

NUMÉRIQUE

CYB-152

Analyste SOC et recherche de menaces

Surveiller, détecter et répondre : collecte des journaux, règles de détection, triage des alertes, investigation, recherche proactive de menaces et escalade, dans un centre opérationnel de sécurité.



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

Identifier les sources de journaux utiles et les intégrer dans un outil de supervision.



Objectif 02

Écrire et ajuster des règles de détection.



Objectif 03

Trier et qualifier des alertes selon leur gravité.



Objectif 04

Mener une investigation et établir la chronologie d'un incident.



Objectif 05

Conduire une chasse aux menaces fondée sur une hypothèse et escalader de façon structurée.



Public visé et prérequis



Pour qui

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



Prérequis

Administrer des systèmes et réseaux, connaître TCP/IP.



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



Supervision et journaux - Rôle et organisation d'un SOC



Supervision et journaux - Sources de journaux



Supervision et journaux - Normalisation et corrélation



Supervision et journaux - Référentiels de techniques d'attaque



Détection et triage - Règles de détection



Détection et triage - Faux positifs et ajustement



Détection et triage - Triage et qualification



Détection et triage - Playbooks



Investigation - Chronologie



Investigation - Analyse de postes et de flux



Investigation - Indicateurs de compromission



Investigation - Périmètre de l'incident



Chasse aux menaces et escalade - Hypothèses de chasse



Chasse aux menaces et escalade - Requêtes de recherche



Chasse aux menaces et escalade - Escalade et communication



Chasse aux menaces et escalade - 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 : sources vérifiées, triage et chronologie évalués. 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 outils de supervision (SIEM). 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.