

PROFIL DE FONCTIONNALITÉS ET DE SÉCURITÉ - SAS ET STATION BLANCHE (RÉSEAUX NON CLASSIFIÉS)

GUIDE ANSSI

ANSSI-PG-076
01/07/2020



Informations



Attention

Ce document rédigé par l'ANSSI présente les « **Profil de fonctionnalités et de sécurité - Sas et station blanche (réseaux non classifiés)** ». Il est téléchargeable sur le site www.ssi.gouv.fr.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence ouverte v2.0 » publiée par la mission Etalab [6].

Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

Ces recommandations n'ont pas de caractère normatif, elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	01/07/2020	Version initiale

Table des matières

1 Introduction	3
1.1 Contexte et objectif	3
1.2 Objet du document	3
1.3 Définitions	4
1.4 Abréviations	4
2 Descriptif du produit	5
2.1 Descriptif général du produit	5
2.2 Environnement d'utilisation	5
2.3 Périmètre du produit	6
2.3.1 Matériel	6
2.3.2 Logiciel	6
2.4 Descriptif des utilisateurs	6
3 Hypothèses	7
3.1 Hypothèses sur l'environnement	7
3.2 Hypothèses sur le produit	7
4 Biens sensibles à protéger	8
4.1 Biens sensibles du produit	8
4.2 Biens sensibles de l'environnement	9
5 Menaces	11
5.1 Profils des attaquants	11
5.2 Descriptif des menaces	11
6 Fonctions du produit	13
6.1 Fonctions de sécurité du produit	13
Annexe A Matrices de couverture	20
A.1 Couverture des biens par les menaces	21
A.2 Couverture des menaces par les fonctions de sécurité	22
Annexe B Exemple : Station blanche à deux clés	23
B.1 Environnement d'utilisation	23
B.2 Périmètre du produit	23
B.3 Menaces	24
B.3.1 Profils des attaquants	24
Annexe C Exemple : Sas	26
C.1 Environnement d'utilisation	26
C.2 Périmètre du produit	26
C.3 Menaces	27
C.3.1 Profils des attaquants	27
Bibliographie	29

1

Introduction

1.1 Contexte et objectif

Les menaces liées à la connexion de périphériques amovibles dans les systèmes d'information sont diverses :

- insertion d'un fichier malveillant dans le système d'information à protéger ;
- attaque en intégrité/confidentialité lors du transfert du fichier sur un média amovible ;
- média réalisant des attaques au niveau de la pile logicielle du média amovible ;
- média réalisant des attaques en déni de service au niveau du contrôleur de média ;
- média se comportant comme un périphérique de type clavier ou souris et permettant de véhiculer des fichiers malveillants sur le système d'information à protéger.

Dans certains cas, le périphérique amovible est le seul moyen de transférer des informations d'un système à un autre (cas des systèmes isolés par exemple). Ce constat impose aux entités de se protéger en installant des outils spécifiques au sein de leur système d'information pour prévenir les risques liés à ces médias.



Information

L'utilisation d'équipements de type sas ou station blanche doit se faire dans un objectif global de contrôle des médias amovibles. En effet, le déploiement de tels équipements n'est pas suffisant et doit être accompagné de mesures organisationnelles définissant la politique de gestion des médias amovibles (limitation de l'usage des médias amovibles, désactivation des ports des médias amovibles sur les postes non dédié à ces transferts, etc.).

1.2 Objet du document

Le présent document constitue le profil de fonctionnalités et de sécurité pour les sas et les stations blanches. Il a pour objectif de définir les fonctions de sécurité attendues et les exigences associées à ce type de produit. C'est un élément de doctrine destiné à aider les clients dans leur expression du besoin et les éditeurs dans la conception de leur produit.

Les éditeurs doivent l'utiliser comme profil de protection tout en respectant les exigences qui y sont décrites dès lors qu'ils souhaitent présenter ce type de produit en qualification.



Attention

Cette version traite de l'import des données sur des réseaux non classifiés. L'export des données et les réseaux classifiés ne sont pas traités dans ce document.

1.3 Définitions



Exigence

Contrainte sur une fonction.



Point d'insertion de données

Poste de travail ou serveur dont les ports de médias amovibles sont au moins en partie ouverts afin de permettre l'import de données vers le réseau opérationnel.



Station blanche

Poste de travail ou serveur isolé du réseau opérationnel, dédié à l'analyse anti-malware des médias amovibles et des données qui y sont stockées. Ce dispositif donne des garanties raisonnables quant à l'innocuité du média amovible et des données transférées vers le réseau opérationnel.



Sas d'import de données

Association d'une station blanche et d'un point d'insertion de données. Lors d'un import de données, l'utilisation de la station blanche et du point d'insertion de données est impératif. La station blanche et le point d'insertion de données sont physiquement cloisonnés. Ce dispositif, interconnecté au réseau opérationnel, garantit l'innocuité du média amovible et des données transférées à destination de ce réseau.

1.4 Abréviations

- **HID** : Human interface Device. Il s'agit d'un périphérique informatique utilisé par un humain (clavier, souris, etc.).
- **PID** : Point d'insertion de données.
- **SI** : Système d'information.

2

Descriptif du produit

2.1 Descriptif général du produit

Le produit considéré est un sas d'import de données ou une station blanche destiné à assurer un contrôle des supports amovibles et des données présentes. Seules les données sélectionnées par l'opérateur pourront être transférées vers un réseau opérationnel. Le produit doit agir en coupure pour éviter, autant que possible, l'insertion sur le réseau opérationnel d'éléments non conformes à la politique de sécurité.

2.2 Environnement d'utilisation

L'environnement du produit, ainsi que les attaquants menaçant les biens sensibles à protéger, sont décrits selon la figure 1 (les attaquants sont positionnés selon les cas d'usage conformément aux annexes B et C du présent document).

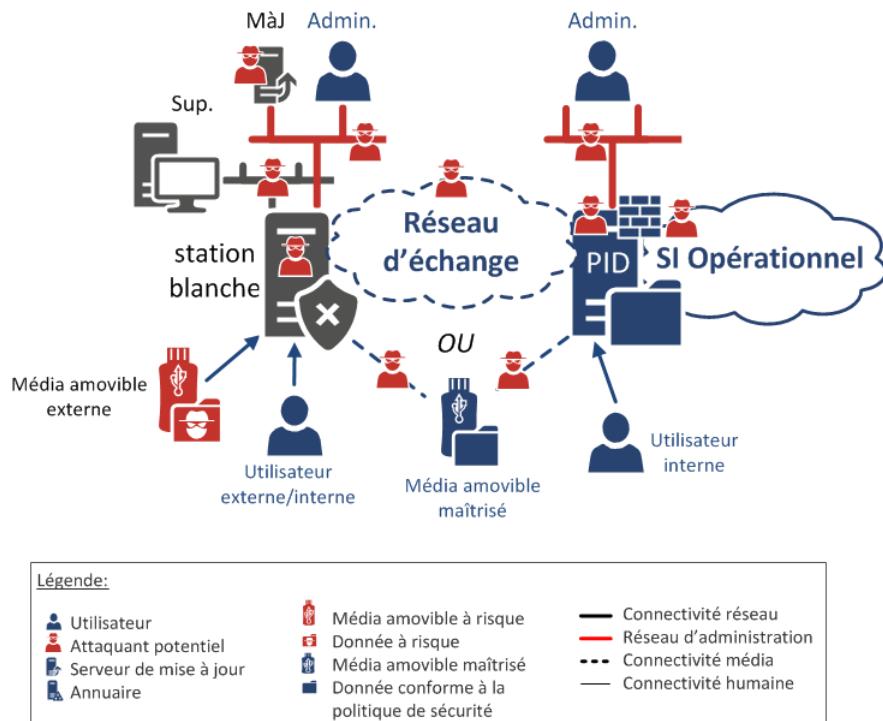


FIGURE 1 – Architecture de l'environnement du produit et présence de l'attaquant

2.3 Périmètre du produit

2.3.1 Matériel

Le périmètre matériel du produit contient :

- la station blanche ;
- le PID éventuel s'il est spécifique à la solution.

