cegedim.cloud

RFC 2350

- cegedim.cloud CSIRT

1 LES INFORMATIONS SUR LE DOCUMENT

Ce document contient une description de CSIRT cegedim.cloud conforme à la spécification RFC 2350. Il fournit des informations de base sur CSIRT cegedim.cloud, décrit ses responsabilités ainsi que les services qu'il offre.

1.1 Date de la dernière mise à jour

Version	Date	Description des modifications
1.0	08/05/2025	Création du document RFC 2350

1.2 Liste de distribution pour les notifications

Il n'existe pas de liste de distribution publique pour les notifications de nouvelles versions de ce document.
Les mises à jour seront annoncées via le site officiel de cegedim.cloud à l'adresse suivante : https://www.cegedim.cloud/csirt.

1.3 Emplacements où ce document peut être consulté

La version actuelle de ce document est disponible à l'adresse suivante : https://www.cegedim.cloud/csirt.
Pour des raisons de validation, une version signée numériquement (GPG) est disponible à l'adresse : https://www.cegedim.cloud/csirt.

1.4 Authentification de ce document

Ce document est signé avec la clé GPG du CSIRT cegedim.cloud.

La clé publique est disponible à l'adresse :
https://cegedim.cloud/wp-content/uploads/2025/10/public.asc

KeyID : DE2F 24B1 2CCD 89AF
Empreinte : 885D94F099025163DA55FBE9DE2F24B12CCD89AF

2 LES INFORMATIONS DE CONTACT DU CSIRT

2.1 Nom de l'équipe

cegedim.cloud CSIRT (Computer Security Incident Response Team).

2.2 Adresse

cegedim.cloud
137 rue d'Aguesseau,
92100 Boulogne-Billancourt, France

2.3 Fuseau horaire

Europe/Paris, UTC+1 (UTC+2 pendant l'heure d'été).

2.4 Numéro de téléphone

Le numéro du CSIRT est partagé avec les membres constituants.
Les organismes ne faisant pas partie des constituants peuvent contacter le CSIRT via le formulaire disponible sur le portail cegedim.cloud.
Lien : Contact - Cegedim Cloud.

2.5 Adresse e-mail

- Pour les signalements d'incidents : incident-csirt-cc@cegedim.com
- Pour les demandes générales : contact-csirt-cc@cegedim.com

2.6 Autres moyens de communication

Aucun autre moyen de communication n'est accepté pour les signalements d'incidents.

2.7 Clé publique

La clé publique GPG du CSIRT cegedim.cloud est disponible à :
https://cegedim.cloud/wp-content/uploads/2025/10/public.asc
Elle est utilisée pour les communications sécurisées et la signature des documents.

2.8 Membres de l'équipe

Les membres du CSIRT cegedim.cloud ne sont pas listés publiquement, mais ils s'identifieront par leur nom complet lors des communications officielles liées à un incident.

2.9 Horaires d'ouverture

Le CSIRT cegedim.cloud opère du lundi au vendredi, de 9h00 à 18h00 (heure de Paris). En dehors de ces horaires, un service d'astreinte est disponible pour les incidents critiques signalés à : incident-csirt-cc@cegedim.com

2.10 Autres informations

Des informations générales sur le CSIRT cegedim.cloud sont disponibles à l'adresse : https://www.cegedim.cloud/csirt.

2.11 Point de contact pour les clients

Les clients doivent utiliser les canaux mentionnés dans les sections 2.4 et 2.5 pour contacter le CSIRT.

3 LA CHARTE DU CSIRT

3.1 Mission

Le CSIRT cegedim.cloud a pour mission de protéger les infrastructures informatiques de cegedim.cloud et de ses clients contre les incidents de sécurité, en assurant une réponse rapide et efficace aux menaces et en promouvant des mesures proactives pour réduire les risques.

3.2 Constituants

Le CSIRT cegedim.cloud dessert principalement :

- Les clients ayant souscrit un contrat de service avec cegedim.cloud.
- Les entités internes de cegedim.cloud utilisant ses services cloud.
- Les partenaires et fournisseurs directement connectés aux infrastructures de cegedim.cloud.

Remarque : Aucun support direct n'est fourni aux utilisateurs finaux.
Ces derniers doivent contacter leur administrateur système ou leur centre d'opérations de sécurité (SOC) pour assistance.

3.3 Parrainage et affiliation

Le CSIRT cegedim.cloud est une entité interne de cegedim.cloud, opérant sous l'autorité de la direction de cegedim.cloud
Le CSIRT collabore avec d'autres CSIRT nationaux et internationaux sur une base de besoin.

3.4 Autorité

Le CSIRT cegedim.cloud agit en tant que conseiller pour les équipes de sécurité locales de ses clients et partenaires.
Il n'a pas d'autorité directe sur les systèmes externes, mais peut émettre des recommandations opérationnelles pour résoudre les incidents.

4 LA POLITIQUE DU CSIRT

4.1 Types d'incidents et niveau de support

Le CSIRT cegedim.cloud gère tous les types d'incidents de sécurité affectant ses infrastructures ou celles de ses clients, incluant, mais sans s'y limiter :

- Code malveillant (malware).
- Tentatives d'intrusion ou intrusions confirmées.
- Attaques de déni de service (DoS/DDoS).
- Violations de contenu ou abus.
- Vulnérabilités des actifs.

Le niveau de support dépend de la gravité, du type d'incident, et des ressources disponibles. Une réponse initiale est généralement fournie dans un délai d'un jour ouvrable pour les incidents signalés pendant les heures d'ouverture.

