Reagieren in Sekunden statt Stunden.
SOAR – Automatisierung im Sicherheitsbetrieb.

SOAR (Security Orchestration, Automation and Response) automatisiert wiederkehrende Reaktionsabläufe im Sicherheitsbetrieb. Argos entwickelt und betreibt Playbooks, die Geschwindigkeit und Konsistenz in Ihr Vorfallmanagement bringen und Ihr Team entlasten.

>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.

Automatisierte Playbooks

Playbooks übernehmen Standardschritte von der Anreicherung eines Alarms bis zur Ersteindämmung – etwa Isolierung oder Sperrung – in geprüfter Qualität.

Threat-Intel-Anreicherung

Jeder eingehende Alarm wird automatisch mit Kontext aus Threat Intelligence angereichert, damit Analysten sofort mit vollem Bild arbeiten.

Nahtlose Integration

SOAR verbindet SIEM, EDR und Ticketing zu einem durchgängigen Reaktionsfluss – vorhandene Werkzeuge arbeiten zusammen statt nebeneinander.

Eskalation an Analysten

Komplexe Fälle werden automatisiert vorbereitet und mit vollem Kontext an Analysten übergeben – Freigabe und Bewertung bleiben in Expertenhand.

Für wen: Für Teams, bei denen Geschwindigkeit und Konsistenz im Vorfallmanagement entscheidend sind und die Routineaufgaben automatisieren wollen.

Bei einem Angriff entscheidet jede Minute – manuelle Reaktion kostet Zeit, den teuersten Faktor im Ernstfall. Argos automatisiert die wiederkehrenden Schritte mit geprüften Playbooks: Sie reagieren in Sekunden statt Stunden – in konsistenter Qualität, rund um die Uhr und unabhängig von der Auslastung.

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

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

Bildmotive: KI-generierte Symbolbilder

Argos SOAR vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos SOAR
Reaktionszeit	Manuelle Schritte kosten Stunden	**Reaktion in Sekunden** messbar kürzere MTTR
Konsistenz	Qualität schwankt mit Tageszeit und Auslastung	**Geprüfte Playbooks, gleiche Qualität** rund um die Uhr
Kontext	Analysten sammeln Informationen manuell	**Automatische Anreicherung** Threat Intelligence bei jedem Alarm
Werkzeuge	SIEM, EDR und Ticketing arbeiten isoliert	**Ein durchgängiger Reaktionsfluss** Integration statt Insellösungen
Expertise	Routine bindet Analysten, Komplexes wartet	**Analysten für komplexe Fälle frei** Freigabe bleibt in Expertenhand

Ihr Leistungsumfang im Überblick

- Entwicklung und Betrieb automatisierter Playbooks
- Alarm-Anreicherung aus Threat Intelligence
- Automatisierte Ersteindämmung wie Isolierung oder Sperrung
- Integration in SIEM, EDR und Ticketing
- Vorbereitete Eskalation komplexer Fälle an Analysten
- Kontinuierliche Playbook-Optimierung und MTTR-Messung

> **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 & Analyse

Sie klären mit Argos, welche Reaktionsabläufe sich wiederholen, welche Werkzeuge im Einsatz sind und wo Automatisierung am meisten Zeit spart.

02
Playbook-Entwicklung

Argos entwickelt die Playbooks, integriert SIEM, EDR und Ticketing und prüft jeden automatisierten Schritt, bevor er in den Betrieb geht.

03
Regelbetrieb

Playbooks laufen rund um die Uhr, Argos misst Reaktionszeiten, optimiert kontinuierlich und eskaliert komplexe Fälle mit vollem Kontext an Analysten.

> *„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 SOAR 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/soar →

Termin buchen

Bildmotive: KI-generierte Symbolbilder