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 et les connaissances indispensables à sa prise de fonction. Un retour d'expérience sur les chantiers et la démarche à mettre en œuvre dans le rôle sont détaillés par des 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 :**
  - **Enjeux de sécurité des SI dans les organisations**
  - **Connaissances techniques essentielles**
  - **Organisation de la sécurité et normes ISO27001**
  - **Politiques de sécurité, audit de sécurité et indicateurs**
  - **Méthodes d'appréciation des risques**
  - **Aspects juridiques de la sécurité des SI**
  - **Sensibilisation à la sécurité des SI et gestion des incidents**

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, RSSI adjoint, responsables sécurité opérationnelle à la production, correspondant local de sécurité des systèmes d'information**
- **Techniciens devenus RSSI, souhaitant acquérir des notions en gouvernance et management de la sécurité des SI**
- **Spécialistes de domaines transverses des systèmes d'information (qualité, audit, gestion de projets) devant compléter leurs compétences dans le domaine de la sécurité des systèmes d'information**

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

- **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 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 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**
- **Evaluation de pré-formation envoyée avant le début de la formation**
- **Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et d'exercices pratiques**
- **Examen final à la fin de la formation (cf certification)**

Ces évaluations ont pour but de valider les compétences acquises.

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 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 de la sécurité des systèmes d'information (1 jour)

- Introduction
  - Objectifs de la cybersécurité
  - Objectifs des organisations
  - Alignement stratégique organisation / cybersécurité
  - Objectifs et organisation de la formation
- Enjeux de la cybersécurité
  - Sécurité des SI, de l'information, informatique et cybersécurité
  - Vocabulaire : critères et objectifs
  - Le critère de preuve
  - Vocabulaire : incident et risque
- Activités du RSSI
  - Le RSSI, polyvalent face aux enjeux
  - La politique de sécurité
  - Le programme de sécurité
  - Les mesures de sécurité
  - Le RSSI dans les projets
  - Le RSSI et les associations professionnelles
- Introduction à la menace cyber
  - Gérer le risque

- Dans la peau d'un attaquant
- Sécurité - Règles de base

Aspects techniques de la cybersécurité (1 jour)

- Introduction à la cryptographie
- Sécurité réseau
  - Principes de base du réseau
  - Attaques et mesures
  - Pare-feu et proxy
  - Architecture sécurisée
- Sécurité applicative
  - Vulnérabilités mémoire
  - Vulnérabilités web
  - Développement sécurisé
- Sécurité système
  - Principes
  - Contrôle d'accès
  - Veille sécurité
  - Mise à jour
  - Sauvegarde
  - Journalisation
  - Protection du poste de travail
  - Équipements mobiles
  - Auditer son SI

Système de Management de la Sécurité de l'Information (normes ISO 2700x) (1/4 journée)

- Introduction à ISO 27001
- Systèmes de management et SMSI
  - Exemples de systèmes de management
  - Propriétés des systèmes de management
  - Processus du SMSI
- Introduction à ISO 27002
- Comment utiliser les normes
- Conclusion et bienfaits du SMSI ISO 27001

Politiques de sécurité (1/4 journée)

- Définitions
- Hiérarchie et utilité des politiques de sécurité
- Politiques spécifiques, organisation et exemples
- Rédaction, élaboration et mise en œuvre des politiques
- Révision des politiques
- Synthèse et éléments indispensables des politiques

Indicateurs en sécurité des SI (1/4 journée)

- Introduction et règles d'or
- Sources de collecte des indicateurs
- Spécification des indicateurs et exemples
- Indicateurs dérivés et exemples
- Risques sur les indicateurs, questions pratiques et erreurs à éviter

Audit (1/4 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 (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
- Évaluation du risque
- Traitement des risques (réduction, partage, maintien, refus)
- Notion de risque résiduel
- Acceptation du risque

Aspects juridiques de la SSI (1/2 journée)

- Focus sur 3 obligations générales de protection du SI
  - Un bref panorama des obligations de SSI
  - LPM et OIV
  - NIS, OSE et FSN
  - RGPD
- Synthèse des principales règles de la SSI au sein des organisations
  - Détecter les incidents
  - Journaliser les activités
  - Encadrer les usages dans les organisations
  - Contractualiser avec les prestataires
- Le volet pénal : réagir aux atteintes à la sécurité des systèmes d'information
  - L'importance de la gestion de crise
  - La qualification des faits de cybercriminalité

Sensibilisation à la sécurité des SI (1h)

- Mesure de sécurité
- Programme de sensibilisation
- Objectif de la sensibilisation
- Moyens de sensibilisation et vecteurs de communication
- Sources d'information
- Conseils
- Rappel des objectifs
- Coûts
- Évaluation

Gestion des incidents en sécurité des SI (1h)

- Définitions
- Exemples d'incidents liés à la sécurité
- Objectifs de la gestion des incidents liés à la SSI
- Étapes de la gestion d'un incident
  - Préparation, identification et analyse, confinement, endiguement, éradication, recouvrement, retour d'expérience

- Erreurs à éviter
- Outils
- Ressources

Acheter des prestations en sécurité des SI (1h)

- Contexte et objectifs
- Acheter la SSI
  - Définition
  - Le service achats
  - Le processus achats
  - Avant / pendant
  - Après
  - Augmentez votre pouvoir d'achat

Examen (1h30)

Témoignage et retour d'expérience d'un RSSI (1h30)

Pour aller plus loin

Nous vous recommandons de suivre les formations suivantes :

Formations axées sur la technique :

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

Formations axées sur le juridique :

- **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 sur l'organisationnel :

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