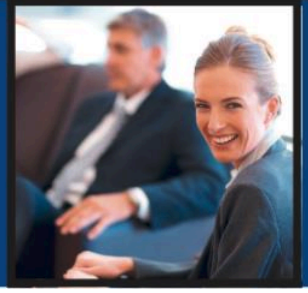
Be Certain with Belden

En partenariat avec



Cybersécurité sur le matériel Hirschmann (PrC)

Cible

Cette formation a été conçue pour fournir une mise en pratique avancée pour les ingénieurs de production, de maintenance ou d'études devant mettre en œuvre des protocoles de sécurité réseau.

Pré-requis

Les participants doivent suivi les formations **CT1, CT2 et CP1** impérativement avant celle-ci ou avoir des connaissances approfondies sur Ethernet, IP, TCP et UDP, ainsi qu'une bonne maitrise des produits Hirschmann (vlans, redondances, diagnostics …). Il est conseillé d'avoir suivi le cours **EiS** au préalable.

Objectif

Comprendre dans le détail les principes et cibles de la cyber-sécurité, les demandes de l'ANSSI en environnement industriel ainsi que les protections à mettre en œuvre. Aller plus loin dans la connaissances des 3 protocoles de l'automatisme industriel : Profinet, modBus/TCP et Ethernet/IP.

Contenu de la formation

IV – Sécuriser votre réseau Hirschmann (308p)

- 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).

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

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.
- 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
- Authentification radius des utilisateurs
- Mise en place d'ACL et configurations de règles avec un pare-feu stateful.
- …

Après avoir suivi la formation EiS qui vous présente l'état de la situation concernant la cyber-sécurité des sites industriels - enjeu majeur affiché par le gouvernement français – nous aborderons ici les différentes solutions de protection et plus spécifiquement celles adaptées aux équipements de la marque Hirschmann. La mise en sécurité d'un switch/routeur Hirschmann (v9 et/ou HiOS) sera examinée en détail avec des mises en pratique. Authentification Radius, Des maquettes avec des switchs, routeurs et pare-feux seront utilisées pour vous former sur ces mécanismes.

Ce cours vous apporte les bonnes pratiques à appliquer sur le matériel Hirschmann selon les concepts préalablement abordés dans la formation EiS concernant la sécurité en environnement industriel.

Le PC est impératif et à la charge des participants (min. 1 pour 2 personnes) avec droit d'administrateur local (installation de logiciel et désactivation de pare-feu).

Langue

- PrCf Français

Durée

3 jours
9:00 – 17:00

Calendrier / lieu / prix

https://www.abinternetwork.com/cursus-belden

Actualisation

Réactualisé en 2022 – complété en 2023