



Communiqué de presse

SPIE lance son SOC en Suisse

Berne, le 26 juin 2024 – *SPIE Suisse, filiale du groupe SPIE, leader européen indépendant des services multi-techniques dans les domaines de l'énergie et des communications, annonce le lancement de son offre SOC (Centre Opérationnel de Sécurité). Ce service complet offre aux entreprises suisses de toute taille une détection des cyberattaques avancées, une surveillance 24h/24, 7j/7 et un service de renseignement sur les cybermenaces.*

Un partenariat stratégique pour renforcer la cybersécurité

Cette nouvelle offre SOC est le fruit d'un partenariat stratégique entre les deux entreprises de services numériques de SPIE en Suisse et en France, qui ont, toutes deux, apporté leur expertise et leur expérience dans le domaine de la cybersécurité. En France, SPIE ICS exploite son propre SOC avec succès, au service de plus de 100 clients français et internationaux. En Suisse, SPIE ICS SA propose depuis 2015 des solutions et des services de cybersécurité en portant une attention particulière à l'évaluation des risques, à la conformité et à la sensibilisation.

Un portefeuille complété par une solution de SOC 24/7

Poursuivant une stratégie axée sur la cybersécurité, SPIE ICS SA enrichit désormais son portefeuille avec le lancement de sa solution nommée « Core SOC ». Ce centre opérationnel de sécurité, pierre angulaire de son offre, propose des services de détection avancés

disponibles 24h/24, 7j/7. Complété par une plateforme de gestion SIEM/XDR¹ flexible et agnostique, il est adapté aux exigences spécifiques de chaque client.

Ce service inclut une source de renseignement des cybermenaces pour une mise à jour rapide des modèles de détection face aux nouvelles attaques et une chasse proactive des menaces pour prévenir toute compromission des environnements clients. De plus, le SOC s'intègre de manière transparente dans l'environnement existant du client et peut être complété avec des services supplémentaires SPIE pour une détection améliorée sur les réseaux industriels.

« Avec le lancement de Core SOC, nous franchissons une étape importante afin d'augmenter la visibilité et le taux de détection des cyberattaques des actifs numériques de nos clients. En combinant notre expertise locale avec nos ressources globales, nous sommes en mesure d'offrir un service de cybersécurité robuste, complet et flexible », déclare Christophe Francey, Chief Technology Officer chez SPIE ICS SA. Il ajoute : « Ce service renforce notre engagement à fournir des solutions innovantes et adaptées aux besoins spécifiques de nos clients suisses. »

Les points forts de « Core SOC » proposé par SPIE ICS SA

- **Intégration simple dans l'écosystème IT existant et flexibilité de déploiement** pour une compatibilité parfaite avec les infrastructures actuelles.
- **Cyber Threat Intelligence** de pointe, pour une adaptation continue des défenses face aux menaces émergentes.
- **Surveillance avancée de l'infrastructure** pour une détection proactive et précise des attaques. La plateforme intelligente de SPIE améliore le taux de détection et offre une meilleure visibilité pour le client, permettant une détection plus rapide et une réduction significative du temps moyen de détection (Mean Time to Detect - MTTD).
- **Support local et multilingue** en allemand, français et anglais, et certifications ISO 27001 et ExpertCyber² garantissant des normes élevées de sécurité et de qualité.
- **Tarification simple et transparente**, conçue pour être compétitive, qui facilite la planification budgétaire. Le paiement par appareil offre l'avantage de ne pas être facturé par log, permettant ainsi l'injection d'un volume illimité de logs pour le même périmètre.
- **Les experts hautement qualifiés de SPIE ICS SA** apportent une valeur ajoutée essentielle au SOC, en assurant une analyse approfondie et une réponse efficace aux incidents, garantissant ainsi la sécurité optimale de l'environnement de ses clients.

¹ Les SIEM (Security information and event management) sont des systèmes centralisés qui offrent une visibilité totale sur l'activité du réseau des entreprises, permettant ainsi de réagir aux menaces en temps réel. Plateforme d'incidents de sécurité unifiée qui utilise l'IA et l'automatisation, XDR (Extended Detection and Response) offre aux organisations un moyen holistique et efficace de se protéger contre les cyberattaques avancées et de répondre à celles-ci.

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

En complément de son SOC, SPIE ICS SA propose des services de protection optionnels, tels que la gestion des solutions d'EDR/MDR³, des outils de Deception (HoneyPot⁴) et de Détection/Intervention Réseau (NDR) spécifiques aux environnements OT⁵. Ces services supplémentaires permettent de renforcer la surveillance, d'approfondir la protection des terminaux utilisateurs, et d'améliorer la sécurité des réseaux industriels en détectant et neutralisant les menaces sophistiquées avant qu'elles n'affectent les opérations. Avec son service « Core SOC 24/7 », SPIE ICS SA est en mesure de protéger les actifs de ses clients en toute confiance. Pour en savoir plus sur le portefeuille de cybersécurité de SPIE, visitez : cybersecurity.spie.ch.

A propos de SPIE Suisse

SPIE Suisse est une filiale du groupe SPIE, leader européen indépendant des services multi-techniques dans les domaines de l'énergie et des communications.

Employant environ 560 personnes sur 8 sites répartis sur tout le territoire suisse, les divisions ICS (Information & Communication Services), MTS (Multi-Technical Services) et IFS (Integral Facility Services) offrent prestations et solutions dans les domaines du numérique, de l'automatisation des bâtiments ainsi que de la « Smart City », du « Smart Building » et du « Facility Management ».

Avec le groupe SPIE et Global Workspace Alliance, SPIE Suisse bénéficie d'un réseau mondial qui lui permet de prendre en charge intégralement de grands mandats internationaux. Cette offre de prestations de services est complétée par un Service Center performant disponible 24 heures sur 24 en quatre langues.

Avec plus de 50 000 collaborateurs et un fort ancrage local, le groupe SPIE a réalisé, en 2023, un chiffre d'affaires consolidé de 8,7 milliards d'euros et un EBITA consolidé de 584 millions d'euros.

Contacts presse

SPIE

Pascal Omnes
Directeur de la communication du
Groupe
Tél. +33 (0)1 34 41 81 11
pascal.omnes@spie.com

SPIE Suisse

Tamara Obielum
Directrice marketing et communication
Tél. +41 58 301 10 70
Tamara.obielum@spie.com

Jenni Kommunikation AG

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

Pour en savoir plus, visitez www.spie.ch et <https://www.linkedin.com/company/spie-switzerland/>

³ Les solutions EDR sont conçues pour offrir aux entreprises une sécurité des postes de travail. L'objectif principal de l'EDR est d'intégrer plusieurs couches de prévention des menaces, de détection et de réponse dans une solution unique. MDR est la prise en charge de l'exploitation d'un outil EDR par un spécialiste de la sécurité et permet de déléguer la gestion de la sécurité à un expert via un service SOC.

⁴ Dans le domaine de la cybersécurité, les honeypots sont des serveurs ou des systèmes dérobés qui sont déployés à côté des systèmes que les organisations utilisent réellement pour la production. Les Honeypots sont conçus pour ressembler à des cibles attrayantes, et ils sont déployés pour permettre aux équipes informatiques de surveiller les réponses de sécurité du système et de rediriger l'attaquant loin de la cible prévue (fortinet.com).

⁵ OT : Operational Technology (technologies d'exploitation, systèmes utilisés pour la production)

