ZURICH
Resilience Solutions

“Eine einzige Stunde Ausfallzeit in kritischen OT-Systemen kann Millionen kosten

OT-Cyber-Resilienz: Strategisches Industrie-risikomanagement

OT-IT-Konvergenz schafft neue Risikoprofile mit erheblichen betrieblichen, finanziellen und sicherheitsrelevanten Auswirkungen für Produktionsumgebungen.

Wir begegnen diesen Herausforderungen, indem wir umfassende Lösungen anbieten, um Schwachstellen zu identifizieren, Risiken zu mitigieren und industrielle Steuerungssysteme vor Cyberbedrohungen zu schützen.

Ihre Herausforderung

Anstieg der Cyberangriffe
Ausgenutzte Sicherheitslücken in der Operational Technology (OT) können zu Betriebsunterbrechungen, finanziellen Verlusten (wie Geschäftsausfällen oder Untersuchungskosten), potenziellen Sicherheitsrisiken und sogar körperlichen Schaden führen.

Erhöhte Angriffsfläche
Die zunehmende Vernetzung von industriellen Steuerungssystemen (ICS), SCADA und Informationstechnologie (IT) schafft neue Einstiegspunkte für Cyber-Bedrohungen.

Neue regulatorische Anforderungen für Betriebstechnologien
Mit den NIS2-Richtlinie müssen mehr Unternehmen und Sektoren, die OT und industrielle Steuerungssysteme nutzen, eine verbesserte Cyber-Resilienz durch ergriffene Cyber-Sicherheitsmaßnahmen nachweisen.

Ihre Vorteile

- **Stärkung der technischen NIS2-Konformität**
- **Bedrohungen und Schwachstellen eindämmen**
- **Cyber-Bedrohungen überwachen detektieren und darauf reagieren**
- **Bewertung der Incident-Bereitschaft**

OT-Sicherheitsreise

ZURICH
Resilience Solutions

> OT-Sicherheit ist viel mehr als nur das Einsetzten von Sensoren zur Überwachung von Netzwerkanomalien

Risikobewertung & technische Konformität

- OT-Bedrohungen identifizieren
- Sicherheitsstatus gemäß IEC 62443 und internen Branchen-Benchmark bewerten
- Eine nicht-störende Sicherheitsstrategie entwickeln
- Gesundheits-, Sicherheits- und Umweltaspekte (HSE) priorisieren
- Umsetzbare Empfehlungen und einen Fahrplan für die Implementierung erhalten
- Hohe Verfügbarkeit / System-Resilienz sicherstellen
- Einhaltung der NIS2-Richtlinie oder des CRA (Cyber Resilience Act) für Geräte erreichen

OT-Sicherheitstests

- Reale Angriffe simulieren, um die Resilienz und vorhandene Kontrollen zu testen
- Technische Schwachstellen identifizieren
- Maßgeschneiderte Abhilfestrategie erhalten
- Bewusstsein durch Sicherheitsschulungen und Simulationen verbessern

OT Monitoring & Incident Response

- Betriebsprozesse und Systeme rund um die Uhr überwachen
- Potenzielle Bedrohungen in Echtzeit detektieren und analysieren
- Fortschrittliche Erkennung und Reaktion mit Claroty oder Nozomi implementieren
- Integration in bestehende IT- und OT-Infrastruktur

Incident-Response-Plan & Krisenübungen

- Einen robusten Incident-Response-Plan entwickeln
- Vorfälle in OT-Systemen simulieren
- Bereitschaft testen, um Vorfälle schnell zu erkennen, zu mindern und den Betrieb wiederherzustellen
- Lücken identifizieren und Reaktionsstrategie verbessern
- Ausfallzeiten und betriebliche Auswirkungen minimieren

Cyber x Industrie Experten

ZURICH
Resilience Solutions

Wir kombinieren Cyber- und Industrieingenieure, um kritische Infrastrukturen zu sichern, Abläufe zu optimieren und die Einhaltung von Compliance sicherzustellen.

Cyber Experten

Michael Guiao
Senior Cyber Risk Engineer
Germany
michael.guiao@zurich.com

Liane Velten
Cyber Risk Engineer
Germany
liane.velten@zurich.com

120 Cyber Risk Ingenieure weltweit

ZRS Industrie-Experten

- Produktion & Fertigung
- Energie & Versorgung
- Öl & Gas
- Transport & Logistik
- Wasser- & Abfallwirtschaft
- Bauwesen
- Chemie
- Pharma & Gesundheitswesen

1000 Riskoingenieure weltweit in den Bereichen Fertigung, Energie & Versorgung, Öl & Gas, Transport & Logistik, Pharma, Gesundheitswesen, Lebensmittel & Getränke, Chemie, Bergbau & Metalle, Wasser, Landwirtschaft und Bauwesen.

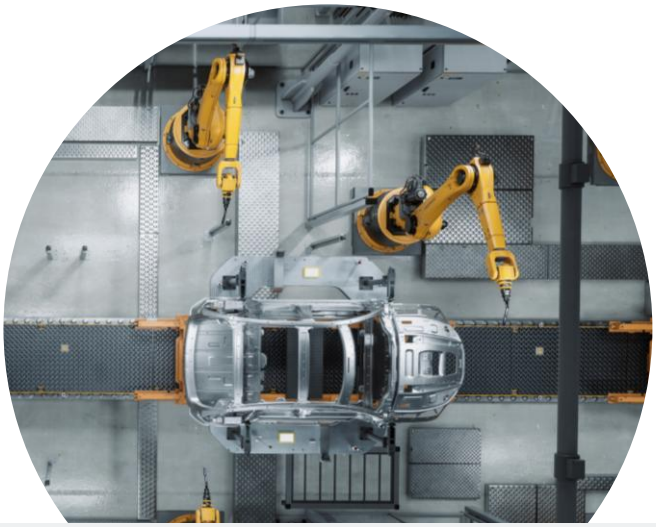
Kontaktieren Sie uns

michael.guiao@zurich.com | liane.velten@zurich.com

ZURICH
Resilience Solutions

Warum Zurich Cyber Resilience Solutions?

- Unterstützung bei der Verbesserung der Versicherbarkeit
- Kombination von Schadendaten und Branchen-Benchmarking
- Maßgeschneiderte Servicepakete für jede Unternehmensgröße und deren Anforderungen
- Team aus Cyber-Spezialisten mit Branchenrisikoexperten
- Globale Präsenz für Remote- und Vor-Ort-Lösungen



Zurich Resilience Solutions

Veröffentlichungsdatum: März 2025