Programme de la formation

La cybersécurité sans faille

En groupe sur site

21 heures sur 3 jour(s)

Tout public · De 1 à 10 participants

400 € HT / 480 € TTC par participant

Description courte

Le développement des réseaux, la multiplication des briques logicielles et matérielles, l'utilisation de nombreux terminaux et des objets connectés sont autant de facteurs augmentant les risques pouvant porter atteinte à la sécurité de l'I.T. (Information Technology), de l'O.T. (Operational Technology) et de beaucoup d'autres items

Pour avoir une cybersécurité sans faille, Il est nécessaire d'avoir une gouvernance technique et organisationnelle globale et rigoureuse car la solidité d'une chaîne est donnée par la solidité du maillon le plus faible

Dans ce cours concret, le stagiaire apprendra les techniques et l'organisation à mettre en œuvre pour assurer une forte cybersécurité avec des exemples concrets.

Profil des participants

DSI, RSSI, technicien sécurité, auditeur, chef de projet, architecte du SI, concepteur-développeur; administrateur système ou réseau, et plus généralement toute personne s'intéressant à la cybersécurité

Prérequis

Connaissance de base en informatique

Objectifs

- Connaître les intrusions, les menaces et les défauts potentiels sur l'I.T., l'O.T., le réseau,

  les accès physiques, les locaux

- Apprendre les techniques à mettre en œuvre pour prévenir ou sinon corriger ces intrusions,

  ces menaces et défauts et comment les agencer et les superviser

- Mettre en place une organisation et une gouvernance adéquates

Aptitudes et compétences visées / attestées

Physiquement l'I.T. et l'O.T. sont constitués de systèmes (informatiques ou industriels) situés dans des locaux ou embarqués, et de terminaux locaux ou distants, fixes ou mobiles, le tout communiquant par des réseaux. Il est donc nécessaire de protéger chaque composant et leurs interconnexions et d'avoir une vision globale et sans faille de l'ensemble

Contenu

1. **Les principes de base de la cybersécurité**

- Information Technology, Système d'Information, Operational Technology

- Qu'est-ce que la cybersécurité ?

- L'importance de la cartographie statique et dynamique

- L'identification des agents de menaces : les malwares, les virus, les bugs logiciels, les maladresses, les catastrophes naturelles, etc.

- Recenser les vulnérabilités possibles à partir des menaces et de la cartographie

- Les standards : ANSSI, CVE, CERT-FR, OWASP, NIST etc.

- La politique de sécurité et la défense en profondeur

- Exercices

2. La sécurité des systèmes

2.1 Les systèmes informatiques I.T.

- Les exigences et les différentes architectures

- Sécuriser les logiciels de base : systèmes d'exploitation, SGBD, utilitaires

- Les outils pour l'intégrité des données stockées et de flux

- Les outils pour la disponibilité du service

- Comment sécuriser les applications, les webservices et les serveurs. Les problèmes liés à la virtualisation

- Les pentests (tests d'intrusion), le SIEM, les techniques d'Inforensic

- La supervision logicielle et métier, l'Intelligence artificielle, le Big Data

- Exercices

2.2 Les systèmes industriels O.T. (optionnel)

- Les différentes architectures, l'industrie 4.0, le modèle CIM, l'IOT
- L'analyse de risques et les classes de cybersécurité
- Les protocoles industriels et comment les sécuriser
- Exemples d'attaques et comment y pallier
- Les solutions de sécurité et les normes ANSSI
- Le processus d'homologation, les audits et les pentests
- Le pilotage sécurisé de l'OT par l'IT

3. La sécurité des réseaux

- Les différents types de réseaux
- Le modèle TCP/IP
- Les équipements : N.A.T., firewalls, proxies, reverse proxies, UTM, antivirus, antispyware, les systèmes de détection et de prévention d'intrusion etc.
- Les techniques cryptographiques : symétrique, asymétrique, les certificats et les PKI
- La virtualisation des réseaux : VPNs, VLANs, SD-WANs
- Les protocoles SSL/TLS, Https, SSH et Open SSH. Evaluer leur sécurité
- La supervision du réseau avec l'Intelligence artificielle des équipements pour détecter les anomalies, le Big data pour stocker et analyser les logs réseaux
- Exercices

4. La sécurité des datacenters et des locaux

- Le plan d'infrastructure technique des datacenters
- La mise en place de plans de continuité d'activités « disaster recovey » et de moyens de fonctionnement en mode dégradé
- La stratégie de sauvegarde et d'archivage des données
- L'exploitation sécurisée du SI. Le pilotage de l'O.T. par l'I.T.
- La sécurité du cloud avec les niveaux de sécurité attendus
- La protection des locaux à partir des vulnérabilités et des menaces possibles
- Exercices

5. La sécurité des terminaux

- Les menaces orientées postes clients et les outils pour les sécuriser

- Les vulnérabilités des navigateurs et des supports amovibles

- Les normes Wifi. Sécuriser les accès Wifis

- La sécurité des terminaux mobiles et des objets connectés

- Les méthodes d'identification/authentification/contrôles d'opérations

- Exercices

6. Les méthodes d'analyse de risques et le Machine Learning

- Etude des différents risques potentiels

- L'analyse de risques et les standards (Méhari, EBIOS, ISO27001, ISO27002, ISO27005,

EBIOS)

- Les contraintes légales et les aspects juridiques

- Les audits de sécurité (techniques, organisationnels, de conformité)

- Les organes de contrôles

- L'IA(Intelligence Artificielle) et le ML (Machine Learning) pour les outils de cybersécurité

- Les attaques sur le Machine Learning et comment s'en protéger

- Exercices

7. La gouvernance et conclusion

- L'organisation à mettre en œuvre : rôles métiers, sensibilisation des intervenants, formation, documentation, communication

- Les tableaux d'indicateurs

- Le schéma directeur SSI

- La veille technologique

- Superviser la cybersécurité par la gouvernance et l'améliorer continûment

- L'avenir de la sécurité et conclusion

- Exercices

Pédagogie et organisation

Le nombre de stagiaires peut varier de 1 à 10 personnes. La tarification de base est dégressive en fonction du nombre de participants et négociable

Formation avec un formateur, qui peut être suivie selon l'une des 2 modalités suivantes :

1 - Par visioconférence : Google/meet, Microsoft Teams, ou autre

2 - Le formateur se déplace dans les locaux du client

Chaque stagiaire dispose du support de cours et des corrigés en format power point qui leur seront envoyés avant le cours

Pour une meilleure assimilation, le formateur alterne tout au long du cours les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe

Positionnement et Modalités d'évaluation des acquis

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis

Mode de validation

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur ;

Evaluation qualitative de fin de formation

Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Financements possibles

Financement possible par les OPCO

Modalités et délai d'accès

2 jours avant la formation

Référent handicap

PERSONNES EN SITUATION DE HANDICAP : *(mise en place de compensation...)*

Contact : Référent handicap 02 51 84 95 55 / 06 28 70 45 28 / nadiahadjeri@cadresenmission.com

Intervenant

La formation est animée par un professionnel de l'informatique, certifié TOGAF (The Open Group Architecture Framework) et de la pédagogie, en veille technologique permanente et possédant une longue expérience en technologies numériques et méthodologies pour les utiliser correctement