Best

Devenir Responsable de la Sécurité du Système d'Information

Appréhendez toutes les dimensions du métier

Présentiel ou en classe à distance

7 jours (49 h)
+ activité à distance

Prix inter : 5.290,00 € HT
Forfait intra : 17.990,00 € HT

Réf.: MG802

La formation **Devenir RSSI** apporte une vision complète du métier de **Responsable de la Sécurité des Systèmes d'Information**. Elle couvre la **gouvernance SSI**, la gestion des risques, **ISO 27001**, EBIOS RM, NIS2, DORA, la continuité d'activité et les architectures de cybersécurité. Elle intègre également les nouveaux enjeux de l'**IA en cybersécurité** pour piloter efficacement une stratégie SSI.

A qui s'adresse cette formation ?

- Responsables métiers ou informatiques souhaitant évoluer vers le métier de RSSI
- RSSI opérationnels souhaitant appréhender les nouvelles missions du RSSI

- Bonne culture générale sur les infrastructures IT
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

Avant

- Un quiz de consolidation des prérequis

Pendant

1 - 1ÈRE PARTIE : LE MÉTIER DE RSSI, SON RÔLE, SES RESPONSABILITÉS, SON PÉRIMÈTRE D'ACTION ET SES MÉTHODES DE TRAVAIL (4 jours)

2 - Introduction : Quels sont les enjeux de la SSI ?

- Définitions, périmètres et terminologies fondamentales de la SSI
- Identification des enjeux de sécurité pour l'organisation
- Compréhension des principales menaces informatiques Introduction à l'analyse des risques liés au système d'information

3 - Les missions du RSSI

- Conseiller la Direction générale sur les obligations légales et les risques SSI
- Formaliser une stratégie de cybersécurité et définir un plan d'action
- Élaborer et maintenir un référentiel SSI
- Participer à la mise en place de la gouvernance de la sécurité

- Conseiller et accompagner la maîtrise d’ouvrage et la maîtrise d’oeuvre
- Former et sensibiliser les collaborateurs à la cybersécurité
- Réaliser une veille juridique, réglementaire et technologique proactive
- Conduire des audits et des contrôles de conformité
- Mesurer l’efficacité des dispositifs de sécurité mis en oeuvre

4 - Les obligations légales et les exigences SSI

- Responsabilités civiles délictuelle et contractuelle
- Principales obligations légales applicables à la sécurité des systèmes d’information
- PPST : protection des informations relatives au potentiel scientifique et technique de la nation
- Respect de la vie privée et secret des correspondances
- SOX – Sarbanes-Oxley Act
- RGPD – Règlement général sur la protection des données
- Lois LSF, LCEN et LSQ
- CPI : Code de la propriété intellectuelle
- Directive NIS 2
- Règlement DORA
- LPM : Loi de programmation militaire

5 - Identification des autorités compétentes et référentiels

- ANSSI, Politiques de sécurité des systèmes d’information (PSSI) et Référentiel général de sécurité (RGS)
- Agence Française de la santé numérique
- Référentiel PCI DSS
- Commission nationale de l’informatique et des libertés (CNIL)

6 - Les contrats

7 - La gouvernance de la SSI

- Niveaux de maturité SSI et différents modèles d’organisation
- Mise en place des comités de pilotage, d’arbitrage, de suivi et d’homologation
- Articulation entre la voie hiérarchique et la voie fonctionnelle
- Coordination de la SSI avec les autres fonctions de l’organisation
- Notification des incidents et gestion des alertes de sécurité

8 - Formalisation d'une stratégie SSI

- Adjonction d'outils et bonnes pratiques
- Orientée enjeux ou orientée SMSI
- Les étapes de la formalisation d'une feuille de route

9 - La gestion des risques

- Principes du management des risques selon la norme ISO 31000
- Gestion des risques liés à la sécurité de l’information selon la norme ISO/IEC 27005
- Études de cas
- Mesures de sécurité de la norme ISO/IEC 27002
- Mise en place d’un SMSI selon la norme ISO/IEC 27001

10 - La définition d'un référentiel SSI

- Lettre d'engagement de la direction
- Lettre de nomination du RSSI
- La politique générale de protection de l'information
- Comment construire la politique sécurité système d'information ?
- Chartes
- Guides et procédures

11 - Mise en oeuvre d'une méthode d'intégration SSI dans les projets

- Gestion des risques numériques avec EBIOS RM
- Adaptation de l’intégration de la SSI aux différents types de projets

12 - 2ÈME PARTIE : DE LA THÉORIE À LA PRATIQUE (3 jours)

13 - L'état de l'art des solutions technique de sécurité du SI

- Sécurité des accès : filtrage réseau et applicatif, WAF, CASB, authentification et gestion des habilitations
- Détection des intrusions, journalisation et supervision de la sécurité
- Approches Zero Trust et SD-WAN Sécurisation des échanges

- Sécurité des serveurs : durcissement, hébergement et virtualisation
- Sécurisation des postes de travail fixes et mobiles Sécurité des applications
- Sécurisation des environnements conteneurisés avec Docker

14 - L’intelligence artificielle dans la cybersécurité

- Identification des principales typologies d’attaques utilisant l’IA
- Utilisation de l’intelligence artificielle au service de la cybersécurité
- Compréhension des limites de l’IA appliquée à la sécurité informatique
- Application des bonnes pratiques pour encadrer son utilisation

15 - Les architectures SSI

- Périphériques
- En profondeur

16 - Introduction aux plans de continuité des activités et plans de secours

- Fondamentaux de la continuité des activités
- Le modèle du BCI et de la norme ISO 22301
- Les différents plans : PCA, PCO, PSI, PGC, PCOM...
- Les phases d'un projet de PCA

