Développez vos talents
Certifiez vos compétences

Gouvernance et Juridique

Rôles et missions du RSSI (Responsable de la Sécurité des SI)

5 jours (35h00) | ★★★★½ 4,6/5 | SEC-RSSI | Certification RSSI (incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cybersécurité › Gouvernance et Juridique

À l'issue de ce stage vous serez capable de :

- Maîtriser les concepts, approches, normes, méthodes et techniques pour exercer un rôle de premier plan et accompagner la transformation digitale en tant que RSSI au sein d'une organisation
- Comprendre le but, le contenu et la corrélation entre les différentes composantes du rôle à tenir, sur les plans de la gouvernance et de la gestion opérationnelle ou technique
- Conseiller une organisation sur les meilleures pratiques de gestion de la cybersécurité et de la sécurité de l'information.

Niveau requis

Avoir des connaissances de base en sécurité de l'information et des concepts connexes.

Public concerné

RSSI, candidats à la fonction de RSSI, responsables d'actifs digitaux d'une organisation, chefs de projets ou consultants souhaitant comprendre les enjeux liés à la sécurité informatique d'une entreprise, managers responsables de la gestion IT d'une entreprise ainsi que la gestion des risques en Cybersécurité, membres d'une équipe de sécurité de l'information, conseillers experts en technologie de l'information et/ou experts techniques voulant se préparer pour un poste de RSSI.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1

Gouvernance SSI (partie 1) : La gouvernance globale de la SSI

- Concepts et principes de base en sécurité de l'information
- Cadre normatif de base (ISO 27001 et normes assimilées)
- Etablissement du contexte et des enjeux de sécurité de l'information
- Structuration de la filière SSI au sein d'une organisation
- Pilotage de la sécurité des systèmes d'information et cybersécurité
- Aspects de sensibilisation et de formation à la sécurité des systèmes d'information
- Le support d'un programme SSI (documentation, ressources...)

Jour 2

Gouvernance SSI (partie 2) : La gestion des risques

- Vecteurs d'attaque communs, agents de menaces, motifs et types d'attaques
- Threat Intelligence et appréciation des risques SSI
- Evaluation des risques SSI (y compris journalisation et audits)
- Traitement des risques SSI
- Les incidents en cybersécurité, leurs conséquences et la réponse à y apporter
- Gestion de crise et des urgences, niveaux de préparation

Jour 3

Gouvernance SSI (partie 3) : Gérer la sécurité opérationnelle

- Gouvernance de la SSI et application des meilleures pratiques
- Politiques et procédures à mettre en oeuvre pour encadrer la SSI
- Surveillance et mesure de l'efficacité d'un programme SSI (KPI et tableaux de bord)
- Encadrer et piloter la sécurité des réseaux et des systèmes
- Sécurité du contrôle d'accès et gestion des identités
- Aspects de sécurité applicative
- La cryptographie et son bon usage dans le cadre d'une gestion cohérente de la SSI
- Audits interne et externe des systèmes d'information
- Le SOC (Security Operations Center ou Cellule de Sécurité Opérationnelle)

Jour 4

Aspects légaux de la SSI

- Les bases du droit (hiérarchie des normes, responsabilité, sanctions...)
- Aspects de responsabilité légale du RSSI
- Panorama du cadre réglementaire (y compris "Loi informatique et libertés" et RGPD)
- Investigation, collecte et gestion de la preuve numérique
- Légalité du contrôle au sein de l'entreprise (surveillance, accès au poste de travail...)
- Accessibilité et opposabilités des moyens télécoms
- Suivi des anomalies et intrusions, dépôts de plaintes

Jour 5

La cybersécurité opérationnelle par l'exemple

- Présentation des menaces et des vecteurs d'attaques les plus communs et solutions pour s'en prémunir
- Anatomie d'une attaque réussie (exemples cas réels)
- Virtualisation des systèmes d'information et sécurité du Cloud
- Hardening de systèmes d'information (Windows et Linux)

Passage de la certification

- Cette formation comprend le voucher nécessaire à l'inscription et au passage (ultérieur) de l'examen
- Il devra être passé dans un délai de 2 semaines (maximum) à partir du dernier jour de la session de formation
- L'examen (en français) s'effectue en ligne (live proctoring) et durera en moyenne 4h00
- Ce dernier est composé de 100 questions QCM et 10 questions ouvertes, à livre fermé

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)