Gemeinsam stärker: Synergien zwischen IT- und OT-Security im SOC

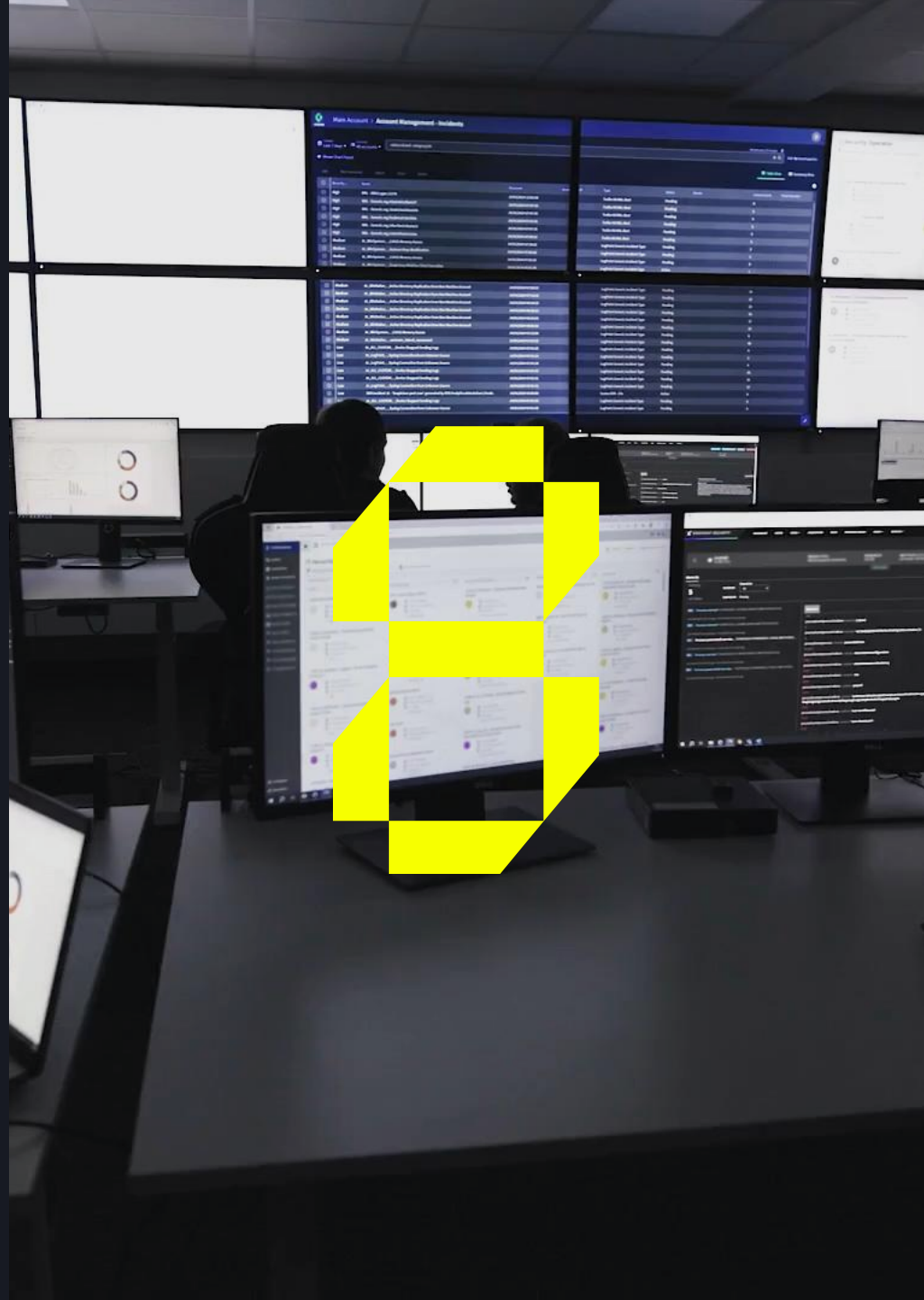
8COM
CYBER SECURITY

Keynote

Gemeinsam stärker: Synergien zwischen IT- und OT-Security im SOC

Richard Jaletzki
Teamlead OT Security

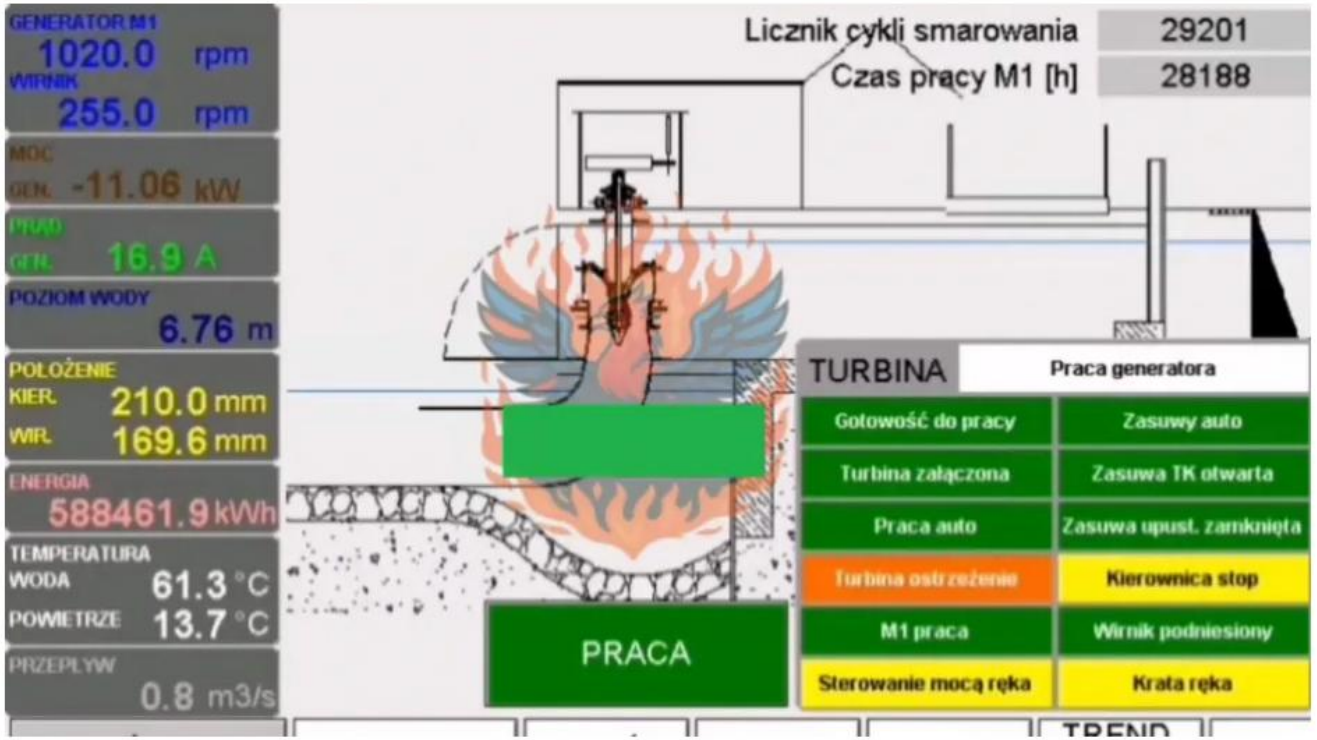
8COM
CYBER SECURITY



LATEST NEWS

Russian Hackers Breach Polish Hydropower Plant in Major Cyberattack

Aug 19, 2025 14:49 Updated Aug 20, 2025 10:10 2 min read



Russian hackers once again breached a small hydropower plant in Poland, disrupting its control systems. (Source: CyberDefence24)

Pro-Russian hackers carried out a cyberattack on a small hydropower plant in Poland's Pomeranian Voivodeship, near Gdańsk. This is the second time the same facility has been targeted in recent months.

