AMOSSYS

Cible de sécurité CSPN

Logiciel Single-tenant MIP NPM en tant que service (SaaS) - version 7.28.0, en hébergement Cloud non privé, sur socle IaaS

Catégorie « Administration et supervision de la sécurité »

Référence : CSPN-ST-MIP-2.09

Date : le 26/04/2023

Code interne : MAL003

Siège : Immeuble Le Ouessant • Bâtiment B • 11 rue Maurice Fabre • 35000 Rennes • France • **www.amossys.fr**
SIRET : 493 348 890 00051 • **NAF** : 6202 A • RCS Rennes B 493 348 890 • SAS au capital de 38.000 Euros

FICHE D'EVOLUTIONS

Révision	Date	Description	Rédacteur(s)
0.01	20/04/2021	Création du document	M. MOREAU
0.02	18/05/2021	Mise à jour du document suite au premier atelier	M. MOREAU
0.03	20/05/2021	Mise à jour du document suite au deuxième atelier	M. MOREAU
1.00	17/06/2021	Version finale	M. MOREAU
1.01	02/02/2022	Mise à jour au démarrage de l'évaluation	M. VOGT
2.02	12/10/2022	Mise à jour au démarrage de la réévaluation	M.CIMA
2.03	18/10/2022	Prise en compte du mode Cloud	M.CIMA
2.04	25/10/2022	Ajout d'hypothèses supplémentaires	M.CIMA
2.05	03/11/2022	Prises en compte des derniers commentaires CORS Finalisation	A.BRU M.CIMA
2.06	20/12/2022	Prise en compte des retours de l'ANSSI	J. CASTEL M.CIMA
2.07	05/01/2023	Prise en compte des retours de l'ANSSI	J. CASTEL M. CIMA
2.08	26/01/2023	Mise à jour version du produit et dénomination	M.CIMA

2.09	25/04/2023	Prise en compte des retours de l'ANSSI	Q. Duchaussoy

Ce document est validé par Maltem Insight Performance

SOMMAIRE

1.INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation, selon le schéma CSPN[1] promu par l'ANSSI[2], du produit «MIP NPM» développé par la société **Maltem Insight Performance**.

La TOE[3] considérée est le produit MIP NPM en logiciel single -tenant en que service (SaaS) version 7.28.0, en hébergement Cloud non privé sur socle IaaS. Ce document est soumis au contrôle technique et qualité d'**AMOSSYS** ainsi qu'à la validation de **Maltem Insight Performance**. Les mises à jour de ce document sont effectuées par l'équipe projet d'**AMOSSYS**.

1.2. IDENTIFICATION DU PRODUIT

Éditeur	**Maltem Insight Performance** 45 Allée Théodore Monod, 64210 Bidart
Lien vers l'organisation	https://www.insight-performance.com
Nom commercial du produit	Maltem Insight Performance Network Performance Monitoring (MIP NPM)
Numéro de la version évaluée	7.28.0
Catégorie du produit	Administration et supervision de la sécurité

1.3. REFERENCES

Pour l'établissement de la présente cible de sécurité, les documents suivants ont été consultés par le rédacteur :

- [MIP]Maltem Insight Performance-FR.pdf
- [MIP] Initial Training-EN.pdf
- [Measures] PARQ M21.1-Complement to Cisco Network Instrumentation EN.pdf
- [Operations] PARQ O-01 Operation&Updates EN.pdf
- [Operations] PARQ O-02 Backup_Standard & Failover options EN.pdf
- [Operations] PARQ O-03 Requests management EN.pdf
- [Operations] PARQ O-04 Governance_Standard EN.pdf
- [Operations] PARQ O-07 SLA EN.pdf
- [Operations] PARQ O-09 Measurement Architecture Security EN.pdf

[1] Certification de Sécurité de Premier Niveau
[2] Agence Nationale de la Sécurité des Systèmes d'Information
[3] *Target Of Evaluation*

-

1.4. GLOSSAIRE

Acronymes	Définitions
BI	*Business Intelligence*
IT	*Information Technology*
KPI	*Key Performance Indicator*
MIP	*Maltem Insight Performance*
NPM	*Network Performance Monitoring*
SI	Système d'Information
SLA	*Service-Level Agreement*
TOE	*Target of Evaluation*

Tableau 1 - Glossaire

2. DESCRIPTION DU PRODUIT

2.1. DESCRIPTION GENERALE

La solution MIP NPM fournit un monitoring avancé des réseaux, des applications et de l'expérience utilisateur sur les SI. Ce monitoring est effectué grâce à des agents dans le cloud, dans les data centers privés, ou sur sites. Cette solution permet aux décideurs IT d'accéder à une vue globale de la capacité et des usages des infrastructures, d'assurer le SLA et de diminuer la durée des pannes informatiques.

