Sichtbarkeit und Schutz für die Produktion.
OT-/IoT-Security – passiv und rückwirkungsfrei.

OT-/IoT-Security schützt vernetzte Produktions- und IoT-Umgebungen, in denen Ausfälle und Manipulationen besonders kritisch sind. Argos Security bringt Sichtbarkeit und Schutz in Umgebungen, die klassische IT-Security oft nicht abdeckt.

>600	<15 Min	≤30 Min	seit 1999	ISO 27001	100 %
Kunden	Erkennung (MTTD)	Rückmeldung (SLA)	Managed Security	TÜV-SÜD-zertifiziert	souveränes CDC ab Q1/2027

Das leistet der Service für Sie.

Asset-Sichtbarkeit

Vollständige Sichtbarkeit und Inventarisierung aller OT- und IoT-Assets – oft die erste komplette Bestandsaufnahme eines gewachsenen Anlagennetzes.

Netz-Segmentierung

Saubere Trennung zwischen IT und OT begrenzt Angriffswege und schützt vor Seitwärtsbewegung in sensible Produktionsumgebungen hinein.

Passive Überwachung

Anomalie- und Bedrohungsüberwachung erfolgt passiv und rückwirkungsfrei – ohne Risiko für Verfügbarkeit und Safety langlebiger, empfindlicher Systeme.

SOC-Integration

OT-Ereignisse fließen in ein zentrales Security-Monitoring und werden im Ernstfall koordiniert beantwortet – ergänzt um Risikoüberblick und transparentes Reporting.

Für wen: Für Industrie und Produktion mit vernetzten Maschinen und Steuerungssystemen, KRITIS-Betreiber mit hohen NIS-2-Anforderungen sowie Betreiber wachsender IoT-/OT-Landschaften und vernetzter Medizin- oder Versorgungstechnik.

Ein unbedachter Scan kann Anlagen stoppen oder Menschen gefährden – klassische IT-Security passt hier nicht. Argos überwacht passiv und rückwirkungsfrei, mit Blick auf Verfügbarkeit und Safety. KI-Agenten helfen, anomales Verhalten in großen Anlagenlandschaften früh zu erkennen – die Bewertung bleibt in Expertenhand.

Auf Seite 2: der direkte Vergleich mit dem klassischen Ansatz →

Ihr direkter Draht: +49 89 45 24 24-100 · kontakt@argos.security

Bildmotiv: KI-generiertes Symbolbild

Argos OT-/IoT-Security vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos OT-/IoT-Security
Methode	Aktive Scans gefährden Anlagen	Passiv und rückwirkungsfrei Verfügbarkeit und Safety im Vordergrund
Sichtbarkeit	Unvollständiges Bild des Anlagennetzes	Inventarisierung aller OT-/IoT-Assets
Angriffswege	IT und OT ohne saubere Trennung vernetzt	Segmentierung zwischen IT und OT Schutz vor Seitwärtsbewegung
Monitoring	OT bleibt blinder Fleck der IT-Security	Integration ins SOC-Monitoring Koordinierte Reaktion im Ernstfall
Compliance	NIS-2-/KRITIS-Anforderungen an OT offen	Nachweise für Produktionsumgebungen Transparentes Reporting

Ihr Leistungsumfang im Überblick

- Sichtbarkeit und Inventarisierung aller OT-/IoT-Assets
- Netz-Segmentierung zwischen IT und OT
- Passive, rückwirkungsfreie Anomalie-Überwachung
- Schutz vor Seitwärtsbewegung
- Risikobasierter Schwachstellen- und Risikoüberblick
- SOC-Integration und transparentes Reporting

Für Ihre Geschäftsleitung: Auswahlsorgfalt belegbar (ISO/IEC 27001 TÜV SÜD, seit 1999, >600 Kunden) · Überwachung erfüllbar (Reporting & Reviews) · SLAs vertraglich statt Best Effort.

Ihr Part: Ansprechpartner & Zugänge im Onboarding – Rollen, Freigaben und Eingriffstiefe werden gemeinsam festgelegt. Details (RACI, SLA-Matrix, AVV/TOM) im Erstgespräch.

Souverän. Deutsch. Nachweisbar.

- SOC-Betrieb aus München – nach deutschem Recht
- Datenhaltung auf Wunsch vollständig in Deutschland
- ISO/IEC 27001 zertifiziert (TÜV SÜD)
- Unterstützt NIS-2-, DORA- und ISO-27001-Nachweise
- DSGVO-konforme Verarbeitung – AVV (Art. 28), TOM & Unterauftragsverarbeiter-Übersicht auf Anfrage
- Ab Q1/2027: 100 % souveränes Cyber Defense Center

So starten Sie mit dem Service

01
Erstgespräch & Inventar

Wir erfassen Ihre Anlagenlandschaft und erstellen die vollständige Inventarisierung aller OT- und IoT-Assets – passiv und ohne Eingriff.

02
Segmentierung & Schutz

Auf Basis des Inventars werden IT und OT sauber getrennt, Angriffswege begrenzt und der Schutz vor Seitwärtsbewegung etabliert.

03
Überwachung im Betrieb

Kontinuierliche, rückwirkungsfreie Anomalieüberwachung – integriert ins SOC-Monitoring, mit koordinierter Reaktion und transparentem Reporting.

Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie OT-/IoT-Security auf Ihre Infrastruktur und Bedrohungslage zugeschnitten wird.



Dr. Nils Kaufmann
Chief Sales Officer

+49 89 45 24 24-100
kontakt@argos.security · www.argos.security

Mehr zur Leistung: argos.security/leistungen/ot-iot-security →

Termin buchen

Bildmotiv: KI-generiertes Symbolbild