22-10-2025 16:52 (CEST)

Nicolas Malbec CEO FIDELILIUM

Certifié par yousign

FIDELILIUM

Libérer & sécuriser la vie numérique

RFC 2350 du CERT FIDELILIUM

Réf : 2025_08_RFC_2350

Contrôle du document			
	Nom	**Fonction**	**Date**
Rédaction			
Approbation	MALBEC	CEO	22/10/2025

Historique			
Date	**Version**	**Description**	**Rédacteur**

FIDELILIUM
Libérer & sécuriser la vie numérique

TLP : GREEN

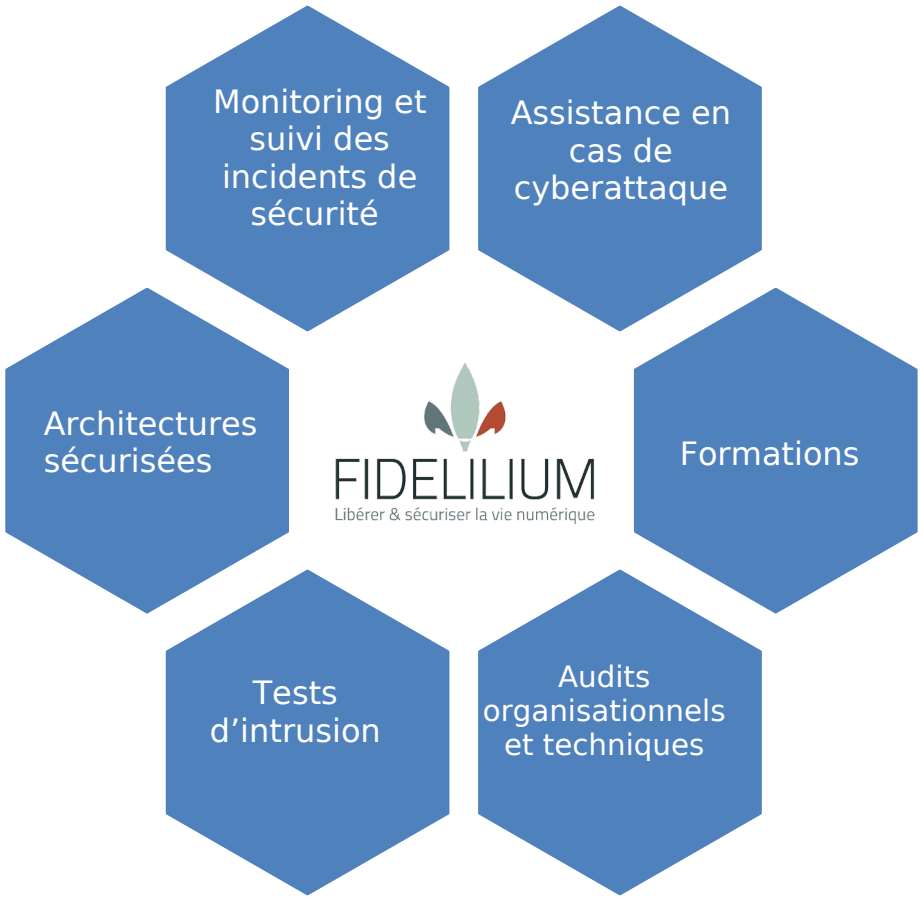
Table des matières

FIDELILIUM
Libérer & sécuriser la vie numérique

TLP : GREEN

À propos de FIDELILIUM

FIDELILIUM est une société française de cybersécurité basée à Versailles, engagée à libérer et sécuriser la vie numérique de ses clients.
FIDELILIUM propose un accompagnement complet, allant de la surveillance à la remédiation post-incident, en passant par la mise en conformité réglementaire et la formation.



FIDELILIUM
Libérer & sécuriser la vie numérique

TLP : GREEN

Le fondateur de FIDELILIUM, bénéficie du titre d'expert en sécurité des systèmes d'information de l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information).
Il cumule près de 30 ans d'expérience dans la défense des systèmes d'information.

Titre ESSI

L'entreprise est référencée sur la plateforme Cybermalveillance.gouv.fr
Ses clients sont les entreprises, les institutions et les particuliers.

FIDELILIUM est fier d'être Professionnel Associé de Défense Angels, le réseau de Business Angels dédié aux technologies stratégiques. Ce partenariat vise à renforcer la cybersécurité des startups innovantes dans des secteurs tels que la défense, l'IA, le quantique ou encore le new space.

Nicolas Malbec est le fondateur de FIDELILIUM. Il est expert en cybersécurité, et a eu une carrière dans la Marine nationale qui lui a permis de servir comme RSSI (CISO) de la Marine nationale et comme chargé de la planification des opérations au commandement de la cyberdéfense.
Il a crée un mastère spécialisé en cybersécurité à l'École Hexagone qui a obtenu le label SecNumEdu de l'ANSSI.

