[Assignement : nom de l’éditeur]

[Assignement : nom du produit]

Sonde réseau de détection des incidents de sécurité

Cible de sécurité

[Assignement : photo du produit]

SOMMAIRE

I. Introduction

I.1. Objet du document

Le présent document constitue la cible de sécurité du produit **[assignement : nom du produit]** dans sa version **[assignement : version du produit]** développé par **[assignement : nom de l'éditeur]** dans le cadre d'une Certification de Sécurité de Premier Niveau (CSPN).

I.2. Identification du produit

Editeur	**[Assignement : nom de l'éditeur]**
Lien vers l'éditeur	**[Assignement : lien vers le site Internet de l'éditeur]**
Nom commercial du produit	**[Assignement : nom commercial du produit]**
Numéro de la version du produit	**[Assignement : version du produit]**
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
CSPN	Certification de sécurité de premier niveau
TOE	*Target Of Evaluation*
TAP	*Test Access Port*

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 en vigueur. Disponible sur http://www.ssi.gouv.fr
[R2]	Recommandations relatives à l'administration sécurisée des systèmes d'information, n° DAT-NT-22/ANSS/SDE/NP du 20 février 2015 Disponible sur http://www.ssi.gouv.fr
[R3]	Mécanismes cryptographiques, règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version en vigueur. Disponible sur http://www.ssi.gouv.fr

II. Description du produit

II.1. Description de la manière d'utiliser le produit

[Assignement : description de la manière d'utiliser le produit].

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

[Raffinement : ce schéma est à refaire par le rédacteur de la cible de sécurité. Les éventuels composants de la sonde ou liés à la sonde devant être déployés au sein du réseau client, du réseau d'administration du client, de l'enclave ou du système d'information du service de détection doivent être identifiés]