L'instrumentation de la performance IT repose sur trois métriques :

- les performances & SLA (Operation/Monitor) ;
- la charge des ressources sensibles (Query) ;
- le trafic aux points clés (Probe).

Les mesures de ces indicateurs sont prises à fréquence variable (dépendant de la métrique), et sont stockées en base de données, sans perte de précision, pour une durée d'un an. Plus précisément, trois bases de données peuplent le portail :

- une base de données de configuration, contenant les coordonnées techniques (adresses IP…) des agents de mesures et des cibles de mesures, les comptes utilisateurs ;
- une base de données contenant les données de mesure (performance, charge, utilisation du portail…) ;
- une base de données contenant les données de trafic.

La suppression de ces données est à la discrétion de Maltem. Un datamart peut également être déployé pour héberger les rapports BI. Chaque type de mesure dispose de différents paramètres ou types de résultats (par exemple : pour un test de chargement d'URL, le nombre de requêtes, le temps de résolution DNS).

Maltem fournit également un service de Smart KPI, produisant une valeur statistique ou une valeur d'état sur un ensemble de mesures pour un même type de mesure.

Il est également possible de définir des périodes de maintenance :

- unitaires : pour une période indéterminée ;
- récurrentes : programmées sur des dates fixes ;

ainsi que des périodes d'analyse, afin de définir des créneaux où la continuité des services est critique (ou, à l'inverse, non nécessaire).

2.2. PRINCIPE DE FONCTIONNEMENT

Pour le monitoring de l'infrastructure, le portail se connecte préalablement au réseau de l'entreprise bénéficiaire par un lien VPN. Il envoie ensuite des requêtes SNMPv3 vers les routeurs et les agents de mesure réseau mis en place.

La solution est automatisable à l'aide de scripts personnalisés.

Il existe deux modes de déploiement :

- On premise : la solution est déployée sur l'infrastructure du client sur des machines virtuelles ou des machines physiques. Le client assure le maintien de celles-ci ;
- Cloud ; la solution est déployée sur notre hébergeur cloud et est composée d'un portail et d'un firewall.

Une fois la TOE déployée, les utilisateurs de la TOE peuvent se connecter via HTTPS au serveur Web mis en place pour paramétrer et visualiser la supervision par la TOE du réseau entreprise bénéficiaire.

2.3. DESCRIPTION DES DEPENDANCES

La TOE repose sur 2 composants externes :

- Des agents (routeur) snmp V3 permettant de mesurer la performance vers les équipements à interroger ;
- un environnement IPSec permettant d'acheminer les flux de manière chiffrée entre l'environnement où se trouve la TOE et le réseau client contenant les agents SNMP ; le tunnel côté TOE est monté par une solution OPNsense. Le tunnel côté client exploite les équipements du client.

D'autre part, la TOE fonctionne dans un environnement conteneurisé et utilise Docker Swarm.

2.4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

2.4.1. Matériel compatible ou dédié

Les agents réseau doivent être des agents SNMP supportant SNMPv3. Il peut s'agir d'agent activé sur des équipements réseau, ou sur des systèmes d'exploitation Linux ou Windows. La solution se déploie en *single-tenant* sur un *cloud* non privé.

2.4.2. Système d'exploitation retenu

La TOE et son environnement Docker Swarm sera installé sur le système d'exploitation Debian 11. Le portail de mesure quant à lui sera hébergé par Amossys.

2.5. PERIMETRE DE L'EVALUATION

2.5.1. Périmètre

L'évaluation porte sur le portail MIP NPM en version 7.28.0 et l'environnement fonctionnant sous Docker Swarm pour le mettre en œuvre, ainsi que les communications utilisateur et métier. Les communications métiers concernent les flux permettant la collecte auprès des agents de mesure réseau. Les agents de mesure réseau - qui ne sont pas fournis avec la TOE - sont hors périmètre

2.5.2. Plateforme d'évaluation

La figure suivante représente la plateforme d'évaluation.

