Security Analytics / Security Operation Center as a Service

swisscom

Die Komplexität heutiger Infrastrukturen – oft hybrid – erschwert die Analyse von Sicherheitsvorfällen und die schnelle und professionelle Reaktion.

SIEM-Systeme (Security Incident and Event Management) für die umfassende Analyse sind teuer und die Fachleute für einen 7x24-Betrieb rar. Doch während in den Unternehmen der Kostendruck auf Budgets und Ressourcen lastet, rüsten Cyberkriminelle auf.

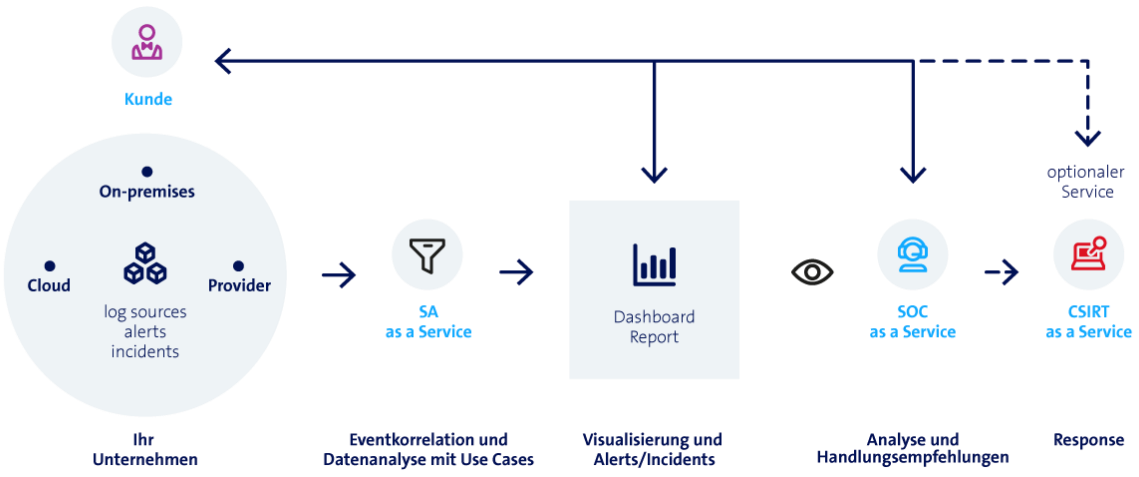
Was ist Security Analytics und SOC as a Service?

Security Analytics (SA) as a Service ist eine skalierbare Big-Data-Plattform, die Logdaten aus verschiedenen Quellen sammelt, aggregiert und korreliert. Die Identifizierung der benötigten Datenquellen basiert auf standardisierten Threat Detection Use Cases, die die aktuellen Cyberbedrohungen adressieren.
Beim Security Operations Center as a Service (SOCaaS) arbeiten professionelle Security Spezialist*innen, die Security Events analysieren, bewerten und Sie als Kunde mit Handlungsempfehlungen informieren für die Adressierung der identifizierten Sicherheitsvorfälle.

Ihre Nutzen mit SA und SOC as a Service

- **Minimierte Ausfall- und Antwortzeiten dank Betrieb rund um die Uhr**
  Ununterbrochene Analyse von Sicherheitsereignissen in ihrem Unternehmen.
- **Expertise und Erfahrung unserer Security-Fachleute**
  Top ausgebildete Security-Spezialist*innen mit breiter und langjähriger Erfahrung.
- **Gefordertes Sicherheitsniveau ohne die Kosten einer eigenen Security-Infrastruktur**
  Sie profitieren von einer zentralen SIEM-Infrastruktur.
- **Individuelle Analytics Use Cases**
  Wir entwickeln neben den von Swisscom zur Verfügung stehenden Analytics Use Cases auch ihre individuellen Use Cases.

So funktionieren SA und SOCaaS



Facts & Figures

Basisleistungen	Security Analytics as a Service: 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: 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.
Optionale Leistungen	Wir entwickeln ihre individuellen Use Cases.
	Sie definieren selbst die Data Retention.
Zusatzservices	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 Mehrwert ergibt sich in den Bereichen Web (Proxy) und Netzwerk (DNS, Netflow und Firewall-Traffic-Daten), was maximale Visibilität erlaubt.
	Digital Risk Protection as a Service (DRPaaS): Sie werden proaktiv informiert über das Vorkommen von sensiblen Geschäfts- und persönlichen Informationen Ihres Unternehmens in öffentlichen und geschlossenen Netzen (z.B. Darknet). Unsere Handlungsempfehlungen für bestätigte Sicherheitsvorfälle setzen Sie selbständig um.

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

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