# Schwachstellen dauerhaft im Griff.
# Vulnerability Management als laufender Prozess.

Vulnerability Management ist der laufende Prozess aus Erkennung, risikobasierter Priorisierung und Nachverfolgung von Schwachstellen. Argos Security betreibt den gesamten Zyklus – bis zur nachweislichen Behebung, mit klarer Sicht auf Ihre Fortschritte.

| | | | | | |
|---|---|---|---|---|---|
| >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.

### Kontinuierliches Scanning

Permanente Erkennung statt jährlicher Momentaufnahme: Ihre Systeme werden kontinuierlich auf Schwachstellen geprüft – während täglich neue Lücken bekannt werden.

### Risikobasierte Priorität

Statt endloser CVE-Listen stehen die richtigen Schwachstellen im Vordergrund: KI-Agenten korrelieren Funde mit Bedrohungsdaten und heben die kritischsten Lücken hervor.

### Konsequente Nachverfolgung

Jede Schwachstelle wird bis zur nachweislichen Behebung nachverfolgt – nahtlos integriert in Ihre Patch- und Change-Prozesse, in enger Abstimmung mit Ihrem Team.

### Reporting mit Trend

Regelmäßiges Reporting zeigt Fortschritt und Trend Ihrer Sicherheitslage und liefert eine jederzeit aktuelle Sicht auf Ihre Assets – auch als Nachweis für NIS-2 und KRITIS.

**Für wen:** Für Unternehmen, die Schwachstellen dauerhaft und risikobasiert im Griff behalten wollen – gewachsene IT-Landschaften, nach NIS-2 und KRITIS regulierte Organisationen und schlanke IT-Teams ohne eigene Ressourcen.

**Ein jährlicher Scan liefert eine lange Liste, die schnell veraltet – genau dort entstehen die Einfallstore.** Argos dreht das um: permanente Erkennung, risikobasierte Priorisierung und konsequente Nachverfolgung bis zur Behebung – als laufender Prozess statt einmaliger Prüfung.

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

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

# Argos Vulnerability Management vs. klassischer Ansatz

der Vergleich auf einen Blick

| Kriterium | Klassischer Ansatz | Argos Vulnerability Management |
|---|---|---|
| **Rhythmus** | Jährlicher Scan, Liste veraltet schnell | **Kontinuierliches Scanning** Permanente Erkennung neuer Schwachstellen |
| **Priorisierung** | Endlose CVE-Listen ohne Kontext | **Risikobasiert statt bloßer Menge** Funde mit Bedrohungsdaten korreliert |
| **Nachverfolgung** | Behebung bleibt offen, niemand prüft nach | **Bis zur nachweislichen Behebung** |
| **Integration** | Losgelöst von Patch- und Change-Prozessen | **Nahtlos in Ihre Prozesse eingebunden** Umsetzung in enger Abstimmung mit Ihrem Team |
| **Compliance** | Kein Nachweis laufenden Managements | **Nachweis für NIS-2 und KRITIS** Regelmäßiges Reporting mit Trend |

## Ihr Leistungsumfang im Überblick

- Kontinuierliches Schwachstellen-Scanning
- Risikobasierte Priorisierung statt endloser CVE-Listen
- Nachverfolgung bis zur nachweislichen Behebung
- Regelmäßiges Reporting mit Trend
- Integration in Ihre Patch- und Change-Prozesse
- Jederzeit aktuelle Sicht auf Ihre Assets

> **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**

Wir erfassen Ihre IT-Landschaft und Assets und definieren Scope, Scan-Rhythmus und die Anbindung an Ihre Patch- und Change-Prozesse.

### 02
**Aufbau & Kalibrierung**

Argos richtet das kontinuierliche Scanning ein und kalibriert die risikobasierte Priorisierung auf Ihre Systeme und Bedrohungslage.

### 03
**Regelbetrieb**

Permanente Erkennung, Priorisierung und Nachverfolgung bis zur Behebung – mit regelmäßigem Reporting und aktueller Sicht auf Ihre Assets.

## Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie Vulnerability Management 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/vulnerability-management →

Termin buchen