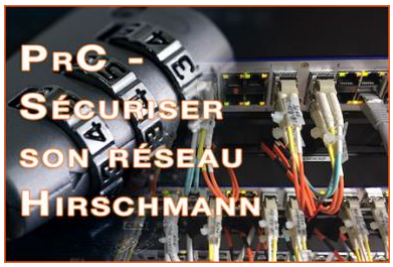
AB inter NET work

Formation Produit

INGENIERIE MISE EN SERVICE AUDIT FORMATION

PrC – Cybersécurité sur le matériel Hirschmann



Après avoir suivi la formation **EiS** qui vous présente l'état de la situation concernant la cybersécurité des sites industriels - enjeu majeur affiché par le gouvernement français avec ses spécificités et besoins – nous aborderons ici les différentes solutions de protection et plus spécifiquement celles adaptées aux équipements de la marque Hirschmann. Pour utilisateurs confirmés en Hirschmann. L'objectif est de comprendre dans le détail les principes et les cibles de la cybersécurité, savoir mettre en œuvre les demandes de l'ANSSI en environnement industriel ainsi que les protections associées (en prenant en compte les attentes spécifiques sur le matériel Hirschmann).

Objectif du cours

Connaître et Mettre en œuvre les différents niveaux de sécurité tel que recommandé par l'ANSSI sur les switchs Hirschmann autant sur la plateforme Classic que HiOS.

Profil des participants

Ingénieur de production ou études, responsable du réseau industriel, maintenance évoluée.

En situation de handicap ? nous contacter

Prérequis

EiA & PrS impératif

Il est fortement conseillé d'avoir suivi le cours **EiS** au préalable.

Matériels utilisés

Fourni : switchs/routeurs et pare-feu Hirschmann (1 pour 2 pers.).

Le **PC est impératif** et à la **charge des participants** (min. 1 pour 2 pers.) avec droit admin. local (installation logiciels & désactivation de pare-feu)

Formateurs

Ils interviennent aussi sur le terrain (60% / 40%) - exclusivement en Hirschmann ; plus de 10 ans de compétences dans les réseaux industriels ; formateurs officiels Hirschmann et certifiés :

HIRSCHMANN HiNE CERTIFIED HIRSCHMANN HiSE CERTIFIED HIRSCHMANN HiSP CERTIFIED

Pédagogie / Évaluations

- Alternance de théorie (**50%**) et pratique (**50%**) ou **(30/70)**
- Vérification des acquis par la pratique – pas de quiz !

Support de cours : **198p** couleur

Durée : - **3** - **jours** x 7 heures

Max : 10 pers. – *idéal* : 4-6pers.

Contenu – réactualisé en 2022 - complété en novembre 2023

IV – Sécuriser votre réseau Hirschmann (198p)

- Documents ANSSI pour vous guider
- Vulnérabilités Hirschmann
- Type d'attaques / Fonctions de Sécurité (HiOS).
- Fonctions de sécurités en L2P/L3P (Classic v9)

Protéger votre équipement réseau

- Bannière d'accès. Activer les bons protocoles d'administration.
- SSH et génération d'une clé spécifique.
- Comptes utilisateurs, rôles et mot de passe.
- Authentification d'accès au switch via Radius. Désactivation des comptes usuels.
- Protection des accès automatismes non sécurisés.
- Chiffrement de la configuration.
- Fermeture des ports.
- Limiter/Désactiver le PoE. ACD : Détection des conflits IP du switch.
- Etat de la sécurité

Renforcer les politiques d'accès au réseau

- Redondances et protections anti-boucle
- Limiter les trafics de diffusion.
- Sécuriser les vlans.
- Sécuriser le routage.
- Accès Radius et 802.1x des équipements terminaux.
- Notification de réapprentissage /de changement d'adresse MAC.
- Sécurité par port (adresses MAC). Contournement des limites HiOS sur la sécurité par port.

Contrôler le trafic réseau malicieux

- Limiter les trafics de diffusion.
- Prévention DOS. Attaque et prévention DHCP snooping.
- Protection avec Inspection Dynamique ARP.
- Protection avec IP Source Guard. Access Control Lists. ACL temporelle, ACL orientée connexion.

Journalisation et analyse

- Mise à l'heure.
- Journaux persistants Audit Trail, Log CLI/SNMP.
- Alarmes SNMP / e-mails.
- Syslog. sFlow.

Supervision et sécurité

- Contrôle des points de sécurité à partir de industrial Hivision 6`
- Paramètre cryptographique, SNMP v1/v2/v3, Trap SNMP v1/v3.
- Détecter/suivre les changements de configuration d'un switch Classic.
- Syslog.
- Détecter les intrus.
- Identifier les attaques de MAC Spoofing.

Documentation du réseau

En Pratique (exercices)

- Sécuriser un switch Hirschmann : niveau basique ; niveau avancée et expert : 44 règles pour Hirschmann et 71 règles ANSSI + règles AB inter NET work
- Génération et changement de certificats numérique
- Comptes nominatifs et centralisés
- Mise en place d'un serveur radius et 802.1x
- Sécuriser les Vlans
- Sécurité par Port & Contournement via ACL pour autoriser un constructeur MAC.
- Authentification radius des utilisateurs
- Mettre en place une sécurité anti-boucle cuivre Sécuriser les redondances.
- Surveiller les changements de configuration
- …