MAJ 05/08/2024

Formation « Responsable cybersécurité industrielle »

Réf : RSSIINDUS

De plus en plus de personnes sont en charge de la cybersécurité industrielle dans les entreprises. Les fonctions de cybersécurité industrielle nécessitent un mix de compétences peu communes sur le marché. Cette formation permet d'accélérer la montée en compétence et prise de fonction d'un responsable cybersécurité dans le domaine industriel via les cours théoriques et panorama mais aussi via des retour d'expériences de RSSI OT ayant pris leur poste depuis plusieurs années.

Objectifs

- Accompagner la prise de fonction d'un responsable cybersécurité industrielle
- Fournir un panorama des connaissances à avoir et des sujets à traiter en cybersécurité industrielle en tant que RSSI
- Donner des directives sur le séquencement des actions à mener, les priorités et l'organisation de la cybersécurité industrielle
- Avoir une visibilité de l'offre disponible sur le marché en termes de solutions et de services spécifiques à l'OT

Durée & horaires

- 3 jours soit 21 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- RSSI ou RSSI adjoint en charge de l'OT
- Responsable cybersécurité, sécurité industrielle
- Correspondants cybersécurité OT
- Consultants en sécurité

Pré-requis

- Formation HS2 SECUCYBER (bases) ou formation équivalente ou expérience comparable
- Formation HS2 SECUINDUS (spécificités SI industriels) ou formation équivalente ou expérience comparable
- Connaissance de bases du fonctionnement des réseaux Ethernet / IP

Méthode pédagogique

- Cette formation est proposée en mode présentiel et peut être accessible en mode distanciel via ZOOM pour les personnes qui ne peuvent ou ne veulent pas se déplacer
- Cours magistral
- Retours d'expérience de RSSI OT
- Démonstrations

Supports

- Support de cours en français au format papier pour le présentiel et au format numérique pour le distanciel (sous réserve du règlement intérieur signé)
- Tous les documents nécessaires à la formation en français ou anglais

- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **À l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h00 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification RSSIINDUS par HS2.**

Programme

Module 0 : Introduction

Introduction sur le monde de la cybersécurité industrielle

- Définition
- Historique
- Architecture types
- Composants
- Acteurs
- Spécificités du monde industriel
- Cybersécurité industrielle

Module 1 : RSSI industriel, son rôle et étapes de construction de sa feuille de route *(roadmap)*

Rôle du RSSI industriel

5 étapes de construction de sa feuille de route *(roadmap)*

- Sensibilisation et communication
- Réaliser des états des lieux de cybersécurité
- Réaliser des analyses de risques
- Construire sa politique de cybersécurité industrielle
- Définir sa feuille de route *(roadmap)*

Focus sur le Cadres *(framework)* opérationnel de cybersécurité industrielle

- Conception de politiques implémentables en usine / en réseaux de transport / en systèmes embarqués
- Utilisation des modèles opérationnels de cybersécurité industrielle

Module 2 : Projets prioritaires pour la sécurisation des sites industriels

Focus sur les projets prioritaires pour les sites industriels

- Rôles et responsabilités
- Sensibilisation et formation
- Cartographie et inventaire
- Cloisonnement réseau (zones & conduits…)
- Accès distants
- Sauvegardes

Module 3 : Suite des projets de sécurisation des sites industriels

Focus sur d'autres thématiques cybersécurité industrielle, chaque thématique abordant également l'offre disponible sur le marché en termes de solutions et de services spécifiques à l'OT

- Gestion des comptes et des droits (AD ou pas, si oui comment)
- Antivirus / EDR
- Filtrage applicatif / data DN-iodes
- Durcissement des systèmes

- Gestion des supports amovibles
- Gestion de l'obsolescence
- Mises à jour des systèmes
- Gestion des incidents et gestion de crise
- Continuité et reprise d'activité
- Journalisation et détection (NIDS OT, SOC & SIEM, sondes)
- Gestion des risques en cybersécurité industrielle (exemple avec EBIOSRM)
- Audit & Contrôle
- Sécurité dans les projets (PAS – Plan d'assurance sécurité)
- Gestion des fournisseurs

Module 4 : Mission du RSSI industriel à l'échelle de son entité
Activités clés à mener au niveau de l'équipe du RSSI indus

Facteurs clés de succès

Notes complémentaires

Module 5 : Les normes et réglementations
Focus sur les standards et les réglementations

- Quelles normes / quel cadre *(framework)* utiliser ? (NIST, 62443, ANSSI…)
- Réglementations (CSF, NIS2…)

Groupes internationaux : comment concilier règles corporate et spécificités

Module 6 : Focus sur le RUN
Après le BUILD, comment assurer le RUN ?

Conclusion

Examen

Pour aller plus loin

Nous vous recommandons de suivre les formations suivantes :

Formations axées sur le juridique :

- **SECUDROIT – Droit de la cybersécurité**

Formations axées sur l'organisationnel :

- **SECUPROJET – Security by Design**
- **EBIOS2018 – EBIOS 2018 Risk Manager**