# Sicherheitsüberwachung aus Deutschland: das CGI SOC

Die Zahl von Cyberattacken nimmt kontinuierlich zu. Minimieren Sie gezielt und zuverlässig Ihre Risiken mit dem in Deutschland betriebenen CGI Security Operations Center (SOC) – rund um die Uhr, das ganze Jahr. So erhalten Sie mit Sicherheit Ihre Handlungsfähigkeit.

## Bereit, wenn es darauf ankommt

Das CGI SOC bietet mehr als nur technisches Monitoring. Wir führen intelligente Bedrohungsanalysen durch, reagieren schnell und verfügen über die notwendige regulatorische Expertise – maßgeschneidert für Ihre Branche.

Unsere sicherheitsüberprüften SOC-Teams arbeiten rund um die Uhr und aus Deutschland heraus; gleichzeitig sind wir durch die globale Vernetzung mit unseren internationalen Kolleginnen und Kollegen immer auf dem aktuellen Stand und kennen die Bedrohungslage.

Dabei passen wir unsere flexibel skalierbaren Leistungen Ihren Anforderungen an – auch wenn Sie im Bereich kritischer Infrastrukturen tätig sind. Durch unseren Shared-Ansatz profitieren Sie in jedem Fall von einer hohen Kosteneffizienz.

### Unsere SOC-Kompetenzen im Einsatz

Gemeinsam gestalten wir Ihre SOC-Leistungen – mit modularen Services, exakt abgestimmt auf Ihre Ziele und die jeweilige Bedrohungslage.

**Protective Monitoring & Triage – Bedrohungen frühzeitig erkennen und einordnen**

Das CGI SOC überwacht Ihre IT-Landschaft rund um die Uhr. So erkennen wir Bedrohungen in nahezu Echtzeit, analysieren verdächtige Aktivitäten und bewerten potenzielle Vorfälle frühzeitig. Mithilfe von Sicherheitsanalysen und aktuellen Informationen über Gefahren identifizieren und behandeln wir Angriffsvektoren, bevor sie zum Problem werden.

## Ihre Vorteile mit dem CGI SOC:

**Zertifiziert und einsatzbereit**

Wir unterstützen Sie bei der Einhaltung von NIS2, DORA und anderen gesetzlichen Vorgaben – mit dokumentierten Prozessen, geprüften Sicherheitsmechanismen und einer zuverlässigen Incident Response. Unsere zertifizierten deutschsprachigen Fachkräfte verfügen auch über Sicherheitsfreigaben für den Einsatz in hochsensiblen Umgebungen.

**Echte 24/7-Verfügbarkeit**

Unsere Sicherheitsexpertinnen und -experten sind das gesamte Jahr für Sie im Einsatz – Tag und Nacht. „Eyes-on-Screen“ gewährleisten sie eine kontinuierliche Überwachung und schnelle Reaktion im Ernstfall.

**Auf Ergebnisse fokussiert**

Wir erkennen Angriffe frühzeitig, senken die Risiken und sichern Ihre Betriebsfähigkeit – mit klaren Verantwortlichkeiten und greifbaren Resultaten, auch im Krisenfall.

**Managed Detection & Response – Sicherheitsvorfälle gezielt stoppen und kontrollieren**

Bei einem Vorfall zählt jede Sekunde. Unser SOC-Team reagiert rasch, strukturiert und gezielt. Durch definierte Prozesse und Playbooks mit unmittelbaren Maßnahmen minimieren wir Schäden und sichern Ihre Betriebsfähigkeit. Wir finden die Ursachen, optimieren Ihre Sicherheitsstrategie und unterstützen Sie mit regelmäßigen Reports, damit Sie fundierte Entscheidungen treffen.

**Threat Hunting – versteckte Bedrohungen aufdecken**

Wir warten nicht auf Alarme, sondern suchen aktiv nach Gefahren. Durch die Analyse verdächtiger Aktivitäten und Anomalien in Ihrer Infrastruktur entdecken wir Angriffsversuche, bevor sie Schaden anrichten. Dafür kombinieren wir aktuelle Cyber Threat Intelligence mit automatisierten Tools, manueller Analyse und modernen KI-Ansätzen – für ein Sicherheitsniveau, das auch zukünftigen Risiken gerecht wird.

**Incident Retainer – im Ernstfall unmittelbar und planvoll reagieren**

Im Krisenfall stehen wir bereit: Mit unserem Incident Retainer Service erhalten Sie unmittelbar direkte Hilfe. Binnen kürzester Zeit unterstützen unsere Vorfallsexpertinnen und -experten Sie bei der strukturierten Bewertung des Vorfalls, der initialen Eindämmung und der Umsetzung geeigneter kurz- und mittelfristiger Reaktionsmaßnahmen – schnell, verlässlich und nachhaltig.

**SIEM- Architecture & Engineering – Sicherheit auf aktuelle Risiken ausrichten**

Wir entwickeln, implementieren und betreiben Ihre SIEM-Umgebung so, dass sicherheitsrelevante Ereignisse zentral überwacht und analysiert werden können. Wir integrieren Datenquellen, definieren intelligente Korrelationsregeln und passen die Lösung laufend an die sich kontinuierlich ändernde Bedrohungslandschaft und neue regulatorische Anforderungen an.

**Vulnerability Management – Schwachstellen beheben**

Unsere kontinuierliche Schwachstellenanalyse identifiziert Sicherheitslücken frühzeitig. Wir priorisieren Risiken und begleiten Sie bei der Umsetzung von Maßnahmen im Rahmen Ihres Patch-Managements. Mit unseren regelmäßigen Reports behalten Sie immer den Überblick.

## Zeit für den nächsten Schritt in der Cybersecurity

Ob Sie bestehende Strukturen optimieren oder einen ganzheitlichen SOC-Ansatz etablieren möchten – wir unterstützen Sie mit fundierter Expertise, passenden Services und dem klaren Blick auf regulatorische Anforderungen.

**Lassen Sie uns gemeinsam herausfinden, wie wir Ihre Sicherheit auf das nächste Level heben.**

## Über CGI

**Insights you can act on**

Als globaler Dienstleister für IT- und Geschäftsprozesse entwickeln wir für unsere Kunden ergebnisorientierte Strategien für ihre digitale Transformation und unterstützen sie mit End-to-End-Services, durch die sie greifbare Ergebnisse erzielen.

Unsere weltweit 94.000 Mitarbeitenden entwickeln innovative Lösungen wie KI entlang der gesamten Wertschöpfungskette und werden im Hinblick auf Zeit- und Budgettreue regelmäßig mit Bestnoten bewertet.

**Weitere Informationen**

Hauke Noormann
Director Consulting Delivery
hauke.noormann@cgi.com

Sebastian Jansen
Director Consulting Services
sebastian.jansen@cgi.com

https://www.cgi.com/de/cybersecurity