Crédit Mutuel ARKEA | CERT CSIRT

CERT ARKEA

-

RFC 2350

Version	Date de publication	Rédacteur	Valideur	Nature
1.0	23/04/2019	Guillaume ROUSSEL	Bruno TIGNAC	Création

Sommaire

A propos de ce document **2**
- Date de dernière mise à jour 2
- Liste de distribution pour notifications 2
- Localisation de ce document 2

Points de contact **2**
- Nom de l'équipe 2
- Adresse 2
- Fuseau horaire 2
- Numéro de téléphone 2
- Adresse de messagerie électronique 2
- Information sur les clefs publiques et le chiffrement 3
- Autres moyens de communication 3
- Membres de l'équipe 3
- Autres informations 3
- Points de contact 3

Charte **3**
- Ordre de mission 3
- Périmètre d'intervention 4
- Support et/ou Affiliation 4
- Autorité 4

Politique **4**
- Types d'incidents et niveau d'intervention 4
- Coopération, interaction et divulgation d'informations 4
- Communication et Authentification 4

Services **5**
- Réponse aux Incidents 5
  - Triage 5
  - Coordination 5
  - Résolution 5
- Activités d’anticipation 5

Formulaires de notification d'un incident **5**

Décharge de responsabilité **6**

1. A propos de ce document

Ce document contient la description du CERT Arkéa conformément à la RFC 2350[1].

1.1. Date de dernière mise à jour

La première version du document (1.0) a été écrite en mars 2019.
Ceci est la version 1.0 de mars 2019.

1.2. Liste de distribution pour notifications

Le CERT Arkéa n'utilise pas de liste de distribution pour les modifications de ce document.

1.3. Localisation de ce document

La dernière version de ce document est publiée sur le site Internet : https://cert.arkea.com

2. Points de contact

2.1. Nom de l'équipe

CERT ARKÉA

2.2. Adresse

CERT Arkéa
CRÉDIT MUTUEL ARKÉA
1, Rue Louis Lichou
29480 LE RELECQ KERHUON

2.3. Fuseau horaire

Paris - CET – Central European Time / HNEC - Heure normale d'Europe centrale / UTC +1

2.4. Numéro de téléphone

+33 2 98 00 51 80

2.5. Adresse de messagerie électronique

Les incidents de sécurité peuvent être déclarés sur l'email cert@arkea.com.

[1] https://www.ietf.org/rfc/rfc2350.txt

2.6. Information sur les clefs publiques et le chiffrement

PGP est utilisé pour les échanges entre le CERT et ses partenaires externes.
La clé publique du CERT est disponible à l'adresse https://cert.arkea.com :

- Identifiant : 0x7959BCAF ;
- Empreinte : F240 9508 905C D404 8936 718F B580 152D 7959 BCAF.

Cette clé peut aussi être téléchargée sur http://pgp.mit.edu/.
Elle est utilisée pour toute information qui nécessite une transmission de manière sécurisée.

2.7. Autres moyens de communication

Il n'existe pas d'autres moyens de contacter le CERT Arkéa à ce jour.

2.8. Membres de l'équipe

Le responsable du CERT Arkéa est Bruno Tignac, Responsable Sécurité Opérationnelle du Groupe Arkéa (RSOP), par ailleurs responsable du service Sécurité des Systèmes d'Information de la Direction de l'Exploitation et des Technologies du groupe Arkéa. L'équipe est composée d'analystes sécurité de ce service.

2.9. Autres informations

Les informations sur le CERT Arkéa sont disponibles sur : https://cert.arkea.com.

2.10. Points de contact

Le moyen de contact à privilégier pour les déclarations d'incident au CERT est l'email : cert@arkea.com.
Nous intervenons principalement en horaires de bureau : 08h-18h.
En cas d'urgence, le numéro de téléphone est joignable 24h/24, 7 jours sur 7, l'astreinte Sécurité décidera d'intervenir directement ou non.