2.3.2 Logiciel

Le périmètre logiciel du produit contient :

- le système d'exploitation de la station blanche ;
- le système d'exploitation du PID si ce dernier est spécifique à la solution ;
- les fonctions de la station blanche ;
- les fonctions éventuellement présentes sur le PID.

2.4 Descriptif des utilisateurs

La liste des types d'utilisateurs susceptibles d'interagir avec le produit est la suivante :

- **Administrateur** : Utilisateur ayant les droits de modifier une partie de la configuration du produit. Il ne peut pas modifier les comptes d'administrateurs ;
- **Super-administrateur** : Utilisateur ayant tous les droits sur le produit et qui peut également créer, modifier ou supprimer les comptes d'administrateurs ;
- **Utilisateur** : Utilisateur ayant les droits nécessaires pour se connecter au réseau opérationnel et également pour transférer des données depuis le produit vers ce réseau.

3

Hypothèses

3.1 Hypothèses sur l'environnement

Les hypothèses sur l'environnement du produit sont les suivantes :

H1 Local

Le produit n'est pas nécessairement dans un local sécurisé et l'attaquant peut avoir accès à toutes les interfaces physiques (Médias et Ethernet). De façon similaire, l'attaquant peut arriver à faire brancher un dispositif piégé (par exemple une clé USB) sur n'importe quel port physique du produit. Il est considéré que l'attaquant ne peut pas démonter le produit ou effectuer d'attaque physique (soudure, etc.).

En revanche, des exemplaires identiques au produit étant disponibles dans le commerce, l'attaquant peut acheter un tel produit afin d'y rechercher des vulnérabilités par tous les moyens à sa disposition.

H2 Poste d'administration

Le poste d'administration du sas ou de la station blanche est sécurisé et maintenu à jour de toutes les vulnérabilités connues concernant le système d'exploitation et les applications utilisées. La station d'administration est installée dans un local à accès contrôlé/protégé.

3.2 Hypothèses sur le produit

Les hypothèses sur le produit sont les suivantes :

H3 Dimensionnement

Le produit est dimensionné pour répondre aux contraintes de l'environnement dans lequel il est déployé (capacité de traitement des fichiers, bande passante éventuelle, etc.).

H4 Utilisateurs

Les utilisateurs du produit sont informés de la manière de l'utiliser et disposent d'une documentation associée.

H5 Administrateurs

Les administrateurs du produit sont compétents, formés et non hostiles.

H6 Consultation des journaux par les administrateurs

Il est considéré que les administrateurs consultent régulièrement les journaux locaux ou déportés générés par le produit.

H7 Intégrité du produit

Le produit est à jour de l'ensemble des correctifs de sécurité en vigueur et des dernières versions des bases antivirales. La configuration usine est également intègre.

H8 Réseau opérationnel

Le réseau de destination (ou réseau opérationnel) n'est pas considéré comme un réseau maîtrisé.

4

Biens sensibles à protéger



Information

Le texte en rouge correspond au(x) bien(s) à prendre en compte de façon facultative.

4.1 Biens sensibles du produit

Les biens sensibles sont les suivants :

B1	Logiciels du produit
----	----------------------

- Les logiciels du produit (système d'exploitation, application, base de signatures virales, etc.) sont considérés comme des biens sensibles. Ils doivent être protégés en disponibilité, intégrité et authenticité.

B2	Base des utilisateurs
----	-----------------------

- La base des utilisateurs et administrateurs du produit, leurs informations d'authentification auprès du produit et leurs droits d'accès sont à protéger en disponibilité, confidentialité et intégrité.

B3	Configuration
----	---------------

- La configuration du produit est à protéger en disponibilité et en intégrité.

B4	Eléments cryptographiques
----	---------------------------

- Le produit traite 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.

B5	Politique de gestion des droits
----	---------------------------------

- Cette politique peut être contenue en local sur le produit ou être obtenue à partir d'un annuaire distant. Ce bien est à protéger en disponibilité et intégrité.

B6

Journaux d'évènements

- Les évènements de sécurité sont journalisés localement **et de façon déportée**. Ce bien est à protéger en disponibilité et intégrité. **Les journaux doivent être également authentifiés lorsqu'ils sont déportés.**

B7

Journaux de transfert de fichier(s)

- Les informations liées au transfert de fichier(s) sont journalisées localement **et de façon déportée**. Ce bien est à protéger en disponibilité et intégrité. **Les journaux doivent être également authentifiés lorsqu'ils sont déportés.**

B8

Contrôleur(s) USB du produit

- Le produit doit être équipé d'une protection contre la destruction par surtension positive ou négative du contrôleur USB. Le contrôleur est à protéger en disponibilité et intégrité.

4.2 Biens sensibles de l'environnement

B9

Les flux du réseau d'administration

- Ce bien est à protéger en confidentialité, intégrité et authenticité.

B10

Le SI opérationnel

- Ce bien est à protéger en intégrité.

B11

Données analysées

- Le fichier à analyser doit être protégé en intégrité.

B12

Média d'import

- Le média utilisé pour l'import des données doit être protégé en intégrité.

B13

Résultat de l'analyse

- Les données issues de l'analyse du fichier par le produit doivent être protégées en confidentialité.

Biens sensibles	Disponibilité	Intégrité	Confidentialité	Authenticité
B1 Logiciels du produit	x	x		x
B2 Base des utilisateurs	x	x	x	
B3 Configuration	x	x		
B4 Eléments cryptographiques	x	x	x	
B5 Politique de gestion des droits	x	x		
B6 Journaux d'évènements	x	x		
B7 Journaux de transfert de fichier(s)	x	x		
B8 Contrôleur(s) USB du produit	x	x		
B9 Les flux du réseau d'administration		x	x	x
B10 Le SI opérationnel		x		
B11 Données du fichier(s) à analyser		x		
B12 Média d'import		x		
B13 Résultat de l'analyse			x	

TABLE 1 – Biens sensibles du produit

5

Menaces

5.1 Profils des attaquants

Les attaquants à considérer sont :

■ **Utilisateur légitime**

Utilisateurs du produit ayant accès à ce dernier et insérant un média compromis ou réalisant une erreur de manipulation ;

■ **Utilisateur non autorisé**

Toute personne pouvant accéder physiquement au produit en exploitation ;

■ **Attaquant avec des droits d'administration**

L'attaquant a réussi à compromettre le compte d'un administrateur. Ce compte peut avoir n'importe quel rôle à l'exception du super-administrateur.

5.2 Descriptif des menaces



Information

Le texte en rouge correspond au(x) menace(s) à prendre en compte de façon facultative.

Les menaces à considérer sont les suivantes :

M1 Compromission

Un attaquant, via l'une des interfaces réseau ou média du produit, prend connaissance ou altère des biens sensibles en confidentialité ou en intégrité (logiciel ou matériel, destruction d'un contrôleur USB, carte SD, etc. ou compromission du SI opérationnel, etc.);

M2 Contournement

Un attaquant, via l'une des interfaces réseau ou média du produit, parvient à transférer des données de manière illégitime, en contournant la politique de sécurité du produit (filtrage, analyse anti-virale, etc.);

M3 Usurpation d'identité

Un attaquant, via l'une des interfaces réseau du produit, usurpe l'identité d'un utilisateur ou d'un administrateur du produit ;

M4 Indisponibilité

Un attaquant, via l'une des interfaces réseau ou média du produit, rend indisponible tout ou partie des fonctions de sécurité du produit de manière temporaire ou définitive (vulnérabilités connues ou non) ;

M5 Corruption d'une mise à jour

Un attaquant parvient à corrompre une mise à jour dans le but d'altérer le fonctionnement du produit (injection de code malveillant dans le firmware, corruption des bases virales, etc.) ;

M6 Corruption des journaux d'évènements

L'attaquant parvient à supprimer ou modifier une entrée dans les journaux d'évènements locaux sans y avoir été autorisé. L'attaquant parvient à modifier ou supprimer une entrée de journal distant émise par le produit sans que le destinataire ne puisse s'en rendre compte. L'attaquant parvient à modifier ou supprimer une émission de journalisation distante sans que le destinataire ne puisse s'en rendre compte ;

M7 Corruption des journaux de transfert de fichier(s)

L'attaquant parvient à supprimer ou modifier une entrée dans les journaux locaux de transfert de fichier(s) sans y avoir été autorisé. L'attaquant parvient à modifier une entrée de journal distant émise par le produit sans que le destinataire ne puisse s'en rendre compte.

