente befinden sich Pins, welche verwendet werden können, um über einen seriellen Port Zugang zu einem Terminal des Linux-Betriebssystems zu bekommen.

Beim Aufschrauben des Gehäuses konnten mehrere Pins gefunden werden, welche mit einem Oszilloskop überprüft wurden. Durch Tests konnte anschließend erkannt werden, dass zwei dieser Pins als Output (TX) und Input (RX) für eine serielle Schnittstelle (UART) genutzt werden. Zur Kommunikation wurde ein Raspberry Pi 4 mit der seriellen Schnittstelle verbunden. Da die Spannungspegel unterschiedlich waren (Komponente 1,8V vs. Raspberry Pi 3,3V), wurde ein sogenannter Level Shifter (Modell „Pololu 2595“) auf einem Steckbrett zwischengeschaltet (siehe Abbildung 1).

Abbildung 1: Anschluss des seriellen Ports an der Komponente (links unten) an einen Raspberry Pi (rechts oben)

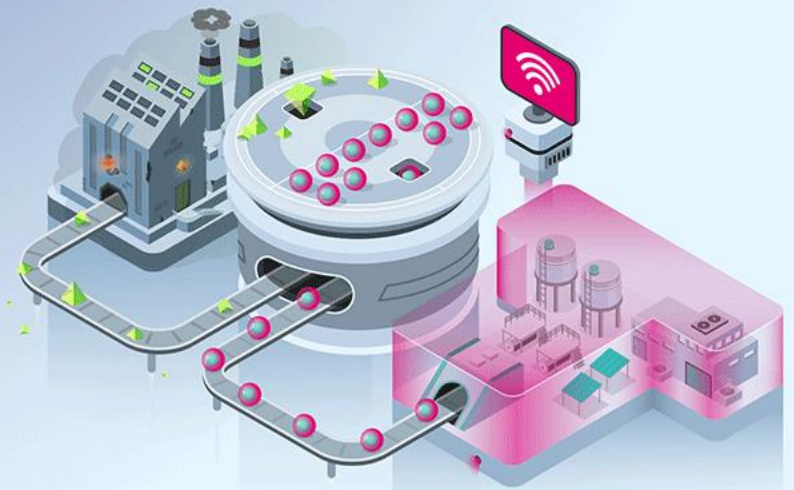
Mithilfe der seriellen Schnittstelle kann ein Angreifer auf die Konsole des Linux-Betriebssystems zugreifen. Dadurch hat er die Möglichkeit Eingaben zu tätigen und Ausgaben des Betriebssystems einzusehen. Der Zugriff auf das Betriebssystem wird durch eine Authentifikation geschützt, die jedoch nur mit einem Standard Passwort konfiguriert ist.

Betroffene Systeme:

Geräte Name	Seriennummer	Firmware Version
xxxxxxxxxxxx	xXxXxXxXxXxXx	xx.xx.xx.xx-x

Maßnahmen:

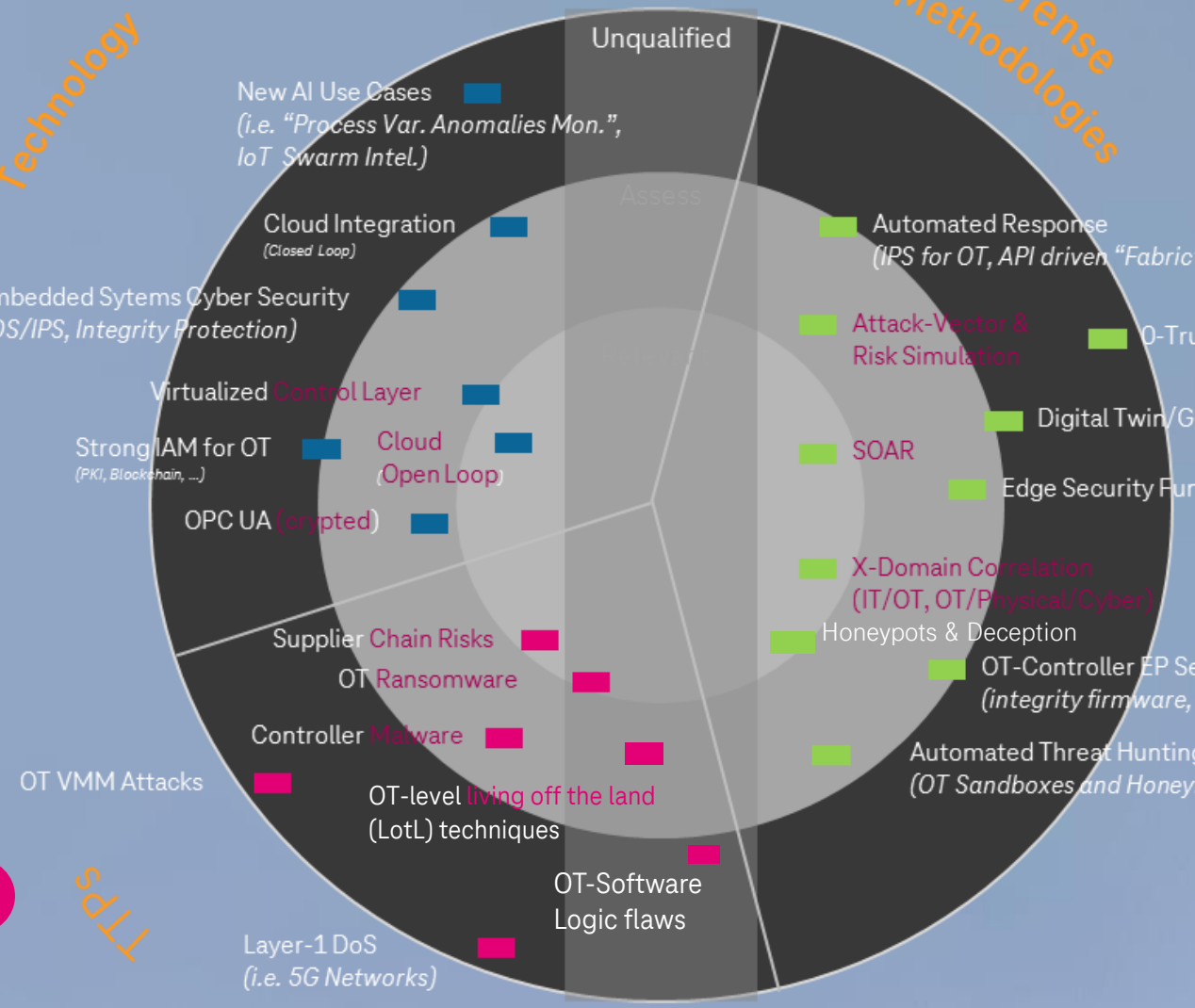
- Bestenfalls sollte die serielle Schnittstelle abgeschaltet werden. Falls dies aus Wartungs-/Recovery Gründen allerdings nicht möglich ist, sollte ein starkes, von Gerät zu Gerät unterschiedliches Passwort konfiguriert werden. Dadurch können Angreifer, die ein Gerät



AI?

