Cybersécurité des systèmes industriels

Guide 2022

se.com/fr

Life Is On Schneider Electric

Cybersécurité des systèmes industriels

Une équipe dédiée Ingénierie Réseaux et Cybersécurité NEC (Network Engineering & Cybersecurity) accompagne les clients dans leur démarche de sécurisation d'infrastructures industrielles.

NEC : des compétences spécifiques

- **Sécurité des systèmes d'information**
  - Normes, standards
  - Méthodologies
  - Solutions

- **Métiers du contrôle commande industriel**
  - Chimie, pétrochimie
  - Production et gestion d'énergie
  - Traitement de l'eau

- **Technologie de l'informatique**
  - Systèmes d'exploitation
  - Bases de données
  - Serveurs web

- **Technologie du contrôle commande industriel**
  - Contrôleurs (PLC, DCS)
  - Supervision (SCADA)
  - Protocoles de communication

L’offre Cybersécurité industrielle

Les matériels et logiciels de contrôle commande Schneider Electric incluent nativement des fonctions de sécurité pour les protéger des cyber-attaques. Cependant, la sécurisation des systèmes industriels s’inscrit dans une démarche globale car les menaces sont multiples et la sécurisation est apportée par un ensemble de protections constituant la Défense en profondeur

1 Audit & évaluation

Inventaire et cartographie :
• Des outils développés spécifiquement pour la découverte des équipements industriels
• Protocoles : Modbus TCP, XIP, UMAS, Ethernet/IP, …

Audit :
• D’architecture, de configuration, de conformité
• Référentiel interne à votre société, ANSSI, IEC62443

Analyse de riques :
• Analyse de risques ISO27005 (EBIOS)
• Une grande expérience des “métiers industriels”

2 Conception

Conseil et expertise :
• Rédaction de cahier des charges et d’appel d’offre
• Rédaction de politique de sécurité
• Mise en place du tableau de bord de la sécurité

Conception d’architecture sécurisée :
• Projet neuf/Système existant
• Définition des étapes, du planning et des budgets compatibles avec vos contraintes
• Sélection de solutions de sécurité compatibles avec le fonctionnement de votre système (solutions testées et validées par nos soins)

3 Mise en œuvre

Intégrateur de multiples solutions :
• Infrastructure réseau
• Pare-feu, NIDS/NIPS, DPI
• Annuaire centralisé
• Sécurité endpoint centralisé (AV, HIPS, whitelisting, contrôle des médias…)
• Gestion centralisée des sauvegardes
• Surveillance du réseau et des équipements

Pour mettre en œuvre la Défense en profondeur, Schneider Electric propose un ensemble cohérent de briques de sécurité dédiées à la protection des automates, des réseaux, des postes de programmation et de supervision.

La loi de programmation militaire (loi n° 2013-1168 du 18 décembre 2013) a introduit d'importantes dispositions relatives à la sécurité des systèmes d'information des opérateurs d'importance vitale.
Ces nouvelles dispositions permettent de renforcer significativement la sécurité des systèmes industriels dont le rôle est primordial pour le fonctionnement de la Nation.

4 MCS (Maintien en Condition de Sécurité)

Pré-requis : connaître son système
- Inventaire et cartographie incluant références matérielles et versions logicielles
- Criticité des composants sur le système

Analyser les vulnérabilités
- Composants du système affectés

Sources d'information
- Sites constructeur (Schneider Electric, Arc informatique…)
- CERT (ICS, IST, privés)

Evaluer les risques
- Exposition (vraisemblance)
- Impact sur le système (perte de production, sécurité des personnes…)

Recommander un plan d'actions
- En fonction du niveau de risque
- Fourniture d'une fiche de vulnérabilité

5 Formation

	Production maintenance	Ingénierie, travaux neufs	Administration RSSI
Basique (1j) Sensibilisation du personnel. Les bonnes pratiques au sein de l'entreprise	☑		
Avancé (2j) Méthodologie, standards de cybersécurité. Utilisation, paramétrage de firewalls	☑	☑	
Expert (3j) Spécificités et protection des systèmes de contrôle-commande industriels		☑	☑

Sommaire

Cybersécurité des systèmes industriels

Assistance à la cartographie

Cybersécurité des systèmes industriels

« « Il est nécessaire d'établir une cartographie :

- *physique du système industriel,*
- *logique du système industriel,*
- *des applications,*
- *de l'administration du système ».*

« La cartographie et la documentation du système industriel devraient être revues régulièrement, à chaque modification du système industriel et au moins une fois par an..».

Source : Guide des mesures détaillées de l'ANSSI.
3.1.2-Cartographie (D.8,R.9)
à la loi de programmation militaire 2014-2019
– Règle 2 relative à l'homologation de sécurité

La solution Schneider Electric

Pour vous accompagner dans votre démarche de création ou de mises à jour de votre cartographie Schneider Electric vous propose un ensemble complet de solutions et de services dédiés. Outil indispensable à la maitrise de son système d'information (SI) et obligatoire pour les Opérateurs d'importance vitale (OIV), la cartographie du SI permet de connaitre l'ensemble des éléments qui le constituent pour en obtenir une meilleure lisibilité, et donc un meilleur contrôle. Elle s'intègre dans une démarche globale de gestion des risques.
Les experts Schneider Electric maîtrise la compétence (SCADA, réseaux, sécurité) et les outils afin de mener à bien cette mission.

Bénéfices client

Anticiper les projets à mettre en œuvre lors la mise en place d'une nouvelle stratégie.

- Assurer la maîtrise et l'évolutivité du SI, en fonction des mutations auxquelles peuvent faire face le métier ou l'organisation.
- Optimiser les coûts par la mutualisation et le calcul d'impact.
- Donner de la visibilité aux différents intervenants : l'utilisateur, le contributeur et l'administrateur
- Proposer un outil collaboratif, partagé par l'écosystème SI, sur la base d'un langage commun, compris par tous.

Description de l'offre

Objectif
L'objectif de cette prestation est d'accompagner le client dans la conception ou la mise a jour de sa cartographie.

