En partenariat avec :

la Sécurité en environnement industriel (EiS)

La cyber-sécurité des sites industriels est un enjeu majeur affiché par le gouvernement français. Nous aborderons dans ce nouveau cours, entièrement refondu en 2019, les différents concepts inhérents à la sécurité : des concepts de base comme les architectures, les menaces, les cibles et les attaquants, les bases de la cryptographie ainsi que les mécanismes utilisés de plus en plus en environnement industriel et ceux qu'il faudrait utiliser ; les faiblesses des protocoles utilisés (industriels et bureautiques) et comment se protéger par logiciel et avec quel matériel.
Un focus sera mis sur le cadre demandé par l'ANSSI et leurs recommandations.

Ce cours vous apporte les bases théoriques que vous pourrez mettre en pratique dans la formation PrC de mise en sécurité du matériel Hirschmann

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).

Cible

Réactualisé en 2023, cette formation apportera une connaissance théorique aux décideurs, ingénieurs de production, de maintenance ou d'études devant prendre en compte les risques et les contraintes de la sécurité sur les réseaux industriels.

Prérequis

Les participants doivent suivi les formations **CT1 et CT2** impérativement avant celle-ci ou avoir des connaissances approfondies sur Ethernet, IP, TCP et UDP.

Objectif

Dans ce cours, les participants apprendront les bases théoriques et tous les fondamentaux liés à la sécurité réseaux : des menaces, des attaquants, de l'analyse de risques jusqu'au logiciel et matériel pour se protéger. Un chapitre est dédié aux exigences de la LPM et des recommandations de l'ANSSI en environnement industriel ainsi que les risques qui ciblent ce milieu ainsi que sur les nouvelles règles Européennes.

Contenu de la formation

I : Enjeux dans les réseaux industriels (291p)

A – Contexte
Différences Réseau OT vs IT. Sécurité vs Sûreté. Statistiques et les attaques dans l'actualité. La sécurité dans l'industrie ?

B – Protéger quoi contre qui ?
Attaquants et motivations. Menaces. Objectifs & Mécanismes à protéger. Cibles des attaques. Méthodologie typique d'une attaque et Anatomie de 3 attaques. Protocoles réseau fragiles / sécurisés.

C – Architecture des réseaux industriels
Architectures anciennes, actuelles, et recommandées. Modèle CIM. Industrie 4.0. Ne pas être connecté : une protection efficace ? Défense en profondeur : zones et conduites. Exemple de zones dans un système ferroviaire

D – Attaques sur les mécanismes réseau
Attaques de déni de services. Attaque du modèle OSI. Spoofing : usurpation ARP / DHCP / DNS. MAC flooding. Attaques via boucle cuivre ; sur les redondances MRP / HR /RC/RSTP ; de vlans ; de routage (RIP, OSPF, VRRP). Sur protocole automatisme.

E – Base de Cryptographie
Définitions - Notion et utilité du chiffrement. Chiffrement symétrique / asymétrique. Authentifier et sécuriser. Clé de sessions. Fonction de hachage. Empreintes et signatures numériques. Chiffrement des échanges. Certificat numérique et utilisation. Vérification. Certificat PGP et X509. Certificats autosignés. Classes de certificats. Encodage X509. Chiffrement et Métadonnées

II : Mettre en œuvre la sécurité (243p)

A – Analyse des risques et Normes. (119p)
Cycle de vie de la sécurité. Niveaux. Stratégie de base. Evaluation des risques. Construire/évaluer son modèle d'analyse des risques. EBIOS et EBIOS RM. Normes : IEC 62443 – ISA 99 – ANSSI – Directive NIS et NIS2. Autres réglementations (Résilience des Entités Critiques, CLOUD ACT, DORA, CRA…) – les assurances cyber – Audit cyber sécurité AB inter NET work

B – Classifications des systèmes d'information industriels (60p)
Réglementation française ; Définitions. Désignation d'un OIV et liste des OIV. Arrêtés sectoriels. Obligations des OIV. Classes 1, 2 & 3. Classification des SII : Exposition, Vraisemblance, Impact. Documents importants sur le site de l'ANSSI.

C – Recommandations de l'ANSSI (64p)
13 Bonnes pratiques pour les systèmes industriels. Règles d'hygiène informatique. Renforcer la sécurité de son SI en 42 points.
Règles de mise en sécurité : profils SCADA / switch / HiOS vs Classic / pare-feu

III : Se protéger en environnement industriel (173p)

A – Protection logicielle
Mot de passe et 2FA. Chiffrement. Choix d'un VPN. Désactivez les ports USB et SMB1. Vos identifiants sont-ils diffusés? RDP. Déchiffrer les attaques de certains ransomwares. OS cloisonnés

B - Protection matérielle
Clés USB : préservatifs et inspection.
Isolation des échanges : pare-feu, tap optique, diode, passerelles. Pare-feux vs ACL. Stateful/Stateless. DPI. Comment écrire les règles ? OPC DA. UTM Stormshield. Surveillance des évènements : Syslog/SIEM. Surveillance du trafic : sFlow/Sondes passives. IDS – IPS – honeypots

C - Gouvernance
NOC-SOC-MOC. PDIS. PCA & PRA. Zero-trust. Assurances. Réagir en cas d'attaque.

En Pratique (exercices)

- Démo de RAZ d'un switch via Ethernet/IP sans droit.
- Démo d'une attaque de type ARP spoofing. Scan d'un réseau.
- Vérification d'une empreinte SHA.
- Mise en place d'OpenGPG pour chiffrer des documents et des emails. Zed! Encrypt.
- Générer un certificat X509.
- Calculer la classe OIV d'un site industriel.

Langue

- EiSf Français

Durée

5 jours
9:00 – 17:00

Calendrier / lieu / prix

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

Actualisation

Actualisé en 2023