SESAME IT

LEAVE ATTACKERS NOWHERE TO HIDE

Société : SESAME IT

Produit : JIZÔ

Sonde réseau de détection des incidents de sécurité

Cible de sécurité

SOMMAIRE

I. HISTORIQUE DE REVISION 3
II. INTRODUCTION 4
II.1. Objet du document 4
II.2. Identification du produit 4
II.3. Acronymes 4
II.4. Glossaire 4
II.5. Documents applicables 4
III. DESCRIPTION DU PRODUIT 6
III.1. Description de la manière d'utiliser le produit 6
III.2. Description de l'environnement prévu pour son utilisation 7
III.3. Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système non fournis avec le produit 8
III.4. Description des utilisateurs typiques concernés 8
III.5. Description du périmètre de l'évaluation 8
IV. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT 9
V. DESCRIPTION DES BIENS SENSIBLES 11
VI. DESCRIPTION DES MENACES 13
VI.1. Profils des attaquants 13
VI.2. Menaces 13
VII. DESCRIPTION DES FONCTIONS DU PRODUIT 15
VII.1. Fonctions métier 15
VII.2. Fonctions de sécurité 16
ANNEXE 1 LISTE DES TACHES ASSOCIEES AUX UTILISATEURS 17
1.1. Opérateur 17
1.2. Opérateur Console 17
1.3. Administrateur sécurité 17
1.4. Auditeur 17
1.5. Administrateur local 18
1.6. Administrateur Système 18
1.7. Administrateur Réseau 18
1.8. Administrateur Update 19
ANNEXE 2 MATRICES DE COUVERTURE 20
1. Menaces et biens sensibles 20
1.1. Menaces et fonctions de sécurité 21
ANNEXE 3 CARACTERISTIQUES TECHNIQUES 22
1. Métadonnées 22
1.1. Extraction de fichiers 27

I. HISTORIQUE DE REVISION

Reference du Document	Auteur	Date d'édition	Ver./Rev.	Modifications apportées
Profil de Protection CSPN Sesame it	JGY	10/2020	V8A	Création
Profil de Protection CSPN Sesame it	JGY	11/2020	V9B	Correction
Profil de Protection CSPN Sesame it	JGY	09/12/2021	V10	Mise à jour
Profil de Protection CSPN Sesame it	AHL	15/02/2024	V11	Mise à jour
Profil de Protection CSPN Sesame it	AHL	19/02/2024	V12	Mise à jour

II. INTRODUCTION

II.1. OBJET DU DOCUMENT

Le présent document constitue la cible de sécurité du produit **Jizô** dans sa version **12.04.02** développé par **SESAME IT** dans le cadre d'une Certification de Sécurité de Premier Niveau (CSPN).

II.2. IDENTIFICATION DU PRODUIT

Éditeur	**SESAME IT**
Lien vers l'éditeur	**https://www.sesame-it.com**
Nom commercial du produit	**JIZÔ**
Numéro de la version du produit	**12.04.02**
Catégorie de produit	Détection d'intrusion réseau

Note : 12.XX.YY

- XX = version majeure
- YY = version mineure

II.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*

II.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.

II.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

Renvoi	Document
[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

III. DESCRIPTION DU PRODUIT

III.1. DESCRIPTION DE LA MANIERE D'UTILISER LE PRODUIT

La sonde Jizô est une solution logicielle (installée sur un serveur Intel) de détection d'intrusion réseau (IDS) développée par la société Sesame-IT. La sonde Jizô analyse le flux réseau et remonte des alertes et des métadonnées et extrait des fichiers dans les flux.
La sonde Jizô possède 6 interfaces de capture, pour un débit maximum traité de 12 Gbps :

- 2 interfaces de capture 10 GE ;
- 4 interfaces de capture 1 GE.

La sonde Jizô s'installe derrière un ou plusieurs TAP(s) unidirectionnel(s) et un chiffreur sur le réseau à surveiller.