Méthodologie
Définir avec le client, le périmètre de la cartographie.

De manière générale, la cartographie est composée de trois visions allant progressivement du métier vers la technique, elles-mêmes déclinées en vues.

- Vision métier

La vue de l'écosystème présente les différentes entités ou systèmes avec lesquels le SI interagit pour remplir sa fonction. La vue métier du système d'information représente le SI à travers ses processus et informations principales, qui sont les valeurs métier au sens de la méthode d'appréciation des risques EBIOS Risk Manager.

- Vision applicative

La vue des applications décrit les composants logiciels du système d'information, les services qu'ils offrent et les flux de données entre eux. La vue de l'administration répertorie les périmètres et les niveaux de privilèges des utilisateurs et des administrateurs.

- Vision infrastructure

La vue des infrastructures logiques illustre le cloisonnement logique des réseaux, notamment par la définition des plages d'adresses IP, des VLAN et des fonctions de filtrage et routage. La vue des infrastructures physiques décrit les équipements physiques qui composent le système d'information ou utilisés par celui-ci.

Périmètre technologique

L'ensemble des équipements d'automatisme de marque Schneider Electric ou de marque tierce est couvert par ce service.
Ces équipements incluent principalement :
- les Systèmes Numériques de Contrôle-Commande (SNCC ou DCS),
- les systèmes de supervision ou Supervisory Control And Data Acquisition (SCADA),
- les Automates Programmables Industriels (API),
- les Interfaces Homme Machine (IHM),
- les réseaux Ethernet ou propriétaires et les équipements réseaux (commutateurs, routeurs, pare-feux).
- les accès distants, l'interconnexion IT/OT,
- les serveurs d'administration, de sauvegarde, applicatifs, etc.

Schneider Electric à votre service

Schneider Electric NEC - Network Engineering & Cybersecurity – est à votre disposition pour vous accompagner dans la mise en œuvre du dossier d'homologation de vos infrastructures industrielles
Contact : FR-NEC@se.com

Audit de sécurité des systèmes d'automatisme et d'informtation industrielle

Cybersécurité des systèmes industriels

« Afin de s'assurer que le niveau de sécurité ne se dégrade pas au cours du temps, il est nécessaire d'effectuer régulièrement des tests ou des audits de cybersécurité. Ceux-ci peuvent être intégrés aux phases de maintenance et de tests fonctionnels. »

Source : ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) - Cybersécurité industrielle. Mesures détaillées.

La solution Schneider Electric

Schneider Electric NEC - Network Engineering & Cybersecurity – est à votre disposition pour mener à bien les audits de sécurité de vos infrastructures industrielles par rapport à un référentiel retenu : ce peut être celui de l'ANSSI ou celui de votre entreprise.

Bénéfices client

- Faire un état des lieux de l'existant : organisation, protection physique, architecture automates, réseau industriel, DMZ, configuration systèmes.
- Lister les écarts par rapport à un référentiel retenu suivant le niveau cybersécurité en place (LPM, directive NIS, guide des mesures détaillées de l'ANSSI, IEC 62443-3 validation du SLT).
- Faire état de recommandations afin d'améliorer le niveau de sécurité du SI industriel
- Proposer un plan d'actions et un accompagnement vers la sécurisation de votre installation
- Réalisation des audits dans le respect des règles fixées par le référentiel PASSI.

Description de l'offre

Partie Organisationnelle et physique

L'objectif est d'identifier et qualifier les vulnérabilités relatives aux différents processus d'exploitation du système et au management de la sécurité. L'audit peut être mené suivant un référentiel interne ou une norme comme par exemple l'ISO/IEC 27001, l'IEC 62443.

Les sujets abordés touchent les politiques et organisation de la sécurité, les interactions entre l'équipe industrielle et la DSI, la sensibilisation et formation des acteurs à la cybersécurité industrielle, les politiques de sauvegarde et restauration, les procédures de mises à jour et gestion des incidents, les indicateurs de suivi, l'intégration de la cybersécurité industrielle dans le cycle de vie du système (cahiers des charges, intégration, développement, tests), PRA, PCA.

L'audit concernera également la sécurité physique comme les moyens de contrôle d'accès physique, les moyens d'accès aux locaux et équipements, les moyens de détections d'intrusion et de surveillance.

Partie Architecture

Cet audit est initié par une analyse documentaire des différents supports techniques et fonctionnels : architecture réseau, plan d'adressage, matrice de flux. Il peut concerner également les interconnexions avec les réseaux tiers (autres sites, internet), l'intégration des stations d'ingénierie, les accès distants pour la maintenance. Il permet de vérifier la conformité aux pratiques de sécurité.

Partie Configuration (automatisme, réseau, SCADA)

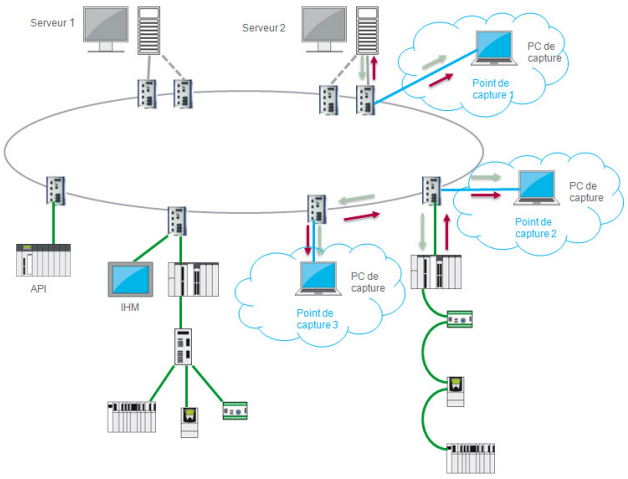
Cette partie permet de vérifier la bonne implémentation des solutions de sécurité constituant le système industriel par rapport aux « bonnes pratiques » (Guides de configuration, normes, etc.). Schneider Electric utilise des outils automatiques permettant la vérification des configurations systèmes. (Gestion des comptes, règles firewall, droits, stratégie de sécurité, etc.)