3. Charte

3.1. Ordre de mission

Les missions du CERT Arkéa sont de :

- Coordonner de manière centralisée la résolution des incidents de sécurité de son périmètre d'intervention ;
- Analyser les incidents et menaces liés à la cybercriminalité, proposer des plans d'action visant à en réduire le risque ;

- Effectuer une veille permanente sur les problématiques de sécurité et le renseignement sur les menaces ciblant le Groupe ;
- Être le relais auprès des communautés Sécurité à l'extérieur du Groupe.

3.2. Périmètre d'intervention

Le CERT Arkéa intervient sur les incidents liés au système d'information du groupe Arkéa et l'ensemble des filiales exerçant des métiers financiers, technologiques, d'assurance, d'immobilier, de crédits à la consommation, de banque privée et de financement.

3.3. Support et/ou Affiliation

Le CERT Arkéa coordonne globalement la « tour de contrôle Sécurité d'Arkéa » et pilote à ce titre, fonctionnellement :

- Le guichet unique Sécurité d'Arkéa ;
- Le Security Operations Center (SOC) Arkéa.

Il travaille en étroite collaboration avec le RSSI du Groupe et ses équipes.

3.4. Autorité

Le CERT Arkéa agit sous l'autorité de la Direction du groupe Arkéa.

4. Politique

4.1. Types d'incidents et niveau d'intervention

Le CERT Arkéa intervient sur tous les incidents de sécurité qui se produisent sur son périmètre d'intervention.

Le niveau d'intervention dépend du type d'incident et de la criticité de celui-ci. Dans la mesure du possible, les incidents sont pris en charge dans l'heure qui suit leur signalement.

4.2. Coopération, interaction et divulgation d'informations

Le CERT Arkéa échange les informations techniques nécessaires avec la communauté Sécurité. Aucune donnée spécifique au Groupe ou donnée à caractère personnel n'est échangée sans l'accord explicite des personnes habilitées et concernées.

4.3. Communication et Authentification

Les communications téléphoniques du CERT Arkéa sont effectuées de manière non chiffrée.

Les emails sont par défaut envoyés non chiffrés. S'ils contiennent des informations sensibles, ils seront envoyés de préférence en utilisant PGP comme spécifié ci-dessus.

5. Services

5.1. Réponse aux Incidents

Le CERT Arkéa assiste les experts du Groupe pour la résolution des incidents de sécurité en apportant son aide sur les aspects organisationnels et techniques.

5.1.1. Triage

- Investigation sur le fait qu'un incident de sécurité est avéré ou non ;
- Identification de la gravité et du périmètre de l'incident de sécurité.

5.1.2. Coordination

- Détermination de la cause de l'incident ;
- Contacts des parties intéressées ;
- Contacts avec les autorités judiciaires et réglementaires en cas de besoin, en lien avec les équipes dédiées ;
- Contacts avec les autres CSIRTs (Computer Security Incident Response Teams) ;
- Préparation des communications internes et externes avec les équipes dédiées ;
- Partage des informations sur les menaces pour mettre en place des mesures proactives.

5.1.3. Résolution

- Suivi et support à la remédiation des incidents de sécurité ;
- Collecte des preuves de l'incident.

5.2. Activités d'anticipation

Le CERT Arkéa est en charge d'effectuer une veille globale Sécurité pour le Groupe.

Les résultats de cette veille peuvent notamment être communiqués par la publication hebdomadaire d'une communication sécurité interne écrite en français.

Le CERT Arkéa coordonne le renseignement sur les menaces liées à la Sécurité de l'Information (notamment sur les activités de Cyber Threat Intelligence).

6. Formulaires de notification d'un incident

Il n'existe pas de formulaire de notification d'un incident de sécurité à ce jour. L'email est le moyen à privilégier pour prévenir le CERT Arkéa.

7. Décharge de responsabilité

Les services du CERT Arkéa sont rendus de la manière la plus efficace possible mais, malgré toutes les précautions prises, certaines actions ne peuvent pas êtgre pleinement opérantes à ce jour.

Le CERT Arkéa ne pourra être tenu pour responsable de toutes les erreurs ou omissions ou d'éventuels dommages causés par les documents qu'il aura produits.