



## Pressemitteilung

### **SPIE lanciert sein SOC in der Schweiz**

**Bern, 26. Juni 2024** – SPIE Schweiz, eine Tochtergesellschaft der SPIE-Gruppe, dem unabhängigen europäischen Marktführer für multitechnische Dienstleistungen im Energie- und Kommunikationsbereich, gibt die Einführung seines SOC-Angebots (Security Operations Center) bekannt. Dieser umfassende Service bietet Schweizer Unternehmen jeder Grösse eine fortschrittliche Erkennung von Cyberangriffen, eine Überwachung rund um die Uhr sowie einen Informationsdienst über Cyberbedrohungen.

Dieses neue SOC-Angebot ist das Ergebnis einer strategischen Partnerschaft zwischen den beiden digitalen Dienstleistungsunternehmen von SPIE in der Schweiz und in Frankreich, die beide ihr Fachwissen und ihre Erfahrung im Bereich der Cybersicherheit eingebracht haben. In Frankreich betreibt SPIE ICS erfolgreich ein eigenes SOC, das über 100 Kunden in Frankreich und international betreut. In der Schweiz bietet SPIE ICS AG seit 2015 Lösungen und Dienstleistungen im Bereich Cybersicherheit an und legt dabei besonderes Augenmerk auf Risikobewertung, Compliance und Sensibilisierung.

#### **Portfolio durch 24/7-SOC-Lösung ergänzt**

In Fortsetzung ihrer auf Cybersicherheit ausgerichteten Strategie erweitert die SPIE ICS AG nun ihr Portfolio mit der Einführung ihrer Lösung namens «Core SOC». Dieses operative Sicherheitszentrum, ein Eckpfeiler des Angebots, bietet fortschrittliche Erkennungsdienste,

die rund um die Uhr verfügbar sind. Ergänzt durch eine flexible und agnostische SIEM/XDR<sup>1</sup>-Managementplattform wird es an die spezifischen Anforderungen jedes Kunden angepasst.

Dieser Service umfasst eine Informationsquelle für Cyberbedrohungen zur schnellen Aktualisierung der Erkennungsmodelle bei neuen Angriffen und eine proaktive Verfolgung von Bedrohungen, um eine Kompromittierung der Kundenumgebungen zu verhindern. Darüber hinaus lässt sich das SOC nahtlos in die bestehende Umgebung des Kunden integrieren und kann mit zusätzlichen SPIE-Diensten für eine verbesserte Erkennung in Industrienetzwerken ergänzt werden.

*«Mit der Einführung von «Core SOC» machen wir einen wichtigen Schritt, um die Sichtbarkeit und die Erkennungsrate von Cyberangriffen auf die digitalen Vermögenswerte unserer Kunden zu erhöhen. Indem wir unser lokales Fachwissen mit unseren globalen Ressourcen kombinieren, können wir einen robusten, umfassenden und flexiblen Cybersicherheitservice anbieten», sagt Christophe Francey, Chief Technology Officer bei SPIE ICS AG. Er fügt hinzu: «Dieser Service stärkt unser Engagement, innovative Lösungen anzubieten, die auf die spezifischen Bedürfnisse unserer Schweizer Kunden zugeschnitten sind.»*

### **Die Stärken von «Core SOC», das von SPIE ICS AG angeboten wird**

- **Einfache Integration** in das bestehende IT-Ökosystem und **flexible Einsatzmöglichkeiten** für eine **nahtlose Kompatibilität** mit der aktuellen Infrastruktur.
- Modernste **Cyber Threat Intelligence** für eine kontinuierliche Anpassung der Abwehrmassnahmen an neue Bedrohungen.
- **Fortgeschrittene Überwachung der Infrastruktur** für eine proaktive und genaue Erkennung von Angriffen. Die intelligente Plattform von SPIE verbessert die Erkennungsrate und bietet dem Kunden einen genaueren Einblick. Dies ermöglicht eine schnellere Erkennung und eine deutliche Reduzierung der durchschnittlichen Zeit bis zur Erkennung (Mean Time to Detect, MTTD).
- **Lokaler und mehrsprachiger Support** in Deutsch, Französisch und Englisch sowie Zertifizierungen nach ISO 27001 und ExpertCyber<sup>2</sup> garantieren hohe Sicherheits- und Qualitätsstandards.
- **Einfache und transparente Preisgestaltung**, die auf Wettbewerbsfähigkeit ausgelegt ist und die Budgetplanung erleichtert. Die Bezahlung pro Gerät bietet den Vorteil, dass nicht pro Log abgerechnet wird, so dass ein unbegrenztes Volumen an Logs für denselben Perimeter eingespeist werden kann.
- **Die hochqualifizierten Experten der SPIE ICS AG** bieten dem SOC einen wesentlichen Mehrwert, indem sie eine gründliche Analyse und eine wirksame Reaktion auf Vorfälle gewährleisten und so die optimale Sicherheit der Umgebung ihrer Kunden garantieren.

