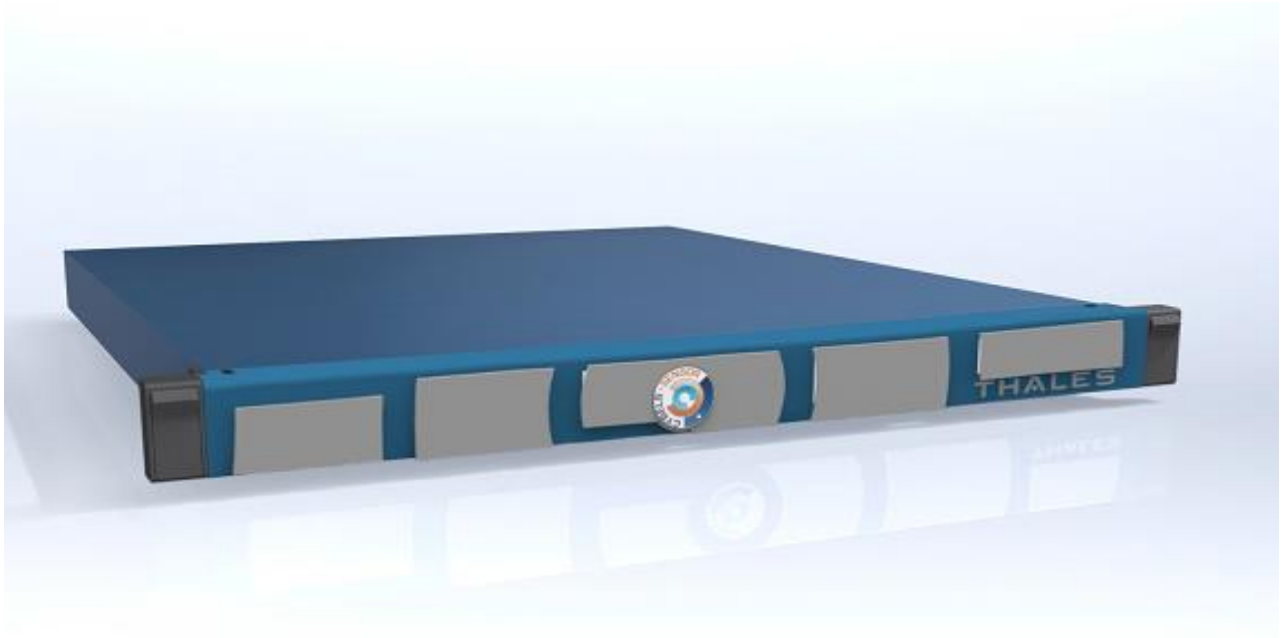
CYBELS SENSOR

Sonde réseau de détection des incidents de sécurité

Cible de sécurité

Thales



SOMMAIRE

I. Introduction

I.1. Objet du document

Le présent document constitue la cible de sécurité[1] du produit CYBELS Sensor dans sa version 2.0.5 développé par Thales dans le cadre d'une Certification de Sécurité de Premier Niveau (CSPN).

I.2. Identification du produit

Éditeur	Thales
Lien vers l'éditeur	https://www.thalesgroup.com
Nom commercial du produit	CYBELS Sensor
Numéro de la version du produit	2.0.5
Catégorie de produit	Détection d'intrusion réseau

I.3. Acronymes

Les acronymes utilisés dans le présent référentiel sont les suivants :

ANSSI	Agence nationale de la sécurité des systèmes d'information
CE	Centre d'Exploitation
CG	Centre de Gestion
CSPN	Certification de sécurité de premier niveau
IDS	*Intrusion Detection System* (Système de détection d'intrusion)
OIV	Opérateur d'Importance Vitale
PDIS	Prestataires de Détection d'Incidents de Sécurité
SFA	*Static File Analysis* (Analyse statique de fichiers)
SIIV	Système d'Information d'Importance Vitale
SOC	*Security Operation Center* (Centre opérationnel de sécurité)
TAP	*Test Access Port*
TOE	*Target Of Evaluation*

1 Ce document a été rédigé à partir du Profil de Protection de référence V1.41 du 12 05 2017/

I.4. Glossaire

Les définitions de « **règle de détection** » et « **incident de sécurité** » sont issus de [R1].

Règle de détection – liste d'éléments techniques permettant d'identifier un incident à partir d'un ou de plusieurs évènements. Une règle de détection peut être un ou des marqueurs, une ou des signatures ou une règle comportementale basée sur un comportement défini comme anormal. Une règle de détection peut provenir de l'éditeur des outils techniques d'analyse utilisés pour le service de détection, du prestataire (veille sur de nouveaux incidents, règle utilisée pour un autre commanditaire, etc.), ou avoir été créée pour répondre à un besoin du commanditaire.

Incident de sécurité – un incident de sécurité est indiqué par un ou plusieurs évènement(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité de compromettre les opérations liées à l'activité de l'organisme et/ou de menacer la sécurité de l'information.

I.5. Documents applicables

Renvoi	Document
[R1]	Prestataires de détection des incidents de sécurité, référentiel d'exigences, version 2.0 du 21 décembre 2017. Disponible sur http://www.ssi.gouv.fr
[R2]	Référentiel Général de Sécurité version 2.0, Recommandations relatives à l'administration sécurisée des systèmes d'information v3.0, n° DAT-NT-22/ANSS/SDE/NP du 11 mai 2021 Disponible sur http://www.ssi.gouv.fr
[R3]	Mécanismes cryptographiques, règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.04 du 01 janvier 2020. Disponible sur http://www.ssi.gouv.fr

II. Description du produit CYBELS Sensor

II.1. Environnement du système CYBELS Sensor

Le produit CYBELS Sensor est une sonde de détection d'intrusion réseau destinée à repérer des activités suspectes ou malveillantes sur la base de signatures. Ces signatures sont exploitées par le moteur de détection d'intrusion, ainsi que par le moteur d'analyse statique de fichiers du produit, afin de générer des évènements de sécurité.

Sur la base des flux analysés, la sonde de détection CYBELS Sensor génère :

- des alertes, correspondant à des évènements de sécurité ;
- des métadonnées relatives au trafic surveillé, venant enrichir les capacités d'investigation pour la qualification d'incidents de sécurité ;
- des fichiers extraits du trafic surveillé ;
- des journaux de fonctionnement, indiquant l'état de fonctionnement du produit.