Nous analysons également la configuration des équipements réseaux tels que les switch, routeurs, firewall.

Quelque soit leur marque, nous analysons la bonne implémentation des protections de cybersécurité disponibles dans la gamme automate ou IHM concernée, les recommandations des fonctions à mettre en œuvre, analyse de l'exposition aux vulnérabilités découvertes et proposition de plan d'actions correctives.

Outils

Claroty, scripts automatisés.



Schneider Electric à votre service

Schneider Electric NEC - Network Engineering & Cybersecurity – est à votre disposition pour vous accompagner lors de cette phase d'audit de conformité de vos infrastructures industrielles.
Contact : FR-NEC@se.com

Analyse des risques

Cybersécurité des systèmes industriels

« L'analyse de risque constitue le cœur des mesures organisationnelles. Elle est le point de départ de toute démarche de cybersécurité et beaucoup d'autres mesures vont dépendre directement de celle-ci.»

Source : ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) - Cybersécurité industrielle. Mesures détaillées.

La solution Schneider Electric

L'analyse des risques est une étape essentielle dans un projet de sécurisation.
Elle permet d'identifier les scénarios de compromission, les vecteurs d'attaque, l'impact de ces scénarios sur le système et d'évaluer leur vraisemblance.
Nos experts sont à votre disposition pour mener à bien l'analyse de risque de votre système industriel, forts de leur expérience dans les métiers d'automatismes.

Bénéfices client

- Identifier les risques liés à vos process afin de les maîtriser.
- Etablir un plan d'action adapté à votre contexte (disponibilité de l'installation, coût financier, etc).
- Utilisation d'outils logiciels labellisés ANSSI.
- Utilisation de méthodes adaptées au contexte industriel.

Description de l'offre

Objectif

L'objectif de cette prestation est d'évaluer les risques auxquels vous devez faire face dans le cadre de l'exploitation de votre système d'automatisme et informatique industriel.
Cette évaluation des risques va permettre :
• d'identifier et d'évaluer l'ensemble des risques cyber vis-à-vis de votre process,
• de définir les actions correctrices,
• de prioriser ces actions et proposer un plan d'action.

Vis-à-vis de votre contexte, l'évaluation des risques vous permettra :
• de décider des mesures à déployer ou non et de justifier vos choix. Ainsi, le non-déploiement ou le report de déploiement d'une mesure, même si cela représente un écart par rapport à votre référentiel pourrait être justifié par un coût plus élevé que le coût estimé pour accepter le risque,
• de définir les priorités dans le déploiement des mesures.

Méthodologie

La méthodologie utilisée peut s'appuyer sur :
• la méthodologie EBIOS 2010 (Expressions des Besoins et Identification des Objectifs de Sécurité) ou RISK MANAGER 2018, méthodologie éprouvée dans le domaine et recommandée par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information),
• la méthodologie d'analyse issue de l'IEC 62433 (Identification du SLA) spécifique à la cybersécurité industrielle,
• la méthodologie issue de la norme ISO 27005,
• l'expérience et l'expertise de Schneider Electric de votre métier et des technologies mises en œuvre dans les systèmes d'information industrielle.

Périmètre technologique

L'ensemble des équipements d'automatisme de marque Schneider Electric ou de marque tierce est couvert par l'évaluation des risques :
• les dits-équipements incluent principalement :
• les Systèmes Numériques de Contrôle-Commande (SNCC ou DCS),
• les systèmes de supervision ou Supervisory Control And Data Acquisition (SCADA),
• les Automates Programmables Industriels (API),
• les Interfaces Homme Machine (IHM) et stations d'ingénierie,
• les réseaux Ethernet ou propriétaires et les équipements réseaux (commutateurs, routeurs, pare-feux),
• les serveurs d'administration, d'accès distant, de back-up, de journalisation.

L'activité humaine étant aussi un vecteur de menace, l'analyse de risque couvre l'ensemble des métiers directement liés à votre système d'automatisme, notamment :
• l'exploitation, dont les opérateurs de conduite de production
• la Maintenance, corrective, préventive ou toute activité de modification
• tout autre métier interagissant avec le système et qui sera porté à notre connaissance.

Schneider Electric à votre service

Schneider Electric NEC - Network Engineering & Cybersecurity – est à votre disposition pour vous accompagner lors de cette phase d'analyse de risque de vos infrastructures industrielles.
Contact : FR-NEC@se.com

Accompagnement à l'homologation

Cybersécurité des systèmes industriels

« L'opérateur d'importance vitale procède à l'homologation de sécurité de chaque système d'information d'importance vitale (SIIV), en mettant en œuvre la procédure d'homologation prévue par sa politique de sécurité des systèmes d'information (PSSI).»

Source: Arrêté sectoriel du 17 juin 2016 relatif à la loi de programmation militaire 2014-2019 – Règle 2 relative à l'homologation de sécurité

La solution Schneider Electric

Pour vous accompagner dans votre démarche d'homologation, Schneider Electric vous propose un ensemble complet de solutions et de services dédiés à la cybersécurité industrielle, depuis l'analyse des risques jusqu'au maintien en condition de sécurité, en passant par l'étude et la mise en œuvre de mesures de sécurité.
Les experts Schneider Electric maîtrisent la triple compétence (SCADA, réseaux, sécurité) nécessaire pour réussir le pari de la cybersécurité industrielle.

Bénéfices client

Préparation à l'audit de la sécurité des systèmes d'information d'importance vitale - SIIV

Gain de temps, économie de ressources grâce à l'accompagnement par nos équipes qui maitrisent parfaitement les exigences des arrêtés sectoriels, ainsi que les normes et les référentiels de cybersécurité industrielle.

