Formation « RSSI »

Réf : RSSI

La fonction de "RSSI" est un métier transverse et multi-facettes. La formation RSSI HS2 apporte au nouveau RSSI un panorama complet des fonctions du RSSI et des attentes des organisations sur le rôle du RSSI, les connaissances indispensables à sa prise de fonction du RSSI et un retour d'expérience sur les chantiers et la démarche à mettre en œuvre dans le rôle sont détaillés par d'anciens RSSI et des consultants expérimentés.

Objectifs

- **Acquérir les compétences indispensables à l'exercice de la fonction responsable de la sécurité des systèmes d'information, à savoir :**
  - **Bases de la cybersécurité**
  - **Enjeux de la SSI au sein des organisations**
  - **Connaissances techniques de base**
  - **Sécurité organisationnelle et normes ISO27001**
  - **Méthodes d'appréciation des risques**
  - **Bases juridiques**
  - **Stratégies de prise de fonction**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Toute personne amenée à exercer la fonction de responsable sécurité des systèmes d'information : RSSI, futurs RSSI, ingénieurs sécurité assistant un RSSI, responsables sécurité à la production**
- **Toute personne amenée à assurer une fonction de correspondant local de sécurité des systèmes d'information ou une fonction similaire.**
- **Techniciens devenus RSSI, souhaitant obtenir une culture de management.**
- **Managers confirmés manquant de la culture technique de base en matière de sécurité des SI ou ne connaissant pas les acteurs du marché**
- **DSI ou auditeurs en systèmes d'information souhaitant connaître les contours de la fonction et les rôles du RSSI**

Pré-requis

- **Il est préférable d'avoir une expérience au sein d'une direction informatique en tant qu'informaticien ou bonne culture générale des systèmes d'information.**
- **Avoir des notions de base en sécurité appliquées au système d'information constitue un plus.**

Méthode pédagogique

- **Cours magistral dispensé à chaque fois par des experts de chaque module**

- **Dans les modules "gestion des risques" et "juridique", des exercices de contrôle des connaissances et dans les autres modules, des démonstrations ou de nombreux exemples pratiques basés sur les retours d'expérience des instructeurs et ceux de leurs clients**
- **Forte interaction entre les formateurs et les stagiaires permettant de rendre les échanges davantage concrets, en corrélation avec les attentes des stagiaires**
- **Animation par un RSSI en activité, présentant sa stratégie de prise de fonction et un retour d'expérience sur des cas concrets et détaillés de projets sécurité menés dans son organisation.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **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

- **A 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 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification RSSI par HS2.**

Programme

Accueil des participants et tour de table

Enjeux et organisation de la sécurité (environ 1,5 jour)

- Critères de sécurité (disponibilité, intégrité, confidentialité, auditabilité)
- Fonction de RSSI, rôles du RSSI
- Environnement du RSSI (production, direction, métiers, conformité, juridique, etc)
- Panorama des référentiels
- Politiques de sécurité (globales, détaillées, sectorielles, géographiques, etc)
- Conformité
- Indicateurs et tableaux de bord SSI (stratégique, tactique, opérationnel)
- Gestion des incidents de sécurité
- Sensibilisation (collaborateurs, informaticiens, direction)
- Ecosystème de la SSI (associations, conférences, etc)

Aspects techniques de la sécurité (environ 1 jour)

- Sécurité du système d'exploitation
- Minimisation et durcissement des systèmes
- Contrôle d'accès
- Gestion des utilisateurs
- Gestion des moyens d'authentification
- Sécurité des applications (sessions, injection SQL, XSS)
- Validation des données (en entrées, traitées, en sortie)
- Développement et environnements de test
- Accès au code source
- Sécurité réseau (routeurs, firewalls)
- Cloisonnement et contrôle d'accès

- Messagerie
- Sécurité du poste de travail, mobilité, télétravail
- Gestion des opérations, gestion des vulnérabilités techniques
- Surveillance, sauvegardes
- Conformité technique
- Typologie des tests d'intrusion et audits de sécurité
- Protection des outils d'audits et des données d'audits

Système de Management de la Sécurité de l'Information (normes ISO 27001) (environ 1/2 journée)

- Bases sur les systèmes de management (définitions, modèle PDCA, propriétés et objectifs)
- Panorama des normes ISO 270xx
- Bases sur ISO 27001 et ISO 27002 et utilisations possibles
- Domaine d'application
- Engagement de la direction
- Surveillance (réexamen régulier, audit interne, revue de direction)
- Amélioration continue

Audit (environ 1/2 journée)

- Typologie des audits (technique, organisationnel, de conformité, de certification)
- Conséquences (inconvénients et objectifs)
- Vocabulaire (basé sur ISO 19011)
- Préparation à l'audit
- Considérations pratiques (formation, communication, intendance, audit à blanc, préparation)
- Démarche d'audit (ISO 19011)
- Avant l'audit, pendant l'audit, après l'audit
- Livrable
- Actions correctives entreprises et suivi
- Réception des auditeurs (maison-mère, ISO27001/HDS, ISAE3401/SOC2, Cour des Comptes, Commission bancaire, etc.)

Gestion de risques (environ 1/2 journée)

- Méthodologies d'appréciation des risques (ISO27001, EBIOS, Mehari)
- Vocabulaire
- Identification et valorisation d'actifs
- Menace, source des risques, vulnérabilités
- Analyse de risque
- Estimation des risques
- Vraisemblance et conséquences d'un risque
- Evaluation du risque
- Traitement des risques (réduction, partage, maintien, refus)
- Notion de risque résiduel
- Acceptation du risque

Aspects juridiques de la SSI (environ 1/2 journée)

- RGPD et Informatique et libertés
- Communications électroniques
- Conservation des traces
- Contrôle des salariés
- Atteintes aux STAD
- Charte informatique
- Comptes à privilège
- Gestion des relations avec les partenaires (infogérance, infonuagique, prestataires en sécurité)

Examen (1h30)

Témoignage d'un RSSI (après l'examen la dernière 1/2 journée)

Pour aller plus loin

Nous vous recommandons de suivre les formations suivantes :

Formations axées techniques :

- **ESSCYBER – Formation Essentiels techniques de la cybersécurité**
- **SECUCYBER – Fondamentaux techniques de la cybersécurité**
- **SECUPKI – Principe et mise en œuvre des PKI**

Formations axées juridiques :

- **SECUDROIT – Droit de la cybersécurité**
- **RGPD – « RGPD : les fondamentaux de la protection des données »**
- **DPO - Délégué à la protection des données (Data Protection Officer)**
- **ISO 27701 (ex. 27552) – Privacy Information Management System (PIMS)**

Formations axées organisationnelles :

- **SECUPROJET – Security by Design**
- **EBIOS2018 – EBIOS 2018 Risk Manager**
- **ISO27LA – ISO 27001 Lead Auditor**