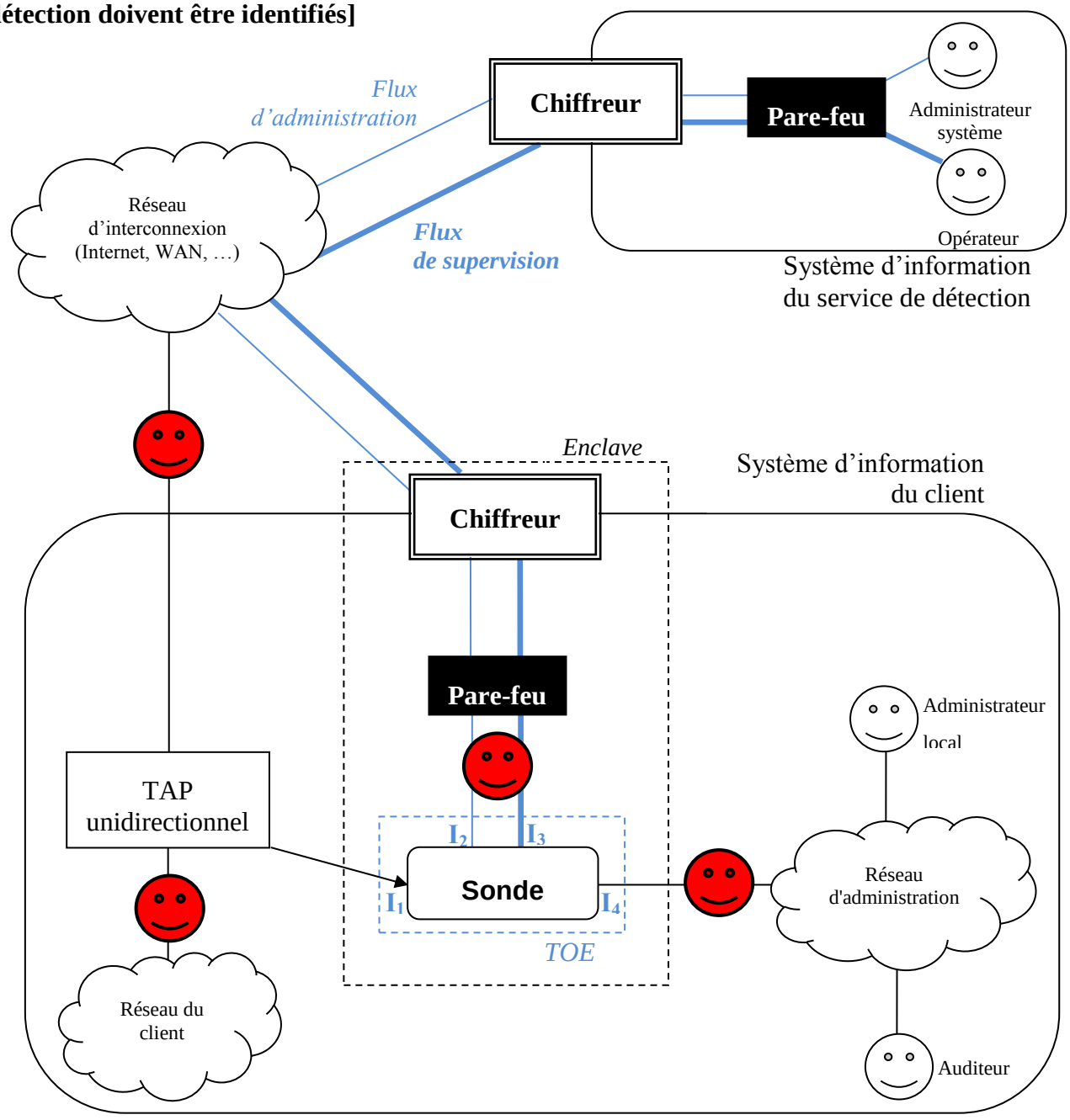

Figure 1: Environnement d'utilisation du produit

Légende : Attaquant

II.3. Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système non fournis avec le produit

[Assignement : description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système non fournis avec le produit]

II.4. Description des utilisateurs typiques concernés

La TOE gère les utilisateurs suivants :

- administrateur local ;
- administrateur système ;
- auditeur ;
- opérateur ;
- **[Assignement : lister d'autres rôles si besoin]**.

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

L'association des utilisateurs avec liste des tâches qu'ils sont autorisés à réaliser est donnée en Annexe 1

II.5. Description du périmètre de l'évaluation

Le périmètre de l'évaluation est constitué de la TOE et de ses **[assignement : nombre d'interfaces réseau]** interfaces réseau.

[Assignement : compléter la liste des interfaces si besoin par exemple par des interfaces systèmes tels que USB, VGA, …]

Le périmètre de l'évaluation est représenté au chapitre II.2.

[Assignement : compléter la description du périmètre de l'évaluation si besoin]

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.

H9 Interfaces réseau

La TOE dispose de **[assignement : nombre d'interfaces réseau]** interfaces réseau physiques différentes et conformément au schéma du chapitre II.2 :

- l'interface $\mathbf{I_1}$ reçoit les flux en provenance du TAP unidirectionnel;
- l'interface $\mathbf{I_2}$ est connectée au système d'information du service de détection et permet aux administrateurs système d'effectuer leurs tâches ;
- l'interface $\mathbf{I_3}$ est connectée au système d'information du service de détection et permet aux opérateurs d'effectuer leurs tâches ;
- l'interface $\mathbf{I_4}$ est connectée au réseau d'administration du client et permet aux administrateurs locaux et aux auditeurs d'effectuer leurs tâches ;
- **[assignement : autres interfaces réseau si besoin]**.

H10 Réseau d'administration

Le réseau d'administration dans le système d'information du client permet aux administrateurs locaux et auditeurs d'effectuer leurs tâches en respectant les exigences de [R2].

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.

[Assignement : autres hypothèses si besoin]

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 permettant de détecter des incidents de sécurité. Ce bien est à protéger en disponibilité, confidentialité et intégrité.

