Digital Risk Protection as a Service

Tout le monde laisse des empreintes numériques un peu partout en ligne. Et celles-ci sont difficiles à contrôler et surveiller. En effet, aujourd'hui, les collaborateurs sont répartis dans le monde entier et accèdent aux données via différents appareils ou réseaux.

Les informations personnelles, techniques ou organisationnelles, parfois confidentielles, sensibles ou secrètes, atterrissent souvent sur des réseaux publics ou fermés (dark web/deep web). Avec des risques pour les entreprises.

Qu'est-ce que Digital Risk Protection (DRP) as a Service?

Les solutions de sécurité classiques ne peuvent pas détecter des risques comme la perte/le vol de données, les problèmes de certificats, les sites web d'hameçonnage ou les copies de sites web dans l'ombre numérique. Nos analystes en cybermenaces collectent et analysent les données publiques et non publiques des entreprises.

La pertinence de ces données est garantie par différentes analyses automatiques et manuelles. Les incidents de sécurité potentiels (Security Incidents) font l'objet d'une escalade avec des recommandations d'actions au client.

Vos avantages avec DRP as a Service

- Identification des risques numériques
  Les menaces indésirables sur l'Internet public, mais aussi sur les réseaux fermés, sont identifiées afin de vous informer du niveau de menace actuel.
- Analystes en cybermenaces
  Détection automatique des hackers sur votre réseau avant que les données ne soient exfiltrées ou cryptées.
- Recommandations d'actions
  Vous décidez des mesures à prendre en fonction des recommandations d'actions proposées.
- Take down de sites web
  Les contenus indésirables, p. ex. un site d'hameçonnage, peuvent être retirés du réseau.

Fonctionnement de Digital Risk Protection as a Service

swisscom

Facts & Figures

Prestations de base	SearchLight Core: Fourniture du Managed Service SearchLight, qui détecte les pertes de données, protège la marque en ligne et réduit les possibilités d'attaque. Cela comprend l'accès au SearchLight Intelligence Repository, aux abonnements, aux rapports et à Shadow Search et couvre les types de risques suivants: données de connexion du personnel, usurpation d'identité de domaines (impersonating domains), problèmes de certificats.
	SearchLight MSSP Edition: En plus de la variante Core, les types de risques suivants sont couverts: documents sensibles marqués, données du personnel, pertes de données techniques, usurpation d'identité de domaines (impersonating domains), risques pour les applications mobiles, faux profils sur les réseaux sociaux, failles exploitables, problèmes de certificats, ports ouverts, appareils mal configurés.
	SearchLight MSSP Premium: En plus de la variante Edition, les prestations suivantes sont fournies: tous les risques de la plateforme SearchLight, y compris ceux proposant un état des lieux et un accès au dark web et aux forums fermés.
Prestations en option	Managed Takedown: Retraits entièrement gérés avec un workflow intégré dans SearchLight. Le service standard comprend des take-downs prédéfinis. Le client peut en déclencher un à partir de n'importe quelle alarme. Il peut alors suivre l'état de l'alarme, consulter les dernières mesures prises par l'équipe de take-down et déposer des documents tels que des modèles d'e-mail.
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'actions 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.
	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.

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

Les informations contenues dans ce document ne constituent pas une offre ferme. Sous réserve de modifications.

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