4.2 Coopération, interaction et divulgation d'informations

Les informations relatives aux incidents, telles que les noms et les détails techniques, ne sont pas partagées sans le consentement explicite de toutes les parties prenantes concernées.

Sauf accord contraire, les informations fournies sont conservées de manière confidentielle. CSIRT cegedim.cloud ne transmettra jamais d'informations à des tiers, sauf obligation légale. Sous réserve de l'acceptation des parties affectées ou d'une autorisation légale, CSIRT cegedim.cloud privilégie le partage des tactiques, techniques et procédures dans le but de prévenir et de réagir à des incidents spécifiques.

Nos priorités premières sont de préserver :

- Le niveau de confidentialité attribué à l'information par son propriétaire. Nous utilisons le protocole « TLP » (tel que défini par FIRST : https://www.first.org/tlp/) pour définir la confidentialité des informations.

- La protection des informations personnelles.

Aucune information sensible ne sera transmise par CSIRT cegedim.cloud à une autre partie sans l'accord préalable du propriétaire de l'information. CSIRT cegedim.cloud traite et gère les informations dans des environnements physiques et techniques sécurisés, conformément à la réglementation française en vigueur relative à la protection des informations.

4.3 Communication et authentification

La méthode de communication privilégiée est le courrier électronique. Les communications sensibles doivent être chiffrées à l'aide de la clé GPG mentionnée dans la section 2.7.
Les signalements d'incidents doivent inclure des informations détaillées pour permettre une analyse efficace.

5 LES SERVICES DU CSIRT

Le CSIRT cegedim.cloud a pour mission de coordonner, soutenir et améliorer la réponse aux incidents de sécurité affectant les systèmes, services et données relevant de son périmètre.
Il agit en tant que point de contact central pour la détection, l'analyse, la mitigation et la résolution des incidents, en collaboration avec l'ensemble des parties prenantes internes et externes.

5.1 Coordination de la réponse aux incidents

Le CSIRT cegedim.cloud assure la coordination globale de la réponse aux incidents entre les différentes parties concernées, incluant :

- L'analyse technique et forensic des incidents.
- La coordination avec les fournisseurs de services Internet (ISP), les partenaires techniques, d'autres CSIRT/CERT, ainsi que les autorités compétentes si besoin.
- La formulation de recommandations pour la mitigation et la résolution des incidents.
- La facilitation de la communication et de la collaboration entre les différentes parties prenantes impliquées dans la gestion des incidents.

5.2 Réponse opérationnelle et assistance technique

Le CSIRT cegedim.cloud fournit un appui opérationnel dans la gestion des incidents, depuis leur détection jusqu'à leur résolution complète.
Les principales activités comprennent :

- Le triage et la qualification des incidents signalés afin d'en évaluer la gravité, l'impact et la priorité d'intervention.
- La coordination des équipes techniques et opérationnelles pour contenir et remédier aux incidents
- Le support sur site, pour les clients ayant souscrit un contrat spécifique, pour l'analyse et la résolution des incidents critiques.
- Le suivi post-incident, incluant l'analyse rétrospective et la documentation.

5.3 Résolution des incidents et amélioration continue

Le CSRIT :

- Fournit des conseils techniques et stratégiques pour éviter la récurrence des incidents
- Propose des mesures préventives et des contrôles compensatoires pour éviter la récurrence.

5.4 Activités proactives

Le CSIRT cegedim.cloud mène des actions proactives destinées à anticiper les menaces, à renforcer la posture de sécurité et à développer les compétences de ses clients. Ces activités incluent :

a. Surveillance et diffusion d'alertes

- Surveillance continue des menaces et vulnérabilités pouvant affecter les systèmes sous leur responsabilité.
- Diffusion d'alertes, bulletins de sécurité et recommandations pour renforcer la posture de sécurité.

b. Analyse et audit de sécurité

- Analyse de vulnérabilités : réalisation régulière de scans des systèmes accessibles publiquement afin d'identifier les vulnérabilités connues. Cela permet une application proactive des correctifs et une atténuation des risques.

- Audit de configuration portant sur :
    1. **Les environnements Active Directory :** ce service permet d'identifier les éventuelles mauvaises configurations ainsi que les vulnérabilités présentes dans l'environnement Active Directory.

    2. **Les environnements Cloud** : ce service analyse l'infrastructure Cloud du client afin de détecter les faiblesses en matière de sécurité et les problèmes de conformité.

c. Tests et exercices

- Tests d'intrusion \ Exercice de Red Teaming : Simulation d'attaques cybernétiques visant à identifier les vulnérabilités exploitables au sein des systèmes et des applications.
- Cette démarche permet d'évaluer l'efficacité des dispositifs de sécurité en place. Participation à des exercices

d. Formation et sensibilisation

- Organisation de sessions de formation, d'ateliers et de campagnes de sensibilisation visant à renforcer la culture de cybersécuritédu personnel et à accroître la vigilance face aux menaces potentielles.
- Mise en œuvre de formations et d'exercices pratiques destinées à développer les compétences et les capacités de réponse aux incidents des équipes de sécurité de ses clients.

Ces activités proactives permettent à nos clients d'identifier et de réduire les risques de sécurité avant qu'ils ne puissent être exploités par des attaquants, mais aussi de renforcer les compétences des collaborateurs, améliorant ainsi leur posture globale en matière de cybersécurité.

6 LA CLAUSE DE NON-RESPONSABILITE

Bien que le CSIRT cegedim.cloud s'efforce de fournir des services précis et efficaces, aucune garantie n'est offerte quant à l'exhaustivité ou à l'absence d'erreurs dans les recommandations fournies.
Les clients et partenaires sont responsables de la mise en œuvre des recommandations.