B4 Flux bruts

Les flux bruts désignent les flux réseau à analyser en provenance du TAP. Ce bien est à protéger en disponibilité, confidentialité et intégrité.

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

Les données contextuelles sont extraites des flux bruts par la TOE. Elles améliorent la détection et la qualification d'incidents (exemple : cartographie réseau). Ce bien est à protéger en disponibilité, confidentialité et intégrité.

[Raffinement : ce bien n'existe que si la TOE extrait des données contextuelles]

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 Eléments 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 possible[1] de considérer des informations techniques complémentaires pour qualifier des incidents (exemple : fichiers malveillants). Ce bien est à protéger en disponibilité, confidentialité et intégrité.

[Raffinement : ce bien n'existe que si la TOE extrait des informations techniques complémentaires]

[Assignement : autres biens sensibles si nécessaire]

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	Eléments cryptographiques	×	×	×	
B12	Informations techniques complémentaires nécessaires à la détection	×	×	×	

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

Tableau 1 : Biens sensibles de la TOE

[1] Cadre légal, modalités contractuelles, etc.

V. Description des menaces

V.1. Profils des attaquants

Les attaquants à considérer pour l'évaluation sont :

- les utilisateurs de la TOE suivants :
  - administrateur local ;
  - opérateur ;
  - auditeur ;
  - **[assignement : autres profils listés au chapitre II.4, hors administrateur système]**.
- toute personne malveillante connectée sur le réseau du client et pouvant ainsi interagir avec la TOE via son interface réseau I_1 ;
- toute personne malveillante située entre la TOE et le chiffreur et pouvant ainsi interagir avec la TOE via ses interfaces réseau I_2 et I_3 ;
- 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 ;
- toute personne malveillante située sur le réseau d'administration du client ou entre la TOE et le réseau d'administration du client et pouvant ainsi interagir avec la TOE via son interface réseau I_4 ;
- toute personne pouvant accéder physiquement à la TOE alors qu'elle est en exploitation.

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

V.2. Menaces

Les menaces à considérer pour l'évaluation sont :

M1 Vol

Un attaquant disposant d'un accès physique à la TOE alors qu'elle est en exploitation la vole et réussit à extraire des informations sensibles en confidentialité.

M2 Compromission

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

M5 Elévation de privilèges

Un auditeur, un administrateur local ou un opérateur **[assignement : autres profils listés au chapitre II.4, hors administrateur système]** élève ses privilèges**.**

M6 Indisponibilité

Un attaquant, via l'une des interfaces 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 I_2, I_3 et I_4 réseau afin de mener des actions malveillantes.

[Assignement : autres menaces si besoin]

VI. Description des fonctions du produit

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.

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. La TOE stocke et prend en compte *a minima* les métadonnées listées en Annexe 1. Lorsque la capacité de stockage maximale est atteinte, la TOE **[sélection : effectue une rotation, ne journalise plus les métadonnées mais continue d'assurer partiellement sa fonction de détection, n'assure plus sa fonction de détection, autres]**.

FM4 Analyse réseau

La TOE analyse les flux bruts, les flux décodés et les métadonnées journalisées par **[sélection : reconnaissance de motifs, reconnaissance de protocoles, analyse comportementale, autres]**. La TOE génère des alertes et éventuellement, des données contextuelles.

FM5 Analyse de fichiers

La TOE analyse les fichiers issus de la fonction de décodage par **[sélection : une correspondance avec une règle de détection, une analyse statique, une analyse dynamique, autres]**. 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 **[sélection : effectue une rotation, ne journalise plus les alertes mais continue d'assurer partiellement sa fonction de détection, n'assure plus sa fonction de détection, autres]**.

FM7 Remontée d'alertes

La TOE envoie les alertes aux opérateurs situés dans le système d'information du service de détection en protégeant leur intégrité et leur confidentialité. Les alertes sont transmises **[sélection : individuellement au fil de l'eau, sous la forme de journaux, autres]**.

