

Factsheet

CSIRT as a Service / CSIRT Rapid Response





**Enable, drive and protect
your business.**

Security incidents are inevitable: your CSIRT can help you mount a rapid, effective response

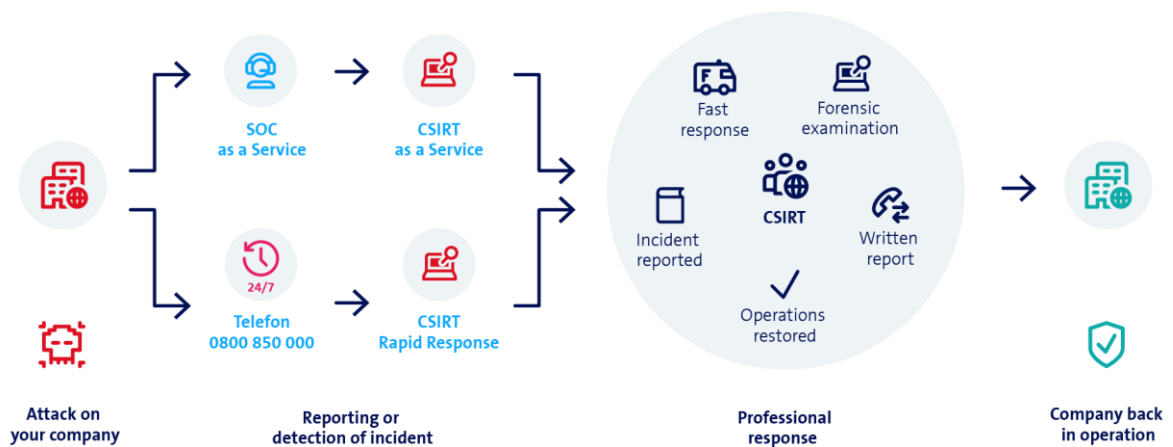
Our CSIRT service offers you fast, effective assistance during cyberattacks to ensure your business continuity in a complex digital landscape.

In a digital business environment where security incidents are inevitable and can have a major impact on your company, it is critical to have immediate, competent support. Our CSIRT as a

Service/Rapid Response offers you precisely that – a specialised cybersecurity incident response team that can take the wheel during a verified security incident. We help you respond to the attack, remove malware and restore operations. This service is available in different forms to flexibly meet your specific needs and guarantee business continuity.

- 
Rapid response to cyberattacks
 Respond quickly and professionally to security incidents.
- 
Benefit from the expertise and experience of our security experts
 Highly trained security specialists with extensive experience acquired over many years.
- 
Detailed security check of compromised systems
 Quickly analyse attack vectors and narrow down affected systems.
- 
Support with the restoration of regular operations
 Help reintegrating affected systems into the production environment.

How CSIRT as a Service / Rapid Response works



Facts & Figures

Basic services

CSIRT as a Service with service contract and SLA:

You call in Swisscom experts for analysis and management. We manage the security incident management process remotely or on your premises and support you in securing evidence and communicating with customers and partners.

CSIRT Rapid Response without SLA:

Rapid Response is comparable to the CSIRTaaS basic service. The only difference is that, in the event of an incident, you can call 0800 850 000 without a service contract. However, there is no guaranteed response time. An onboarding, which is carried out as an initial step with CSIRT as a Service, takes place directly before the service. In addition, there is a flat-rate service fee to pay as well as higher hourly rates.

Options

- Final report in accordance with individual customer specifications in German or English.
- Precautionary inspection of systems that are not directly affected.
- Securing evidence for criminal, civil and public law use in Switzerland.
- Crisis simulations for cyber incidents to prepare you and your team for real threat scenarios.

Supplementary services

Security Analytics as a Service (SAaaS):

As security and big data experts, we offer proven security analytics. Connect log sources and monitor security incidents from the dashboard. The analysis and response is in your hands.

SOC as a Service (SOCaaS):

The dashboard gives you an overview of potential and confirmed security incidents from defined enterprise log data as well as analyses with specific recommendations for action.

Next Generation Digital Risk Protection as a Service (ngDRPaaS):

Identify digital risks in open and closed networks and take action based on our recommendations. The takedown service removes illegal content and offers reporting.

Network Detection and Response as a Service (NDRaaS):

Our AI-powered NDR platform offers you visibility and real-time detection of cyber threats with seamless integration and advanced models.

You can find more information and get in touch with our experts here <https://swisscom.ch/csirt>