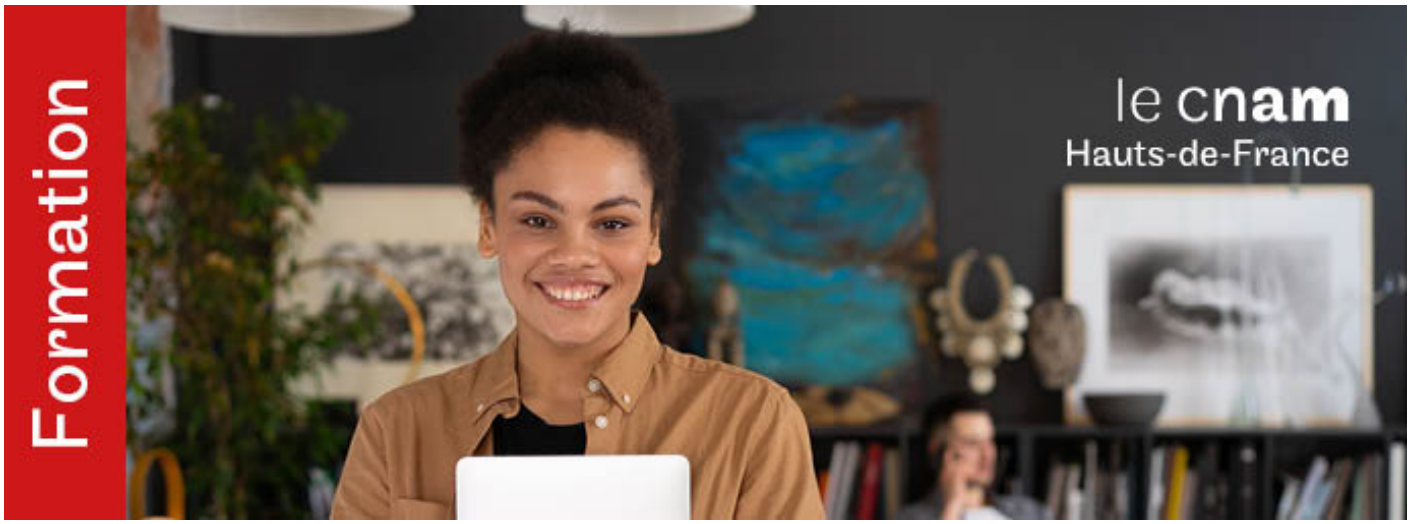

Certificat de spécialisation Cybersécurité et analyse des menaces (cyber threat intelligence)

CS9400A - 8 crédits

Niveau(x) d'entrée : Aucun niveau requis
Niveau(x) de sortie : Aucun niveau spécifique
Lieu(x) : Non proposé en présentiel au Cnam HdF, nous contacter pour possibilité de formation à distance et hybride

Possibilité d'obtention par la VAE AU CNAM

PRÉSENTATION

Public / conditions d'accès

Personnels d'entreprise et de la fonction publique, ingénieurs, chefs de projet, managers, journalistes, étudiants souhaitant se former en cybersécurité ou mettre à jour leurs compétences et ayant déjà des connaissances en système et réseau.
Techniciens spécialisés dans un domaine de l'informatique, architectes système, analystes, programmeurs, développeurs...
Ce certificat de spécialisation s'adresse :
Aux personnes justifiant d'un niveau de formation bac +3 dans un domaine de formation compatible avec la spécialité du CS.
L'enseignement se déroule en modalité 100% distante, avec des temps de webconférences (programmées en fin de journée) obligatoires. Pour s'inscrire, le candidat devra communiquer un CV détaillé et une lettre de motivation à l'adresse psdr3c@lecnam.net.
Il est également proposé en présentiel (au premier semestre), en Polynésie.

Objectifs

Le certificat de spécialisation vise à permettre aux professionnels disposant de connaissances générales en informatique de mieux comprendre les problématiques de sécurité numérique, de cybersécurité et d'analyse des menaces (« cyber threat intelligence »).
Il s'agit de mettre en exergue la relation entre ingénierie sociale et ingénierie technologique, élément souvent sous estimé dans la compréhension des risques et menaces touchants l'espace cyber.
Ce certificat inédit entend fournir les moyens de prévenir et de répondre aux situations de vulnérabilité.

COMPÉTENCES ET DÉBOUCHÉS

Compétences

Identification du panorama de l'espace cyber.
Présentation de la chaîne cybercriminelle.
Acquisition d'une culture générale sur la notion de cybersécurité.
Présentation des concepts de base permettant la compréhension des risques et des menaces et les moyens d'y faire face.
Comprehension des mécanismes des cyber-attaquants, leurs motivations et modi operandi (identification de la cible, préparation de l'attaque, ...).
Connaissance des ressources et bases de données utiles à l'analyse des menaces : whois, certificats, base de données de malwares, CERT, CVE, etc.
Mise en capacité de mesurer les enjeux et les menaces selon le cadre professionnel, savoir envisager les impacts des différents incidents potentiels. Mettre en oeuvre des stratégies de minimisation des vulnérabilités et des risques cyber.

INFORMATIONS PRATIQUES

Projet tutoré.

PROGRAMME

Contenu de la formation

Tronc commun

CyberMenaces : Cybersécurité et analyse des menaces (cyber threat intelligence)	CRM218	4 ects
Projet personnel tutoré	UAIP1X	4 ects

Méthodes pédagogiques:

Pédagogie qui combine des enseignements académiques et des pédagogies actives s'appuyant sur l'expérience en entreprise et le développement des compétences. Equipe pédagogique constituée pour partie de professionnels.

Modalités d'évaluation:

Chaque unité (UE, UA) fait l'objet d'une évaluation organisée en accord avec l'Etablissement public (certificateur) dans le cadre d'un règlement national des examens.

Un référent Cnam est dédié à l'accompagnement de toute personne en situation de handicap. Contactez : hdf_handicap@lecnam.net

Document non contractuel.
Le programme et le volume horaire de cette formation sont susceptibles d'être modifiés en fonction des évolutions du référentiel pédagogique national.

Le Cnam Hauts-de-France vous informe, vous accompagne et vous conseille.

Contactez nos conseillers formation au 0800 719 720 ou hdf_contact@lecnam.net

Tous nos programmes sur www.cnam-hauts-de-france.fr