Formation « RSSI avancé »

Réf : DIRCYBER

Vous avez une expérience de plusieurs années en tant que Responsable de la Sécurité des Systèmes d'Information dans une structure de taille modeste ou moyenne. Votre expérience sur le terrain vous a permis d'apprécier la diversité et la complexité des challenges auxquels doit faire face un leader dans le domaine de la Cybersécurité. Vous désirez donner un nouvel élan à votre carrière et atteindre un niveau de performance vous permettant d'embrasser le rôle de Chief Information Security Officer (CISO) dans des organisations complexes et de dimensions internationales.
La formation DIRCYBER vous fournira la connaissance et les outils vous permettant de développer grandement vos capacités de leadership dans le domaine de la cybersécurité. A l'issue de cette formation hautement interactive et pratique, vous pourrez utiliser de nouvelles techniques vous permettant de définir une stratégie cyber et de mette en place un chantier de transformation et une organisation Cyber fournissant une protection effective et de nouveaux leviers de croissance pour votre entreprise.

Objectifs

- **Fournir les connaissances et les outils permettant de développer grandement vos capacités de leadership dans le domaine de la cybersécurité**
- **Utiliser de nouvelles techniques afin de définir une stratégie cyber**
- **Apprendre à mette en place un chantier de transformation et une organisation Cyber fournissant une protection effective et de nouveaux leviers de croissance pour votre entreprise**

Durée & horaires

- **5 jours soit 35 heures**
- **Horaire : 9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 20 participants**

Public visé

- **Toute personne ayant une expérience de plus de 5 dans la sécurité des systèmes d'information, dont au moins 2 années en tant que RSSI (ou poste équivalent) et visant à devenir un leader dans la sécurité de l'information (typiquement Chief Information Security Officer) dans une organisation large, complexe et de dimension internationale.**
- **RSSI souhaitant définir et mettre en œuvre une stratégie ou un programme de transformation cyber de taille conséquente dans son organisation.**

Pré-requis

- **Avoir plus de cinq années dans la gestion d'équipes en charge de la sécurité de l'information ou de la cybersécurité, dont préférablement 2 ans en tant que RSSI (Responsable de la Sécurité des Systèmes d'Information) dans des entreprises de taille moyenne ou grande.**
- **Avoir une expérience pratique de mise en place d'une partie substantielle d'un programme sécurité de taille conséquente dans une ou plusieurs organisations.**
- **Avoir un bagage fonctionnel solide (à un niveau manager) dans les différents domaines de la sécurité de l'information. Il est fortement recommandé d'avoir participé à la formation RSSI d'HS2 (ou à une ou des formations au contenu équivalent à la formation RSSI d'HS2).**

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. La webcam est obligatoire.**
- **La formation DIRCYBER combine des sections de cours magistral agrémentées de nombreux exercices hautement interactifs. Les participants pourront mettre en pratique les concepts abordés dans la formation lors de multiples mises en situation basées sur des études de cas réalistes. Une partie significative des exercices se déroulera en sous-groupes dans lesquels les participants joueront différents rôles afin de résoudre une problématique commune, assistés parfois par des observateurs ou facilitateurs professionnels. Les participants seront amenés à présenter les résultats de leurs réflexions devant une audience bienveillante et bénéficieront d'un retour leur permettant de progresser dans leur pratique du leadership dans le domaine de la cybersécurité.**
- **Les enseignants ainsi que des facilitateurs et leaders expérimentés fourniront de nombreux retours d'expérience et exemples permettant aux participants de développer leur maturité dans le domaine du leadership et dans le développement et la mise en place de stratégie cyber..**

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)**
- **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 entre 2h00 et 3h00 (format de l'examen en cours de conception) et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification DIRCYBER par HS2.**

Programme

1 - Introduction

- Accueil des participants, présentation de la formation
- Évolution du métier de RSSI, les défis du RSSI, les compétences à développer
- Définir le périmètre du poste de RSSI dans l'entreprise

