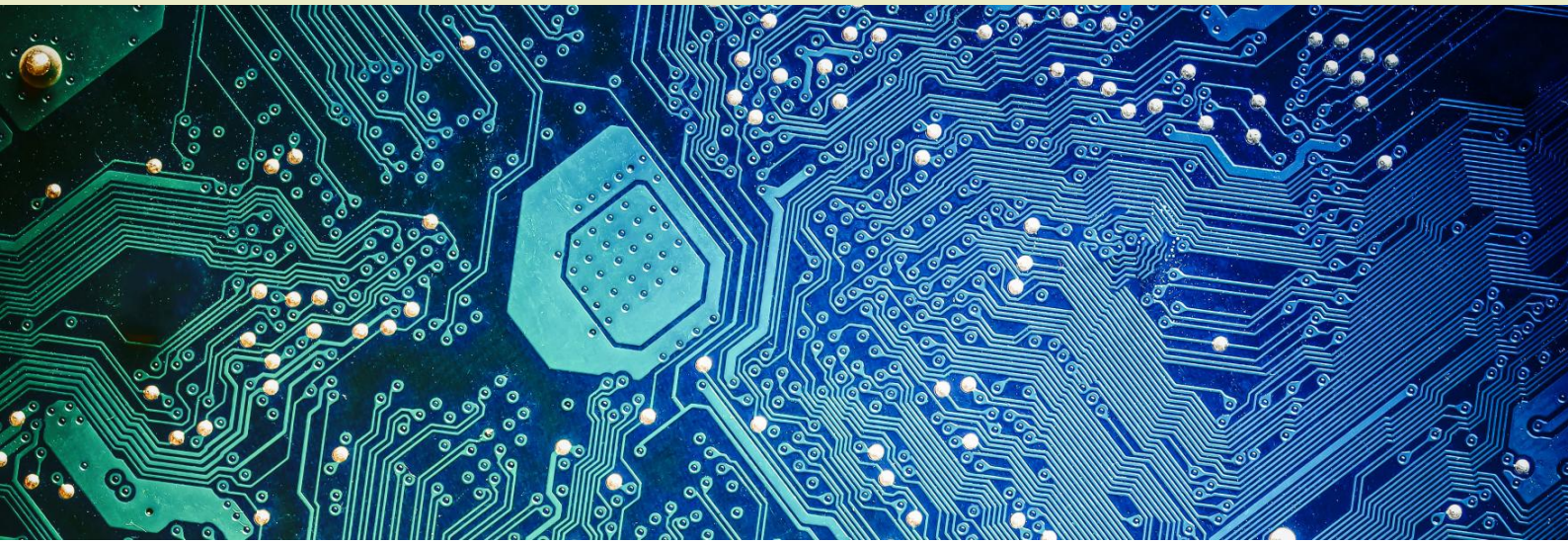
DIPLÔME

Certificat de spécialisation Gestion de risque IT et réponse aux incidents cyber en situation

Code : CS11100A



Niveau d'entrée : Aucun
Niveau de sortie : Aucun
ECTS : 15

Déployabilité
A la carte : Formation pouvant s'effectuer au rythme de l'élève, en s'inscrivant aux unités du cursus
Package : Formation pouvant se suivre en s'inscrivant à un "package" (groupe d'enseignements indissociables)

Compétences et débouchés

Mener, gérer et traiter une analyse des risques cyber (enjeux et menaces techniques et organisationnels), un plan de continuité d'activité en situation d'incident de sécurité, une réponse à incident cyber,
Comprendre et utiliser les outils et méthodes de créativité, de veille, de modélisation et de prototypage de solutions dans l'urgence, d'outils de conception et de communication pour pitcher la solution de remédiation,
Gérer et mettre en place un système de management de la sécurité de l'information (ISMS – ISO 27x), un plan de continuité d'activité à partir d'une architecture technique (SMCA-ISO 27031), un exercice de crise,
Élaborer et mener une réponse à un nouveau risque ou à un incident de sécurité ou à une crise cyber dans « l'action » en vue du maintien de la continuité d'activité,
Comprendre et agir face aux nouvelles menaces, attaques et vulnérabilités des organisations (cas de la gestion des zero-days,...),

Mener une démarche d'investigation et de remédiation post-incident afin de faire évoluer les process opérationnels des organisations en situation de risque et de crise cyber, Savoir rédiger et organiser un plan de Reprise et de Continuité d'Activité (PRA/PCA). Comprendre, organiser et analyser une cellule de crise de coordination (processus, organisation, méthode) en vue de faire évoluer les plans de défense adaptés au contexte de l'organisation étudiée : objectifs, tests, analyse qualification, typologie, mode d'élaboration, qualification de la remédiation.
Etablir et conduire un diagnostic 22301 et 27031 avec une analyse des impacts sur l'activité,
Mettre en œuvre et gérer un processus de détection continus de l'émergence de menaces Savoir accompagner les publics non techniques dans des phases de sensibilisations aux réponses à incident cyber (Phishing, CyberEntrainement),
Effectuer des missions de sensibilisation auprès de publics techniques (Training Technique) ;
Assurer une veille permanente vis-à-vis des scénarios d'attaques, des nouvelles menaces et des vulnérabilités associées ;

Méthodes pédagogiques

Les enseignements théoriques, couplés à des mises en application en travaux dirigés et travaux pratiques sur matériels et logiciels métiers permettront une professionnalisation rapide. L'espace numérique de formation du Cnam (Moodle) permet à chaque enseignant de rendre accessible des ressources spécifiques à ses enseignements. Des modalités plus détaillées seront communiquées au début de chaque cours.

Prérequis et conditions d'accès

Niveau 6, Bac+3 en scientifique, technique ou informatique ou expérience professionnelle significative dans les métiers de l'informatique

MENTIONS OFFICIELLES

Mots-clés

Cybersécurité

Informations complémentaires

Type de diplôme

Certificat de spécialisation

Formacode

Gestion réseau informatique [24220]

Code du parcours

CS11100A

Modules d'enseignement

- → Analyse de risques des données, réseaux et systèmes
- → Créativité - Innovation
- → Gestion d'une réponse à incident Cyber : Exercice d'entrainement
- → Projet final

Blocs de compétences

Un bloc de compétences est constitué d'un ensemble d'Unités qui répond aux besoins en formation de l'intitulé du bloc.
Les unités ci-dessus sont réparties dans les Blocs de compétences ci-dessous.
Chaque bloc de compétences peut être validé séparément.
Information non disponible, pour plus d'information veuillez contacter le Cnam