EduGroupe
Accompagner pour réussir

Parcours certifiant Piloter et animer la sécurité informatique

Référence : **SECPASI**

Durée : **31 jours (217 heures)**

Certification : **Certification professionnelle Piloter et animer la sécurité informatique**

Connaissances préalables

- Il est impératif de justifier d'une expérience professionnelle dans le domaine visé par la certification, acquise au sein de la Direction des systèmes d'information d'une entreprise ou d'une ESN (Entreprise de Services du Numérique) ou de justifier d'un diplôme ou d'une certification de niveau 5 (par exemple : BTS Services Informatiques aux Organisations, BTS Systèmes numériques, DUT informatique, Licence Porfessionnelle Métiers de l'informatique, BUT Informatique, Titres à finalité professionnelle, CQP Administrateur Systèmes et Réseaux, etc.)
- Plus explicitement :
- Connaître le guide d'hygiène sécurité de l'ANSSI ou connaître les bonnes pratiques telles qu'elles sont décrites dans ce guide.
- Fondamentaux réseaux : Modèle OSI - Equipement réseaux - Fonctionnement TCP/UDP - Service applicatif commun (http, DNS, SMTP, SSL).
- Fondamentaux système : Compréhension de base Windows (Service, fonctionnement) - Compréhension de base Linux (CLI, Service, fonctionnement).
- La compréhension de l'anglais est un plus

Profil des stagiaires

- Ce parcours certifiant à des personnes titulaires d'une certification de niveau 5 ou 6 dans le domaine de l'informatique, dont la cybersécurité n'est pas la seule fonction (techniciens systèmes et réseaux, assistance technique dans les ESN, différents profils de la DSI)
- Le périmètre de la certification correspond aux activités des professionnels qui exercent dans les métiers de la Gestion de la sécurité et du pilotage des projets de sécurité ou dans les métiers du Conseil, services et recherche

Objectifs

- A l'issue de la formation, le participant sera capable de mettre en œuvre de manière opérationnelle les principes fondamentaux, les normes et les outils de la sécurité informatique.
- Être en mesure de mettre en place une stratégie de cybersécurité à partir d'une analyse du risque
- Être capable de sécuriser des réseaux, des protocoles, des terminaux et des serveurs
- Pouvoir animer et évaluer la mise en oeuvre de la stratégie de cybersécurité

Certification préparée

- Aucune

Méthodes pédagogiques

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

Formateur

- Consultant-formateur expert en Cybersécurité

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Les fondamentaux de la cybersécurité (35 heures)

2. Jour 1 : Introduction à la cybersécurité

- Matin : Enjeux de la sécurité des systèmes et réseaux ; Analyse des cyberattaques récentes
- Après-midi : Identification de failles sur des scénarios prédéfinis

3. Jour 2 : Architecture et moyens de protection

- Matin : Principes d'architecture sécurisée ; Équipements de sécurité : firewalls, proxys
- Après-midi : Mise en place d'un firewall et test de configurations

4. Jour 3 : Sécurisation des systèmes

- Matin : Sécurisation des systèmes Windows et Linux ; Configurations des politiques de groupe
- 💡 *Après-midi : Atelier de durcissement d'un système Linux*

5. Jour 4 : Veille technologique et menaces émergentes

- Matin : Introduction à la veille technologique ; Exploration des bases de données de vulnérabilités
- Après-midi : Mise en place d'un processus de veille personnalisé

6. Jour 5 : Synthèse et mise en pratique

- Matin : Synthèse des acquis ; Discussion sur les bonnes pratiques de veille et sécurisation
- Après-midi : Révision globale des concepts abordés
- 💡 *Après-midi : Finalisation des projets pratiques ; Activité collaborative : brainstorming en petits groupes pour récapituler et partager les bonnes pratiques identifiées au cours du module.*