Le **Système de détection CYBELS Sensor** permet une surveillance globale de la sécurité. Il intègre les composants suivants :

- la **Sonde de détection** CYBELS Sensor, assurant le rôle de source de collecte d'évènements de sécurité dans le cadre d'un déploiement PDIS ;
- le **Centre de Gestion**, assurant les fonctions d'administration distante des sondes et de consultation des journaux de fonctionnement ;
- le **Centre d'Exploitation**, permettant aux analystes de qualifier les évènements de sécurité sur la base des alertes et métadonnées générées par la sonde.

L'IHM graphique proposée par le Centre de Gestion est une facilité ergonomique tirant partie des interfaces exposées par le composant Sonde de détection aux administrateurs système et opérateurs, et équivaut à ce titre à la configuration manuelle qu'ils peuvent être amenés à effectuer directement sur ce composant.

Le maintien en condition de détection de la sonde CYBELS Sensor est assuré par des mises à jour régulières de signatures, en provenance de la cellule de Cyber Threat Intelligence du groupe Thales, de l'ANSSI, ou d'autres sources externes.

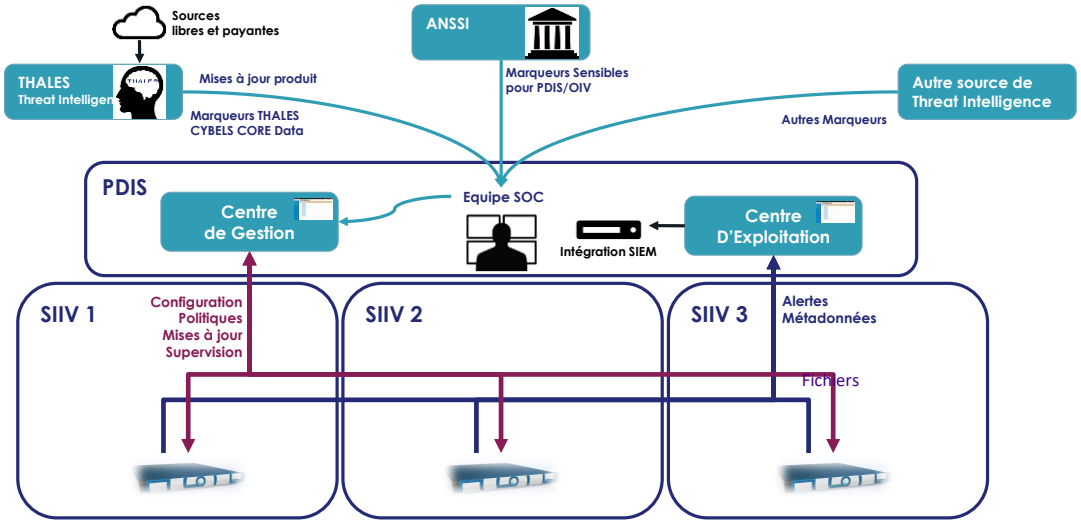


Figure 1: Architecture fonctionnelle

Le logiciel de la sonde CYBELS Sensor ainsi que les interfaces logiques I1 à I5, définies dans la suite du document, constitue la TOE.

Le logiciel intègre les fonctions suivantes :

- **IDS** : fonction de détection d'intrusion ;
- **SFA** : fonction d'analyse statique des fichiers extraits des flux ;

Les interfaces logiques sont intégrées dans le logiciel au travers des fonctions suivantes :

- I1 : fonction technique **d'acquisition des flux bruts**.
- I2 : fonctions **d'administration de sonde** distantes sur le flux d'administration pour l'accès réseau des utilisateurs de type administrateur et opérateur et la transmission des données utiles à l'administration.
- I3 : fonction technique de **remontée des alertes, métadonnées et fichiers** utile à la fonction centrale et distante de **qualification des incidents de sécurité** sur le flux de détection.
- I4 : fonction de **maintenance locale de la sonde** pour l'accès réseau local pour les utilisateurs de type administrateur et opérateur.
- I5 : fonction de **maintenance locale de la sonde** pour l'accès physique des utilisateurs de type administrateur, opérateur et auditeur.

Les données remontées par la TOE vers le service de détection sont de nature technique, destinées exclusivement à la détection d'attaques informatiques et l'autorisation de la remontée de ces données vers le service de détection est sous le contrôle exclusif du client.

II.2. Description de l'environnement prévu pour son utilisation

Dans le cadre de la surveillance de la sécurité d'un système d'information, le service de détection déploie des sondes CYBELS Sensor au sein d'une enclave de collecte chez le client.

La **qualification des incidents de sécurité** est réalisée au sein de l'enclave d'exploitation du service de détection. Le Centre d'Exploitation offre aux analystes des outils pour analyser les évènements de sécurités générés par la sonde. Le Centre d'Exploitation dispose d'interfaces vers les outils tiers d'investigation utilisés par le service de détection.

L'**administration des sondes** est réalisée au sein de l'enclave d'administration du service de détection. Les administrateurs et opérateurs peuvent exécuter des commandes sur la sonde de détection depuis le Centre de Gestion afin d'assurer le service de détection d'intrusions. Il est également possible d'assurer la supervision du service de détection en collectant ses informations de fonctionnement.

La **maintenance locale des sondes** est réalisée dans l'enclave de collecte par les administrateurs. Cet accès offre une possibilité d'administration locale, notamment en cas d'initialisation et de rupture de liaison avec le service de détection. Une consultation en lecture seule des informations d'audit est également mise en œuvre sur cet accès.

L'**acquisition des flux bruts** à analyser est réalisée par un ou plusieurs TAP unidirectionnels non administrables à distance, situés sur le système d'information du client ou sur la passerelle avec le réseau d'interconnexion.

Une agrégation de flux peut être mise en œuvre comme indiqué dans le référentiel d'exigences [R1].

La mise en conformité avec le référentiel d'exigences [R1] nécessitera par ailleurs le déploiement de pare-feux et de chiffreurs sur les systèmes d'information du client et du service de détection.