6

Fonctions du produit

6.1 Fonctions de sécurité du produit



Information

Le texte en rouge correspond au(x) exigence(s) à prendre en compte de façon facultative.

FS1
Obligatoire

Transfert sécurisé de fichier(s) : le produit doit permettre le transfert de fichier(s) depuis un média amovible tout en garantissant l'innocuité du support et des fichiers (le produit doit être conçu de telle sorte que son intégrité et son fonctionnement ne puissent pas être altérés par un média amovible ou un fichier). L'analyse d'un fichier ne doit pas dégrader la disponibilité du produit.

Exigences :

- Le produit effectue un transfert de fichier(s) avec ou sans modification (statification) selon le type de fichier, le format de fichier et l'analyse antivirale ;
- En cas de modification, cette dernière doit échouer si le format de fichier n'est pas reconnu. Si aucune modification n'est réalisée par l'analyse, l'utilisateur doit pouvoir s'assurer que ce fichier est intègre ;
- En cas d'échec de l'analyse des fichiers ou de nocuité avérée d'un fichier, l'utilisateur et les opérateurs du produit doivent être notifiés et aucun des fichiers présents ne doit être transféré ;
- Le transfert ne doit pas être effectué en mode privilégié depuis le système d'exploitation. Les priviléges des applications et processus doivent être réduits au minimum requis ;
- La vérification du type de fichier ne doit pas être contournable par ;
- Le produit doit permettre l'analyse de fichier protégé par un mot de passe (si le mot de passe n'est pas saisi le transfert ne sera pas exécuté) ;
- La saisie du mot de passe, s'il existe, et l'ouverture du document doivent être réalisées dans un environnement cloisonné matériellement ou logiciellement. En cas d'utilisation d'un cloisonnement logiciel, l'environnement doit être dédié et sécurisé conformément au guide de sécurisation d'une configuration GNU/Linux [1] (des mesures similaires doivent être mises en œuvre en cas d'utilisation d'un autre système d'exploitation) ;
- Les fichiers doivent être analysés de manière récursive (à l'intérieur du fichier) dans un court délai (inférieur à 10 minutes pour l'analyse du média) quel que soit le résultat de l'analyse (échec

ou réussi). Lorsque ce délai est échu, une action est réalisée. Cette action peut être configurée par l'administrateur (refus de transfert, demande de validation du transfert par l'utilisateur, etc.).

FS2 Facultatif	Transfert par statification : le produit doit permettre le transfert de certains fichiers selon la méthode de statification.
-------------------	---

Exigences :

- Le transfert par statification ne doit pas s'appliquer sur les fichiers binaires. Ce transfert doit s'appliquer par exemple sur des fichiers images, des fichiers bureautiques (pour suppression des macros par exemple), etc. ;
- Chaque transformation de fichier doit être exécutée dans un environnement cloisonné matériellement ou logiciellement. En cas d'utilisation d'un cloisonnement logiciel, par exemple, un « conteneur » ou une machine virtuelle, il est nécessaire d'appliquer le principe de moindres priviléges conformément au guide de sécurisation d'une configuration GNU/Linux [1] ;

FS3 Obligatoire	Affichage de la liste de fichier(s) : le produit doit permettre de lister le contenu du média d'entrée ainsi que celui de sortie pour la sélection des fichiers à transférer et leurs vérifications.
--------------------	---

Exigences :

- Tous les fichiers contenus dans le média d'entrée doivent être présentés à l'écran (ainsi que leurs métadonnées), y compris les fichiers cachés ;
- Seuls les fichiers sélectionnés doivent être copiés pour l'import. Il est possible d'utiliser une liste blanche des formats de fichiers tolérés incluant les formats de fichiers « Métier » ;
- Le filtrage des fichiers à analyser doit être basé sur une analyse du contenu et pas uniquement sur l'extension ;
- Le produit doit permettre de placer en quarantaine (depuis l'interface du produit) un fichier jugé à risque par l'utilisateur.

FS4 Facultatif	Journalisation sécurisée des transferts de fichiers : le produit doit sauvegarder les informations concernant le transfert de fichier (nom et type de médias d'entrée et de sortie, nom et type de fichier, résultat du transfert, résultat de l'analyse anti-virale, dates, etc.). La station doit assurer l'imputabilité des transferts entrants et/ou sortants.
-------------------	---

Exigences :

- Lorsque la capacité de stockage est atteinte, les opérateurs du produit doivent être notifiés et une rotation du fichier de journalisation doit être effectuée ;
- Les journaux doivent être protégés en intégrité et doivent être accessibles à tout moment par l'administrateur du produit (se référer au guide de mise en oeuvre d'un système de journalisation [2]) ;
- Les fonctions liées à la journalisation doivent être réalisées dans un environnement cloisonné matériellement ou logiciellement. En cas d'utilisation d'un cloisonnement logiciel, l'environnement doit être dédié et sécurisé conformément au guide de sécurisation d'une configuration

GNU/Linux [1]. Des mesures similaires doivent être mises en œuvre en cas d'utilisation d'un autre type de cloisonnement d'environnement (machine virtuelle par exemple) ;

- Les journaux générés doivent contenir les informations concernant l'utilisateur authentifié qui a réalisé le transfert.

FS5
Obligatoire

Analyse de sécurité : le produit doit réaliser une analyse antivirale systématique des fichiers à importer.

Exigences :

- L'analyse antivirale doit s'effectuer uniquement lors du transfert d'un fichier ;
- Le(s) antivirus doi(ven)t être exécuté(s) dans un environnement cloisonné matériellement ou logiciellement. En cas d'utilisation d'un cloisonnement logiciel, par exemple par « conteneur » ou machine virtuelle, il est nécessaire d'appliquer le principe de moindres priviléges conformément au guide de sécurisation d'une configuration GNU/Linux [1]. Quel que soit le cloisonnement utilisé, l'environnement doit être réinitialisé entre deux analyses et le système de fichier racine doit être monté en lecture seule ;
- L'analyse antivirale doit supporter plusieurs moteurs d'antivirus différents. Le choix des moteurs peut être laissé à la discréTION du client ;
- L'analyse antivirale des fichiers doit pouvoir utiliser plusieurs sources de signatures. le choix source peut être laissé à la discréTION du client ;
- L'analyse antivirale des fichiers ne doit pas être contournable ;
- L'authenticité et l'intégrité des mises à jour des signatures et du moteur doivent être vérifiées par le produit ;
- La base antivirale et le moteur doivent pouvoir être mis à jour en mode déconnecté.

FS6
Obligatoire

Chiffrement : le produit stocke les secrets de connexion des administrateurs (Pas d'authentification utilisateur sur la station blanche nécessaire. L'authentification sur le PID s'effectue auprès du SI opérationnel pour les utilisateurs).

Exigences :

- Les secrets de connexion doivent respecter les recommandations de l'annexe B1 du RGS V2 [4] ;
- Le produit doit intégrer un chiffrement de surface complet du disque sur lequel le système d'exploitation est installé (les secrets de connexion des utilisateurs doivent être protégés — en confidentialité et intégrité — des autres processus disposant de droits d'exécution en lecture sur le disque).

FS7
Obligatoire

Identification, authentification et contrôle d'accès : le produit identifie et authentifie les administrateurs permettant de contrôler les ressources selon les droits de ces derniers.

