CYBERMENACES, CYBERSECURITE, CYBERCRISES : COMPRENDRE POUR AGIR

Comprendre la complexité du monde cyber et des enjeux d'un monde connecté de plus en plus complexe et de plus en plus vulnérable

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

Présentation

Publics / 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.

Modalités de validation

Projet tutoré.

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, …).

Mis à jour le 17-04-2024

Code : CS9400A

8 crédits

Certificat de spécialisation

Responsabilité nationale : EPN15 - Stratégies / Julia PIELTANT

Niveau CEC d'entrée requis : Sans niveau spécifique

Niveau CEC de sortie : Sans niveau spécifique

Mode d'accès à la certification :

- Formation continue

NSF : Informatique, traitement de l'information, réseaux de transmission (326)

Métiers (ROME) : Administrateur / Administratrice sécurité informatique (M1801) , Consultant / Consultante informatique (M1806) , Expert / Experte sécurité informatique (M1802) , Ingénieur informaticien / Ingénieure informaticienne (M1805) , Responsable des systèmes informatiques (M1803) , Responsable sécurité informatique (M1802) , Technicien / Technicienne réseau informatique (M1810) , Technicien / Technicienne système informatique (M1810) , Superviseur / Superviseuse help desk en informatique (I1401) , Expert / Experte en cybersécurité (M1802) , Analyste en cybersécurité (M1805) , Développeur / Développeuse de sécurité des systèmes d'information (M1805)

Contact national :

EPN15 - Criminologie Psdr3c
2 rue Camille Guérin
22440 Ploufragan
09 72 31 13 12

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 œuvre des stratégies de minimisation des vulnérabilités et des risques cyber.

psdr3c@Lecnam.net

Enseignements

8 ECTS

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