Son parcours professionnel, notamment au sein de la Marine, lui a permis d'acquérir une vision globale et de nouer de nombreux partenariats.
Il a également dû se confronter aux exigences des opérations militaires en tant que commandant de navire de combat.

1. À propos du document

Ce document contient une description du CERT FIDELILIUM conformément à la spécification RFC 2350. Il fournit des informations sur l'équipe, les services proposés ainsi que les moyens de contact.

1.1 Date de la dernière mise à jour

Version 1.0, éditée le 17 septembre 2025.

1.2 Liste de distribution pour les notifications

Les modifications de ce document seront partagées sur le site internet de FIDELILIUM (https://fidelilium.com/)

1.3 Emplacements où ce document peut être trouvé

La version actuelle de ce document est disponible sur le site web de FIDELILIUM.

1.4 Authentification de ce document

Ce document a été signé avec la clé PGP du CERT FIDELILIUM.
Vous trouverez la signature et notre clé PGP publique à l'adresse suivante : https://fidelilium.com/CERT_fidelilium

1.5 Identification du document

Titre : FIDELILIUM_RFC_2350
Référence : 202508_RFC2350
Date de mise à jour : 12 septembre 2025
Durée de validité : ce document est valide tant qu'il n'existe pas de version ultérieure.

2. Informations sur les moyens de contact

2.1 Nom de l'équipe

Nom : CERT FIDELILIUM

2.2 Adresse

FIDELILIUM, 25 rue du Maréchal Foch 78000, Versailles, France

2.3 Fuseau horaire

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

2.4 Numéro de téléphone

01 89 71 43 78

2.5 Numéro de fax

Non applicable

2.6 Autres moyens de télécommunication

cert@fidelilium.com

2.7 Adresse électronique

contact@fidelilium.com

2.8 Clés publiques et informations sur le chiffrement

Informations concernant la clé PGP utilisée pour les échanges avec le CERT FIDELILIUM :

- ID utilisateur : CERT FIDELILIUM (cert@fidelilium.com)
- ID de clef : 0x6158540A
- Empreinte : 6158540a1928446bcdc1b9584c0fc84611a96e74

Vous trouverez la signature et notre clé PGP publique à l'adresse suivante : htpps://fidelilium.com/CERT_fidelilium

2.9 Membres de l'équipe

L'équipe CERT FIDELILIUM est composée d'experts en sécurité informatique, dont l'identité n'est pas divulguée publiquement. L'identité de ces membres de l'équipe pourrait être révélée au cas par cas, en respectant les restrictions liées au besoin d'en connaître.

2.10 Autres informations

Des informations complémentaires sont disponibles sur le site internet :
https://fidelilium.com

2.11 Point de contact client

Le CERT FIDELILIUM est joignable par téléphone, ou par e-mail.
L'e-mail est le moyen de contact privilégié.

En cas d'urgence, veuillez utiliser le tag [URGENT] dans le champ objet de votre e-mail.

En dehors des heures d'ouverture, il est possible de s'appuyer sur les portails institutionnels pour signaler un incident :
www.cert.ssi.gouv.fr/contact/
www.cybermalveillance.gouv.fr/diagnostic

3. Charte

3.1 Ordre de mission

L'objectif du CERT FIDELILIUM est d'apporter une assistance pour répondre à toute entreprise, organisation, ou personne physique, confrontée à un incident de cybersécurité. Les missions du CERT FIDELILIUM portent sur la réponse à incidents et la remédiation. Cette équipe répond également à des enjeux de prévention, en appuyant les organisations souhaitant améliorer leur niveau de maturité en cybersécurité.

Ses missions se déclinent à travers les activités suivantes :

- Surveillance & veille : assurer une veille proactive sur les menaces, vulnérabilités et attaques.
- Gestion des incidents : recevoir, analyser, qualifier, coordonner et résoudre les incidents de sécurité.
- Communication : diffuser des alertes, recommandations et bonnes pratiques aux bénéficiaires.
- Prévention : proposer des actions de durcissement et d'amélioration de la posture de sécurité.
- Coopération : participer à des échanges d'information et de bonnes pratiques avec d'autres CERT.
- Sensibilisation et formations : le CERT FIDELILIUM dispense des formations à la demande, et assure systématiquement des actions de sensibilisation à la cybersécurité.

3.2 Bénéficiaires

- Clients de FIDELILIUM (PME, ETI, Établissements publics, associations)
- Utilisateurs, réseaux et systèmes affiliés aux services de FIDELILIUM

3.3 Affiliation

Le CERT FIDELILIUM est opéré par les équipes de cybersécurité de la société FIDELILIUM.

3.4 Autorité

Le CERT FIDELILIUM opère sous l'autorité de la direction de la société FIDELILIUM.

