RFC 2350 CSIRT-ATLANTIC

Version 0.5 – 2024-07-16

Association Caribéenne pour la Cybersécurité (ACCYB)
SIREN 918714890
60 chemin de Reynald, Roujol, 97170 Petit-Bourg

A propos du document

Ce document contient une description du CSIRT-ATLANTIC de l'Agence Caribéenne pour la Cybersécurité tel que recommandée par la RFC2350[1]. Il présente des informations sur l'équipe, les services proposés et les moyens de contacter le CSIRT-ATLANTIC.

1.1. Date de la dernière mise à jour

Ceci est la version 0.5 de ce document, éditée le 16 juillet 2024.

Elle correspond à une version intermédiaire dans l'attente de la création de la ligne téléphonique du CSIRT-ATLANTIC.

1.2. Liste de distribution pour les modifications

Toutes les modifications apportées à ce document seront partagées via le canal suivant :

- https://csirt.accyb.org

1.3. Où trouver ce document

Ce document est disponible sur le site du CSIRT-ATLANTIC :

- https://csirt.accyb.org

1.4. Authenticité du document

Ce document a été signé à l'aide de la clé PGP du CSIRT-ATLANTIC.

La clé PGP publique, son identifiant et son empreinte sont disponibles sur le site internet du CSIRT-ATLANTIC à l'adresse suivante :

- https://csirt.accyb.org

1.5. Identification du document

Titre : RFC 2350 du CSIRT-ATLANTIC

Version : 0.5

Date de mise à jour : 16 juillet 2024

Durée de validité : ce document est valide tant qu'il n'existe pas de version ultérieure.

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

Informations de contact

2.1. Nom de l'équipe

Nom court : CSIRT-ATLANTIC

Nom complet : CSIRT- Atlantic Territories Liaison, Analysis, Networking, and Information security Coordination

2.2. Adresse

CSIRT-ATLANTIC
ACCYB, Agence Caribéenne pour la Cybersécurité
60 Chemin de Reynald
Roujol
97170 PETIT-BOURG, Guadeloupe

2.3. Zone horaire

CET/CEST : Guadeloupe (GMT-04:00)

2.4. Numéro de téléphone

+XXX XXX XXX XXX

2.5. Numéro de Fax

Aucun à ce jour.

2.6. Autres moyens de communication

Aucun à ce jour.

2.7. Adresse E-Mail

csirt-atlantic_at_accyb.org

2.8. Clé publique et informations liées au chiffrement

Commenté [YK1]: Ajouter date d'expiration de la clé

Commenté [YK2R1]: @Cédric PRADEL

PGP est utilisé pour garantir la confidentialité et l'intégrité des échanges avec le CSIRT-ATLANTIC. Identifiant utilisateur : ACCYB – CSIRT-ATLANTIC

Identifiant de la clé : 0x67A31EB306D56787

Empreinte de la clé : CFD2 DB9F C8F2 B281 56B8 3063 BC1F EADB

Expiration de la clé : 30 juin 2025

La clé PGP publique est disponible à cette adresse : https://csirt.accyb.org ainsi que sur les principaux serveurs de clés PGP :

- https://pgp.circl.lu
- https://pgp.mit.edu
- https://keys.openpgp.org
- https://keyserver.ubuntu.com
- https://keyserver.pgp.com

2.9. Membres de l'équipe

L'équipe est constituée de plusieurs membres :

- Un responsable;
- Plusieurs analystes.

2.10. Autres informations

Aucune à ce jour.

2.11. Contact

Le CSIRT-ATLANTIC est disponible durant les heures ouvrées, soit de 09h00 à 12h30 et de 13h30 à 17h00, du lundi au vendredi (hors jours fériés).

Pour joindre le CSIRT-ATLANTIC, le moyen de communication privilégié est le numéro de téléphone +XXX XXX XXX XXX et, en seconde intention, par courriel à l'adresse csirt-atlantic_at_accyb.org.

Nous encourageons l'utilisation de chiffrement avec les informations présentées dans le paragraphe 2.8 Clé publique et informations liées au chiffrement pour assurer l'intégrité et la confidentialité des échanges.

2.11.1. Dénomination et glossaire

ATLANTIC : Atlantic Territories Liaison, Analysis, Networking, and Information security Coordination

CSIRT : Computer Security Incident Response Team

BÉNÉFICIAIRE : Il désigne les collectivités (mairies, epci, epic, communautés de communes...) , les organismes publics, les PME, les ETI, ou les associations à ancrage régional qui bénéficient des services de réponse à incident du CriC-NA

BÉNÉFICIAIRE AVANCÉ : Il désigne les bénéficiaires qui ont adhéré à l'association *Agence Caribéenne pour la Cybersécurité*

Charte

3.1. Ordre de mission

Le CSIRT-ATLANTIC est l'équipe de réponse aux incidents de sécurité informatique des territoires de Guadeloupe, Guyane, Martinique, Saint-Barthélemy, Saint-Martin et de Saint-Pierre & Miquelon. Son objectif est d'apporter une assistance aux organisations de son territoire (décrites dans le paragraphe 3.2 Bénéficiaires) pour répondre aux incidents cyber auxquels elles font face.

3.2. Bénéficiaires

Les entités pouvant bénéficier de l'accompagnement du CSIRT-ATALNTIC sont les organisations localisées sur les territoires des îles de Guadeloupe, Guyane, Martinique, Saint-Barthélemy, Saint-Martin et Saint-Pierre & Miquelon, comprenant notamment :

- Les PME ;
- Les ETI ;
- Les collectivités territoriales et les établissements publiques associés ;
- Les associations.

