Comprendre la cybersécurité - Devenir acteur de sa sécurité et de celle de son entreprise

Durée : **3** jours **Prix :** 2 875 € HT

Contexte

Le numérique est une révolution. Il transforme notre société. Nous sommes de plus en plus connectés, nous sommes de plus en plus adeptes de ces nouveaux usages numériques.

Cependant, la face obscure de ces usages, c'est la multiplication des menaces et risques d'attaques qui peuvent se produire avec de nombreux types d'agresseurs potentiels : les États, les criminels isolés, les bandes organisées, les terroristes ... On ne les compte plus malheureusement.

L'espionnage industriel n'a jamais été aussi facile et à la portée de tout un chacun, des organisations et des personnes physiques sont victimes de chantage au quotidien, la prise en otage des données est plus facile et plus rentable que la prise d'otages humains, des documents confidentiels des États et des organisations sont publiés sur les réseaux sociaux, les chefs d'entreprise et Hauts Responsables font l'objet des intimidations. La vie privée des personnes n'est pas épargnée car il est aujourd'hui facile d'allumer la caméra de l'ordinateur, de la tablette, ou du smartphone d'une cible à son insu et violer ainsi sa vie privée. Il y a des exemples très récents où des grandes chaînes de télévision ont été piratées pour diffuser des messages de propagande. Aucune activité n'est épargnée. Certains grands Ports ont été obligés de suspendre leurs activités pendant des heures car la chaîne logistique avait été piratée.

Il est donc indispensable, face à aux différents types de menaces, d'être acteur de sa propre sécurité et de celle des autres, de comprendre ces menaces, de comprendre le numérique de manière à mieux s'en protéger.

Une culture de défense doit désormais être un levier de protection dans les organisations. C'est l'essence même de cette proposition. Prendre le risque de ne rien faire est la pire des stratégies dans un monde en pleine mutation.

Objectifs

- Instaurer une culture de sécurité et un changement de comportement durable.
- Découvrir et assimiler la sécurité informatique.
- Appréhender et comprendre les attaques informatiques.
- Identifier les menaces informatiques.
- Adopter les bonnes pratiques pour se protéger.

Public visé

Tout public.

Prérequis

Aucun.

Modalités pratiques

Méthodologie pédagogique

Exposé, échanges d'expérience, études de cas.

Méthodologie d'évaluation

Le stagiaire reçoit en amont de la formation un questionnaire permettant de mesurer les compétences, profil et attentes du stagiaire. Tout au long de la formation, les stagiaires sont évalués au moyen de différentes méthodes (quizz, ateliers, exercices et/ou de travaux pratiques, etc.) permettant de vérifier l'atteinte des objectifs. Un questionnaire d'évaluation à chaud est soumis à chaque stagiaire en fin de formation pour s'assurer de l'adéquation des acquis de la formation avec les attentes du stagiaire. Une attestation de réalisation de la formation est remise au stagiaire.

Programme

Module 1 : Les fondamentaux de la cybersécurité

- Comment fonctionne Internet ?
- Un monde numérique hyperconnecté
- Une diversité d'équipements et de technologies
- Le cyberespace, nouvel espace de vie
- Un espace de non-droits ?
- Évaluation des acquis

Module 2 : Un monde à hauts risques

- Qui me menace et comment ?
- Les attaques de masse
- Les attaques ciblées
- Les différents types de menaces
- Les sources de motivation des attaquants
- Les conséquences pour les victimes de cyberattaques
- Évaluation des acquis

Module 3 : Les acteurs de la cybersécurité

- Les acteurs nationaux
- Les acteurs internationaux
- Les sociétés de services et d'édition de logiciels de sécurité
- Les acteurs internes à l'organisation
- Évaluation des acquis

Module 4 : Protéger le cyberespace

- Choisir ses mots de passe
- Mettre à jour régulièrement ses logiciels
- Bien connaître ses utilisateurs et ses prestataires
- Effectuer des sauvegardes régulières
- Sécuriser l'accès WI-FI
- Être prudent avec son smartphone ou sa tablette
- Protéger ses données lors de ses déplacements

- Être prudent lors de l'utilisation de sa messagerie
- Télécharger ses programmes sur les sites officiels des éditeurs
- Être vigilant lors d'un paiement sur Internet
- Séparer les usages personnels et professionnels
- Prendre soin de son identité numérique
- Évaluation des acquis

Module 5 : les règles d'or de la sécurité

- Généralités
- Les données
- Risques sur les données
- Protéger les données
- Responsabilités face aux risques
- Évaluation des acquis

Module 6 : Anonymat et recherche d'information dans le Darknet

- Présentation du Darknet
- Pourquoi accéder au Darknet
- Comment accéder au Darknet

Module 7 : Ingénierie sociale

- Comprendre les principes de l'ingénierie sociale
- Les objectifs de l'ingénierie sociale
- Les techniques de l'ingénierie sociale
- Les moyens de se protéger de l'ingénierie sociale