IoT Security

Inno Radar



Virtualization

Cloud

Crypto

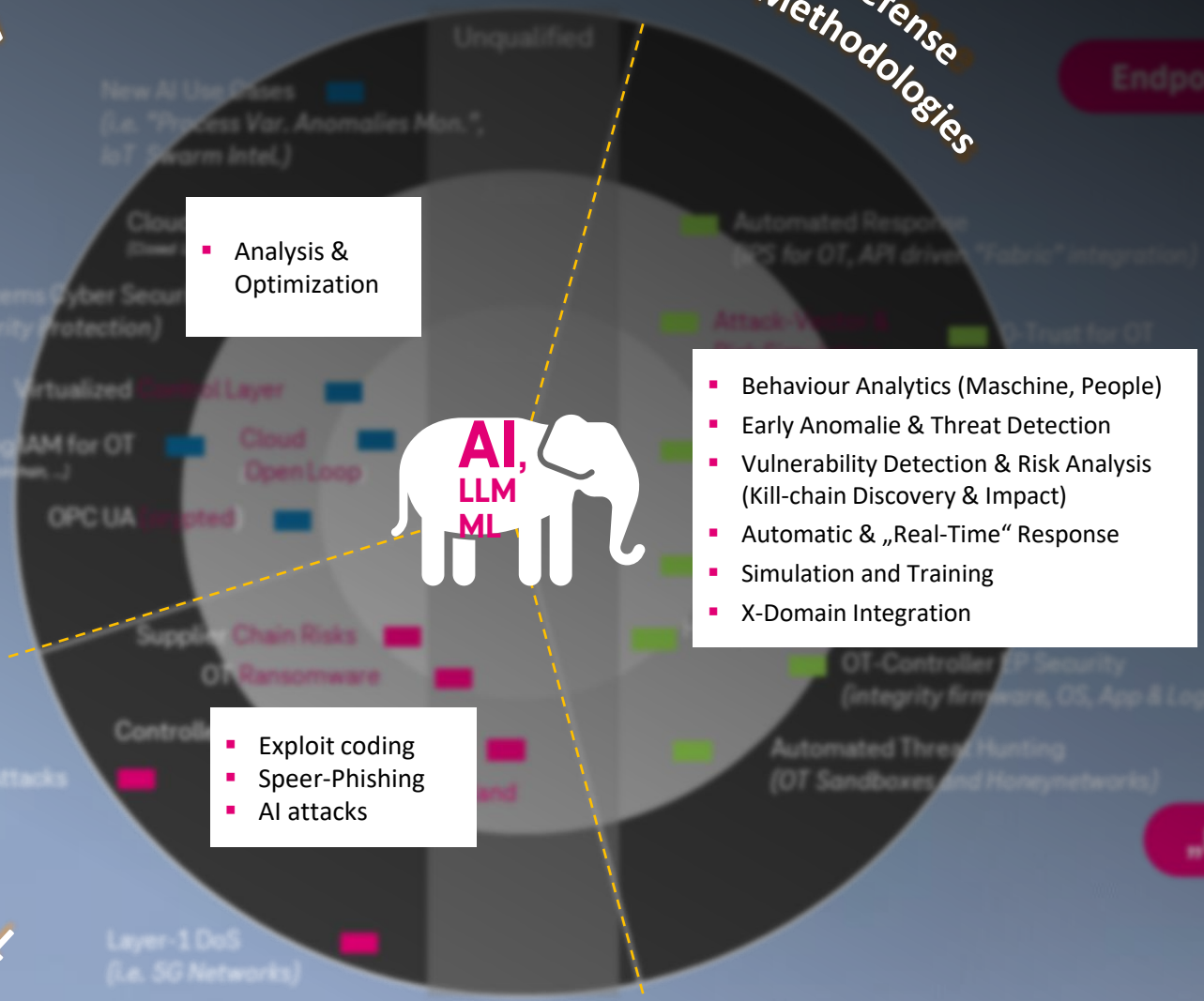
Wireless

Endpoint

Automation

„Real Time" Response

AI Impact



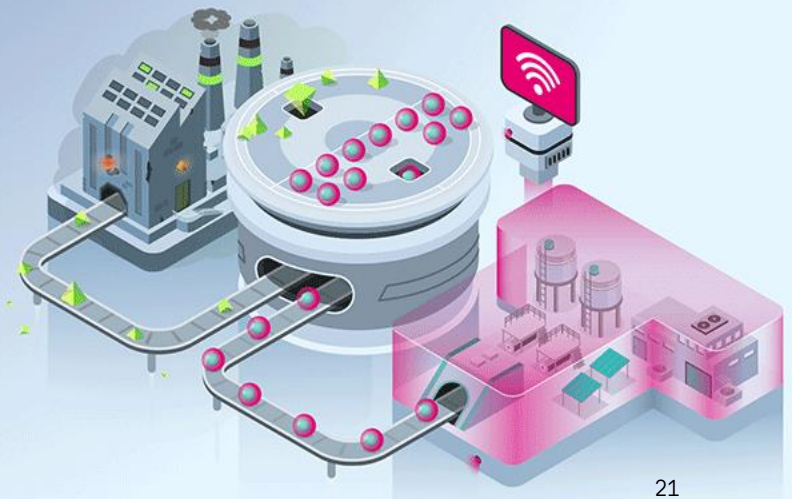
Virtualization
Cloud
Crypto
Wireless
Endpoint
Automation
„Real Time“ Response

Geh es auch ohne AI?