FM8 Remontée de métadonnées

La TOE envoie les métadonnées aux opérateurs situés dans le système d'information du service de détection en protégeant leur intégrité et leur confidentialité. Les métadonnées sont transmises **[sélection : individuellement au fil de l'eau, sous la forme de journaux, autres]**.

FM9 Corrélation

La TOE réalise des traitements sur les alertes, les métadonnées journalisées et les données contextuelles.

[Raffinement : cette fonction métier n'existe que si la TOE l'implante]

[Assignement : autres fonctions métier]

VI.2. Fonctions de sécurité

FS1 Chiffrement

La TOE chiffre **[sélection : son système de fichiers, son fichier d'échange, autres]** 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 **[assignement : liste des utilisateurs autorisés]** 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 permet **[assignement : liste des utilisateurs autorisés]** de mettre à jour la base de règles de détection.

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 **[sélection : effectue une rotation, ne journalise plus les opérations effectuées par les utilisateurs et par elle-même mais continue d'assurer sa fonction de détection, n'assure plus sa fonction de détection, autres]**.

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

Seul l'administrateur local est autorisé par la TOE à :

- activer ou désactiver l'envoi d'informations techniques complémentaires par la TOE vers le service de détection des incidents de sécurité ;
- activer ou désactiver le stockage sur la TOE des informations techniques complémentaires ;
- définir la durée maximale de stockage sur la TOE des informations techniques complémentaires ;
- consulter ou récupérer les informations techniques complémentaires stockés sur la TOE.

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

La TOE **[assignement : comportement de la TOE lorsque le débit des flux transmis par le TAP unidirectionnel est supérieur à la capacité de traitement de la TOE]** lorsque le débit des flux transmis par le TAP unidirectionnel est supérieur à la capacité de traitement de la TOE.

La TOE **[assignement : comportement de la TOE lorsque la capacité de rétention des journaux de fonctionnement et d'alertes est atteinte]** lorsque la capacité de rétention des journaux de fonctionnement et d'alertes est atteinte.

[Assignement : autres fonctions de sécurité]

Annexe 1 Liste des tâches associées aux utilisateurs

I. Administrateur Système

L'administrateur système réalise les tâches suivantes :

- mise à jour du système d'exploitation de la TOE ;
- redémarrage de la TOE ;
- **[Sélection : liste des fonctions définies en Annexe 4]**.

II. Administrateur local

L'administrateur local réalise les tâches suivantes :

- lecture des informations relatives aux règles de détection :
  - identifiant de la règle de détection ;
  - propriétaire de la règle de détection ;
  - auteur de la règle de détection ;
  - date de création de la règle de détection ;
  - niveau de sensibilité ou de classification de la règle de détection ;
- activer ou désactiver l'envoi des informations techniques complémentaires aux opérateurs ;
- activer ou désactiver le stockage sur la TOE des informations techniques complémentaires ;
- définir la durée maximale de stockage sur la TOE des informations techniques complémentaires ;
- consulter ou récupérer les informations techniques complémentaires stockés sur la TOE.
- consultation de l'ensemble des journaux de fonctionnement générés par la TOE.
- **[Sélection : liste des fonctions définies en Annexe 4]**.

III. Auditeur

L'auditeur réalise les tâches suivantes :

- lecture des informations relatives aux règles de détection :
  - identifiant de la règle de détection ;
  - propriétaire de la règle de détection ;
  - auteur de la règle de détection ;
  - date de création de la règle de détection ;
  - niveau de sensibilité ou de classification de la règle de détection ;
- consultation des journaux de fonctionnement ;
- **[Sélection : liste des fonctions définies en Annexe 4]**.

IV. Opérateur

L'opérateur réalise les tâches suivantes :

- ajout de règles de détection ;
- suppression de règles de détection ;
- **[Sélection : liste des fonctions définies en Annexe 4]**.

