PDVSYSTEME
Industrial IT

Unternehmergespräch ENERGIE

Security-Bedarfe eines produzierenden Unternehmens

Produktion im Fadenkreuz

- Professionalisierte Angreifer
- Wirtschaftlich motiviert
- Produktion = attraktives Ziel

Wer wir sind.

Und warum wir den Bedarf kennen.

118 Mitarbeiter

3 Standorte

hochqualifizierte IT-Spezialisten

Industrial IT

Services & Solutions

über 40 Jahre Expertise

UNSERE HALTUNG
wertschätzend, vertrauens- und respektvoll, auf Augenhöhe

IT-Infrastruktur.

Hardware | Software | Netzwerksysteme

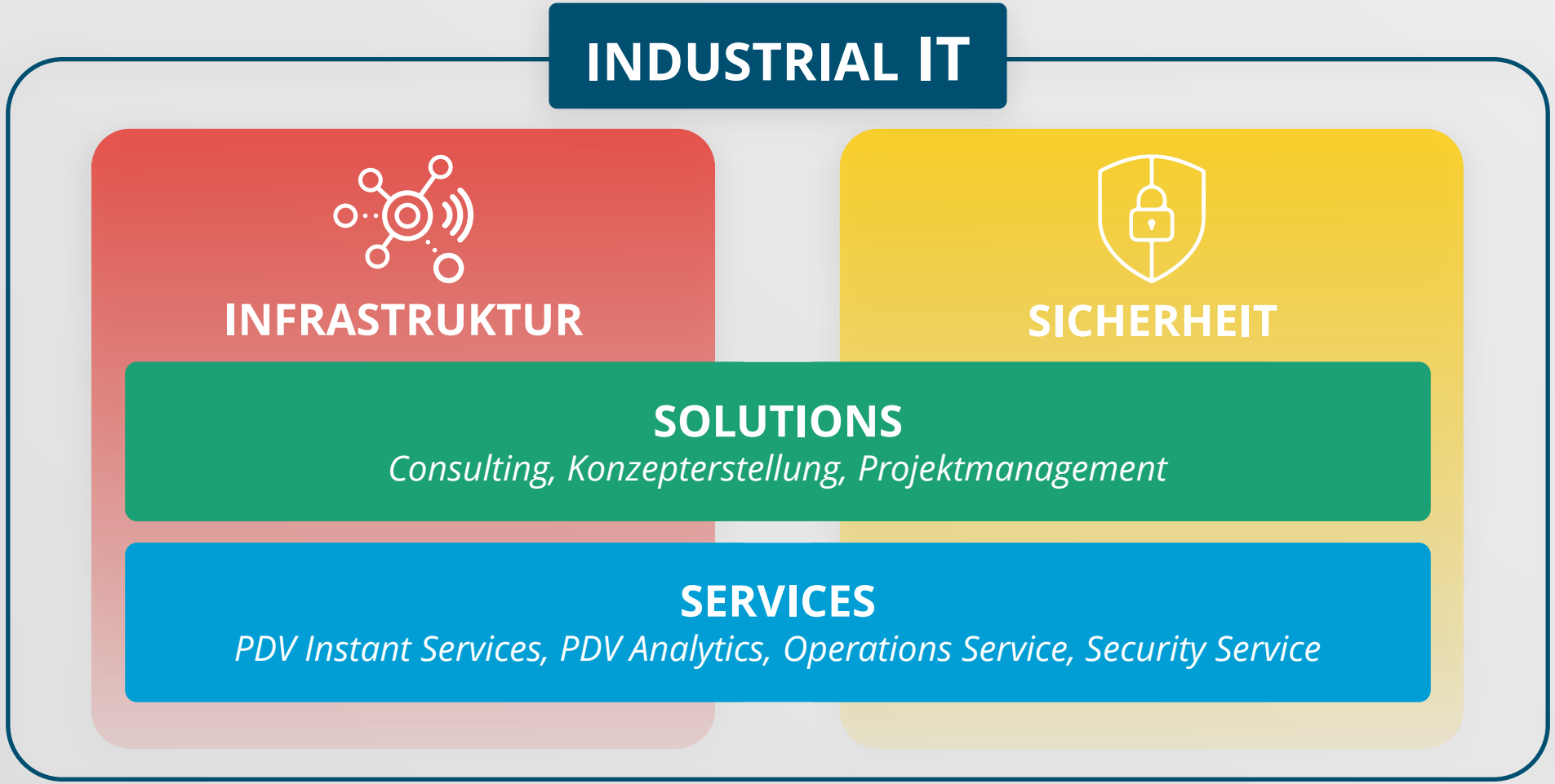
IT-Security.