Description de l'offre

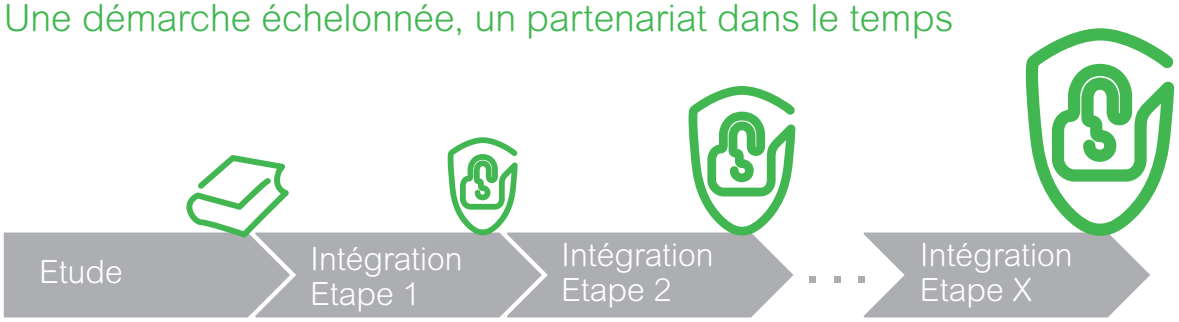
Objectif

L'objectif de cette prestation est d'accompagner l'opérateur d'importance vitale – OIV pour l'homologation de ses systèmes critiques.

Méthodologie

La démarche consiste à analyser le système et proposer un plan d'action visant à réduire les risques.
Elle est découpée en plusieurs étapes échelonnées dans le temps :
- l'analyse des risques,
- la réduction des risques à l'aide de mesures de sécurité organisationnelles et techniques,
- la justification de l'acceptation des risques résiduels.

Une démarche échelonnée, un partenariat dans le temps



Le dossier de sécurité est rédigé en parallèle de la démarche. Il permettra de simplifier la phase de validation qui sera effectuée par l'opérateur lui-même ou par un prestataire qualifié PASSI :
- audit de la sécurité du SIIV.

Périmètre technologique

L'ensemble des équipements d'automatisme de marque Schneider Electric ou de marque tierce est couvert par ce service.
Ces équipements incluent principalement :
- les Systèmes Numériques de Contrôle-Commande (SNCC ou DCS),
- les systèmes de supervision ou Supervisory Control And Data Acquisition (SCADA),
- les Automates Programmables Industriels (API),
- les Interfaces Homme Machine (IHM),
- les réseaux Ethernet ou propriétaires et les équipements réseaux (commutateurs, routeurs, pare-feux).

Maintien en condition de sécurité - MCS

Tout au long du cycle de vie de votre système industriel, de nouvelles vulnérabilités sont découvertes sur nos matériels et logiciels mis en œuvre dans vos process.
Grâce à notre contrat de service MCS vous êtes alerté lors de la survenance d'un nouveau risque détecté et nous vous proposons dans un délai de 72 heures une méthode de mitigation du risque adaptée.

Schneider Electric à votre service

Schneider Electric NEC - Network Engineering & Cybersecurity – est à votre disposition pour vous accompagner lors de la mise en œuvre du dossier d'homologation de vos infrastructures industrielles.
Contact : FR-NEC@se.com

Pare-feu STORMSHIELD SNi40

Cybersécurité des systèmes industriels

«Lorsque des flux non-IP doivent transiter entre deux zones distinctes, un filtrage devrait être effectué sur les identifiants source et destination. Par exemple, dans le cas d'Ethernet, on pourra effectuer le filtrage sur les adresses MAC source et destination.

Par ailleurs, on pourra faire un filtrage sur les protocoles autorisés.»

Source : ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) - Cybersécurité industrielle. Mesures détaillées.

La solution Schneider Electric

Co-développé avec Schneider Electric et Stormshield, le pare-feu SNi40 est un dispositif de sécurité souverain qui a fait l'objet d'une labellisation CSPN par l'ANSSI.

Les règles de filtrage du pare-feu Stormshield SNi40 permettent de configurer les requêtes de communication autorisées vers les systèmes de contrôle commande et les SCADA (lecture / écriture, commandes systèmes RUN, STOP…).

Le pare-feu SNi40 est spécialement conçu pour résister aux agressions extérieures des environnements industriels telles que les chocs, les interférences électromagnétiques, les poussières ou encore les températures extrêmes.
Sa fiabilité et ses possibilités de redondance assurent un haut niveau de disponibilité de vos procédés.

Bénéfices client

Protéger le parc automates et les SCADA contre les cyber-menaces :

- sécurisation des protocoles industriels,
- blocage des requêtes de lectures / écritures,
- blocage des tentatives de mise en STOP des automates programmables,
- filtrage des équipements connectés,
- fonction routage / mode transparent,
- fonction VPN IPSEC / SSL,
- certification ANSSI – CSPN,
- mise en œuvre par nos experts certifiés sur les technologies Stormshield.

Description de l'offre

Le pare-feu SNi40 pour réseaux Ethernet industriels est un dispositif de sécurité conçu pour protéger les réseaux industriels, les systèmes d'automatisme, les systèmes SCADA et les process contre les attaques informatiques (cyber attaques) externes.

Le pare-feu SNi40 offre une protection sur mesure pour la base installée et les nouvelles installations exigeant un niveau de sécurité et de disponibilité renforcés.

Il permet de délimiter des zones sécurisées au sein d'un système global. Le pare-feu SNi40 inclut les fonctions suivantes :

- pare-feu applicatif : permet de créer des règles qui identifient les équipements autorisés à communiquer à l'aide du protocole TCP-Modbus et gère le filtrage des requêtes Modbus et UMAS,
- routeur : assure le routage des paquets d'une interface réseau vers une autre,
- mode bridge (transparent),
- VPN : Gestion sécurisée des flux (IPSEC, SSL),
- consignation d'événements : maintien un fichier-journal des événements de sécurité et permet l'accès local ou distant à ce journal,
- haute disponibilité en architecture redondante,
- gestion d'authentification.

Caractéristiques principales

Connectivité

- Interfaces 10/100/1000 cuivre: 5
- Slots 1Gbps SFP : 2
- Port Série : 1
- Ports USB : 1 USB 2.0, 1 USB 3.0

Performances

- Débit Firewall (UDP 1518 octets): 4,8 Gbps

VPN

- Débit IPSec - AES128/SHA1: 1,1 Gbps

Protocole

- Supportés : Modbus, S7, EtherNet/IP, OPC UA
- En développement : IEC-60870-5-104, OPC DA (Classic)

Schneider Electric à votre service

Schneider Electric NEC - Network Engineering & Cybersecurity – est à votre disposition pour vous accompagner dans la mise en œuvre du pare-feu Stormshield SNi40.
Contact : FR-NEC@se.com

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 sur un système industriel.