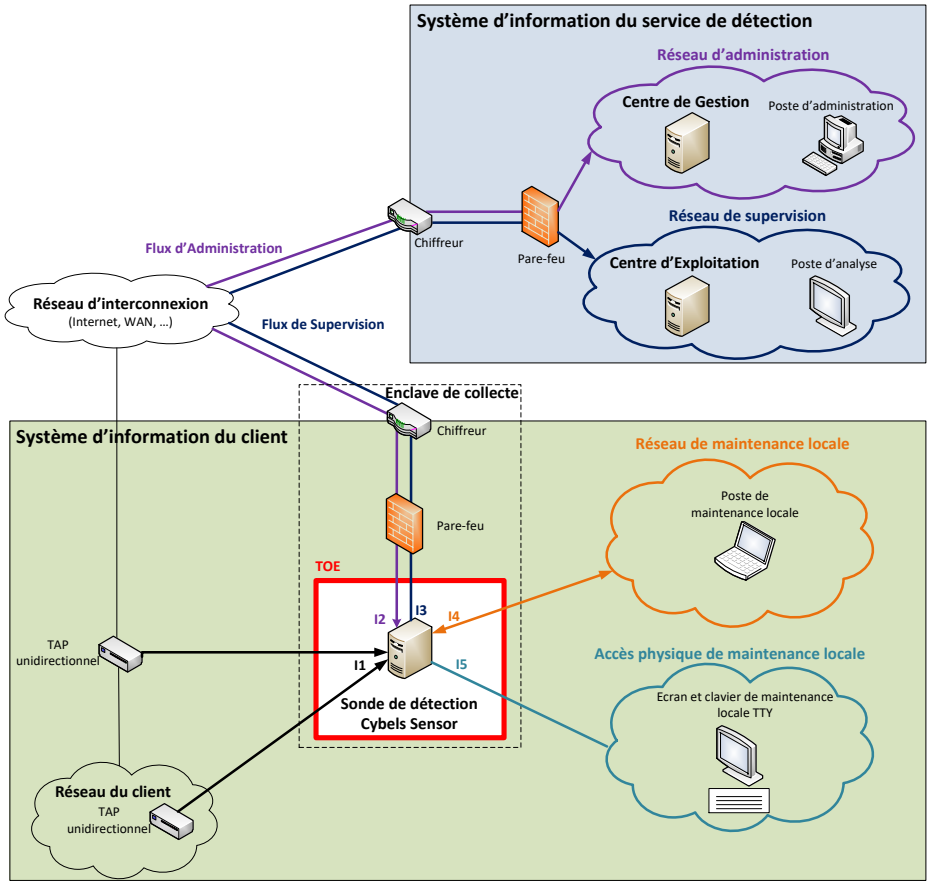


Figure 2 : Environnement de la sonde CYBELS Sensor

II.3. Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système

II.3.1. Configuration type

La configuration matérielle type de la TOE est présentée dans le tableau ci-dessous.

Mémoire	64 Go
Stockage	300 Go système 2,4 To données
Interfaces réseau	Cartes réseau dédiée à la capture de flux (interface I1)
	SFP supportés pour la capture de flux (interface I1) 1 Gbps cuivre 10 Gbps optique mono mode 1/10 Gbps optique multi mode Interfaces 1 Gbps d'administration et de remontées de détection (interface I2, I3, I4)
Interfaces physiques	Connectique physique pour la clé de déchiffrement du disque Port USB natif sur la carte mère Connectique physique pour un écran Port VGA natif sur la carte mère Connectique physique pour un clavier Port USB natif sur la carte mère

II.3.2. Options matérielles

La sonde CYBELS Sensor ne dispose pas d'option matérielle.

II.4. Description des utilisateurs typiques concernés

La TOE gère les utilisateurs suivants :

- administrateur système ;
- opérateur ;
- auditeur.

Pour des raisons de simplification, le terme « **utilisateur** » regroupe indifféremment les rôles listés ci-dessus.

La TOE remonte les alertes, métadonnées et fichiers sur le flux de détection à destination du Centre d'Exploitation.

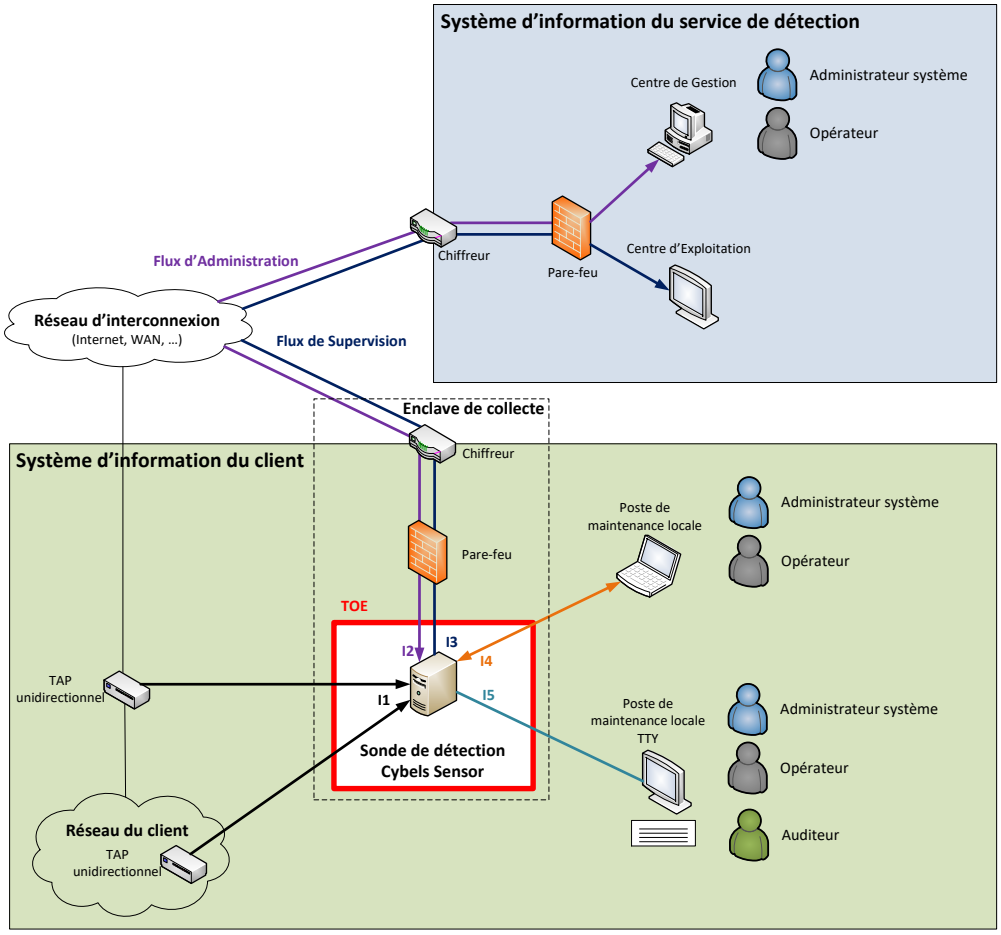


Figure 3 : Description des utilisateurs typiques de la TOE

II.5. Description du périmètre de l'évaluation

II.5.1. Périmètre de la TOE et interfaces

La TOE à considérer correspond au logiciel de la sonde CYBELS Sensor ainsi que les interfaces logiques I1 à I5. Le périmètre de l'évaluation est constitué de la TOE et de ses interfaces représentées sur la « Figure 3 : Description des utilisateurs typiques de la TOE ».

