

Atos a usage interne

Cyber Threat Intelligence Requirement

auteur(s) : Ledoux Alexis

n° de document : CTI-TPLAMBER-IR

version : 1.0

statut : Draft

source : Atos

date du document : 21 avril 2021­

­

­

nombre de pages : 7

© Copyright 2021, Atos S.E. Tous droits réservés. Toute reproduction en tout ou partie de ce document est interdite sauf autorisation préalable expresse et écrite de l’auteur. Pour toute question ou remarque se rapportant à ce document, veuillez contacter Atos, 0650926231.

­­­Table des Matières

[1 Introduction 4](#_Toc72921847)

[2 Demandeur 5](#_Toc72921848)

[3 Traitement de la demande 7](#_Toc72921849)

Liste des modifications

| version | Date | Description | Auteur(s) |
| --- | --- | --- | --- |
| 1.0 | 25/05/2021 | Création du document | Alexis Ledoux |
|  |  |  |  |
|  |  |  |  |

­­­­

# Introduction

Cette fiche permet de demander un nouveau besoin ou pour préciser ce qu’est un besoin. Chaque renseignement demandé est à renseigner dans la colonne de droite. Des informations sont disponibles en dessous de la zone de remplissage. Si certains points ne sont pas pertinents pour ce besoin, il n’est pas nécessaire de le remplir.

La partie 3. Traitement de la demande n’est pas à compléter avant l’envoi initial et sera rempli après la réception.

# Demandeur

| Informations | |
| --- | --- |
| NOM Prénom | LEDOUX Alexis |
| Entité | SOC |
| Date de la demande | 2021-05-28 |
| Degré de priorité | normal |

*Informations :*

* *Degré de priorité*: Préciser si le degré de priorité est urgent, normal ou faible

| Généralités | |
| --- | --- |
| Type de besoin | IR |
| Description du Besoin | Enrichir les logs sur l'outil de sécurité qui les envoie en se basant sur la forme du log son contenu et l'IP source qui émet le logs autrement dit la metadonnée device.ip, car la seule metadonnée actuelle qui peut nous renseigner est device.type et ce n’est pas clair. |
| Sous-besoins/sous-étapes |  |
| Format de livraison | Enrichissement sur RSA |
| Date de livraison |  |
| Fréquence du Besoin |  |

*Informations :*

* *Type de Besoin*: Préciser si le besoin est un IR (besoin continu dans le temps) ou PIR (ponctuel, limité dans le temps)
* *Description du Besoin*: Décrire le besoin ainsi que son contexte
* *Sous-besoins/sous-étapes* : Si applicable, renseigner toutes les étapes nécessaires pour satisfaire cette demande
* *Date de livraison*: Si applicable, préciser la date pour laquelle ce besoin doit être satisfait
* *Fréquence du Besoin*: Si applicable, indiquer la fréquence de répétition de ce besoin
* *Format de livraison*: Si applicable, Préciser le format dans laquelle le besoin doit être réalisé (fichier texte, rapport, …)

| Impacts | |
| --- | --- |
| Adaptations/changements du workflow prévues | Nouvelle métadonnée pour l’analyse |
| Résultat prévus, prévisions sur les performances | Gain de temps lors de l’analyse |

*Informations :*

* *Adaptations/changements du workflow prévues*: Citer tous les changements fonctionnels prévus liés à cette demande
* *Résultat prévus, prévisions sur les performances*: Citer tous les résultats et impacts de ce besoin

# Traitement de la demande

Cette partie sera complétée après la réception de ce document.

| Informations | |
| --- | --- |
| NOM Prénom réception |  |
| Entité réception |  |
| Date de réception de la demande |  |
| Date de traitement |  |
| Validation |  |

*Informations :*

* *Validation*: Préciser si la demande est acceptée ou refusée