Synergien zwischen IT- und OT-Security im SOC

1 IT vs. OT

8COM CYBER SECURITY

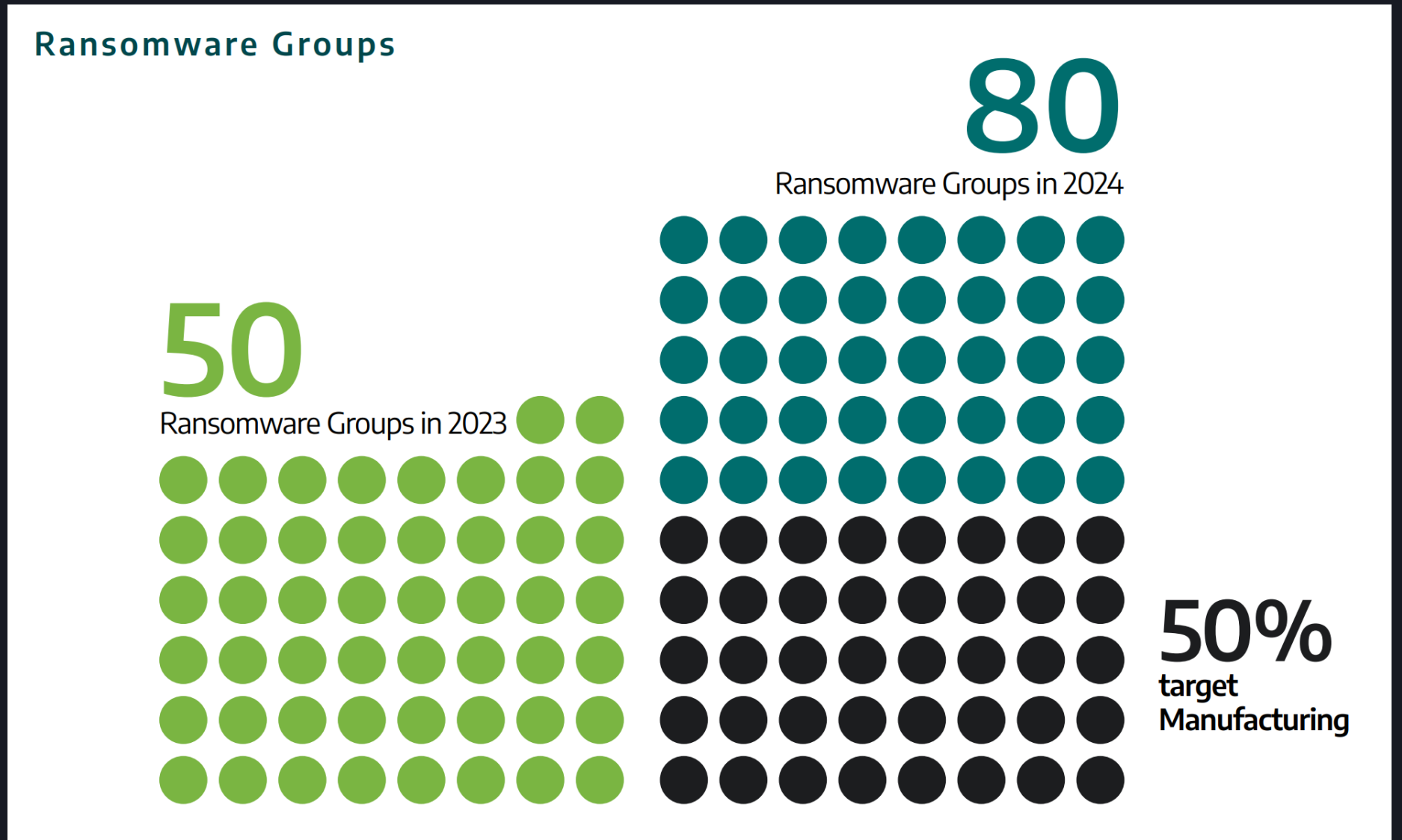
Unterschiede zwischen IT und OT

IT (Information Technology) „Computer bewegt Daten“	OT (Operational Technology) „Computer bewegt Dinge“
Datenverarbeitung und Kommunikation	Steuerung physischer Prozesse
E-Mail, Datenbanken, ERP, …	Industrieanlagen, Roboter, SCADA, HVAC, Zugangssteuerung, …
Updates und Patches regelmäßig möglich “Patch Tuesday”	Updates schwierig, planungsintensiv „Patch September“
Ausfälle sind i.d.R. nicht Geschäftskritisch	Ausfälle bedeuten Produktionsstopp, Umwelt- und Gesundheitsgefahren