La TOE sera ainsi évaluée sur un matériel équipé des interfaces suivantes :

Interface logique	Type d'interface physique	Nombre d'interface physique	Condition d'allocation
I1	Réseau (cuivre ou optique)	2	Interfaces physiques dédiées
I2	Réseau (cuivre)	1	Interface physique mutualisable avec I3
I3	Réseau (cuivre)	1	Interface physique mutualisable avec I2
I4	Réseau (cuivre)	1	Interface(s) physique(s) dédiée(s)
I5	Clavier (connectique USB), clé USB (connectique USB) et écran (connectique VGA)	2 USB et 1 VGA	Interfaces physiques dédiées

Les utilisateurs de la TOE cités au chapitre précédent peuvent opérer :

Interface logique	Type d'interface physique	Type d'accès	Profils accédant à l'interface logique
I1	Réseau	Capture de flux bruts	Aucun (interface technique pour la capture des flux bruts)
I2	Réseau	Administration distante	Administrateur système et Opérateur.
I3	Réseau	Remontée des alertes, métadonnées, et fichiers	Aucun (interface technique pour la remontée des alertes et métadonnées et fichiers)
I4	Réseau	Administration locale	Administrateur système et Opérateur.
I5	Clavier et écran	Administration locale	Administrateur système, Auditeur, Opérateur

II.5.2. Plateforme d'évaluation de la sécurité de la TOE

La figure suivante présente la plateforme d'évaluation de la sécurité de la TOE :

- Un poste de génération d'attaques A2 et A4 est placé sur le réseau d'interconnexion, afin de lancer des attaques externes ;
- Un poste de Gestion (administration locale, distante et d'exploitation) permet de tester :
  - la remontée des journaux de fonctionnement de la TOE ;
  - la remontée de métadonnées, d'alertes et de fichiers par la TOE ;
  - la protection des flux en confidentialité et en intégrité sur les flux I2, I3 et I4.
- Un accès écran/clavier qui permet :
  - à l'auditeur de consulter les journaux de fonctionnement, ainsi que des informations relatives aux règles de détection ;
  - les opérations de maintenance locale (installation, réparation, mise en service, configuration) pour les administrateurs.

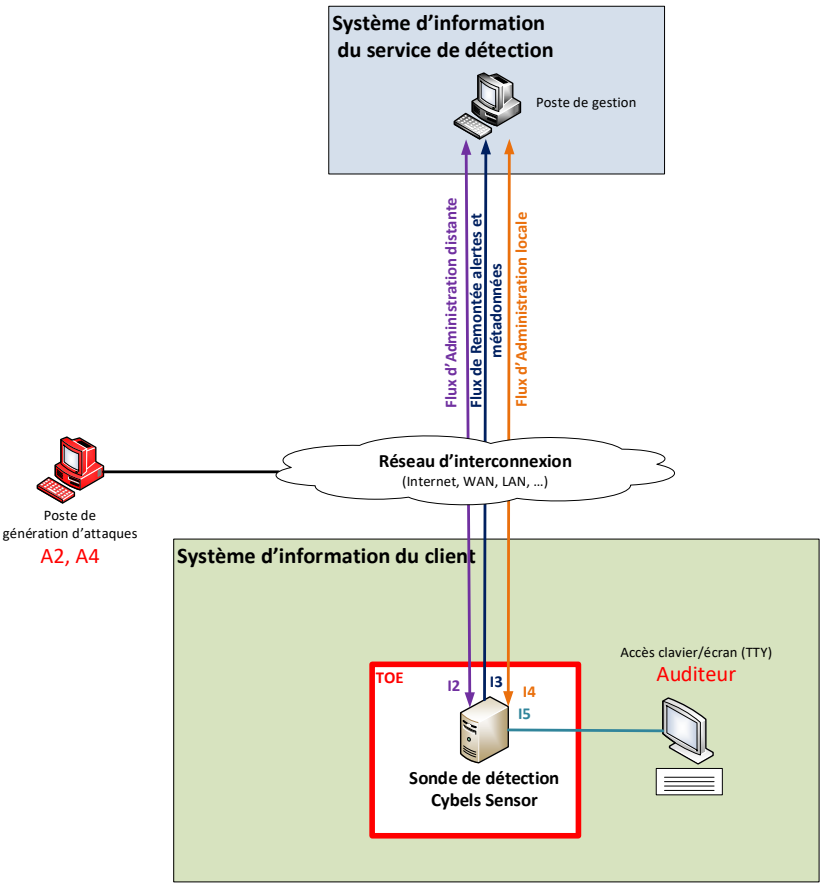


Figure 4 : Périmètre de l'évaluation de la sécurité de la TOE

II.5.3. Plateforme d'évaluation des capacités métier de la TOE

La figure suivante présente la plateforme d'évaluation des capacités métier de la TOE :

- Un poste de génération d'attaques A1 et A3 est placé sur le réseau du client, afin de lancer des attaques internes ;
- Un poste de génération de trafic permettent de simuler un fonctionnement nominal de trafic réseau légitime ;
- Un poste de Gestion (administration locale, distante et d'exploitation) permet de tester :
  - la remontée de métadonnées, d'alertes et de fichiers par la TOE ;

