Règlement de classification des incidents

Réglementation complémentaire au contrat de participation bLink

Table des matières

1. Contenu

Ce règlement régit la classification, la notification et le processus de notification des dysfonctionnements liés à la sécurité et des dysfonctionnements opérationnels par les participants.

2. Contexte

SIX BBS SA («SIX») est le prestataire du service bLink. Les fournisseurs et utilisateurs de services participant à la plate-forme bLink sont soumis à des exigences de sécurité particulières en raison des données échangées. Le respect des exigences de sécurité est un élément essentiel des services fournis au client final.

Le service bLink est fourni par SIX à un grand nombre de participants. Face à un nombre d'établissements financiers aussi élevé, des règles claires concernant la classification des dysfonctionnements et la communication que cela implique sont essentielles.

3. Types de dysfonctionnements

SIX distingue deux types de dysfonctionnements: les dysfonctionnements liés à la sécurité et les dysfonctionnements opérationnels.

Les dysfonctionnements liés à la sécurité comprennent toutes les perturbations de l'écosystème bLink, c'est-à-dire les fournisseurs de services, les opérateurs de plate-forme et/ou les utilisateurs de services, qui représentent une violation de la sécurité des données. Ces dysfonctionnements sont traités conformément à SIX Security Event and Information Management et utilisent les informations existantes pour identifier les dysfonctionnements liés à la sécurité ou les analyses médico-légales.

Les dysfonctionnements opérationnels comprennent toutes les perturbations qui affectent le fonctionnement, la fonctionnalité et la disponibilité de l'écosystème bLink, c'est-à-dire les fournisseurs de services, les opérateurs de plate-forme et/ou les utilisateurs de services. Ces dysfonctionnements sont traités conformément à SIX IT Service Management et utilisent les informations existantes décrivant le comportement des applications et de l'infrastructure, ou l'écart par rapport au comportement normal, ainsi que d'autres informations pour identifier la cause profonde de la perturbation.

4. Catégories de dysfonctionnements

4.1 Dysfonctionnements liés à la sécurité (SIEM)

Les dysfonctionnements concernant la sécurité sont classés selon le Tableau 1. La catégorisation suivante s'applique au traitement des dysfonctionnements:

- Les dysfonctionnements des niveaux Critical et Serious sont traités comme des Incidents majeurs.
- Les dysfonctionnements de niveau Severe sont traités comme des dysfonctionnements de niveau 2 selon l'Annexe 3 du contrat de participation.
- Les dysfonctionnements de niveau Minor sont traités comme des dysfonctionnements de niveau 1 selon l'Annexe 3 du contrat de participation.
- Les dysfonctionnements de niveau Negligible (marginal) ne sont pas soumis à l'accord d'exploitation et sont utilisés pour le contrôle des processus internes.

4.2 Anomalies dans le comportement d'accès

Conformément au point 16 lettre a du contrat de participation, SIX examine les anomalies dans le comportement d'accès. Les dispositions suivantes s'appliquent:

1. Détection: SIX vérifie en permanence (24 heures sur 24 et 7 jours sur 7) si les demandes des utilisateurs de services présentent des irrégularités d'accès, en vérifiant notamment si la demande d'un participant est envoyée à SIX au moyen d'une combinaison de caractéristiques d'identification («Caractéristiques d'identification») que le participant a préalablement communiquées à SIX (p. ex. adresse IP, et/ou certificat) ou si une demande a été enregistrée indépendamment par SIX (p. ex. caractéristiques comportementales spécifiques). Si ce n'est pas le cas, il y a irrégularité. SIX applique la diligence habituellement requise lorsqu'elle vérifie les demandes du participant pour détecter des irrégularités.
2. Alerte/ouverture d'incident dans le Security Operation Center («SOC») de SIX: si SIX constate qu'une demande d'un participant contient une irrégularité, l'événement est immédiatement enregistré et l'examen plus détaillé de l'irrégularité dans le SOC est lancé (7 j/7 – 24 h/24) conformément au ch. 3 ci-après.
3. Réaction: SIX prendra immédiatement des mesures adaptées aux irrégularités pour empêcher un accès non autorisé aux données ou la mise en péril de la sécurité de la plate-forme ou de l'échange de données traitées par son intermédiaire. En particulier SIX

