@ www.esa-management.data.com

ESA MANAGEMENT
DATA & DIGITAL

FORMATION PROFESSIONNELLE CONTINUE

MASTÈRE DATA ENGINEER EN CYBER SECURITÉ

PRÉSENTATION

Avoir un collaborateur ayant les compétences liées à la prévention des cyberattaques est devenu pour les entreprises une nécessité. A l'heure actuelle, la cyber criminalité est de plus en plus fréquente et représente un risque important pour les organisations. Ces dernières doivent pouvoir mettre en place une stratégie afin des se prémunir de toutes les intrusions possibles sur les réseaux.

Le Data Engineer en cyber sécurité va pouvoir par ses compétences, assurer un rôle d'analyste des risques et élaborer une mise en œuvre et un suivi d'une stratégie cyber sécurité des entreprises.

OBJECTIFS DE LA FORMATION

Le mastère a pour objectifs de valider les compétences de Data Engineer en cyber sécurité.

Activités complexes qui va permettre au titulaire du mastère d'exercer un métier en plein essor. La cyber sécurité est en effet un pôle en développement dans les entreprises.

Format : Blended-learning **Durée : 320 heures**
Modalité : à votre rythme
Prix : 4 200 € TTC

Possibilité de payer en 6 prélèvements de 700 €TTC, le premier dès l'inscription puis le 05 des cinq mois suivants. Il peut-être pris en charge par votre entreprise.

Prérequis : titulaire au moins d'un diplôme de niveau 6 ou d'une expérience d'un an dans une fonction d'encadrement dans laquelle la cyber sécurité devient l'un des enjeux stratégiques.

Compétences visées

- Analyser les besoins en cyber sécurité de l'entreprise dans un environnement de travail donné,
- Elaborer, mettre en œuvre et suivre une stratégie de cyber sécurité de l'entreprise,
- Mettre en place et piloter une stratégie des systèmes de sécurité de l'entreprise.

PUBLIC CONCERNÉ

- des salariés dont l'entreprise envisage une stratégie en cyber sécurité,
- des salariés en évolution de carrière,
- des salariés en reconversion professionnelle,
- des demandeurs d'emploi...

DÉBOUCHÉS

- Data Engineer
- Data Protection Officer
- Business Intelligence Manager

Vos principaux intervenants

Khaldoun SERHAL
FORMATEUR EXPERT
- Global Lead Account Partner BNP Paribas, Sopra Steria Consulting
- Sales Director, IBM
- Senior Manager, Deloitte Consulting
- Financial Sector - Strategy & Operations, HSBC
- Inspection Générale, HSBC
- Financial Sector, PwC France

DOMAINES D'EXPERTISES
Management, IT Strategy, Management Consulting, Sales Strategy, Processus commerciaux, Informatique décisionnelle, Business Intelligence, Analytics, Conseil en management, Assurance, Banque

Philippe COLLAS
FORMATEUR EXPERT
Coach-consultant, PhilCoDev
Principal, SECOR
Corporate VP HR Development, AXA en France

DOMAINES D'EXPERTISES
Risk management, cyber-risques, cyber sécurités, Business strategy

MASTÈRE DATA ENGINEER EN CYBER SECURITÉ

PROGRAMME

ACTIVITE I - ANALYSE DES BESOINS EN CYBER SÉCURITÉ DE L'ENTREPRISE DANS UN ENVIRONNEMENT DE TRAVAIL DONNÉ

- Analyser les demandes et besoins de l'entreprise en s'appuyant sur des informations utiles en lien avec le système de cyber sécurité actuel afin de définir le cadre du projet et les objectifs à atteindre.
- Auditer la sécurité des systèmes d'information de l'entreprise à travers des tests d'intrusion et d'analyse après incident de façon automatisé afin d'identifier les risques liés.
- Elaborer une cartographie des cyber risques, selon les différentes typologies de risques (stratégiques, de conformité, financiers, opérationnels) en appréciant le niveau d'acceptabilité des impacts (gravité/intensité) afin de synthétiser et définir les priorités dans un processus visant une aide à la décision
- Elaborer le cahier des charges du projet de gestion des systèmes de sécurité de l'entreprise en définissant les moyens nécessaires aux différentes tâches le composant (collaborateurs, responsabilités), leurs durées respectives et les résultats attendus afin de cadrer toutes les étapes de sa mise en œuvre.

