Devenir un RSSI performant et piloter la cybersécurité

Date et durée

Code formation : GSI005FR
Durée : 6 jours
Nombre d'heures : 42 heures

Description

Dans un paysage numérique où les cyberattaques se professionnalisent, le rôle du **Responsable de la Sécurité des Systèmes d'Information** (RSSI) est devenu central pour la survie des organisations. Cette formation de 6 jours vous apprendra à endosser cette **responsabilité stratégique** en maîtrisant à la fois les leviers de gouvernance, les obligations réglementaires (NIS2, RGPD) et les réalités techniques du terrain.
Ce programme de **formation RSSI** complet vous offrira une vision à 360° du métier. Vous naviguerez entre la définition d'une **Politique de Sécurité (PSSI)**, la gestion de crise et la conception d'architectures résilientes. Vous mettrez notamment l'accent sur la **méthode EBIOS Risk Manager** à travers des ateliers dédiés pour transformer l'analyse de risques en outil de décision.
Au terme de ces cours, vous serez armé pour structurer une **démarche de sécurité globale**, crédible face à votre direction et opérationnelle pour vos équipes techniques. Vous disposerez de toutes les clés pour protéger les actifs critiques et assurer la **continuité d'activité** de votre entreprise.

Objectifs

À l'issue de cette formation, vous atteindrez les objectifs de compétences suivants :

- identifier les missions stratégiques et les responsabilités du RSSI ;
- maîtriser les référentiels normatifs et les obligations légales (RGPD, NIS2) ;
- structurer une gouvernance SSI efficace au sein de l'organisation ;
- définir une stratégie de sécurité globale et son plan d'action associé ;
- piloter la gestion des risques et le traitement des incidents de sécurité ;
- garantir la conformité réglementaire et auditer le niveau de sécurité ;
- déployer les solutions techniques de protection du SI (réseaux, systèmes) ;
- concevoir des architectures de sécurité robustes et résilientes ;
- élaborer et tester les plans de continuité (PCA) et de secours (PSI) ;
- gérer le facteur humain à travers la sensibilisation et la formation ;
- assurer une veille active sur les menaces et les évolutions juridiques ;
- réaliser des audits réguliers pour contrôler l'efficacité du dispositif.

Points forts

- **Vision exhaustive** : vous couvrirez l'intégralité du spectre RSSI, de la gouvernance stratégique (Partie 1) à l'implémentation technique (Partie 2).
- **Focus méthodologique** : vous consacrerez un module entier à la pratique approfondie de la méthode EBIOS Risk Manager.

- **Densité du programme** : vous bénéficierez de 6 jours de formation pour traiter en profondeur chaque pilier du métier, sans survol.
- **Expertise certifiée** : vous apprendrez auprès de formateurs RSSI expérimentés, certifiés ISO 27001 et EBIOS RM.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre cette formation nécessite le prérequis suivant :

- **Connaissance de base :** une bonne compréhension des concepts de cybersécurité et du fonctionnement des systèmes d'information est recommandée.

Public

Cette formation s'adresse aux professionnels souhaitant prendre des responsabilités en cybersécurité. Le public inclut notamment :

- les **futurs RSSI et RSSI en poste** désireux de consolider leur posture managériale et technique ;
- les **DSI et administrateurs réseau** souhaitant évoluer vers le pilotage de la sécurité ;
- les **consultants en cybersécurité** cherchant à acquérir une vision globale de la gouvernance ;
- les **responsables conformité et risques** qui doivent intégrer la dimension cyber dans leur périmètre.

Programme

Partie 1 : Les aspects managériaux

Module 1 : comprendre le rôle et les missions du RSSI

- Le rôle et les missions du RSSI.
- La gouvernance de la SSI et son positionnement dans l'organisation.
- Les enjeux et les menaces actuels de la cybersécurité.

Module 2 : maîtriser les référentiels et le cadre réglementaire

- Les normes et standards de la SSI (ISO 27001, ISO 27005, ISO 22301, NIST).
- Les réglementations et obligations légales (RGPD, LPM, NIS2, Cloud Act).
- Le rôle des autorités compétentes (ANSSI, CNIL).

Module 3 : définir une stratégie SSI performante

- L'élaboration d'une politique de sécurité du SI (PSSI).
- La gestion des identités et des accès.
- La protection des données et la classification des informations.

Module 4 : piloter la gestion des risques cyber

- Les méthodes d'analyse des risques (EBIOS RM, ISO 27005).
- L'identification et l'évaluation des menaces.
- Les stratégies d'atténuation et de traitement des risques.

Module 5 : gérer les incidents et la réponse à crise

- Le plan de réponse aux incidents.
- L'analyse forensique et la gestion de crise.
- Les retours d'expérience et l'amélioration continue.

Module 6 : assurer la conformité et l'audit de sécurité

- L'audit de conformité et les contrôles SSI.
- Les indicateurs et tableaux de bord de cybersécurité.
- La sensibilisation et la formation des collaborateurs.

Module 7 : pratiquer la méthodologie EBIOS Risk Manager

- Cadrer l'étude : définir le périmètre, les missions et le socle de sécurité.
- Identifier les sources de risques (OFE) et élaborer les scénarios stratégiques.
- Construire les scénarios opérationnels et évaluer leur vraisemblance.
- Définir la stratégie de traitement du risque et le plan d'action de sécurité.

Partie 2 : La SSI en pratique

Module 8 : déployer les solutions techniques de sécurité

- La sécurité des accès (authentification forte, contrôle des identités, SSO et NAC).
- La sécurité des échanges et le chiffrement (VPN, IPSec, TLS, PKI et WAF).
- La sécurité des serveurs et des postes de travail (EDR, antivirus et durcissement système).
- La sécurité des applications et le développement sécurisé.

Module 9 : concevoir des architectures et segmenter le SI

- La conception d'architectures sécurisées.
- Les zones de confiance et la mise en place de DMZ.
- Les firewalls et les proxys : filtrage réseau et applicatif.
- La supervision et la détection des menaces (SIEM, IDS/IPS).
- Le SaaS et l'approche SDWAN.

Module 10 : élaborer un plan de continuité (PCA/PRA)

- L'élaboration d'un Plan de Continuité d'Activité (PCA).
- Le déploiement du Plan de Reprise d'Activité (PRA).
- Les tests et simulations de cybercrises.
- La gestion de crise et la communication en cas d'incident.

Module 11 : gérer le facteur humain et la sensibilisation

- La sensibilisation et la formation des collaborateurs.
- La gestion des accès et des habilitations.
- La lutte contre l'ingénierie sociale et le phishing.

Module 12 : assurer la veille juridique et réglementaire

- La conformité aux normes et réglementations (ISO 27001, RGPD, NIS2).
- La gestion des obligations légales et la notification des incidents.
- Les relations avec les autorités compétentes, comme l'ANSSI.

Module 13 : contrôler et auditer le dispositif SSI

- L'évaluation de la conformité des systèmes.
- La planification et la réalisation d'audits de sécurité.
- La gestion des plans d'action et l'amélioration continue.