   Cas a: révoquera immédiatement une connexion d'utilisateur du participant et bloquera le certificat du participant ou de l'utilisateur (certificat) si les caractéristiques comportementales sont utilisées pour des demandes provenant de plusieurs adresses IP inconnues, et déterminera avec le participant, dans les 15 minutes, si les adresses IP inconnues sont utilisées par lui. Dès que le participant confirme que les adresses IP utilisées sont valides, le blocage du certificat est annulé et les adresses IP sont enregistrées comme élément des caractéristiques identifiables.

   Cas b: déterminera avec le participant dans les 15 minutes si ce dernier utilise une adresse IP inconnue , lorsque ses caractéristiques d'identification, pour une demande, sont utilisées en provenance d'une adresse IP inconnue. Si le participant n'est pas joignable durant ce laps de 15 minutes ou si le participant confirme qu'il n'utilise pas l'adresse IP utilisée, SIX bloquera de manière préventive le certificat du participant ou de l'utilisateur concerné (certificat) avec effet immédiat. SIX continuera d'essayer de joindre le participant. Dès que le participant confirme que les adresses IP utilisées sont valides, le blocage du certificat est annulé et les adresses IP sont enregistrées comme élément des caractéristiques identifiables.

Les demandes avec un certificat bloqué ou les demandes provenant d'une adresse IP bloquée ne seront plus traitées par SIX. L'utilisateur de services peut demander le déblocage d'une adresse IP ou l'annulation du blocage s'il prouve ultérieurement qu'il utilise toujours l'adresse IP.

Si un certificat d'un utilisateur de services est bloqué, les fournisseurs de services concernés seront informés conformément à l'Annexe 3 du contrat de participation.

