Author	Lukas Szabo
Date	01/11/2021
Version	1.5
Classification	C1 - public
Pages	9, incl. cover page

SIX SIRT Team Charter

RFC 2350

Document information

This document provides the form description of the SIX Security Incident Response Team (SIX SIRT) based on the RFC 2350 requirements.

1.1. Date first published

The first official version of the document has been published on 25/04/2018.

1.2. Date of last update

This is version 1.5 with the last date of update on 01/11/2021.

1.3. Distribution list for notifications

This document is kept current in the location described in 1.3 of this document. Any updates will be distributed internally for review before updating. For any questions regarding the document, please contact sirt(at)six-group.com.

1.4. Locations where this document may be found

This document is available internally and on the SIX public website.

1. Contact information

1.1. Name of the team
SIX Security Incident Response Team
Short name: SIX SIRT

1.2. Address
Hardturmstrasse 201
8021 Zurich, Switzerland

1.3. Timezone
GMT +1 (CET)

1.4. Telephone number
Only available internally.

1.5. Other communications
Not applicable.

1.6. Electronic mail address
sirt(at)six-group.com

1.7. Public keys & encryption information
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: OpenPGP totemomail

mQENBGFJif8BCADTwNuGiWkMf089fFC/k6mmLUulEcH032i+FjDetCPtYnvMMi2T
8QA0TcHxTDlyFLVl2rkb6Z922B4Qm1SOwBn4M2NDtkI0p45NiCtlhskSBoImMdXK
7J1K/v4JnnpTSLWymqP/4LnM0ZyJqwDTOk5phA1H2zmMgdFqq5mxba6/YwxpoptH
fV6Nt7pgzn7qiJKgolOSaEioEJPLVRcXlbR9BI3CRYDWGOJZCeX0c6CovgBJOFQs
+sDOJ2PTDLtncY2VL9XQHlvVhwlNRr+B2rDubYxPi2aW47tz9o/jwraGWhTPMKRQ
UpqUNBkszn8sJVILJkGm48NabiVQQ4Zqy4W9ABEBAAG0GVNpcnQgPHNpcnRAc2l4
LWdyb3VwLmNvbT6JAhwEEwEIAAYFAmFJif8ACgkQw+kCKgSUCLvPvhAAmiUiD/6F
6KGko8jRxLZolKb4QN4d1j7TBlvhjJROv9VKXaquM0BrncYOGEep3JVW7AQFj3Yi
btxR2UrtjAkfu9MJ01/B51uyhTfwYLdkHXxbyJZrcVGdOHgpIDizpOBSuGmlSUYW
FUJI8PAR/3QP3L/8EFvWjL4vqJzrbwy4heBDwyEeHctYeFkji9a7xdbvoNs90l43
Eeys5fbEIMmALOz18g92JEeLEJ04e8cSFO706j2PMCjtoY+vLfOS9SSfm4sWi8np
iPOT7Bp812APtE5itfJFMfSHc218VRmpbl1jpBPOH0a3BvFMln8PF5y95CcK+LET
fvuaKd/Smhck7kYvqR1YY5QH29pt/gQ5eY2xnsb+uS6T0d1unFzrKdIleHiqI5x9
wsyEVygHosW6m7Vqcr62aVqSw+G055N7m/Q/cOsLZXbcl4kGI5V4yOomYa4CrW8C
7YPuK4GwgR8lYKjPfCpSlTzV22srHaTOlWWSAXDbhUmCUtj3vLADDgtmf46klDja
frZ3nGGj9SozKM024fYY+JjcjMfstN1ipobci7JKclvT3kOEcmlvhOTFzgwYVUgB
aGH1LmRfiNzdgOU5maef7uQpx213KzNEOSDlpQ+RF34OQ1lAk3WbOHUxpfcnsQBs
ypu6E1EhRIzTxU6yL/t/0HCbPzlNHUbu7TiJATYEEwEIACAFAmFJigAGCwkIBwMC
BBUICQoEFgIDAQIbDwUJA8JnAAAKCRCZMBXFFNKBNnA+B/9h3JFa9oZWtdp7zkeN
abXFCpdKOLUvBH3NDQv14iDXIv2wrgRPkHyjQOZnHXJgFjnreKwlflkBJ0bLj6Nb
62cdb1hBkARrmq28JDHK+WmDngGCk0kZHS24uSBgptvx91Rd4WeQcTkXvLmMiWjR
gnWV2u1ff25d28YmqzEVz6F9JGSkl0IIWHzAcJz3zeNVOTHDMvlgynxoukNzYQSb
spQqEKdPzIFMjihCCNsXpeTMx8dx5O1C8kCi7bEg3v78czJLuIrdM7+hjToHBhct
n+EJgKe+Yu2IKSrJJCKbPcYOASmOMEe+vJLIBNcaHQD6N/v4Vrh2KMJbeMVO9Ng7
+Wxh=ZfYA
-----END PGP PUBLIC KEY BLOCK-----

1.8. Team members
No public information about the SIX SIRT team members is provided.

1.9. Other information
Not available.

1.10 Points of customer contact
The preferred method for contacting the SIX SIRT is via e-mail sirt(at)six-group.com.

Additionally, potential information security incidents can be submitted through the Responsible Disclosure portal at:
https://www.six-group.com/en/products-services/newservices/contacts/soc.html

2. Charter

2.1. Mission statement

The core mission of the SIX Security Incident Response Team (SIRT) is to provide information, guidance and assistance to reduce the risks of information security incidents as well as leading the response to such incidents in a professional, effective and timely manner when they occur. Additionally, the SIX SIRT is responsible for independent reporting of risk arising from such incidents. The mandate and full authority is described in 3.3 and 3.4. This mandate applies to the whole of SIX Group including its international subsidiaries.

