Digital Risk Protection as a Service

Menschen hinterlassen online überall digitale Fussabdrücke. Diese lassen sich kaum kontrollieren und überwachen. Denn die Mitarbeitenden sind heute über die ganze Welt verteilt und greifen mit verschiedenen Geräten und über diverse Netze auf Daten zu.

Persönliche, technische oder organisatorische Informationen, teils vertraulich, sensibel oder geheim, werden oft in öffentlichen oder geschlossenen Netzen (Dark Web/Deep Web) wiedergefunden. Das birgt Gefahren für Unternehmen.

Was ist Digital Risk Protection (DRP) as a Service?

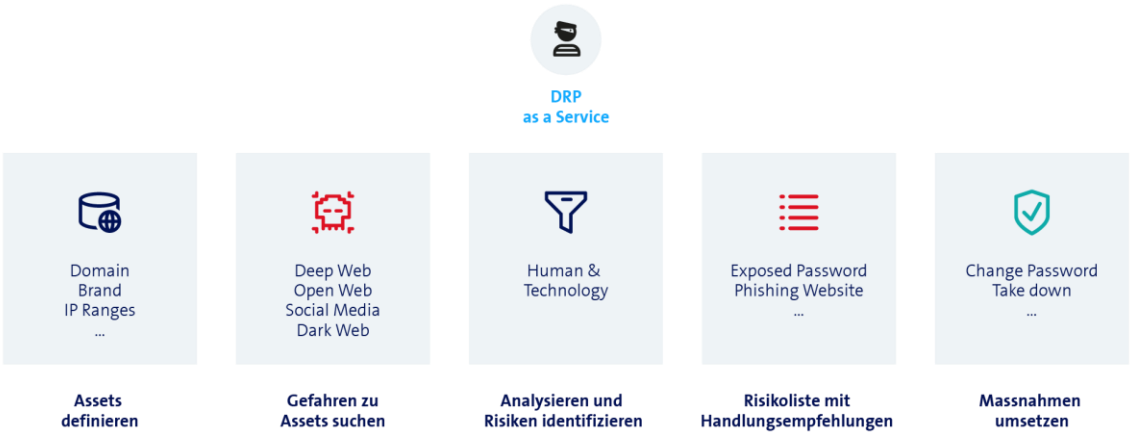
Herkömmliche Sicherheitslösungen können die Risiken wie Datenverlust/Diebstahl, Zertifikatsprobleme, Phishing-Webseiten oder Kopien von Webseiten im digitalen Schatten nicht detektieren. Unsere Cyberthreat-Analysten sammeln und analysieren öffentlich und nicht öffentlich verfügbare Daten über ein Unternehmen.

Die Relevanz dieser Daten wird durch verschiedene automatische und manuelle Analysen gewährleistet. Potenzielle Sicherheitsvorfälle (Security Incidents) werden mit einer Handlungsempfehlung an den Kunden eskaliert.

Ihre Nutzen mit DRP as a Service

- **Identifizierung von digitalen Risiken**
  Unerwünschte Gefährdungen im öffentlichen Internet, aber auch in geschlossenen Netzen werden identifiziert, damit Sie über die aktuelle Bedrohungslage informiert sind.
- **Cyberthreat-Analysten**
  Automatisierte Erkennung von Angreifern in Ihrem Netzwerk, bevor Daten exfiltriert oder verschlüsselt werden.
- **Vorschlag von Handlungsempfehlungen**
  Sie entscheiden über die einzuleitenden Massnahmen aufgrund der vorgeschlagenen Handlungsempfehlungen.
- **Takedown von Websites**
  Unerwünschte Inhalte, wie beispielsweise eine Phishing-Webseite, können vom Netz genommen werden.

So funktioniert Digital Risk Protection as a Service



swisscom

Facts & Figures

Basisleistungen	SearchLight Core: Bereitstellung des SearchLight Managed Service, der Datenverluste aufdeckt, die Online-Marke schützt und die Angriffsfläche reduziert. Beinhaltet den Zugriff auf das SearchLight Intelligence Repository, Abonnemente, Berichte und Shadow Search. Deckt die folgenden Risikotypen ab: Anmeldedaten von Mitarbeitenden, Identitätsmissbrauch von Domänen (impersonating domains), Zertifikatsprobleme.
	SearchLight MSSP Edition: Zusätzlich zur Serviceausprägung Core werden die folgenden Risikotypen abgedeckt: Sensible, markierte Dokumente, Mitarbeiterdaten, technische Datenverluste, Identitätsmissbrauch von Domänen (impersonating domains), Risiken für mobile Apps, gefälschte Social Media Profile, ausnutzbare Schwachstellen, Zertifikatsprobleme, offene Ports, falsch konfigurierte Geräte.
	SearchLight MSSP Premium: Zusätzlich zur Serviceausprägung Edition werden folgende Leistungen erbracht: Alle Risiken der SearchLight-Plattform, einschliesslich derer, die Situationsbewusstsein und Einblicke in das Dark Web und geschlossene Foren bieten.
Optionale Leistungen	Managed Takedown: Vollständig verwaltete Takedowns mit einem integrierten Workflow in SearchLight. Zum Standardservice gehören vorgefertigte Takedowns. Der Kunde kann von jedem Alarm aus einen Takedown einleiten. Von dort aus kann der Kunde den Status des Alarms verfolgen, alle Aktualisierungen der vom Takedown-Team ergriffenen Massnahmen einsehen und Dokumente wie E-Mail-Muster hochladen.
Zusatzservices	Security Analytics as a Service (SAaaS): Wir sind Fachleute in den Themen Security und Big Data und stellen Ihnen unsere bewährte Security-Analytics-Infrastruktur zur Verfügung. Schliessen Sie weitere Logquellen aus der Cloud, On-Premises oder von einem Managed Provider an und erhalten Sie im Dashboard einen Überblick über potenzielle Sicherheitsvorfälle. Analyse und Reaktion auf Sicherheitsvorfälle übernehmen Sie selbst.
	SOC as a Service (SOCaaS): Sie erhalten via Dashboard einen Überblick über potenzielle und bestätigte Sicherheitsvorfälle aus definierten Logdaten Ihrer Unternehmung sowie Analysen mit konkreten Handlungsempfehlungen. Auf kritische Security Incidents reagieren Sie selbständig.
	CSIRT as a Service (CSIRTaaS): Zur Analyse und Bewältigung von Sicherheitsvorfällen ziehen Sie Fachleute von Swisscom bei. Wir leiten den Security-Incident-Management-Prozess remote oder bei Ihnen vor Ort und unterstützen Sie bei der Beweissicherung sowie der Kommunikation mit Kunden und Partnern.
	Network Detection and Response as a Service (NDRaaS): Wird als Erweiterung zu den statischen Erkennungsmöglichkeiten von SAaaS durch eine dynamische Threat Detection basierend auf Machine-Learning-Modellen unterstützt. Der Service wird zusammen mit einer Partnerfirma erbracht. Der Mehrwert ergibt sich in den Bereichen Web (Proxy) und Netzwerk (DNS, Netflow und Firewall-Traffic-Daten), was maximale Visibilität erlaubt.

Mehr Informationen und den Kontakt zu unserem Experten finden Sie auf **swisscom.ch/drp**

Swisscom (Schweiz) AG Geschäftskunden, Postfach,
CH-3050 Bern, Tel. 0800 800 900, www.swisscom.ch/enterprise

swisscom