[Assignement : autres utilisateurs si besoin]

Annexe 2 Matrices de couverture

I. Menaces et biens sensibles

		B1 Logiciels de la TOE	B2 Base des utilisateurs	B3 Règles de détection	B4 Métadonnées	B5 Fichiers malveillants	B6 Configuration	B7 Journaux de fonctionnement	B8 Journaux d'alertes	B9 Informations techniques complémentaires nécessaires à la détection	B10 Eléments cryptographiques
M1	Vol		**C**	**C**	**C**	**C**	**C**	**C**	**C**	**C**	**C**
M2	Compromission	**IA**	**CI**	**CI**	**CI**	**CI**	**CI**	**CI**	**CI**	**CI**	**CI**
M3	Contournement	**IA**		**I**				**I**	**I**		
M4	Usurpation d'identité		**CI**								
M5	Elévation de privilèges	**IA**	**CI**	**CI**	**CI**	**CI**	**CI**	**CI**	**CI**	**CI**	**CI**
M6	Indisponibilité	**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**

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	**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 fichiers malveillants et d'informations techniques	**FS8** Cloisonnement	**FS9** Dimensionnement
M1	Vol		×	×							
M2	Compromission			×	×		×	×		×	
M3	Contournement	×				×	×				×
M4	Usurpation d'identité			×			×				
M5	Elévation de privilèges			×	×		×		×		
M6	Indisponibilité	×					×				
M7	Manipulation malveillante de flux							×			

Tableau 3 : Couverture des menaces par les fonctions de sécurité

Annexe 3 Caractéristiques techniques

I. Métadonnées

Métadonnées		Commentaire	Supportée par le produit ?
flux Netflow	ip[2].source		**[Sélection : oui, non]**
	ip.destination		**[Sélection : oui, non]**
	port.source		**[Sélection : oui, non]**
	port.destination		**[Sélection : oui, non]**
	protocole		**[Sélection : oui, non]**
	pkts	Nombre de paquets transmis	**[Sélection : oui, non]**
	bytes	Nombre d'octets transmis	**[Sélection : oui, non]**
	flags	Concaténation de l'ensemble des flags TCP observés	**[Sélection : oui, non]**
	start_date	Date de début	**[Sélection : oui, non]**
	end_date	Date de fin	**[Sélection : oui, non]**
	duration	Durée du flux	**[Sélection : oui, non]**
Session HTTP	timestamp	Date de début de la session	**[Sélection : oui, non]**
	ip.client		**[Sélection : oui, non]**
	ip.serveur		**[Sélection : oui, non]**
	port.client		**[Sélection : oui, non]**
	port.serveur		**[Sélection : oui, non]**
	http[3].request.line.method		**[Sélection : oui, non]**

[2] ip : inclut IPv4 et IPv6

	http.request.line.uri	Brute, c'est-à-dire sans aucun décodage.	**[Sélection : oui, non]**
	http.request.header.user_agent		**[Sélection : oui, non]**
	http.request.header.referer		**[Sélection : oui, non]**
	http.request.body.length	Volume de payload HTTP envoyé au serveur	**[Sélection : oui, non]**
	http.response.status.code	Code retour	**[Sélection : oui, non]**
	http.response.header.server	Server agent	**[Sélection : oui, non]**
	http.response.body.length	Volume de payload HTTP retourné	**[Sélection : oui, non]**
	http.response.body.mime_type	Type mime du contenu envoyé par le serveur	**[Sélection : oui, non]**
Requêtes DNS	timestamp		**[Sélection : oui, non]**
	ip.source		**[Sélection : oui, non]**
	ip.destination		**[Sélection : oui, non]**
	port.source		**[Sélection : oui, non]**
	port.destination		**[Sélection : oui, non]**
	dns.query.name		**[Sélection : oui, non]**
	dns.query.type		**[Sélection : oui, non]**
	dns.query.txid		**[Sélection : oui, non]**
	dns.response.flags	Format hexadécimal	**[Sélection : oui, non]**
	dns.response.flags.rcode	Format hexadécimal	**[Sélection : oui, non]**
Réponses DNS	timestamp		**[Sélection : oui, non]**
	ip.source		**[Sélection : oui, non]**
	ip.destination		**[Sélection : oui, non]**
	port.source		**[Sélection : oui, non]**
	port.destination		**[Sélection : oui, non]**

