



Security Operations

Security Operations Center (SOC)

**FRÜHZEITIGE ERKENNUNG  
& SOFORTIGE REAKTION  
FÜR IHRE INFRASTRUKTUR**

KRITIS-konforme Sicherheitsservices aus Deutschland

## SIND IHRE DATEN UND NETZWERKE RUND UM DIE UHR GESCHÜTZT?

### **KRITIS-Security lässt sich nicht lizenzieren – aber outsourcen!**

Organisationen mit kritischen Infrastrukturen sind seitens des BSI mit besonderen regulatorischen Vorgaben konfrontiert. Sie müssen sicherstellen, dass sie unbeeinträchtigt arbeiten, damit es nicht zu Versorgungsengpässen, Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen kommt. Umfassende Massnahmen zur Informationssicherheit sind erforderlich, um die Anforderungen des IT-SiG 2.0 zu erfüllen sowie die verschiedensten Gefahren abzuwehren.

Oberstes Ziel ist es, unternehmenskritische Systeme inklusive industrieller Steuerungssysteme und eingebetteter Software von Geräten auch im Internet der Dinge vor Befall von Schadsoftware, Spionage oder missbräuchlicher Nutzung zu schützen.

Eine Vielzahl an Lösungen am Markt trägt dazu bei, die Sicherheit zu gewährleisten. Die Komplexität der verschiedenen Systeme und Lösungen ist jedoch gross. Die Kosten für Lizenzen und Personal sind sehr hoch, die Verfügbarkeit eigener qualifizierter Mitarbeiter ist unzureichend. Es fehlen ein durchgängiges Sicherheitsmanagement, die notwendige kontinuierliche Systemüberwachung und fundierte Analysen.

## OUTSOURCING IST EINE OPTION, ABER ... ... WIE ZUVERLÄSSIG IST DER OUTSOURCING-PARTNER WIRKLICH?

### **Anforderungen an ein risikofreies Outsourcing der Informationssicherheit:**

- Leistungsfähiger Anbieter im Bereich Managed Security Services
- Umfassendes Sicherheitsportfolio
- Minimum Tier-3-Rechenzentrum mit Option auf mehrere Standorte
- Betriebsstandorte der Rechenzentren in Deutschland
- Zertifizierte Service-Organisation
- Vollständige Service-Erbringung aus Deutschland
- Transparente Eigentümerstrukturen

### **Was tun?**

Unsere Antwort: Als Ihr Spezialist im Bereich Managed Services für kritische Infrastrukturen decken wir gemeinsam mit unseren Partnern sämtliche Anforderungen an ein sicheres und zuverlässiges Outsourcing ab. Wir sorgen in unserem Security Operations Center für Sicherheit rund um die Uhr. Dabei realisieren wir Ihre Sicherheitsanforderungen und -ziele zu monatlich kalkulierbaren Kosten.

**Einfach. Sicher. IS4IT Schweiz.**



# SECURITY OPERATIONS CENTER

## Unser Vorgehen

Auf Basis Ihrer definierten Sicherheitsanforderungen wird deren Abdeckung durch die im Einsatz befindlichen Lösungen evaluiert und bei Bedarf um entsprechende Werkzeuge ergänzt.

Grundlage eines erfolgreichen SOC ist eine datenschutzkonforme Netzwerkanalyse mithilfe von Werkzeugen. So kann nicht nur die IT-Sicherheit einzelner Netzwerke, sondern die Lage in mehreren Netzwerken zeitgleich überwacht werden. Sämtliche Meldungen Ihrer sicherheitsrelevanten Systeme werden in einer SIEM-Appliance (Security Information and Event Management) in Echtzeit zusammengefasst. Diese erlaubt es unseren Security-Experten, sowohl ein Monitoring als auch eine Analyse durchzuführen, um verborgene Bedrohungen zu erkennen und abzuwehren. Zur Optimierung und Automatisierung der Incident-Response-Prozesse kommt Security Orchestration, Automation and Response (SOAR) zum Einsatz.