Unterschiede zwischen IT und OT

Schutzbedarfe in der IT „Daten schützen“	Schutzbedarfe in der OT „Betrieb sichern“
	0. Sicherheit (Safety)
1. Vertraulichkeit	1. Verfügbarkeit
2. Integrität	2. Integrität
3. Verfügbarkeit	3. Vertraulichkeit

Dragos 2025 OT/ICS Cybersecurity Report



8COM

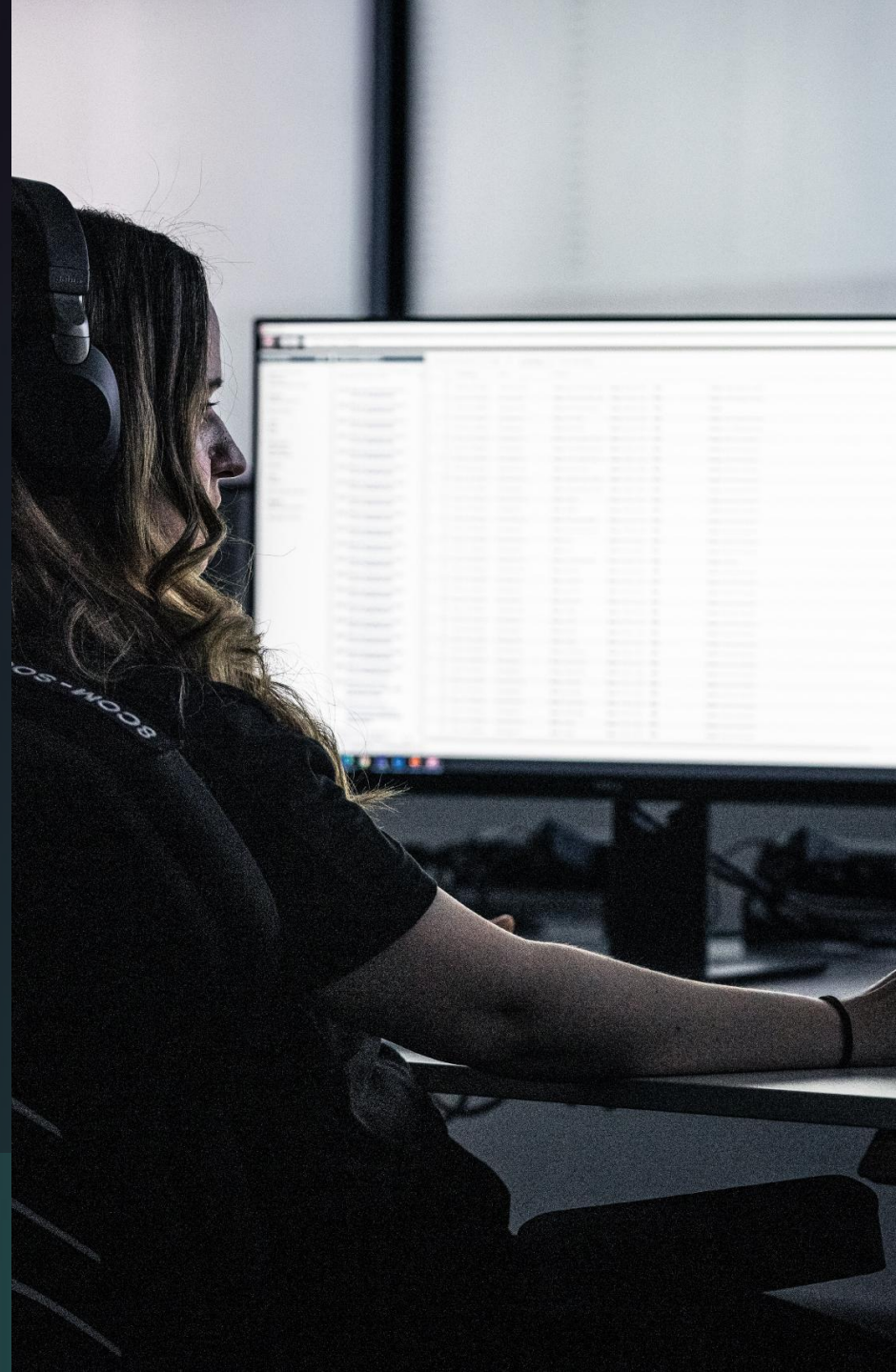
BSI Lagebericht 2024

Gefährdungslage KRITIS

- Ransomware-Angriff auf Software-Dienstleister Energie (Leitsysteme, Prozesssteuerung)
- Ransomware-Angriff auf Hersteller von industriellen Steuerungssystemen
- DDoS auf Energiebetreiber, vorübergehender Teilausfall der kritischen Infrastruktur

- Ziele, bei denen mutmaßlich eine hohe Bereitschaft zur Lösegeldzahlung besteht

8COM



Synergien zwischen IT- und
OT-Security im SOC

2 OT Security Operations Center

as a Service

8COM
CYBER SECURITY

OT SOC as a Service

Service-Beschreibung

- Passive Asset-Erkennung – Rückwirkungsfrei, physisch garantierbar
- Angriffs- und Anomalieerkennung, Schwachstellen- und Risikoanalyse
- Alarmbearbeitung durch zertifizierte Analysten: 24/7/365, Tag und Nacht
- Integration in unser deutsches Security Operations Center
- Incident Response Team für schnelle Reaktion bei Bedrohungen
- Korrelation mit IT-Sicherheitsereignissen für ein ganzheitliches Sicherheitsbild

8COM

Kombiniertes IT/OT SOC

Synergieeffekte eines kombinierten IT/OT SOC-Betriebs

- **Holistische Bedrohungserkennung**
  Angriffe aus der IT ins OT-Netz frühzeitig erkennen
- **Wechselwirkungen zwischen den Netzen**
  Bessere Einschätzung, ob ein IT-Vorfall auf die OT wirkt
