Author	Florian Fortin
Date	21/06/2023
Version	1.6
Classification	C1 - public
Pages	9, incl. cover page

SIX SMIR Team Charter

RFC 2350

Document information

This document provides the form description of the SIX Security Monitoring and Incident Response Team (SIX SMIR) 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 1.6 with the last date of update on 10/05/2023.

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 soc(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 Monitoring and Incident Response Team
Short name: SIX SMIR

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
soc(at)six-group.com

1.7. Public keys & encryption information
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: OpenPGP Kiteworks
mQENBGOwzkIBCADOfCEhTmrOMES8IeUyOpIAtMJn6/QS7KsnjHvp2D/TCUje/tuM
8uWx5FZfa+8wM2LGVekVmzolZv1wCOaV13kdJYHIdILLpF4lk0edEi6zg4iguz5+
ZDsDEOoEawP+s9+PkUttNmxT2stYSz3/CN/XpkiWuyfyXw8pT2z14cl5EwxkaI8F
Pgui2Ae9Z2AZ7I9RnQec2P4QaWXlbMpYKc67X9ReudDVf0uRa6Wf30N4AZF+a/Ur
SaDtpLOSFuH29I+JMjJDnFsDod3OX1ue9Wx2wuHaF53uCCm835zyc6/oAuq6Oy8Z
r/ccnttHW3++pzoUYjPwVo0dOMqEeoCaQfUNABEBAAG0F1NvYyA8c29jQHNpeC1n
cm91cC5jb20+iQIcBBMBCAAGBQJjsM5CAAoJEMPpAioElAi7GiMP/0BF4viuAY4+
RM+umwirQIzG4RfA43WCm/EGQOCRZgQ3HpqxZp5J3mb/SjOKkjdA2zyqqK0uKaEI
555/LPmgAQdiN+hgQ89XLCrLj4GFhWTVTxlmZHpPjbGICCxQGHkb69XXCbbmqhUa
OO2seqMKDNmYbBQNDmpHoqu9gSykY0fE8+vnU6YmZDGifo1sQLaSUYFPg0rSlbOO
JyjejyMJ85sgtow4hs/Av44D/gAi/LrPKRUguM0jyGACSvDY+biui93iZbp8bTAE
h7LBS9Nwzklj067R8Va0BLgZm1KCk+TwYTqBpWvT4xLJtXVh5ewcYSNbNjRnZE7H
kFzahRh7HLxczu6URscyQmBxW+jO+byBlBFVhzCHcR2IZfrLQPtRqkiNpSd5Fqt6
H6506hzLANEcY2ZJMQuIYaQqXAfeJRqHxJoafMb9ykrZlqXP9oWlJAERHkxYpVCR
EfezXLWvP9hB4JnLGeFNZCrCHCJmfU2ajRvJhrjWQNInrXZTK5UjIWL9s/HG9Pal
MSrGWAzbv+fwJuMeey6EiqNLRBUJPe5ykvfEMBhaRBV0hxn0mOc5z+5/h+rucLYW
uhBAGODyI7hZ18Buv/gVKyUe9s4vHBZKuX1PbjNAJ4QqwJhLEKApswKWsnAktuoi
kXCCUMC5sqOoGwPIErCGpNV93iU2L/RciQE5BBMBCAAjBQJjsM5CBgsJCAcDAgQV
CAkKBBYCAwECHgECGw8FCQPCZwAACgkQwYWgIy2Cpfj0Xwf+NY6CDcfl7WEtc+u9
dTizuwfCCej1GAYvpR5SI/ZDQQvly9KyZ40r9sgcHsYA9OStHIkGndmc4F6Iijw2
yveJsXZs4u/T/hBgT0r63nynDbtBNhnE2uumW8pucRC0ICrnjkAoMvQI6Fm7/2L+
wYirXQeBnKvu6fDZUWZfdv3sAWfrcktfZC/AfasWQ+iycgFjk8XaKVa6EiiYVBnl
5YKkhp45K0nasmDKF8SdxZpjgqS8WNJOCjVKBXptrVrMTgtM4hEvX6EO29t3kVNZ
XR1IQaTkKW2PqIYqIGN2KSJtjN+6wKQ+K53dy0Oc1ehBBIarc+DQhTFukF2x+5V5 O45CCw==
=2J5U -----END PGP PUBLIC KEY BLOCK-----

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

1.9. Other information
Not available.

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

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

2. Charter

2.1. Mission statement

The core mission of the SIX Security Monitoring and Incident Response Team (SIX SMIR) 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 SMIR 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 SMIR 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 SMIR 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 SMIR is responsible for threat hunting and security advisory capabilities. Last but not least, SIX SMIR 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 SMIR 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 SMIR 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 SMIR 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 SMIR 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 SMIR 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 SMIR 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 SMIR will vary depending on the type and severity of the incident and SIX SMIR's resources available at the time. In general the, the target service level for responding to any incidents reported via email to the SIX SMIR is 90% within 1 business day. The SIX SMIR also has an on-duty team member available for emergencies on a 24x7 basis.

3.2. Cooperation, interaction and disclosure of information

SIX SMIR 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 SMIR as well as policies from SIX, all of which (in this order) are respected by the team. The SIX SMIR also actively collaborates with the Swiss GovCERT as well as different law enforcement agencies and regulatory bodies within Switzerland. Among others, the SIX SMIR is an active member of FIRST, the WFE GLEX security community, FS-ISAC as well as the SWIFT community.

SIX SMIR 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 SMIR 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 SMIR information security incident management system.

3.3. Communication and authentication

Communication with SIX SMIR 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 SMIR provides the following services to the SIX organization.

- Security Operations Center (24/7 monitoring & incident response)
- Point of contact for all cyber security incidents
- Technical support for compliance and legal investigations (including forensic analysis)
- Performing of purple teaming exercises in collaboration with internal Parties
- Technical security advisory & table-top exercise support

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