CSIRT as a Service/CSIRT Rapid Response

Aucune entreprise n'est à l'abri d'un incident de sécurité. Leur traitement nécessite une Cybersecurity Incident Response Team (CSIRT) spécialisée, tels des pompiers face à un incendie.

La forte interconnexion et la complexité croissante des entreprises modernes augmentent les failles potentielles et le risque d'être touché par une cyberattaque.

En quoi consiste CSIRT as a Service/Rapid Response?

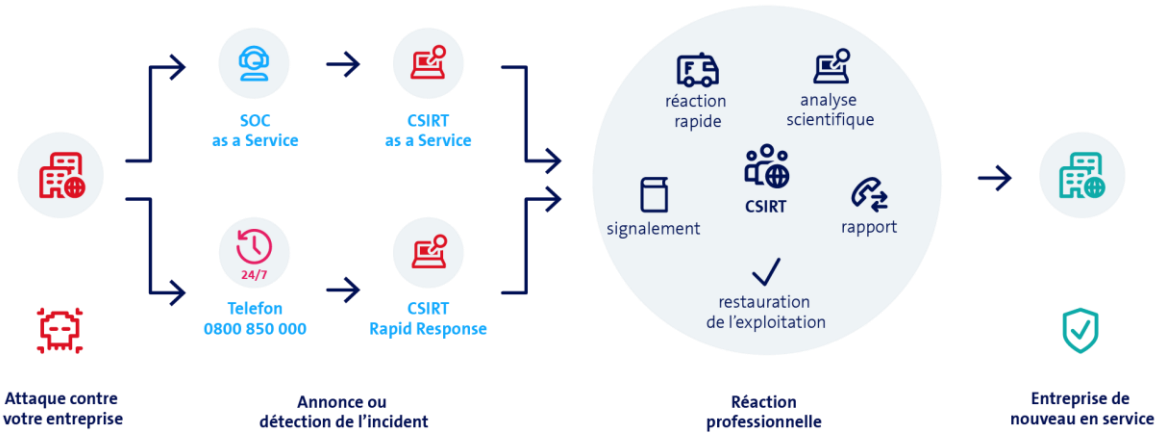
Les incidents de sécurité peuvent avoir un impact significatif sur l'entreprise, sans possibilité de toujours les éviter. La réaction rapide et professionnelle d'une Cybersecurity Incident Response Team (CSIRT) est alors décisive.

En cas d'incident vérifié, l'équipe aide le client à fournir la bonne réponse, à éliminer les logiciels malveillants et à rétablir l'activité. La prestation de base est disponible en deux variantes.

Vos avantages avec CSIRT as a Service/Rapid Response

- **Réponse rapide aux cyberattaques**
  Réagir de façon rapide et professionnelle aux incidents de sécurité.
- **Expertise et expérience de nos spécialistes en sécurité**
  Nos experts en sécurité sont parfaitement formés et disposent d'une grande expérience.
- **Contrôle de sécurité détaillé des systèmes compromis**
  Analyse rapide des vecteurs d'attaque et délimitation circonscription des systèmes concernés.
- **Aide au rétablissement de l'activité normale**
  Assistance pour réintégrer les systèmes concernés dans l'environnement de production.

Fonctionnement de CSIRT as a Service/Rapid Response



swisscom

Facts & Figures

Prestations de base	CSIRT as a Service avec contrat de service et SLA: L'analyse et la résolution sont réalisées par des experts Swisscom. Nous assurons le Security Incident Management à distance ou dans vos locaux et vous assistons dans la conservation des preuves et la communication avec les clients et les partenaires.
	CSIRT Rapid Response sans SLA: Cette solution est comparable à la prestation de base de CSIRTaaS. Dans ce cas précis, vous appelez le 0800 850 000 en cas d'incident, sans contrat de service. Aucun délai de réaction n'est toutefois garanti. Un onboarding, réalisé dès la phase initiale avec CSIRT as a Service, a lieu ici juste avant l'intervention. De plus, un forfait d'intervention est facturé et les tarifs horaires sont plus élevés.
Prestations en option	Rapport final selon les spécifications du client et dans le format souhaité, en allemand ou en anglais.
	Analyses supplémentaires en dehors du Security Incident Management (p. ex. attribution, mise en route de poursuites pénales, etc.).
	Contrôle préventif des systèmes non directement concernés.
	Conservation des preuves à des fins pénales, civiles et de droit public en Suisse.
	File Analysis Solution (uniquement pour les clients outsourcing), accès direct aux fichiers clients pour des analyses approfondies. Sans cette option, Swisscom dans son rôle de Provider ne peut pas accéder directement aux fichiers clients, comme le prévoit la directive de l'entreprise.
Services supplémentaires	Security Analytics as a Service (SAaaS): Nous sommes spécialisés dans la sécurité et le Big Data et mettons à votre disposition notre infrastructure Security Analytics éprouvée. Raccordez d'autres sources de log depuis le cloud, on premise 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.
	SOC as a Service (SOCaaS): Un tableau de bord vous fournit un aperçu des incidents de sécurité potentiels et confirmés à partir des historiques de votre entreprise, ainsi que des analyses avec des recommandations d'action concrètes. Vous réagissez de manière autonome aux incidents de sécurité critiques.
	Network Detection and Response as a Service (NDRaaS): Solution instaurée comme une extension des possibilités de détection statiques de SAaaS, via une Threat Detection dynamique basée sur des modèles de machine learning. Le service est fourni en collaboration avec une entreprise partenaire. 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 informé de manière proactive dès que des données commerciales et personnelles sensibles de votre entreprise apparaissent sur les réseaux publics et fermés (p. ex. Darknet). Vous appliquez en toute autonomie nos recommandations d'action en cas d'incidents de sécurité confirmés.
	Reconstruction de l'infrastructure IT par nos experts en infrastructure, selon les spécifications du client.

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

Swisscom (Suisse) SA Clients Commerciaux, case postale, CH-3050 Berne Téléphone 0800 800 900, www.swisscom.ch/enterprise