Security Analytics/Security Operation Center as a Service

The complexity of today's infrastructures, which are often hybrid, makes it difficult to analyse security incidents and ensure a rapid, professional response.

SIEM (Security Incident and Event Management) systems for comprehensive analysis are expensive and companies will rarely have the specialist staff to support 24/7 operation. And while cost pressures are impacting company budgets and resources, cybercriminals are stocking up their arsenals.

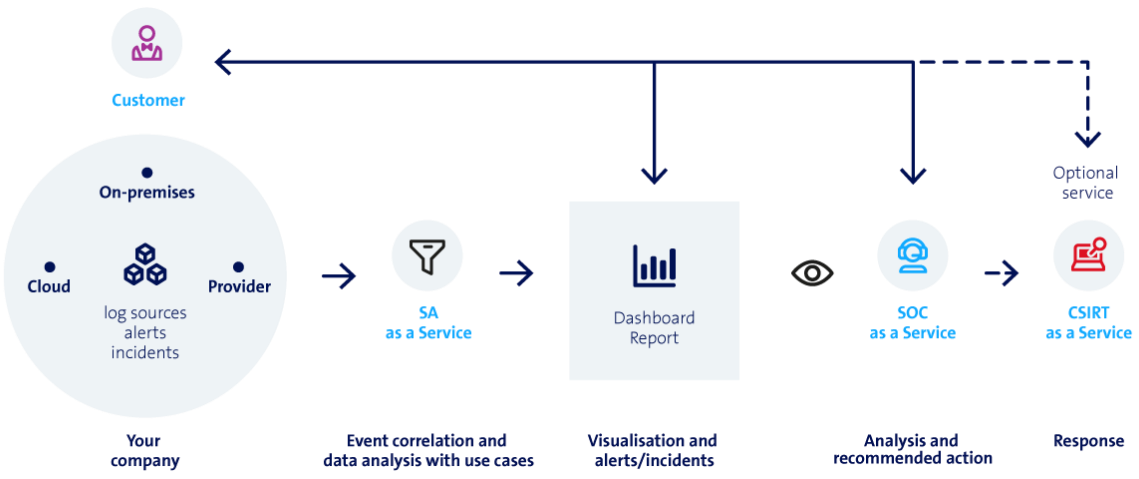
What is Security Analytics and SOC as a Service?

Security Analytics (SA) as a Service is a scalable big data platform for collecting, aggregating and correlating log data from a range of different sources. Required data sources are identified on the basis of standardised threat detection use cases that address current cyber threats.
With Security Operations Center as a Service (SOCaaS), professional security specialists analyse and assess security events before recommending action you can take to address any security incidents.

The benefits of SA and SOC as a Service

- Minimal downtime and response times thanks to round-the-clock operation
  Uninterrupted analysis of security events in your company.
- Access to the expertise and experience of our security experts
  Our highly trained security specialists offer extensive experience acquired over many years.
- The required security level without the costs of your own security infrastructure
  You benefit from a central SIEM infrastructure.
- Individual analytics use cases
  In addition to providing the standard Swisscom analytics use cases, we also develop individual use cases for you.

How SA and SOCaaS work



swisscom

Facts & Figures

Basic services	Security Analytics as a Service: We are experts in security and big data, and provide you with our proven security analytics infrastructure. Connect additional log sources from the cloud, on premise or from a managed provider, and see an overview of potential security incidents on the dashboard. You can analyse and respond to security incidents yourself.
	SOC as a Service: This dashboard provides an overview of potential and confirmed security incidents from your company's defined log data as well as analyses with specific recommendations for action. You react independently to critical security incidents.
Optional services	We develop your individual use cases.
	You define the data retention period yourself.
Additional services	CSIRT as a Service (CSIRTaaS): You call in Swisscom experts for the analysis and management of security incidents. We manage the security incident management process remotely or on your premises and support you in securing evidence and communicating with customers and partners.
	Network Detection and Response as a Service (NDRaaS): Supported by dynamic threat detection based on machine learning models as an extension to the static detection capabilities of SAaaS. The added value arises in the areas of web (proxy) and network (DNS, NetFlow and firewall traffic data), which allows maximum visibility.
	Digital Risk Protection as a Service (DRPaaS): You are proactively informed if sensitive business and personal information from your company is found on public and closed networks (e.g. the dark web). You implement our recommended actions for confirmed security incidents independently.

You can find more information and our expert's contact details at **swisscom.ch/soc**

Swisscom (Switzerland) Ltd Enterprise Customers, P.O. Box,
CH-3050 Berne, Telephone 0800 800 900, www.swisscom.ch/enterprise

swisscom