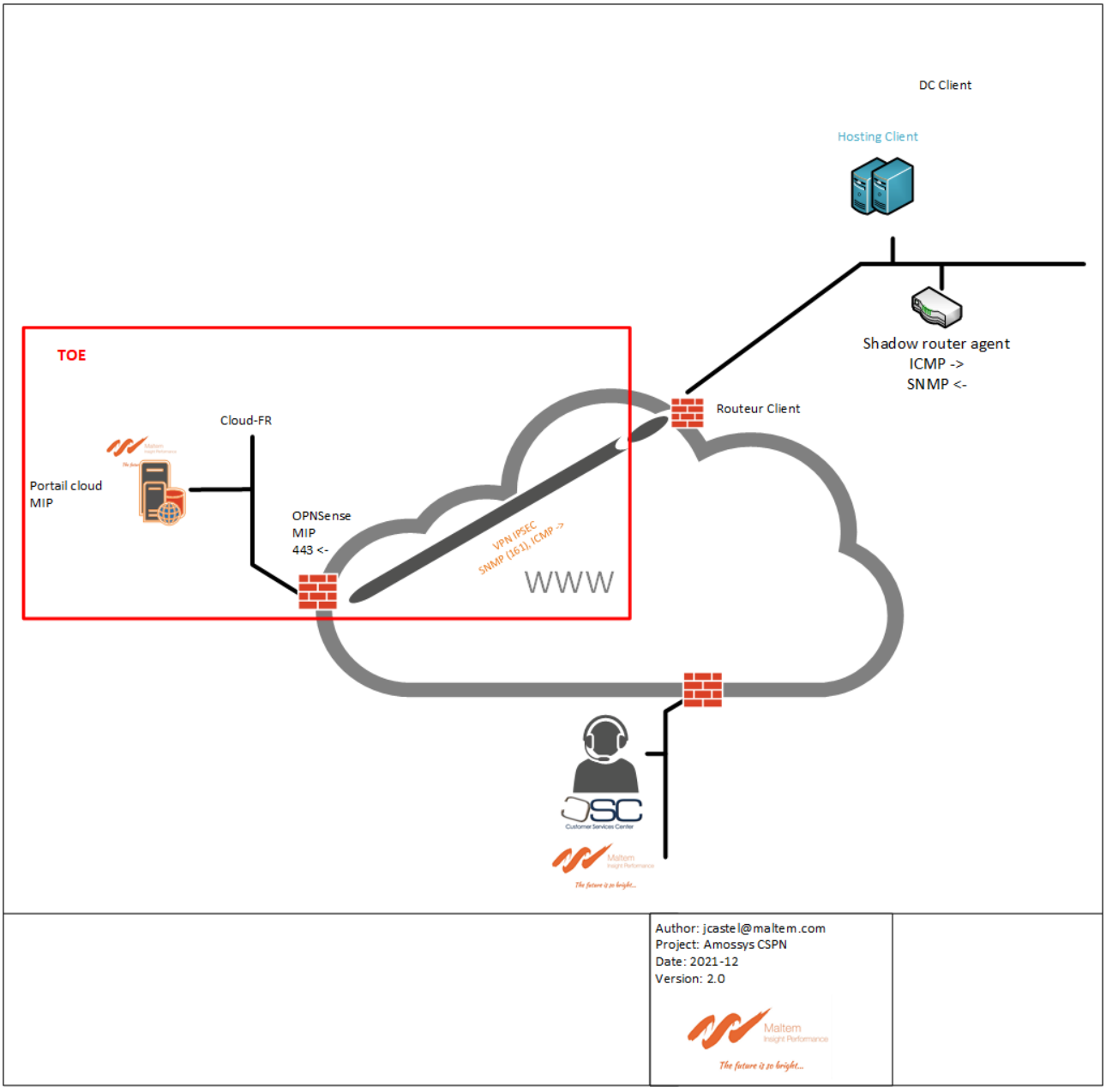

Figure 1 – Schéma de déploiement cloud commercialisé par Maltem

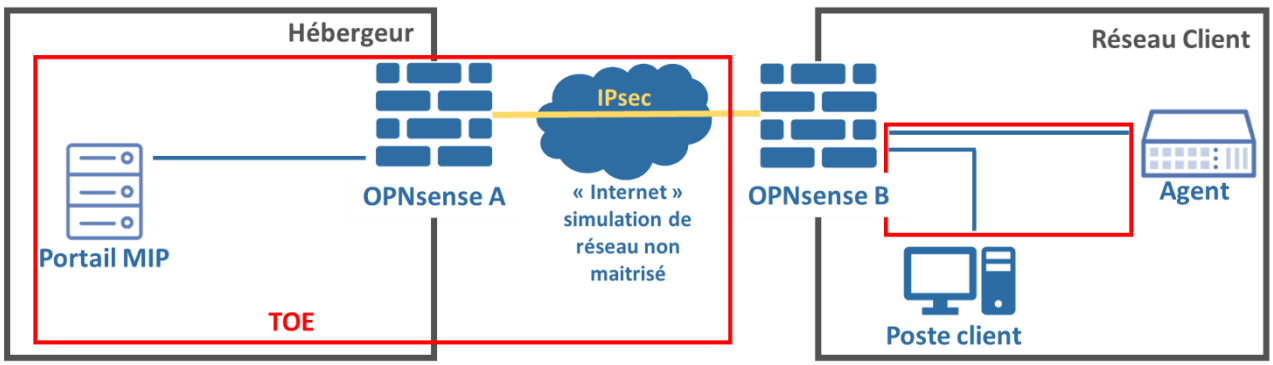

Figure 2 Plateforme d'évaluation (schéma proposé par AMOSSYS)

3. PROBLEMATIQUE DE SECURITE

3.1. DESCRIPTION DES UTILISATEURS TYPIQUES

Par définition, les utilisateurs concernent les personnes et services applicatifs qui interagissent avec le produit évalué.

Les rôles suivants doivent être pris en considération dans le cadre de l'évaluation de sécurité :

- ***Utilisateur final :*** Utilisateur final de la TOE, qui utilise le portail MIP NPM en tant que service, en lecture seule ;
- ***Administrateur métier :*** Administrateur en charge de l'administration de la TOE, de paramétrer l'utilisation qui peut en être faite par les utilisateurs finaux, de gérer les comptes utilisateurs finaux, d'ajouter ou supprimer des équipements à mesurer, de produire des rapports ;
- ***Intégrateur :*** Administrateur système en charge du socle technique. En production, il s'agit de l'équipe d'infrastructure Maltem ;
- ***Fournisseur de socle :*** Administrateur de l'infrastructure technique et officier de sécurité. En production, il s'agit d'OVH ou de Maltem.

Les utilisateurs finaux et les administrateurs métier sont regroupés par la dénomination « **bénéficiaire** » du service. L'entreprise déployant utilisant la solution MIP NPM est **bénéficiaire**.