3.3. Affiliation

Ce CSIRT-ATLANTIC est affilié à l'Agence Caribéenne pour la Cybersécurité (ACCYB).

3.4. Autorité

Le CSIRT-ATLANTIC réalise ses activités sous l'autorité de l'Agence Caribéenne pour la Cybersécurité (ACCYB), dont la Région Guadeloupe, la collectivité territoriale de Guyane et les collectivités d'outre-mer de Saint-Barthélemy et de Saint-Martin assurent la présidence en tant que membre de droit.

Politiques

4.1. Types d'incidents et niveau d'intervention

Le périmètre d'action du CSIRT-ATLANTIC couvre tous les incidents de sécurité informatique touchant les organisations de son territoire décrites dans le paragraphe 3.2 Bénéficiaires.

Les missions principales du CSIRT-ATLANTIC sont :

- Offrir une réponse de premier niveau pour les incidents cyber survenant chez ses bénéficiaires ;
- Rediriger ses bénéficiaires vers des prestataires territoriaux pour la remédiation de l'incident ;
- Agir comme un relai entre le CERT-FR, les prestataires régionaux, les services de Police et de Gendarmerie et les bénéficiaires ;
- Consolider les statistiques d'incidentologie à l'échelle inter-régionale (Guadeloupe, Guyane, Saint-Barthélemy et Saint-Martin).

4.2. Coopération, interaction et partage d'information

Les informations relatives à un incident telles que le nom de la structure et les détails techniques ne sont pas publiées sans l'accord de la partie nommée.

Le CSIRT-ATLANTIC peut être amené à communiquer des informations aux autres CSIRT régionaux ou au CERT-FR lorsqu'une structure sollicite leur appui. De la même manière, des informations pourront être partagées à un CSIRT sectoriel (santé, maritime, aviation, ...) à des fins de capitalisation des incidents propres au secteur concerné.

La diffusion d'information sera traitée en accord avec le protocole TLP défini par FIRST (https://www.first.org/tlp).

4.3. Communication et authentification

Le CSIRT-ATLANTIC conseille fortement l'utilisation de canaux de communication sécurisés et du chiffrement PGP, en particulier pour communiquer des informations confidentielles ou sensibles.

Les informations non confidentielles ou peu sensibles peuvent être transmises via des courriels non chiffrés

Services

5.1. Réponse aux incidents

L'activité principale du CSIRT-ATLANTIC est de venir en aide à ses bénéficiaires en proposant un service de réponse de premier niveau aux incidents cyber et de les aider à affiner leur choix de prestataire pour les accompagner dans la suite de la résolution des incidents.

En particulier, il propose les services détaillés dans les paragraphes suivants.

5.1.1.Triage

- Récupération du signalement et prise de contact avec le déclarant ;
- Collecte d'informations sur l'incident et confirmation ou évaluation de la nature de l'incident ;
- Détermination de la sévérité de l'incident (son impact) et de son périmètre (nombre de machines affectés) ;
- Catégorisation de l'incident.

5.1.2.Coordination

- Identification du meilleur partenaire au sein du dispositif national de réponse aux incidents pour accompagner le demandeur ;
- Accompagnement dans la diffusion, le cas échéant, de signalements vers les autorités compétentes de l'Etat selon la nature de l'incident. Notamment, mais de manière non exhaustive :
  - A l'ANSSI en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs ;
  - A la Commission Nationale de l'Informatique et des Libertés (CNIL) en cas de violation de données à caractère personnel.

5.1.3.Résolution

- Proposition d'actions réflexes, notamment des mesures d'urgence pour limiter l'impact de l'incident ou des mesures destinées à faciliter les investigations et le traitement de l'incident ;
- Partage d'une liste restreinte de prestataires de proximité capables d'assurer la résolution et la remédiation de l'incident ;
- Suivi des phases de résolution et de remédiation.

5.2. Activités proactives

Le CSIRT-ATLANTIC pourra aussi proposer des services proactifs à ses bénéficiaires, notamment :

- Des services de veille ;
- Des analyses de menaces ;
- Veille d'exposition sur Internet;
- Un bulletin de veille à destination d'abonnés.

Formulaires de notification d'incident

Un formulaire de notification est disponible en ligne à cette adresse :

https://www.accyb.org/fr/alertreports/HandleFirstForm

En cas de déclaration par courriel, pour faciliter la prise en compte des signalements, les éléments suivants sont si possibles à fournir :

- Informations sur l'organisation touchée (nom, contact de la direction et des équipes techniques, taille...) ;
- Informations de contact du demandeur comprenant notamment : nom, fonction et numéro de téléphone ;
- Chronologie de l'incident : date et heure du début de l'incident et de sa détection ;
- Description de l'incident comprenant notamment l'impact sur l'organisation et le nombre et type de machines
- touchées ;
- Actions effectuées depuis la détection de l'incident ;
- Toute autre résultat d'investigations déjà menées ;
- Architecture du système d'informations ;
- Outils et politiques de défense contre les incidents en place ;
- Si le demandeur est déjà en contact avec un prestataire de réponse aux incidents de sécurité informatique ;
- Services attendus de la part d'une équipe de réponse aux incidents.

Décharge de responsabilité

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, le CSIRT-ATLANTIC n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultant de l'utilisation des informations contenues.