7. Module 2 : les fondamentaux de la réglementation de la cybersécurité (7 heures)

- Matin : Cadre réglementaire ; Introduction à la réglementation : RGPD et normes ISO ; Étude des obligations liées aux données personnelles
- Après-midi : Application et bonnes pratiques
- 💡 *Après-midi : Cas pratiques : analyse d'une étude d'impact (PIA) ; Atelier collaboratif : élaboration d'une politique de conformité adaptée ; Synthèse et réponses aux questions des participants*

8. Module 3 : Pilotage d'un plan d'action en cybersécurité (70 heures)

9. Jour 1-2 : Introduction à la PSSI et planification

- Matin : Principes et structure de la PSSI
- Après-midi : Identification des contraintes et ressources

10. Jour 3-5 : Gestion de projet appliquée

- Planification des tâches et gestion des ressources
- Utilisation d'outils pratiques : création d'un projet type

11. Jour 6-7 : Communication et collaboration

- 💡 *Animation de réunions : scénarios et jeux de rôle*
- 💡 *Gestion des parties prenantes : études de cas*

12. Jour 8-9 : Rédaction et recommandations

- Préparation d'un rapport stratégique
- 💡 *Simulation de présentation à un comité fictif*

13. Jour 10 : Synthèse et évaluation

- Bilan global du module
- 💡 *QCM et étude de cas final pour valider les acquis*

14. Module 4 : Analyse et évaluation des risques de sécurité (42 heures)

15. Jour 1-2 : Fondamentaux de la gestion des risques

- Matin : Introduction aux concepts clés et typologie des risques
- Après-midi : Exploration des normes ISO et SMSI

16. Jour 3-4 : Cartographie des actifs et analyse des risques

- Matin : Techniques de cartographie et identification des actifs critiques
- 💡 *Après-midi : Atelier sur l'établissement d'un contexte de gestion des risques*

17. Jour 5 : Analyse et évaluation des risques

- Matin : Application de la méthode EBIOS
- 💡 *Après-midi : Rédaction des recommandations et plans d'action*

18. Jour 6 : Synthèse et validation

- Matin : Discussion sur les plans de gestion des risques
- 💡 *Après-midi : Évaluation finale (cas pratique et QCM)*

19. Module 5 : Organisation et coordination des réponses à incident (14 heures)

20. Jour 1 : Introduction et plans de continuité

- Matin : Principes de gestion des incidents et présentation des PCA/PRA
- 💡 *Après-midi : Atelier de constitution d'équipes et de rédaction de procédures*

21. Jour 2 : Mise en situation et synthèse

- 💡 *Matin : Simulation de gestion de crise avec analyse des incidents*
- 💡 *Après-midi : Discussion sur les bonnes pratiques et évaluation finale*

22. Module 6 : Mise en œuvre d'actions de contrôle de cybersécurité (21 heures)

23. Jour 1 : Organisation et outils d'audit

- Matin : Introduction aux objectifs et planification des actions de contrôle
- Après-midi : Présentation des outils d'audit et d'évaluation

24. Jour 2 : Mise en pratique des audits

- 💡 *Matin : Atelier d'audit de configuration et de tests utilisateurs*
- Après-midi : Identification et correction des vulnérabilités

25. Jour 3 : Supervision et synthèse

- Matin : Analyse des rapports d'audit et présentation des recommandations
- Après-midi : Synthèse et évaluation finale avec un cas pratique complet

26. Module 7 : Sensibilisation et formation des équipes (28 heures)

27. Jour 1 : Principes et enjeux de la sensibilisation

- Matin : Introduction aux concepts de sensibilisation et conduite du changement
- 💡 *Après-midi : Atelier sur les objectifs et attentes des utilisateurs finaux*

28. Jour 2 : Supports et bonnes pratiques

- Matin : Création et personnalisation de supports de sensibilisation
- 💡 *Après-midi : Simulation de sessions interactives (phishing, mots de passe)*

29. Jour 3 : Mise en place d’un plan de formation

- Matin : Analyse des besoins et élaboration de parcours
- Après-midi : Sélection et évaluation des formations

30. Jour 4 : Synthèse et évaluation

- *Matin : Simulation de sessions de sensibilisation*
- *Après-midi : Évaluation finale et réflexion sur l’impact des actions*

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