Digital Risk Protection as a Service

Muoversi nel mondo online significa lasciare impronte digitali ovunque. Controllarle e monitorale è impossibile. Oggi i collaboratori sono sparsi in tutto il mondo e accedono ai dati con tanti device e su diverse reti.

Capita spesso che informazioni personali, tecniche oppure organizzative, magari anche riservate, sensibili o segrete, vengano ritrovate in reti pubbliche o chiuse (dark web / deep web). Con grandi rischi per le imprese.

Che cos'è Digital Risk Protection (DRP) as a Service?

Le soluzioni di sicurezza tradizionali non sono in grado di rilevare rischi come le fughe e/o i furti di dati, i problemi con i certificati, i siti web di phishing e le copie di siti web nella «digital shadow». I nostri analisti Cyberthreat raccolgono e analizzano i dati di un'azienda disponibili in ambienti pubblici o non pubblici.

La rilevanza di questi dati viene garantita da diverse verifiche automatiche e manuali. I potenziali incidenti di sicurezza vengono portati all'attenzione del cliente con una raccomandazione operativa.

I vantaggi di DRP as a Service

- Identificazione dei rischi digitali
  Vengono identificati i pericoli indesiderati sulla rete internet pubblica ma anche nelle reti chiuse per tenervi sempre informati sulle minacce correnti.
- Analisti Cyberthreat
  Rilevamento automatizzato dei malintenzionati nella vostra rete prima che possano rubare o cifrare dati.
- Proposta di raccomandazioni operative
  Decidete voi che misure adottare sulla base delle raccomandazioni operative proposte.
- Takedown di siti web
  I contenuti indesiderati, come ad esempio un sito web di phishing, possono essere rimossi dalla rete.

Come funziona Digital Risk Protection as a Service

swisscom

Facts & Figures

Prestazioni di base	SearchLight Core: Fornitura del SearchLight Managed Service, che rileva le fughe di dati, protegge il marchio online e limita le potenziali vulnerabilità. Include l'accesso al SearchLight Intelligence Repository, abbonamenti, report e Shadow Search. Copre i seguenti tipi di rischio: credenziali dello staff, abuso d'identità nei domini (impersonating domains), problemi con i certificati.
	SearchLight MSSP Edition: In aggiunta alla versione Core, vengono coperti i seguenti tipi di rischio: documenti sensibili contrassegnati, dati dei collaboratori, fughe di dati tecnici, rischi per le applicazioni mobili, profili contraffatti sui social media, vulnerabilità sfruttabili, porte aperte, errori di configurazione dei device.
	SearchLight MSSP Premium: In aggiunta alla versione Edition, vengono fornite le prestazioni seguenti: tutti i rischi della piattaforma SearchLight, inclusi quelli che offrono consapevolezza della situazione e accesso al dark web e a forum chiusi.
Prestazioni opzionali	Managed Takedown: Takedown completamente gestiti con un workflow integrato in SearchLight. Il servizio standard include i takedown predefiniti. Il cliente può disporre un takedown per ogni allarme. Da quel momento, il cliente può seguire lo stato dell'allarme, consultare tutti gli aggiornamenti sulle misure adottate dal Takedown Team e caricare documenti come modelli di e-mail.
Servizi supplementari	Security Analytics as a Service (SAaaS): Siamo specialisti in fatto di Security e big data e mettiamo a vostra disposizione la nostra affermata infrastruttura per la Security Analytics. Integrate ulteriori fonti di log dal cloud, on premises oppure da un managed provider e ricevete nel dashboard una panoramica dei potenziali incidenti di sicurezza. Vi occupate in autonomia di analisi e reazione agli incidenti di sicurezza.
	SOC as a Service (SOCaaS): Ricevete sul dashboard una panoramica di tutti gli incidenti di sicurezza potenziali e confermati in base alla valutazione di dati di log definiti della vostra azienda nonché analisi con raccomandazioni operative concrete. In caso di incidenti di sicurezza critici reagite in autonomia.
	CSIRT as a Service (CSIRTaaS): Ricorrete agli specialisti Swisscom nelle fasi di analisi e risposta agli incidenti di sicurezza. Gestiamo il processo di security incident management, in remoto oppure da voi in azienda, e vi assistiamo nelle fasi di raccolta delle prove e comunicazione con clienti e partner.
	Network Detection and Response as a Service (NDRaaS): Integra le funzionalità di rilevamento statiche di SAaaS con una Threat Detection dinamica basata su modelli di machine learning. Il servizio viene fornito insieme a una ditta partner. Offre un valore aggiunto su web (proxy) e rete (DNS, netflow e firewall traffic data), garantendo la massima visibilità.

Trovate maggiori informazioni e il contatto con il nostro esperto su **swisscom.ch/drp**

Swisscom (Svizzera) SA Clienti Commerciali, casella postale,
CH-3050 Berna, Telefono 0800 800 900, www.swisscom.ch/enterprise