# Cyber Security Hub

More intelligent, rapid and precise.
The new security.

Geared towards the Swiss financial center: the Cyber Security Hub provides banks and insurance companies with reliable, relevant information on current risks and dangerous developments.

Protection against cyber attacks is a important basis for the attractiveness and stability of the Swiss financial center. Collaboration with the organizations involved improves protection against cyber risks. The key elements of the Cyber Security Hub are:

- Sharing information and experiences.
- Coordinated measures in the event of attacks and subsequent evaluation.

A common platform from an independent provider is an absolute necessity for this. The Cyber Security Hub is a core responsibility for SIX, the main infrastructure provider for the Swiss financial center.

To protect the critical infrastructure of the Swiss financial center, SIX has set up a Security Operations Center (SOC). It works around the clock (24x7x365) and uses a unique sector-specific threat intelligence. One key task here is constantly updating use cases with optimized detection rules geared in particular towards the risks of the Swiss financial center with the latest information on the current threat situation.

All this knowledge flows into the Cyber Security Hub so that all members can benefit from the experiences of the community.

## The Benefits

"As **CEO/CIO,** I bolster the employees in my security team, network them with colleagues and improve the cyber resilience of my organization."

"As **CISO/CRO,** I receive compiled information for C-level so that I'm always aware of current trends and developments. This enables me to prioritize countering risks and defensive actions correctly."

"As **Head SOC,** I receive information that is relevant for the banks and insurance companies. This enables me to set the right short- and medium-term focus points in the risk management process."

"As **Security Analyst,** I receive information about cyber risks, dangers and attacks that I can put to use in real time for defensive actions. I don't have to worry about the quality and currency of the various sources."

## Who Is the Offering Aimed At?

It is of particular benefit for small and medium-sized banks and insurance companies. They often do not have sufficient resources for such activities alongside handling security issues.

The SIX SOC obtains information from a range of national and international sources, evaluates and selects it, and compiles it for the Swiss financial sector. SIX has a dedicated research team for this as constant development is required due to changing patterns of attack.

| | Strategic briefings | Exchange of best practices and use cases | Shared threat intelligence |
|---|---|---|---|
| | SIX briefings keep stakeholders up-to-date with relevant information. | Repository for registered users, who exchange information and best practices. | SIX gathers, filters and enhances the cyber security threat intelligence for common use. |
| **Content** | Report on threat situation. | Use cases, runbooks and incident reports from SIX and users. | Information on threat in structured form with references to use cases. |
| **Responsibilities of SIX** | SIX creates reports on information from various feeds and expands on this with information from its own sources. | SIX shares individual cases. SIX prepares user data for common use (anonymization, relevance, common standards, etc.). | SIX gathers, manages, enhances and saves information on threats. SIX monitors and enhances feeds. |
| **User responsibilities** | | Users submit own cases and best practices anonymously. These are then reviewed together. | Users submit own cases and threats anonymously and give feedback. |
| **Target audience** | CISO, CRO, CSO. | Heads of security operations, analysts, engineering leads. | Security analysts on duty. |
| **Timing** | Ready for use within months, useful for years. | Ready for use within days, useful for months. | Ready for use within seconds, useful for weeks. Links to threats, investigations, solution models. |
| **Distribution** | Personal meetings, phone and video conferences, instant messaging, e-mail, etc. | | |
| **Cycle** | Biannually (more frequently as required). | | Real-time feeds and regular meetings. |
| **Basic rules** | Trusted communities are defined at the suggestion of SIX. SIX manages the group. A community comprises at least three companies. Chatham House Rules apply. No information should leave the group. | | |

## What Does the Cyber Security Hub Offer?

Information prepared specifically for the target groups – banks and insurance companies – on cyber security:

- **Strategic:** Threat Landscape Report for strategic briefing of decision-makers.
- **Tactical:** Library with best practice use cases and playbooks of SIX and other participants.
- **Operative:** Threat information (indicators of compromise) from SIX and other participants who can read the systems.

SIX shares information on the basis of its own findings from research and cyber threats. In addition, SIX selects and compiles relevant information from various national and international sources. SIX operates the necessary infrastructure – such as a threat intelligence platform – and organizes accompanying events including closed user group meetings to share the information. Participating banks and insurance companies share anonymized information in these meetings.

All Swiss banks and insurance companies regulated by FINMA are invited.



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

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