Security Operation Center as a Service

Il nostro team di esperti monitora e si occupa della vostra infrastruttura di sicurezza 24 ore su 24, vi allerta in caso di problemi e propone contromisure in modo da avere il controllo sugli incidenti rilevanti per la sicurezza.

Con il nostro Security Operation Center as a Service (SOCaaS) ci occupiamo dell'analisi di potenziali minacce.
Un Security Operation Center è decisivo al fine di garantire la sicurezza della vostra organizzazione e individuare e combattere efficacemente potenziali minacce. Il nostro personale altamente specializzato nella sicurezza analizza gli avvisi di sicurezza (security alert) e identifica e valuta gli incidenti di sicurezza (security incident) che ne derivano, riguardo alla loro criticità e alle conseguenze dei possibili rischi per la vostra organizzazione. Prime reazioni in ambito pre-approved action come anche raccomandazioni operative vi consentiranno di reagire velocemente ai cyberattacchi.

I vantaggi di SOCaaS

Veloce individuazione dei cyberattacchi

Monitoraggio 7/24 degli avvisi di sicurezza della vostra infrastruttura di sicurezza. ✓

Verifica delle possibili ripercussioni sulla vostra organizzazione

Identificazione e valutazione degli incidenti di sicurezza riguardo alla loro criticità, conseguenze e potenziali rischi per la vostra organizzazione. ✓

Prima reazione a cyberattacchi attivi

In ambito pre-approved action vengono effettuate autonomamente misure di contenimento da parte del SOC. ✓

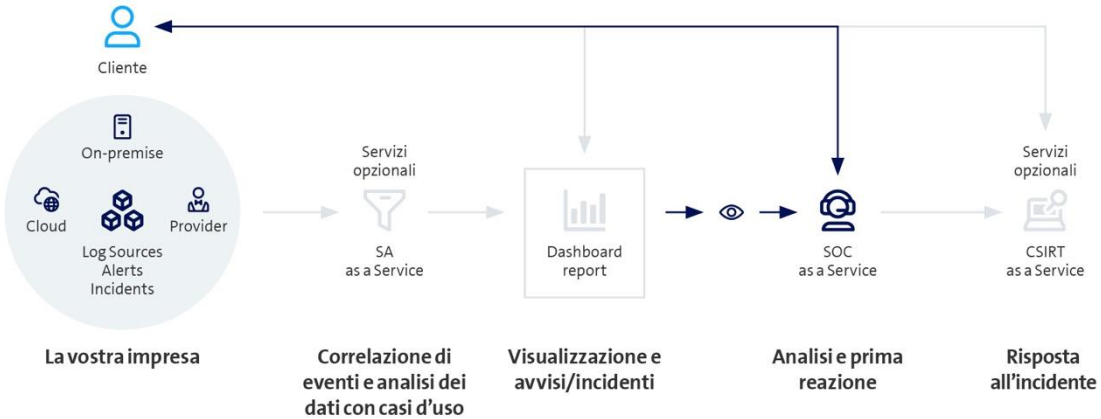
Consultazione con raccomandazioni operative concrete e istruzioni

Consulenza diretta riguardo all'ulteriore procedura da seguire in caso di un evento critico per la sicurezza. ✓

Esperienza intersettoriale in materia di sicurezza e competenza

Vasta competenza ed esperienza pluriennale del personale esperto in materia di sicurezza che vi segue. ✓

Come funziona SOCaaS



swisscom

Facts & Figures

Servizi di base

Il Security Alert Management comprende tutte le attività di monitoraggio e analisi di eventi e avvisi di sicurezza che vengono generati nell'ambito del servizio Security Analytics as a Service o attraverso un sistema di sicurezza supportato da terze parti. Gli incidenti di sicurezza identificati vengono analizzati nel dettaglio e la criticità, le conseguenze e il potenziale rischio per l'organizzazione vengono valutati e verificati assieme al cliente. Qualora dovesse trattarsi di cyberattacchi attivi, sulla base di procedure e processi affermati vengono concordate con i clienti e avviate le prime misure di contenimento oppure esse vengono effettuate autonomamente in ambito pre-approved action da parte del SOC.

Servizi aggiuntivi

- **Security Analytics as a Service (SAaaS):**
  Il nostro personale esperto è specializzato in sicurezza e big data e mette a vostra disposizione la comprovata infrastruttura Security Analytics di Swisscom in versione piattaforma SOC. Potrete collegare ulteriori fonti di log dal cloud, on-premise o da un managed provider per avere nel dashboard una panoramica dei potenziali incidenti di sicurezza. L'analisi e la reazione agli incidenti di sicurezza sarà compito vostro.
- **CSIRT as a Service (CSIRTaaS):**
  Per analizzare e far fronte agli incidenti di sicurezza potrete rivolgervi al personale esperto Swisscom. Noi guideremo il processo di Security Incident Management da remoto o in loco presso di voi e vi aiuteremo nella raccolta delle prove nonché nella comunicazione con clienti e partner.
- **Network Detection and Response as a Service (NDRaaS):**
  Come ampliamento delle possibilità statiche di individuazione di SAaaS, questo servizio viene supportato da un rilevamento dinamico delle minacce sulla base di modelli di apprendimento automatico. Il valore aggiunto risulta nei campi del web (Proxy) e della rete (DNS, Netflow e dati di traffico del firewall), consentendo la massima visibilità.
- **Digital Risk Protection as a Service (DRPaaS):**
  Verrete informati in modo proattivo sull'esistenza di informazioni aziendali e personali sensibili riguardo alla vostra impresa su reti ufficiali e private (p. es. Darknet). Le nostre raccomandazioni operative riguardo a potenziali incidenti di sicurezza verranno messe in atto da voi autonomamente.
- **XDR as a Service (by Palo Alto Networks):**
  La gestione delle licenze, la gestione del ciclo di vita e dello stato degli agenti XDR, la configurazione delle security policy, la comunicazione di nuove funzioni e variazioni, come anche una valutazione annuale delle security policy sono a cura di Swisscom.
- **Microsoft XDR as a Service:**
  La gestione del ciclo di vita degli agenti XDR, la gestione dello stato dei componenti per i servizi, la configurazione delle security policy, la comunicazione di nuove funzioni e variazioni, come anche una valutazione annuale delle security policy sono a cura di Swisscom.

Per maggiori informazioni e per contattare i nostri esperti si prega di consultare swisscom.ch/soc

Swisscom (Svizzera) SA Enterprise Customers, casella postale, CH-3050 Berna, tel. 0800 800 900, www.swisscom.ch/enterprise