TOMs gegen Cyberbedrohungen

PDV Leitbild. Vision.

„Unser Beitrag zur Verfügbarkeit von kritischen Infrastrukturen und Produktionsprozessen ist unverzichtbar.“

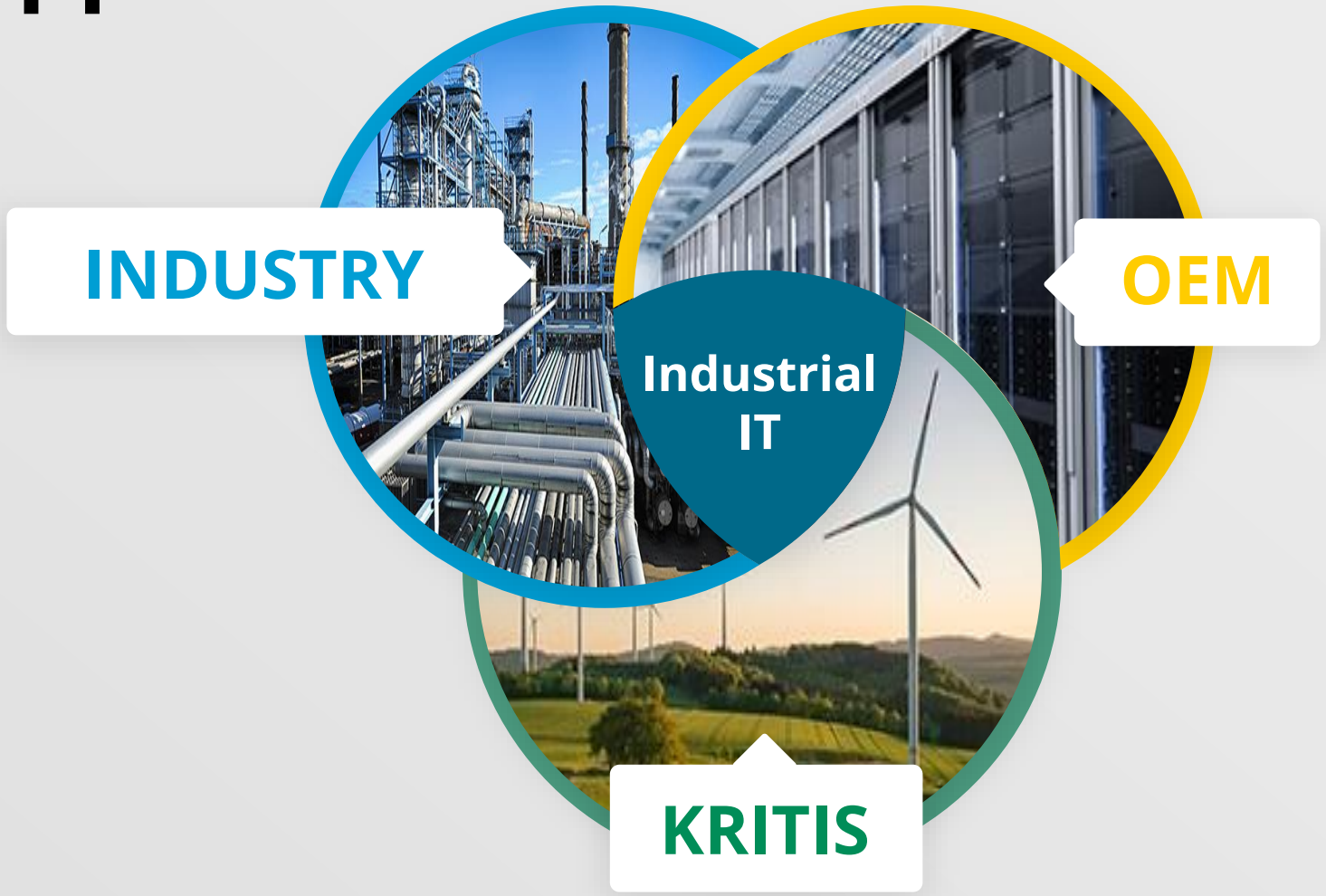
Spezialist für Infrastruktur und Sicherheit.



PDV-Systeme GmbH

Unsere Kunden.

Unsere Zielgruppen.



Warum gerade die Produktion?

- Stillstand = unmittelbarer Schaden
- Hoher Zeitdruck zur Wiederaufnahme
- Komplexe, gewachsene IT/OT-Landschaften

IT und OT: Zwei Welten, eine Realität.

IT-Zone

Schnittstellen:
Fernwartung,
Cloud,
Lieferanten,
Identitäten

OT-Zone

Was ein Angreifer vorab über ein Unternehmen erfährt?