La répartition des rôles est présentée dans le tableau suivant.

Rôle	Socle (IaaS)	Tenue du rôle
Utilisateur final (Utilisateur principal, tiers, externe)	Utilisation métier	Rôles tenus par le bénéficiaire
Administrateur métier (Administrateur TOE)	Paramétrage métier	Rôles tenus par le bénéficiaire et l'intégrateur
Administrateur système	Logiciel et données	Rôles tenus par l'intégrateur
	Intergiciels et autres logiciels de base	Rôles tenus par l'intégrateur
	Système d'exploitation	Rôles tenus par l'intégrateur
	Ressources virtualisées	Rôles tenus par l'intégrateur et le fournisseur du socle
Administrateur de l'infrastructure technique	Couche de virtualisation	Rôles tenus par le fournisseur du socle
	Machines physiques, réseau et stockage	Rôles tenus par le fournisseur du socle
Officier de sécurité	Sécurité des locaux et du personnel	Rôles tenus par le fournisseur du socle

Tableau 2 - Répartition des rôles

Les droits utilisateur sont modifiables par les administrateurs. Par défaut, un compte administrateur est préconfiguré sur la TOE à cet effet.

3.2. DESCRIPTION DES BIENS SENSIBLES

Par définition, un bien sensible est une donnée (ou fonction) jugée comme ayant de la valeur par la TOE. Sa valeur est estimée selon des critères de sécurité (aussi appelés besoins de sécurité) : disponibilité, intégrité, confidentialité et authenticité.