La sonde est opérée et administrée via 8 profils utilisateurs :

- Les utilisateurs de la sonde qui sont situés dans le système d'information du service de détection et du client :
  - Opérateur ;
  - Opérateur Console.
  - Administrateur Sécurité ;
  - Auditeur ;
  - Administrateur local.
- Les administrateurs du système :
  - Administrateur Système ;
  - Administrateur Réseau ;
  - Administrateur Update.

Elle met à la disposition de certains profils (Administrateur sécurité, Administrateur local, Auditeur et Opérateur) sur la sonde :

- Des alarmes de fonctionnement concernant la sonde (informations liée à la maintenance);
- Des journaux d'utilisation et de fonctionnement ;
- Des alertes liées à la détection sur signature ;
- Des statistiques de fonctionnement de la sonde.

Elle peut aussi transférer ces informations vers un outil centralisé.

La sonde Jizô propose les fonctionnalités métier suivantes :

- Détection d'intrusion basée sur l'utilisation de signatures ;
- Génération de métadonnées ;
- Extraction de fichiers ;
- Mécanisme de remontée d'alertes ;
- Mécanisme de transfert de métadonnées et de fichiers extraits.

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.

III.2. DESCRIPTION DE L'ENVIRONNEMENT PREVU POUR SON UTILISATION

La sonde Jizô est connectée au réseau en dérivation.

Les flux bruts du réseau sont capturés par la sonde grâce à 6 TAPs unidirectionnels.

