Security Analytics / Security Operation Center as a Service

La complessità delle infrastrutture odierne, spesso ibride, rende più difficile analizzare gli incidenti di sicurezza e reagire in modo rapido e professionale.

I sistemi SIEM (Security Incident and Event Management) per l'analisi completa hanno un prezzo elevato e non è facile trovare persone qualificate che assicurino l'operatività h24. Ma mentre la pressione sui costi grava sui budget e sulle risorse delle imprese, i cybercriminali affilano le loro armi.

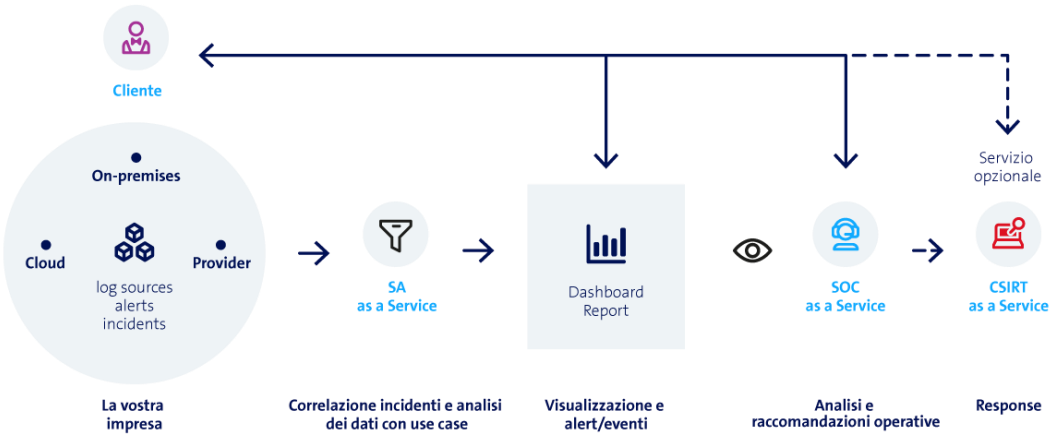
Che cos'è Security Analytics und SOC as a Service?

Security Analytics (SA) as a Service è una piattaforma big data scalabile che raccoglie, aggrega e correla dati di log da diverse fonti. Le fonti di dati necessarie vengono identificate sulla base di use case standardizzati per la Threat Detection che si concentrano sulle minacce informatiche del momento.
Nel Security Operations Center as a Service (SOCaaS) lavorano professionisti della Security che analizzano gli eventi di sicurezza, li valutano e informano il cliente con raccomandazioni operative per rispondere agli incidenti di sicurezza identificati.

I vantaggi di SA e SOC as a Service

- Tempi di reazione e inattività ridotti al minimo grazie al funzionamento h24
  Analisi ininterrotta degli eventi di sicurezza nella vostra impresa.
- Specialisti di Security con esperienza e competenza al vostro servizio
  Personale altamente specializzato con una vasta esperienza pluriennale.
- Il livello di sicurezza richiesto senza i costi di un'infrastruttura interna per la Security
  Sfruttate un'infrastruttura SIEM centrale.
- Use case individuali per l'analytics
  Oltre agli use case per l'analytics messi a disposizione da Swisscom, sviluppiamo anche i vostri use case individuali.

Come funzionano SA e SOCaaS



Facts & Figures

Prestazioni di base	Security Analytics as a Service: 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: 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.
Prestazioni opzionali	Sviluppiamo i vostri use case individuali.
	Scegliete voi la data retention.
Servizi supplementari	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. Offre un valore aggiunto su web (proxy) e rete (DNS, netflow e firewall traffic data), garantendo la massima visibilità.
	Digital Risk Protection as a Service (DRPaaS): Venite informati proattivamente della presenza di informazioni personali e commerciali sensibili della vostra azienda in reti pubbliche e chiuse (ad es. darknet). Vi occupate in autonomia dell'implementazione delle nostre raccomandazioni operative per gli incidenti di sicurezza confermati.

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

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

swisscom