Exigences :

- Le produit doit intégrer les recommandations relatives au guide de sécurisation de la configuration d'un système GNU/Linux [1].
Des mesures similaires doivent être mises en œuvre en cas d'utilisation d'un autre système d'exploitation.

FS8 Obligatoire	<i>Intégrité des logiciels</i> : le produit permet de mettre à jour les logiciels le constituant (système d'exploitation et logiciel(s) spécifique(s)).
--------------------	--

Exigences :

- L'authenticité et l'intégrité de la mise à jour des logiciels du produit doivent être vérifiées ;
- Le système ne doit pas pouvoir être mis à jour avec une version antérieure des logiciels qui le composent (système d'exploitation, logiciels métiers, bases antivirales, etc.).
- Les fichiers binaires, les politiques de sécurité et les configurations de la solution logicielle du produit doivent être protégés en intégrité.

FS9 Obligatoire	<i>Intégrité des journaux d'évènements</i> : le produit journalise l'ensemble des opérations effectuées par les utilisateurs et par lui-même (hors transfert de fichier(s)).
--------------------	---

Exigences :

- Lorsque la capacité de stockage est atteinte, une rotation des fichiers est effectuée (conformément au guide de mise en œuvre d'un système de journalisation [2]) ;
- Les journaux doivent être protégés en intégrité ;
- Les journaux doivent pouvoir être émis à un collecteur. Les journaux déportés doivent être protégés en intégrité et authenticité ;
- Les fonctions liées à la journalisation doivent être exécutées avec des comptes non privilégiés.

FS10 Obligatoire	<i>Protection des flux</i> : les flux d'administration entrants et sortants du produit doivent être sécurisés.
---------------------	---

Exigences :

- Le produit protège en confidentialité, en intégrité et en authenticité, toutes les actions réalisées à distance par les administrateurs ;
- Le produit doit être équipé d'une interface d'administration dédiée conformément au guide [3].

FS11 Obligatoire	<i>Cloisonnement</i> : les fonctions métier (administration, transfert, analyse, etc.) du produit sont cloisonnées afin de limiter la prise de contrôle à distance et le risque de rebond.
---------------------	---

Exigences :

- Chaque processus doit être exécuté dans un environnement cloisonné matériellement ou logiciellement, par exemple par « conteneur » ou machine virtuelle.

- L'analyse de fichier doit être réalisée dans l'espace utilisateur du système d'exploitation et doit permettre d'identifier l'utilisateur ayant effectué le transfert (conformément au guide de cloisonnement système [5]).

FS12
Obligatoire

Dimensionnement : le produit doit être correctement dimensionné afin de prendre en compte les contraintes de délai de transfert, de capacité de stockage etc.

Exigences :

- Le produit doit être résilient lorsque la capacité de rétention des journaux de fonctionnement et d'alertes est atteinte ;
- Le produit doit être correctement dimensionné afin de prendre en compte une durée d'analyse du média acceptable par l'utilisateur (inférieur à 10 minutes par exemple). Cette durée peut être configurée par l'administrateur.

FS13
Obligatoire

Intégrité des médias entrants et sortants : le produit doit garantir l'intégrité des médias insérés, qu'ils soient entrants ou sortants.

Exigences :

- Des mesures organisationnelles doivent être proposées par le soumissionnaire afin d'éviter la mise en place de médias pouvant présenter un firmware non légitime ;
- Les flux de données échangés entre les médias d'entrée et de sortie et le produit doivent être unidirectionnels (se reporter à l'annexe C du présent document) ;
- L'analyse effective du média par le produit doit être vérifiée avant d'importer des données du PID vers le SI opérationnel.

FS14
Obligatoire

Intégrité du produit : quel que soit le média d'entrée ou de sortie, son insertion ne doit pas porter atteinte à l'intégrité du produit.

Exigences :

- Les ports autres que ceux utilisés par les médias d'entrée et de sortie doivent être physiquement inaccessibles ;
- Dans le cas d'une station blanche, les contrôleurs des interfaces des médias d'entrée et de sortie doivent être composés de firmware distincts et la compromission d'une interface d'entrée ne doit pas compromettre l'interface de sortie (voir l'annexe B) ;
- Dans le cas d'une station blanche, l'utilisation du même média sur le point d'entrée de la station et le point de sortie est à proscrire (voir l'annexe B) ;
- Le produit ne doit pas permettre l'amorçage depuis un support amovible ;
- Aucun des fichiers importés ou présents sur le média d'entrée ne doit pouvoir être exécuté par le produit ;
- L'intégrité et l'authenticité du processus de démarrage du système doivent être vérifiées (Secure Boot) ;

- L'accès aux paramètres de démarrage (BIOS, UEFI, UBOOT, etc.) du produit doit être protégé par authentification ;
- Les médias d'entrée et de sortie doivent être montés par le produit uniquement en tant que « MassStorage » (pas de montage de périphérique HID par exemple) ;
- Le média d'entrée doit être monté uniquement en lecture seule ;
- **Un formatage standard doit être réalisé sur le média de sortie lors de la validation du transfert de fichier ;**
- **Les contrôleurs de média du produit doivent être protégés contre les surtensions (positives ou négatives) ;**
- Le produit doit mettre en œuvre des mécanismes de protection physique contre l'effraction afin d'éviter ou de détecter une tentative de piégeage du produit ;
- Effectuer un effacement cryptographique de l'environnement utilisé. En effet, les données utilisées et produites lors du transfert de fichier(s) doivent pouvoir être effacées du produit (en mémoire et sur le disque) afin de réinitialiser l'environnement.

FS15 Obligatoire	<i>Filtrage dans le cas d'un PID raccordé à un réseau</i> : Le produit doit protéger l'accès direct au réseau opérationnel depuis le PID.
---------------------	--

Exigences :

- Le filtrage est unidirectionnel et assuré par une fonction de pare-feu ou de diode (se reporter à l'annexe B du présent document) ;
- Le filtrage autorise uniquement les communications sur des ports jugés nécessaires ;
- **Pour accéder au réseau opérationnel depuis le PID, un espace de stockage dédié sera mis en place pour effectuer les transferts de fichier depuis le poste de travail de l'utilisateur.**

Plusieurs architectures ont été identifiées pour réaliser les fonctions de sécurité du produit. Les deux suivantes sont traitées en exemple dans les annexes du document :

- un sas d'import de données qui permet d'utiliser un seul média amovible et de transférer les données souhaitées sur le réseau opérationnel au travers d'un espace d'échange ;
- une station blanche avec deux médias amovibles : un média amovible externe et un media amovible maîtrisé pour transférer les données depuis la station blanche vers le réseau opérationnel.

Annexe A

Matrices de couverture

A.1

Couverture des biens par les menaces

M1 Compromission	IA	CI	I	CI	I	I	(I)	I	CI	I	I	
M2 Contournement de la politique de sécurité	AI											
M3 Usurpation d'identité		CI										A
M4 Indisponibilité	D	D	D	D	D	D	(D)	D				
M5 Corruption d'une mise à jour	IA		I									
M6 Corruption des journaux d'évènements									DI			
M7 Corruption des journaux de transfert										(DI)		
B1 Logiciels du produit												
B2 Base des utilisateurs												
B3 Configuration												
B4 Eléments cryptographiques												
B5 Politique de gestion des droits												
B6 Journal aux d'évenements												
B7 Journal aux de transfert de fichiers(s)												
B8 Contrôleur(s) USB du produit												
B9 Les flux du réseau d'administration												
B10 Le SI opérationnel												
B11 Fichier(s) à analyser												
B12 Média d'import												
B13 Résultat de l'analyse												