## Das Angebot

- Analyse und Definition Ihrer Sicherheitsanforderungen
- Übernahme vorhandener Security-Lösungen und Inbetriebnahme weiterer Komponenten bei Bedarf
- Betrieb aller notwendigen Systeme über abgesicherten Fernzugriff
- Einsatz einer BSI-zugelassenen Datendiode zur Gewährleistung von Zonenkonzepten
- Betrieb der SIEM-Infrastruktur erfolgt auf Ihren Systemen (On-Prem, Cloud oder hybrid), sodass die Daten Ihr Haus nicht verlassen müssen
- Betrieb der SOAR-Infrastruktur erfolgt im Security Operations Center (SOC) unserer Mutter, der IS4IT GmbH, das in einem nach ISO 9001:2015, ISO/IEC 27001 und ISAE 3402 zertifizierten T3-Plus-Rechenzentrum in Deutschland betrieben wird
- Umsetzung auf Basis vereinbarter SLAs (24x7) gemäß Ihren Betriebszeiten
- Umfassendes Reporting für Ihr Management

## Ihr Nutzen

- Optimaler Schutz Ihrer kritischen Infrastruktur unter Einhaltung aller rechtlichen Vorgaben
- Risikominimierung durch punktgenaue Umsetzung Ihrer Anforderungen
- Schutz durch Experten und Entlastung Ihrer Mitarbeiter
- Umsetzung der BSI-Normen und -Regularien (SzA)
- Höchste Vertraulichkeit dank Geheimschutzbetreuung
- Keine direkte Zugriffsmöglichkeit durch ausländische Dienste oder Organisationen dank vollständiger Umsetzung in Deutschland
- Optimale Gewährleistung Ihrer Service Level Agreements
- Kosteneffiziente und -transparente Durchführung zu kalkulierbaren Kosten

## SOAR & SIEM

<b>Firewall</b>	<b>Honeypots</b>	<b>IPS</b>
<b>Netzwerk-Analysen</b>	<b>Mail Security</b>	
<b>Browsing Security</b>	... ..	

**Definierte Security-Anforderungen**

## UNSERE SECURITY-PARTNER

Wir setzen auf weltweit erfolgreiche und erprobte Sicherheitstechnologie, wenn es um die Realisierung kosteneffizienter und gleichzeitig modernster und ausgereifter Security-Lösungen entsprechend Ihren Anforderungen und Ihrem Kostenrahmen geht.



## WARUM IS4IT SCHWEIZ AG?

Die IS4IT Schweiz AG mit Sitz in Zug ist als spezialisierter IT-Dienstleister für Informationssicherheit in der Schweiz Teil der IS4IT-Unternehmensgruppe.

Als Cybersecurity-Spezialist richten wir uns mit unserem Full-Service-Angebot an Unternehmen und Organisationen mit erhöhtem IT-Schutzbedarf. Unser Cybersecurity-Lösungsportfolio deckt Themen wie Informationssicherheitsstrategien, Sicherheitsarchitekturen und -infrastrukturen, Defensive und Offensive Security bis hin zu Incident Management, Datenschutz und Zertifizierungen sowie Governance, Risk Management & Compliance (GRC) umfassend ab.

Die von uns konzipierten Lösungen können direkt umgesetzt und als Managed Services betrieben werden. Für verschiedene IT-Services wie Managed SOC, Managed SIEM, Managed SOAR oder Managed Data Protection greifen wir auf die KRITIS-konforme und zertifizierte Infrastruktur der IS4IT-Gruppe zurück, nutzen zertifizierte deutsche Rechenzentren und garantieren etablierte, sichere Strukturen und Prozesse. Auch eine Geheimschutzbetreuung ist möglich.

Wir übernehmen dabei für unsere Kunden stets die Gesamtkoordination und -verantwortung.

**Wir leben, was wir empfehlen ... tagtäglich!**

**Daher ist die IS4IT-Gruppe Ihr idealer Partner. Wir sollten uns kennenlernen.**



**IS4IT Schweiz AG**  
Allmendstrasse 1  
6300 Zug  
Schweiz  
telefon +41 41 7200090  
info@is4it.ch

IS4IT KRITIS GmbH  
Kraichgaublick 13  
74847 Obrigheim  
Deutschland  
telefon +49 6262 9262594  
info@is4it-kritis.de

IS4IT GmbH  
Grünwalder Weg 28b  
82041 Oberhaching  
Deutschland  
telefon +49 89 6389848-0  
info@is4it.de

IS4IT Cyber Security Austria GmbH  
Franz-Josefs-Kai 49/19  
1010 Wien  
Österreich  
telefon +43 676 889854401  
info@is4it.at

Zertifikate/Siegel der IS4IT KRITIS GmbH

