RSSI : Maîtriser la fonction et piloter la cyberdéfense de l'entreprise

Durée : 3 jours (21 heures)

CONNAISSANCES PREALABLES

- Connaissances générales des systèmes d'information et de leur fonctionnement
- Expérience dans l'informatique, l'exploitation, l'administration système ou la gestion des risques appréciée.

PROFIL DES STAGIAIRES

- Futurs Responsables de la Sécurité des Systèmes d'Information (RSSI)
- RSSI nouvellement nommés
- DSI, responsables informatiques et responsables infrastructures
- Responsables cybersécurité
- Managers souhaitant structurer la gouvernance de la sécurité de leur organisation.

OBJECTIFS

À l'issue de la formation, les participants seront capables de :

- Comprendre les responsabilités et les missions du RSSI
- Mettre en œuvre une gouvernance de la cybersécurité adaptée à leur organisation
- Réaliser une analyse des risques cyber et définir une stratégie de protection
- Construire et piloter une politique de sécurité des systèmes d'information (PSSI)
- Organiser la gestion des incidents et la réponse aux cyberattaques
- Assurer la conformité réglementaire et normative de l'entreprise
- Développer une démarche d'amélioration continue de la sécurité.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Alternance d'apports théoriques, de retours d'expérience et de bonnes pratiques issues du terrain.
- Études de cas inspirées de situations réelles rencontrées par des RSSI et des responsables cybersécurité.
- Ateliers pratiques de construction d'une gouvernance sécurité, d'analyse des risques et de gestion d'incidents.
- Exercices collaboratifs de pilotage de crise cyber et de prise de décision.
- Échanges d'expériences entre participants et analyse de cas concrets d'organisations publiques et privées.
- Remise de modèles et outils directement réutilisables en entreprise (PSSI, tableaux de bord, plans d'actions, matrices de risques).

FORMATEUR

- Consultant expert en cybersécurité disposant d'une expérience significative dans les fonctions de RSSI, de gouvernance de la sécurité des systèmes d'information, de gestion des risques cyber et de mise en conformité réglementaire.

METHODE D'EVALUATION DES ACQUIS

- Évaluation initiale des connaissances en début de formation.
- Validation progressive des acquis à travers les exercices et ateliers réalisés durant les trois jours.
- Études de cas permettant de mesurer la capacité à appliquer les concepts de gouvernance, de gestion des risques et de pilotage de la cybersécurité.
- Questionnaire d'évaluation des connaissances en fin de formation.
- Débriefing collectif et individuel des travaux réalisés..

CONTENU DU COURS

Jour 1 : Comprendre le rôle du RSSI et structurer la gouvernance cybersécurité (7h)

Module 1 : Positionner la fonction RSSI dans l'organisation (2h)

Objectifs

- Comprendre les missions et responsabilités du RSSI.
- Identifier les interactions entre le RSSI, la direction et les métiers.
- Définir un modèle de gouvernance adapté à son organisation.

Contenu

- Évolution des menaces et enjeux cyber actuels.
- Le rôle du RSSI : missions stratégiques, opérationnelles et réglementaires.
- Positionnement du RSSI dans l'entreprise.
- Relations avec la Direction Générale, la DSI, les métiers et les partenaires.
- Pilotage de la cybersécurité et indicateurs de gouvernance.

Atelier collectif :

Cartographier les parties prenantes de la cybersécurité dans son organisation et définir les responsabilités associées.

Module 2 : Construire une gouvernance cybersécurité efficace (2h)

Objectifs

- Structurer une gouvernance de la sécurité adaptée aux enjeux métiers.
- Définir les mécanismes de pilotage de la cybersécurité.

Contenu

- Principes de gouvernance cyber.
- Définition d'une stratégie cybersécurité.
- Organisation des comités de sécurité.
- Gestion budgétaire et arbitrage des priorités.
- Communication avec la direction.

Brainstorming encadré :

Identifier les principaux enjeux de cybersécurité d'une organisation et les traduire en objectifs de gouvernance.

Module 3 : Élaborer une politique de sécurité des systèmes d'information (2h)

Objectifs

- Comprendre les composantes d'une PSSI.
- Structurer les politiques et procédures de sécurité.