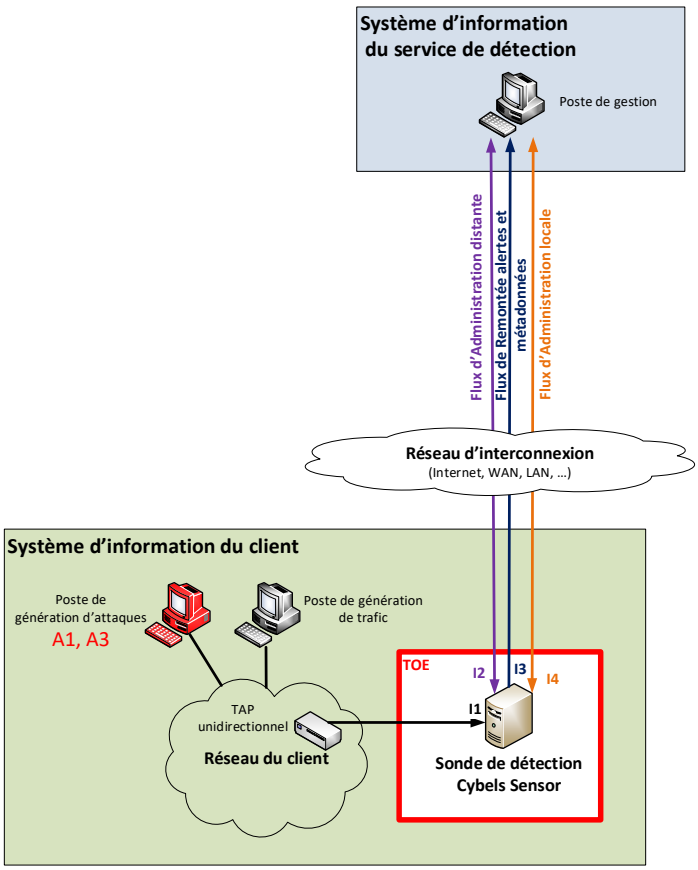


Figure 5 : Périmètre de l'évaluation des capacités métier de la TOE

III. Description des hypothèses sur l'environnement

Les hypothèses sur l'environnement de la TOE sont les suivantes :

H1 Dérivation

La TOE est placée en dérivation des flux à analyser et non en coupure.

H2 TAP unidirectionnel

La dérivation vers la TOE des flux à analyser est réalisée par un TAP unidirectionnel non administrable à distance. Il est recommandé que le TAP unidirectionnel soit qualifié au niveau élémentaire par l'ANSSI comme le précisent les exigences [R1].

H3 Dimensionnement

La TOE est dimensionnée pour répondre aux contraintes de l'environnement dans lequel est déployée la TOE (traitement du débit des flux à analyser, capacité de stockage, etc.).

H4 Utilisateurs

Les utilisateurs de la TOE sont formés à son utilisation et disposent de sa documentation.

H5 Base de règles de détection

La TOE dispose d'une base de règles de détection à jour et testées préalablement avant d'être importées dans la TOE. Elle ne comporte pas de règles mal formées.

H6 Conformité légale et réglementaire

La TOE est déployée selon les lois et réglementations en vigueur.

H7 Système d'information du service de détection

Le système d'information du service de détection respecte les exigences [R1].

H8 Enclave

L'enclave respecte les exigences de [R1]. Des chiffreurs qualifiés et utilisés selon leurs conditions d'emploi sont notamment déployés au plus près de la TOE pour diminuer le risque de compromission des informations lorsqu'elles transitent entre le service de détection des incidents de sécurité et la TOE. Les attaques physiques sur le produit sont exclues, mais les attaques des auditeurs via la console sont une possibilité.

H9 Interfaces réseau et USB/VGA

La TOE dispose de huit interfaces physiques différentes (dont 5 interfaces réseaux, 2 USB et 1 VGA), et conformément au schéma du chapitre II.2 :

- l'interface $\mathbf{I_1}$ (composée de deux interfaces physiques de capture réseau) reçoit les flux en provenance du TAP unidirectionnel ;
- l'interface $\mathbf{I_2}$ (composée d'une interface physique réseau) est connectée au système d'information du service de détection et permet aux administrateurs système, et opérateurs d'effectuer leurs tâches ;

- l'interface **I_3** (composée d'une interface physique réseau) est connectée au système d'information du service de détection et permet à la TOE de remonter les alertes, métadonnées et fichiers analysés ;
- l'interface **I_4** (composée d'une interface physique réseau) est connectée à un réseau de maintenance locale (non connecté au système d'information du client) utilisé par les administrateurs lors de l'installation et de la maintenance, ou en cas d'indisponibilité de la liaison avec le système d'information du service de détection. Un opérateur peut également l'utiliser pour redémarrer les services métier relatif à la détection ou déployer des règles. ;
- l'interface **I_5** (composée d'une interface physique USB/VGA et une autre interface physique USB) permet aux auditeurs, administrateurs système et opérateurs d'effectuer leurs tâches localement.

H10 Réseau d'administration

La TOE ne nécessite pas d'interfaçage avec le réseau d'administration du système d'information du client. Les opérations locales sur les interfaces I4 et I5 doivent être effectuées depuis un accès de maintenance temporaire.

H11 Désactivation des fonctions natives d'administration à distance

Les fonctions d'administration à distance offertes nativement par des matériels constituant la TOE (ex. : carte réseau) sont désactivées.

H12 Personnel administrateur de confiance

Les profils « Administrateur Système » et « Opérateurs » sont attribués uniquement à des personnes de confiance. Ces personnes ne tenteront pas d'usurper ni d'élever leur privilège vers un autre compte administrateur disposant de plus de droits.

IV. Description des biens sensibles

Les biens sensibles de la TOE sont les suivants :

B1 Logiciels de la TOE

Les logiciels de la TOE sont considérés comme des biens sensibles. Ils doivent être protégés en disponibilité, intégrité et authenticité.

B2 Base des utilisateurs

La base des utilisateurs de la TOE, leurs informations d'authentification auprès de la TOE et leurs droits d'accès à la TOE sont à protéger en disponibilité, confidentialité et intégrité.

B3 Règles de détection

Les règles de détection permettent de détecter des incidents de sécurité. Ce bien est à protéger en disponibilité, confidentialité et intégrité. L'intégrité est effectuée par un contrôle d'accès (seul le rôle autorisé peut changer le contenu des règles sur la TOE).

B4 Flux bruts

Cette version de la TOE ne permettant pas la capture pour stockage sur le disque et la remontée au service de détection des flux bruts, ce bien n'a pas de persistance.

B5 Métadonnées

Les métadonnées sont extraites des flux bruts par la TOE. Ce bien est à protéger en disponibilité, confidentialité et intégrité.

B6 Fichiers à analyser

Les fichiers à analyser sont extraits des flux bruts par la TOE. Ce bien est à protéger en disponibilité, confidentialité et intégrité.

B7 Alertes

La TOE génère des alertes déclenchées par les règles de détection. Ce bien est à protéger en disponibilité, confidentialité et intégrité.

B8 Données contextuelles

Ce bien est inexistant car aucune donnée contextuelle n'est apportée par la TOE. La TOE génère uniquement des alertes, métadonnées et des fichiers extraits du flux.

B9 Configuration

La configuration de la TOE est à protéger en disponibilité, confidentialité et intégrité.

B10 Journaux de fonctionnement

L'ensemble des opérations effectuées par la TOE et par les utilisateurs est journalisé. Ce bien est à protéger en disponibilité, confidentialité et intégrité.

B11 Éléments cryptographiques

La TOE manipule et stocke des éléments cryptographiques (mots de passe, clés de chiffrement / déchiffrement, clés de signature, vérification de signatures, etc.) pour assurer ses fonctions de sécurité. Ce bien est à protéger en disponibilité, confidentialité et intégrité.