- **Unified View**
  Zentrale Sichtbarkeit über alle Tools und Netzbereiche hinweg
- **Wissenstransfer**
  Spezialwissen über IT-Vorfälle findet auch in der OT Anwendung
- **Kollaborative Abwehrstrategien**
  Ganzheitliche Meldeketten und Notfallprotokolle

8COM

Incident Handling in der OT

- Root cause analysis
  Technischer Vorfall oder Cyber-Angriff?
- Beurteilung, ob IT-Vorfall auf OT wirkt
- Incident Response Readiness: Gemeinsame Prozesse und Eskalationspfade für IT und OT
- Kürzere Reaktionszeiten durch SOC-Prozesse und bereits erhobene Daten
- Krisenmanagement & Krisenkommunikation
- Gerichtsverwertbare Gutachten und Handlungsempfehlungen
- Unterstützung durch externe Fachanwaltskanzlei (Legal Response Service)
- Aktive Verbesserungen durch gemeinsames „Lessons Learned“

8COM

Synergien zwischen IT- und
OT-Security im SOC

3 Pain Points

8COM
CYBER SECURITY

8com OT SOC: Pain Points

Dediziertes OT SOC statt Eigenleistung
Vom Erfahrungsschatz des etablierten SOC-Teams profitieren und den Fokus auf den eigenen Kernkompetenzen behalten.

Alle an Bord holen
Vorbehalte in der OT betrachten und eine gemeinsame Strategie erarbeiten.

Sichtbarkeit schaffen
Eine aktuelle Asset-Liste ist sehr hilfreich – wir unterstützen gern.

Meldekette etablieren
Notfallpläne erweitern, so dass bei Vorfällen alle Bereiche einbezogen werden können.

Sie haben noch Fragen?

Sprechen Sie mich gerne an!

8COM
CYBER SECURITY

Richard Jaletzki
Teamlead OT Security

richard.jaletzki@8com.de
+49 6321 48 446 – 2095
+49 151 72457327

8com.de/newsletter