Angriffspfade sehen, bevor Angreifer sie nutzen. Continuous Threat Exposure Management.

CTEM macht kontinuierlich sichtbar, wie ein Angreifer zu Ihren kritischen Systemen gelangen könnte – und priorisiert die wenigen Stellen mit der größten Wirkung. Argos bindet die Erkenntnisse direkt an das 24/7-Cyber-Defense-Center an.

>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.

Angriffspfad-Modell

Kontinuierliche Modellierung der realen Angriffspfade zu Ihren kritischen Assets – mit Asset- und Identitäts-Kontext statt isolierter, gleichrangiger Schwachstellenlisten.

Choke-Point-Analyse

Identifikation der wenigen Stellen, an denen ein Eingriff die größte Hebelwirkung hat – risikobasiert priorisiert, damit Ihr Team an den wirklich kritischen Risiken arbeitet.

Validierung & Maßnahmen

Argos prüft, welche Pfade real ausnutzbar sind und die größte Wirkung hätten, leitet priorisierte Maßnahmen ab und begleitet die Unterbrechung der kritischsten Angriffspfade.

CDC-Integration

Die Erkenntnisse fließen direkt in Priorisierung und Monitoring des 24/7-Cyber-Defense-Centers ein – proaktive Härtung und reaktive Erkennung greifen ineinander.

Für wen: Für Organisationen, die ihre Angriffsfläche proaktiv und kontinuierlich reduzieren wollen, statt nur punktuell zu scannen – von NIS-2- und KRITIS-Unternehmen über den Finanzsektor (DORA) bis zu Automotive und TISAX.

Ein Scanner listet Schwachstellen – gleichrangig, punktuell und ohne Bezug zu Ihren kritischen Assets. CTEM zeigt die realen Angriffspfade zu Ihren kritischen Assets und priorisiert die wenigen Choke Points mit der größten Wirkung – fortlaufend neu bewertet, sobald sich Ihre Umgebung ändert.

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

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

Argos Continuous Threat Exposure Management (CTEM) vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos Continuous Threat Exposure Management (CTEM)
Sichtweise	Isolierte Schwachstellen, gleichrangig gelistet	Reale Angriffspfade zu kritischen Assets mit Asset- und Identitäts-Kontext
Priorisierung	Endlose Listen ohne klare Reihenfolge	Choke Points mit größter Wirkung risikobasiert statt gleichrangig
Frequenz	Punktuelle Scans, oft nur einmal im Jahr	Kontinuierliche Neubewertung sobald sich Ihre Umgebung ändert
Umsetzung	Analyse endet mit dem Bericht	Begleitung bis zur Unterbrechung der kritischsten Angriffspfade
Betrieb	Ergebnisse bleiben vom Monitoring entkoppelt	Direkte CDC-Integration Erkenntnisse fließen ins 24/7-Monitoring ein

Ihr Leistungsumfang im Überblick

- Kontinuierliche Angriffspfad-Modellierung
- Risikobasierte Priorisierung und Choke-Point-Analyse
- Validierung real ausnutzbarer Angriffspfade
- Konkrete, priorisierte Handlungsempfehlungen
- Verständliches Exposure-Reporting
- Anbindung an das 24/7-Cyber-Defense-Center

> **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
Scoping & Discovery

Wir legen fest, welche Assets und Prozesse wirklich kritisch sind, und erfassen anschließend Angriffsflächen, Schwachstellen und mögliche Pfade.

02
Priorisierung & Validierung

Angriffspfade werden bewertet, die kritischsten Choke Points priorisiert – und geprüft, welche Pfade real ausnutzbar die größte Wirkung hätten.

03
Mobilisierung

Maßnahmen werden umgesetzt, die Exposure wird kontinuierlich neu bewertet. Die Erkenntnisse fließen in Priorisierung und Monitoring des CDC ein.

Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie Continuous Threat Exposure Management (CTEM) 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/ctem →

Termin buchen