



Cybersécurité des systèmes industriels

Industrial Privileged Access Management (i-PAM)

« Les comptes bénéficiant de droits spécifiques sont des cibles privilégiées par les attaquants qui souhaitent obtenir un accès le plus large possible au système d'information. Ils doivent faire l'objet d'une attention toute particulière. »

ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) - Guide d'Hygiène Informatique - Mesure 5 des 42 mesures.



La proposition Schneider Electric

Que ce soit pour des questions de gestion de production, de planification, ou d'accès à distance, les systèmes industriels sont de plus en plus connectés aux systèmes d'information, et sont par conséquent confrontés aux mêmes problématiques de cybersécurité.

C'est dans ce contexte que Schneider Electric propose d'étendre les bonnes pratiques de sécurité informatique au monde industriel. De ce besoin est né l'i-PAM, une solution de gestion des accès à privilèges, conçue pour sécuriser et maîtriser les accès des exploitants, mainteneurs et des télé-mainteneurs aux architectures industrielles.

Grâce à ses fonctionnalités de traçabilité des connexions et d'imputabilité des actions, l'i-PAM permet aux industriels de définir et de savoir qui accède à quoi, quand, et pourquoi, prérequis indispensable pour une bonne mise en œuvre d'une politique de sécurité dans un environnement industriel.



Bénéfices clients

Protéger le parc d'automates et les SCADA contre les cyber-menaces tout en assurant :

- La conformité aux normes en vigueur (NIS, LPM, ISO 27000, NERC CIP, SP-800-82)
- La continuité de service
- La gestion facilitée des accès des prestataires externes
- Une intégration facilitée dans l'environnement existant et une adoption utilisateurs garantie

> Description de l'offre

L'offre i-PAM protège les comptes à privilèges des SCI et systèmes SCADA et trace les accès entre les Systèmes de Contrôle Commande, les environnements IT, l'Internet et les utilisateurs à distance. Basée sur la technologie Bastion de WALLIX, l'offre i-PAM est disponible dans des appliances industrielles qui possèdent des caractéristiques de résistance à la chaleur, aux vibrations ou encore à l'eau. i-PAM permet de :

- Optimiser la configuration avec l'auto-découverte de tous les comptes à privilèges Windows et Linux,
- Contrôler et protéger les accès aux équipements, aux automates et aux bus de terrain : gestion des identifiants, accord de connexion sur certains équipements et selon certaines fréquences,
- Appliquer une politique granulaire de connexion des utilisateurs internes et externes,
- Sécuriser et gérer la rotation automatique des mots de passe et des clés SSH, en particulier ceux des utilisateurs à distance avec le SCI,
- Isoler les systèmes critiques par le contrôle d'accès à des serveurs de rebond,
- Alerter en temps réel le département IT, les responsables de la technologie opérationnelle et l'équipe en charge de la sécurité afin de détecter, réagir automatiquement et stopper la progression d'une attaque en cours, réduisant ainsi au minimum les perturbations et les éventuels dommages causés à l'entreprise,
- Tracer et enregistrer les connexions, bénéficier d'un audit en temps réel et de reportings complets.

I-PAM s'appuie sur la technologie Bastion de WALLIX, seule suite logicielle certifiée CSPN par l'ANSSI.



Schneider Electric à votre service

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

Contact : FR-NEC@schneider-electric.com