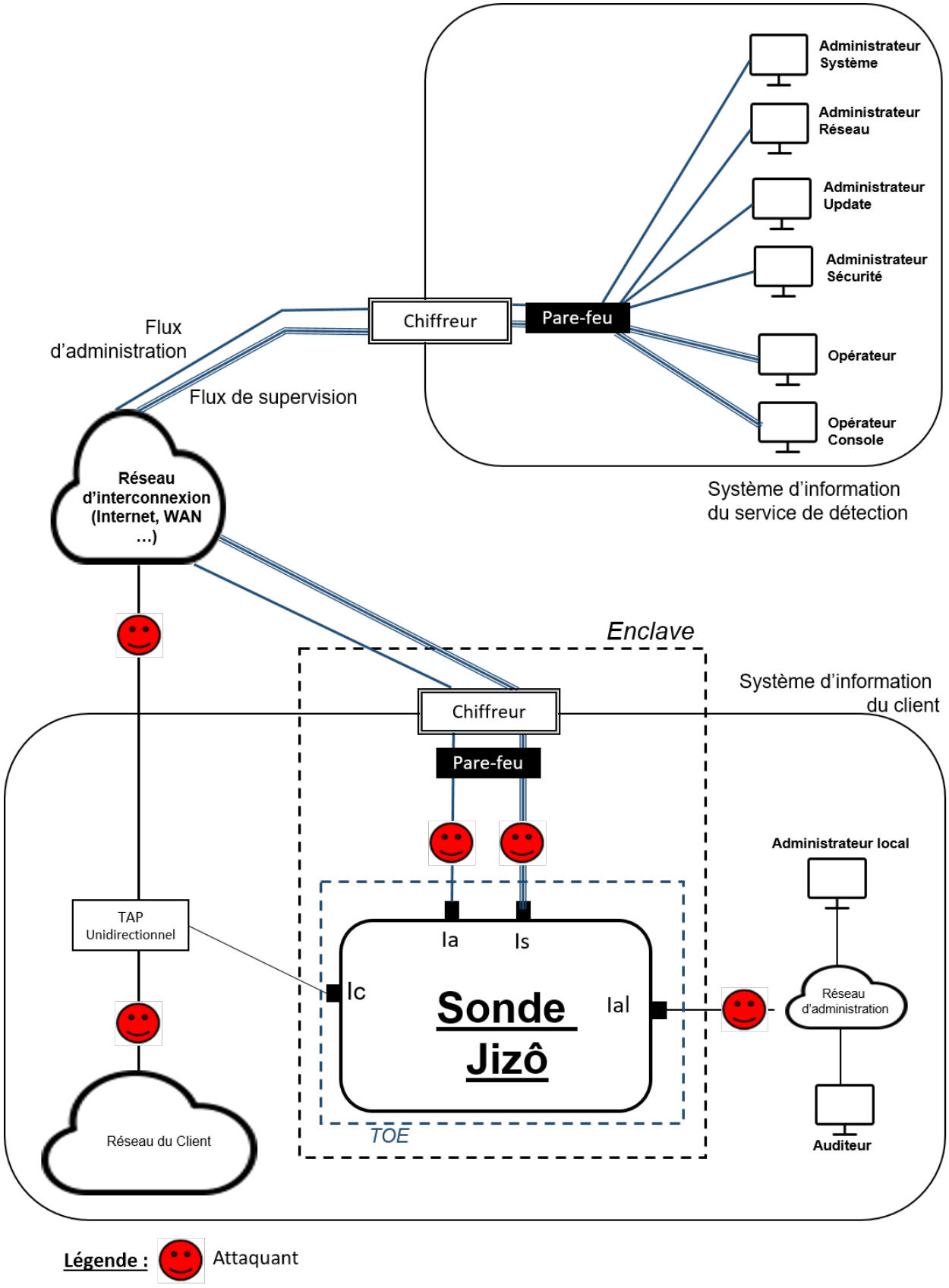


Figure 1: Environnement d'utilisation du produit

III.3. DESCRIPTION DES DEPENDANCES PAR RAPPORT A DES MATERIELS, DES LOGICIELS ET/OU DES MICROPROGRAMMES DU SYSTEME NON FOURNIS AVEC LE PRODUIT

Liste de dépendances logicielles non fournies :

- Suricata (Stable) version 6.0.4 (recompilée);
- Debian 11

Liste des dépendances matérielles non fournies :

- Server HPE ProLiant DL360 Gen10:
  - 2 x Intel Xeon-Silver 4108 (1.8GHz_8-core_85W) ;
  - 16 x 16GB (1x16GB) Dual Rank x8 DDR4-2666 ;
  - 3 x 600GB SAS 12G Enterprise 15K ;
  - Lecteur optique HP SATA DVD-ROM ;
  - 1 x Ethernet 10 Go 2 ports 562SFP+ ;
  - FlexFabric 10Gb 2-port 534FLR-SFP+ ;
  - Smart Array P408i-a SR Gen10 ;
  - 2 x 800W Flex Slot Platinum Hot Plug ;
  - Trusted Platform Module 2.0 Gen10 ;
  - iLO Adv.

III.4. DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNES

La TOE gère les utilisateurs suivants :

- opérateur ;
- opérateur Console ;
- administrateur Sécurité ;
- auditeur ;
- administrateur local ;
- administrateur système ;
- administrateur Réseau ;
- administrateur Update ;

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

III.5. DESCRIPTION DU PERIMETRE DE L'EVALUATION

Le périmètre de l'évaluation est constitué de la TOE et de ses **9** interfaces réseau.

- Interfaces de collecte (Ic) : 4 interfaces 1 GE et 2 interfaces 10 GE, débit maximum traité de 12 Gbps ;
- Interface de supervision (Is) ;
- Interface d'administration (Ia) ;
- Interface d'administration locale (Ial).

Le périmètre de l'évaluation est représenté au chapitre 0.

IV. DESCRIPTION DES HYPOTHESES 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 **9** interfaces réseau physiques différentes et conformément au schéma du chapitre 0 :

- l'interface $\mathbf{I_c}$ reçoit les flux en provenance du TAP unidirectionnel. La sonde Jizô possède 6 interfaces $\mathbf{I_c}$;
- l'interface $\mathbf{I_{al}}$ est connectée au système d'information du client et permet aux administrateurs local at auditeur d'effectuer leurs tâches. La sonde Jizô possède 1 interface $\mathbf{I_{al}}$;
- l'interface $\mathbf{I_a}$ est connectée au système d'information du service de détection et permet aux Administrateurs Système, Administrateur Sécurité, Administrateur Réseau et Administrateur Update d'effectuer leurs tâches. La sonde Jizô possède 1 interfaces $\mathbf{I_a}$;
- l'interface $\mathbf{I_s}$ est connectée au système d'information du service de détection et permet aux Opérateurs et Opérateurs Console d'effectuer leurs tâches. La sonde Jizô possède 1 interface $\mathbf{I_s}$.

