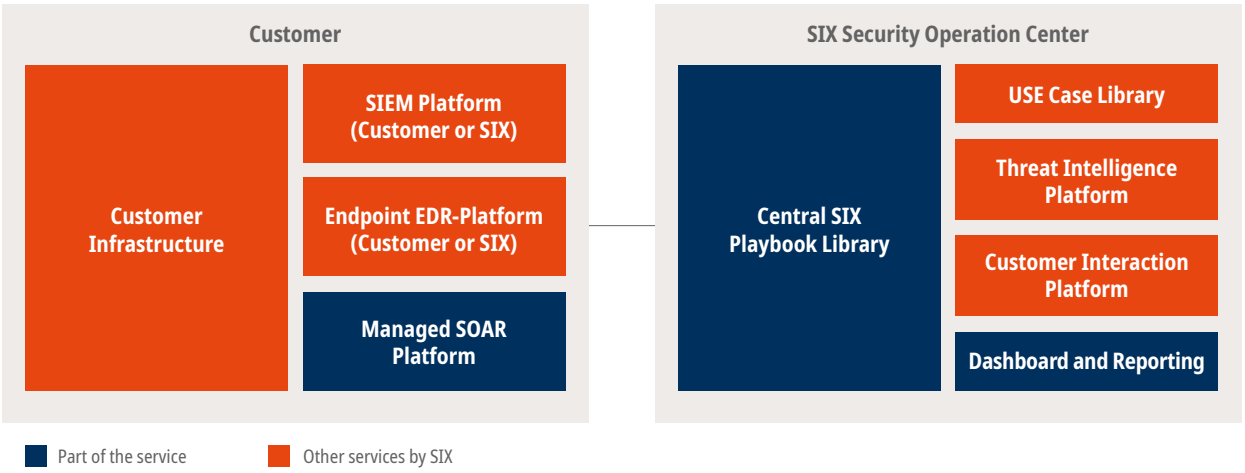
Managed SOAR

Security Orchestration, Automation and Response

Managed SOAR helps to relieve your security experts and shortens the response time in case of security incidents. Additionally, it can drive the automation of your workflows.



How Your Business Will Benefit

- Finance-driven playbooks by SIX: Benefit from the intellectual property of SIX and how SIX protects its own system-critical infrastructure.
- Cheaper and better-skilled resources: Maximize the cost-effectiveness of your security staff.
- Simplified governance, risk, and compliance: Make use of the vast experience of SIX in regulations and compliance in the financial industry.

How Your SOC Will Benefit

- Increased consistency of the cyber security incident response process: Automate your workflow.
- Reduced time for triage, analysis and response: Gain more time for advanced security projects.
- Take the boring and repetitive work off your SOC analysts.

About the Service

Operation and Management of the Platform

SIX helps to configure, adapt and manage the necessary components for you to respond more effectively to incidents. This means that SIX operates, and continuously manages, the SOAR Platform at your premises.

SIX deploys and maintains the SOAR platform. It will be rolled out in at least two instances (test and productive).

The service includes upgrades and patches. SIX integrates your SIEM solution to provide you with generated incidents, or relevant events, on your SOAR Platform.

Security Orchestration

Orchestrate Your Entire Workflow and Integrate Your Tools.

The service includes the orchestration of your various tools such as SIEM, ticketing system, e-mail, threat intelligence platform, potential customer identity provider or CMDB. This gives you the opportunity to investigate and response to security incidents. The service also includes training and the predefined basic or standard set of playbooks. Playbooks are always developed in close cooperation.

The Following Features Can Be Part of the Service:

1. You use the functionalities provided by the SOAR Platform, such as default playbook integration and automation.
2. You use the automations and playbooks provided by SIX, such as abstracted platform-independent commands, for individual investigation steps.
3. You create your own playbooks and ensure compatibility. SIX will be happy to support and advise you.

Security Automation

Move Human Interaction Into a Workflow.

SIX supports you in automating multiple manual actions to implement a SIEM and integrates your SIEM solution via workflows so that they work together using the SOAR Platform. SIX helps companies configure, customize, integrate, and deploy SOAR playbooks to reduce response time.

The Following Features Can Be Part of the Service:

1. Support in tuning and learning what can be automated.
2. Analysis of the quality of the workflows.

Security Investigation and Response

The solution is adapted to your guidelines, tools and processes. Our experts will consult, support and advise you.

Features:	
On-premise platform management	Included
Availability based on the SLA	99.9%
Integration of default playbooks (content pack)	Included
Integration of generic playbooks by SIX	Optional
Development and integration of customer-specific playbooks	Optional
Integration to your SIEM	Included
Integration to your ticketing system	Included
R/W access to test environment	Optional
R/W access to productive environment	n/a

SIX – Your Strong Partner from the Financial Industry

Your Benefits

- SIX is the only service provider in Switzerland offering Cyber Threat Intelligence (CTI) that is focused on financial topics.
- SIX develops use cases for the financial sector and updates them on an ongoing basis.
- SIX is itself system-critical, and as an operator of system-critical infrastructures it has an insider's view of relevant, sector-specific threats.

The Following May Also Be of Interest to You:

- SOC as a Service
- Incident Response Support
- Digital Risk Monitoring
- Vulnerability Management

SIX Group Services AG
Pfingstweidstrasse 110
P. O. Box
8005 Zurich

T + 41 58 399 3993
cybersecurity@six-group.com
www.six-group.com/cybersecurity

Your Contact
Dieter Bartl
Senior Cyber Security Sales Manager
T +41 58 399 3575
dieter.bartl@six-group.com