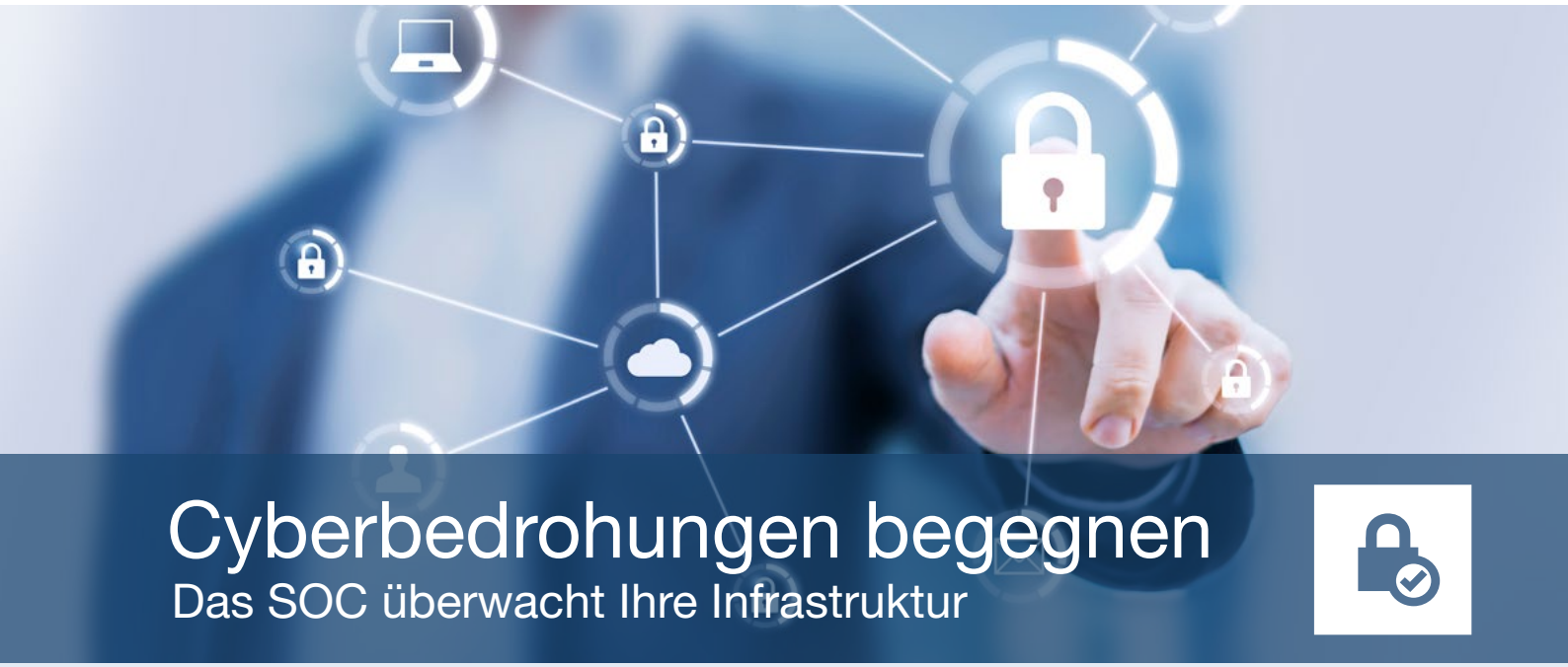
ITRIS ONE AG



Cyberbedrohungen begegnen

Das SOC überwacht Ihre Infrastruktur

Um Cyberangriffe abzuwehren, müssen Anomalien erkannt werden, die klassische Prävention reicht nicht mehr. Ein Security Operations Center (SOC) überwacht das Firmennetzwerk und fügt Daten aus unterschiedlichen Quellen zu einem Gesamtbild zusammen. So werden Abweichungen frühzeitig erkannt, Schaden kann vermieden werden.

Ein SOC ist kosten- und ressourcenintensiv und nicht jede Unternehmung benötigt das gleiche Setup. ITRIS One bietet gemeinsam mit Arctic Wolf, dem Marktführer für Managed Detection & Response (MDR), Managed-SOC-Leistungen an. Die Erfahrung aus über 4000 aktiven SOC-Kunden und die Service- und Infrastruktur-Kompetenz der ITRIS One sorgen dafür, dass jede Lösung genau auf die Bedürfnisse des einzelnen Unternehmens abgestimmt ist.

> „Jedes Unternehmen braucht Schutz vor Cyberangriffen. Unsere Managed-SOC-Angebote bieten die massgeschneiderte Lösung."

Wir haben die Stärken von ITRIS One und Arctic Wolf in einer gemeinsamen Architektur gebündelt. Das ITRIS One Incident & Response Team kümmert sich gemeinsam mit dem Service Desk (SPOC) um die auf der Arctic-Wolf-Plattform erkannten Vorfälle. Dabei spielt es keine Rolle, ob sich die Infrastruktur vor Ort in ihrem Rechenzentrum befindet oder in der Cloud. Durch regelmässige Reports und Auswertungen sieht das Team die Angriffsflächen und kann frühzeitig Massnahmen festlegen.