[3] Inclut HTTP/1.0, HTTP/1.1 HTTP/2 et les compressions http.

	dns.response.record.name		**[Sélection : oui, non]**
	dns.response.record.type		**[Sélection : oui, non]**
	dns.response.record.ttl		**[Sélection : oui, non]**
	dns.response.record.value		**[Sélection : oui, non]**
sessions SMTP	timestamp		**[Sélection : oui, non]**
	ip.client		**[Sélection : oui, non]**
	ip.serveur		**[Sélection : oui, non]**
	port.client		**[Sélection : oui, non]**
	port.serveur		**[Sélection : oui, non]**
	smtp.command.helo		**[Sélection : oui, non]**
	smtp.command.mail_from	A minima le nom de domaine de l'adresse mail vu dans la commande MAIL FROM	**[Sélection : oui, non]**
	smtp.command.rcpt_to	A minima l'ensemble des noms de domaines des adresses mails vus dans la commande RCPT TO séparés par des ','	**[Sélection : oui, non]**
	smtp.data.header.from	A minima le nom de domaine de l'adresse mail vu dans la commande MAIL FROM	**[Sélection : oui, non]**
	smtp.data.header.to	A minima l'ensemble des noms de domaines des adresses mails séparés par des ','	**[Sélection : oui, non]**
	smtp.data.header.reply-to	A minima le nom de domaine de l'adresse mail	**[Sélection : oui, non]**
	smtp.data.header.cc	A minima l'ensemble des noms de domaines des adresses mails séparés par des ','	**[Sélection : oui, non]**
	smtp.data.header.bcc	A minima l'ensemble des noms de domaines des adresses mails séparés par des ','	**[Sélection : oui, non]**
	smtp.data.header.cci	A minima l'ensemble des noms de domaines des adresses mails séparés par des ','	**[Sélection : oui, non]**
	smtp.data.header.subject_md5	**[Assignement : préciser le ou les algorithmes d'empreintes numériques]** du sujet du mail	**[Sélection : oui, non]**
	smtp.data.header.message-id		**[Sélection : oui, non]**

	smtp.data.header.x-mailer		**[Sélection : oui, non]**
	smtp.data.header.user-agent		**[Sélection : oui, non]**
	smtp.data.header.x-originating-ip		**[Sélection : oui, non]**
	smtp.data.header.relays	Liste des relais IP/domaine du mail séparés par des ','	**[Sélection : oui, non]**
	smtp.data.body_md5	MD5 du corps du message ; *attention* MD5 du texte brut uniquement si présent, MD5 du texte enrichi si pas de texte brut, "NULL" si pas de contenu ; ne pas intégrer les pièces jointes dans le calcul	**[Sélection : oui, non]**
	smtp.attachments	Liste des **[Assignement : préciser le ou les algorithmes d'empreintes numériques]** des fichiers attachés séparés par des ','	**[Sélection : oui, non]**
les métadonnées liées aux fichiers	timestamp		**[Sélection : oui, non]**
	ip.source		**[Sélection : oui, non]**
	ip.destination		**[Sélection : oui, non]**
	port.source		**[Sélection : oui, non]**
	port.destination		**[Sélection : oui, non]**
	ip.proto		**[Sélection : oui, non]**
	file.size		**[Sélection : oui, non]**
	file.md5		**[Sélection : oui, non]**
	file.extension	Extension du fichier	**[Sélection : oui, non]**
	file.type	Type déterminé par les analyseurs syntaxiques	**[Sélection : oui, non]**
	file.magic		**[Sélection : oui, non]**
	file.parent.md5	**[Assignement : préciser le ou les algorithmes d'empreintes numériques]** du conteneur du fichier, i.e l'archive contenant le fichier	**[Sélection : oui, non]**
Certificats X509	timestamp		**[Sélection : oui, non]**
	ip.source		**[Sélection : oui, non]**
	ip.destination		**[Sélection : oui, non]**

