TLP:WHITE

CERT-METSYS

RFC-2350

Dernière modification le : 20/03/2023

Version : 1.0

METSYS

TABLE DES MATIERES

TLP:WHITE

1. INFORMATION

Le présent document présente une description du CERT-METSYS en accord avec les spécifications définies dans le standard RFC2350[1]. Ce dernier expose une description succincte du CERT-METSYS. Il est donc décrit dans ce document les services fournit par le CERT-METSYS et les responsabilités que ce dernier prend.

1.1. VERSION DU DOCUMENT

Version 1.0, publié le 20/03/2023

1.2. LISTE DE DISTRIBUTION

Le CERT-METSYS ne dispose d'aucune liste de distribution. Cependant, l'adresse cert@metsys.fr peut être considérée comme tel.

Le présent document est tenu à jour à l'endroit indiqué au point 1.3.

Si vous avez des questions concernant les mises à jour du présent document, veuillez contacter l'adresse électronique du CERT-METSYS indiqué au point 2.8.

1.3. LIEU DE PUBLICATION DU DOCUMENT

La version actuelle de ce document peut être consultée sur la page web du cert METSYS :

- https://www.metsys.fr/expertises/managed-services/cert/

Il convient de contrôler que vous disposez de la version la plus récente.

1.4. AUTHENTICITE DU DOCUMENT

Le présent document a été signé avec la clé PGP du CERT-METSYS. Cette signature est disponible sur le site web du CERT-METSYS :

- https://www.metsys.fr/expertises/managed-services/cert/

Référez-vous à la section 2.8 pour disposer de notre clé publique.

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

2. CONTACTS

2.1 NOM

CERT-METSYS

2.2 ADRESSE

CERT-METSYS

METSYS - Ile-de-France - Boulogne-Billancourt

121 Rue d'Aguesseau

92100 Boulogne-Billancourt

France

2.3 FUSEAU HORAIRE

CET/CEST UTC+1

2.4 NUMERO DE TELEPHONES

- +33 1 84 19 07 27

2.5 NUMERO DE FAX

Non disponible.

2.6 AUTRE CANAL DE COMMUNICATION

Non disponible.

2.7 ADRESSE DE COURRIER ELECTRONIQUE

Si vous voulez nous contacter à propos d'une information sur un incident de sécurité ou d'une menace cyber ciblée, Envoyez-nous un message à l'adresse suivante à l'adresse suivante : cert@metsys.fr

2.8 CLE PUBLIQUE ET INFORMATIONS DE CHIFFREMENT

Le CERT-METSYS utilise le protocole PGP pour assurer la sécurité de ces communications :

- User ID: CERT-METSYS <cert[at]metsys.fr>
- Key ID: 0xC325800B
- Fingerprint: 8CDC80D4C6A1FE4331835A2C66532197C325800B

La clé publique que nous utilisons est disponible sur :

https://www.metsys.fr/wp-content/uploads/2023/01/CERT-METSYS_public.asc

Il est imposé par le CERT-METSYS d'utiliser la présente clé à chaque fois que des informations doivent être envoyées au CERT-METSYS de manière sécurisée.

2.9 COMPOSITION DE L'EQUIPE

- Le directeur du CERT-METSYS est Nicolas Verdier.

L'équipe du CERT-METSYS est composée d'ingénieurs en cybersécurité et d'analystes CERT-METSYS. Aucune information nominative relative aux membres du CERT-METSYS n'est diffusée dans le présent document pour des raisons de sécurité et de confidentialité. Une dérogation à cette pratique pourra être faite selon le besoin d'en connaître.

2.10 AUTRES INFORMATIONS

L'ensemble des informations que vous pouvez trouver publiquement sur le CERT-METSYS et Metsys sont indiqué sur les pages suivantes :

https://www.metsys.fr/

https://www.metsys.fr/expertises/managed-services/cert/

2.11 POINTS DE CONTACT AVEC LES CLIENTS

Afin de contacter le CERT-METSYS, il est préférable d'utiliser l'adresse suivante :

cert@metsys.fr

Veuillez utiliser notre clé cryptographique pour assurer l'intégrité et la confidentialité. En cas d'urgence, veuillez utiliser l'étiquette [URGENT] dans le champ sujet de votre e-mail.

Les heures d'ouverture de CERT-METSYS de 9h à 18h du lundi au vendredi excepté les jours fériés français.

En cas d'extrême nécessité, le CERT-METSYS assure une Astreinte 24/7 sur le numéro suivant :

- *+33 1 84 19 07 27*

3. CHARTE

3.1. MISSIONS

Notre mission principale en tant que CERT-METSYS, est de mettre en place une coordination et la réponse aux incidents de cybersécurité liées à des attaques criminelles pour l'organisme de Metsys et des clients du CERT-METSYS.