B12 Informations techniques complémentaires nécessaires à la qualification d'incidents

Outre les alertes et métadonnées, il peut s'avérer dans certains cas possibles de considérer des informations techniques complémentaires pour qualifier des incidents (exemple : fichiers malveillants). Ce bien est à protéger en disponibilité, confidentialité et intégrité.

La TOE génère des fichiers extraits du flux.

Biens sensibles		D	I	C	A
B1	Logiciels de la TOE	×	×		×
B2	Base des utilisateurs	×	×	×	
B3	Règles de détection	×	×	×	
~~B4~~	~~Flux Bruts~~	~~×~~	~~×~~	~~×~~	
B5	Métadonnées	×	×	×	
B6	Fichiers à analyser	×	×	×	
B7	Alertes	×	×	×	
~~B8~~	~~Données contextuelles~~	~~×~~	~~×~~	~~×~~	
B9	Configuration	×	×	×	
B10	Journaux de fonctionnement	×	×	×	
B11	Éléments cryptographiques	×	×	×	
B12	Informations techniques complémentaires	×	×	×	

Légende : Disponibilité (D), Intégrité (I), Confidentialité (C), Authenticité (A).

Tableau 1 : Biens sensibles de la TOE

V. Description des menaces

V.1. Profils des attaquants

Les attaquants à considérer pour l'évaluation sont :

- les utilisateurs de la TOE suivants :
  - auditeur.
- toute personne malveillante connectée sur le réseau du client et pouvant ainsi interagir avec la TOE via son interface réseau I_1 (attaquant A1) ;
- toute personne malveillante située entre la TOE et le chiffreur d'enclave et pouvant ainsi interagir avec la TOE via ses interfaces réseau I_2 et I_3 (attaquant A2) ;
- toute personne malveillante située sur le réseau d'interconnexion ou entre le TAP unidirectionnel et le réseau d'interconnexion et pouvant ainsi interagir avec la TOE via son interface réseau I_1 (attaquant A3) ;
- toute personne malveillante située sur le réseau de maintenance locale ou entre la TOE et le réseau de maintenance locale et pouvant ainsi interagir avec la TOE via son interface réseau I_4 (attaquant A4) ;

Sauf mention contraire, le terme « **attaquant** » regroupe l'ensemble des profils d'attaquants présentés ci-dessus.

Remarque 1 : La menace d'une attaque sur le lien réseau entre le TAP et la TOE n'est pas comprise dans le périmètre de l'évaluation. En revanche, toute action malveillante sur l'interface réseau I1 est bien incluse dans le périmètre de l'évaluation.

Remarque 2 : Conformément à l'hypothèse H12, les administrateurs système et les opérateurs disposent de droits privilégiés pour la réalisation de leurs tâches et sont considérés de confiance. Le service de détection doit notamment respecter les exigences organisationnelles de [R1].

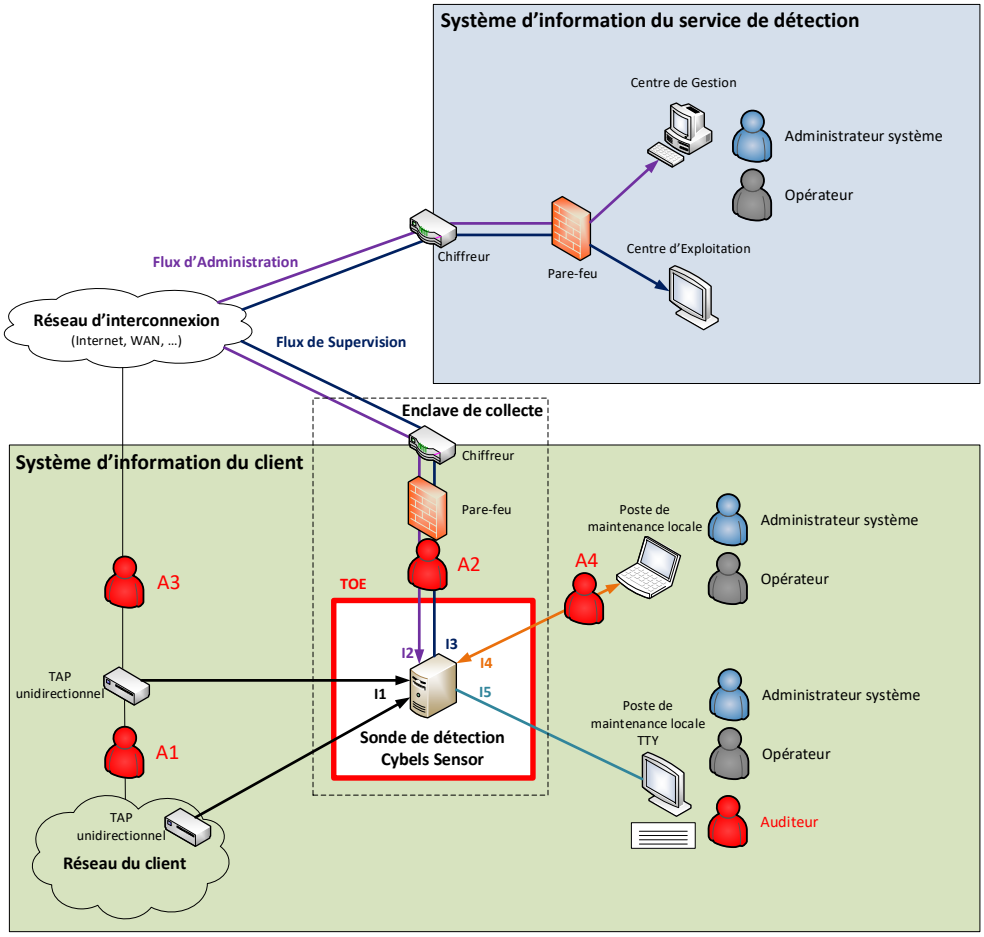


Figure 6 : Profil et positionnement des attaquants

V.2. Menaces

Les menaces à considérer pour l'évaluation sont :

M1 Vol

Un attaquant dispose d'un accès physique à la TOE, la vole et réussit à extraire des informations sensibles en confidentialité.

M2 Compromission

Un attaquant, via l'une des interfaces I1 à I5 réseau de la TOE, prend connaissance (mise en défaut de la confidentialité) ou altère (mise en défaut de l'intégrité) des biens sensibles en confidentialité ou en intégrité.

