



Station d'analyse et de décontamination des supports amovibles

Cybersécurité des systèmes industriels

« Agence Nationale de la Sécurité des Systèmes d'Information Classe 1 :

• **Recommandation 233 :**
Une politique d'utilisation des médias amovibles devrait être définie

• **Recommandation 235 :**
Une station de décontamination devrait être installée afin d'analyser et décontaminer tous les périphériques amovibles avant de les utiliser sur un système industriel

• **Recommandation 236 :**
La connexion des périphériques amovibles qui n'ont pas été vérifiés par la station de décontamination devrait être interdite. »

La solution Schneider Electric

L'utilisation des supports amovibles sur le SI Industriel est quotidienne : extraction de données process, maintenance, gestion des patchs, récupération de journaux, mise à jour des systèmes d'exploitation et des firmwares sont des opérations obligatoires et régulières.

Les supports amovibles et les consoles de maintenance deviennent alors des vecteurs majeurs de propagation de virus y compris sur des systèmes isolés.

Dans un contexte de risques majeurs Schneider propose une solution de station d'analyse et de décontamination des supports amovibles répondant aux préconisations de l'ANSSI et qui protège des risques de corruption et de perte de données, d'arrêt de production ou de modification du comportement de votre SI.

Bénéfices client

Protéger votre SI des infections par supports amovibles :

- Une solution d'analyse et de décontamination autonome
- Une protection renforcée des systèmes industriels - SCADA
- Un contrôle strict des supports amovibles de vos prestataires
- Une intégration sans contraintes dans votre SI existant

Description de l'offre

L'offre SAS USB est une solution se composant de 3 éléments : une station blanche qui analyse et décontamine vos supports USB, un serveur qui pilote l'ensemble de vos bornes, récupère l'historique de leurs analyses, etc. Enfin avec l'agent WorkStation Protect, le Kub vous offre la possibilité de bloquer tous les périphériques externes n'ayant pas été analysés.

- Une station blanche composée de 2 à 5 moteurs antivirus
- Des mises à jours en mode « online » ou en mode « offline » dans des environnements durcis ou isolés.
- Contrôlez et protégez les accès à vos équipements, aux automates, en utilisant l'agent Workstation Protect. Bloquez l'accès des périphériques de stockage aux ports USB. Seuls les supports amovibles ayant été certifiés par un KUB seront autorisés pour une durée définie par votre politique de sécurité.
- Surveillez l'ensemble de l'activité de vos KUB grâce à la console d'administration permettant de récupérer l'ensemble de leurs analyses.
- Intégrez facilement votre architecture KUB avec vos outils de supervision (SIEM, Syslog, etc.)
- Utilisez l'écran de la station pour sensibiliser vos utilisateurs à la cyber sécurité en leur offrant du contenu sous forme de vidéo ou de texte pendant l'analyse de leur support.

Schneider Electric s'appuie sur la technologie Kub
Cleaner de KUB SOLUTIONS pour sa solution de
décontamination de périphériques

KUB

Powered by Netlor / Groupe RAS



Schneider Electric à votre service


Schneider Electric NEC - Network Engineering & Cybersecurity – est à votre disposition pour vous accompagner dans la mise en œuvre de Kub.

Contact : FR-NEC@schneider-electric.com

Schneider Electric
Direction Promotion et Communication
Centre PLM
F-38050 Grenoble cedex 9
Tél: 0 825 012 999
www.schneider-electric.fr

Réalisation : INEDITS L'Elan Créatif • Photos : Schneider Electric • Impression :

ZZ6079

Ce document a été imprimé
sur du papier écologique. 

09/2017