



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

With Security Analytics as a Service (SAaaS), Swisscom provides a platform to proactively detect security incidents throughout the entire system landscape.

In the current highly connected and digitised world, it is essential for you to effectively protect your corpo-

rate resources against cyber threats. This is where our Security Information and Event Management (SIEM) comes in. It is an indispensable tool that comprehensively protects your company and proactively detects and averts potential security incidents.

Security Analytics as a Service

Your advantages with SAaaS

SIEM Platform as a Service

You benefit from an SIEM platform that collects, aggregates and correlates Log Data from various data sources.



Threat Detection Use Cases

Quick response to potential security incidents thanks to 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.

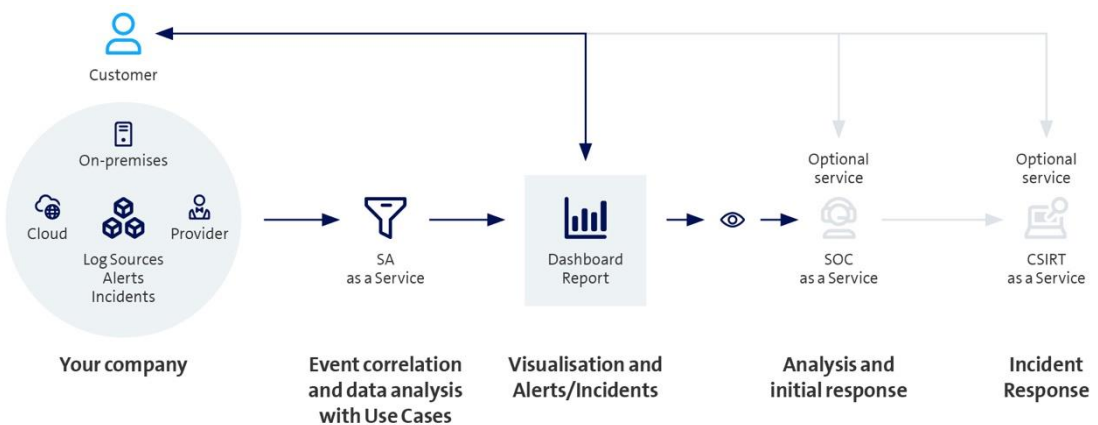


Basic Service Functions

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 is used for collecting, aggregating and correlating Log Data from various sources, to quickly detect and respond to potential security incidents. Regulatory requirements are dealt with through the Compliance and Security Reporting. The flexible Security Analytics Platform scales seamlessly with your growing system landscape, so as to adapt to changing requirements.

Optional services

- We develop your individual Use Cases.
- You define the Data Retention Time.
- You select the Threat Detection Technology.

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](https://www.swisscom.ch/soc)