Security Operation Center as a Service

Notre équipe chevronnée surveille et encadre votre infrastructure de sécurité 24 heures sur 24, vous alerte en cas de problèmes et propose des contre-mesures pour contrôler les incidents liés à la sécurité.

Avec notre Security Operation Center as a Service (SOCaaS), nous prenons en charge l'analyse des menaces potentielles.
Un Security Operation Center est déterminant pour garantir la sécurité de votre organisation et détecter et combattre efficacement des menaces potentielles. Nos spécialistes en sécurité professionnelles analysent les alertes de sécurité (Security Alerts) et identifient et évaluent la criticité et les répercussions de risques possibles sur votre organisation des incidents de sécurité (Security Incidents) qui en résultent. Des réactions initiales dans le cadre d'actions pré-approuvées ainsi que des recommandations vous permettent de réagir rapidement aux cyberattaques.

Vos avantages avec SOCaaS

Détection rapide des cyberattaques

Surveillance 7x24 h des alertes de sécurité de votre infrastructure de sécurité. ✓

Vérification de répercussions possibles sur votre organisation

Identification et évaluation de la criticité, de la répercussion et du risque potentiel sur votre organisation des incidents de sécurité. ✓

Réaction initiale à des cyberattaques actives

Le SOC réalise de manière autonome des mesures d'endiguement dans le cadre d'actions pré-approuvées. ✓

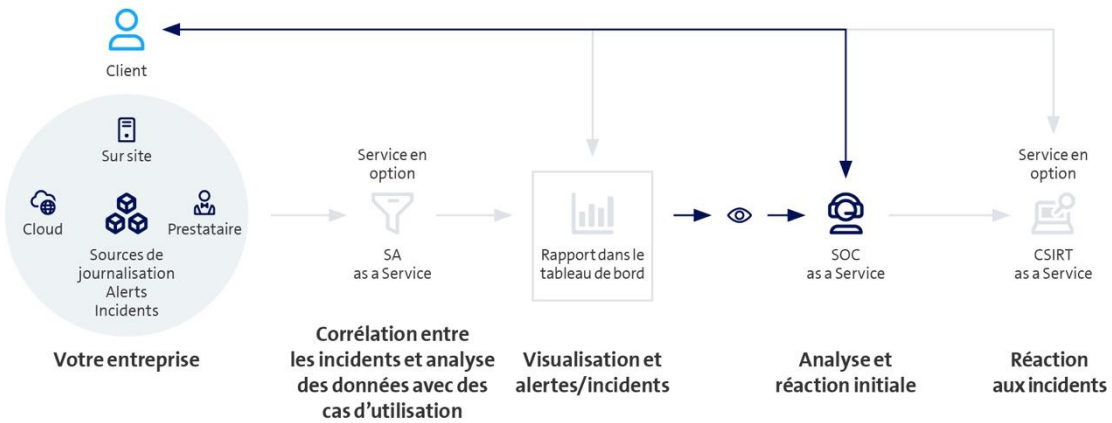
Consultation avec des recommandations et des instructions concrètes

Consultation directe quant à la suite des événements en cas d'incident de sécurité. ✓

Expérience et expertise intersectorielle en sécurité

Vaste expertise et expérience de longue date des spécialistes en sécurité engagées. ✓

Voici comment fonctionne SOCaaS



swisscom

Facts & Figures

Services de base

La gestion des alertes de sécurité englobe toutes les activités de surveillance et d'analyse des événements de sécurité et des alertes de sécurité générés dans le cadre de Security Analytics as a Service ou par un système de sécurité tiers soutenu. Les incidents de sécurité identifiés sont analysés dans le détail et leur criticité, répercussion et risque potentiel pour l'organisation sont évalués et vérifiés conjointement avec le client. S'il s'agit de cyberattaques actives, de premières mesures d'endiguement sont convenues avec le client et engagées sur base de procédures et processus établis ou réalisées de manière autonome par le SOC dans le cadre des actions pré-approuvées.

Services supplémentaires

- **Security Analytics as a Service (SAaaS):**
  Nos spécialistes sont des expert.e.s en matière de sécurité et de Big Data et mettent à votre disposition l'infrastructure Security Analytics éprouvée de Swisscom en guise de plateforme SOC. Raccordez d'autres sources de journalisation depuis le cloud, sur site ou d'un Managed Provider et obtenez une vue d'ensemble des incidents de sécurité potentiels dans le tableau de bord. Vous gérez vous-même l'analyse et la réaction aux incidents de sécurité.
- **CSIRT as a Service (CSIRTaaS):**
  Vous avez recours aux spécialistes de Swisscom pour analyser et gérer les incidents de sécurité. Nous menons le processus de gestion des incidents de sécurité à distance ou sur place dans vos locaux et vous aidons à préserver les preuves et à communiquer avec vos clients et partenaires.
- **Network Detection and Response as a Service (NDRaaS):**
  Solution instaurée comme une extension des possibilités de détection statiques de SAaaS, via une détection dynamique des menaces basée sur des modèles de machine learning. La valeur ajoutée se situe dans les domaines du web (proxy) et du réseau (DNS, Netflow et données de trafic du pare-feu), assurant une visibilité maximale.
- **Digital Risk Protection as a Service (DRPaaS):**
  Vous êtes informée de manière proactive dès que des informations commerciales et personnelles sensibles de votre entreprise apparaissent sur les réseaux publics et fermés (p.ex. Darknet). Vous appliquez en toute autonomie nos recommandations en cas d'incidents de sécurité potentiels.
- **XDR as a Service (by Palo Alto Networks):**
  La gestion des licences, la gestion du cycle de vie et de l'état de santé des agents XDR, la configuration des politiques de sécurité, la communication des nouvelles fonctions et des modifications et une évaluation annuelle des politiques de sécurité incombent à Swisscom.
- **Microsoft XDR as a Service:**
  La gestion du cycle de vie des agents XDR, la gestion de l'état de santé des composants du service, la configuration des politiques de sécurité, la communication des nouvelles fonctions et des modifications et une évaluation annuelle des politiques de sécurité incombent à Swisscom.

Vous trouverez de plus amples informations et les données de contact de nos experts sous swisscom.ch/soc

Swisscom (Suisse) SA Enterprise Customers, Case postale, CH-3050 Berne, tél. 0800 800 900, www.swisscom.ch/enterprise