Security Analytics as a Service

Boost your cyber security with a Security Analytics Platform that detects threats to your system landscape in real time.

Our Security Analytics as a Service is a state-of-the-art cybersecurity solution based on our AI-powered SOC platforms to effectively address the ever-growing threat of cyberattack.
In the current highly connected and digitised world, it is essential for you to effectively protect your corporate resources against cyber threats. This is where our Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) comes in- essential tools to protect your business and proactively detect and respond to potential security incidents.

Your advantages with SAaaS

SIEM Platform

SIEM platform for the collection, aggregation and correlation of log data from different data sources in conjunction with the SOAR platform used by the Security Operation Center for orchestration and automation. ✓

Threat Detection Use Cases

A rapid response to potential security incidents is facilitated by AI-powered threat detection use cases. ✓

Compliance and Reporting

Compliance and Security Reporting for regulatory requirements. ✓

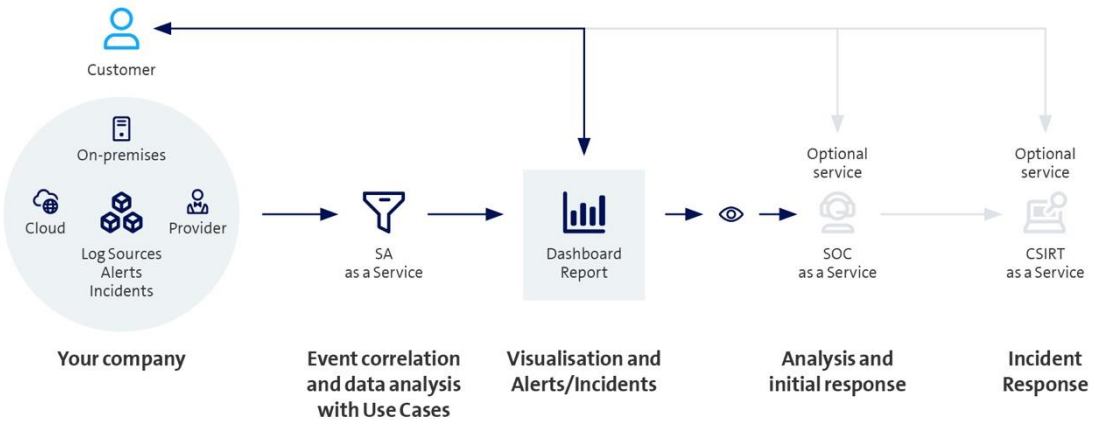
Scalability and Flexibility

Scalability and the capacity to adapt to a growing system landscape. ✓

Basic Service Functions

Basic Service Functions of the SOC Platform: Incident Management, Change Management, Service Request Management, SLA Reporting. ✓

How SAaaS works



swisscom

Facts & Figures

Basic services

Security Analytics as a Service (SAaaS) is used to quickly detect and respond to potential security incidents. By collecting, aggregating and correlating log data from multiple sources, attacks can be detected early. SAaaS then draws on the Security Orchestration, Automation and Response (SOAR) capabilities to take immediate, semi-automated countermeasures and contain the attack as quickly as possible. Our flexible SOC platform based on Microsoft, Palo-Alto Networks or Splunk seamlessly scales as your system grows and adapts to your changing needs. Regulatory and compliance requirements are also met via special security reports and customer-specific use cases.

Optional services

- We develop your individual Use Cases.
- You define the Data Retention Time.
- You select the Threat Detection Technology.
- You can detect and alert on critical vulnerabilities through the integration of vulnerability management.

Additional services

- **Security Operation Center as a Service (SOCaaS):**
  Our professional security specialists analyse security alerts. They then identify and assess the resulting security incidents based on how critical they are and the impact of possible risks to your organisation. Initial responses within the context of pre-approved actions and operational recommendations allow you to respond quickly to cyber attacks. You respond independently to critical security incidents.
- **CSIRT as a Service (CSIRTaaS):**
  You consult experts from Swisscom to analyse and manage security incidents. We carry out the security incident management process remotely or on your premises and support you in documenting evidence and communicating with customers and partners.
- **Network Detection and Response as a Service (NDRaaS):**
  An extension to the static detection options of SAaaS, it is supported by a dynamic Threat Detection based on Machine-Learning Models. It brings added value in the areas of: Web (Proxy) and Network (DNS, Netflow and Firewall Traffic Data), which facilitates maximum transparency.
- **Digital Risk Protection as a Service (DRPaaS):**
  You are proactively informed when sensitive business and personal information from your company features in public and closed networks (e.g. darknet).
  You can independently implement our operational recommendations for handling potential security incidents.
- **XDR as a Service (by Palo Alto Networks):**
  Swisscom is responsible for: licence management, lifecycle and health management of the XDR agents, configuration of the security policies, communicating new functions and changes, and an annual security policy assessment.
- **Microsoft XDR as a Service:**
  Swisscom is responsible for the: lifecycle management of the XDR agents, health management of the service components, configuration of the security policies, communicating new functions and changes, and an annual security policy assessment.

You can find more information and the contact details of our experts at swisscom.ch/soc

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

swisscom