

NUMÉRIQUE

CYB-163

Cybersécurité : les fondamentaux techniques

Les fondamentaux techniques de la cybersécurité : menaces, vulnérabilités, sécurité des postes, des réseaux, des comptes et des sauvegardes, et premiers réflexes de réponse à incident.



DURÉE

11 heures



FORMAT

Visio



TARIF

Sur devis



FINANCEMENT

Étude OPCO



NIVEAU

Selon prérequis



Validation et reconnaissance

Attestation de fin de formation et certificat de réalisation. Cette formation ne prépare pas à une certification enregistrée au RNCP ou au répertoire spécifique.



Une formation adaptée à vos besoins

Questionnaire avant la session avec un court exercice technique : fonction, environnement (systèmes, réseau, cloud), outils, niveau. Les travaux pratiques sont adaptés au contexte des participants.



Délai d'accès

Sous 15 jours selon les disponibilités, après analyse du besoin.



Accessibilité

Les besoins d'aménagement sont étudiés avant la session avec notre référent handicap.



Ce que vous saurez faire à l'issue de la formation



Objectif 01

Décrire les principales menaces et leurs modes opératoires.



Objectif 02

Appliquer les mesures d'hygiène informatique aux comptes et aux postes.



Objectif 03

Vérifier les protections de base d'un réseau de petite entreprise.



Objectif 04

Mettre en place une stratégie de sauvegarde et tester une restauration.



Objectif 05

Appliquer les premiers réflexes de réponse à incident.



Public visé et prérequis



Pour qui

Techniciens et administrateurs débutants.
Référénts informatiques de PME. Profils en reconversion vers la cybersécurité.



Prérequis

Utiliser couramment Windows et un navigateur.



Déroulement de la formation

Dates, horaires, lieu ou accès à distance sont confirmés dans la convocation. Le livret d'accueil, le règlement et les contacts utiles sont transmis avant la session.

Programme détaillé

01	02	03	04	05	06	07	08	09	10	11	12
----	----	----	----	----	----	----	----	----	----	----	----

11 heures · 12 séquences · programme adapté après positionnement



Menaces et comptes - Menaces et acteurs



Menaces et comptes - Hameçonnage et ingénierie sociale



Menaces et comptes - Mots de passe et authentification forte



Menaces et comptes - Guide d'hygiène informatique de l'ANSSI



Postes et réseau - Mises à jour et protection des postes



Postes et réseau - Droits administrateurs



Postes et réseau - Pare-feu et Wi-Fi



Postes et réseau - Inventaire

**Sauvegardes et incidents - Stratégie de sauvegarde et isolement****Sauvegardes et incidents - Tests de restauration****Sauvegardes et incidents - Premiers réflexes et alerte****Sauvegardes et incidents - Ressources d'assistance publiques****Méthodes pédagogiques et évaluation****Méthodes pédagogiques**

Apports techniques et démonstrations. Travaux pratiques en laboratoire isolé, jamais sur des systèmes de production. Études de cas d'incidents réels anonymisés. Supports et fiches réflexes remis à chaque participant.

**Évaluation des acquis**

Pendant : exercices et configurations vérifiés. En fin de formation : cas noté et quiz. Questionnaire de satisfaction à chaud.

**Moyens et supports pédagogiques**

Un ordinateur par participant avec droits d'administration ou machine virtuelle. Laboratoire virtuel isolé fourni pour les travaux pratiques. En classe virtuelle : connexion stable, webcam et micro.

**Financement**

Financement possible par l'entreprise ou son OPCO selon les règles applicables et après accord écrit. Aucune prise en charge n'est garantie avant cet accord.

NOVA ACADEMY - société par actions simplifiée (SAS) - SIRET 993 541 879 00017. Déclaration d'activité n° 76 34 14584 34. Cet enregistrement ne vaut pas agrément de l'État. Certification CERT_S0626_0811 délivrée par CEVA Solution, pour les actions de formation. Contact : formation@capsulecom-nova.fr.