CRM218 - CyberMenaces : Cybersécurité et analyse des menaces (cyber threat intelligence)

Mis à jour le 11-02-2025

Code : CRM218

Unité d'enseignement de type cours

4 crédits

Volume horaire de référence (+/- 10%) : **40 heures**

Responsabilité nationale :
EPN15 - Stratégies / 1

Contact national :

EPN15 - Criminologie Psdr3c

2 rue Camille Guérin
22440 Ploufragan
09 72 31 13 12

psdr3c@Lecnam.net

Présentation

Prérequis

Ce certificat de spécialisation s'adresse :

• aux titulaires d'un diplôme bac+ 3 dans un domaine de formation compatible avec la spécialité du certificat ;

• aux personnes justifiant d'un niveau de formation dans un domaine compatible avec la spécialité du certificat de spécialisation et bénéficiant des procédures de validation des études supérieures (VES), de validation des acquis de l'expérience (VAE) et de validation des acquis personnels et individuels (VAPP).

L'admission des auditeurs se fait sur dossier candidature, sous réserve d'acceptation par les responsables de la formation.

Objectifs pédagogiques

Ce certificat entend répondre à un besoin grandissant d'acquisition de nouvelles compétences par les professionnels face aux problématiques de sécurité numérique et de cyber-sécurité. C'est une formation aux enjeux et menaces liés à l'espace cyber pour les entreprises et les administrations, ainsi qu'aux moyens de prévention et de réponses à des incidents.

Plus spécifiquement, ce certificat vise à :

• acquérir une culture générale sur la notion de cybersécurité et connaître les concepts de base permettant la compréhension des risques et des menaces ainsi que les moyens d'y faire face ;

• comprendre les mécanismes des cyber-attaquants, leurs motivations et modi operandi (identification de la cible, préparation de l'attaque, etc.) ;

• connaître les ressources et bases de données utiles à l'analyse des menaces : whois, certificats, bases de données de malwares, CERT, CVE, etc ;

• être capable de mesurer les enjeux et les menaces selon le cadre professionnel, de savoir envisager les impacts des différents incidents potentiels et de mettre en œuvre des stratégies de minimisation des vulnérabilités et des risques cyber.

Programme

Contenu

1) panoramas des enjeux et menaces liés à la cybersécurité dans le monde professionnel (intrusion ciblée, APT, malware, ransomware, …) ; description de la chaîne cybercriminelle et de l'évolution du paysage des cyber-menaces.
2) bases d'architecture technique, matériel et logicielle ; présentation des concepts et des pratiques nécessaires à la mise en œuvre de moyens de lutte contre les incidents de sécurité numérique et de cybersécurité.
3) analyse les mécanismes des cyber-attaquants ; présentation des ressources utiles disponibles.
4) prévention des incidents : aspects techniques, opérationnels et stratégiques du renseignement des cyber-menaces ; mise en place d'une réponse efficace et précise en cas d'attaque(s).

Modalités de validation

- Contrôle continu
- Projet(s)
- Mémoire

Description des modalités de validation

Mémoire sur projet