- AI kann bei Anomalie- und Mustererkennung hilfreich sein
  - In großen, komplexen Netzen hilfreich

- Richtige Anwendung und „Tuning“ kann komplex sein
- Durch mangelnde Transparenz erfordert manchmal Übung einzuschätzen, welchen Aussagen man trauen kann

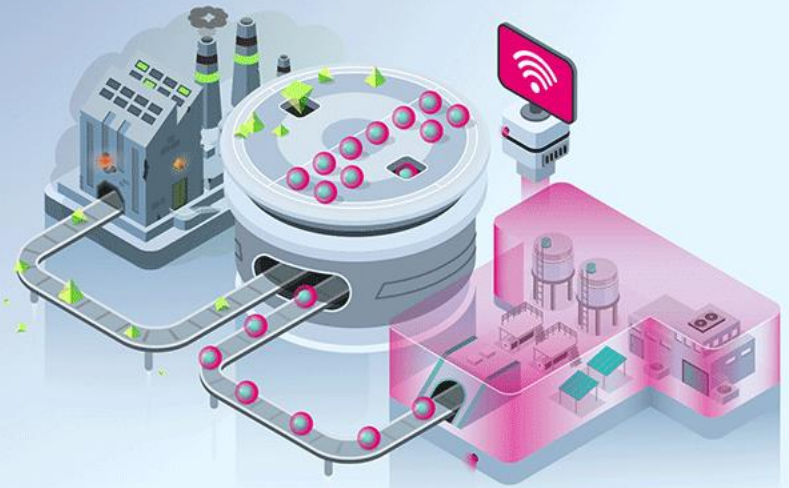
- 3 simple Detection-Szenarien sind besser als keins



Top ~~3~~ 4

0. Your [redacted]
1. Ransomware
2. Remote Access
3. Suppy Chain

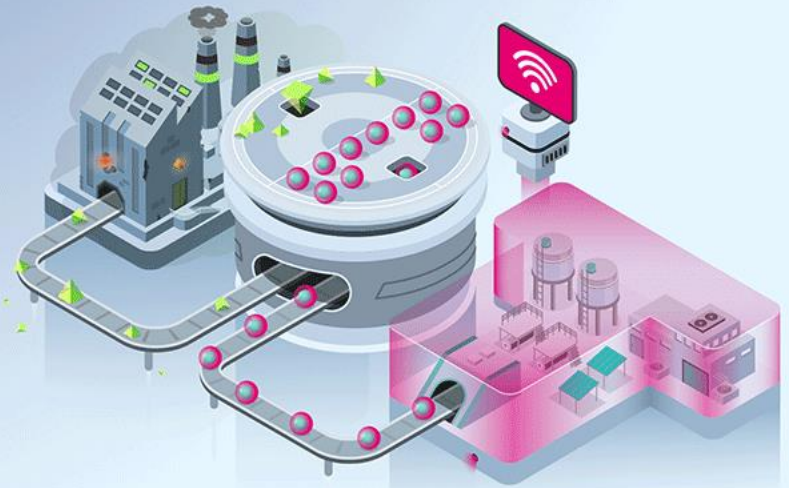
AI can actually be helpful, sometimes ;-)

