

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. Enfin, nous terminons le cours par un examen plus en détail des trois protocoles de l'automatisme industriel : Profinet, ModBus/TCP et Ethernet/IP.


Contenu

Objectif du cours

Connaître et Mettre en œuvre les différents niveaux de sécurité sur les switches Hirschmann autant sur la plateforme Classic que HiOS. Comprendre le fonctionnement des protocoles industriels usuels afin d'en définir les règles de filtrage ...

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 : switches/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 :



Pédagogie / Évaluations

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

Support de cours : **199p** couleur

Durée : - **3 - jours** x 7 heures

Max : 10 pers. – idéal : 4-6pers.

IV – Sécuriser votre réseau Hirschmann (256p)

- o Type d'attaques / Fonctions de Sécurité (HiOS).
- o Fonctions de sécurités en L2P/L3P (Classic v9)

Protéger votre équipement réseau

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

Renforcer les politiques d'accès au réseau

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

Contrôler le trafic réseau malicieux

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

Journalisation et analyse

- o Mise à l'heure.

- o Journaux persistants Audit Trail, Log CLI/SNMP.
- o Alarmes SNMP / e-mails.
- o Syslog. sFlow.

Supervision et sécurité

- o Contrôle des points de sécurité à partir de industrial Hivision 6.
- o Détecter/suivre les changements de configuration d'un switch Classic.
- o Syslog.
- o Détecter les intrus.
- o Identifier les attaques de MAC Spoofing.

Documentation du réseau

V - Protocoles automatismes et sécurité (126p)

- o Présentation des 3 grands protocoles industriels.
- o Détail des échanges Profinet S7 ; PN-IE ; Profinet IO / SRT / IRT / Profisafe.
- o Détail des échanges ModBus/TCP. IO scanning ; Global Data ; RTPS.
- o Détail des échanges Ethernet/IP ; Messagerie ; I/O.
- o OPC, Ancien modèle : OPC DA et Nouvelle architecture : OPC UA

En Pratique (exercices)

- o Sécuriser un switch Hirschmann : niveau basique ; niveau avancée et expert
- o Mise en place d'un serveur radius et 802.1x.
- o Mise en place d'ACL et configurations de règles avec un pare-feu stateful.
- o Examen de captures de flux automatismes.