4. Politique

4.1 Types d'incidents et niveau de soutien

Le CERT FIDELILIUM intervient sur une grande variété d'incidents de sécurité. Le soutien apporté varie en fonction du type et de la gravité de l'incident. L'accompagnement s'opère tout au long du processus, depuis la prise de contact jusqu'à la clôture de l'incident.

Les principaux services rendus par le CERT FIDELILIUM sont :

- Réception des signalements d'incidents 24h/24, 7j/7
- Analyse des incidents
- Réponse aux incidents
- Remédiation
- Analyse des vulnérabilités et des logiciels malveillants
- Réponse aux vulnérabilités
- Analyse et partage des renseignements sur les menaces.

4.2 Collaboration, interaction et partage d'informations

Les informations concernant un incident, telles que le nom de l'entité concernée et les détails techniques, ne sont publiées qu'avec l'accord préalable de la partie mentionnée.
Toutefois, les informations reçues par le CERT FIDELILIUM peuvent être partagées en interne avec divers membres de la société.
Le CERT FIDELILIUM souligne l'importance de la coordination et du partage d'informations entre les CERT, les SOC et les entités similaires. Dans ce cadre, le CERT FIDELILIUM peut être amené à communiquer des informations, sous réserve d'accord préalable, à ces fournisseurs de services de cybersécurité.

4.3 Communication et authentification

Il est recommandé que les courriels adressés au CERT FIDELILIUM soient signés à l'aide de PGP. Pour les courriels contenant des informations sensibles, le chiffrement et la signature PGP sont impératifs.

5. Services proposés

5.1 Réponse aux incidents

Le CERT FIDELILIUM fournit à ses clients des services de réponse aux incidents de cybersécurité depuis la prise de contact jusqu'à la clôture de l'incident.
Le CERT FIDELILIUM intervient sur tout types d'incidents, impliquant des technologies de l'information et de la communication.
Il propose les services détaillés aux points ci-dessous.

5.1.1 Classement des incidents

- Réception du signalement et prise de contact avec le déclarant
- Collecte des informations relatives à l'incident, suivi de la confirmation ou de l'évaluation de sa nature
- Évaluation de la gravité de l'incident, de son impact ainsi que de son périmètre
- Classification de l'incident selon sa typologie.

5.1.2 Coordination des incidents

- Catégorisation des informations liées à l'incident (fichiers journaux, informations de contact, etc.)
- Assistance, si nécessaire, dans la transmission des signalements aux autorités compétentes de l'État, en fonction de la nature de l'incident. Cela peut inclure :
    - L'ANSSI, en cas d'incident majeur de cybersécurité susceptible d'avoir un impact sur d'autres secteurs
    - La CNIL, en cas de violation de données à caractère personnel

5.1.2 Résolution des incidents

- Proposition de mesures immédiates, incluant des actions d'urgence visant à limiter l'impact de l'incident, ainsi que des actions facilitant les investigations et la gestion de l'incident.
- Analyse des systèmes compromis
- Remédiation
- Récupération et reconstruction

5.2 Mesures proactives de cybersécurité

- Action de sensibilisation auprès des bénéficiaires
- Actualités sur le site internet

5.3 Audit et évaluation de la sécurité

Le CERT FIDELILIUM propose des audits de cybersécurité. Ce service vise à diagnostiquer l'exposition d'un système d'information sur Internet et à en évaluer les risques en matière de cybersécurité.

Dans le cadre de cet audit, les actions suivantes sont menées :

- Cartographie des systèmes exposés sur Internet (technologies et serveurs utilisés, configuration, état des mises à jour, etc.) afin d'identifier la surface d'attaque
- Recherche de fuites de données et évaluation de leur criticité
- Détection de vulnérabilités potentielles : équipements non référencés mauvaises configurations, identifiants faibles ou par défaut, vulnérabilités Web, et analyse de leur exploitabilité.

5.4 Formulaires de signalement des incidents

Le CERT FIDELILIUM ne dispose pas d'un formulaire spécifique pour les réponses aux incidents, mais il est utile de fournir les informations suivantes lors de la prise de contact :

- Coordonnées de la personne à contacter (courriel, numéro de téléphone)
- Chronologie de l'incident. Précisez la date et l'heure auxquelles l'incident a commencé, ainsi que l'heure et la date auxquelles il a été détecté.
- Description de l'incident
- Impacts de l'incident.
- Mesures prises : listez les actions réalisées avant l’intervention de nos équipes.

6. Clause de non-responsabilité

Bien que le CERT FIDELILIUM s'engage à assurer l'exactitude et la diligence dans la création d'informations, de notifications et d'alertes, il n'assume aucune responsabilité pour toute erreur, omission ou dommage résultant de l'utilisation des informations fournies.