M3 Contournement

Un attaquant, via l'une des interfaces I1 à I5 réseau de la TOE, leurre la fonction de détection de la TOE, de telle sorte qu'une règle de détection devant générer une alarme n'en génère aucune.

M4 Usurpation d'identité

Un attaquant, via l'une des interfaces I1 à I5 réseau de la TOE, usurpe l'identité d'un utilisateur de la TOE.

M5 Élévation de privilèges

Un auditeur élève ses privilèges**.**

M6 Indisponibilité

Un attaquant, via l'une des interfaces I1 à I5 réseau de la TOE, rend indisponible tout ou partie des fonctions de sécurité de la TOE de manière temporaire ou définitive.

M7 Manipulation malveillante de flux

Un attaquant, ne disposant pas d'accès légitime à la TOE, écoute, altère, injecte ou rejoue des données échangées entre les utilisateurs et la TOE via ses interfaces réseau I_2, I_3 et I_4 afin de mener des actions malveillantes.

VI. Description des fonctions de CYBELS Sensor

Les fonctions de la TOE sont les suivantes :

VI.1. Fonctions métier

FM1 Capture

La TOE capture l'ensemble du trafic en provenance du TAP et le transmet sous la forme de flux bruts aux fonctions de décodage et d'analyse réseau.

La TOE rejette des paquets lorsque le débit des flux transmis par le TAP unidirectionnel est supérieur à la capacité de traitement de la TOE.

FM2 Décodage

La TOE décode, selon leur protocole, les flux bruts qu'elle transmet sous la forme de flux décodés aux fonctions de journalisation de métadonnées, d'analyse de fichiers et d'analyse réseau. Les flux décodés peuvent prendre notamment la forme de métadonnées et de fichiers extraits.

FM3 Journalisation des métadonnées

La TOE journalise des métadonnées à partir des flux décodés uniquement en cas d'indisponibilité de la fonction de remontée des métadonnées. La TOE stocke et prend en compte à minima les métadonnées. Lorsque la capacité de stockage maximale est atteinte, la TOE ne journalise plus les métadonnées mais continue d'assurer partiellement sa fonction de détection.

FM4 Analyse réseau

La TOE analyse les flux décodés et les métadonnées par reconnaissance de protocoles et reconnaissance de motifs. La TOE génère des alertes.

FM5 Analyse de fichiers

La TOE analyse les fichiers issus de la fonction de décodage par analyse statique. La TOE génère des alertes.

FM6 Journalisation des alertes

La TOE journalise les alertes déclenchées par les règles de détection. Lorsque la capacité de stockage maximale est atteinte, la TOE effectue une rotation.

FM7 Remontée d'alertes

La TOE envoie les alertes au système d'information du service de détection en protégeant leur intégrité et leur confidentialité. Les alertes sont transmises individuellement au fil de l'eau.

La TOE ne transmet plus les journaux d'alertes lorsque la capacité de rétention avant envoi (capacité distincte de celle de rétention locale) de ces journaux est atteinte.

FM8 Remontée de métadonnées

La TOE envoie les métadonnées aux analystes sur le système d'information du service de détection en protégeant leur intégrité et leur confidentialité. Les métadonnées sont transmises individuellement au fil de l'eau.

FM9 Corrélation

Cette fonction métier n'est pas mise en œuvre sur la TOE.

FM10 Remontée de fichiers

La TOE envoie les fichiers extraits aux analystes sur le système d'information du service de détection en protégeant leur intégrité et leur confidentialité. Les fichiers extraits sont transmis individuellement au fil de l'eau.

FM11 Mise à jour des règles de détection

La TOE permet à l'opérateur de mettre à jour les bases de règles de détection.

VI.2. Fonctions de sécurité

FS1 Chiffrement du système de fichiers

La TOE chiffre son système de fichiers conformément à [R3].

FS2 Identification, authentification et contrôle d'accès

La TOE identifie et authentifie les utilisateurs. Elle contrôle l'accès des utilisateurs aux ressources de la TOE en fonction de leurs droits d'accès.

FS3 Mise à jour des logiciels

La TOE permet à l'administrateur système de mettre à jour les logiciels de la TOE. La TOE vérifie l'authenticité des logiciels avant installation.

FS4 Mise à jour de règles de détection

La TOE met en place des mécanismes de contrôle lors de la mise à jour des bases de règles de détection garantissant que le contenu ainsi importé n'impacte pas la sécurité de la TOE.

FS5 Journalisation de fonctionnement

La TOE journalise l'ensemble des opérations effectuées par les utilisateurs et par elle-même. Lorsque la capacité de stockage maximale est atteinte, la TOE effectue une rotation des journaux. (i.e. : La TOE effectue une rotation des journaux lorsque la capacité de rétention des journaux de fonctionnement et d'alertes est atteinte.)

FS6 Protection des flux

La TOE protège en confidentialité et en intégrité toutes les actions réalisées à distance par les utilisateurs et les informations échangées avec le service de détection.

FS7 Activation/désactivation du stockage, de la remontée d'informations techniques complémentaires nécessaires à la qualification d'incidents

Cette version de la TOE ne permettant pas la capture et la remontée au service de détection des informations techniques complémentaires, cette fonction de sécurité n'existe pas.

FS8 Cloisonnement

Les fonctions métier de la TOE sont cloisonnées afin de limiter la prise de contrôle à distance et le risque de rebond.

FS9 Dimensionnement

N/C

FS10 Remontée des journaux de fonctionnement

La TOE envoie les journaux de fonctionnement au système d'information du service de détection en protégeant leur intégrité et leur confidentialité. Les évènements sont transmis individuellement au fil de l'eau.

Annexe 1 Liste des tâches associées aux utilisateurs

Le tableau ci-dessous liste les tâches relatives :

- aux utilisateurs gérés par la TOE :
  - administrateur système ;
  - opérateur ;
  - auditeur.