Tableau 1: Niveaux de dysfonctionnements liés à la sécurité

Information Security Incident Severity Matrix

	Level 5 (Negligible)	Level 4 (Minor)	Level 3 (Serious)	Level 2 (Severe)	Level 1 (Critical)
Brand protection (lead by CMC-EC)	Registration of domain name(s) that contains any of the SIX brands without approval (no active use).	Emails impersonating any of the SIX brands to steal credentials (no URL). Unauthorised creation or usage of social media account containing SIX brands.	Emails impersonating any of the SIX brands to steal credentials (including a webpage). Active use of a domain (web, email, etc.) to impersonate any of the SIX brands.	Emails impersonating any of the SIX brands to steal credentials (including good quality webpage impersonating SIX). A non-critical SIX website gets compromised and/or defaced.	SIX corporate or customer-service websites get defaced and/or escalated incident with media exposure.
Data leakage	SIX internal information disclosed externally.	SIX internal information is publicly disclosed or employee information disclosed (<10). SIX customer information disclosed (<10).	SIX confidential information is or SIX customer simple PII information disclosed (1+). SIX employee internal information disclosed (10+). SIX confidential customer information is disclosed (<10).	SIX secret information or customer PII extended information is disclosed (1+). SIX employee confidential or secret information is disclosed (1+). The information is not made public. 100+ records of lower classification is disclosed publicly.	SIX secret (internal and/or customer) or sensitive PII information is disclosed and publicly available (1+). Escalated incident with media exposure.
Denial of service[a] (lead by CIT-[a])	(d)DoS attack with limited impact on SIX operations or reputation. No customer impact.	(d)DoS attack with noticeable impact on SIX operations or reputation. No customer impact.	(d)DoS attack with significant impact on SIX operations or reputation and/or noticeable customer impact.	(d)DoS attack with large impact on SIX operations or reputation and/or significant customer impact.	(d)DoS attack with major impact on SIX operations or reputation and/or large service interruption for a large number of customers.
Malicious code	Malicious code on a single corporate asset. Malicious code in user-managed context.	Same malicious code in user mode on multiple corporate assets (<5).	Same malicious code on multiple corporate assets in user space (<10). Malicious code on single corporate asset with possible escalated privileges.	Same malicious code on multiple corporate assets (10+). Malicious code on multiple corporate assets with confirmed escalated privileges (1+). Malicious code on a high value or crown jewel corporate asset (1).	Malicious code on multiple high value or crown jewel corporate assets (1+), e.g. Active Directory. Escalated incident with media exposure.
Security policy violation	User without administrative privileges violating a security policy not resulting in an incident.	User with local administrator privileges violating a security policy not resulting in an incident. User without admin privileges violating a security policy repeatedly (more than 2 times) or resulting in an incident.	User with local administrative privileges violating the security policy multiple times. User with global administrative privileges violating the security policy not resulting in an incident.	User with global administrative privileges violating the security policy multiple times. User with local admin privileges violating the security policy resulting in an incident.	User with global administrative privileges violating the security policy resulting in an incident or compromise of the account.
Social engineering	Employee being targeted by a generic phishing campaign. Non-harmful message (with or without links or attachments).	Multiple employees being targeted by a generic phishing campaign. Employee that responded to a phishing attack. Phishing attack targeting the banking sector.	Multiple employees that responded to phishing attack. High value employee being targeted by phishing campaign. Employee(s) being targeted by a phishing campaign for high value information. Phishing attack targeting SIX specifically.	Employee(s) that responded to phishing attack with financial impact/loss or data disclosure. Multiple high value employees being targeted by phishing campaign.	Escalated incident with financial impact, loss or data disclosure.
System vulnerability	Attackers can collect information about the host via open ports, services, software versions, OS, etc. leading to disclosure of other vulnerabilities. CVSS V3 0.1 - 3.9 score.	Attackers can collect sensitive information about the host leading to disclosure of other known vulnerabilities. CVSS V3 4.0 - 6.9 score.	Publicly available & known vulnerabilty with attackers potentially having access to security settings, disclosure of file contents, directory browsing, read access to files etc. CVSS V3 7.0 - 8.9 score.	Publicly avialable & known vulnerability where attackers can gain control of the host, collect confidential information or execute commands remotely or cause a DoS scenario. Vulnerability specific to the banking sector. CVSS V3 9.0 - 10.0 score.	Attackers can easily gain control of a host (or multiple), which can lead to the compromise of the entire network. Severe vulnerability actively exploited in the wild and/or resulting in a DoS scenario for a cricital service. Escalated incident with media exposure.
Unauthorised acccess	Customer credentials being used on SIX service by an unauthorised party. Network scanning activity by an unknown party on resources exposed to the internet.	Multiple customer credentials being used on SIX service by an unauthorised party. Employee credentials being used by an unauthorised party.	Multiple employees credentials being used by an unauthorised party.	High value employee credentials being used by an unauthorised party. Social media account being used by an unauthorised party.	Multiple high value employee credentials being used by an unauthorised party. Escalated incident with media exposure.

4.3 Dysfonctionnements opérationnels (Incidents)

Dans le cas de dysfonctionnements opérationnels, l'impact de la perturbation et l'urgence du traitement sont évalués. L'impact est évalué sur une échelle à 4 niveaux:

1 – Impact à grande échelle

2 – Impact significatif / majeur

3 – Impact modéré / limité

4 – Impact faible / localisé

L'urgence est également évaluée sur une échelle à 4 niveaux (1-faible, 2-moyen, 3-élevé, 4-critique).

La combinaison de ces deux valeurs donne la priorité du traitement des dysfonctionnements (voir le le Tableau 2).

