

L'essentiel

Code(s) NSF	326
Formacode(s)	31006
Type d'enregistrement	Enregistrement sur demande
Date d'échéance	31/12/2021

Certificateur(s)

M2I · SIRET : 33354415300344

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
M2I TECH	79504509500010	Former et organiser l'évaluation
SCRIBTEL FORMATION	39336786700024	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le certificat « Sécurité inforensic » permet aux apprenants d'acquérir les compétences pour identifier et évaluer l'ensemble des méthodes de rétropection faisant suite à une menace de sécurité, afin de préconiser les mesures d'urgence pour en limiter la propagation. Il pourra ainsi collecter et analyser l'information se trouvant dans un programme informatique pour retrouver les traces des activités d'utilisateurs et prouver un délit numérique. Le candidat sera capable de :

- Appliquer les bonnes pratiques.
- Evaluer des actions de maîtrise des risques.
- Maîtriser les outils d'analyse et de traitement des fichiers infectés.
- Mettre en place les principes généraux de prévention.

COMPÉTENCES ATTESTÉES

Appliquer les normes et standards de sécurité.

Identifier les menaces de sécurité.

Assurer la sécurité des systèmes et des équipements.

Analyser les données numériques.

Mettre en oeuvre les contre-mesures efficaces.

Optimiser le dispositif de protection informatique.

Etre autonome dans l'exécution des tâches.

Assurer la veille technique.

Activité 1 : Application d'une démarche de sécurisation suivant une méthodologie

- Identifier les aspects éthiques, économiques

et

juridiques de la sécurité.

- Posséder une vision exhaustive et synthétique de la sécurité.
- Identifier les risques de sécurité.
- Diagnostiquer les composantes de la sécurité.

- Mobiliser les moyens organisationnels, financiers, juridiques et humains dans la sécurisation du Système d'Information
 - Appliquer les normes et standards de sécurité.
- Activité 2 : Sécurisation d'un système d'information
- Déployer de manière efficace les dispositifs de sécurité.
 - Contrôler les accès locaux et distants, filaires et non filaires
 - Administrer la sécurité dans des systèmes d'exploitation différents.
 - Distribuer un code sécurisé dans une application informatique distribuée.
 - Mettre en place une veille sur la sécurité informatique.

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

- Ce Certificat est ouvert aux candidats justifiant d'un diplôme de niveau bac+3 dans le domaine de l'informatique ou d'une expérience professionnelle d'au moins deux ans dans un domaine compatible. La maîtrise des commandes Linux est indispensable.
- Les candidats sont sélectionnés après un entretien et tests de positionnement.

Base légale

Date d'échéance de l'enregistrement 31/12/2021

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RS6093

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/2679/>

Demande CPF — formations engagées

Dossiers CPF engagés	37
Montant total engagé	115 571 €
Coût moyen par dossier	3 124 €
Durée moyenne	523 h
Période	04/2020 – 11/2021
France compétences	77 %
France Travail	13 %
Reste à charge titulaire	7 %
État	3 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.