TOSA CYBER

GESTIC FORMATION
Formation Professionnelle • Logiciel • Solution Informatique

Pré-requis

> Savoir utiliser un ordinateur (basique).
> Posséder des notions sur la sécurité informatique.
> Savoir naviguer sur Internet (basique).

Objectifs

> Reconnaître les acteurs de la cybersécurité et leurs rôles, les types d'attaquants et leurs cibles, les entités à contacter au besoin.
> Maîtriser les principaux types d'attaques (vecteurs, cibles, impacts potentiels), ainsi que les connaissances et compétences liées à l'identité numérique et à l'authentification.
> Savoir sécuriser ses données et ses appareils sur le lieu de travail en identifiant l'exposition des données sur un poste de travail et en les limitant, en manipulant les appareils amovibles et le stockage externe, en reconnaissant les principales techniques d'attaque par ingénierie sociale pour protéger les données et les personnes du facteur humain.
> Être capable de mettre à jour des logiciels et de télécharger à partir de sources fiables.
> Être capable de voyager et de travailler dans un environnement externe en toute sécurité.
> Être capable de sécuriser physiquement l'accès aux terminaux, et d'utiliser les bons outils et techniques pour utiliser en toute sécurité un réseau sans fil.
> Être capable de limiter les données exposées lors d'un déplacement externe.
> Être capable de reconnaître une tentative d'hameçonnage et de prendre les mesures adéquates, d'utiliser le stockage en nuage et les sauvegardes, et de manipuler en toute sécurité les fichiers externes.
> Être conscient des risques liés à l'exposition de ses données personnelles.
> Être capable de protéger sa vie privée.
> Valider le TOSA Cyber et obtenir une attestation de passage ou un diplôme, en fonction du score obtenu. Score sur une échelle de 1 à 1000. Délivrance de la certification si le score est supérieur à 550.

Modalités d'évaluation

Test adaptatif

> Le niveau des questions s'adapte au niveau du candidat tout au long du déroulement du test.
> 35 questions : **60 minutes**
> Des questionnaires au fil de l'eau sous format numérique seront effectués sur les thématiques abordées.

Public

> Salarié, non salarié, gérant, gérant non salarié, artisan, demandeur d'emploi.

Compétences

> Utilisation de l'outil informatique (ordinateur, tablette, smartphone).
> Sensibilité aux nouvelles technologies numériques.
> Appétence à l'environnement numérique.
> Être à l'écoute des progrès technologiques.

Qualités - Aptitudes

> Veille.
> Assiduité.
> Vigilance.
> Autonomie.
> Écoute.
> Pertinence.

Délai d'accès

> Selon le calendrier en cours - Merci de prendre contact avec notre service.

Durée

> 4 jours soit 28 heures.

Tarif

> 850€HT/jour soit 1020€TTC/jour en intra-entreprise - Nous consulter.

Lieu

> En nos locaux à Biard. Possibilités en vos locaux sous conditions - Nous contacter.

Méthodes mobilisées

> 100% face à face pédagogique.
> Notre pédagogie est basée sur des présentations et des cas concrets seront explicités, analysés pour une meilleure compréhension des risques et permettront de formater une mise en place des parades.

« Selon le rythme de pratique, il faut de 1 à 3 mois pour acquérir solidement le contenu d'un déroulé pédagogique »

Créé le 10/2022
Mise à jour 01/2024

> Des démonstrations techniques pourront être réalisées.
> Chaque stagiaire travail sur un PC.
> Support de cours inclus.
> Intra-Entreprise ou Inter-Entreprises.
> Présentiel ou distanciel (visio) - Nous contacter.

Contenu

Audit de positionnement - questionnaire numérique au fil de l'eau

Module 1 : Le monde de la Cybersécurité

> Pouvoir distinguer et nommer les différents acteurs institutionnels ou individuels de la cybersécurité afin d'identifier l'interlocuteur adapté.
> Reconnaître les risques et objectifs d'attaquants potentiels dans le but de classifier les différentes zones de risque.
> Connaître et appliquer les réflexes à avoir en cas d'attaque avérée ou soupçonnée.
> Caractériser un mot de passe fort et maîtriser les outils adaptés afin de se garantir la sécurité de son authentification.

Module 2 : La sécurité au bureau

> Repérer les possibles expositions d'informations afin de limiter au maximum les vecteurs d'attaque possible sur son poste de travail.
> Reconnaître les principales méthodes de manipulation utilisées par les attaquants afin de protéger les données et personnes du facteur humain.
> Connaître les risques liés aux périphériques amovibles personnels ou externes pour manipuler leurs données de façon sécurisée.
> Comprendre l'intérêt de sécurité des mises à jour logicielles et savoir les appliquer, afin de maintenir un espace de travail actualisé.

Module 3 : La sécurité en déplacement

> Reconnaître les compromissions possibles des terminaux physiques, afin de les sécuriser efficacement en déplacement.
> Connaître et appliquer les bonnes pratiques de sécurité liées aux téléphones portables.
> Nommer les risques des réseaux sans fil, pour appliquer les outils et réflexes de sécurité de connexion à des réseaux externes.
> Distinguer les potentielles sources de fuite de données lors d'un déplacement externe, afin de limiter la diffusion d'informations sensibles.

Module 4 : La sécurité à la maison

> Savoir reconnaître rapidement une tentative d'hameçonnage afin d'appliquer la mesure adaptée à son traitement.
> Connaître les applications et utilités des outils de GED et services cloud afin de garantir la continuité des activités.
> Comprendre les dangers des fichiers externes dans le but de les manipuler de façon sécurisée.
> Distinguer la frontière de son espace numérique personnel, afin de maintenir sa vie privée protégée en travaillant dans un univers numérique.

Audit de positionnement - questionnaire numérique au fil de l'eau.

Votre contact

> **Marina Laurent** • Assistante Administrative et Commerciale : **m.laurent@gestic-formation.com 05 49 52 55 04**

Accessibilité

> Nos locaux sont accessibles au public en situation de handicap.
> Centre Handi-Accueillant.
> **Amélie Bertin** • Référente Handicap : **a.bertin@gestic-formation.com**.

« Selon le rythme de pratique, il faut de 1 à 3 mois pour acquérir solidement le contenu d'un déroulé pédagogique »