Ein Alert ist noch kein Vorfall.
SOC as a Service aus München.

Argos Security betreibt Ihr Security Operations Center als Service: 24/7-Monitoring, Erkennung und Bewertung von Sicherheitsvorfällen – mit deutschsprachigen Analysten in München. Statt roher Alarme erhalten Sie bewertete, priorisierte Vorfälle mit klarer Handlungsempfehlung.

1.000+	<15 Min	24/7/365	2–4 Wochen	seit 1999	ISO 27001
Kunden	Erkennung (MTTD)	Monitoring aus München	bis zum Regelbetrieb	Managed Security	TÜV-SÜD-zertifiziert

Das leistet der Service für Sie.

24/7-Monitoring

Rund um die Uhr, 365 Tage im Jahr – mit Detection-Regeln, die aus der Threat Intelligence individuell auf Ihre Infrastruktur und Bedrohungslage kalibriert werden.

Bewertung statt Alarmflut

Jeder Alarm wird bewertet und priorisiert. Eskaliert wird nur, was ein echter Vorfall ist – mit Kontext und Handlungsempfehlung, damit Ihr Team handlungsfähig bleibt.

Erkennung unter 15 Minuten

Deutschsprachige Analysten in München, KI-/agentic-gestützte Analyse und eingespielte Eskalationswege – die Anbindung erfolgt in der Regel innerhalb von 2–4 Wochen.

Nachweisbar für Audits

Transparentes Reporting für Audit und Management, revisionssichere Dokumentation und belastbare Nachweise für NIS-2, KRITIS, DORA und ISO 27001.

Für wen: Für mittelständische Unternehmen mit **250 bis 5.000 Mitarbeitenden** in Deutschland, Österreich und der Schweiz, die kein eigenes 24/7-SOC aufbauen wollen – vom Unternehmen ohne eigenes Security-Team bis zur Organisation mit Nachweispflichten nach NIS-2, KRITIS, DORA oder ISO 27001.

Ein eigenes SOC ist für die meisten Unternehmen nicht wirtschaftlich zu betreiben: 24/7-Schichtbetrieb, knappe Spezialisten, ständige Regelpflege. **SOC as a Service schließt diese Lücke** – und ist zugleich die Grundlage des Cyber Defense Center. Auf Seite 2: der Vergleich.

Bildmotive: KI-generierte Symbolbilder

Argos SOC as a Service vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos SOC as a Service
Betrieb	Eigenes 24/7-Schichtteam aufbauen und halten	**Managed Service aus dem SOC in München** Deutschsprachige Analysten, kein Schichtbetrieb bei Ihnen
Alarme	Alarme werden ungefiltert weitergeleitet	**Bewertet und priorisiert vor der Eskalation** Nur echte Vorfälle erreichen Ihr Team
Erkennung	Standardregeln, selten nachgeschärft	**Auf Ihre Bedrohungslage kalibriert** Erkennungszeit (MTTD) unter 15 Minuten
Ausbau	Jede weitere Fähigkeit ein eigenes Projekt	**Modular zum Cyber Defense Center** IR-Retainer, IR-Readiness, Threat Intelligence
Compliance	Nachweise mühsam manuell erstellt	**Reporting und revisionssichere Ablage** Unterstützt NIS-2-, KRITIS- und DORA-Nachweise

Ihr Leistungsumfang im Überblick

- ✓ 24/7-Monitoring aus dem Security Operations Center in München
- ✓ Individuell kalibrierte Detection-Regeln aus der Threat Intelligence
- ✓ Bewertung und Priorisierung jedes Alarms – Erkennungszeit (MTTD) unter 15 Minuten
- ✓ Eskalation echter Vorfälle mit klarer Handlungsempfehlung
- ✓ Transparentes Reporting für Audit und Management
- ✓ Modularer Ausbau zum Cyber Defense Center (IR-Retainer, IR-Readiness, Threat Intelligence)

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

Für Ihre Geschäftsleitung: Auswahlsorgfalt belegbar (ISO/IEC 27001 TÜV SÜD, seit 1999, 1.000+ Kunden) · Überwachung erfüllbar (Reporting & Reviews) · Erkennung und Eskalation vertraglich geregelt statt Best Effort.

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

So starten Sie mit dem Service

01

Erstgespräch & Scoping

Wir erfassen Ihre IT-Landschaft, Log-Quellen und Compliance-Anforderungen und definieren den Umfang Ihres SOC.

02

Anbindung & Kalibrierung

Log-Quellen werden angebunden, Detection-Regeln auf Ihre Bedrohungslage kalibriert, Eskalationswege und Ansprechpartner festgelegt – in der Regel in 2–4 Wochen.

03

24/7-Regelbetrieb

Das SOC überwacht, bewertet und eskaliert rund um die Uhr – mit Reporting, Threat-Intelligence-Anreicherung und laufender Optimierung der Erkennung.

> *„Dank der professionellen und schnellen Hilfe können wir Vorfälle jederzeit und schnell bereinigen. Die umfassende und kompetente Beratung inklusive rechtlicher Betreuung ist unbezahlbar."*
>
> Sascha Prütz, Vorstand, WIIT AG

Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie SOC as a Service 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/soc-as-a-service →

Termin buchen

07-2026

Bildmotive: KI-generierte Symbolbilder