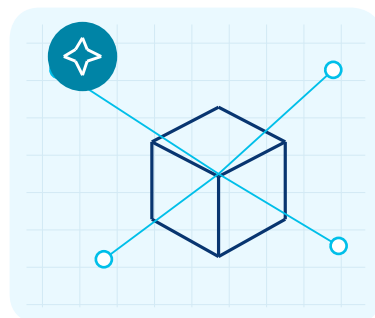


NUMÉRIQUE

CYB-161

Sécurité des réseaux avancée

Concevoir et défendre un réseau : segmentation, filtrage, accès distants, réseaux sans fil, détection d'intrusion, durcissement des équipements et supervision.



DURÉE

14 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

Concevoir une segmentation du réseau en zones de confiance.



Objectif 02

Rédiger et auditer des règles de filtrage.



Objectif 03

Sécuriser les accès distants et les réseaux sans fil.



Objectif 04

Mettre en place une détection d'intrusion et une analyse des flux.



Objectif 05

Durcir les équipements et sécuriser leur administration.



Public visé et prérequis



Pour qui

Administrateurs systèmes et réseaux.
Responsables et analystes de la sécurité.
Développeurs et ingénieurs.



Prérequis

Administrer des réseaux et des systèmes.



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	13	14	15	16
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

14 heures · 16 séquences · programme adapté après positionnement



1 Architecture et segmentation - Zones de confiance



2 Architecture et segmentation - VLAN et filtrage



3 Architecture et segmentation - Pare-feu et règles



4 Architecture et segmentation - Recommandations de l'ANSSI



5 Accès distants et sans-fil - VPN



6 Accès distants et sans-fil - Accès zéro confiance principes



7 Accès distants et sans-fil - Wi-Fi d'entreprise



8 Accès distants et sans-fil - Postes nomades



Détection - Sondes de détection



Détection - Analyse de flux



Détection - Corrélation avec les journaux



Détection - Réponse



Durcissement et administration - Durcissement des équipements



Durcissement et administration - Réseau d'administration



Durcissement et administration - Mises à jour



Durcissement et administration - Audit de configuration

✓ 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 : architectures et configurations vérifiées. 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 avec équipements réseau virtuels. 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.