

Threat Detection & Response

Protection complète de l'entreprise grâce à la détection en amont et à l'action professionnelle lors des attaques de Cyber Security

Actuellement, des volumes considérables d'informations d'entreprise et personnelles sont disponibles sur différentes sources de données (réseaux, applications, terminaux, Social Media, Cloud, Darknet, etc.). Face à une mise en réseau et à une numérisation qui ne cessent de progresser, les menaces sont de plus en plus multiformes. C'est la raison pour laquelle il est essentiel d'identifier en amont les incidents menaçant la sécurité.

La Threat Detection & Response professionnelle requiert des processus, des outils spécifiques, plusieurs années d'expérience et des collaborateurs extrêmement spécialisés. Une entreprise ne peut plus, à elle seule, comprendre les attaques de Cyber Security qui ne cessent d'évoluer et réagir en conséquence. Un partenaire expérimenté apporte dans ce cas son soutien.

Swisscom protège avec succès depuis des années l'infrastructure de réseau, les données des clients et des produits ainsi qu'elle-même contre les cybermenaces. Elle utilise ces expériences pour réduire les cyber-risques avec le concours des clients. Une bonne

visualisation des données permet une identification en amont des incidents de sécurité potentiels. L'analyse en temps réel et la réaction appropriée lors d'un Security Incident améliorent le niveau de sécurité et la mobilisation des ressources au sein de l'entreprise.

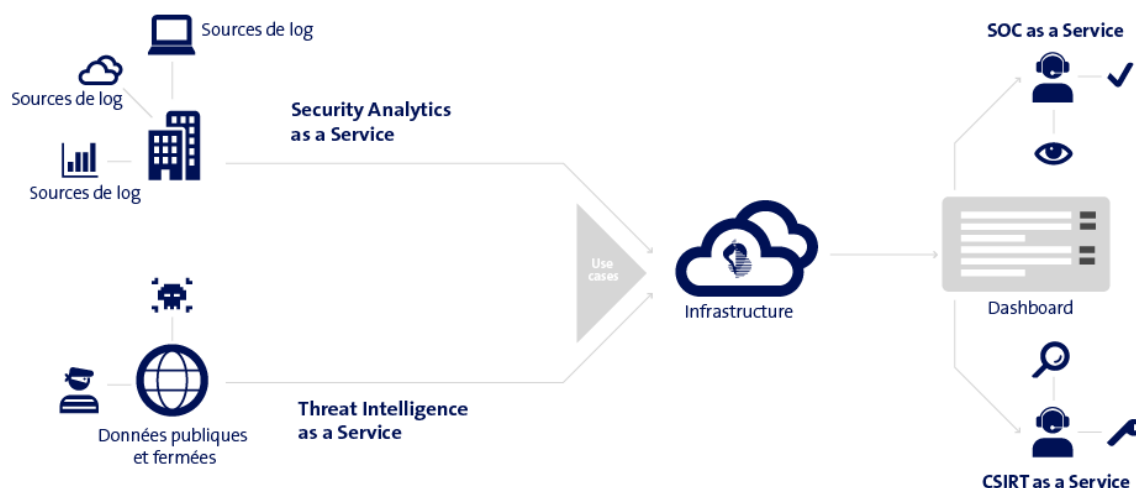
La Threat Detection & Response vous permet de choisir entre quatre variantes de services, en fonction de l'étendue du soutien que doit vous apporter Swisscom en matière de Cyber Security.

