CSIRT Hauts-de-France

RFC2350

Juillet 2024

CSIRT Hauts-de-France - Bâtiment Place
172 Avenue de Bretagne, 59000 LILLE
Siret : 910 770 064 00012

Table des matières

1. À propos du document

Ce document contient une description du CSIRT Hauts-de-France tel que recommandé par la RFC2350[1]. Il présente des informations sur l'équipe, les services proposés et les moyens de contacter le CSIRT HdF.

1.1 Date de dernière mise à jour

Ceci est la version 1.5 de ce document, éditée le 08/07/2024

1.2 Liste de distribution pour les modifications

Toutes les modifications apportées à ce document seront partagées via les canaux suivants :

- https://csirt-hdf.fr/politique-de-confidentialite/

1.3 Où trouver ce document

Ce document peut être trouvé sur le site du CSIRT HdF : https://csirt-hdf.fr/

1.4 Identification du document

Titre : RFC 2350 du CSIRT HdF
Version : 1.5
Date de mise à jour : 08/07/2024
Durée de validité : ce document est valide tant qu'il n'existe pas de version ultérieure.

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

2. Informations de contact

2.1 Nom de l'équipe

Nom court : CSIRT HdF
Nom complet : CSIRT Hauts-de-France

2.2 Adresse

149 avenue de Bretagne, Lille 59000

2.3 Zone horaire

CET/CEST : Paris (GMT+01:00, et GMT+02:00 heure d'été)

2.4 Numéro de téléphone

0 806 700 111

2.5 Numéro de Fax

Aucun

2.6 Autres moyens de communication

Aucun

2.7 Adresse E-Mail

jelahmar@csirt-hdf.fr

2.8 Membres de l'équipe

L'équipe est constituée de 5 membres :

- Un responsable du CSIRT ;
- Un adjoint au responsable ;
- Trois analystes.

Le responsable du CSIRT HdF est MONSIEUR CHEKIB GHARBI.

2.9 Autres informations

Aucune à ce jour.

2.10 Contact

Le CSIRT HdF est disponible durant les heures ouvrées, soit de 9 heures à 12h30 et de 14h à 17 heures 30 du lundi au vendredi (hors jours fériés). Pour les heures non ouvrées, les appels seront pris par le CERT-FR, soit les nuits (de 17h30 à 9h), les week-ends et jours fériés plus durant les creux de 12h30 à 14h.

Pour joindre le CSIRT HdF, le moyen de communication privilégié est par sa page de dépôt BlueFiles disponible à l'adresse suivante :

https://bluefiles.com/app/drop-page/cb12270ea54742d9d89265deaa04b17b927b23c0fda0ba064b480d45dd44fcf7/

En cas d'urgence, veuillez spécifier la balise [URGENT] dans le champ objet de votre courriel. Le CSIRT HdF est aussi joignable par téléphone au 0 806 700 111 .

3. Charte

3.1 Ordre de mission

Le CSIRT HdF est l'équipe de réponse aux incidents de sécurité informatique de la région HAUTS-DE-FRANCE. 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 HdF sont les organisations localisées sur le territoire de la région HAUTS-DE-FRANCE, comprenant notamment :

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

3.3 Affiliation

Ce CSIRT est affilié à la région Hauts-de-France

3.4 Autorité

Le CSIRT HdF réalise ses activités sous l'autorité de de la région Hauts-de-France.

4. Politiques

4.1 Types d'incidents et niveau d'intervention

Le périmètre d'action du CSIRT HdF 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 HdF sont :

- Offrir une réponse de premier niveau pour les incidents cyber survenant chez ses bénéficiaires ;
- Accompagner les bénéficiaires du dispositif (§ 3.2) victimes d'un incident informatique et les orienter vers des prestataires en sécurité informatique, référencés de la région ;
- Contribuer à la sensibilisation des entreprises de la région de manière permanente en relayant les informations disponibles auprès des organismes d'état et d'entreprises spécialisées en cybersécurité.;
- Alerter les bénéficiaires de ces menaces et vulnérabilités ;
- 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 régionale.

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 HdF 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…) 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 HdF conseille fortement l'utilisation de canaux de communication sécurisés, en particulier pour communiquer des informations confidentielles ou sensibles.

Les informations non confidentielles ou sensibles peuvent être transmises via des courriels non chiffrés à l'adresse :

jelahmar@citc-eurarfid.com

5. Services

5.1 Réponse aux incidents

L'activité principale du CSIRT HdF 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[2] 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 HdF pourra aussi proposer des services proactifs à ses bénéficiaires, notamment :

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

[2] Redirection éventuelle vers ACYMA, le CERT-FR ou autre CSIRT (e.g. sectoriel)

6. Formulaires de notification d'incident

Un formulaire permettant de notifier le CSIRT HdF est disponible à l'adresse :

https://csirt-hdf.fr/contact/

Pour faciliter la prise en compte des signalements, les éléments suivants sont 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.

7. Décharge de responsabilité

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