Contenu

- Rôle et objectifs de la PSSI.
- Classification des actifs et des données.
- Gestion des accès et des responsabilités.
- Sensibilisation et culture sécurité.
- Déclinaison des politiques opérationnelles.

Atelier :
Construction du squelette d'une PSSI adaptée à un contexte d'entreprise.

Module 4 : Synthèse et atelier de gouvernance (1h)

Objectifs

- Consolider les notions abordées durant la journée.
- Construire une première vision de gouvernance cyber.

Étude de cas fil rouge :
Définition d'une organisation cybersécurité pour une PME ou une ETI confrontée à des enjeux de transformation numérique.

Jour 2 : Piloter les risques et renforcer la résilience de l'entreprise (7h)

Module 5 : Mettre en œuvre une démarche de gestion des risques cyber (2h30)

Objectifs

- Identifier et évaluer les risques de sécurité.
- Prioriser les actions de traitement.

Contenu

- Notions fondamentales de risque.
- Identification des actifs critiques.
- Menaces, vulnérabilités et scénarios de risque.
- Présentation des méthodes EBIOS RM et ISO 27005.
- Traitement et acceptation du risque.

Atelier :
Construction d'une cartographie simplifiée des risques cyber.

Module 6 : Définir les contrôles de sécurité (1h30)

Objectifs

- Identifier les mesures de sécurité adaptées aux risques.
- Construire un plan de sécurisation cohérent.

Contenu

- Contrôles organisationnels.
- Contrôles techniques.
- Gestion des identités et des accès.
- Protection des infrastructures et des données.
- Gestion des prestataires et fournisseurs.

Travail en groupe :
Associer des mesures de sécurité à différents scénarios de risques.

Module 7 : Organiser la gestion des incidents de sécurité (2h)

Objectifs

- Structurer une réponse efficace aux incidents.
- Organiser les rôles et responsabilités.

Contenu

- Cycle de vie d'un incident.
- Détection, qualification et escalade.
- Communication de crise.
- Coordination avec les équipes techniques.
- Retour d'expérience et amélioration continue.

Exercice de simulation :
Traitement d'un incident de cybersécurité de type ransomware.

Module 8 : Atelier de pilotage des risques (1h)

Objectifs

- Consolider les acquis de la journée.

Étude de cas :
Élaboration d'un plan de traitement des risques à partir d'un scénario d'entreprise.

Jour 3 : Conformité, pilotage opérationnel et gestion de crise (7h)

Module 9 : Maîtriser les référentiels et obligations réglementaires (2h)

Objectifs

- Comprendre les principaux cadres réglementaires et normatifs.
- Identifier leurs impacts sur l'organisation.

Contenu

- RGPD et protection des données.
- Directive NIS2.
- ISO 27001 et ISO 27002.
- ISO 22301 et continuité d'activité.
- Audits et exigences de conformité.

Atelier :
Analyse des écarts entre une organisation fictive et les exigences réglementaires.

Module 10 : Organiser la cyberdéfense de l'entreprise (2h)

Objectifs

- Comprendre les mécanismes de surveillance et de protection.
- Définir un dispositif de cyberdéfense adapté.

Contenu

- Veille de sécurité.
- Gestion des vulnérabilités.
- Supervision et SOC.
- Threat Intelligence.
- Exercices de crise cyber.

Brainstorming guidé :
Définition des capacités de cyberdéfense prioritaires selon le contexte de l'organisation.

Module 11 : Piloter la performance cybersécurité (2h)

Objectifs

- Construire des indicateurs pertinents.
- Communiquer efficacement auprès de la direction.

Contenu

- Tableaux de bord RSSI.
- KPI et KRI cybersécurité.
- Reporting exécutif.

- Pilotage de la maturité sécurité.
- Construction d'une feuille de route.

Atelier :
Création d'un tableau de bord RSSI destiné à un comité de direction.

Module 12 : Exercice final – Construire sa feuille de route RSSI (1h)

Objectifs

- Mobiliser l'ensemble des acquis de la formation.
- Formaliser une stratégie cybersécurité cohérente.

Cas pratique de synthèse :
À partir d'une organisation fictive :

- Identification des enjeux.
- Définition de la gouvernance.
- Priorisation des risques.
- Construction d'un plan d'actions sur 12 mois.
- Présentation des recommandations au groupe.

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à mailto:referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.