• Recommandation 236 : la connexion des périphériques amovibles qui n'ont pas été vérifiés par la 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.

Schneider Electric à votre service

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

i-PAM bastion pour automates M580

Cybersécurité des systèmes industriels

" Tous les comptes disposant de privilèges importants comme les comptes administrateurs devraient être protégés par un mécanisme d'authentification comme un mot de passe par exemple. Les comptes utilisateurs et administrateurs devraient être strictement séparés ». « Des rôles devraient être définis, documentés et implémentés pour que les comptes des utilisateurs aient des privilèges correspondant exactement à leurs missions. "

La solution Bastion pour Automates M580

Que ce soit pour des questions de gestion de production ou d'accès à distance, les systèmes industriels sont de plus en plus connectés et sont 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 une solution de bastion industriel, conçue pour sécuriser et maîtriser les accès aux architectures industrielles.

Grâce à ses fonctionnalités de traçabilité des connexions le bastion 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

- Traçabilité

Garantir la traçabilité et enregistrer les connexions des accès entre les systèmes de contrôles commandes, l'environnement IT, internet et les utilisateurs sur site ou à distance.

- Sécurisé

Contrôler et protéger les accès aux équipements, aux automates et aux IHM par la gestion des identifiants avec accord de connexion sur certains équipements et à certaines fréquences.

- Solution plug & play

Solution préconfigurée pour un déploiement **simple et rapide.**

- Conformité aux normes de cybersécurité

Une solution unique sur le marché basée sur la technologie **Bastion de WALLIX, certifiée CSPN par l'ANSSI.**

Pré-requis

L'utilisateur doit possèder des droits "administration" sur la machine de maintenance.

Description de l'offre

Basée sur la technologie Bastion de WALLIX, l'offre i-PAM est une solution simple et préconfigurée (pour 2 automates et un maximum de 3 profils utilisateurs) pour sécuriser et maitriser les accès des exploitants, personnels lors de la mise en service, la maintenance et l'assistance à distance aux automates industriels.

Authentification de l'utilisateur

La connexion à l'automate s'effectue après :

- L'authentification de l'utilisateur par : login et mot de passe,
- Association des profils avec des droits spécifiques prédéfinis pour cet utilisateur : administrateur ou utilisateur,

Connexion de l'utilisateur au Bastion M580

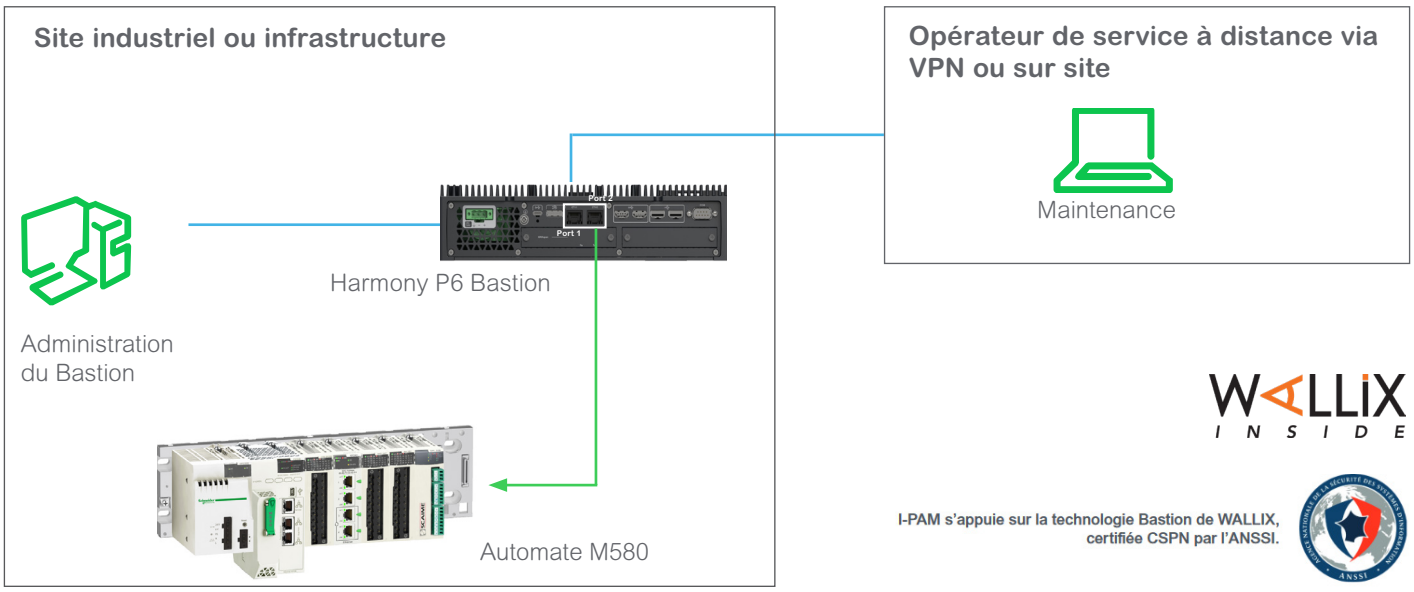
Etablissement de la connexion avec l'automate, et ouverture d'une session utilisateur.

