RFC 2350 - CSIRT EXODATA Cyberdefense

Version 1.0 - 20-01-2023

Exodata Cyberdefense
4 Rue Emile Hugot 97490 Sainte-Clotilde
www.exodata.fr

1. Information du document

Ce document contient une description du CSIRT EXODATA Cyberdefense tel que recommandé par la RFC2350. Il présente des informations sur l'équipe, les services proposés et les moyens de contacter le CSIRT EXODATA Cyberdefense.

1.1. Date de la dernière mise à jour

Ce document est la version 1.0 de la RFC2350 du CSIRT EXODATA Cyberdefense, publié le 17 janvier 2023.

1.2. Liste de diffusion pour les notifications

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

- https://www.exodata.fr/cybersecurite/csirt-as-a-service/uploads/RFC2350
- InterCERT-FR / réseau de Français CSIRT - www.cert.ssi.gouv.fr/csirt/intercert-fr

Il est possible d'envoyer des requêtes sur les informations mises à jour dans ce présent document à l'adresse e-mail de l'équipe CSIRT EXODATA Cyberdefense : incidents@exodata-csirt.fr. Ces échanges peuvent être sécurisés par l'utilisation de l'infrastructure PGP.

1.3. Lieux où ce document peut être retrouvé

La dernière version de ce document peut être retrouvée sur le site du CSIRT EXODATA Cyberdefense à l'emplacement suivant : https://www.exodata.fr/cybersecurite/csirt-as-a-service/uploads/

1.4. Authentification et intégrité de ce document

Ce document a été signé avec la clé PGP du CSIRT EXODATA Cyberdefense.
La signature et la clé publique du CSIRT EXODATA Cyberdefense (Identifiant et empreinte) sont disponible sur le site du CSIRT EXODATA Cyberdefense : https://www.exodata.fr/cybersecurite/csirt-as-a-service/contact

1.5. Identification du document

Titre : RFC2350 du CSIRT EXODATA Cyberdefense
Version : 1.0
Date de mise à jour : 20/01/2023
Expiration : ce document est valide jusqu'à sa prochaine nouvelle version disponible.

2. Information de contact

2.1. Nom de l'équipe

Nom officiel : CSIRT EXODATA Cyberdefense
Nom usuel : CSIRT EXODATA

2.2. Adresse

EXODATA Cyberdefense
Equipe CSIRT
4 rue Emile Hugot
97490 Sainte-Clotilde

2.3. Fuseau horaire

RET / UTC+4 (Heure de la Réunion)

2.4. Numéro de téléphone

+33 (0)9 71 05 77 59

2.5. Numéro de FAX
Non applicable

2.6. Autre télécommunication
Non applicable

2.7. Adresse de messagerie électronique
incidents@exodata-csirt.fr

2.8. Clés publiques et informations de chiffrement
CSIRT EXODATA Cyberdefense utilise la clé PGP suivante :
ID utilisateur : incidents@exodata-csirt.fr
ID clé : 0x81932F45B59FE677
Empreinte : DCCA FC27 9CDB 3D71 9D98 6088 8193 2F45 B59F E677

La clé PGP peut être récupérée sur des serveurs de clés publiques tels que https://keys.openpgp.org/search?q=incidents%40exodata-csirt.fr ou directement sur le site du CSIRT EXODATA Cyberdefense : Clé PGP.

2.9. Membres de l'équipe
L'équipe du CSIRT EXODATA Cyberdefense est composée d'experts en sécurité informatique.

La liste des membres de l'équipe du CSIRT EXODATA Cyberdefense n'est pas disponible publiquement. L'identité des membres peut être divulguée au cas par cas, en fonction du besoin d'en connaître.

2.10. Autre information
Consulter le site web du CSIRT EXODATA Cyberdefense à l'adresse https://www.exodata.fr/cybersecurite/csirt-as-a-service pour obtenir des informations complémentaires.

2.11. Point de contact clients
Le CSIRT EXODATA Cyberdefense est disponible durant les heures ouvrées, soit de 8 heures à 19 heures du lundi au vendredi (hors jours fériés).
Pour joindre le CSIRT EXODATA Cyberdefense, le moyen de communication privilégié est par courriel à l'adresse incidents@exodata-csirt.fr. Merci d'utiliser la clé cryptographique PGP du CSIRT EXODATA Cyberdefense pour garantir l'intégrité et la confidentialité des informations échangées.
En cas d'urgence, veuillez spécifier la balise [URGENT] dans le champ objet de votre courriel.

3. Charte
3.1. Ordre de missions

3.2. Bénéficiaires

Les entités pouvant bénéficier de l'accompagnement du CSIRT EXODATA Cyberdefense sont les organisations localisées sur les territoires Français métropolitain, d'outres-mers et du reste du monde, appartenant aux catégories suivantes :

- Les multinationales ;
- Les PME ;
- Les ETI ;
- Les collectivités territoriales et les établissements publiques ;

- Les établissements de santé.