Öffentliche Quellen

Unternehmenswebseite (Standorte, Technologien, Partner)

Pressemitteilungen & Ausschreibungen

Geschäftsberichte / Zertifizierungen

Mitarbeiter & Organisation

(Rollen, Verant-wortlichkeiten)

Stellenausschreibungen (Technologien, Systeme)

Konferenzen & Vorträge

Technische Spuren

Domains, IP-Ranges, Zertifikate

Cloud-Dienste, VPN-Gateways

Leaks aus früheren Vorfällen

Vom Angriff zur Auswirkung

- ❌ **Produktionsstillstand**
- ❌ Qualitätsverlust
- ❌ Lieferketteneffekte
- ❌ Reputationsschäden
- ❌ **Safety-Risiken**

Governance & Verantwortung

- **Klare Zuständigkeiten IT / OT / Produktion**
- Gemeinsames Risikoverständnis
- Explizite Risikoakzeptanz
- Verankerung in Unternehmenszielen

Transparenz & Sichtbarkeit

- **Vollständige Asset-Übersicht**
- Kenntnis von Abhängigkeiten
- Klassifizierung nach Kritikalität
- Laufende Aktualisierung

Identitäten & Zugriffssteuerung

- Zentrale Identitäten (Mitarbeiter, Dienstleister)
- **Trennung IT / OT-Zugriffe**
- Prinzip der minimalen Berechtigung
- **Gesicherte Fernzugriffe**

Technische Resilienz

- **Segmentierung IT / OT / Produktion**
- **Trennung kritischer Produktions-bereiche**
- Backup & Recovery
- Wiederherstellungstests

Prozesse & Menschen

- Definierte Incident-Response-Prozesse
- Einbindung Produktion & Instandhaltung
- Regelmäßige Übungen
- Schulung & Sensibilisierung

Typische Herausforderungen

- ⚠️ Fokus auf Tools statt Strategie
- ⚠️ **Fehlende OT-Einbindung**
- ⚠️ Keine realistischen Szenarien
- ⚠️ **Security vs. Produktion als Gegenspieler**

Einstieg

Schritt 1 – Analyse & Transparenz

- [ ] Inventar der IT- und OT-Systeme
- [ ] Kritikalität der Geschäftsprozesse erfassen
- [ ] Erste Risikoeinschätzung

Schritt 2 – Verantwortlichkeiten klären

- [ ] Wer ist für Informationssicherheit zuständig?
- [ ] Rollen & Zuständigkeiten definieren (IT / OT / Management)

Umsetzung

Schritt 3 – Technische & organisatorische Controls

- [ ] Zugriffskontrolle & Identitäten
- [ ] Segmentierung IT/OT
- [ ] Backup & Recovery
- [ ] Notfallprozesse (Incident Response)

Schritt 4 – Awareness & Schulung

- [ ] Sensibilisierung der Mitarbeiter
- [ ] Einbindung von Produktion und Instandhaltung
- [ ] Übungen und Testfälle

Kontrolle & Verbesserung

Schritt 5 – Monitoring & Audit

- [ ] Regelmäßige Kontrolle der Maßnahmen
- [ ] Schwachstellen prüfen & dokumentieren

Schritt 6 – Lessons Learned / Anpassung

- [ ] Maßnahmen an neue Risiken anpassen
- [ ] Erfahrungen aus Vorfällen nutzen

NIS2-Konformität

Roadmap-Schritte	NIS2-Pflichten
Analyse & Transparenz	*Risikoanalyse, Asset-Kenntnis, Nachweisführung*
Verantwortlichkeiten klären	*Governance, Meldepflicht, Zuständigkeit*
Technische & organisatorische Controls	*Technische Mindeststandards, Backup, Segmentierung*
Awareness & Schulung	*Sicherheitskultur, Schulungen*
Monitoring & Audit	*Kontrolle, Reporting, Dokumentation*
Lessons Learned / Anpassung	*Kontinuierliche Verbesserung, Lessons Learned dokumentieren*

Pragmatismus & Priorisierung

- Transparenz schaffen
- Fernzugriffe absichern
- Segmentierung
- Backup & Recovery leben
- Notfallorganisation – Ausfallpläne „Was ist komplett ohne IT/Strom möglich?“

Resilienz einfach machen!

Übergang zur Energiewirtschaft

Gleiche Bedrohungen, ähnliche technische Realität

Höhere gesellschaftliche und regulatorische Verantwortung

Lessons Learned aus Produktion übertragbar

PDVSYSTEME
Industrial IT

Vielen Dank.

PDV-Systeme GmbH