



# Aumentate la vostra cybersicurezza con una piattaforma Security Analytics che individua le minacce del vostro ambiente di sistema in tempo reale.

**Con Security Analytics as a Service (SAaaS), Swisscom offre una piattaforma per individuare in modo proattivo gli incidenti di sicurezza su tutto l'ambiente di sistema.**

Nel mondo attuale, altamente interconnesso e digitale, è fondamentale proteggere efficacemente le proprie

risorse aziendali da cyberminacce. E proprio a questo riguardo entra in gioco Security Information and Event Management (SIEM): uno strumento indispensabile per proteggere a tutto campo la vostra impresa e individuare in modo proattivo e contrastare i potenziali incidenti di sicurezza.

## I vantaggi di SAaaS

### Piattaforma SIEM come servizio

Beneficerete di una piattaforma SIEM per la raccolta, l'aggregazione e la correlazione dei dati log da varie fonti di dati.



### Rilevamento delle minacce – casi d'uso

Possibilità di veloce reazione a potenziali incidenti di sicurezza (security incident) attraverso i casi d'uso nel rilevamento delle minacce.



### Compliance e Reporting

Compliance e Security Reporting per requisiti normativi.



### Scalabilità e flessibilità

Scalabilità e capacità di adattamento per il crescente ambiente di sistema.

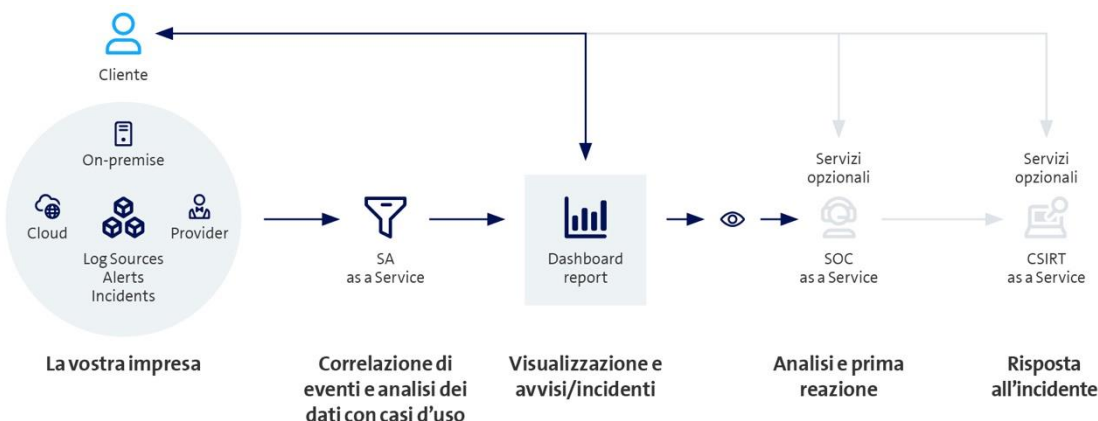


### Funzioni base di assistenza

Funzioni base di assistenza della piattaforma SOC: gestione degli incidenti, gestione del cambiamento, gestione delle richieste di assistenza, SLA reporting.



## Come funziona SAaaS





## Facts & Figures

### Servizi di base

Security Analytics as a Service viene impiegato per la raccolta, l'aggregazione e la correlazione dei dati log da varie fonti di dati per individuare rapidamente e reagire a potenziali incidenti di sicurezza. I requisiti normativi vengono trattati attraverso il Compliance e Security Reporting. La flessibile piattaforma Security Analytics si adatta senza problemi al vostro crescente ambiente di sistema adeguandosi alle vostre mutevoli esigenze.

### Servizi opzionali

- Noi sviluppiamo i vostri casi d'uso individuali.
- Voi stessi definite la durata di conservazione dei dati.
- Voi scegliete la tecnologia di rilevamento delle minacce.

### Servizi aggiuntivi

- **Security Operation Center as a Service (SOCaaS):**  
Il nostro personale altamente specializzato nella sicurezza analizza gli avvisi di sicurezza (security alert) e identifica e valuta gli incidenti di sicurezza (security incident) da ciò risultanti 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. Agli incidenti di sicurezza critici reagirete voi stessi autonomamente.
- **CSIRT as a Service (CSIRTaaS):**  
Per analizzare e far fronte agli incidenti di sicurezza consultate il personale esperto Swisscom. 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](https://www.swisscom.ch/soc)