TELONIC

CLAROTY

Systeme von Claroty schließen die Sicherheitslücke, die entsteht, wenn lediglich herkömmliche IT-Sicherheitstools auf industrielle und andere vernetzte Umgebungen angewendet werden.

OT (Operational Technology) = Hardware & Software zur Steuerung industrieller Anlagen, Prozesse, Infrastruktur

Problem: Klassische IT-Security-Lösungen greifen hier nicht

Risiko: Angriffe auf Produktions- und Versorgungsnetze können Ausfälle, Produktionsstillstand oder sogar Gefahr für Menschenleben verursachen.

- Fertigung & Industrieanlagen
- Energie & Versorger
- Healthcare
- Transport & Logistik
- Kritische Infrastrukturen

Mehr Features & tiefere Integration als Nozomi, Darktrace, Armis, Microsoft Defender for IoT etc.

Unique Selling Point: Kombination aus Visibility + Risk Management + Remote Access in EINER Plattform.

PORTFOLIO

- **xDome**
  SaaS-Plattform für Visibility, Risiko- & Bedrohungsmanagement
- **Continuous Threat Detection (CTD)**
  laufende OT/IoT-Überwachung
- **Secure Remote Access (SRA)**
  sicherer Fernzugriff für Wartungspartner
- **Edge**
  leichtgewichtige OT-Security für kleinere Standorte/Filialen
- **Collector**
  HW/VM zum passiven Datensammeln via SPAN/RSPAN

Vorteile

Mehr Features als der Wettbewerb	Visibility, Remote Access, Risk Management, Threat Detection & Simulation
Beste Protokollabdeckung	OT/IoT/IIoT
Flexibles Asset Discovery	aktiv und passiv
SaaS & On-Premise	
Compliance Unterstützung	z.B. KRITIS, ISO, NIS2
Integrierte Secure Remote Access Lösung	keine Insellösung nötig

Claroty schützt OT- und IoT-Umgebungen, wo klassische IT-Security versagt. Mit voller Transparenz, sicherem Fernzugriff und aktiver Bedrohungserkennung hilft Claroty unseren Kunden, Ausfälle und Angriffe zu verhindern – und gleichzeitig Compliance-Anforderungen zu erfüllen. **Für bessere Cyber- und operative Resilienz.**

Ihr Ansprechpartner:

Lucca Ruhland

Security & Monitoring Specialist

✉