	port.source		**[Sélection : oui, non]**
	port.destination		**[Sélection : oui, non]**
	ip.proto		**[Sélection : oui, non]**
	hostname		**[Sélection : oui, non]**
	certificate.md5 (haché du certificat)		**[Sélection : oui, non]**
	certificate.body (contenu du certificat)		**[Sélection : oui, non]**
	certificate.version		**[Sélection : oui, non]**
	certificate.serial_number		**[Sélection : oui, non]**
	certificate.signature_algorithm		**[Sélection : oui, non]**
	certificate.issuer.cn		**[Sélection : oui, non]**
	certificate.issuer.o		**[Sélection : oui, non]**
	certificate.issuer.ou		**[Sélection : oui, non]**
	certificate.issuer.c		**[Sélection : oui, non]**
	certificate.validity.not_before		**[Sélection : oui, non]**
	certificate.validity.not_after		**[Sélection : oui, non]**
	certificate.subject.cn		**[Sélection : oui, non]**
	certificate.subject.o		**[Sélection : oui, non]**
	certificate.subject.ou		**[Sélection : oui, non]**
	certificate.subject.c		**[Sélection : oui, non]**
	certificate.subject_public_key.public_key_algorithm		**[Sélection : oui, non]**
	certificate.standard_extensions.basic_constraints		**[Sélection : oui, non]**
	certificate.standard_extensions.name_constraints		**[Sélection : oui, non]**
	certificate.standard_extensions.policy_constraints		**[Sélection : oui, non]**
	certificate.standard_extensions.key_usage		**[Sélection : oui, non]**
	certificate.standard_extensions.extended_key_usage		**[Sélection : oui, non]**

	certificate.standard_extensions.subject_key_identifier		**[Sélection : oui, non]**
	certificate.standard_extensions.authority_key_identifier		**[Sélection : oui, non]**
	certificate.standard_extensions.subject_alternative_name		**[Sélection : oui, non]**
	certificate.standard_extensions.issuer_alternative_name		**[Sélection : oui, non]**
	certificate.standard_extensions.subject_directory_attributes		**[Sélection : oui, non]**
	certificate.standard_extensions.crl_distribution_points		**[Sélection : oui, non]**
	certificate.standard_extensions.inhibit_any_policy		**[Sélection : oui, non]**
	certificate.standard_extensions.private_key_usage_period.not_before		**[Sélection : oui, non]**
	certificate.standard_extensions.private_key_usage_period.not_after		**[Sélection : oui, non]**
	certificate.standard_extensions.certificate_policies		**[Sélection : oui, non]**
	certificate.standard_extensions.policy_mappings		**[Sélection : oui, non]**
	certificate.signature.signature_algorithm		**[Sélection : oui, non]**

II. Extraction de fichiers

Format de fichiers	Supporté par le produit ?
PDF	**[Sélection : oui, non]**
DOC	**[Sélection : oui, non]**
XLS	**[Sélection : oui, non]**
PPT	**[Sélection : oui, non]**
RTF	**[Sélection : oui, non]**
HTML	**[Sélection : oui, non]**
JS	**[Sélection : oui, non]**
SWF	**[Sélection : oui, non]**
AS 2.3	**[Sélection : oui, non]**

GIF	**[Sélection : oui, non]**
PNG	**[Sélection : oui, non]**
JPEG	**[Sélection : oui, non]**
TIFF	**[Sélection : oui, non]**
JAR	**[Sélection : oui, non]**
Fichier d'aide Windows (HLP)	**[Sélection : oui, non]**
[Assignement : autres formats de fichiers]	**[Sélection : oui, non]**

Annexe 4 Liste des tâches

[Raffinement : une même tâche peut être affectée à plusieurs profils d'utilisateur. Cette annexe est à supprimer une fois l'Annexe 1 complétée.]

