Les fondamentaux de la cybersécurité dans le secteur de la santé

ORGANISATION :
Mixte

DATES ET HORAIRES :

DUREE :

LIEU

FORMATEUR
0

OBJECTIFS PÉDAGOGIQUES

- Expliquer l'état actuel de la cybersécurité en santé en France
- Concevoir les principaux mécanismes de cyberattaque et leurs impacts
- Identifier les risques d'atteinte à la sécurité des systèmes d'information et les bons usages associés (bonnes pratiques de sécurité)
- S'informer sur la réglementation liée à la sécurité des systèmes d'information et à la protection des données à caractère personnel

PRÉ-REQUIS

Cette formation ne nécessite aucun prérequis.

PROGRAMME DE LA FORMATION

PARTIE 1 : Panorama du contexte de la Cybersécurité et des menaces actuelles

- Tour d'horizon de la situation et événements marquants sur la Cybersécurité : activité sectorielle, chiffres, types de menaces
- Focus sur le secteur de la santé et la situation du secteur au regard des menaces actuelles

PARTIE 2 : Comprendre l'écosystème cyber et ses différentes organisations

- Principales définitions et vocabulaire de la cyber sécurité
- Organismes mondiaux et étatiques de cyber sécurité : Rôles, périmètre, etc...
- Les groupes d'attaquants

PARTIE 3 : Identification et compréhension des principales menaces

- Les menaces sur le secteur de la santé et les principaux vecteurs d'attaques.
- Détails et mode opératoire des principaux scénarios d'attaques : Phishing, Ransomware, Fraude au président, DDOS, Virus, faux virement, Vol et usurpation d'identité

PARTIE 4 : Détection et lutte contre les menaces

- S'organiser pour lutter
- Principaux dispositifs de détection et de lutte contre la menace

PARTIE 5 : La gestion de l'incident de sécurité et les dispositifs de réponses aux attaques

- L'incident de sécurité : Définition, Détection, analyse, qualification, et traçabilité
- Les premiers réflexes en cas d'attaque cyber
- Dispositif d'escalade et gestion de la crise cyber
- Les assistances externes : PRIS, CERT, CISRT, Assurances cyber...
- Dispositif de sauvegarde
- Plan de continuité d'activité & Plan de reprise d'activité

PARTIE 6 : Retour d'expérience et plan d'actions cyber

- Construire son retour d'expérience et communiquer auprès des différentes instances décisionnelles
- Élaboration d'un plan d'action consécutif à une attaque cyber

PARTIE 7 : Les bonnes pratiques en matière de Cyber sécurité

- Identifier
- Protéger
- Détecter
- Répondre
- Restaurer

MÉTHODE PÉDAGOGIQUE

WELIOM propose cette formation sous la modalité synchrone :

- En présentiel (dans les locaux du client ou une salle de formation à l'extérieur de ses bureaux)
- En distanciel (classe virtuelle)
- En Blended-Learning/formation mixte : du présentiel et du distanciel peuvent être envisagé sur demande.

MOYENS ET SUPPORTS PÉDAGOGIQUE

WELIOM utilise les enseignements de la pédagogie active pour construire ses formations, avec une juste répartition de la théorie et de la pratique.

Nos formations sont constituées des éléments suivants :

- Un apport de connaissances sur l'ensemble des sujets abordés
- Des mises en situation et des cas concrets
- Des exercices pratiques et des quiz pour animer et favoriser l'engagement du stagiaire

Les supports pédagogiques correspondants sont donc fournis :

- Le support de cours fourni au format numérique
- Les exercices et descriptions des cas concrets
- Des quiz et réponses attendues

Des ressources documentaires peuvent également être mises à disposition des apprenants par le formateur.

MODALITES D'ÉVALUATION

En amont de la formation

- Une qualification du besoin est faite, par entretien avec le donneur d'ordre. Un questionnaire est également envoyé aux stagiaires avec leur convocation pour comprendre leurs enjeux et leurs attentes, prendre en compte la spécificité de leur activité mais également le niveau de maturité de leur organisation et des compétences du stagiaire sur les sujets abordés.

Au début de la formation

- Un test de positionnement identifie le niveau des apprenants sur le sujet de la formation et recueille leurs attentes.

Tout au long de la formation

- Évaluation continue des acquis avec des questions orales, des quiz, des exercices, des cas pratiques et des mises en situation.

A la fin de la formation

- Évaluation pour mesurer l'acquisition des compétences.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application dans la vie professionnelle, ou les impacts sur le projet professionnel en cas de recherche d'emploi.