TABLE 2 – Atteintes aux biens sensibles en fonction des menaces

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

A.2

Couverture des menaces par les fonctions de sécurité

	Compromission							Contournement de la politique de sécurité							Usurpation d'identité							Indisponibilité							Corruption d'une mise à jour							Corruption des journaux d'évenements							Corruption des journaux de transfert																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																												
	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29	M30	M31	M32	M33	M34	M35	M36	M37	M38	M39	M40	M41	M42	M43	M44	M45	M46	M47	M48	M49	M50	M51	M52	M53	M54	M55	M56	M57	M58	M59	M60	M61	M62	M63	M64	M65	M66	M67	M68	M69	M70	M71	M72	M73	M74	M75	M76	M77	M78	M79	M80	M81	M82	M83	M84	M85	M86	M87	M88	M89	M90	M91	M92	M93	M94	M95	M96	M97	M98	M99	M100	M101	M102	M103	M104	M105	M106	M107	M108	M109	M110	M111	M112	M113	M114	M115	M116	M117	M118	M119	M120	M121	M122	M123	M124	M125	M126	M127	M128	M129	M130	M131	M132	M133	M134	M135	M136	M137	M138	M139	M140	M141	M142	M143	M144	M145	M146	M147	M148	M149	M150	M151	M152	M153	M154	M155	M156	M157	M158	M159	M160	M161	M162	M163	M164	M165	M166	M167	M168	M169	M170	M171	M172	M173	M174	M175	M176	M177	M178	M179	M180	M181	M182	M183	M184	M185	M186	M187	M188	M189	M190	M191	M192	M193	M194	M195	M196	M197	M198	M199	M200	M201	M202	M203	M204	M205	M206	M207	M208	M209	M210	M211	M212	M213	M214	M215	M216	M217	M218	M219	M220	M221	M222	M223	M224	M225	M226	M227	M228	M229	M230	M231	M232	M233	M234	M235	M236	M237	M238	M239	M240	M241	M242	M243	M244	M245	M246	M247	M248	M249	M250	M251	M252	M253	M254	M255	M256	M257	M258	M259	M260	M261	M262	M263	M264	M265	M266	M267	M268	M269	M270	M271	M272	M273	M274	M275	M276	M277	M278	M279	M280	M281	M282	M283	M284	M285	M286	M287	M288	M289	M290	M291	M292	M293	M294	M295	M296	M297	M298	M299	M300	M301	M302	M303	M304	M305	M306	M307	M308	M309	M310	M311	M312	M313	M314	M315	M316	M317	M318	M319	M320	M321	M322	M323	M324	M325	M326	M327	M328	M329	M330	M331	M332	M333	M334	M335	M336	M337	M338	M339	M340	M341	M342	M343	M344	M345	M346	M347	M348	M349	M350	M351	M352	M353	M354	M355	M356	M357	M358	M359	M360	M361	M362	M363	M364	M365	M366	M367	M368	M369	M370	M371	M372	M373	M374	M375	M376	M377	M378	M379	M380	M381	M382	M383	M384	M385	M386	M387	M388	M389	M390	M391	M392	M393	M394	M395	M396	M397	M398	M399	M400	M401	M402	M403	M404	M405	M406	M407	M408	M409	M410	M411	M412	M413	M414	M415	M416	M417	M418	M419	M420	M421	M422	M423	M424	M425	M426	M427	M428	M429	M430	M431	M432	M433	M434	M435	M436	M437	M438	M439	M440	M441	M442	M443	M444	M445	M446	M447	M448	M449	M450	M451	M452	M453	M454	M455	M456	M457	M458	M459	M460	M461	M462	M463	M464	M465	M466	M467	M468	M469	M470	M471	M472	M473	M474	M475	M476	M477	M478	M479	M480	M481	M482	M483	M484	M485	M486	M487	M488	M489	M490	M491	M492	M493	M494	M495	M496	M497	M498	M499	M500	M501	M502	M503	M504	M505	M506	M507	M508	M509	M510	M511	M512	M513	M514	M515	M516	M517	M518	M519	M520	M521	M522	M523	M524	M525	M526	M527	M528	M529	M530	M531	M532	M533	M534	M535	M536	M537	M538	M539	M540	M541	M542	M543	M544	M545	M546	M547	M548	M549	M550	M551	M552	M553	M554	M555	M556	M557	M558	M559	M560	M561	M562	M563	M564	M565	M566	M567	M568	M569	M570	M571	M572	M573	M574	M575	M576	M577	M578	M579	M580	M581	M582	M583	M584	M585	M586	M587	M588	M589	M590	M591	M592	M593	M594	M595	M596	M597	M598	M599	M600	M601	M602	M603	M604	M605	M606	M607	M608	M609	M610	M611	M612	M613	M614	M615	M616	M617	M618	M619	M620	M621	M622	M623	M624	M625	M626	M627	M628	M629	M630	M631	M632	M633	M634	M635	M636	M637	M638	M639	M640	M641	M642	M643	M644	M645	M646	M647	M648	M649	M650	M651	M652	M653	M654	M655	M656	M657	M658	M659	M660	M661	M662	M663	M664	M665	M666	M667	M668	M669	M670	M671	M672	M673	M674	M675	M676	M677	M678	M679	M680	M681	M682	M683	M684	M685	M686	M687	M688	M689	M690	M691	M692	M693	M694	M695	M696	M697	M698	M699	M700	M701	M702	M703	M704	M705	M706	M707	M708	M709	M710	M711	M712	M713	M714	M715	M716	M717	M718	M719	M720	M721	M722	M723	M724	M725	M726	M727	M728	M729	M730	M731	M732	M733	M734	M735	M736	M737	M738	M739	M740	M741	M742	M743	M744	M745	M746	M747	M748	M749	M750	M751	M752	M753	M754	M755	M756	M757	M758	M759	M760	M761	M762	M763	M764	M765	M766	M767	M768	M769	M770	M771	M772	M773	M774	M775	M776	M777	M778	M779	M780	M781	M782	M783	M784	M785	M786	M787	M788	M789	M790	M791	M792	M793	M794	M795	M796	M797	M798	M799	M800	M801	M802	M803	M804	M805	M806	M807	M808	M809	M810	M811	M812	M813	M814	M815	M816	M817	M818	M819	M820	M821	M822	M823	M824	M825	M826	M827	M828	M829	M830	M831	M832	M833	M834	M835	M836	M837	M838	M839	M840	M841	M842	M843	M844	M845	M846	M847	M848	M849	M850	M851	M852	M853	M854	M855	M856	M857	M858	M859	M860	M861	M862	M863	M864	M865	M866	M867	M868	M869	M870	M871	M872	M873	M874	M875	M876	M877	M878	M879	M880	M881	M882	M883	M884	M885	M886	M887	M888	M889	M890	M891	M892	M893	M894	M895	M896	M897	M898	M899	M900	M901	M902	M903	M904	M905	M906	M907	M908	M909	M910	M911	M912	M913	M914	M915	M916	M917	M918	M919	M920	M921	M922	M923	M924	M925	M926	M927	M928	M929	M930	M931	M932	M933	M934	M935	M936	M937	M938	M939	M940	M941	M942	M943	M944	M945	M946	M947	M948	M949	M950	M951	M952	M953	M954	M955	M956	M957	M958	M959	M960	M961	M962	M963	M964	M965	M966	M967	M968	M969	M970	M971	M972	M973	M974	M975	M976	M977	M978	M979	M980	M981	M982	M983	M984	M985	M986	M987	M988	M989	M990	M991	M992	M993	M994	M995	M996	M997	M998	M999	M1000	M1001	M1002	M1003	M1004	M1005	M1006	M1007	M1008	M1009	M10010	M10011	M10012	M10013	M10014	M10015	M10016	M10017	M10018	M10019	M10020	M10021	M10022	M10023	M10024	M10025	M10026	M10027	M10028	M10029	M10030	M10031	M10032	M10033	M10034	M10035	M10036	M10037	M10038	M10039	M10040	M10041	M10042	M10043	M10044	M10045	M10046	M10047	M10048	M10049	M10050	M10051	M10052	M10053	M10054	M10055	M10056	M10057	M10058	M10059	M10060	M10061	M10062	M10063	M10064	M10065	M10066	M10067	M10068	M10069	M10070	M10071	M10072	M10073	M10074	M10075	M10076	M10077	M10078	M10079	M10080	M10081	M10082	M10083	M10084	M10085	M10086	M10087	M10088	M10089	M10090	M10091	M10092	M10093	M10094	M10095	M10096	M10097	M10098	M10099	M100100	M100101	M100102	M100103	M100104	M100105	M100106	M100107	M100108	M100109	M100110	M100111	M100112	M100113	M100114	M100115	M100116	M100117	M100118	M100119	M100120	M100121	M100122	M100123	M100124	M100125	M100126	M100127	M100128	M100129	M100130	M100131	M100132	M100133	M100134	M100135	M100136	M100137	M100138	M100139	M100140	M100141	M100142	M100143	M100144	M100145	M100146	M100147	M100148	M100149	M100150	M100151	M100152	M100153	M100154	M100155	M100156	M100157	M100158	M100159	M100160	M100161	M100162	M100163	M100164	M100165	M100166	M100167	M100168	M100169	M100170	M100171	M100172	M100173	M100174	M100175	M100176	M100177	M100178	M100179	M100180	M100181	M100182	M100183	M100184	M100185	M100186	M100187	M100188	M100189	M100190	M100191	M100192	M100193	M100194	M100195	M100196	M100197	M100198	M100199	M100200	M100201	M100202	M100203	M100204	M100205	M100206	M100207	M100208	M100209	M100210	M100211	M100212	M100213	M100214	M100215	M100216	M100217	M100218	M100219	M100220	M100221	M100222	M100223	M100224	M100225	M100226	M100227	M100228	M100229	M100230	M100231	M100232	M100233	M100234	M100235	M100236	M100237	M100238	M100239	M100240	M100241	M100242	M100243	M100244	M100245	M100246	M100247	M100248	M100249	M100250	M100251	M100252	M100253	M100254	M100255	M100256	M100257	M100258	M100259	M100260	M100261	M100262	M100263	M100264	M100265	M100266	M100267	M100268	M100269	M100270	M100271	M100272	M100273	M100274	M100275	M100276	M100277	M100278	M100279	M100280	M100281	M100282	M100283	M100284	M100285	M100286	M10028