Evaluation : Etude de cas pratique portant sur l'analyse des besoins d'une entreprise en terme de Cyber Sécurité.

ACTIVITÉ II - ELABORATION, MISE EN ŒUVRE ET SUIVI D'UNE STRATÉGIE DE CYBER SÉCURITÉ DE L'ENTREPRISE

- Elaborer un plan de mitigation des cyber risques en caractérisant les différentes actions à réaliser et en mettant en place un plan de prévention afin d'établir une feuille de route priorisant et organisant les moyens à mobiliser.
- Mettre en œuvre le plan de mitigation en adaptant les différents outils de gestion des risques cyber, en assurant le lien avec la gouvernance des risques de l'entreprise en terme de prise de décision tout en s'appuyant sur une veille technologique sur l'évolution de la cybercriminalité afin d'obtenir une gestion efficace et opérationnelle du dispositif mis en place dans une logique d'amélioration continue.
- Assurer le pilotage des risques cyber auprès des collaborateurs en définissant les indicateurs de performance et de suivi des risques cyber, en s'appuyant sur des techniques de communication collaboratives et des outils de conduite de projet tout en adaptant les mesures de gestion des cyber risques au regard des exigences métiers afin d'obtenir les résultats attendus par la gouvernance de l'entreprise et faciliter la prise de décisions d'actions correctives.
- Assurer le suivi de la stratégie de sécurité mise en place en s'appuyant sur différents indicateurs de performance afin d'apporter des actions correctives si besoin est.

Evaluation : Etude de cas pratique portant sur l'élaboration, la mise en œuvre et le suivi d'une stratégie de cyber sécurité.

ACTIVITÉ III - MISE EN PLACE ET PILOTAGE DES SYSTÈMES DE SÉCURITÉ DE L'ENTREPRISE

- Définir la nouvelle stratégie de l'entreprise centrée sur le système de cyber sécurité de l'entreprise ainsi que ses outils en quantifiant le coût global de cette stratégie. Elaborer un planning de réalisation cohérent avec les objectifs attendus dans le temps, notamment financier en fonction des priorités métiers de croissance, de gestion des risques et de réduction des coûts.

Evaluation : Etude de cas pratique portant sur l'accompagnement à la mise en place du système de cyber sécurité de l'entreprise.

Décrochez un Mastère à votre rythme !

MODALITÉS PÉDAGOGIQUES

L'ingénierie pédagogique de cette formation qui s'appuie sur 360 Learning, plateforme de collaborative learning est un juste équilibre entre :

- des notions théoriques
- des démonstrations, de solutions, de challenge, des cas d'usage...
- des exercices pratiques des techniques de l'exploitation d'un système de cyber sécurité

Chacune des trois parties doit être validée par une note égale ou supérieure à 10/20 pour obtenir le MASTERE DATA ENGINEER EN CYBER SECURITE délivré par ESA MANAGEMENT.

RESSOURCES PÉDAGOGIQUES

Chaque bloc est composé :

- de vidéos,
- de démonstrations et cas d'usages,
- d'un suivi interactif par e-mail entre l'apprenant et l'enseignant,

VOUS ÊTES INTÉRESSÉ(E) PAR CETTE FORMATION ?

Admission et contact : Fetta ETTER

13 rue Fernand Léger, 75020 Paris
01 85 73 31 09 I 06 15 02 96 71
fetta-etter@esa-management.com
www.esa-management.data.com