



In einem Umfeld, in dem Cyberangriffe allgegenwärtig sind, ist unser Angebot «Core SOC» ein gebrauchsfertiger Service, der alle wesentlichen Elemente enthält, um Bedrohungen für Ihre Infrastruktur erkennen zu können. Durch die Kombination unserer lokalen Expertise mit unseren globalen Ressourcen können wir Unternehmen jeder Grösse einen robusten, umfassenden und flexiblen Cybersecurity-Service anbieten.

SCHLÜSSELELEMENTE

Unser Team aus **mehrsprachigen Spezialisten in der Schweiz** analysiert in enger Zusammenarbeit mit den Kunden die von unserem Detection Tool gemeldeten Ereignisse, um Bedrohungen abzuwehren.

Unser **effektives Filtersystem reduziert irrelevante Alarmer** und ermöglicht es Ihnen dadurch, sich auf kritische Vorfälle zu konzentrieren und Reaktionszeiten zu verbessern.

Die **erweiterte Kontextualisierung** ermöglicht ein schnelles Reagieren, minimiert Eskalationen und verhindert das wiederholte Auftreten der Vorfälle. Gleichzeitig werden Aktionen priorisiert und Sie erhalten einen Überblick über alle Bedrohungen.

24/7 SOC-SERVICE

Unser **24/7 Advanced Detection Service** ist entscheidend, um sicherheitsrelevante Ereignisse in Echtzeit sichtbar zu machen und die Sicherheit Ihres Informationssystems zu gewährleisten.

Dieser proaktive Ansatz ermöglicht es, **diese Bedrohungspotenziale zu erkennen und auf sie zu reagieren**, bevor sie sich auf das



Dieser Service stärkt unser Engagement für innovative und auf die spezifischen Bedürfnisse unserer Schweizer Kunden zugeschnittene Lösungen.



CHRISTOPHE FRANCEY
Chief Technology Officer
SPIE ICS SA

Unternehmen auswirken. Zudem lässt sich dieses flexible und anpassbare SOC auf die spezifischen Anforderungen jedes Kunden zuschneiden.

CYBERTHREAT HUNTING

Dieser Service beinhaltet eine Informationsquelle über Cyberbedrohungen zur raschen Aktualisierung von Erkennungsmodellen bei neuen Angriffen sowie ein **proaktives Threat Hunting**, um jegliche Beeinträchtigungen von Kundenumgebungen zu verhindern.

IN KÜRZE

Vorteile

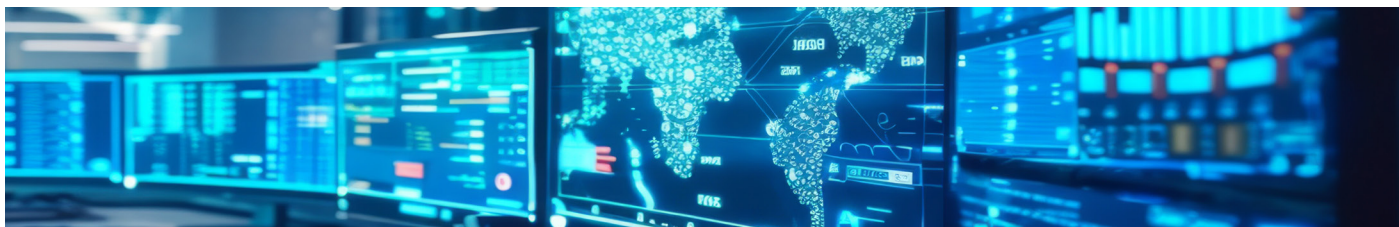
- Erhöhte Sicherheit Ihrer digitalen Assets sowie Ihrer Infrastruktur
- Vermindertes Risiko und Einhaltung der geltenden Vorschriften
- Förderung einer proaktiven Sicherheitskultur
- Schutz Ihres Unternehmens und Ihres Markenimages

Highlights

- Integriertes und verwaltetes SIEM-/XDR-Tool
- 24-Stunden-Überwachung und -Alarmierung
- In der Schweiz ansässige Analysten
- Erstklassige Aufklärung über Cyberbedrohungen
- Schnelle Reaktion auf Vorfälle
- Flexibel einsetzbar

Warum SPIE ICS ?

- Qualität und Sicherheit: zertifiziert nach ISO 9001 und ISO 27001
- Präsenz in der Schweiz mit Support in den Sprachen Deutsch, Französisch, Englisch
- Erfahrung und Expertise in leistungsstarken Managed Services
- Wettbewerbsfähige Preise und klare KPIs



UNSER ANGEBOT CORE SOC IM ÜBERBLICK

- **Rund-um-die-Uhr-Überwachung und -Alarmierung**, unterstützt durch unsere Analysten in der Schweiz
- **Aufklärung über die wichtigsten aktuellen Cyberbedrohungen** zur kontinuierlichen Anpassung der Abwehr an neue Bedrohungen
- Cloud-basiertes **SIEM/XDR** mit integriertem Log-Speicher für eine sorgfältige Analyse und eine **schnelle Reaktion auf Vorfälle**
- Verfügbare SOAR-Funktionen zur Automatisierung von Abhilfemassnahmen
- Mehr als 800 gebrauchsfertige Erkennungsregeln mit mehr als 7 Millionen Kompromittierungsindikatoren (Indicators of Compromise, IoC) und mehr als 70 Millionen Beobachtungsdaten
- Nutzung der Frameworks MITRE ATT&CK und Cyber Kill Chain zur Kontextualisierung
- Erstellen massgeschneiderter Regeln und IoCs, falls erforderlich, zur Anpassung an Ihren Kontext
- Flexibler Einsatz, mit oder ohne Agent, für eine nahtlose Integration mit den bestehenden Infrastrukturen

Als Ergänzung zu ihrem SOC bietet die SPIE ICS AG optional Schutzdienstleistungen an, wie:

- Management von EDR-/MDR-Lösungen
- Tools zur Täuschung von Angreifern (Honeypot) und zur Netzwerkerkennung und -reaktion (Network Detection and Response, NDR)

Diese zusätzlichen Dienste ermöglichen eine verstärkte Überwachung, einen vertieften Schutz von Benutzerendgeräten und eine verbesserte Sicherheit von Industrienetzwerken, indem sie ausgeklügelte Bedrohungen erkennen und neutralisieren, bevor sie den Betrieb beeinträchtigen können.

SPIE ICS UNTERSTÜTZT SIE MIT DEM SERVICE CORE SOC ALS VERTRAUENSWÜRDIGER PARTNER BEIM SCHUTZ IHRER VERMÖGENSWERTE



Qualität und sicherheit

Zertifiziert nach ISO 9001 und 27001



Erfahrung und Expertise

in erfolgreichen Managed Services



Lokaler Support

in der Schweiz in 3 Sprachen (DE/FR/EN)

ZU UNSEREM CYBERSECURITY-PORTFOLIO



KONTAKTIEREN SIE UNS

SPIE ICS AG
Freiburgstrasse 251
3018 Bern, Schweiz

Telefon +41 58 301 11 11
info.ch@spie.com
www.spie.ch

SPIE, sharing a vision for the future