CSIRT WHALLER

Description CSIRT Whaller – RFC 2350

CSIRT-WHALLER
csirt@whaller.fr

TLP CLEAR

Table des matières

Classification	Public	Sensible	Privé	Confidentiel
	X			

I. A propos de ce document

Afin d'assurer un haut niveau de Cybersécurité à ses clients et partenaires, Whaller met en œuvre un CSIRT. Il pourra ainsi collaborer efficacement à l'échelle nationale avec d'autres entités dans le partage d'éléments mais également en apportant des services de veille à ses clients. L'approche pour piloter ce processus est celle définie par l'ENISA.

1. Dernière mise à jour

Ce document est la version 1.0 du 06/03/2024

2. Notification des modifications

Les modifications apportées à ce document ne sont pas notifiées

3. Lieu de publication

La version actualisée du présent document est disponible à l'adresse https://whaller.com/csirt

4. Authenticité du document

Le présent document est signé par la clef PGP du CSIRT Whaller

5. Identification du document

- Titre : Description CSIRT Whaller – RFC 2350
- Version : 1.0
- Date 06/03/2024
- Expiration : Ce document est valide jusqu'à son remplacement par une nouvelle version.

II. Informations de contact

1. Nom

Nom complet : Centre de réponse à incident de Whaller
Nom abrégé : CSIRT WHALLER

Classification	Public	Sensible	Privé	Confidentiel
	X			

2. Adresse

WHALLER
3, rue Salomon de Rothschild
92150 Suresnes
France

3. Fuseau horaire

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

4. Numéro de téléphone

N/A

5. Numéro de Fax

N/A

6. Autres moyens de communication

N/A

7. Messagerie électronique

L'adresse courriel de contact est : csirt@whaller.fr

8. Clé publique et moyens de chiffrement

CSIRT Whaller
Email : csirt@whaller.fr
Identifiant de la clé : 0x8750B7A947E35C41
Empreinte : 11B8 1371 FD27 E007 8E71 C91C 8750 B7A9 47E3 5C41
Expiration : 06/03/2027

La clef publique est disponible à l'adresse https://whaller.com/csirt/

9. Composition de l'équipe

L'équipe est constituée d'ingénieurs en Cybersécurité. La liste nominative des membres n'est pas publique pour des raisons de confidentialité.

10. Autres informations

Les informations sur le CISRT Whaller sont disponibles à l'adresse https://whaller.com/csirt

Classification	Public	Sensible	Privé	Confidentiel
	X			

11. Contact

Le moyen de communication à utiliser pour contacter le CSIRT Whaller est la messagerie électronique. Il est recommandé de faire usage de la clef PGP indiquée afin de garantir la confidentialité et l'intégrité des données transmises.
Horaires de fonctionnement : Lundi – Vendredi 08h-18h (hors jours fériés en France).

III. Charte

1. Missions

Le CSIRT peut conseiller nos clients, prendre les mesures nécessaires à la gestion des incidents de Cybersécurité sur le périmètre établi.
Le CSIRT a la responsabilité de tenir à jour la liste des incidents, de collecter les artefacts techniques mais également en assurer la capitalisation et le partage. C'est également lui qui assure la veille sur la menace d'origine cyber.
Le CSIRT Whaller est localisé en France a pour missions :

- la réponse à incident
- le suivi des vulnérabilités
- l'analyse des codes malveillants
- la collecte d'artefacts techniques (IOC)
- être le point de contact unique pour les incidents d'origine cyber internes ou externes
- assurer une veille sur la menace en interne et en externe

2. Périmètre d'action

Le CSIRT Whaller couvre l'ensemble des activités numérique de Whaller et des services hébergés pour nos clients mais également le système d'information interne de Whaller.

3. Parrainage et affiliation

Le CSIRT Whaller est un CSIRT privé qui échange avec ses partenaires institutionnels mais également d'autres CSIRT.

4. Autorité

Le CSIRT Whaller agit sous l'autorité du directeur Cybersécurité de Whaller.

IV. Politiques

1. Types d'incidents et niveau de support

La typologie des incidents est définies dans une procédure interne.
Il existe 4 niveaux de priorité d'incidents :

- Niveau 0 : Pré-incident, aucun impact sur les activités de Whaller
- Niveau 1 : Incident isolé (un compte utilisateur, un poste de travail…), aucun impact sur les activités de Whaller
- Niveau 2 : incident affectant plusieurs ressources (serveurs, poste utilisateur, comptes…), un impact sur les activités de Whaller
- Niveau 3 : incident majeur affectant une grande partie des ressources, un impact fort sur les activités de Whaller

Le CSIRT-Whaller coordonne la réponse à incident en lien avec la direction Tech de Whaller et les clients impactés. Il communique systématiquement aux clients concernés un rapport d'incident ainsi que les éléments techniques disponibles. Une capitalisation est effectuée sur les incidents afin d'améliorer les capacités de détection ultérieures.
Le niveau de service offert par le CSIRT Whaller est conditionné par les ressources disponibles pour le prendre en charge.

2. Coopération, interaction et confidentialité de l'information

Le CSIRT Whaller échange des informations avec ses clients et partenaires au travers d'une plateforme d'échange d'IOC mise à disposition de ces derniers.
Les informations et éléments techniques nécessaires sont communiquées aux autorités judiciaires en cas de dépôt de plainte.
Des échanges avec d'autres CERT/CSIRT peuvent être effectués en s'appuyant sur des canaux de transmission sécurisés.
Aucune données nominatives ne sont transmises sauf si ces dernières contribuent à l'identification d'une menace.

3. Communication

Le vecteur de communication à utiliser est la messagerie électronique.
Les échanges d'informations doivent s'opérer en utilisant des protocoles sécurisés. A ces fins le CSIRT Whaller met à disposition une clef publique OpenPGP.
Les informations sont transmises en appliquant le protocole de partage d'information (TLP) dont une description est disponible à l'adresse :
https://www.cert.ssi.gouv.fr/csirt/politique-partage/

V. Services

1. Sensibilisation

Le CSIRT Whaller propose au travers du blog Whaller des contenus de sensibilisation à disposition du public.

2. Réponse à incident

Le CSIRT Whaller propose les services suivants dans le cadre d'une réponse à un incident d'origine cyber.

- Détection des incidents
- Analyse technique et corrélation avec des éléments déjà connus
- Contact avec les équipes SSI des clients concernés
- Collecte des informations et mise en forme dans un rapport d'incident
- Coordination avec les autorités (ANSSI, autorités judiciaires..)

3. Veille

Le CSIRT Whaller réalise une veille sur les menaces. Un état mensuel de la menace observée par le CISRT Whaller est communiqué à nos clients et partenaires.

VI. Formulaire de déclaration d'incident

Les signalements d'incidents doivent être réalisés via l'adresse csirt@whaller.fr. Il est demandé de fournir les informations suivantes :

- Date et heure de survenue et/ou détection de l'incident
- Les éléments techniques (adresses IP, login utilisateur…) qui permettront un ciblage précis dans la recherche d'IOC.

VII. Décharge de responsabilité

Bien que toutes les précautions d'usage et vérifications aient été prises lors de la communication de toute information, le CISRT Whaller se décharge de toute responsabilité pour les erreurs, omissions, et préjudices résultant des informations fournies.