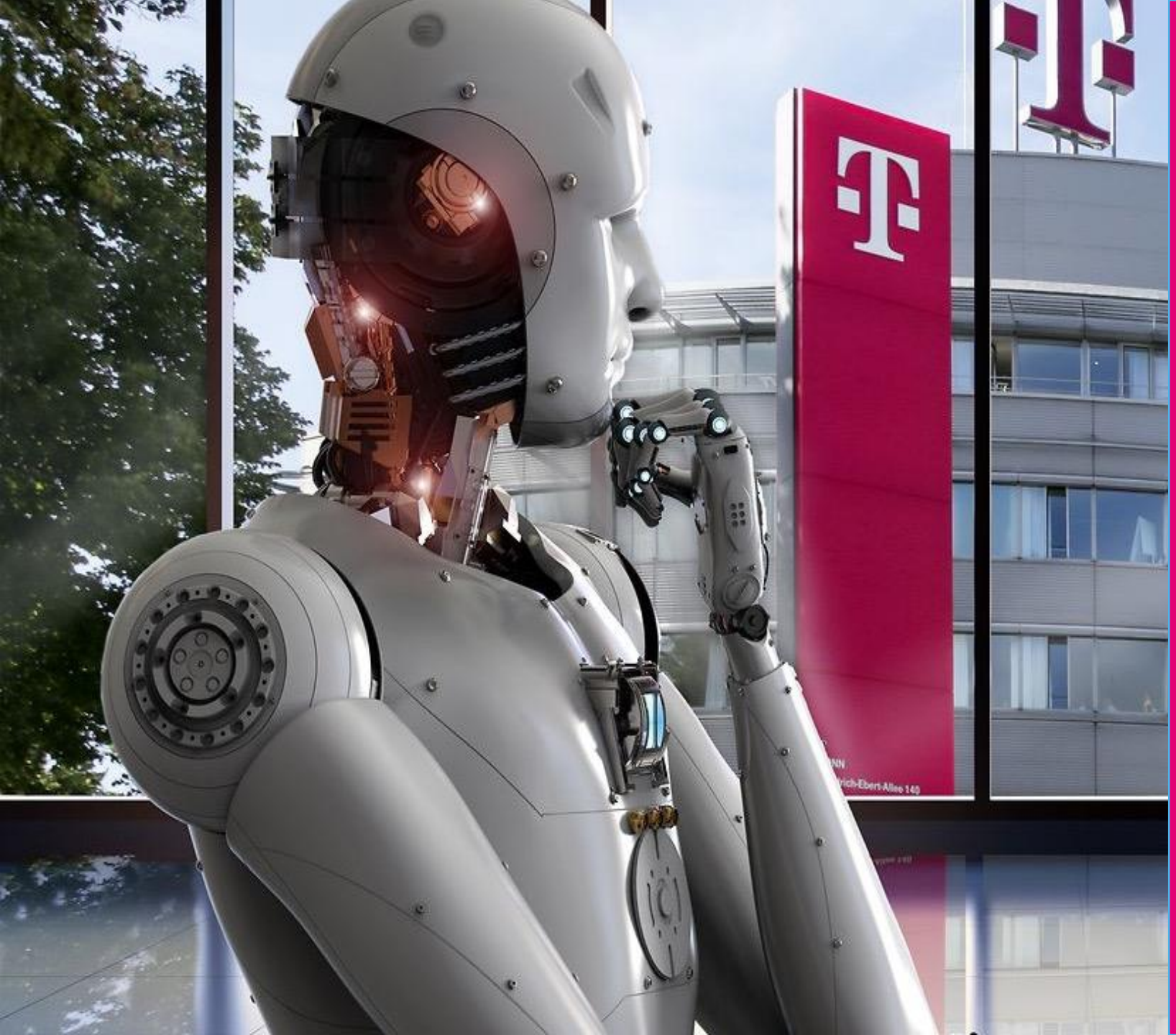


Top ~~3~~ 4

0. Your IT Dependencies?
1. Ransomware
2. Remote Access
3. Suppy Chain

AI can actually be helpful, sometimes ;-)





IoT Security

Thank You!

Bernd Jäger
bernd-jaeger@telekom.de
GRID, GCFA, GCIA, GREM, GWASP, CISSP
Practice Lead ICS/IoT Security