LA CYBERSÉCURITÉ AU COEUR DE VOS MÉTIERS

# Escouade Cyber

RFC 2350

Version 1.0 | 03/06/2024 | Public | TLP:CLEAR

# SOMMAIRE

# EVOLUTIONS DU DOCUMENT

**Personnes ayant contribué à la rédaction de ce document :**

| Contributeurs | Rédigé par | Approuvé par | Date |
|---|---|---|---|
| JRE, AMD | JRE | AMD | 03/06/2024 |

**Evolutions du document :**

| Version | Date | Nature des modifications |
|---|---|---|
| 1.0 | 03/06/2024 | Version initiale |

**Votre contact WALLACK :**

| Contact | @mél | Téléphone |
|---|---|---|
| Escouade Cyber – WALLACK | escouade@wallack.fr | 02 99 22 02 85 |

# A PROPOS DU DOCUMENT

Ce document contient une description de l'équipe Escouade Cyber de Wallack tel que recommandé par la RFC2350[1].

Il présente des informations sur l'équipe, les services proposés et les moyens de contacter Wallack pour bénéficier d'une intervention de l'Escouade Cyber.

## Liste de distribution pour les modifications

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

- Le site internet de Wallack : https://www.wallack.fr/rfc2350

## Où trouver ce document

Ce document peut être trouvé sur le site de Wallack :

https://www.wallack.fr/pdf/rfc2350/Wallack-EscouadeCyber-rfc2350-v1.0.pdf

## Authenticité du document

Ce document a été signé à l'aide de la clé PGP de Wallack.

La clé PGP publique, son identifiant et son empreinte sont disponibles sur le site internet de Wallack à l'adresse suivante :

https://www.wallack.fr/pgp

L'empreinte cryptographique attestant de l'intégrité de ce document est disponible sur le site internet de Wallack à l'adresse suivante :

https://www.wallack.fr/pdf/rfc2350/Wallack-EscouadeCyber-rfc2350-v1.0.pdf.sig

## Identification du document

Titre : Escouade Cyber – RFC 2350

Version : 1.0

Date de mise à jour : 03/06/2024

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

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

# INFORMATIONS DE CONTACT

## Nom de l'équipe

Nom complet : WALLACK - Escouade Cyber

Nom court : Escouade Cyber

## Adresse

Wallack

91 route Nationale

35650 LE RHEU

## Zone horaire

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

## Numéro de téléphone

Il est nécessaire de passer par le standard de Wallack au 02 99 22 02 85 pour joindre l'Escouade Cyber.

Pour les partenaires du CSIRT, une ligne directe peut être communiquée (voir adresse courriel de contact).

## Numéro de fax

Non applicable

## Adresse E-Mail

escouade@wallack.fr

## Clé publique et informations liées au chiffrement

PGP est utilisé pour garantir la confidentialité et l'intégrité des échanges.

Identifiant utilisateur : escouade@wallack.fr

Identifiant de la clé : 1761 98D1 5AEA DB5E

Empreinte : 8C52 BEE0 DB69 5898 B35D D4E1 1761 98D1 5AEA DB5E

La clé PGP publique est disponible à cette adresse :

https://www.wallack.fr/pgp

## Membre de l'équipe

L'équipe de l'Escouade Cyber de Wallack est composée d'analystes ou de spécialistes de la cybersécurité.

Pour des raisons de confidentialité, les noms des membres de l'équipe ne sont pas rendus publics.

Veuillez contacter directement Wallack pour de plus amples informations.

## Autres informations

Aucune à ce jour.

## Contact

L'Escouade Cyber est joignable de 8h30 à 17h30 du lundi au vendredi (hors jours fériés).

Pour joindre l'Escouade Cyber, les moyens de communication privilégiés sont :

- le standard téléphonique de Wallack au 02 99 22 02 85
- le courriel à l'adresse escouade@wallack.fr

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

# CHARTE

## Ordre de mission

L'Escouade Cyber est l'équipe de réponse à incident de Wallack. Elle opère dans le cadre des prestations de service suivantes :

- La prestation Référent Cyber pour les clients ayant souscrit à cette prestation avant la cyberattaque.
- La prestation Escouade Cyber pour les autres clients.

Son objectif est d'apporter une assistance technique et organisationnelle à ses clients pour faire face aux incidents cyber qui les affectent.

