Cyber Security

More intelligent, rapid and precise.
The new security.

Tailored for the Swiss financial center:
The Security Operations Center (SOC) protects banks and insurance companies from cyber attacks.

Business data is a company's most precious commodity. Several studies have shown that companies in Switzerland tend to underestimate the risk of a cyber attack. SIX has set up the first cognitive Security Operations Center (SOC) tasked with protecting the critical infrastructure of the Swiss financial center. The SOC of SIX works around the clock (24x7x365) and is the first in Switzerland to use IBM Watson Cognitive Computing. In the words of Thomas Rhomberg, Head Security Operations & Transformation, the SOC enables attacks to be evaluated "more intelligent, rapid and precise".

What Are My Advantages of the Security Operations Center (SOC)?

As **CEO/CIO,** I provide my organization with optimal and cost-efficient protection using the same system that protects the key components of the Swiss financial center's critical infrastructure.

As **CISO/CRO,** I can rapidly close any gaps in resources or skills in my organization while complying with the regulatory requirements (e.g. FINMA or SWIFT). I can deploy my scarce human resources to carry out other profitable, important tasks.

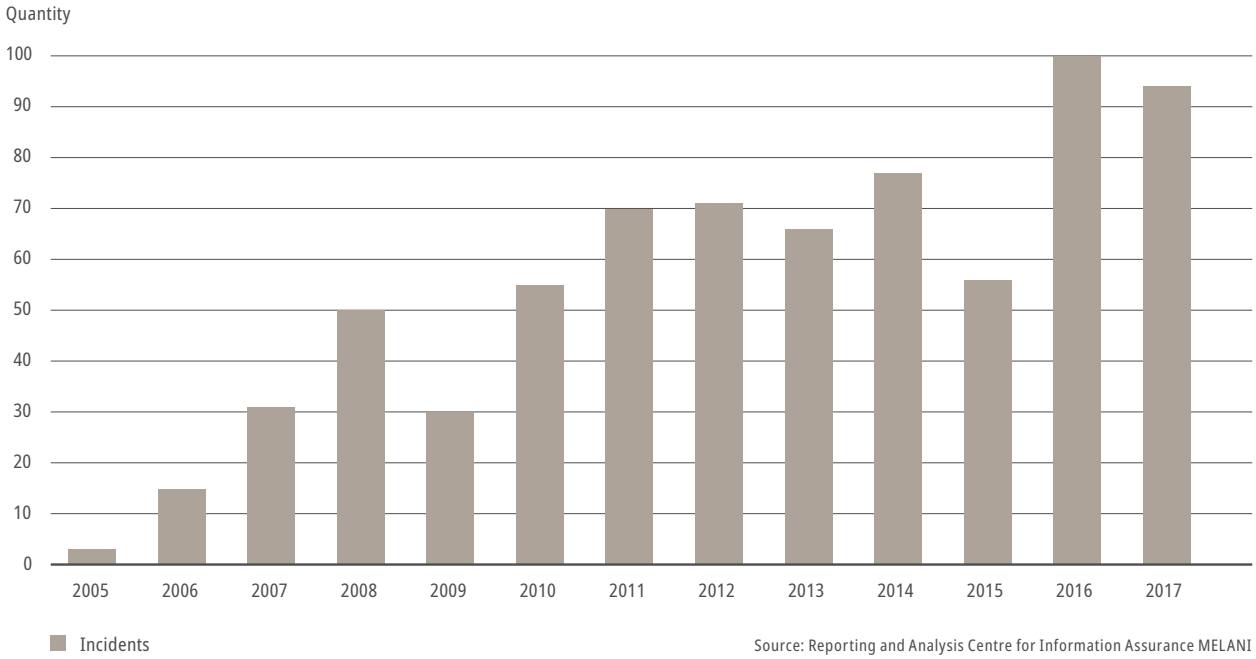
As **Head SOC,** I am able to rapidly detect and appropriately respond to attacks. I constantly benefit from state-of-the-art technologies and build on use cases that are targeted at the specific risks to which the Swiss financial center is exposed. I am also kept constantly up to date: promptly, around the clock, seven days a week.

As a **Security Analyst,** I can focus on my key tasks and I am efficiently supported in monitoring and with the triage of reports. I don't lose time in elaborating the triage of false alarms.

Who Is the Offering Aimed At?

As the operator of the stock exchange, SIX has to be able to rely on maximum security. The SOC must duly satisfy the highest demands – SIX uses it itself too. The MSS offering of SIX provides small and medium-sized banks and insurances with access to a security solution that is otherwise developed only by the big banks for their own purposes. Thanks to the compliance experience of SIX, the solution has been aligned to meet regulatory requirements, even when these are subject to change. Data remains with the client at all times; only security incidents are passed on for analysis – data always remains in Switzerland at all times.

Reported Threats And/Or Incidents at the Reporting and Analysis Centre for Information Assurance MELANI: 2005–2017



Source: Reporting and Analysis Centre for Information Assurance MELANI

The Biggest Threat for Companies

1,765 cyber attacks on companies were registered in 2017 that involved stealing 2.6 billion data records. These virtual break-ins are expensive: IBM estimates the average cost per attack at USD 3.62 million, or USD 141 per each stolen record.

Swiss companies are also a popular target. According to the MELANI Reporting and Analysis Centre for Information Assurance, the number of incidents is on the increase, having risen from 3 to 94 between 2005 and 2017. Banks and insurance companies are very much also the victim of attacks.

Ginni Rometty, CEO and Chair of IBM, already put it as follows in 2015: "Cyber crime is the greatest threat to every company in the world."

According to an IBM study, the average time to identify data theft is 191 days, with another 66 days to respond to it. The response time is strongly correlated with cost: the longer it takes to ward off an attack, the more expensive it is for the company in question.

What Does Managed Security Services (MSS) Offer?

What: Security events are collected and correlated in real time to detect security incidents and attacks. Suspicious incidents are being investigated by SIX security experts in Zurich. If the suspicion is confirmed, the specialists prepare a recommendation for action and alert the customer's incident response team.

How: State-of-the art technology: Use of Switzerland's first cognitive Security Operations Center (SOC). Thanks to cognitive computing, we can evaluate attacks "more intelligent, rapid and precise", says Thomas Rhomberg, Head Security Operations & Transformation.

Where: The customer retains the data – only security incidents are passed on for analysis – but data remains in Switzerland at all times.

Compatibility: Operation and maintenance of the SIEM system.

Updates: Constant updating of detection rules with access to a use case library that is especially focused on the risks to which the Swiss financial center is exposed, and to the latest findings of the current threat situation.

SIX Group Services AG
Pfingstweidstrasse 110
P.O. Box
CH-8021 Zürich

T + 41 58 399 3538
mss@six-group.com
www.six-group.com