Vos avantages

Avec Threat Detection & Response

- > vous êtes informé en temps réel sur la menace actuelle et les incidents de sécurité potentiels (concernant votre entreprise)
- > les risques potentiels sont analysés 24 h/24
- > vous utilisez des Tools et des processus établis
- > vous n'avez à vous préoccuper ni du développement ni de l'exploitation d'une infrastructure de Security Analytics
- > vous profitez de Swisscom CSIRT et de l'écosystème de notre Security Partner

La solution en bref



Facts & Figures

Threat Detection & Response – Variantes de service

Security Analytics as a Service

Vous obtenez un aperçu sur le Dashboard sur les incidents de sécurité potentiels issus des données de log définies de votre entreprise. Vous assurez vous-même l'analyse et la réaction aux incidents de sécurité

Pourquoi Security Analytics as a Service de Swisscom:

Nous sommes spécialisés dans la Security et le Big Data et nous mettons à votre disposition notre infrastructure de Security Analytics éprouvée. Vous profitez par ailleurs d'un Threat Intelligence Feed optimisé pour la Suisse, qui ne peut être obtenu nulle part ailleurs sous cette forme.

SOC as a Service

Vous obtenez un aperçu sur le Dashboard sur les incidents de sécurité potentiels et confirmés issus des données de log définies de votre entreprise ainsi que des analyses avec des recommandations d'action concrètes. Vous réagissez vous-même aux Security Incidents critiques.

Pourquoi SOC as a Service de Swisscom:

Nous offrons depuis plus de 10 ans des services SOC pour les entreprises suisses en Suisse et à l'étranger. Nos analystes SOC savent de quoi il retourne et peuvent interpréter de manière compétente les Security Events & Incidents.

CSIRT as a Service

Vous définissez de manière autonome les incidents de sécurité critiques ou vous utilisez SOC as a Service. Vous faites appel aux experts de Swisscom pour l'analyse et la maîtrise de ces incidents. Nous dirigeons le processus de Security Incident Management soit à distance soit chez vous sur place, nous vous assistons dans l'établissement des preuves ainsi que dans la communication avec les clients et les partenaires.

Pourquoi CSIRT as a Service de Swisscom:

Le Swisscom CSIRT (Computer Security Incident Response Team) a recours à des Tools établis, à des processus et experts en Incident Response expérimentés. Il est depuis plusieurs années à la pointe du CSIRT et vous permet de profiter de cette expertise en tant que client.

Threat Intelligence as a Service

Vous êtes informé de manière proactive sur l'apparition d'informations sur l'activité et les personnes de votre entreprise dans les réseaux publics et fermés (par ex. Darknet). Vous appliquez de manière autonome nos recommandations d'action pour des incidents de sécurité confirmés.

Pourquoi Threat Intelligence as a Service:

Swisscom exploite les infrastructures TIC pertinentes et dispose à ce titre d'une vue d'ensemble unique sur les cyber-risques réels en Suisse. Nous savons comment y réagir.

Facts & Figures

Étendue de la prestation

	SA as a Service	SOC as a Service	CSIRT as a Service	TI as a Service
Heures d'assistance				
5 x 8	●			●
7 x 24		●	●	
Infrastructure SLA				
99,9%	●	●		●
Prestations				
Release Management	●	●		●
Detection	●	●		●
Response			●	
Infrastructure Big Data	●	●		●
Log & Data-Collection	●	●		●
Use Cases prédéfinis	●	●		●
Log & Data-Analytics	●	●		●
Threat Intelligence Feeds	●	●		●
Security Event Notification	●			
Security Event Management		●		●
Security Incident Notification		●		●
Security Incident Management			●	
Swisscom CSIRT			●	
Incident Response Forensic			●	
Dashboard	●	●		●
Reporting en temps réel	●	●		●

● inclus dans le prix

Entrez dans l'avenir numérique avec Swisscom

Les entreprises visionnaires profitent des possibilités de la numérisation pour réinventer l'avenir. Swisscom explore également de nouveaux domaines d'activité grâce à de nombreuses innovations.

Notre mission consiste donc à vous aider à tirer profit des chances offertes par la numérisation. Pour vous, nous connectons la meilleure infrastructure de réseau avec une conservation des données sécurisée, une gestion de projet solide, une implémentation réussie et de nombreuses solutions innovantes.

Bienvenue au pays de tous les possibles.

Vous trouverez des informations supplémentaires, y compris pour contacter nos experts, sur [swisscom.ch/detection](https://www.swisscom.ch/detection)