



Author Adrian Schoch
Date 2025/08/19
Version 1.7
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 2018/04/25.

1.2. Date of last update

This is version 1.7 with the last date of update on 2025/08/19.

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-----

```
mQGNBGeQ+x0BDADX4YQO5kcpj94PLYgl1tUhlFBIDKkpqajV/VFxuWCFY7Etx/lzsQqLQAJHdMaZ
REoGDuuHZI1A0/L4es6mHCuJINBp94+b9wxHpsTg5+i/JZhQcl0E+1YZ+eC6OIVvOekgTMG1Htfda3
Jd6c5/Htu8kqHL7zXnV/Mffb5QdUKGdTfUpAlx00SPYsdcgLDQWAnwYM5E0JCz6XrTJAdU7KPOFnj
OIP+/CHRA2RQ4GYj1okH+vBugXB9tIbgFSCdl4dtaRwXLys0FGDs9ppq3wv5y9US3eZhAcntiXhEue
39143cdBNx/mJfipRW7rO1cT+LK58+r3c/wbNGrxGI5T7xM/p0HDo8HElyK3JPUriQGoMvXuEiEOsAg
3reUec6FWlpTRteuTyEeP4z59XnmaLO5IYLMJwDnl8GWSS8D+yOAoSih2tSqBhyg5sqT6Cej+E3qC
glyV3Jgla6RYfHXexzT+4g3aQ2eKvWHgsnbinHStr7pj4PVJU95dirSjzZFPIMAEQEAAbQbU09DIFNJ
WCA8c29jQHNpeC1ncm91cC5jb20+iQHUBBMBCAA+FiEEuF9GENgvfVvhqYtTEKop6aoda8sFame
Q+x0CGwMFCQPCO5MFCwkIBwIGFQoJCAAsCBBYCAwECHgECF4AACgkQEKop6aoda8uZjAwAo
E0MadGqE80xVznD4boyKwRRFKwI6jPJVVWgQ50V6hSrY5SGNEgOP8Y3b6nypZ/v5/OHlqcjWBoh2
+BTDOhI90Tin2sEddwDI+7vkqiKs0KpY7StaXMSRVBCnoSXvQDyR7ON5kXoZlrPpgF6XDwrPnoiJsL
psTCw86sqIEVvnkb10ymMpFKMiaB0SV7J6g4+UJA4f/XZCFbjTqk/2aaiPrClcwX7UOeq2gTJC299uE
hXjbYNwsByYtno1qVFPJNGlTl8DpnkAgOVm4toCWdSUR2oz5lq5KgXNnnwhn8hgMi9WoaMoPBKC
L3DeHQN40GuAZZBuyNPF+PBQ/c5jqIxtNYRr99NrOz0icH2BHI69nvwS05/yxbAJW9qD1yFBLb/JGG
UoNt5+YLrZDjJr9uP1Rm7Mq0JTbWJV3kBinbFWiOnrrUtcwJ29vFYptgGXA5PqCqQZBGY6YUdsEV
MfxOo4prS5yrxj1Te6wjTXKFclwU+SjyG1SuS6mYn5P4nZM/SuQGNBGeQ+x0BDAC+QFgSEb4E1f
kQ2zOw6KkPcXCft6aDYSQ8mjsleugf7aAJFnsqVlKYGcWbAySDleuSWmhfUN5bW/F/DiwrTitKcoRjs
EyalhwFCm5+a2g63JvoHKbaN6QshgMQMnA/Wxb6VqP98J6TURPZA+gBIJ/BCxSgkFrDzZ1icWjem
Oam7i2x1RkW6tMaeWmNRzjTL8ALmTJBFkuzaVb4UKNth8COnirQ9pC+jyv1SRf6A8z+coPeL2yuPR
ukZvclEE2VuHU+7F3rLOVJpMejQlhTR4+H5sBZBgfXwRPDfgdEUpk83llcln1UhjiMTqf6N3pN2D5Ke
Wmmp6HXQR7O5QHojQj2scEH8Sr9KNrbRws88MyXv2UuRhxD81HAVmfrdS/UrcZP6I+rWU3FXHq
vdocJMCr2QoUXVgeojPMJ7XrQ5FfwBg1NDH00q9CiPfZCtOI1Wbq3v8vXTINp5TO92llo5dO10DwlK
yKUGRMhEgBLF9/SZHfb4UZ/cLXWeHI2lo7LVcAEQEAAAYkBVAAQYAQgAJhYhBLhfRhDYl31b4amL
UxCqKemqHWvLBQJnkPsdAhsMBQkdWjuTAAoJEBcQqKemqHWvLf3YL+wTlyvB7SDJSokaB/IHqksg
cLLtum8cWyQyDsWDRdRzcyT+D3OaLikdwUzYJSbodZUEwXwuJSjrFefExRiMHT/gTGfIHfSD6i4FP5
IVFFodbBNigB7uThoflIdL9RUCz5ulbUb8mOy+g1nPHRAtR1f50+i9ljuxjjVIQwGdXVi3ig0eSN5dx/QtS
qJ0aQzivmN+PAku8Ld7+xwBBqIT2grozz8A1Es6bg9LzL1hhHjrA/D+dSM2mYTTdqZqFEeX1eu3Cd
NOdaZTsSvlsfiD1N5ih2EgzkN4QRa8hT+BS/Op3q/q1zQT8JAjCs0xAOMWhL7fVENc42DpLx6GicQt
MZUYHx2DgctvKLyU8trpFICVr8p6z2ZJNA38kwE4wNyFxAUIN5Z9Fo+WRjaM7TUXpsv5Gwpgd+YE
6WVR33GPS3hWhEzmVsiBzu7qDyu9+G9kccViOxxdXUBGoq27/gDXztFmzqha9GrsfPeTLAB9wh4H
6rYBbpGVdu1jq/RyS9Q===mBQe
```

-----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](mailto:soc@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/contacts/services/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.