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

Présentation

Publics / conditions d'accès

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

Compétences

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 ;

Mis à jour le 08-12-2021

Code : CS11100A

15 crédits

Certificat de spécialisation

Responsabilité nationale : EPN05 - Informatique / Véronique LEGRAND

Niveau CEC d'entrée requis : Sans niveau spécifique

Niveau CEC de sortie : Sans niveau spécifique

Mode d'accès à la certification :

NSF :

Métiers (ROME) :

Contact national :

EPN05 -IRSM

2 rue Conté
75003 Paris

KONTOULI Konstantina
konstantina.kontouli@lecnam.net

Enseignements

15 ECTS

Analyse de risques des données, réseaux et systèmes	SEC104 6 ECTS
Gestion d’une réponse à incident Cyber : Exercice d’entrainement	SEC109 2 ECTS
Créativité - Innovation	USMP08 3 ECTS
Projet final	UACB03 4 ECTS