Session de travail

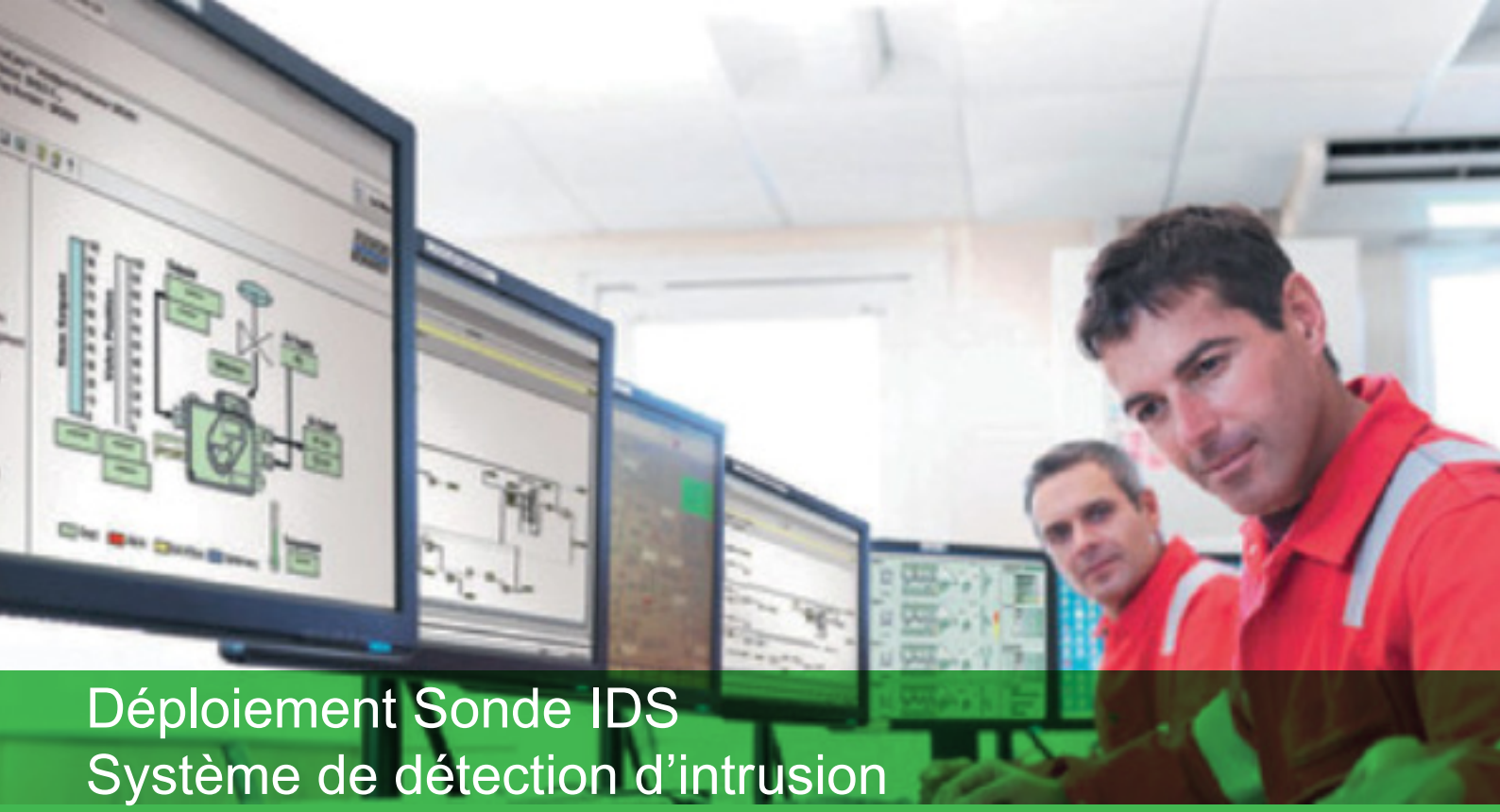
- La traçabilité des connexions sont disponibles en visualisation en temps réel,
- Ces informations sont stockées et restent disponibles si besoin, afin d'investiguer à la suite d'un problème détecté afin de trouver les causes.

Fin de Session

- Quand l'utilisateur a fini, il se déconnecte du bastion, le bastion termine la session automate.



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



Déploiement Sonde IDS
Système de détection d'intrusion

Cybersécurité des systèmes industriels

« « Il est recommandé de déployer des sondes de détection au niveau des passerelles d'interconnexion pour pouvoir analyser l'ensemble du trafic circulant entre les sites ».

« Une sonde de détection devrait être déployée au niveau de la passerelle de connexion pour pouvoir analyser l'ensemble du trafic entrant et sortant. »

ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) - Mesures détaillées [R.279], [R181]

La solution Schneider Electric

Pour vous accompagner dans la mise en place d'une solution de détection d'intrusion, Schneider Electric vous propose un accompagnement de la définition et du dimensionnement de la solution à sa mise en service.

Les experts Schneider Electric maîtrisent et ont l'expérience de la mise en place de solution de détection dans le milieu industriel sur de nombreux site de production

Bénéfices client

- Détection des menaces et des anomalies
(Identifiez les menaces zero-day et connues avec les cinq moteurs de détection de Deep Packet Inspection (DPI) de CTD.)
- Gestion des vulnérabilités
(Identifiez les appareils présentant des vulnérabilités connues pour une atténuation rapide et efficace.)
- La gestion d'actifs
(Découvrez et gérez automatiquement les appareils IoT et OT avec une interface centralisée et conviviale.)
- Console de gestion d'entreprise
(Consolidez et gérez de manière centralisée les données de plusieurs sites disparates.)

Description de l’offre

La plate-forme assure, de façon proactive, une protection des systèmes industriels de contrôle, ainsi qu’une surveillance des réseaux quant à des menaces cyber. Les responsables d’équipements industriels peuvent ainsi étendre leur politique de sécurité aux travailleurs à distance ainsi qu’aux prestataires externes accédant aux systèmes critiques, toutes les actions étant enregistrées. Cette détection en continu des menaces permet de dresser une cartographie précise des actifs industriels, d’identifier des configurations non conformes, de surveiller les interactions entre les différents équipements et de pointer des anomalies synonymes de malveillance.

Les alertes précises et contextualisées procurent aux responsables sécurité des sites industriels de précieuses informations. Ils peuvent ainsi efficacement mener l’enquête, et, si besoin, résoudre le problème et assurer rapidement un retour à la normale.

