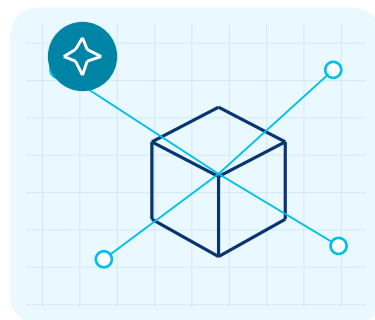


NUMÉRIQUE

CYB-162

Investigation numérique (forensic)

Mener une investigation numérique après un incident : préservation des preuves, acquisition, analyse de disques, de mémoire et de journaux, chronologie et rapport exploitable.



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

Appliquer les règles de préservation des preuves et de chaîne de conservation.



Objectif 02

Réaliser des acquisitions de disques, de mémoire et de journaux.



Objectif 03

Analyser les artefacts d'un système compromis.



Objectif 04

Analyser une capture mémoire.



Objectif 05

Établir une chronologie et rédiger un rapport d'investigation.



Public visé et prérequis



Pour qui

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



Prérequis

Administrer Windows et Linux et connaître la réponse à incident.



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



Préserver et acquérir - Réponse à incident et investigation



Préserver et acquérir - Ordre de volatilité



Préserver et acquérir - Acquisition et intégrité



Préserver et acquérir - Cadre juridique des preuves
repères



Analyser les systèmes - Systèmes de fichiers



Analyser les systèmes - Artefacts Windows et Linux



Analyser les systèmes - Journaux



Analyser les systèmes - Persistance



9

Analyser la mémoire - Capture mémoire



10

Analyser la mémoire - Processus, connexions, injections



11

Analyser la mémoire - Outils d'analyse



12

Analyser la mémoire - Corrélation



13

Chronologie et rapport - Chronologie consolidée



14

Chronologie et rapport - Hypothèses et preuves



15

Chronologie et rapport - Rapport



16

Chronologie et rapport - Retour d'expérience

✓ 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 : acquisition et constats vérifiés. En fin de formation : rapport 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 images disques et mémoire de test. 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.