

Formation « Essentiels techniques de la cybersécurité »

Réf : ESSCYBER

Bien que la cybersécurité, ou sécurité des systèmes d'information (SSI), soit aujourd'hui une nécessité absolue, elle apparaît pour beaucoup comme un domaine obscur réservé aux spécialistes. Or la cybersécurité est l'affaire de tous, et il est important que chaque acteur soit capable de comprendre et d'appliquer, chacun à son niveau, les bonnes pratiques de sécurité.

Cette formation a pour but d'expliquer aux stagiaires pourquoi la SSI est indispensable en dressant un état des lieux des menaces et des attaques les plus courantes, puis pour chaque domaine (réseau, système, applications), de présenter les mesures et les bonnes pratiques permettant de se prémunir contre ces attaques.

Objectifs

- Acquérir le vocabulaire de la SSI.
- Comprendre le fonctionnement global d'un système d'information
- Connaître le contexte actuel de la cybersécurité (sources de menaces, attaques courantes...)
- Comprendre les mesures de sécurité et les bonnes pratiques permettant de contrer ces attaques

Durée & horaires

- 2 jours soit 14 heures
- De 09h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Toute personne souhaitant s'initier à la cybersécurité
- Responsable de la sécurité (RSSI) de formation non technique
- Chef de projet ou acteur d'un projet sécurité

Cette formation est accessible à un public plus large que la formation SECUCYBER en permettant aux personnes au profil non informaticien ou non technique d'obtenir une vision opérationnelle de la cybersécurité

Pré-requis

- Cette formation ne nécessite pas de prérequis particuliers, elle est accessible à un large public.

Méthode pédagogique

- Cours magistral avec de nombreux exemples pratiques

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- Cette formation n'est pas certifiante.

Programme

Sécurité : concepts fondamentaux

- Concepts de base
- Gestion du risque : vulnérabilité, menace, impacts métiers
- Dans la peau d'un attaquant
- Principes de base : connaître son SI, moindre privilège, défense en profondeur, prévention et détection

Cryptographie

- Chiffrement
- Hachage
- Signature
- TLS
- PKI/IGC

Sécurité des réseaux

- Principes de base
- Attaques
- Contrôle d'accès
- Filtrage et relaying
- Architecture sécurisée
- WiFi

Sécurité des applications

- Vulnérabilités web : le TOP 10 de l'OWASP
- Vulnérabilités mémoire
- Attaques et défenses

- Processus de développement

Intelligence Artificielle

- Principes de base de l'IA
- Attaques et mesures

Sécurité des systèmes

- Contrôle d'accès
- Minimisation et durcissement
- Veille sécurité
- Mise à jour
- Sauvegarde
- Journalisation
- Protection du poste de travail
- Equipements mobiles