Security Operation Center as a Service

Our experienced team monitors and manages your security infrastructure around the clock, alerts you in the event of problems, and suggests countermeasures to maintain control over incidents relating to security.

Our Security Operation Center as a Service (SOCaaS) conducts the analysis of any potential threats.
A Security Operation Center is vital for ensuring the security of your organisation and effectively detecting and averting potential threats. 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.

Your advantages with SOCaaS

Quick detection of cyber attacks

7/24 Monitoring of the security alerts of your security infrastructure. ✓

Review of the potential impact on your organisation

Identification and assessment of security incidents based on how critical they are, possible level of impact, and potential risk to your organisation. ✓

Initial response to active cyber attacks

Mitigation measures are performed autonomously through the SOC within the context of our Pre-Approved Actions. ✓

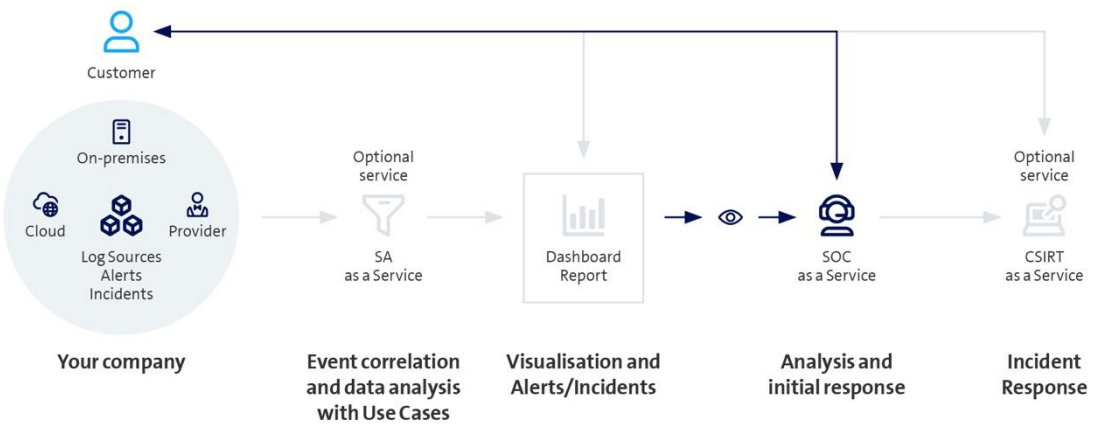
Consultation with specific operational recommendations and instructions

Direct advice on how to proceed in the event of a security incident. ✓

Cross-industry experience and expertise in matters of security

The security specialists hired have a vast expertise and many years of experience. ✓

How SOCaaS works



swisscom

Facts & Figures

Basic services

Security Alert Management covers all activities relating to the monitoring and analysis of events and security alerts generated within the scope of the Security Analytics as a Service or by a 3rd Party Security System. All identified security incidents are analysed in detail. Just how critical they are and their level of impact and potential risk for the organisation is assessed and then verified together with the customer. If these are active cyber attacks then, working off established procedures and processes, initial mitigation measures are discussed and initiated with the customer, or carried out autonomously by the SOC within the scope of the Pre-Approved Actions.

Optional services

- Discover hidden threats before they cause any damage with advanced threat hunting.

Additional services

- **Security Analytics as a Service (SAaaS):**
  We are experts in security, big data and artificial intelligence, and place our proven security analytics infrastructure at your disposal as a SOC platform. Connect other log sources from the cloud, on-premises or from a managed provider to get an overview of potential security incidents on the dashboard. You perform the analyses and responses to 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