Annexe B

Exemple : Station blanche à deux clés

B.1 Environnement d'utilisation

Les principes généraux sont schématisés figure 2.

L'utilisateur insère un média amovible externe sur la station blanche et désigne les éléments à transférer. Si les éléments sont conformes à la politique de sécurité appliquée, ils sont transférés sur un média amovible maîtrisé.

Ce média amovible est ensuite branché sur le PID. Le PID vérifie : la présence d'un média maîtrisé et le précédent traitement par la station blanche. L'utilisateur authentifié récupère les éléments. C'est à lui qu'incombe la responsabilité de les insérer sur le réseau opérationnel.

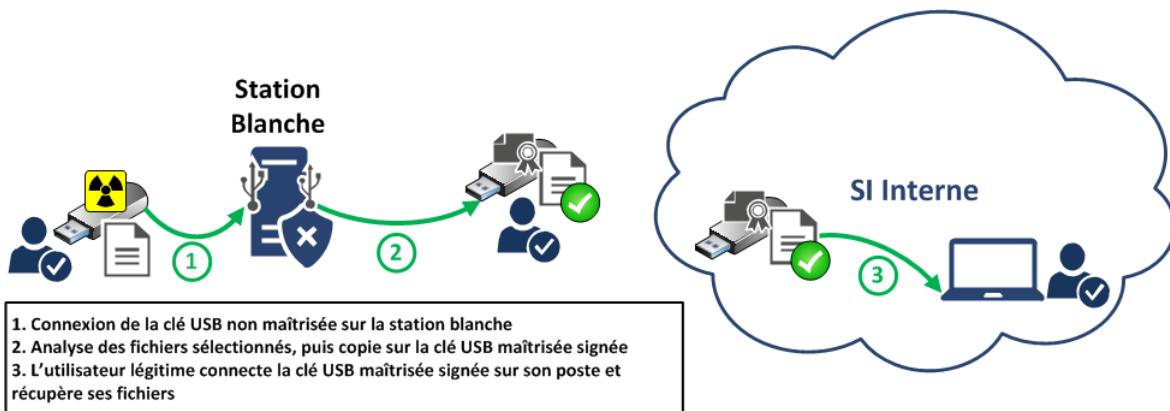


FIGURE 2 – Station blanche : principes généraux

B.2 Périmètre du produit

Le périmètre du produit est décrit à la figure 3. Deux composants majeurs doivent être présents : la station blanche et le PID. L'utilisateur insère le média amovible sur l'interface I3. Les données sont transférées sur un média amovible maîtrisé par l'interface I4. Ce média amovible maîtrisé est ensuite branché sur l'interface I5 pour être récupérées sur le PID. La connexion au serveur d'authentification interne s'effectue par l'interface I6. L'ensemble des composants sont administrés, supervisés et mis à jour au travers de réseaux d'administration¹ (Interfaces I1, I2, I7, I8).

