

Résumé de « Profil de fonctionnalités et de sécurité – SAS et station blanche (réseaux non classifiés) », *Guide ANSSI, ANSSI-PG-076, 01/07/2020.*

Menaces

- Insertion d'un fichier malveillant dans le SI à protéger
- Attaque en intégrité/confidentialité lors du transfert de fichier sur un média amovible
- Média réalisant des attaques au niveau de la pile logicielle du média amovible
- Média réalisant des attaques en DoS au niveau du contrôleur du média
- Média se comportant comme un périphérique de type clavier ou souris, et permettant de véhiculer des fichiers malveillants sur le SI.

Profil des attaquants

- 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.

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.

- Il faut que le produit agisse en coupure pour éviter, autant que possible, l'insertion sur le réseau opérationnel d'éléments non conformes à la politique de sécurité.
- Un journal d'événements doit être présent localement et de façon déportée. Ces journaux doivent également être authentifiés lorsqu'ils sont déportés.
- 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.
- Le produit doit permettre l'analyse de fichiers protégés par un mot de passe.
- L'ouverture d'un document doit être réalisé dans un environnement cloisonné matériellement ou logiquement.

Menaces

- Compromission
- Contournement
- Usurpation d'identité
- Indisponibilité
- Corruption d'une mise à jour
- Corruption des journaux d'événements

Import des données

- SAS d'import de données
- Station blanche avec deux médias amovibles
 - Média amovible externe
 - Média amovible maîtrisé

Station blanche à deux clés

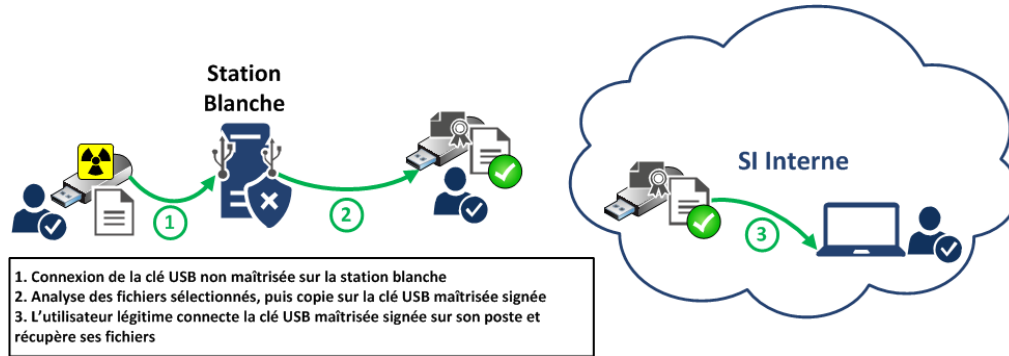


Figure 1 – Station blanche : principes généraux [Fig. 2 du document original]

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 impérative. 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.

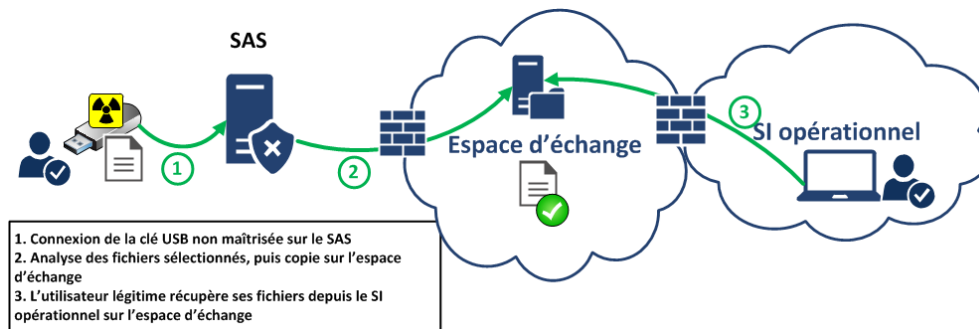


Figure 2 - SAS : principes généraux [Fig. 5 du document original]

Limites

- Il est considéré que l'attaquant ne peut pas démonter le produit ou effectuer d'attaque physique (soudure, etc.).
- 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.
- La station d'administration doit être installée dans un local à accès contrôlé/protégé.