3.3. Affiliation

Le CSIRT EXODATA Cyberdefense est membre du Campus Cyber de Nouvelle Aquitaine.

3.4. Autorité

CSIRT EXODATA Cyberdefense opère sous l'autorité du Directeur du pôle Cybersécurité du groupe EXODATA.

4. Politiques

4.1. Type d'incidents et niveau d'assistance

Le périmètre d'action du CSIRT EXODATA Cyberdefense couvre tous les incidents de sécurité informatique touchant les organisations des territoires décrites dans le paragraphe 3.2 Bénéficiaires.
Le niveau de soutien dépend du type et de la gravité de l'incident de sécurité en question, du nombre d'entités affectées, et des ressources disponibles au moment de l'évènement.

4.2. Coopération, interaction et divulgation d'informations

La publication d'informations relatives à un incident telles que le nom de la structure et les détails techniques est réalisée uniquement après avoir obtenu l'accord de la partie nommée.
Le CSIRT EXODATA Cyberdefense peut être amené à communiquer des informations aux 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 à des fins de capitalisation des incidents propres au secteur concerné toujours avec l'accord préalable du client.
Toutes les informations sont transmises en fonction de leur classification et du principe du besoin de savoir.
Le CSIRT EXODATA Cyberdefense traite l'information dans des environnements physiques et logiques sécurisés conformément aux réglementations existantes en matière de protection de l'information défini par l'agence nationale de la sécurité des systèmes d'information (ANSSI).

4.3. Communication et authentification

La méthode de communication privilégiée est le courrier électronique.
Pour l'échange d'informations sensibles et la communication authentifiée CSIRT EXODATA Cyberdefense utilise plusieurs solutions de chiffrement.
Par défaut, toutes les communications sensibles doivent être chiffrées avec notre clé publique PGP détaillée dans la section 2.7.
Les informations générales non restreintes peuvent être transmises par téléphone, courrier ordinaire ou courrier électronique non chiffré.
Le CERT EXODATA Cyberdefense respecte le protocole de partage d'information Traffic Light Protocol (TLP : https://www.first.org/tlp) qui se présente sous la forme de balises BLANC, VERT, AMBRE ou ROUGE en fonction du niveau de confidentialité des données échangées.

5. Services

5.1. Réponse à incident

Le CSIRT EXODATA Cyberdefense interviendra pour ses clients bénéficiaires (sous forme d'abonnement) en priorité ainsi que toutes les entités subissant un incident de sécurité de manière opportuniste.
Voici les services qu'offre le CSIRT EXODATA Cyberdefense à ses clients :

- Gestion de crise (soutien & coordination de la réponse à incident)
- Communication lors de la réponse à incident
- Réponse à incident (traitement & analyse et réponse aux incidents)
- Forensics (analyse et réponse techniques des artefacts)
- Réponse aux incidents sur site et à distance

- Cyber Threat Intelligence (renseignement sur les cybermenaces)

5.1.1. Triage, qualification de l'incident

- Prise en charge du signalement de la victime de l'incident de sécurité ;
- Collecte d'informations auprès du déclarant afin de qualifier la nature de l'incident ;
- Déterminer la sévérité de l'impact de l'incident / son périmètre au sein du système d'informations ;
- Catégorisation de l'incident de sécurité.

5.1.2. Coordination de l'incident

- Catégorisation des informations liées à l'incident ;
- Notification des autres parties concernées sur la base du besoin de savoir.

5.1.3. Traitement de l'incident

- Analyse des systèmes compromis ;
- Isolation des machines compromises
- Aide à l'Eradication de la cause d'un incident de sécurité et de ses impacts.
- Conseils pour le plan de rétablissement des services.
- Etablissement d'un RETEX

5.1.4. Activités proactives

Le CSIRT EXODATA Cyberdefense propose des services proactifs à ses clients, notamment :

- Des services de veille ;
- Des analyses de menaces cybersécurité ;
- Un bulletin d'alerte en fonction de l'actualité à destination de ses clients abonnés.

5.1.5. Gestion des vulnérabilités

- Analyse des nouvelles vulnérabilités faisant l'actualité ;
- Rédaction de rapport de vulnérabilités à ses clients abonnés.

5.1.6. Analyse des cybermenaces (Cyber Threat Intelligence CTI)

- Collecte de flux d'indicateurs de compromission (IOC) pour aider les clients abonnés et les partenaires à détecter et à prévenir les menaces et à analyser les incidents.

6. Formulaires de rapport d'incident

Un formulaire permettant de notifier le CSIRT EXODATA Cyberdefense d'un incident est disponible sur le site https://www.exodata.fr/cybersecurite/csirt-as-a-service en bas de page dans la rubrique "Contactez notre équipe CSIRT".

7. Décharge de responsabilité

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, le CSIRT EXODATA Cyberdefense n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultant de l'utilisation des informations contenues dans ce présent document.
Si vous constatez une erreur dans ce document merci de nous le signaler par mail. Ces-dernières seront corrigées dans les délais les plus rapides possible.