1. Se référer au guide [3] pour plus d'informations.

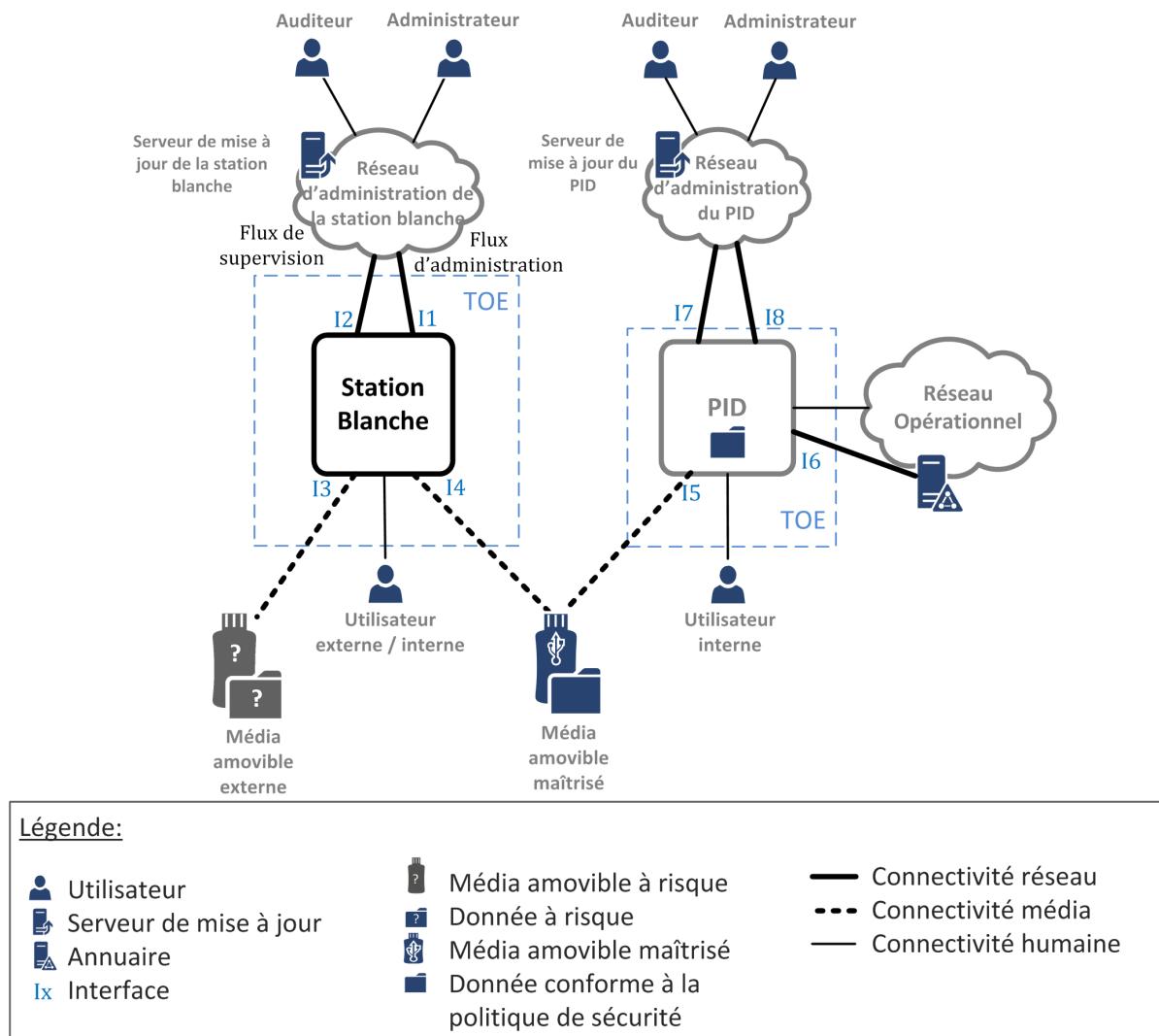
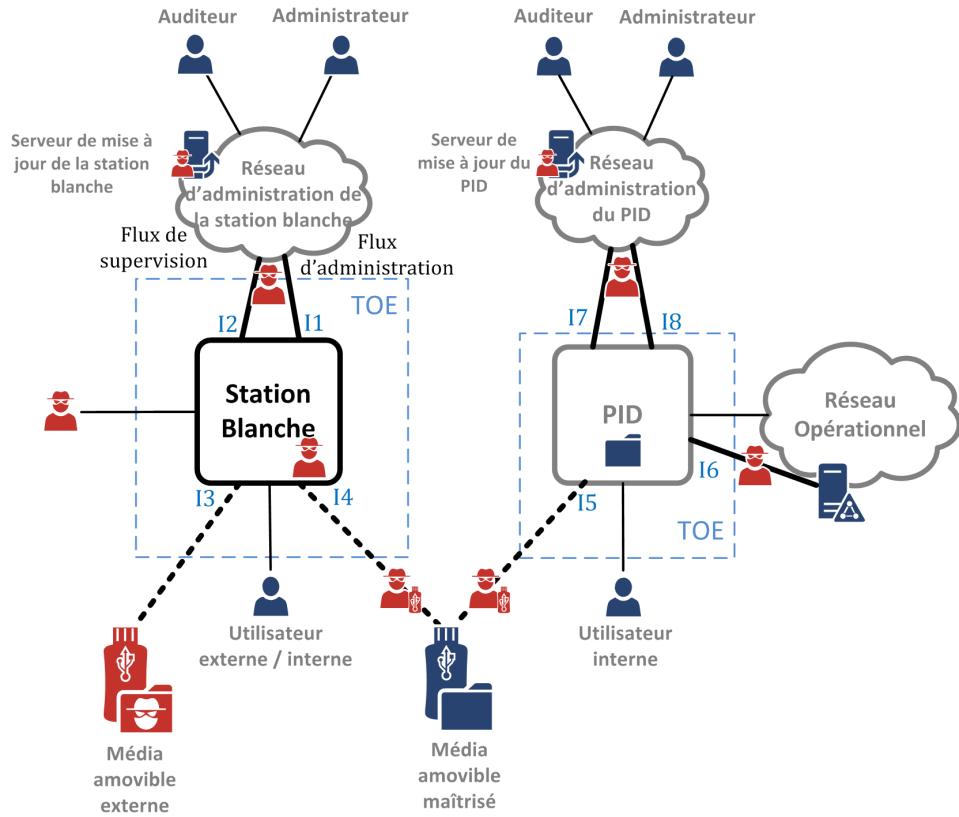


FIGURE 3 – Station blanche : détails et interfaces

B.3 Menaces

B.3.1 Profils des attaquants

Ces attaquants peuvent être positionnés comme représentés sur la figure 4.



Légende:

- | | | |
|------------------------|--|----------------------|
| Utilisateur | Média amovible à risque | Connectivité réseau |
| Attaquant potentiel | Donnée à risque | Connectivité média |
| Serveur de mise à jour | Média amovible maîtrisé | Connectivité humaine |
| Annuaire | Donnée conforme à la politique de sécurité | |
| lx Interface | | |

FIGURE 4 – sas : positionnement des attaquants

Annexe C

Exemple : Sas

C.1 Environnement d'utilisation

Les principes généraux sont schématisés figure 5.

L'utilisateur insère un média amovible externe sur le sas et désigne les éléments à transférer. Si les éléments sont conformes à la politique de sécurité appliquée, ils sont transférés dans un espace d'échange. Depuis le réseau opérationnel, un utilisateur authentifié récupère les éléments transférés sur cet espace d'échange. C'est à lui qu'incombe la responsabilité de les insérer sur le réseau opérationnel.

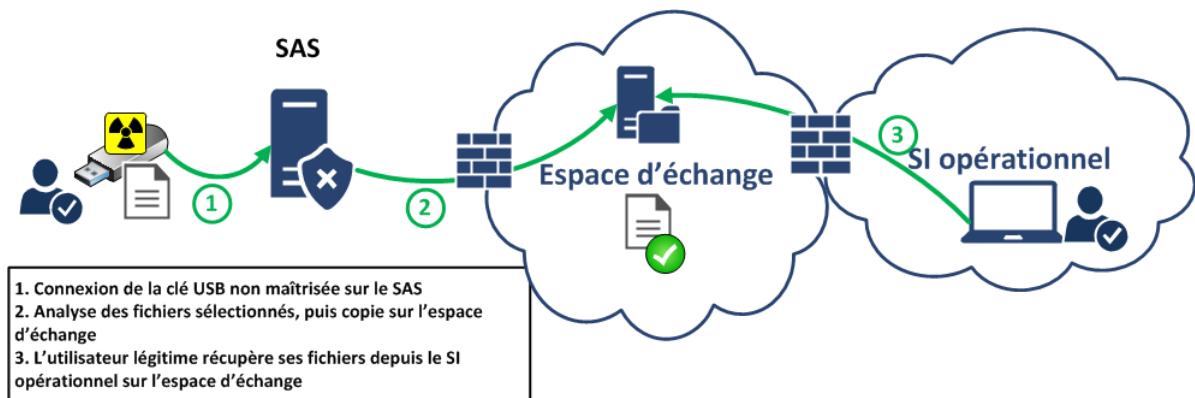


FIGURE 5 – Sas : principes généraux

C.2 Périmètre du produit

Le périmètre du produit est décrit à la figure 6. Deux composants majeurs doivent être présents : le sas d'import et l'espace d'échange (l'ensemble des éléments de la figure ci-dessous constitue une passerelle d'importation de fichier(s)). L'utilisateur insère le média amovible sur l'interface I3. Les données sont transférées sur l'espace d'échange par l'interface I9 et récupérées depuis le réseau opérationnel par l'interface I10. La connexion au serveur d'authentification interne s'effectue par l'interface I6. L'ensemble des composants sont administrés, supervisés et mis à jour en passant au travers de réseaux d'administration² (Interfaces I1, I2, I7, I8).

