

NUMÉRIQUE

CYB-157

Cryptographie appliquée

Comprendre et utiliser correctement la cryptographie : chiffrement symétrique et asymétrique, hachage, signatures, certificats, TLS, gestion des clés et erreurs d'implémentation à éviter.



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

Expliquer les principes du chiffrement symétrique, asymétrique et du hachage et choisir des algorithmes recommandés.



Objectif 02

Utiliser signatures et codes d'authentification pour garantir intégrité et authenticité.



Objectif 03

Gérer le cycle de vie de certificats dans une infrastructure de clés publiques.



Objectif 04

Configurer TLS selon les recommandations en vigueur.



Objectif 05

Organiser la gestion des clés et repérer les erreurs d'implémentation courantes.



Public visé et prérequis



Pour qui

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



Prérequis

Développer ou administrer 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
----	----	----	----	----	----	----	----	----	----	----	----

11 heures · 12 séquences · programme adapté après positionnement



Principes et algorithmes - Chiffrement symétrique et modes



Principes et algorithmes - Chiffrement asymétrique



Principes et algorithmes - Hachage, MAC, signatures



Principes et algorithmes - Recommandations de l'ANSSI



Certificats et TLS - PKI et autorités



Certificats et TLS - Cycle de vie des certificats



Certificats et TLS - TLS
versions, suites, configuration



Certificats et TLS - Tests de configuration

**Clés et implémentation - Génération et stockage des clés****Clés et implémentation - Modules matériels et coffres**
principes**Clés et implémentation - Erreurs courantes d'implémentation****Clés et implémentation - Cryptographie post-quantique**
état et calendrier à vérifier**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 configuration vérifiés. En fin de formation : revue notée 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 outils cryptographiques. 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.