

Sécurité Inforensic

CATEGORIE : C

Vue d'ensemble

Domaine(s) d'activité professionnel dans lequel(s) est utilisé la certification :

Transverse : ■ **Public et privé / tous les domaines d'activités**

Code(s) NAF : **62.02A**

Code(s) NSF : **326**

Code(s) ROME : **M1805**

Formacode : **31006**

Date de création de la certification : **20/06/2016**

Mots clés : **Test d'intrusion**, **inforensique**,
analyse inforensic, **Cyber sécurité**

Identification

Identifiant : **2679**

Version du : **08/04/2017**

Références

Consensus, reconnaissance ou recommandation :

Formalisé :

- [Segments qui tirent la croissance en 2020](#)
- [Les spécialistes de la cyber sécurité](#)

Non formalisé :

- **L'évolution de l'utilisation d'internet, oblige beaucoup d'organisations à mettre en place un système d'information très développé pour être viable. Ces systèmes d'information, et donc internet, peuvent contenir des informations très critiques pour le déroulement des activités organisationnelles. L'entreprise, les organisations, doivent se protéger contre les fichiers pollués, contre les intrusions et les accès non autorisés. Dans cette perspective, se munir d'un système de sécurité informatique est devenu une composante essentielle de l'infrastructure des entreprises (et des organisations). La sécurité des entreprises face aux «**

cyber-menaces » : En cas de compromission du système d'information, il sera nécessaire de comprendre les failles de sécurité. Les compétences de l'expert lui permettront de définir quelle vulnérabilité a été exploitée par l'outil illégal, et de proposer un correctif approprié. La formation reste dans le cadre légal.

Descriptif

Objectifs de l'habilitation/certification

Le certificat « Sécurité inforensic » permet aux apprenants d'acquérir les compétences pour identifier et évaluer l'ensemble des méthodes de rétrospéction 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.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- non

Descriptif général des compétences constituant la certification

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.

Modalités générales

Notre certification est fondée sur l'acquisition de compétences répondant aux besoins identifiés par les acteurs économiques. La durée recommandée est de 200 heures, les compétences qui conduisent à la certification sont construites de manière modulaire de façon à tenir compte des acquis des personnes. L'objectif est d'orienter le(s) candidat(s) vers une combinaison de modules, lui permettant d'obtenir, en fonction de ses acquis, la certification. La durée peut varier en fonction des résultats des tests de positionnement permettant de créer des parcours adaptés. Une formation vise la polyvalence et l'ouverture à la vision de 360° exigée par le numérique.

Toutes les compétences d'une session sont systématiquement évaluées tout au long de la formation.

Public visé par la certification

Tous publics

Les étudiants sont accueillis tous les jours par un professionnel en activité consacrant une partie de son temps à la formation.

Un formateur référent est chargé de la sélection et du suivi des candidats, il est garant du respect du programme et supervise l'équipe des formateurs. Il complète le livret d'évaluation et prépare les candidats au certificat.

Des solutions de Blended learning (présentiel +e-learning) : Afin de nous adapter de façon constante aux évolutions technologiques innovantes, nous avons mis en place des solutions qui s'ajoutent au présentiel. Une plate-forme est disponible pour les étudiants et contient les supports de cours au format numérique et les tutoriaux. Ces modules permettent d'approfondir et de renforcer les connaissances acquises en présentiel.

Parce que nous sommes en relation permanente avec des professionnels, cela nous permet d'être en veille permanente et nous adaptons notre pédagogie à la réalité professionnelle. Notre approche reproduit les situations professionnelles et favorise les connaissances transférées. La mise en application de nos formations repose sur des cas concrets d'entreprise et mises en situation, qui poussent le stagiaire, non seulement à comprendre, mais à intégrer les points importants de son apprentissage.

Liens avec le développement durable

Aucun

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

La certification « Sécurité Infoforensic » constitue une validation fiable aux demandes actuelles du marché. La certification permet l'acquisition de compétences pour détecter les fichiers infectés qui ont permis l'intrusion, les analyser, les décortiquer et apporter les correctifs nécessaires et améliorer la sécurité du SI « Système d'Information » après l'attaque. Elle témoigne d'un niveau opérationnel de l'expertise de son détenteur dans ce domaine. Le professionnel dispose alors d'un argument décisif pour l'obtention d'un emploi ou d'une mission.

Pour l'entité utilisatrice

L'ensemble des organisations est concerné par le piratage informatique ou l'incident de sécurité majeur. Les compétences de la certification permettent de fournir des solutions pour aider les entreprises à se protéger dans le cyberspace. L'examen certifiant est un outil fiable d'évaluation et de valorisation des compétences effectives des salariés. Inscrit dans un dispositif global de mise en situation d'entreprise, rendant ainsi, le candidat opérationnel et expert dans la spécialisation. Elle permet ainsi la montée en compétences des salariés et la possibilité d'une mobilité interne.

Evaluation / certification

Pré-requis

- 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.

Compétences évaluées

Centre(s) de passage/certification

- Sur nos centres Paris/Ile de France : Rue de Picpus, Rue de Chaillot ou La Defense; et nos centres-régionaux-
<http://www.m2informatique.fr>

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.

Niveaux délivrés le cas échéant (hors nomenclature des niveaux de formation de 1969)

-

La validité est Permanente

Possibilité de certification partielle : non

Matérialisation officielle de la certification :

Certificat nominatif des compétences professionnelles acquises et décrites dans le référentiel de certification délivré par M2I Formation

Plus d'informations

Statistiques

Depuis le deuxième semestre 2016, nous certifions une vingtaine de candidats. Nous avons une forte croissance du nombre d'inscrit depuis le début de l'année 2017.

Autres sources d'information

—