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.

V. 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.
Non Applicable

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 (fichiers extraits). Ce bien est à protéger en disponibilité, confidentialité et intégrité.

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 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.

VI. DESCRIPTION DES MENACES

VI.1. PROFILS DES ATTAQUANTS

Les attaquants à considérer pour l'évaluation sont :

- les utilisateurs de la TOE suivants :
  - opérateur ;
  - opérateur Console.
  - administrateur Sécurité ;
  - auditeur ;
  - administrateur local ;
  - administrateur Système ;
  - administrateur Réseau ;
- toute personne malveillante connectée sur le réseau du client et pouvant ainsi interagir avec la TOE via son interface réseau I_c ;
- toute personne malveillante située entre la TOE et le chiffreur et pouvant ainsi interagir avec la TOE via ses interfaces réseau I_a et I_s ;
- 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_c ;
- 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_{al} ;
- 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.

VI.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 Élévation de privilèges

Un auditeur, un administrateur local, un opérateur, un Administrateur Système, un Administrateur Sécurité, un Administrateur Réseau ou un Opérateur Console 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.

VII. DESCRIPTION DES FONCTIONS DU PRODUIT

Les fonctions de la TOE sont les suivantes :

VII.1. FONCTIONS METIER

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 3. Lorsque la capacité de stockage maximale est atteinte, la TOE **effectue une rotation et continue d'assurer sa fonction de détection.**

FM4 Analyse réseau

La TOE analyse les flux bruts, les flux décodés et les métadonnées journalisées par **reconnaissance de motifs et reconnaissance de protocoles**. 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 **correspondance avec une règle de détection**. 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 et continue d'assurer sa fonction de détection.**

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 **individuellement au fil de l'eau.**

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 **individuellement au fil de l'eau.**

FM9 Corrélation

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

Non Applicable

VII.2. FONCTIONS DE SECURITE

FS1 Chiffrement

La TOE chiffre son système de fichiers, son fichier d'échange (swap), 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 Update 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 **aux profils opérateurs** 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 **effectue une rotation et continue d'assurer sa fonction de détection**.

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 (fichiers extraits) 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 stockées 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 traite le flux jusqu'au limite de dimensionnent, lorsque le débit des flux transmis par le TAP unidirectionnel est supérieur à la capacité de traitement, le flux supplémentaire n'est pas analysé et la sonde Jizô fonctionne partiellement.

  La TOE continue d'assurer sa fonction de détection lorsque la capacité de rétention des journaux de fonctionnement et d'alertes est atteinte.

ANNEXE 1 LISTE DES TACHES ASSOCIEES AUX UTILISATEURS

1.1. OPERATEUR

L'opérateur réalise les tâches suivantes :

- ajout de règles de détection ;
- suppression de règles de détection ;
- édition des règles de détection ;
- consultation des alertes et des logs metadata;
- consultation du dashboard de synthèse des alertes et de l'état du système ;
- consultation et export des logs rules (actions sur les règles).

Retiré : consultation des alarmes et des statistiques de fonctionnement de la sonde

1.2. OPERATEUR CONSOLE

L'opérateur Console réalise les tâches suivantes :

- ajout de règles de détection ;
- suppression de règles de détection ;
- édition des règles de détection.

