Foxboro Evo™

Protégez vos installations avec un système d'automatisation sécurisé

Avec Foxboro Evo, Schneider Electric propose une infrastructure de contrôle-commande sécurisée ainsi que des services en Cyber Sécurité conçus pour vous aider à vous conformer aux directives et/ou réglementations, et à protéger les actifs les plus critiques de vos sites : votre personnel, votre propriété intellectuelle et vos équipements. Foxboro Evo vous permet de fiabiliser votre process et d'intégrer la Cyber Sécurité dans le système de contrôle industriel.

Aperçu de l'offre

- ePolicy Orchestrator (ePO)
- Virus Scan
- Host Intrusion Detection (HIDS)
- Data Loss Prevention (DLP)
- Active Directory (A/D)
- Durcissement matériel
- Whitelisting
- Station Assessment Tool (SAT)
- Backup Exec System Recovery (BESR)

Avec le besoin croissant de sécuriser les infrastructures, le rôle du système Foxboro Evo est devenu de plus en plus important. Les fonctions de sécurité de la version « Security Enhanced » du système Foxboro incluent : la possibilité de gérer de manière centralisée les droits d'accès des utilisateurs (AD) et le système anti-virus (ePO), un système de détection d'intrusion (HIDS) et une détection de pertes de données (DLP).

Gestion centralisée de la sécurité

McAfee ePolicy Orchestrator (McAfee ePO) est un logiciel de gestion centralisée de la sécurité.
ePO facilite le déploiement et le management de la politique de sécurité sur les stations. Le déploiement d'agents sur les stations et la mise en œuvre de stratégies garantissent une sécurisation centralisée et en temps réel de vos équipements.

foxboro.com/foxboroevo

Life Is On Foxboro by Schneider Electric

Prévenir plutôt que guérir

Les analyses anti-Virus permettent de prévenir, détecter, et supprimer les logiciels malveillants. Ces derniers incluent, sans y être limités, les virus, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires.
La prévention et la détection en amont réduisent les menaces et les dommages potentiels aux biens et aux personnes.

Détecter une tentative d'intrusion

Le système de détection d'Intrusion (HIDS) surveille et analyse le fonctionnement interne d'un ordinateur. Il surveille tout ou partie du comportement dynamique et de l'état d'un système informatique. Outre les activités telles que l'inspection dynamique des paquets réseau visant spécifiquement cet ordinateur, un système HIDS peut détecter quel programme accède à quelles ressources. Il peut découvrir, par exemple, qu'un traitement de texte a soudainement, et de façon inexpliquée, commencé à modifier la base de données des mots de passe du système.

Certified Device ISASecure®

Plus d'informations sur le site :

www.foxboro.com/foxboroevo

Protégez vos équipements et votre propriété intellectuelle

Les systèmes de prévention de perte de données permettent aux entreprises de réduire les risques de divulgation involontaire d'informations confidentielles. Ces systèmes identifient, surveillent et protègent les données par l'inspection approfondie du contenu et l'analyse de la sécurité contextuelle.

• **Active Directory (AD)** est un service d'annuaire créé par Microsoft® pour les domaines réseaux Windows®. Active Directory permet une centralisation de l'administration et de la sécurisation des réseaux. Il permet d'authentifier et d'attribuer les autorisations aux utilisateurs et aux ordinateurs, d'appliquer les politiques de sécurité, et d'installer ou mettre à jour les logiciels. Les systèmes Foxboro sécurisés qui utilisent AD ont la possibilité de lier les politiques ePo à celles d'AD pour contrôler les ordinateurs Foxboro ainsi que pour la gestion des comptes Foxboro.

• **Le durcissement des stations Foxboro** est réalisé en usine (désactivation des ports, des composants Windows et des services non utilisés). Le durcissement du système est nécessaire car l'installation par défaut du système d'exploitation est davantage axée sur la facilité d'utilisation plutôt que sur la sécurité.

• **La mise en œuvre du « Whitelisting »** permet de n'autoriser l'exécution que de certains programmes identifiés (et par conséquence d'interdire tous les autres). Cela rend la protection plus simple puisqu'il ne faut se soucier que des logiciels connus.

Maintenir la sécurité sur toute la durée de vie de l'installation

Foxboro EVO Station Assessment Tool (SAT) est un outil installé automatiquement sur tous les postes de travail (à partir de la V8.5). Il permet un d'établir automatiquement un « état des lieux » de la station (versions logicielles, mises à jour de sécurité installées, etc..)
Symantec Backup Exec System Recovery (BESR) facilite la gestion des tâches de sauvegarde et de restauration des multiples stations du réseau. BESR permet de planifier les sauvegardes à exécuter automatiquement sans perturber l'utilisation du réseau. Il inclut un cryptage des sauvegardes.

Le changement est permanent : nouveaux employés, intervenants extérieurs, nouveaux OS, nouvelles versions de logiciels, modification ou mise en place d'une nouvelle unité de production. Ces changements constituent des failles qui peuvent être exploitées. Maintenir à jour et protéger votre installation au quotidien est un défi.
Le système Foxboro Evo « Security Enhanced » et les équipes Schneider Electric vous aident à répondre aux exigences de Cyber-Sécurité, à protéger vos investissements et à garantir un haut niveau de sécurité et de sûreté.

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 :

ZZ5573

Ce document a été imprimé sur du papier écologique.

09/2017