Configuration réseau

- consultation de la configuration réseau de la TOE ;
- édition de la configuration réseau de la TOE ;
- mise à jour des règles de détection de la TOE.

Règles de détection

- ajout de règles de détection ;
- suppression de règles de détection ;
- édition des règles de détection ;
- activation ou désactivation de règles de détection ;
- consultation des informations relatives aux règles de détection :

[Sélection :
  - **un identifiant unique de la règle de détection ;**
  - **le propriétaire de la règle de détection ;**
  - **l'auteur de la règle de détection ;**
  - **la source de la règle de détection ;**
  - **la date de création de la règle de détection ;**
  - **la description de la règle de détection ;**
  - **les phases d'attaque détectées par la règle ;**
  - **le niveau de sensibilité ou de classification de la règle de détection ;**
  - **les modalités de diffusion de la règle de détection ;**
  - **les modalités de gestion de la règle de signature ;**
  - **une description de la méthode d'analyse des évènements ;**
  - **la possibilité ou non de réaliser des recherches en sources ouvertes ;**
  - **les descriptions et/ou les identifiants des vulnérabilités (CVE par exemple) dont les tentatives d'exploitation ou les exploitations sont détectées par la règle ;**
  - **les consignes à appliquer en cas de déclenchement de la règle de détection.]**

- consultation de l'état (activé ou non) de l'option d'extraction d'informations techniques complémentaires vers les opérateurs ;
- consultation de l'état (activé ou non) de l'option d'envoi d'informations techniques complémentaires vers les opérateurs ;
- consultation de la durée maximale de stockage sur la TOE des informations techniques complémentaires.

Gestion des éléments cryptographiques

- gestion (création, import, export, destruction, etc.) des éléments cryptographiques de la TOE.

Version

- consultation de la version de la TOE.

Mise à jour des logiciels

- mise à jour des logiciels de la TOE ;
- consultation de la liste des logiciels de la TOE et de leur version.

Mise à jour système

- mise à jour du système d'exploitation de la TOE ;
- consultation de la version du système d'exploitation de la TOE.

Gestion du temps de référence

- consultation du temps de référence de la TOE ;
- édition du temps de référence de la TOE.

Journaux de fonctionnement

- consultation des journaux de fonctionnement générés par la TOE ;
- suppression des journaux de fonctionnement générés par la TOE.

Journaux d'alertes

- consultation des journaux d'alertes générés par la TOE ;
- suppression des journaux d'alertes générés par la TOE.

Gestion des utilisateurs

- création des comptes associés aux rôles [assignement : liste des rôles] ;
- suppression des comptes associés aux rôles [assignement : liste des rôles] ;
- modification des comptes associés aux rôles [assignement : liste des rôles] ;
- consultation des attributs [assignement : liste des attributs] des comptes associés aux rôles [assignement : liste des rôles] ;
- édition des attributs [assignement : liste des attributs] des comptes associés aux rôles [assignement : liste des rôles].

Arrêt et démarrage des fonctions métier

- arrêt des fonctions métier de la TOE ;
- démarrage des fonctions métier de la TOE ;
- redémarrage des fonctions métier de la TOE.

Arrêt et démarrage

- arrêt de la TOE ;
- démarrage de la TOE ;
- redémarrage de la TOE.

Supervision du fonctionnement

- consultation des statistiques de fonctionnement de la TOE : **[assignement : lister les statistiques]**.

[Assignement : autres tâches]