Ainsi, la mission du CERT-METSYS est d'aider sa circonscription à se protéger contre des attaques intentionnelles et opportunistes qui pourraient entraver l'intégrité de leurs actifs informatiques et nuire à leurs intérêts. Dans cet objectif, le CERT-METSYS est en charge des activités de Digital Forensics and Incident Response (DFIR).

3.2. CIRCONSCRIPTION

Le CERT-METSYS prend en charge la réponse aux incidents et fournit un suivi pour l'ensemble de ces clients et pour le système d'informations de Metsys.

De plus, le CERT-METSYS fournit selon le contrat de support Service Level Agreement souscrit par ces clients divers activités de réponse aux incidents, et ce, en tant que CERT commercial.

Les clients que le CERT-METSYS peut actuellement prendre en charge sont répartis sur le territoire français. Les opérations menées sur le territoire national par le CERT-METSYS concerne les :

- Les organisations du secteur privé ;
- Les organisations du secteur public ;
- Les organisations commerciales.

3.3. PARRAINAGE

Le CERT-METSYS est soutenu par METSYS S.A.

Le CERT-METSYS entretient de nombreux contacts avec les différents CERT nationaux via sa coopération avec l'InterCERT France.

3.4. AUTORITE

Le CERT-METSYS opère dans le cadre de contrats validés et signés par ses clients.

L'équipe n'a aucune autorité pour demander la réalisation d'actions sur les systèmes et réseaux sur les périmètres impactés.

Le CERT-METSYS a pour principal prérequis de travailler en coopération active avec les administrateurs système et réseau, ainsi qu'avec les utilisateurs de ses clients.

4. STRATEGIE

4.1. TYPES D'INCIDENTS ET NIVEAU DE SUPPORT

La cellule CSIRT de Metsys intervient dans le cadre de missions de réponse à incidents et d'investigation numérique sur des périmètres complexes. Metsys se positionne sur ces périmètres en complémentarité directe de son offre SOC qui traite pour sa part de la surveillance des événements de sécurité, ainsi que de la résolution des incidents de sécurité de niveaux 1 et 2.

L'équipe CSIRT intervient pour sa part lorsque l'impact de l'incident nécessite une intervention rapide et proportionnelle, généralement donnant lieu à la mise en place d'une cellule de crise.

Lorsque les incidents arrivent, ils sont classés par ordre de priorité en fonction de leur gravité apparente et de leur étendue.

COOPERATION, ECHANGES, ET CONFIDENTIALITE DE L'INFORMATION

Le CERT-METSYS échangera toutes les informations qu'ils jugent nécessaires avec les autres CERT/CSIRT susceptibles d'être concernés selon le besoin d'en connaître.

Les informations communiquées, sont opérées dans le cadre légal français.

En effet, le CERT-METSYS participe activement à la coopération des CERT nationaux, l'InterCERT France. Dans ce cadre, il participe à son activité et notamment via le partage d'informations.

Toutes les informations confidentielles sont traitées par le CERT-METSYS, indépendamment de leur priorité. Toutes les données sensibles (données personnelles, configurations de système, vulnérabilités connues avec leurs emplacements) sont stockées dans un environnement sécurisé, et sont chiffrées.

Le CERT-METSYS respecte le protocole TLP2.0 (https://www.first.org/tlp/). Les informations sont donc systématiquement partagées avec les étiquettes ***AMBRE, VERT, GREEN AMBRE+STRICT ou RED***, ces étiquettes seront appliquées de manière adaptée au contexte.

4.2. COMMUNICATION

Afin de transmettre des informations sensibles, le CERT-METSYS utilise comme dit dans la précédente section, le protocole TLP2.0.

De plus, le CERT-METSYS respecte dans ces communications le cadre légal imposé par la législation Française.

La méthode de communication privilégiée par le CERT-METSYS est le courrier électronique. Pour l'échange d'informations sensibles ainsi que pour les communications signées, le CERT-METSYS utilise le protocole PGP (chiffrement et/ou signature chiffrée des messages).

Toutes les communications sensibles au CERT-METSYS doivent être chiffrées avec notre clé publique comme détaillée dans la section *2.8 Clé publique et informations de chiffrement.*

En cas d'urgence absolue, c'est-à-dire sans avoir la possibilité de communiquer par d'autres moyens, une communication téléphonique sera acceptée. Pour ce type de communication, le CERT-METSYS préfère l'utilisation de solution chiffrée, mais considère qu'une communication téléphonique non chiffrée restera suffisante.

