Security Operation Center as a Service

Unser erfahrenes Team monitort und betreut Ihre Sicherheits-infrastruktur rund um die Uhr, alarmiert Sie bei Problemen und schlägt Gegenmassnahmen vor, um die Kontrolle über sicherheitsrelevante Vorfälle zu haben.

Mit unserem Security Operation Center as a Service (SOCaaS) übernehmen wir die Analyse der potenziellen Bedrohungen.
Ein Security Operation Center ist entscheidend, um die Sicherheit Ihrer Organisation zu gewährleisten und potenzielle Bedrohungen effektiv zu erkennen und zu bekämpfen. Unsere professionellen Security Spezialist*innen analysieren Sicherheitswarnungen (Security Alerts) und identifizieren und bewerten daraus resultierende Sicherheitsvorfälle (Security Incidents) auf deren Kritikalität und Auswirkungen von möglichen Risiken auf Ihre Organisation. Erstreaktionen im Rahmen von Pre-approved Actions sowie Handlungsempfehlungen erlauben Ihnen eine schnelle Reaktion auf Cyberangriffe.

Ihre Nutzen mit SOCaaS

Schnelle Erkennung von Cyberangriffen

7/24 Monitoring der Security Alerts Ihrer Sicherheitsinfrastruktur. ✓

Überprüfung möglicher Auswirkungen auf Ihre Organisation

Identifizierung und Bewertung von Security Incidents auf deren Kritikalität, Auswirkung und potenzielles Risiko auf Ihre Organisation. ✓

Erstreaktion auf aktive Cyberangriffe

Im Rahmen von Pre-approved Actions werden Eindämmungsmassnahmen autonom durch das SOC durchgeführt. ✓

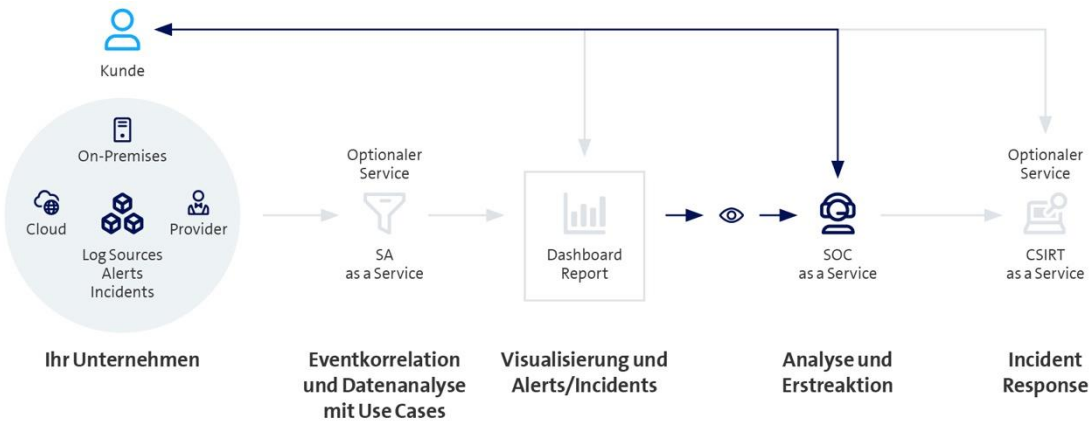
Konsultation mit konkreten Handlungsempfehlungen und -Anweisungen

Direkte Beratung über das weitere Vorgehen bei einem Security Incident. ✓

Branchenübergreifende Security-Erfahrung und Expertise

Breite Expertise und langjährige Erfahrung der eingesetzten Security-Spezialist*innen. ✓

So funktioniert SOCaaS



swisscom

Facts & Figures

Basisleistungen

Das Security Alert Management umfasst sämtliche Tätigkeiten zum Monitoring und zur Analyse von Security Events und Security Alerts, die im Rahmen der Service-Ausprägung Security Analytics as a Service oder durch ein unterstütztes 3rd Party Security System generiert wurden. Identifizierte Security Incidents werden detailliert analysiert und die Kritikalität, Auswirkung und potenzielles Risiko für die Organisation bewertet und gemeinsam mit dem Kunden verifiziert. Sollte es sich dabei um aktive Cyberangriffe handeln, werden basierend auf etablierten Prozeduren und Prozessen, erste Eindämmungsmassnahmen mit dem Kunden abgesprochen und eingeleitet oder im Rahmen der Pre-approved Actions autonom durch das SOC durchgeführt.

Zusatzservices

- **Security Analytics as a Service (SAaaS):**
  Unsere Spezialist*innen sind Fachleute in den Themen Security und Big Data und stellen Ihnen Swisscom bewährte Security-Analytics-Infrastruktur als SOC-Plattform zur Verfügung. Schliessen Sie weitere Logquellen aus der Cloud, On-Premises oder von einem Managed Provider an und erhalten Sie im Dashboard einen Überblick über potenzielle Sicherheitsvorfälle. Analyse und Reaktion auf Sicherheitsvorfälle übernehmen Sie selbst.
- **CSIRT as a Service (CSIRTaaS):**
  Zur Analyse und Bewältigung von Sicherheitsvorfällen ziehen Sie Fachleute von Swisscom bei. Wir leiten den Security-Incident-Management-Prozess remote oder bei Ihnen vor Ort und unterstützen Sie bei der Beweissicherung sowie der Kommunikation mit Kunden und Partnern.
- **Network Detection and Response as a Service (NDRaaS):**
  Wird als Erweiterung zu den statischen Erkennungsmöglichkeiten von SAaaS durch eine dynamische Threat Detection basierend auf Machine-Learning-Modellen unterstützt. Der Mehrwert ergibt sich in den Bereichen Web (Proxy) und Netzwerk (DNS, Netflow und Firewall-Traffic-Daten), was maximale Visibilität erlaubt.
- **Digital Risk Protection as a Service (DRPaaS):**
  Sie werden proaktiv informiert über das Vorkommen von sensiblen Geschäfts- und persönlichen Informationen Ihres Unternehmens in öffentlichen und geschlossenen Netzen (z.B. Darknet). Unsere Handlungsempfehlungen für potenzielle Sicherheitsvorfälle setzen Sie selbstständig um.
- **XDR as a Service (by Palo Alto Networks):**
  Lizenz-Management, Lifecycle- und Health Management der XDR-Agenten, Konfiguration der Security Policies, Kommunikation von neuen Funktionen und Änderungen und ein jährliches Security Policy Assessment sind in der Verantwortung von Swisscom.
- **Microsoft XDR as a Service:**
  Lifecycle Management der XDR-Agenten, Health Management der Service-Komponenten, Konfiguration der Security Policies, Kommunikation von neuen Funktionen und Änderungen und ein jährliches Security Policy Assessment sind in der Verantwortung von Swisscom.

Mehr Informationen und den Kontakt zu unseren Experten finden Sie auf swisscom.ch/soc

Swisscom (Schweiz) AG Enterprise Customers, Postfach,
CH-3050 Bern, Tel. 0800 800 900, www.swisscom.ch/enterprise