Angriffe sichtbar, bevor Schaden entsteht.
SIEM as a Service aus dem 24/7-SOC.

Ein SIEM bündelt sicherheitsrelevante Log- und Ereignisdaten aus Ihrer gesamten IT zentral und macht verdächtige Muster sichtbar. Argos Security betreibt Ihr SIEM als Managed Service – korreliert, kalibriert und eskaliert rund um die Uhr aus dem SOC.

>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.

Zentrale Log-Aggregation

Sicherheitsrelevante Logs, Events und Verhaltensmuster aus Ihrer gesamten IT laufen zentral zusammen – eine Sicht statt verteilter Insel-Tools über alle Standorte.

Echtzeit-Korrelation

Echtzeit-Korrelation und Anomalie-Erkennung führen verteilte Spuren zusammen und machen Angriffe sichtbar, bevor Schaden entsteht – statt erst im Schadensfall.

Kalibrierte Detection

Detection-Regeln werden auf Ihre Bedrohungslage kalibriert und kontinuierlich optimiert – angereichert mit Threat Intelligence aus dem Cyber Defense Center.

24/7-Alarmierung

Alarmierung und Eskalation erfolgen aus dem 24/7-SOC: Analysten bewerten die Lage, sodass aus Alarmen belastbare Vorfallentscheidungen werden – ohne Alarmflut.

Für wen: Für Unternehmen, die zentrale Sichtbarkeit über ihre IT-Sicherheitslage brauchen und Angriffe früh erkennen wollen – etwa Mittelstand ohne eigenes SOC, NIS-2- und KRITIS-Organisationen sowie compliance-getriebene Unternehmen.

Ein selbst betriebenes SIEM erzeugt vor allem Daten und Alarme – die Bewertung bleibt an Ihrem Team hängen. Argos übernimmt Korrelation, Regelkalibrierung, Bewertung und Eskalation aus dem 24/7-SOC. KI-Agenten unterstützen beim 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 SIEM as a Service vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos SIEM as a Service
Betrieb	Eigenbetrieb bindet Team und Know-how	**Managed Service aus dem 24/7-SOC** Deutschsprachige Analysten aus München
Alarme	Alarmflut ohne Bewertung und Kontext	**Belastbare Vorfallentscheidungen** Bewertung und Eskalation durch Experten
Regeln	Statische Standard-Regeln	**Auf Ihre Bedrohungslage kalibriert** Kontinuierlich optimiert
Sichtbarkeit	Insel-Tools, über die IT verteilte Spuren	**Zentrale Sicht auf die gesamte IT** Angereichert mit Threat Intelligence
Compliance	Nachweise mühsam manuell erstellt	**Reporting und revisionssichere Ablage** Unterstützt NIS-2- und KRITIS-Nachweise

Ihr Leistungsumfang im Überblick

- Zentrale Log-Aggregation über die gesamte IT
- Echtzeit-Korrelation und Anomalie-Erkennung
- Auf Ihre Bedrohungslage kalibrierte Detection-Regeln
- Alarmierung und Eskalation aus dem 24/7-SOC
- Compliance-Reporting und revisionssichere Aufbewahrung
- Threat-Intelligence-Anreicherung 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
Erstgespräch & Scoping

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

02
Anbindung & Kalibrierung

Log-Quellen werden angebunden, Detection-Regeln auf Ihre Bedrohungslage kalibriert und die Eskalationswege ins SOC eingerichtet.

03
24/7-Regelbetrieb

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

> *„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 SIEM 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/siem →

Termin buchen