So funktioniert ein SOC

In regelmässigen Assessments wird die Wirksamkeit der Sicherheitsmassnahmen geprüft und ausgewiesen; in den monatlichen Concierge-Meetings werden alle Resultate und Erkenntnisse besprochen und gemeinsam weitere Massnahmen definiert. ITRIS One unterstützt ihre Kunden bei deren Umsetzung.

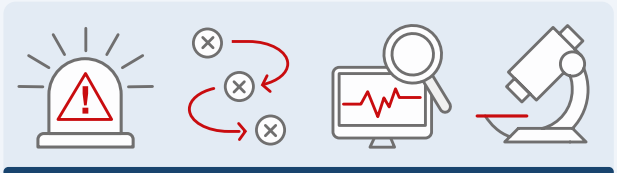
IHRE ERFOLGSFAKTOREN

- Für Ihre Fragen die richtigen Experten
- Der gleiche Partner für Beratung, Durchführung und Betrieb (ggf. mit Kooperationspartnern)
- Betriebsverantwortung bei ITRIS One und Arctic Wolf
- Meetings zur Verbesserung der Prävention
- Reportings über Incidents, Komponenten und Prozesse
- Kontinuierliches Monitoring aller sicherheitsrelevanten Parameter und sofortiges Eingreifen bei Anomalien

DARUM ITRIS

- Einer der führenden Schweizer ICT-Serviceprovider
- Jahrzehntelange Erfahrung bei der Entwicklung und Umsetzung modernster IT-Lösungen und Services
- Ausgewählte Partner ergänzen das Expertenwissen
- Agile und leistungsfähige IT-Infrastruktur-Lösungen
- Breites, massgeschneidertes Service-Portfolio
- Langjährige Erfahrung bei Cybersecurity-Lösungen

MANAGED SOC ARCHITEKTUR



INCIDENT | PROCESS | DETECTION | ANALYSIS

- Erfassen und Kategorisieren von Incidents
- Incident-Erstanalyse durchführen
- Auslösen der Incident-Eskalation, falls erforderlich über das Service Desk von ITRIS One
- Vorfallsanalyse durchführen und Vorfallsreaktionen erkennen

INITIAL SUPPORT | RESTORE | REPORTING

- Vorfallsbearbeitung, Mitigation
- Einleiten von Sofortmassnahmen (z. B. Systemisolation)
- Massnahmen zur Erreichung des Normalzustandes durchführen
- Vorkommnisse dokumentieren, Prozesse und Massnahmen prüfen

Der Weg zum Managed SOC mit ITRIS One und Arctic Wolf ist einfach: In der Onboarding-Phase (30 Tage) gibt es sowohl ein Projekt- als auch ein technisches Kick- off, das Portal wird vorgestellt, die Sensoren verschickt und die Log-Quellen konfiguriert. Während der nächsten 90 Tage (Go-live) übernimmt das Concierge Security Team den Kundenservice (zweiwöchentliche Meetings, 24/7-Monitoring durch das Triage Team, unlimitierte Guided Incident Response). Ab jetzt gibt es Erkenntnisse über die konkrete Situation. Danach, im Betriebszustand, hat der Kunde unlimitierten Zugriff auf das Concierge Security Team. Und sobald ein relevantes Sicherheitsereignis erkannt wurde, startet der Incident-Management-Prozess zur Schadensbegrenzung. ITRIS One bringt nicht nur die eigene, jahrzehntelange Erfahrung bei der Konzeption der Lösung ein, sondern begleitet auch die Onboarding- und Go-live-Phase sowie den gesamten Betrieb.

So hilft Ihnen ITRIS One

In der Onboarding- und Go-live-Phase ist ITRIS One der SPOC für den Kunden und koordiniert alle Tätigkeiten. Wir konfigurieren alle Log-Quellen, richten die VPN-Verbindung zum SOC ein und begleiten beim Rollout der Agenten und beim Finetuning. Im Betriebszustand kümmern wir uns als SPOC um erkannte Incidents, leiten gemeinsam mit dem Kunden ggf. Sofortmassnahmen ein (Response) und stellen bei Bedarf den Normalzustand wieder her (Recovery). Zudem begleiten wir die regelmässigen Concierge Meetings und forensischen Untersuchungen und setzen die aus den Meetings gewonnen Erkenntnisse zur Verbesserung der Prävention um. Auch bei externen Assessments arbeiten wir mit. Dieses Paket schützt ihr Unternehmen genau so vor Cyberangriffen, wie Sie es brauchen.

LERNEN WIR UNS KENNEN

Viele Wege führen zu ITRIS One. Kontaktieren Sie uns für ein persönliches Gespräch – telefonisch unter **056 418 64 64** oder über unsere anderen Kanäle.

UNSER ANGEBOT

Leistungsfähige Datacenter, zeitsparende Kommunikationslösungen, zuverlässige Netzwerke, moderne Workplace- oder wirksame Sicherheitskonzepte; On-Premise-, Managed-, Cloud- oder Hybrid-Cloud-Lösungen.

ITRIS ONE AG

ITRIS One AG
Hauptsitz
Industriestrasse 169 CH-8957
Spreitenbach
Tel. +41 56 418 64 64
Mail one@itris.ch
Web www.one.itris.ch

Für Sie vor Ort sind wir ausserdem in weiteren Niederlassungen in Chur, Gland, Gossau, Lamone, Reinach, Tagelswangen, Urtenen-Schönbühl.

© ITRIS AG • 20230811