La catégorisation suivante s'applique au traitement des dysfonctionnements:

- Les dysfonctionnements avec les priorités Critical et High sont traités comme des Incidents majeurs conformément à l'Annexe 3 du contrat de participation.
- Les dysfonctionnements avec la priorité Medium sont traités comme des dysfonctionnements de niveau 2 conformément à l'Annexe 3 du contrat de participation.
- Les dysfonctionnements avec la priorité Low sont traités comme des dysfonctionnements de niveau 1 selon l'Annexe 3 du contrat de participation.

Impact	Urgence	Priorité
1 - considérable/étendu	1 - critique	critique
2 - significatif/important	1 - critique	critique
1 - considérable/étendu	2 - élevé	critique
3 - modéré/limité	1 - critique	élevé
2 - significatif/important	2 - élevé	élevé
4 - mineur/localisé	1 - critique	élevé
1 - considérable/étendu	3 - moyen	élevé
3 - modéré/limité	2 - élevé	élevé
2 - significatif/important	3 - moyen	moyen
4 - mineur/localisé	2 - élevé	moyen
3 - modéré/limité	3 - moyen	moyen
4 - mineur/localisé	3 - moyen	moyen
1 - considérable/étendu	4 - faible	faible
2 - significatif/important	4 - faible	faible
3 - modéré/limité	4 - faible	faible
4 - mineur/localisé	4 - faible	faible

Tableau 2: Priorité des dysfonctionnements opérationnels

5. Processus de signalement des dysfonctionnements

L'illustration 1 présente le processus de signalement des dysfonctionnements (qui fait partie de la gestion des incidents) pertinent pour les participants.