Une des caractéristiques essentielles de la plate-forme est sa capacité à explorer les niveaux les plus profonds des protocoles réseaux industriels sans incidence négative sur le système. Cela permet aux utilisateurs finaux d’identifier les anomalies tout en protégeant les réseaux industriels complexes et sensibles. Les logiciels de sécurité informatique traditionnels ont souvent recours à des requêtes actives qui laissent une trace sur le réseau. À terme, elles sont susceptibles de perturber les opérations. À l’inverse, la plate-forme adopte une approc

Schneider Electric à votre service

Schneider Electric NEC - Network Engineering & Cybersecurity – est à votre disposition pour vous accompagner dans la dans la mise en œuvre de sonde IDS.
Contact : FR-NEC@se.com

Maintien en condition de sécurité
Contrat de support

Cybersécurité des systèmes industriels

« Un processus de veille sur les menaces et vulnérabilités devrait être mis en place ».

« La gestion de l'obsolescence n'est pas directement une mesure de cybersécurité mais elle y contribue. Les équipements en phase d'obsolescence peuvent contenir de nombreuses vulnérabilités qui ne seront jamais corrigées. La gestion de l'obsolescence est un processus pouvant donc être utile et nécessaire pour la gestion des vulnérabilités. »

ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) - Mesures détaillées [R.85], § 3.3.8

La solution Schneider Electric

Schneider Electric a développé une offre de services innovante et personnalisable pour maintenir vos équipements dans un état de sécurité sur la base de votre référentiel :

- maintien en Condition Opérationnel,
- maintien en Condition de Sécurité,
- contrat de support technique.

Bénéfices client

- Meilleure maîtrise technique des installations réseau et surveillance de l'état de ces installations vis-à-vis des risques de cybersécurité.
- Accès aux experts Techniques en Cybersécurité de Schneider Electric.
- Être informé sur les évolutions réglementaires.
- Maintien dans le temps d'une base saine et performante pour la mise en place de vos applications d'automatisme.
- Meilleure maîtrise technique des installations réseau afin d'envisager en toute sérénité les évolutions futures.
- Optimisation des coûts de maintenance.
- Rapidité de remplacement en cas de défaillance matérielle et/ou logicielle.

Description de l'offre

Support technique téléphonique
- Accès téléphonique aux experts en Cybersécurité de Schneider Electric.
- Délai de prise en compte de la demande garanti.
- Intervention technique à distance ou sur site.

Abonnements logiciels
- Gestion de vos abonnement logiciels par un interlocuteur unique.
- Maintien à jour des logiciels.
- Surveillance du cycle de vie produit.
- Surveillance des vulnérabilités.

Gestion matérielle
- Maintien en Condition Opérationnel du matériel de cybeMatériel déployé (obsolescence, support constructeur, compatibilité).
- Gestion de la garantie du matériel / extension de garantie.
- Surveillance du cycle de vie produit.
- Surveillance des vulnérabilités.
- Maintenance périodique et maintien de la performance.
- Intervention d'Experts pour le contrôle de maintenance des installations.
- Mise à jour des équipements et logiciels.
- Contrôle de la performance des installations.
- Analyse des logs et défaillance du système.

Maintien des compétences techniques
- Tutorat sur les compétences techniques.
- Formation en cybersécurité.

Intervention express en Cybersécurité
- Aide au rétablissement de l'installation industrielle en cas de cyberattaque.
- Déplacement d'une équipe dédiée sous délai garantie.

Service Bureau
- Mise en place d'une équipe dédié.

Schneider Electric à votre service

Schneider Electric NEC - Network Engineering & Cybersecurity – est à votre disposition pour vous accompagner dans le maintien en condition de sécurité de vos installations.
Contact : FR-NEC@se.com

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 mesure 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.

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 principales

Un outil robuste adapté à l'industrie :
- Processeur Intel® Core™ i5-6300U vPro™
- Windows 10 Entreprise LTSC
- 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@se.com

Sécurité et disponibilité des process
Automate programmable Modicon M580 ePAC

Cybersécurité des systèmes industriels

« Pour les automates, lorsque les équipements le permettent, les mécanismes suivants devraient être activés :

• la protection d'accès à la CPU et/ou au programme ;

• la restriction des adresses IP pouvant se connecter ;

• la désactivation du mode de programmation à distance. »

« Les outils devraient être labellisés. »

Source : ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) - Mesures détaillées [R.218], [R220]

La solution Schneider Electric

La gamme d'automates programmables Schneider Electric M580 inclut nativement des fonctions de sécurité avancées pour protéger les process critiques des cyber-attaques

Sécurisation des accès :
Processeur, communications, mémoire, modes de fonctionnement.

Durcissement du système :
Contrôle d'intégrité, gestion des services inutilisés.

Traçabilité des évènements de sécurité :
Détection des tentatives d'intrusion et de corruption, journalisation des évènements (Syslog).

Les automates programmables de dernière génération Schneider Electric M580 sont développés selon le process Secure Development Lifecycle (SDL) qui garantit la gestion de la cybersécurité tout au long du cycle de vie du système.

Bénéfices client

Sécurité, fiabilité et conformité

- Sécurité et Fiabilité des opérations
- Facilité de configuration des paramètres de sécurité
- Conformité aux réglementations de cybersécurité les plus exigeantes (LPM / ANSSI).

Description de l'offre

Développé en conformité avec EDSA ISA Secure certification (IEC62443-4).
L'automate M580 dispose de fonctions de sécurité étendues :

Intégrité Système, Firmware, et Software.

- Vérifications d'intégrité du système en temps réel : processeur, mémoire, tâches système.
- Firmware M580 signé et chiffré : algorithmes SHA256 – RSA4096 – AES256.
- Logiciel applicatif signé avec vérification de signature permanente.

Contrôles d'accès renforcés.