5. SERVICES

5.1. REPONSE A L'INCIDENT

Le CERT-Metsys propose les services de sécurité informatique suivants :

- Détection des incident ;
- Analyse de l'incident ;
- Reconstruction chronologique ;
- Assistance à la remédiation ;
- Coordination ;
- Piloter et mener les actions de communication à destination des équipes techniques et décisionnelles.

5.1.1 Triage des incidents

Le CERT-METSYS mène avant tout traitement d'un incident une évaluation de la gravité de ce dernier. Il s'agit ici d'un premier niveau de réponse, que nous considérons comme la prise en compte de l'incident. Dans ce niveau, il est question de clore les faux positifs remontés ;

Si le niveau 1 estime qu'il est nécessaire que l'incident requière plusieurs opérateurs ou une investigation plus approfondie, l'incident déclenche le deuxième niveau de réponse à incident;

Si l'incident relève d'une crise cyber, un troisième niveau de réponse est appliqué et activera la cellule de crise du CERT-METSYS en coordination avec le(s) client(s) ciblé(s).

5.1.2 Coordination des incidents

Afin d'apporter une coordination dans la réponse aux incidents, il est défini par le CERT-METSYS les points suivants :

- Une politique de confidentialité des données sera appliquée à l'ensemble des informations que le CERT-METSYS traitera. Elles seront donc classifiées selon leur type et leur implication (fichiers de log, contacts, informations, etc.)

- Les différentes parties impliquées et concernées seront notifiées sur la base du besoin dans d'en connaître, conformément à la politique de divulgation des données.

5.1.3 Résolution des incidents

Le CERT-METSYS se donne comme objectif dans sa mission de réponse à incident :

- D'analyser les systèmes compromis des clients de sa circonscription ;
- Si cette analyse révèle des comportements malveillants d'un acteur sur le SI, il sera alors d'ordre pour le CERT-METSYS de procéder à l'élimination de la cause du dit incident de sécurité (vulnérabilité exploitée), et de ses effets de bord.

5.2. ACTIVITES PROACTIVES

Le CERT-METSYS assure une activité de réponse aux incidents de sécurité, mais aussi de détection pour ces clients grâce à son SOC. Cela passe par l'élimination des cyberattaques, des perturbations, des vulnérabilités en matière de sécurité, des logiciels malveillants, et fournit des recommandations pour s'attaquer aux problématiques au sein de son système d'informations.

De plus le CERT-METSYS réalise une veille sur les menaces, les vulnérabilités, les scénarios d'attaques et les mesures de sécurité nécessaires pour protéger les systèmes d'information de ces clients. Les informations liées à la veille pourront être échangées avec les autres CERT si cela s'avère utile, sur le principe du besoin d'en connaître.

Par conséquent, le SOC-Metsys propose et réalise les activités proactives suivantes en coordination avec le CERT-METSYS :

- Prévention des incident ;
- Détection des incident ;

Le CERT-METSYS quant à lui propose les activités proactives suivantes :

- Réaction ;
- Conseil en vue d'une mise en conformité.

6. FORMULAIRE DE DÉCLARATION D'INCIDENT

Les clients existant du CERT-METSYS dispose d'une plateforme dédiée à la déclaration d'incident.

Pour un contact avec des entités extérieures à sa clientèle, le CERT-METSYS ne possède pas de formulaire type pour la déclaration d'un incident de sécurité. Ainsi, nous vous prions de nous contacter par mail, à l'adresse cert@metsys.fr, pour nous signaler un incident de sécurité.

Pour toute urgence ou crise cyber, veuillez nous fournir les informations suivantes :

- Coordonnées et informations sur l'organisation (nom du contact, nom de l'organisation et adresse) ;
- Adresse électronique, numéro de téléphone ;
- Adresse(s) IP, FQDN(s), et tout autre élément technique pertinent avec observations associées ;
- Le cas échéant, résultats de l'analyse ou extrait du journal montrant le problème ;
- Au cas où vous souhaiteriez transférer des courriels, veuillez inclure tous les en-têtes de courriel, le corps du message et toutes les pièces jointes, si possible et dans la mesure où les règlements et la législation en vigueur vous y autorisent.

7. AVERTISSEMENTS

Le CERT-METSYS ne pourra aucunement être tenu responsable en cas d'erreur, ou d'omission de certaines informations ou pour tout préjudice impliqué en raison des informations contenues dans le présent document.

Nous vous prions de nous faire part de toutes erreurs ou oublis liés à ce document, afin que nous puissions améliorer ce dernier.