RSSI : Le Responsable de la Sécurité des Systèmes d'Information

Acquérir les compétences indispensable à l'exercice de la fonction responsable de la sécurité des systèmes d'information.

Stage pratique
Qualité du logiciel - Software Craftsmanship

Code :
RSSI

Durée :
5 jour(s) (35,00 heures)

Exposés : **60 %**
Cas pratiques : **20 %**
Echanges d'expérience : **20 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 3 780,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

DESCRIPTION

Historiquement, la fonction de RSSI était réservée à des spécialistes de la sécurité. Souvent de culture technique, ils avaient fait toute leur carrière dans le domaine. En quelque sorte, c'était un poste réservé à une niche de techniciens d'élite, passionnés par la question. Depuis, l'interconnexion massive des systèmes d'information ainsi que la migration de l'économie vers Internet a fait exploser les besoins en sécurité. Les solutions techniques se sont multipliées au fur et à mesure des menaces, conduisant à une complexification de la sécurité. Ceci a induit un besoin de compétences en management..

Aujourd'hui, la fonction de RSSI est devenue une fonction stratégique. S'il doit toujours avoir une bonne culture technique, le responsable sécurité est maintenant avant tout un manager. Il doit définir des politiques, préserver la conformité du système d'information par rapport aux différents référentiels, prendre les bonnes décisions en cas d'incident, comprendre les problèmes techniques et prêcher la bonne parole auprès du management et du personnel. En résumé, il doit faire le grand écart entre les orientations stratégiques et les décisions opérationnelles de tous les jours. Il doit savoir parler au management tout en pilotant des projets et en résolvant des problèmes purement techniques.

La formation proposée a précisément été conçue dans le but d'apporter au RSSI tous les éléments dont il a besoin pour assurer ses fonctions.

OBJECTIFS PEDAGOGIQUES

Objectif opérationnel :

Acquérir les compétences indispensable à l'exercice de la fonction responsable de la sécurité des systèmes d'information.

Objectifs pédagogiques :

À l'issue de cette **formation RSSI** vous aurez acquis les connaissances et compétences nécessaires pour :

- Définir et comprendre les enjeux de sécurité des SI dans les organisations

- Posséder les connaissances techniques essentielles
- Mettre en oeuvre l'organisation de la sécurité et la norme ISO27001
- Connaitre la politique de sécurité, et savoir auditer la sécurité et les indicateurs
- Maitriser les méthodes d'appréciation des risques
- Connaitre les aspects juridiques de la sécurité des SI
- Avoir une sensibilisation à la sécurité des SI et gestion des incidents

PUBLIC CIBLE

Ce stage s'adresse tant aux nouveaux ou futurs RSSI qu'aux RSSI expérimentés qui souhaitent se remettre à niveau et échanger sur les bonnes pratiques du métier avec d'autres RSSI.

Sont également concernés, les Ingénieurs en sécurité des systèmes d'information souhaitant rapidement acquérir toutes les compétences leur permettant d'évoluer vers la fonction de RSSI, ainsi que les Directeurs des Systèmes d'Information ou auditeurs en systèmes d'information souhaitant connaître les contours de la fonction et les rôles du RSSI.

PRE-REQUIS

Pour suivre ce cours, il est nécessaire de posséder une expérience en tant qu'informaticien au sein d'une direction informatique ou d'avoir une bonne culture générale des systèmes d'information. Des notions de base en sécurité appliquées au système d'information constituent un plus.

J'évalue mes connaissances pour vérifier que je dispose des prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

METHODE PEDAGOGIQUE
Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique des formateurs, complétés de travaux pratiques et de mises en situation.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

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 DES 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

TÉMOIGNAGE ET RETOUR D'EXPÉRIENCE D'UN RSSI (1h30)

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com