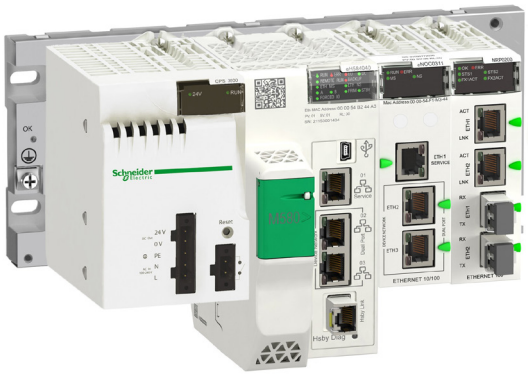
- Mots de passe chiffrés.
- Désactivation des services inutilisés : HTTP, FTP, EIP, DHCP, BOOTP, SNMP, ...
- Protection des modes RUN / STOP.

Communication sécurisée.

- Communication entre automate et console de maintenance sécurisée. Protocole IPSEC.

Conformité aux exigences en vigueur (IEC62443-4, LPM, ISO 27000, Achilles L2, ANSSI-CSPN).
Disponibilité des installations (fiabilité des matériels, mécanismes de redondance « Hot Standby »).

L'automate programmable Schneider Electric M580 est certifié 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 du M580.

Contact : FR-NEC@se.com

PLC-diag : surveillance d'état automate

Cybersécurité des systèmes industriels

« La mise en place de moyens de surveillance et de détection augmente la visibilité sur le système industriel concerné et augmente la vitesse de réaction en cas d'attaque, permettant d'en limiter les conséquences. »

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

La solution Schneider Electric

PLC-diag est une solution permettant de surveiller les automates programmables Schneider Electric du réseau industriel et d'afficher de façon centralisée les écarts de fonctionnement des automates (variation des temps de cycles, anomalies liées aux communications, modification des firmwares et des programmes applicatifs…) qui pourraient traduire une cyber-attaque.

Bénéfices client

Fournir un moyen de détection actif d'attaques sur les systèmes industriels :

- modification firmwares,
- modification programme applicatif,
- détection de nouvel équipement sur le réseau,
- surveillance de l'état des automates,
- détection de compromission des données,
- Journaux d'événements au format Syslog ou trap SNMP.

Description de l'offre

PLC-diag est un module qui interroge cycliquement les automates de gammes Schneider Electric.
Sa fonction est de détecter toute variation importante pour la sécurité : temps de cycles, charges des coupleurs de communication, modifications des logiciels embarqués (firmwares, applicatifs), dépassement de seuils des variables process... Ces informations sont remontées vers une supervision de sécurité via le protocole Syslog ou sous forme de trap SNMP.

Principales informations surveillées par le système :

- version des systèmes d'exploitation,
- version des applications,
- dépassements de seuils des variables API,
- temps d'exécution des tâches maître et rapide,
- nombre de requêtes de communication process traitées,
- nombre de requêtes http / FTP traitées,
- nombre de connexions TCP ouvertes en mode serveur / client.

Caractéristiques techniques

Le module peut fonctionner selon 2 modes :

- Inséré dans un rack automate Schneider Electric, il utilise le bus fond de panier pour remonter les informations de l'API.
- Installé sur rail DIN avec son alimentation, il fonctionne en autonomie et peut interroger jusqu'à 32 API de gamme Schneider Electric.

Certifications

- IEC/EN 61131-2
- CSA 22.2 No.142
- UL 508
- IACS
- CE
- CSA
- RohS
- ATEX

Schneider Electric à votre service

Schneider Electric NEC - Network Engineering & Cybersecurity – est à votre disposition pour vous accompagner dans la mise en œuvre de la solution PLC-diag.
Contact : FR-NEC@se.com

Formation

Cybersécurité des systèmes industriels

« La formation des intervenants sur un système industriel est un élément indispensable pour en assurer la cybersécurité.

La formation devra contenir les éléments de sensibilisation aux risques induits par les technologies de l'information et de la communication ainsi qu'une présentation de la politique de sécurité des systèmes d'information.»

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

La solution Schneider Electric

Afin de former l'ensemble du personnel d'une entreprise, Schneider Electric a développé des modules de formation dédiés à la cybersécurité des systèmes industriels. Nos stages sont dispensés dans nos locaux ou sur site client ; nos formateurs sont des experts de terrain confrontés au quotidien à vos contraintes industrielles.

Bénéfices client

Un parcours de formation adapté aux exigences industrielles et aux différents interlocuteurs de l'entreprise :

- Sensibilisation du personnel aux cyber-risques.
- Connaissance des standards et méthodologies.
- Conception, administration et maintenance.
- Formation labélisée SecNumedu-FC.

SecNumedu
ANSSI

Description de l'offre

	Production Maintenance		
SENCYB (1j) Formation 1er niveau du personnel. Les bonnes pratiques au sein de l'entreprise	☑		
CYBINDUS (3j) Spécificités et protection des systèmes de contrôle-commande industriels.		☑	☑

SecNumedu
ANSSI

Formation SENCYB

Plus qu'une sensibilisation, il s'agit d'une formation de premier niveau pour comprendre les risques et les enjeux, et intégrer les bonnes pratiques.

• Objectif :
- être informé sur les risques et les cyber-menaces,
- comprendre et accepter les règles de bonne pratique de sécurité.

• Moyen :
- présentations, films, ateliers pratiques

Formation CYBINDUS

La formation Cybindus a reçu l'attestation de conformité au référentiel SecNumedu Formation Continue.

• Objectif :
- comprendre les spécificités des systèmes de contrôle-commande industriels,
- comprendre les difficultés à résoudre pour sécuriser ces systèmes,
- identifier des solutions viables dans un contexte industriel,
- être en mesure de définir un plan de sécurité pertinent/

• Moyen :
- travaux sur plateforme de démonstration Cybersécurité industrielle Schneider Electric.

Schneider Electric à votre service

Schneider Electric NEC - Network Engineering & Cybersecurity – est à votre disposition pour adapter le parcours de formation à vos besoins spécifiques (prise en compte de votre référentiel SI, de vos contraintes architectures et produits utilisés).
Contact : FR-NEC@se.com

Life Is On | Schneider Electric

se.com/fr

Schneider Electric France
Direction Marketing Communication France
35, rue Joseph Monier - CS 30323
F92506 Rueil-Malmaison Cedex

Conseils et services
se.com/fr/contact

07/2022 - ZZ7220-B