Angriffe kennen keine Tool-Grenzen. Managed XDR aus dem Argos SOC.

Managed XDR verbindet die Erkennung über Endpoint, Netzwerk, Cloud und Identität zu einem korrelierten Gesamtbild. Argos betreibt XDR als Managed Service und überwacht, korreliert und reagiert 24/7 aus dem SOC – mit klaren Eskalationen und Response.

>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.

Erkennung über Ebenen

Ebenenübergreifende Erkennung über Endpoint, Netzwerk, Cloud und Identität – einzelne Signale werden zu einem zusammenhängenden Angriffsbild korreliert.

24/7 aus dem SOC

Deutschsprachige Analysten überwachen und reagieren rund um die Uhr aus dem Cyber Defense Center in München – mit klarer Eskalation und Reporting.

Aktive Eindämmung

Managed Detection and Response mit aktiver Eindämmung stoppt Bedrohungen koordiniert, bevor sie sich weiter über Ihre Umgebung ausbreiten können.

Threat Hunting

Proaktives Threat Hunting deckt verborgene Bedrohungen auf, die einzelne Tools übersehen – ergänzt um kontinuierliche Optimierung der Erkennungslogik.

Für wen: Für Unternehmen, die komplexe, mehrstufige Angriffe zuverlässig erkennen und koordiniert darauf reagieren wollen.

Moderne Angriffe halten sich nicht an Tool-Grenzen – einzelne Lösungen sehen jeweils nur einen Ausschnitt. Argos führt die Telemetrie aller Ebenen zusammen und macht mehrstufige Angriffe sichtbar, die sonst durchrutschen. KI-Agenten korrelieren und priorisieren, 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

Argos Managed XDR vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos Managed XDR
Sichtfeld	Isolierte Tools sehen nur Ausschnitte	**Korreliertes Bild über alle Ebenen.** Endpoint, Netzwerk, Cloud und Identität.
Mehrstufigkeit	Laterale Bewegungen bleiben unsichtbar	**Mehrstufige Angriffe werden sichtbar.** Signale werden zum Angriffsbild verknüpft.
Reaktion	Alarm ohne koordinierte Antwort	**MDR mit aktiver Eindämmung.** 24/7-Response aus dem SOC.
Alarmflut	Unpriorisierte Alarme binden das Team	**KI-gestützte Priorisierung.** Die Bewertung bleibt in Expertenhand.
Optimierung	Statische Erkennungsregeln veralten	**Erkennungslogik wird laufend optimiert.**

Ihr Leistungsumfang im Überblick

- Erkennung über Endpoint, Netzwerk, Cloud und Identität
- Korrelation einzelner Signale zum Angriffsbild
- 24/7-Monitoring und Response aus dem SOC
- Managed Detection and Response mit aktiver Eindämmung
- Proaktives Threat Hunting
- Klare Eskalation, Reporting und laufende Optimierung

> **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
Analyse und Anbindung

Argos analysiert Ihre IT-Landschaft und bindet die Telemetrie aus Endpoint, Netzwerk, Cloud und Identität an das SOC an.

02
Korrelation und Tuning

Die Erkennungslogik wird auf Ihre Umgebung abgestimmt; Signale aller Ebenen werden zu einem zusammenhängenden Angriffsbild korreliert.

03
24/7-Regelbetrieb

Das SOC überwacht rund um die Uhr, dämmt Bedrohungen aktiv ein und optimiert die Erkennung kontinuierlich – mit klarer Eskalation und Reporting.

> *„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 Managed XDR 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/managed-xdr →

Termin buchen