Les biens à protéger sont les suivants :

- biens sensibles de l'utilisateur final :

- **B1.Données d'authentification des utilisateurs**

  Les données d'authentification (identifiants et mots de passe) des utilisateurs (y compris les administrateurs métiers) sont stockées en base de données sur le portail et doivent être protégées. Elles incluent également les rôles associés à chaque utilisateur. *C'est un bien sensible de l'utilisateur final de la TOE.*

  Besoin de sécurité : disponibilité, intégrité, confidentialité.

- **B2.Données métier**

  Les données métier sont les données collectées auprès des agents de collecte via SNMP, et celles issues de leur traitement par la TOE. Elles sont stockées en base de données sur le portail et doivent être protégées. *C'est un bien sensible de l'utilisateur final de la TOE.*

  Besoin de sécurité : disponibilité, intégrité, confidentialité.

- biens sensibles de la TOE :

- **B3.Flux réseau**

  Les données métier et utilisateur transitant entre les agents de mesure, le portail de mesure et Maltem doivent être protégées.

  C'est un bien sensible de l'utilisateur final de la TOE.

  Besoin de sécurité : disponibilité, intégrité, confidentialité et authenticité.

- biens sensibles de l'administrateur métier :

- **B4.Configuration**

  La configuration des agents de mesure est stockée sur le portail et doit être protégée.

  C'est un bien sensible de l'administrateur métier de la TOE.

  Besoin de sécurité : disponibilité, intégrité, confidentialité.

Les besoins de sécurité de chacun des biens à protéger sont synthétisés dans le tableau suivant.

Biens sensibles	Disponibilité	Intégrité	Confidentialité
B1.Données d'authentification des utilisateurs	√	√	√
B2.Données métier	√	√	√
B3.Flux réseau	√	√	√
B4.Configuration	√	√	√

Dans le cas du déploiement SaaS, l'appartenance des biens sensibles devant être protégés est présentée dans le tableau suivant.

Bien sensible	Appartenance à l'utilisateur final	Appartenance à l'administrateur métier	Appartenance à la TOE
B1.Données d'identification et authentification	√	√	
B2. Données métier	√		
B3. Flux réseau			√
B4. Configuration		√	

Tableau 3 - Appartenance des biens sensibles

3.3. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

Par définition, les hypothèses sont des déclarations portant sur le contexte d'emploi de la TOE ou de son environnement.

Les hypothèses sur l'environnement de la TOE suivantes doivent être considérées :

- **H1.Administrateurs**
- Les administrateurs métiers, système, et infrastructure de la TOE sont formés aux bonnes pratiques de sécurité et à l'utilisation de cette dernière. Il s'agit de rôles considérés comme « de confiance » dans le périmètre d'analyse retenu.

- **H2.Installation**

  Les agents de mesure sont déployés sur des systèmes sains, exempts de chevaux de Troie et autres maliciels, en suivant les guides d'installation adéquats.

- **H3.Pare-feu OPNsense et shadow router**

  Le pare-feu OPNsense installé côté client, ainsi que le shadow router (routeur qui réalise des mesures de délai réseau) sont tous deux considérés comme correctement installés et de confiance.

- **H4.Iaas et mécanisme de virtualisation**

  La solution IaaS (incluant le mécanisme de virtualisation) utilisée remplit son rôle et est considéré comme de confiance.

Dans le cas du déploiement SaaS :

- L'hypothèse H1 est associée à l'**administrateur métier** de la TOE ;
- Les hypothèses H1, H2, H3 sont associées à l'**administrateur système** ;
- Les hypothèses H1, H2, H3 et H4 sont associées à l'**administrateur d'infrastructure technique** et à l'**officier de sécurité**.

3.4. DESCRIPTION DES MENACES

Par définition, une menace est une action ou un événement susceptible de porter préjudice à la sécurité de la cible évaluée.

Les agents menaçants à considérer pour l'évaluation de sécurité doivent être les suivants :

- Hors-bénéficiaire : Attaquant sur le réseau ;
- Intra-bénéficiaire :
  - employé de l'entreprise utilisant la TOE disposant d'un compte légitime ;
  - employé de l'entreprise utilisant la TOE ne disposant pas de compte légitime ;
- Inter-bénéficiaire :
  - autre bénéficiaire partageant le même *Cloud* non privé.

Les administrateurs ne sont pas considérés comme des attaquants.

Les menaces qui portent sur les biens sensibles de la TOE sont les suivantes :

- **M1.Usurpation d'identité**

  Un attaquant parvient à usurper l'identité d'un utilisateur légitime de la TOE.

