

Rund um die Uhr geschützt – mit Security Operations von agilimo.

Cybersicherheit mit System: 24/7-Überwachung, automatisierte Forensik und skalierbare Services für Ihr Unternehmen.

Wenn jede Sekunde zählt: Wir halten Sie handlungsfähig – auch im Ernstfall.

IT-Systeme sind heute permanent im Visier von Cyberkriminellen – und Angriffe sind oft nur schwer erkennbar. Die Folgen reichen von Betriebsunterbrechung bis zur Existenzbedrohung.

Ein Security Operations Center (SOC) bietet die nötige Sichtbarkeit und Reaktionsfähigkeit. Als externes SOCaaS (Security Operations Center as a Service) sorgt agilimo für proaktive Abwehrmaßnahmen – skalierbar, rund um die Uhr verfügbar und vollständig in Deutschland betrieben.

Für wen ist ein SOC sinnvoll?

Pflicht für einige. Nützlich für alle mit erhöhtem Schutzbedarf.

- Organisationen der kritischen Infrastruktur (KRITIS)
- Mittelständische Unternehmen mit wachsendem Risiko
- Firmen mit 24/7-Betriebsanforderung
- Organisationen, die sich nicht auf einfache Schutzsoftware verlassen wollen
- Unternehmen mit NIS2-Verpflichtung

Ihre Vorteile mit SOCaaS

agilimo als Managed Security Service Provider (MSSP):

- 24/7-Überwachung durch deutsches SOC
- Automatisierte Cyber-Forensik und Eskalation
- Erfüllung von BSI/NIS2/ISO27001-Anforderungen
- Schnelle Reaktionszeiten auf sicherheitsrelevante Vorfälle
- Integration bestehender Systeme (Firewalls etc.)
- Proaktive Threat Intelligence und Darknet-Monitoring
- Skalierbarkeit von Startups bis Enterprise-Umgebungen
- Transparente Kosten pro Endpoint

Cybersecurity – made in Germany

agilimo ist zertifizierter Spezialist für hochsichere IT-Infrastrukturen und wurde mehrfach als TOP-Innovator im deutschen Mittelstand ausgezeichnet. Unser SOC-Team vereint moderne Detection-Technologie mit menschlicher Expertise – und entwickelt maßgeschneiderte, mehrstufige Sicherheitskonzepte unter Berücksichtigung der Cyber-Kill-Chain.



SOCaaS von agilimo

Drei Module – Ein Ziel: Ihre Sicherheit.

Unsere modularen SOCaaS-Pakete wachsen mit Ihrem Bedarf – vom schnellen Einstieg bis zur hoch-regulierten Umgebung. Alle Module basieren auf deutschem Hosting, BSI-orientierter Umsetzung und kompromissloser Qualität „Made in Germany“.

	SOC Essential	SOC Standard	SOC Premium
Überwachung von Systemen mittels EDR	☑	☑	☑
Kundendashboard mit Übersicht sicherheitsrelevanter Ereignisse	☑	☑	☑
24/7 Überwachung durch das SOC	☑	☑	☑
Automatisierte Ticket-Erstellung bei verifizierten sicherheitsrelevanten Vorfällen	☑	☑	☑
Ein quartalsweiser Service-Report	☑	☑	☑
Darkscan Essentials	☑	☑	☑
30 Tage Datenspeicherung	☑	☑	☑
Datenspeicherung von bis zu 180 Tagen	optional	☑	☑
Asgard Agent (Incident Response Essential)	optional	☑	☑
Überwachung von Systemen mittels XDR	-	☑	☑
Monatliche Reports und Review-Meetings	-	☑	☑
Einbindung in E-Mail-Verteiler	-	☑	☑
Logfile-Analyse inkl. Installation des Log Collectors	-	☑	☑
Entwicklung und Einsatz dedizierter Detection Rules	-	☑	☑
Anbindung gängiger Systeme	-	☑	☑
Darkscan Premium	optional	optional	☑
Kontinuierliche forensische Scans mit dem APT-Scanner THOR	optional	optional	☑
Entwicklung und Anbindung von Custom Integrations	-	-	☑
Zusätzliche Reports auf Anfrage	-	-	☑
SLA bei kritischen Vorfällen innerhalb von 15–30 Minuten	-	-	☑
Telefonische Erreichbarkeit des SOC-Teams	-	-	☑
Proaktives Threat Hunting	-	-	☑
Volle Integration und Betrieb vorhandener SIEM-/SOAR-Systeme	-	-	☑
Kundendashboard mit Live-Daten in Echtzeit	-	-	☑
Single Point of Contact (SPOC)	-	-	☑
Incident Response bei realen Vorfällen	optional	optional	optional

Bereit für mehr Sicherheit und Reaktionsstärke?

Unsere Experten beraten Sie individuell – oder Sie starten direkt mit Ihrem persönlichen SOCaaS-Paket. Mehr Informationen zu Kosten finden Sie unter: www.agilimo.de/soc