---

<sup>1</sup> SIEM (Security Information and Event Management) sind zentralisierte Systeme, die einen vollständigen Einblick in die Netzwerkaktivitäten von Unternehmen bieten und es ermöglichen, auf Bedrohungen in Echtzeit zu reagieren. Als einheitliche Plattform für Sicherheitsvorfälle, die KI und Automatisierung nutzt, bietet XDR (Extended Detection and Response) Organisationen eine ganzheitliche und effektive Möglichkeit, sich vor fortgeschrittenen Cyberangriffen zu schützen und auf diese zu reagieren.

<sup>2</sup> [Expertcyber \(afnor.org\)](https://www.expertcyber.com)

Zusätzlich zu ihrem SOC bietet SPIE ICS AG optionale Schutzdienste an, wie z.B. die Verwaltung von EDR/MDR<sup>3</sup>-Lösungen, Deception Tools (Honeypot<sup>4</sup>) sowie Network Detection/Intervention (NDR), die speziell für OT<sup>5</sup>-Umgebungen entwickelt wurden. Diese zusätzlichen Dienste ermöglichen eine bessere Überwachung, einen besseren Schutz von Endgeräten und eine höhere Sicherheit von Industriernetzwerken durch die Erkennung und Neutralisierung hochentwickelter Bedrohungen, bevor sie den Betrieb beeinträchtigen können. Mit ihrem «Core SOC 24/7»-Service ist die SPIE ICS AG in der Lage, die Vermögenswerte ihrer Kunden vertrauensvoll zu schützen. Weitere Informationen über das Cybersecurityportfolio von SPIE ICS AG finden Sie unter: [cybersecurity.spie.ch](https://cybersecurity.spie.ch)

## Über SPIE Schweiz

Als Tochtergesellschaft der SPIE-Gruppe, dem unabhängigen europäischen Marktführer für multitechnische Dienstleistungen im Energie- und Kommunikationsbereich, ist SPIE Schweiz in den Bereichen ICT, Multitechnik und Facility Management tätig.

Die Divisionen ICS (Information & Communication Services), MTS (Multi-Technical Services) und IFS (Integral Facility Services) bieten mit rund 560 Mitarbeitenden an 8 Standorten in der ganzen Schweiz Dienstleistungen an, die auf die Herausforderungen der Märkte "Smart City", "Energies", "e-efficient Buildings" und "Industry Services" zugeschnitten sind.

Mit der SPIE-Gruppe und der Global Workspace Alliance verfügt SPIE Schweiz über ein globales Netzwerk, das es ihr ermöglicht, wichtige internationale Mandate in ihrer Gesamtheit zu übernehmen. Ergänzt wird das Serviceangebot durch ein leistungsfähiges Service Center, das 24 Stunden am Tag in vier Sprachen zur Verfügung steht.

Mit mehr als 50 000 Mitarbeitern und Mitarbeiterinnen und einer starken lokalen Präsenz erwirtschaftete die SPIE-Gruppe im Jahr 2023 einen konsolidierten Umsatz von 8,7 Milliarden Euro und einen konsolidierten EBITA von 584 Millionen Euro.

## Medienkontakte

### SPIE

Pascal Omnès  
Group Communications Director  
Tel. +33 (0)1 34 41 81 11  
[Pascal.omnes@spie.com](mailto:Pascal.omnes@spie.com)

### SPIE Schweiz

Tamara Obielum  
Director Marketing & Communication  
Tel. +41 58 301 10 70  
[Tamara.obielum@spie.com](mailto:Tamara.obielum@spie.com)

### Jenni Kommunikation AG

Sylvana Zimmermann  
Consultant  
Tel. +41 (0)44 388 60 80  
[sylvana.zimmermann@jeko.com](mailto:sylvana.zimmermann@jeko.com)

Weitere Informationen finden Sie unter [www.spie.ch](https://www.spie.ch) und <https://www.linkedin.com/company/spie-switzerland/>

---

<sup>3</sup> EDR-Lösungen wurden entwickelt, um Unternehmen Sicherheit am Arbeitsplatz zu bieten. Das Hauptziel von EDR besteht darin, mehrere Ebenen der Bedrohungsabwehr, Erkennung und Reaktion in einer einzigen Lösung zu integrieren. MDR ist die Übernahme des Betriebs eines EDR-Tools durch einen Sicherheitsspezialisten und ermöglicht es, das Sicherheitsmanagement über einen SOC-Dienst an einen Experten zu delegieren.

<sup>4</sup> Im Bereich der Cybersicherheit sind Honeypots gekaperte Server oder Systeme, die neben den Systemen eingesetzt werden, die Ihre Organisation tatsächlich für die Produktion verwendet. Honeypots sind so gestaltet, dass sie wie attraktive Ziele aussehen, und sie werden eingesetzt, damit die IT-Teams die Sicherheitsreaktionen des Systems überwachen und den Angreifer vom geplanten Ziel weglenken können. (fortinet.com)

<sup>5</sup> OT: Operational Technology (Betriebstechnologien, für die Produktion verwendete Systeme).