- **M2.Contournement du contrôle d'accès**

  Un utilisateur légitime de la TOE parvient à contourner les droits d'accès et ainsi à élever ses privilèges, ou un autre bénéficiaire partageant le même socle parvient à accéder à des informations de la TOE.

- **M3.Corruption des données métier**

  Un attaquant parvient à corrompre les données métier, par exemple afin de falsifier les mesures relevées par les agents.

- **M4.Corruption de la configuration**

  Un attaquant parvient à altérer la configuration de la TOE portant sur les agents de mesure.

- **M5.Vol d'authentifiants**

  Un attaquant parvient à récupérer les authentifiants d'utilisateurs légitimes de la TOE.

- **M6.Corruption des authentifiants**

  Un attaquant parvient à altérer les authentifiants d'utilisateurs légitimes de la TOE.

- **M7.Vol de données métier**

  Un attaquant hors-bénéficiaire parvient à récupérer les données métier de la TOE.

- **M8.Corruption des flux réseau**

  Un attaquant parvient à dégrader le lien VPN entre un agent de mesure et le pare-feu, ou entre Maltem et le portail. Similairement, un attaquant parvient à dégrader le chiffrement effectué avec SNMPv3 entre les différents composants de la TOE.

- **M9.Usurpation des serveurs**

  Un attaquant parvient à se faire passer pour le portail auprès des agents de mesure, ou pour Maltem auprès du portail.

3.5. DESCRIPTION DES FONCTIONS DE SECURITE

Par définition, les fonctions de sécurité sont l'ensemble des mesures techniques et mécanismes mis en œuvre dans la TOE pour protéger de façon proportionnée les biens sensibles de la TOE contre les menaces identifiées.

Les fonctions de sécurité essentielles de la TOE sont les suivantes :

- **F1.Identification et authentification de chaque utilisateur du bénéficiaire**

  La TOE permet d'identifier et d'authentifier chaque utilisateur disposant d'un compte légitime.

- **F2.Contrôle d'accès et gestion des droits entre utilisateurs du bénéficiaire**

  La TOE permet de cloisonner les services fournis au bénéficiaire en fonction des privilèges de l'utilisateur courant.

- **F3.Stockage sécurisé**

  La TOE permet de stocker les données utilisateur, métier, ainsi que la configuration des agents de mesure de manière sécurisée.

- **F4.Communications sécurisées**

  La TOE permet d'établir une connexion sécurisée entre portail de mesure et agents de mesure. La communication entre les utilisateurs et la TOE est également sécurisée.

3.6. MATRICES DE COUVERTURES

3.6.1. Menaces et biens sensibles

La matrice suivante présente la couverture des menaces sur les biens sensibles (les lettres "D", "I", "C" et "A" représentent respectivement les besoins de Disponibilité, Intégrité, Confidentialité et Authenticité) :

	B1.Données d'authentification des utilisateurs	B2.Flux réseau	B3.Données métier	B4.Configuration
M1.Usurpation d'identité	**DIC**		**DIC**	**DIC**
M2.Contournement du contrôle d'accès	**DIC**		**DIC**	**DIC**
M3.Corruption des données métier			**DI**	
M4.Corruption de la configuration				**DI**
M5.Vol d'authentifiants	**C**			
M6.Corruption des authentifiants	**DI**			
M7.Vol de données métier			**C**	
M8.Corruption des flux réseau	**C**	**DIC**	**C**	
M9.Usurpation des serveurs		**CA**		

Tableau 4 - Couverture des biens sensibles par les menaces

3.6.2. Menaces et fonctions de sécurité

La matrice suivante présente la couverture des menaces par les fonctions de sécurité :

	F1.Identification et authentification de chaque utilisateur du bénéficiaire	F2.Contrôle d'accès et gestion des droits entre utilisateurs du bénéficiaire	F3.Stockage sécurisé	F4.Communications sécurisées
M1.Usurpation d'identité	√			
M2.Contournement du contrôle d'accès		√		
M3.Corruption des données métier	√	√		
M4.Corruption de la configuration	√	√	√	
M5.Vol d'authentifiants	√	√	√	√
M6.Corruption des authentifiants	√	√		
M7.Vol de données métier			√	√
M8.Corruption des flux réseau				√
M9.Usurpation des serveurs				√

Tableau 5 - Couverture des menaces par les fonctions de sécurité

Fin du document