2 - Analyse et compréhension de l'organisation

- Historique de l'organisation
- Mission, Vision, Objectifs et Stratégie de l'organisation
- La culture de l'organisation
- Identifier, analyser, influence et tirer le meilleur parti des parties prenantes
- Réussir sa prise de fonction
- Soutenir et être soutenu au sein de l'entreprise
- Utiliser au mieux la communauté Cyber

3 - Gestion des risques de l'information

- Les fondamentaux de l'appréciation des risques de l'information
- Identification des actifs, inventaire et classification, « crown jewels », flux d'information
- Identification des menaces cyber (PEST, MITRE ATT&CK)

- Identification des contraintes légales et réglementaires

4 - Créer de la clarté organisationnelle : Le modèle

- Objectifs et bénéfices de la clarté organisationnelle, chaînon manquant à la plupart des organisations peu performantes
- Introduction à une approche structurée pour définir la clarté organisationnelle
- La discipline, élément clé de la réussite d'une stratégie Cyber

5 – Les éléments fondamentaux préalables à la stratégie Cyber

5.1 Raison d'être : pourquoi existons-nous ?

- Penser au-delà de la protection de l'information, alignement avec la mission et raison d'être de l'entreprise et avec le périmètre d'action du RSSI
- Méthodologies pour définir le premier niveau de la Mission de l'équipe Cyber

5.2 Les valeurs fondamentales : comment nous comportons-nous ?

- Les valeurs, fondements de l'identité de l'équipe Cyber
- Les différents types de valeurs : fondamentales, aspirationnelles, comportementales (« permission to play »), accidentelles
- Identifier des valeurs fondamentales de l'équipe Cyber en phase avec l'organisation.

5.3 Que faisons-nous ?

- Définir clairement les activités de l'équipe Cyber
- Le deuxième niveau de définition de la Mission de l'équipe Cyber

6 - Définir la stratégie Cyber

6.1 Comment allons-nous réussir ?

- Qu'est-ce qu'une stratégie ?
- Identifier un GOA « Grand Objectif Audacieux – le principe du hérisson
- Définir les « ancres stratégique » ou « piliers stratégiques »
- Définir la Vision de l'organisation Cyber

6.2 Définir le plan stratégique

- Utilisation d'un référentiel (framework) pour organiser les activités Cyber
  - Revue des référentiels les plus courants
  - Quel(s) référentiel(s) choisir pour votre organisation
  - Quand et comment créer son propre référentiel ?
- Analyse détaillée des activités et services Cyber existants (As-Is)
- Analyse de la maturité cyber de l'organisation
- Définir l'état futur de la sécurité (To-Be)
- Gap Analysis et Définition des activités du programme Cyber
- Priorisation des activités du programme Cyber et production du Plan

7 - Obtenir le support de la Direction et du Conseil D'Administration

- Créer un Business Case et un récit convaincants
  - Définir les bénéfices d'un programme Cyber
  - Analyse de l'audience et l'art du « story-telling »
- Les clés d'une réunion convaincante avec la Direction et le Conseil d'administration

8 - Implémentation de la Stratégie Cyber

- Design d'un Modèle organisationnel Cible pour l'organisation Cyber
  - Le business model de l'équipe
  - Définition d'un catalogue d'activités et de services
  - Principes de design de l'équipe (localisation, outsourcing, délégation)
- Gestion des ressources et des capacités Cyber

9 - Développer une équipe Cyber hautement performante

- Les bonnes personnes avant tout
- Développer les 5 principes d'une équipe hautement performantes
- Communiquer la clarté organisationnelle
- Renforcer la clarté organisationnelle

10 - Responsabilités Opérationnelles du RSSI

- La gestion du risque cyber au quotidien
- La gestion de la conformité
  - Mise en place d'une approche de certification
  - Gestion des audits internes et externes
- La gestion du budget Cyber
- Le pilotage de la Cyber par les métriques
  - Revue opérationnelle des services
  - La création et mise en place d'un tableau de bord cyber effectif