Catégorie	Détail de la tâche	Administrateur système	Opérateur	Auditeur
Version				
	consultation de la version de la TOE	OK	OK	OK
Tâches courantes				
	effacement des fichiers inutiles de leur espace utilisateur	OK	OK	
Gestion du temps de référence				
	consultation du temps de référence de la TOE (consultation de la date et de l'heure)	OK	OK	OK
	édition du temps de référence de la TOE (configuration de la date et de l'heure)	OK		
	modification du fuseau horaire de l'horloge système	OK		
Gestion des utilisateurs				
	édition de l'attribut 'mot de passe' du compte personnel	OK	OK	OK
	édition de l'attribut 'mot de passe' des comptes associés aux rôles 'administrateur système', 'opérateur'	OK		
	édition de l'attribut 'mot de passe' des comptes associés aux rôles 'auditeur'	OK		
	création des comptes associés aux rôles 'administrateur système', 'opérateur'	OK		
	suppression des comptes associés aux rôles 'administrateur système', 'opérateur'	OK		
	consultation de la liste des utilisateurs	OK		
Gestion des éléments cryptographiques				
	consultation de la configuration IPsec de la TOE	OK		
	modification de la configuration IPsec de la TOE	OK		
	rétablissement de la configuration IPsec usine de la TOE	OK		
	activation / désactivation d'un tunnel IPsec de la TOE	OK		
	mise à jour des certificats IPsec de la TOE	OK		
	renouvellement des clés SSH de la TOE	OK		
	renouvellement des clés SSH d'authentification d'un client	OK		
	modification du mot de passe de chiffrement du disque dur de la TOE	OK		

Catégorie	Détail de la tâche	Administrateur système	Opérateur	Auditeur
Journaux de fonctionnement				
	consultation des journaux de fonctionnement générés par la TOE	OK	OK	OK
	consultation des journaux de démarrage de la TOE	OK	OK	
	récupération des journaux de démarrage de la TOE	OK		
Supervision du fonctionnement				
	consultation de l'état des services	OK	OK	
	diagnostic d'une interface physique de la TOE	OK		
	diagnostic d'une installation	OK		
	vérification de l'intégrité du système	OK		
	réinitialisation de la base d'intégrité de référence du système	OK		
	consultation de l'état des services de journalisation et de l'état des tunnels IPsec (Rsyslog des CE/CG et état d'activation d'IPsec)	OK		
	obtention des statistiques d'analyse réseau de la TOE		OK	
	obtention des statistiques d'analyse de fichiers de la TOE		OK	
Arrêt et démarrage				
	arrêt de la TOE	OK		
	redémarrage de la TOE	OK		
	redémarrage des interfaces de capture de la TOE	OK		
Mise à jour système et des logiciels (commande commune)				
	mise à jour du système d'exploitation et des logiciels de la TOE	OK		
	affichage du jeu de clé de mise à jour (version LPM ou non LPM)	OK		
Configuration réseau				
	consultation de la configuration réseau de la TOE	OK		
	édition de la configuration réseau de la TOE	OK		
	rétablissement de la configuration réseau de la TOE	OK		
	activation / désactivation de la journalisation des paquets rejetés par le pare-feu	OK		
	consultation des adresses IP des interfaces I2 et I3 de la TOE			OK
Arrêt et démarrage des fonctions métier				
	redémarrage du service d'analyse réseau de la TOE		OK	
	redémarrage du service d'analyse de fichiers de la TOE		OK	
	activation / désactivation du service d'analyse de fichiers de la TOE		OK	
Règles de détection : analyse réseau				
	consultation des informations relatives aux règles de détection IDS : identifiant unique et description de la règle de détection (mais pas les paramètres de détection)		OK	

Catégorie	Détail de la tâche	Administrateur système	Opérateur	Auditeur
	consultation des informations relatives aux règles de détection IDS : description de la règle de détection (mais pas l'identifiant unique et les paramètres de détection)			OK
	consultation des informations relatives aux règles de détection IDS : identifiant de politique active		OK	
	déploiement des règles de détection IDS		OK	
	consultation de la configuration du service d'analyse réseau de la TOE		OK	
	configuration du service d'analyse réseau de la TOE		OK	
	configuration des éléments générés par le service d'analyse réseau de la TOE : création des alertes, génération des métadonnées, génération des métadonnées des fichiers attachés aux flux et génération des hash des fichiers attachés aux flux		OK	
Règles de détection : analyse de fichiers				
	consultation des informations relatives aux règles de détection de l'analyse de fichiers : intégralité de la règle de détection		OK	
	consultation des informations relatives aux règles de détection de l'analyse de fichiers : nom et métadonnées de la règle de détection (mais pas les paramètres de détection)			OK
	consultation des informations relatives aux règles de détection de l'analyse de fichiers : identifiant de la politique active		OK	
	déploiement de règles de détection d'analyse de fichiers		OK	
Journaux d'alertes				
	consultation des journaux d'alertes générés par la TOE		OK	
Fonctions d'analyse portées par le Centre d'Exploitation (hors périmètre de l'évaluation)				
	consultation des journaux d'alertes générés par la TOE			
	consultation des métadonnées extraites des flux bruts par la TOE			

Annexe 2 Matrices de couverture

I. Menaces et biens sensibles

		B1 Logiciels de la TOE	B2 Base des utilisateurs	B3 Règles de détection	B4 ~~Flux Bruts~~	B5 Métadonnées	B6 Fichiers à analyser	B7 Alertes	B8 ~~Données Contextuelles~~	B9 Configuration	B10 Journaux de fonctionnement	B11 Éléments cryptographiques	B12 Information techniques complémentaires
M1	Vol		C	C	~~C~~	C	C	C	~~C~~	C	C	C	C
M2	Compromission	IA	CI	CI	~~CI~~	CI	CI	CI	~~CI~~	CI	CI	CI	CI
M3	Contournement	IA		I				I			I		
M4	Usurpation d'identité		CI										
M5	Élévation de privilèges	IA	CI	CI	~~CI~~	CI	CI	CI	~~CI~~	CI	CI	CI	CI
M6	Indisponibilité	D	D	D	~~D~~	D	D	D	~~D~~	D	D	D	D
M7	Manipulation malveillante de flux	IA	CI	CI	~~CI~~	CI	CI	CI	~~CI~~	CI	CI	CI	CI

Légende : Disponibilité (D), Intégrité (I), Confidentialité (C), Authenticité (A).

Tableau 2 : Atteintes aux biens sensibles en fonction des menaces

II. Menaces et fonctions de sécurité

		FM1-FM9 Fonctions métier liées à la détection	FS1 Chiffrement du disque	FS2 Identification, authentification et contrôle d'accès	FS3 Mise à jour des logiciels	FS4 Mise à jour des règles de détection	FS5 Journalisation de fonctionnement	FS6 Protection des flux	FS7 Activation /désactivation de la manipulation de fichier…	FS8 Cloisonnement	FS9 Dimensionnement	FS10 Remontée des journaux de fonctionnement
M1	Vol		×	×								
M2	Compromission			×	×		×	×		×		×
M3	Contournement	×				×	×				*	
M4	Usurpation d'identité			×			×					
M5	Élévation de privilèges			×	×		×		*			×
M6	Indisponibilité	×					×					×
M7	Manipulation malveillante de flux							×				

Tableau 3 : Couverture des menaces par les fonctions de sécurité