FORMATION RESPONSABLE MANAGEMENT DES INCIDENTS DE SECURITE de L'INFORMATION (ISO 27035)

Ref. **CRMIS-08**
Durée : 4.0 jour(s) / 28.0 heures

Les systèmes d'information sont omiprésents dans notre quotidien et prennent une place stratégique pour les entreprises. Une mise à mal de ces systèmes peut engendrer de lourdes conséquences et mettre en péril la pérénité d'une entreprise. Pour pouvoir se prémunir des menaces il faut maitriser la connaissance de son système et de ses vulnérabilités et pouvoir réagir au mieux lorsqu'un incident de sécurité survient. Cela est possible en suivant des recommandations internationales, notamment celle de ISO 27035.
Cette certification permet de valider un ensemble de savoirs necessaires pour mettre en place un processus de management de la gestion des incidents de sécurité

Elle s'inscrit dans un shéma de Formation visant à valider les fiches métiers de l'ANSSI suivantes : Consultant en cybersécurité, Formateur en cybersécurité, Évaluateur de la sécurité des technologies de l'information, responsable SOC, responsable CSIRT, auditeur de la sécurité organisationnelle, RSSI.

Pré-requis :

Connaissances SSI
Connaissances Systemes

Personnes concernées :

Responsables gestion des incidents de sécurité de l'information
Chefs de projets sécurité
Architectes sécurité
Intégrateur sécurité
Personne étudiant la cyber-sécurité
Responsable sécurité
Auditeur sécurité
Formateur

ECSF METIERS ASSOCIE :
Cyber Incident responder, Chief Information Security Officer, Cybersecurity auditor

Objectifs :

Décrire le processus de gestion des incidents de sécurité de l'information
Acquérir le vocabulaire nécessaire à la gestion des incidents de sécurité de l'information
Etablir le processus de management de la gestion des incidents selon la norme ISO 27035

Préparer la mise en œuvre du processus

Programme :

JOUR 1

Les normes ISO et la gestion des incidents SI :

Famille ISO 27035
27043 et autres normes
Approche structurée
Vocabulaire
Présentation de la 27035-1
Présentation de la 27035-2
Présentation de la 27035-3

TD : études des normes et des processus associés, Quizz, Etudes de cas

JOUR 2

Mise en place du management de la gestion des incidents SI

Définition des objectifs
politiques
resources
compétences
formation
communiquation
plan de gestion des incidents SI
Création d'une IRT
Support technique
Test

TD : mise en pratique des points abordés via une étude de cas. Travail en groupe

JOUR 3

Mise en place suite

Détection et rapport
Evaluation et décisions
Réponses
Analyses
Rapports final et conclusion
Amélioration continue

TD : mise en pratique des points abordés via une étude de cas. Travail en groupe

JOUR 4

Préparation examen final : quizz sur l'ensemble des points abordés, étude de cas sur la mise en œuvre d'un processus de gestion des incidents de la sécurité de l'information

Examen final : QCM sur le processus de gestion des incidents de la sécurité de l'information selon l'ISO 27035, Mise en situation spécifique. Etude de cas et élaboration d'un processus de gestion des incidents de sécurité de l'information

Démarche pédagogique :

Formation orientée sur la pratique
70% de pratique et 30% de théorie

Evaluation et validation :

EXAMEN : PASSAGE DE LA CERTIFICATION DE PERSONNES

Partie théorique et pratique
Le temps destiné au passage de la certification est de 2H.
L'examen est composé de 3 parties :

- QCM,
- Mise en situation sur points spécifiques,
- Mise en situation sur cas concrets.

Bureau Veritas Certification assure l'examen final de ce programme de formation.

L'examen valide des domaines de compétences en relation avec les profils métiers identifiés par l'European union agency for cybersecurity via l'European Cybersecurity Skills Framework