Angriffe stoppen, bevor sie beginnen.
Das Cyber Defense Center.

Threat Intelligence, Attack Surface Management, Incident-Response-Bereitschaft und 24/7-SOC-Betrieb – als ein Service, aus einer Hand. KI-gestützte Analyse, verantwortet von deutschsprachigen Analysten in München.

>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

Vier Bausteine. Ein Schutzschild.

SOC as a Service

24/7-Monitoring mit individuell auf Ihre Infrastruktur und Bedrohungslage kalibrierten Detection-Regeln – kein Alert-Weiterleiten, sondern bewertete, priorisierte Vorfälle.

IR-Retainer

Vertraglich garantierte Reaktionszeiten in vier SLA-Stufen – erste Rückmeldung in bis zu 30 Minuten. Im Ernstfall reagieren eingespielte IR-Teams mit bis zu 20 Spezialisten.

IR-Readiness

Jährlicher Cyber Resilience Check, zwei IR-Plan-Workshops und eine Tabletop Exercise – Ihre Organisation kennt den Ernstfall, bevor er eintritt.

Threat Intelligence

Threat Briefings nach dem Industriestandard MITRE ATT&CK, Attack Surface Management und Darknet-Monitoring – bis zur Ransomware-Frühwarnung.

Für wen: Unternehmen im DACH-Raum, die eine proaktive, umfassende Cyberabwehr aus einer Hand suchen – statt nur reaktiver Erkennung.

Klassische SOC-Anbieter liefern Alerts – die Bewertung bleibt bei Ihnen. Das CDC liefert aktiv gemanagte Sicherheit: Angriffswege werden geschlossen, bevor sie ausgenutzt werden, und im Ernstfall steht die komplette Reaktionskette bereit – von der Eindämmung über Forensik bis zur entscheidungsreifen Vorbereitung Ihrer NIS-2-konformen Meldung.

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

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

Argos CDC vs. klassisches SOC

der Vergleich auf einen Blick

Kriterium	Klassisches SOC	Argos Cyber Defense Center
Ansatz	Reaktiv – Alarm, wenn der Angriff läuft	**Proaktiv:** Bedrohungslage & Angriffsoberfläche werden laufend analysiert
Meldepflichten	Nicht enthalten	**Unterstützung bei Ihrer fristgerechten NIS-2- & DSGVO-Meldung** – vorbereitet und dokumentiert; die Meldung bleibt bei Ihnen
Reaktionszeit	Ticketprozess, Best Effort	**Vertragliche SLA-Stufen** – erste Rückmeldung in bis zu 30 Minuten
Ernstfall	IR muss extern zugekauft werden	**Integrierte IR-Teams mit bis zu 20 Spezialisten** – Abläufe vorab geklärt
Team	Anonymer Follow-the-Sun-Betrieb	**Deutschsprachige Analysten in München**, fester Lead im IR-Retainer
Datenhaltung	Global verteilt	**Auf Wunsch vollständig in Deutschland**

Ihr Leistungsumfang im Überblick

- Bewertete, priorisierte Incidents statt Alert-Flut
- Regelmäßige Threat Briefings zu Ihrer Bedrohungslage
- Attack Surface Management & Darknet-Monitoring (neun Kategorien)
- Jährlicher Cyber Resilience Check + Tabletop Exercise
- Fester IR-Lead, transparentes Reporting für Audit & Management

> **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 CDC

01
Kickoff & Notfallbereitschaft

Schutzbedarf definiert, Eskalationswege festgelegt, Notfall-Hotline eingerichtet.

02
Anbindung & Kalibrierung

Onboarding ans SOC in der Regel in 2–4 Wochen – Detection-Regeln werden auf Ihre Infrastruktur kalibriert.

03
Aktiv gemanagte Sicherheit

24/7-Regelbetrieb mit Threat Briefings und regelmäßigen Reviews – gemanagt, nicht nur dokumentiert.

> *„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 das Cyber Defense Center auf Ihre Infrastruktur und Bedrohungslage kalibriert wird.

Dr. Nils Kaufmann
Chief Sales Officer

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

Case Study: Studiosus Reisen →

Termin buchen