In addition to incident response, the SIX SIRT proactively gathers, analyses and disseminates relevant threat intelligence in order to prevent, prepare for and communicate about upcoming attacks against the SIX Group. By maintaining a continuous overview of the threat landscape, the team is able to support other security teams in order to challenge, adjust, improve or introduce new security controls in a timely manner and effectively protect the SIX Group from cyber attacks.

As a center of competence, the SIX SIRT collaborates closely with the SIX Security Operations Center (SOC) as a point of escalation, support and guidance, and oversees all of the relevant information security processes and capabilities. In addition to threat intelligence and information security incident management, the SIX SIRT is responsible for threat hunting and security advisory capabilities. Last but not least, SIX SIRT actively develops roadmaps and sets future priorities, designs requirements, reviews and controls the quality as well as leads continuous improvement of all of the capabilities. The SIX SIRT also acts as the official point of contact for law enforcement agencies with regards to information security incidents.

2.2. Constituency

The constituency of the SIX SIRT consists of infrastructure and services offered by SIX and its international subsidiaries as well as SIX employees in order to be clear where the team as an internal organization is legally allowed to perform responses to information security incidents. In case of leased infrastructure and managed services, the SIX SIRT is only intervening in incidents involving the underlying infrastructure managed by SIX unless otherwise agreed with the provider.

2.3. Sponsorship and/or affiliation

The SIX SIRT has a reporting line to the Head Cyber Security with a dotted reporting line to the Chief Security Officer and the Chief Risk Officer at SIX.

2.4. Authority

The mandate and full authority to act as the central point of expertise and guidance as well as help mitigate any threats resulting from information security incidents has been given to the SIX SIRT team by the SIX CSO in line with the Annex 16 of the S2 Security Regulation and within the framework as defined by SIX HR and Legal.

3. Policies

3.1. Types of incidents and level of support

SIX SIRT is authorized to address all types of information security incidents which occur, or threaten to occur within the limits of the team's constituency. Upon intake, incidents are prioritized according to their severity and impact as well as classified into one of the following 8 categories.

The level of support given by the SIX SIRT will vary depending on the type and severity of the incident and SIX SIRT's resources available at the time. In general the, the target service level for responding to any incidents reported via email to the SIX SIRT is 90% within 1 business day. The SIX SIRT also has an on-duty team member available for emergencies on a 24x7 basis.

3.2. Cooperation, interaction and disclosure of information

SIX SIRT is a member of different intelligence sharing communities and works closely together with CERT/CSIRT teams worldwide. There are legal restrictions on the flow of information from SIX SIRT as well as policies from SIX, all of which (in this order) are respected by the team. The SIX SIRT also actively collaborates with the Swiss GovCERT as well as different law enforcement agencies and regulatory bodies within Switzerland. Among others, the SIX SIRT is an active member of FIRST, the WFE GLEX security community, FS-ISAC as well as the SWIFT community.

SIX SIRT takes all appropriate measures to respect the confidentiality of all incoming information regardless of its priority. Neither personal nor overhead data are exchanged unless explicitly authorized. Next to the corporate security policy on data classification, SIX SIRT applies the Traffic Light Protocol (https://www.us-cert.gov/tlp) for information that is shared and/or distributed with trusted parties.

The TLP colour should be indicated within the subject or at the beginning of the email message or document. If contact is through phone or video conference, the TLP classifications should be stated prior to the delivery of the information. All incident-related with other teams should be tagged with a unique identifier and recorded within the SIX SIRT information security incident management system.

3.3. Communication and authentication

Communication with SIX SIRT occurs by various means, including telephone, e-mail and in person. Telephones will be considered sufficiently secure to be used unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If necessary, please use encryption as advised above.

The trustworthiness of the communicating entity will be tested through the resources available. In order to ensure authenticity of information, please use PGP signatures.

4. Services

The SIX SIRT provides the following services to the SIX organization.

Reactive services	Proactive services	Quality management services
Alerts and warnings	Announcements	Risk analysis
Incident handling	Technology watch	Security consulting
Incident analysis	Development of security tools	Awareness building
Incident response	Intrusion detection services	Education/training
Incident coordination	Security awareness raising	Product evaluation
Vulnerability handling		
Vulnerability analysis		
Vulnerability coordination		
Artifact handling		
Artifact analysis		
Artifact coordination		
Forensic analysis		

5. Incident reporting forms

SIX offers the possibility to submit potential vulnerabilities and incidents through the ‘Report a Cyber Security Incident’ form online.
https://www.six-group.com/en/products-services/newservices/contacts/soc.html

6. Disclaimer

While SIX SIRT will take every necessary precaution in the preparation of information, notifications and alerts, SIX SIRT assumes no responsibility for errors, omissions, or damages resulting from the use of the information contained within.