



# CyberTec - Console de maintenance sécurisée

Cybersécurité des systèmes industriels

*« Il a été décidé d'accorder un traitement spécial aux consoles de programmation et stations d'ingénierie qui apportent des outils additionnels importants à un attaquant. Leur présence permanente dans le système industriel suffit à justifier un niveau maximal. »*

Source : ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) - Méthode de classification et mesures principales.

## La solution Schneider Electric

Console de programmation durcie et sécurisée :

- Durcie pour résister aux contraintes industrielles
- Sécurisée pour résister aux cyber-menaces
- Validée avec les logiciels Schneider Electric installés

Protection contre les attaques ciblées et les nouveaux virus, mêmes inconnus :

- Sécurisation des ports de communication
- Blocage des accès Internet
- Gestion des clés USB et des périphériques amovibles
- Protection contre les virus de type « BadUSB »
- Chiffrement de données
- Barrage contre l'installation de logiciels indésirables
- Protection contre les APT

## Bénéfices client

Garder le contrôle des PC d'ingénierie et de maintenance :

- Gestion des consoles de programmation
- Filtrage des machines connectées aux SCADA et aux systèmes de contrôle-commande
- Gouvernance des sous-traitants

## Description de l'offre

CyberTec est une console de programmation et maintenance dont le système d'exploitation a été sécurisé, conformément au guide CIS et au guide de sécurisation de l'ANSSI, afin de résister aux cyber-menaces.

### Sécurisation du BIOS

- Boot uniquement sur le disque dur
- Option TPM activée
- Secure boot / UEFI



### Politique utilisateurs

Les politiques d'accès aux périphériques, d'exécution d'applications, de mise à jour, etc... sont dynamiques en fonction de l'utilisateur authentifié. L'utilisateur du quotidien ne dispose que des droits nécessaires au travail de tous les jours.

### Contrôle des exécutables

Seules les applications présentes dans la liste blanche peuvent s'exécuter, de plus la modification des fichiers et exécutables est contrôlée.

### Contrôle des périphériques

- Désactivation des périphériques, Bluetooth, Wifi, lecteur carte SD
- Contrôle des clés USB autorisées à se connecter par numéro de série
- Contrôle des drivers USB, interdiction de connecter des périphériques USB non connus

### Chiffrement

Afin de garantir la confidentialité des données contenues sur le disque dur, celui-ci est chiffré avec une solution certifiée EAL3.

### HIPS

Host-based Intrusion Prevention System est un outil de durcissement du système et de défense qui empêche l'exploitation des vulnérabilités logicielles.

## Caractéristiques techniques

### Un outil robuste adapté à l'industrie :

- Processeur Intel® Core™ i5-6300U vPro™
- Ecran 14» LCD HD (1366 × 768 pixels) Matrice Active (TFT)
- Design fin et léger (env. 1,99 kg et 29,8 mm)
- 4 Go RAM et Disque Dur SSD de 256 Go
- 3 ports USB 3.0, 1 port HDMI, 1 port LAN, 1 lecteur carte SD
- Excellente autonomie de la batterie jusqu'à 11 heures
- Véritable port série, VGA
- Température de fonctionnement de -10 C à +50 C
- Boîtier en magnésium robuste façon nid d'abeille et poignée de transport
- Résistance aux chocs et vibrations



### Schneider Electric à votre service

Schneider Electric NEC - Network Engineering & Cybersecurity - est à votre disposition pour vous accompagner dans la mise en service et la formation de CyberTec.

Contact : [FR-NEC@schneider-electric.com](mailto: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](http://www.schneider-electric.fr)

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

ZZ5472

Ce document a été imprimé  
sur du papier écologique.



09/2017