DIGITAL ACT®
ACADEMY

CMMC

Cybersecurity Maturity Model Certification Certified Professional

1. Présentation

A l'ère du digital, nombreux sont les domaines d'activité qui font face à des incidents de sécurité. Le domaine de la défense n'est pas en reste. C'est pourquoi en 2019, le Département de la Défense des Etats-Unis d'Amérique -DoD-, a créé le cadre **CMMC** -**C**ybersecurity **M**aturity **M**odel **C**ertification-.

Le CMMC est un mécanisme de vérification qui a pour objectif d'évaluer le niveau de maturité des organisations en matière de protection des informations non classifiées telles que les informations sur des contrats fédéraux ou encore, des informations contrôlées non classifiées.

En matière de cybersécurité, le CMMC englobe divers standards internationaux. Il intègre un certain nombre de processus et de pratiques répartis sur cinq niveaux de certification cumulatifs.

A travers une session de quatre (4) jours, les participant(e)s pourront acquérir une connaissance complète du modèle CMMC et de ses exigences. La certification Certified Professional est un prérequis pour les certifications : Certified Assessor Level 1, Certified Assessor Level 3 et Certified Instructor.

2. Objectifs

- Comprendre les domaines, les capacités, les niveaux, les processus et pratiques du modèle CMMC ;
- Reconnaître la corrélation entre le modèle CMMC, la clause 52.204-21 du FAR, la clause 252.204-7012 du DFARS, le NIST SP 800-171 et d'autres standards internationaux ;
- Interpréter les exigences du modèle CMMC dans le contexte spécifique d'un organisme en quête de certification -OSC- ;
- Aider un organisme à mettre en œuvre et à gérer efficacement les exigences du modèle CMMC ;
- Acquérir des connaissances sur la méthodologie et le processus d'évaluation du modèle CMMC.

3. Public cible

Cette formation s'adresse principalement aux professionnels souhaitant faire partie de l'écosystème CMMC, nous pouvons citer parmi eux : responsables de la sécurité, évaluateurs et instructeurs certifiés, fournisseurs du ministère de la défense et de la base industrielle de la défense, consultants en cybersécurité.

4. Durée

04 jours

5. Prérequis

Il est recommandé que les participant(e)s disposent d'une connaissance générale des concepts et principes de la cybersécurité et des technologies de l'information.

6. Certification

L'examen -CMMC Certified Professional- est inclus dans le coût de la formation et n'est disponible qu'en langue anglaise.

L'examen a une durée de trois (3) heures et couvre les cinq domaines de connaissances suivants :
Domaine 1 : Sources de données et gouvernance
Domaine 2 : Écosystème CMMC-AB
Domaine 3 : Éthique
Domaine 4 : Modèle CMMC
Domaine 5 : Mise en œuvre CMMC

© DIGITAL ACT ACADEMY 2023

7 Programme

Jour 1 Introduction aux parties prenantes, au modèle et aux pratiques CMMC de niveau 1

Jour 2 Processus et pratiques CMMC des niveaux 2 et 3

Jour 3 Processus et pratiques CMMC des niveaux 4 et 5

Jour 4 Rôles et responsabilités, éthique et méthodologie d'évaluation de l'écosystème CMMC-AB

© DIGITAL ACT ACADEMY 2023