1.3. ADMINISTRATEUR SECURITE

L'Administrateur Sécurité réalise les tâches suivantes :

- consultation de l'ensemble des journaux de fonctionnement générés par la TOE.
- Gestion des utilisateurs :
    - Création des comptes associés aux rôles : Administrateur sécurité, Opérateur, Auditeur
    - Suppression des comptes associés aux rôles : Administrateur sécurité, Opérateur, Auditeur
    - Modification des comptes associés aux rôles : Administrateur sécurité, Opérateur, Auditeur
    - Consultation/édition des attributs associés aux rôles : Administrateur sécurité, Opérateur, Auditeur

        Liste des attributs :
        - Activation/desactivation du compte
        - Adresse IP
        - Numéro de port
        - Identifiant de connexion/username
        - Activation/desactivation de l'accès au dashboard
        - Ré-activation du compte après 5 échecs de connexion
- Consultation des logs d'activité et export
- Consultation des statistiques de fonctionnement de la sonde Jizô ;
- Consultation des alarmes de fonctionnement (alarmes liées à la maintenance) de la sonde Jizô ;
- Consultation du dashboard de synthèse de l'état du système (état de la sonde et nombre d'alertes, sous forme d'histogramme, par type de protocole sur 30j max)

  Retiré : consultation des règles de détection

1.4. 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 ;
    - retiré : auteur et niveau de sensibilité de la règle de détection
- consultation des journaux de fonctionnement : users logs et rules logs.

1.5. 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 stockées sur la TOE.
- consultation de l'ensemble des journaux de fonctionnement générés par la TOE.
- 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.

1.6. ADMINISTRATEUR SYSTEME

L'administrateur système réalise les tâches suivantes :

- consultation de la liste des logiciels de la TOE et de leur version;
- consultation de la version du système d'exploitation de la TOE;
- arrêt de la TOE;
- redémarrage de la TOE;
- arrêt des fonctions métier de la TOE, unitaire ou global;
- démarrage des fonctions métier de la TOE, unitaire ou global;
- redémarrage des fonctions métier de la TOE, unitaire ou global;
- consultation du temps de référence de la TOE;
- édition du temps de référence de la TOE.

1.7. ADMINISTRATEUR RESEAU

L'Administrateur Réseau réalise les tâches suivantes :

- modification du nom de la sonde de la TOE ;
- modification de la configuration réseau de la TOE ;

- édition de la configuration réseau de la TOE ;
- redémarrage du réseau de la TOE ;
- arrêt des fonctions métier de la TOE ;
- démarrage des fonctions métier de la TOE ;
- redémarrage des fonctions métier de la TOE.

1.8. ADMINISTRATEUR UPDATE

L'Administrateur Update réalise les tâches suivantes :

- mise à jour du système d'exploitation de la TOE ;
- mise à jour des logiciels de la TOE;
- redémarrage de la TOE;
- gestion des éléments cryptographiques de la TOE (certificats et clés).

ANNEXE 2 MATRICES DE COUVERTURE

1. 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

1.1. MENACES ET FONCTIONS DE SECURITE

		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 CARACTERISTIQUES TECHNIQUES

1. METADONNEES

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

[2] ip : inclut IPv4 et IPv6

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

	http.request.header.user_agent		**oui**
	http.request.header.referer		**oui**
	http.request.body.length	Volume de payload HTTP envoyé au serveur	**oui**
	http.response.status.code	Code retour	**oui**
	http.response.header.server	Server agent	**non**
	http.response.body.length	Volume de payload HTTP retourné	**non**
	http.response.body.mime_type	Type mime du contenu envoyé par le serveur	**non**
Requêtes DNS	timestamp		**oui**
	ip.source		**oui**
	ip.destination		**oui**
	port.source		**oui**
	port.destination		**oui**
	dns.query.name		**oui**
	dns.query.type		**oui**
	dns.query.txid		**oui**
Réponses DNS	timestamp		**oui**
	ip.source		**oui**
	ip.destination		**oui**
	port.source		**oui**
	port.destination		**oui**
	dns.response.record.name		**oui**
	dns.response.record.type		**oui**
	dns.response.record.ttl		**oui**
	dns.response.record.value		