## Bénéficiaires

Les entités pouvant bénéficier d'une intervention de l'Escouade cyber sont les organisations publiques ou privées, comprenant des SI classiques, de santé, ou industriels, comprenant jusqu'à 1500 collaborateurs et localisées dans les régions suivantes :

- Bretagne
- Ile-de-France
- Normandie
- Pays de la Loire

## Affiliation

L'Escouade Cyber est une équipe de réponse à incident opérant dans le cadre des prestations de la société Wallack SAS (SIREN 877 494 823).

L'entreprise est spécialisée dans la cybersécurité des TPE, PME, ETI et des collectivités territoriales comprenant moins de 1500 collaborateurs ou agents.

Tous les collaborateurs opérant dans le cadre de l'Escouade Cyber disposent d'un contrat de travail avec la société Wallack SAS.

## Autorité

L'Escouade Cyber obtient sa légitimité d'intervention par la signature d'un contrat de prestation avec l'organisation bénéficiaire.

# POLITIQUES

## Types d'incidents et niveau d'intervention

Le périmètre d'action de l'Escouade Cyber couvre tous les incidents de sécurité des systèmes d'information touchant les organisations décrites dans le paragraphe *Bénéficiaires*.

Les capacités principales de l'Escouade Cyber sont :

- L'accompagnement organisationnel à la gestion de crise à la suite d'un événement cyber ;
- L'investigation numérique pour comprendre les causes de l'événement et mesurer son étendue ;
- La construction et l'accompagnement au déploiement d'un plan de remédiation en lien avec les équipes internes du client.

## 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, ni partagées sans l'accord explicite du client.

L'Escouade Cyber peut être amenée à communiquer des informations à des CSIRT régionaux, des CSIRT sectoriels, le CERT-FR ou d'autres CERT lorsque ces derniers ont été sollicités par le client ou que des dispositions réglementaires imposent une notification.

L'Escouade Cyber peut être amenée à communiquer des informations à la Gendarmerie Nationale ou à la Police Nationale dans le cadre d'un dépôt de plainte effectué par le client.

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

## Communication et authentification

L'Escouade Cyber privilégie l'utilisation de canaux de communication sécurisés (comme des plateformes d'échanges de fichiers ou le chiffrement PGP), en particulier pour communiquer des informations confidentielles ou sensibles.

L'Escouade Cyber utilise PGP pour signer/chiffrer les courriels sensibles.

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

# SERVICES

## Réponse aux incidents

L'activité principale de l'Escouade Cyber est d'apporter à ses clients une expertise dans la gestion des incidents de cybersécurité. Cela se décline en trois catégories :

### Assistance à la gestion de crise – Profil RSSI

- Assistance à la création d'une cellule de crise cyber et à son animation ;
- Aide à la décision en contexte de crise cyber ;
- Accompagnement dans les démarches administratives (dépôt de plainte, déclaration CNIL…) ;
- Accompagnement dans les échanges avec les parties prenantes ;
- Assistance dans la communication de crise ;
- Création d'un plan de continuité ou de reprise d'activité ;
- Documentation de la gestion de crise (vérifier la bonne tenue d'une main courante, rédiger des comptes-rendus des échanges, etc.).

### Investigation numérique – Profil Analyste Forensique

- Collecte des preuves techniques de l'incident ;
- Compréhension des techniques utilisées par l'attaquant ;
- Echange avec les experts techniques des parties prenantes ;
- Compilation d'indicateurs de compromissions pour capitalisation ;
- Rédaction de rapports consignant les découvertes effectuées, les actions menées, etc.

### Remédiation – Profil Ingénieur Cybersécurité

- Création d'un plan de remédiation en cohérence avec les investigations numériques ;
- Accompagnement au déploiement du plan de remédiation.

# DECHARGE DE RESPONSABILITE

Ce document rassemble sous un format normalisé (voir RFC 2350) les informations utiles permettant de comprendre les services de l'Escouade Cyber et d'entrer en contact avec l'équipe.

Ce document ne saurait constituer un engagement de la part de l'Escouade Cyber vis-à-vis de tout tiers non lié par un contrat de prestation.

La responsabilité de la société Wallack SAS ne saurait être engagée en cas d'erreur, d'omission, ou de dommages résultant d'actions réalisées par un bénéficiaire ou tout autre acteur sur la base du présent document.