2. Se référer au guide [3] pour plus d'informations.

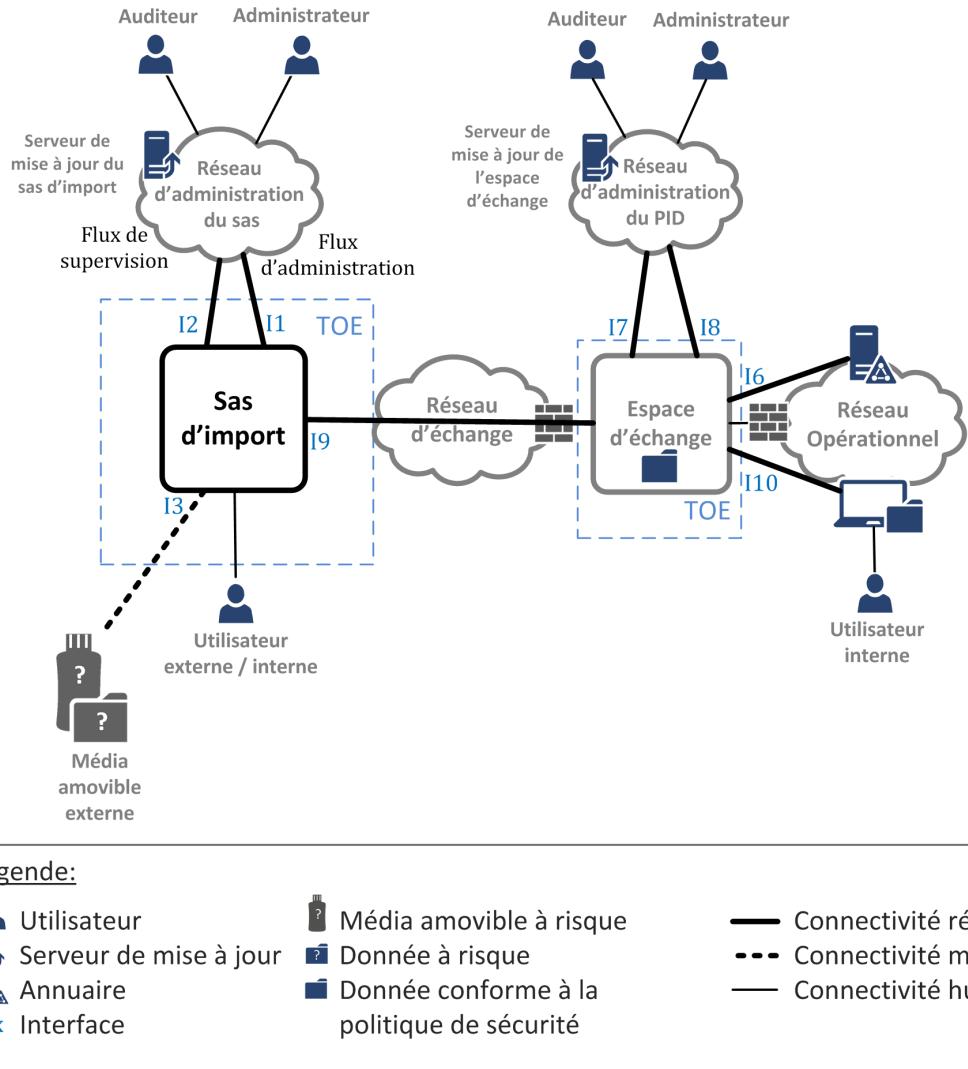


FIGURE 6 – exemple d'une passerelle d'importation de fichier(s) composée d'un sas et d'un espace d'échange

C.3 Menaces

C.3.1 Profils des attaquants

Ces attaquants peuvent être positionnés comme représentés sur la figure 7.

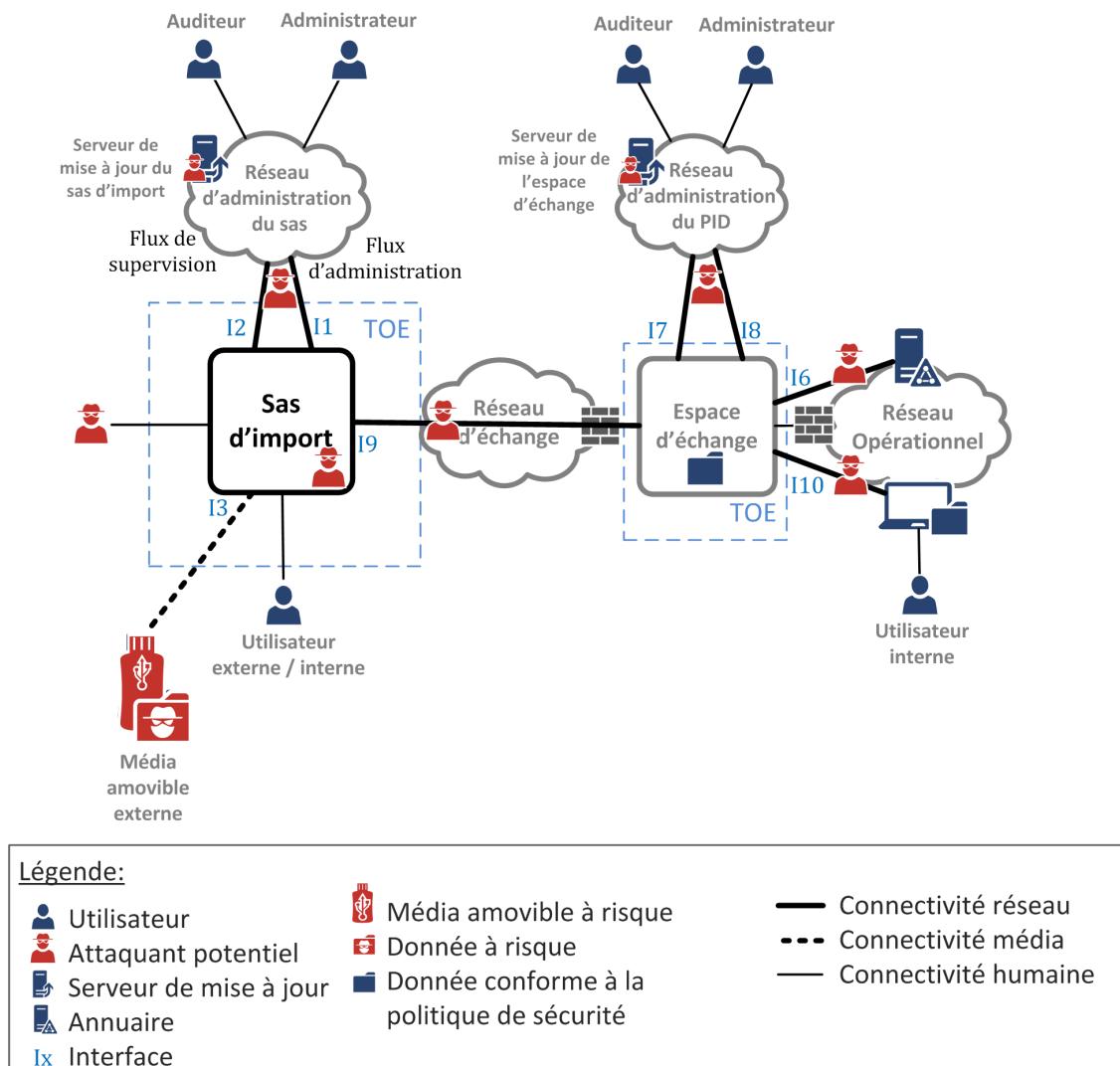


FIGURE 7 – passerelle d'importation de fichier(s) : positionnement des attaquants

Bibliographie

- [1] *Recommandations de configuration d'un système GNU/Linux.*
Guide ANSSI-BP-028 v1.2, ANSSI, 2019.
<https://www.ssi.gouv.fr/reco-securite-systeme-linux>.
- [2] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation.*
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.
<https://www.ssi.gouv.fr/journalisation>.
- [3] *Recommandations relatives à l'administration sécurisée des systèmes d'information.*
Guide ANSSI-PA-022 v2.0, ANSSI, avril 2018.
<https://www.ssi.gouv.fr/securisation-admin-si>.
- [4] *RGS Annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques.*
Référentiel Version 2.03, ANSSI, février 2014.
<https://www.ssi.gouv.fr/rgs>.
- [5] *Recommandations pour la mise en place de cloisonnement système.*
Guide ANSSI-PG-040 v1.0, ANSSI, décembre 2017.
<https://www.ssi.gouv.fr/guide-cloisonnement-systeme>.
- [6] *Licence ouverte / Open Licence.*
Page Web v2.0, Mission Etablab, avril 2017.
<https://www.etalab.gouv.fr/licence-ouverte-open-licence>.

ANSSI-PG-076

Version 1.0 - 01/07/2020

Licence ouverte / Open Licence (Étalab - v2.0)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr



Premier ministre