17 - La prise en compte du facteur humain

- Sensibilisation des collaborateurs aux risques numériques
- Formation des utilisateurs et des équipes
- Communication autour des règles et des bonnes pratiques de sécurité

18 - La veille juridique et technique SSI

19 - Contrôle et audit

- Définition des indicateurs de contrôle
- Les tests intrusifs
- Formalisation et mise à jour des tableaux de bord

20 - Conseils généraux pour réussir dans son métier de RSSI

- Les freins et les difficultés rencontrés par les RSSI (retour d'expérience)
- La bonne appropriation et la bonne communication du rôle du RSSI
- Les erreurs à ne pas commettre, les conseils d'accompagnement au changement

Après

- Un quiz pédagogique pour évaluer vos acquis et approfondir les sujets de votre choix
- Des vidéocasts pour revenir sur les points clés de la formation



Les objectifs de la formation

- Identifier toutes les facettes du métier de Responsable de la Sécurité du SI, son rôle et ses responsabilités
- Savoir construire une politique de sécurité efficace et gérer les risques du SI
- Avoir une vue d'ensemble des mesures techniques de protection des SI
- Disposer d'une méthodologie pour assurer la mise en oeuvre et le suivi de la sécurité
- Connaître les bonnes pratiques pour construire son plan d'action et définir ses indicateurs



Evaluation

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.



Les points forts de la formation

- Un tour d'horizon exhaustif des différents aspects de la mission de RSSI
- Une approche méthodologique participative permettant des échanges entre les participants et le formateur sur des retours d'expériences concrets : le formateur accompagne des RSSI depuis plusieurs années dans l'accomplissement de leurs missions
- Le support de formation est utilisé pour présenter les éléments théoriques et les applications pratiques dans le domaine de la sécurité des SI. Il est adapté au contexte actuel et aux obligations réglementaires en vigueur.
- Les contenus digitaux mis à disposition des participants avant et après la formation renforcent l'efficacité pédagogique du programme et garantissent un bénéfice durable de l'action de formation

Evaluation

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Dates et villes 2027 - Référence MG802

Dernières places disponibles Session garantie

Paris

du 11 janv. au 27 janv.
- du 11 janv. au 14 janv.
- du 25 janv. au 27 janv.

du 22 févr. au 10 mars
- du 22 févr. au 25 févr.
- du 8 mars au 10 mars

du 30 mars au 21 avr.
- du 30 mars au 2 avr.
- du 19 avr. au 21 avr.

du 24 mai au 9 juin
- du 24 mai au 27 mai
- du 7 juin au 9 juin

du 5 juil. au 28 juil.
- du 5 juil. au 8 juil.
- du 26 juil. au 28 juil.

du 6 sept. au 22 sept.
- du 6 sept. au 9 sept.
- du 20 sept. au 22 sept.

du 18 oct. au 10 nov.
- du 18 oct. au 21 oct.
- du 8 nov. au 10 nov.

du 6 déc. au 22 déc.
- du 6 déc. au 9 déc.
- du 20 déc. au 22 déc.

A distance

du 11 janv. au 27 janv.
- du 11 janv. au 14 janv.
- du 25 janv. au 27 janv.

du 22 févr. au 10 mars
- du 22 févr. au 25 févr.
- du 8 mars au 10 mars

du 30 mars au 21 avr.
- du 30 mars au 2 avr.
- du 19 avr. au 21 avr.

du 24 mai au 9 juin
- du 24 mai au 27 mai
- du 7 juin au 9 juin

du 5 juil. au 28 juil.
- du 5 juil. au 8 juil.
- du 26 juil. au 28 juil.

du 6 sept. au 22 sept.
- du 6 sept. au 9 sept.
- du 20 sept. au 22 sept.

du 18 oct. au 10 nov.
- du 18 oct. au 21 oct.
- du 8 nov. au 10 nov.

du 6 déc. au 22 déc.
- du 6 déc. au 9 déc.
- du 20 déc. au 22 déc.

Toulouse

du 11 janv. au 27 janv.
- du 11 janv. au 14 janv.
- du 25 janv. au 27 janv.

du 5 juil. au 28 juil.
- du 5 juil. au 8 juil.
- du 26 juil. au 28 juil.

du 18 oct. au 10 nov.
- du 18 oct. au 21 oct.
- du 8 nov. au 10 nov.

Nantes

du 22 févr. au 10 mars
- du 22 févr. au 25 févr.
- du 8 mars au 10 mars

du 6 sept. au 22 sept.
- du 6 sept. au 9 sept.
- du 20 sept. au 22 sept.

du 6 déc. au 22 déc.
- du 6 déc. au 9 déc.
- du 20 déc. au 22 déc.

Lyon

du 22 févr. au 10 mars
- du 22 févr. au 25 févr.
- du 8 mars au 10 mars

du 6 sept. au 22 sept.
- du 6 sept. au 9 sept.
- du 20 sept. au 22 sept.

du 6 déc. au 22 déc.
- du 6 déc. au 9 déc.
- du 20 déc. au 22 déc.

Aix-en-Provence

du 22 févr. au 10 mars
- du 22 févr. au 25 févr.
- du 8 mars au 10 mars

du 5 juil. au 28 juil.
- du 5 juil. au 8 juil.
- du 26 juil. au 28 juil.

du 18 oct. au 10 nov.
- du 18 oct. au 21 oct.
- du 8 nov. au 10 nov.

Lille

du 30 mars au 21 avr.
- du 30 mars au 2 avr.
- du 19 avr. au 21 avr.

du 6 sept. au 22 sept.
- du 6 sept. au 9 sept.
- du 20 sept. au 22 sept.

du 18 oct. au 10 nov.
- du 18 oct. au 21 oct.
- du 8 nov. au 10 nov.