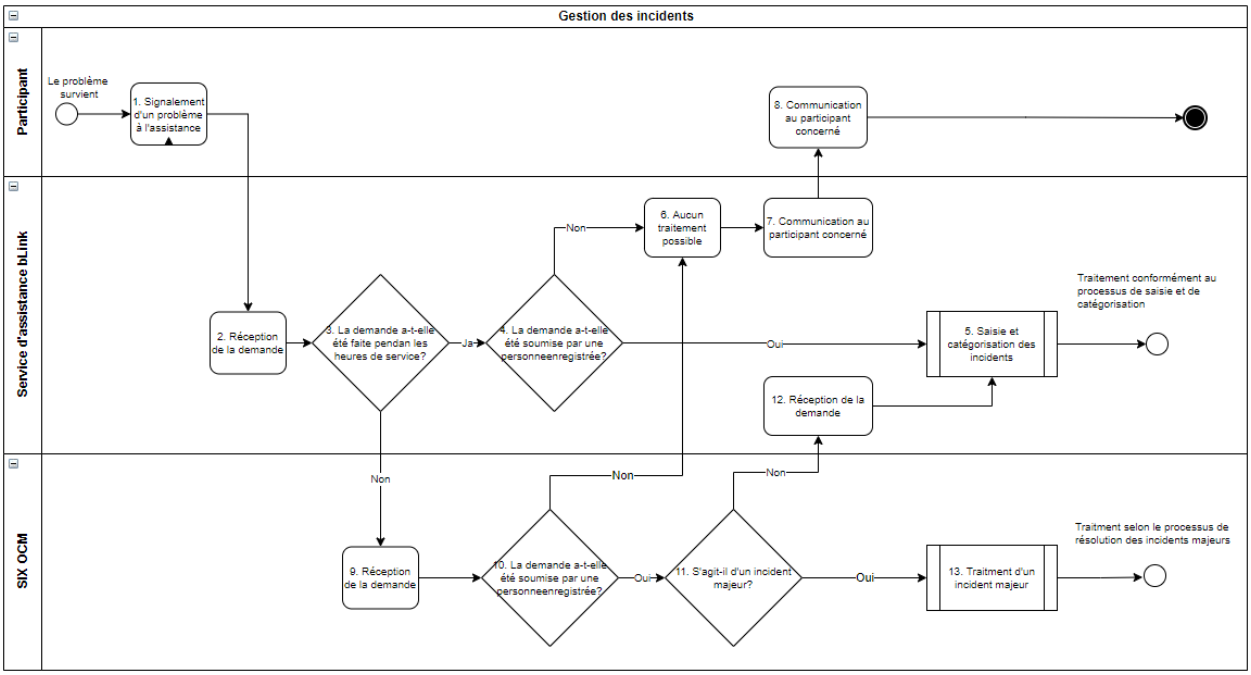

Tableau 1: Processus de signalement des dysfonctionnements

1. Le participant signale son problème au service de support de SIX, indépendamment de l'importance du problème et indépendamment des heures d'assistance définies dans l'accord d'exploitation.
   Remarque: le processus est également déclenché en cas de dysfonctionnements détectés par le contrôle interne de SIX.
2. Le rapport du participant est envoyé au service de support de bLink par téléphone ou par e-mail.
3. Tout d'abord, il convient de déterminer si la demande a été reçue pendant les heures d'assistance telles que formulées à l'Annexe 3 du contrat de participation. Si la demande est reçue en dehors de ces heures d'assistance, les étapes 4 à 8 peuvent être ignorées.
4. Si la demande a été faite pendant les heures d'assistance, il convient alors de déterminer si elle a été faite par une personne du support autorisée. Les règles détaillées sur l'éligibilité des personnes en ce qui concerne le support sont exposées au chapitre 4 de l'Annexe 3 du contrat de participation. Si ce n'est pas le cas, on passe directement à l'étape 6.
5. Si la demande a été présentée par une personne autorisée, elle est saisie et classée par catégorie. La demande est ensuite traitée conformément au processus interne de traitement des dysfonctionnements de SIX.
6. Si la demande a été présentée par une personne qui n'est pas autorisée au support, elle ne peut pas être traitée.
7. Dans ce cas, le support informe le participant que la demande ne peut être traitée faute d'autorisation.
8. Le participant est informé que sa demande n'a pas pu être traitée faute d'autorisation.
9. Si la demande du participant est faite en dehors des heures d'assistance, elle est automatiquement transmise à l'OCM ou, en cas de dysfonctionnement lié à la sécurité, au SOC (qui fait partie de l'OCM).

10. En dehors des heures d'assistance, il importe également de préciser si la demande émane d'une personne qui a droit au support. Si ce n'est pas le cas, l'OCM/SOC prend également en charge les mesures 6 – 8 et informe les participants concernés.
11. Si la demande provient d'une personne ayant droit à une aide, l'OCM/SOC doit décider s'il s'agit d'un Incident majeur ou d'une demande d'aide qui n'est pas urgente.
12. S'il s'agit d'un Incident majeur, il sera traité conformément à la procédure de traitement des dysfonctionnements.
13. Si une demande adressée à l'OCM/SOC en dehors des heures d'assistance ne constitue pas un Incident majeur, la demande sera renvoyée au support, qui la traitera le jour ouvrable suivant conformément au processus documenté à l'Annexe 1.

6. Confidentialité

Les rapports de dysfonctionnement, leur description et leur état sont confidentiels et ne peuvent être transmis à des tiers. Les participants ne sont pas considérés comme des tiers. Les informations ne peuvent être transmises entre les participants que dans le cadre du «besoin d'en connaître».

7. Contrôle de ces règlements

SIX contrôle et évalue périodiquement l'adéquation et l'efficacité de ces dispositions dans la présente annexe.

Les modifications apportées à cette annexe sont basées sur les dispositions du contrat de participation.

8. Mécanismes du recours à la voie hiérarchique

Le mécanisme du recours à la voie hiérarchique prévu à l'Annexe 3 du contrat de participation s'applique.

9. Entrée en vigueur

Le règlement entre en vigueur le 1er janvier 2022.