	dns.response.flags	Format hexadécimal	**oui**
	dns.response.flags.rcode	Format hexadécimal on l'a en libellé texte (pas hexa)	**oui**
sessions SMTP	timestamp		**oui**
	ip.client		**oui**
	ip.serveur		**oui**
	port.client		**oui**
	port.serveur		**oui**
	smtp.command.helo		**oui**
	smtp.command.mail_from	A minima le nom de domaine de l'adresse mail vu dans la commande MAIL FROM	**oui**
	smtp.command.rcpt_to	A minima l'ensemble des noms de domaines des adresses mails vus dans la commande RCPT TO séparés par des ','	**oui**
	smtp.data.header.from	A minima le nom de domaine de l'adresse mail vu dans la commande MAIL FROM	**oui**
	smtp.data.header.to	A minima l'ensemble des noms de domaines des adresses mails séparés par des ','	**oui**
	smtp.data.header.reply-to	A minima le nom de domaine de l'adresse mail	**oui**
	smtp.data.header.cc	A minima l'ensemble des noms de domaines des adresses mails séparés par des ','	**oui**
	smtp.data.header.bcc	A minima l'ensemble des noms de domaines des adresses mails séparés par des ','	**oui**
	smtp.data.header.cci	A minima l'ensemble des noms de domaines des adresses mails séparés par des ','	**oui**
	smtp.data.header.subject_md5	**MD5** du sujet du mail	**oui**

	smtp.data.header.message-id		**oui**
	smtp.data.header.x-mailer		**oui**
	smtp.data.header.user-agent		**oui**
	smtp.data.header.x-originating-ip		**oui**
	smtp.data.header.relays	Liste des relais IP/domaine du mail séparés par des ','	**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	**oui**
	smtp.attachments	MD5 des fichiers attachés séparés par des ','	**oui**
les métadonnées liées aux fichiers	timestamp		**oui**
	ip.source		**oui**
	ip.destination		**oui**
	port.source		**oui**
	port.destination		**oui**
	ip.proto		**oui**
	file.size		**oui**
	file.md5		**oui**
	file.extension	Extension du fichier	**oui**
	file.type	Type déterminé par les analyseurs syntaxiques.	**N/A**
	file.magic		**oui**
	file.parent.md5	**MD5** du conteneur du fichier, i.e l'archive contenant le fichier	**N/A**
Certificats X509	timestamp		**oui**
	ip.source		**oui**

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

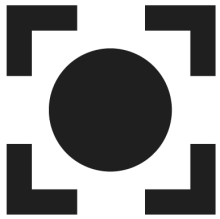
	certificate.standard_extensions.subject_key_identifier		**non**
	certificate.standard_extensions.authority_key_identifier		**non**
	certificate.standard_extensions.subject_alternative_name		**non**
	certificate.standard_extensions.issuer_alternative_name		**non**
	certificate.standard_extensions.subject_directory_attributes		**non**
	certificate.standard_extensions.crl_distribution_points		**non**
	certificate.standard_extensions.inhibit_any_policy		**non**
	certificate.standard_extensions.private_key_usage_period.not_before		**non**
	certificate.standard_extensions.private_key_usage_period.not_after		**non**
	certificate.standard_extensions.certificate_policies		**non**
	certificate.standard_extensions.policy_mappings		**non**
	certificate.signature.signature_algorithm		**non**

1.1. EXTRACTION DE FICHIERS

Format de fichiers	Supporté par le produit ?
PDF	**oui**
DOC	**oui**
XLS	**oui**
PPT	**oui**
RTF	**oui**
HTML	**oui**
JS	**oui**
SWF	**oui**
AS 2.3	**oui**

GIF	**oui**
PNG	**oui**
JPEG	**oui**
TIFF	**oui**
JAR	**oui**
Fichier d'aide Windows (HLP)	**oui**

SESAME IT



LEAVE ATTACKERS NOWHERE TO HIDE