Network Detection and Response as a Service

En raison de leur complexité, les réseaux hybrides et hautement distribués sont difficiles à analyser et à surveiller. Le trafic réseau lui-même est souvent crypté et presque invisible, ce qui complique la détection de logiciels malveillants pour les outils de sécurité.

La détection des menaces sur le réseau avec des Indicators of Compromise statiques pour les logiciels malveillants connus ne suffit plus. Face aux nouvelles attaques évolutives, une défense basée sur l'analyse comportementale s'impose.

En quoi consiste NDR as a Service?

Le trafic réseau crypté et la détection des menaces avec des IOC statiques offrent trop de brèches aux hackers. La protection nécessaire n'est donc plus garantie.

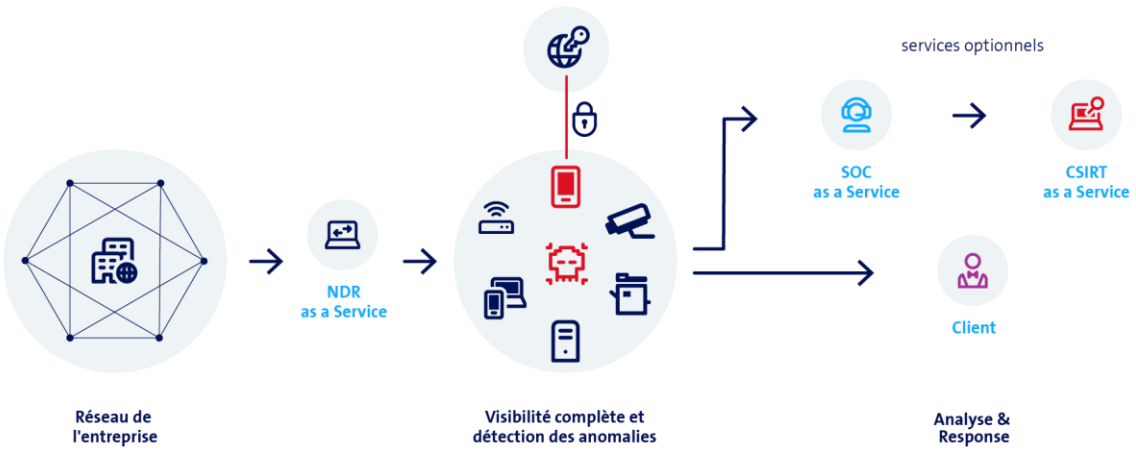
Network Detection and Response (NDR) propose des algorithmes IA puissants et avancés pour sécuriser de manière fiable les réseaux d'entreprise. La solution permet aussi de détecter et de résoudre rapidement les cyberattaques.

La visibilité maximale sur toutes les activités du réseau est au cœur de NDR.

Vos avantages avec NDR as a Service

- **Visibilité sur votre réseau**
  Identifier les failles avant qu'elles ne soient exploitées par les hackers (p. ex. services exposés, Shadow IT).
- **Accès au trafic réseau crypté**
  Détection automatique des attaques sur votre réseau avant que les données ne soient exfiltrées ou cryptées.
- **Use Cases et modèles ML prédéfinis**
  Corrélation automatisée entre les sources et visualisations intuitives.
- **Déploiement rapide**
  Pas de matériel supplémentaire ni d'agents nécessaires.

Fonctionnement de Network Detection and Response



swisscom

Facts & Figures

Prestations de base	On premise: NDR est hébergé sur le site du client et surveillé par le client. Les patches de sécurité sont intégrés en accord avec le client et le fabricant. Si le client recourt à la prestation Security Analytics as a Service (SAaaS) et Security Operation Center as a Service (SOCaaS), un forwarder basé sur un logiciel peut être installé dans l'environnement du client afin de transmettre les incidents de l'application au SOC pour analyse. En cas de soupçons d'incident de sécurité, le client est informé.
	Managed by Swisscom: NDR est hébergé et surveillé via une plateforme de logging dans un centre de calcul Swisscom. Les patches de sécurité sont intégrés par Swisscom. Si le client recourt à la prestation SAaaS et SOCaaS, Swisscom veille à ce que les incidents soient transmis par l'application au SOC pour analyse. En cas de soupçons d'incident de sécurité, le client est informé.
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.
	CSIRT as a Service (CSIRTaaS): L'analyse et la gestion des incidents de sécurité sont réalisées par des spécialistes 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.
	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.

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

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