Certification PECB - Analyse forensique

CATEGORIE : B

Vue d'ensemble

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

Transverse : ▪ **Tous secteurs d'activité**

Code(s) NAF : **63.11Z**, **71.12B**
Code(s) NSF : **326**
Code(s) ROME : **M1806**, **M1803**, **M1802**, **M1801**
Formacode : **31006**

Date de création de la certification : **18/12/2014**
Mots clés : **Inforensique**, **Analyse inforensic**, **Cyber attaque**, **Investigation numérique**

Identification

Identifiant : **3717**
Version du : **16/10/2018**

Références

Consensus, reconnaissance ou recommandation :
Formalisé :

- **Livre blanc défense et sécurité nationale Mission confiée par le Président de la République à Jean-Marie GUEHENNO, Conseiller maître à la Cour des Comptes - 2013**

Non formalisé :

- **Agence nationale de la sécurité des systèmes d'information (ANSSI) Bonnes pratiques / 2009-2018**

Norme(s) associée(s) :

- https://www.iso.org/-obp/ui/fr/#iso:std:iso-iec:27043:ed-1:v1:fr

Descriptif

Objectifs de l'habilitation/certification

La certification garantit que le détenteur a acquis les compétences nécessaires pour réaliser des investigations numériques et analyses relatives à des attaques sur les systèmes d'information. En termes de savoir-faire elle répond aux besoins du marché national et international, qu'il s'agisse d'organisations publiques ou privées dans tous les domaines d'activité, et en particulier des entreprises de services numériques.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- Aucun

Descriptif général des compétences constituant la certification

La certification recouvre cinq compétences :

Analyser le système d'information d'une organisation publique ou privée en vue de collecter les traces d'une attaque informatique (virus, intrusion, etc.).

Public visé par la certification

Tous publics

Exploiter les traces d'une attaque informatique afin de reconstituer le parcours de l'attaquant, d'identifier les informations exfiltrées et de comprendre les vulnérabilités exploitées.
Appliquer des techniques et protocoles d'investigations numériques respectant les procédures légales, en vue de produire des preuves numériques dans le cadre d'une action en justice.
Planifier et exécuter un plan de réponse à un incident de type cyber-attaque, afin d'assurer la protection des preuves numériques.
Rédiger le rapport enregistrant les étapes d'une investigation numérique, afin de garantir que les preuves sont issues de manière irrévocable d'une information numérique.

Modalités générales

La formation conduisant à la certification est proposée en cinq journées (40 heures), en présentiel.

Cette formation est basée sur les meilleures pratiques liées à l'analyse forensique.
Les cours théoriques sont ponctués par de la mise en application. La répartition théorique et pratique est de 40-60%.
Les exercices pratiques sont panachés de travaux dirigés et guidés par l'apprenant et d'exercices en pleine autonomie, afin d'assurer une assimilation des savoir-faire requis.

Liens avec le développement durable

Aucun

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

La certification atteste de l'acquisition d'une méthodologie et de l'expertise technique nécessaires pour réaliser des investigations sur différents systèmes d'information, ainsi que sur la mobilité, en appliquant les principes, les procédures et les techniques d'investigation reconnues. Elle autorise l'intégration au réseau de formateurs et certifiés PECB, sollicités pour leurs compétences auprès de nombreux clients à l'international. Elle est reconnue internationalement par de très nombreuses entreprises employeurs des personnes certifiées, notamment les entreprises de service numérique.

Pour l'entité utilisatrice

La certification facilite la gestion des compétences et le recrutement de spécialistes en investigations forensiques et prévention des cyber attaques. Elle favorise la collaboration inter-organisationnelle en partageant un langage et des processus communs, garantissant aux parties prenantes un bon standard de qualité. Le maintien de la certification dans le temps assure la bonne transférabilité des compétences d'une entité utilisatrice à une autre.

Evaluation / certification

Pré-requis

Le candidat doit disposer de connaissances fondamentales en sécurité de l'information, ainsi que de solides compétences en systèmes d'exploitations (Microsoft, Linux).Il doit posséder les connaissances de base en techniques de hacking.

La certification est accessible aux personnes disposant d'au moins cinq années d'expérience professionnelle.

Centre(s) de passage/certification

- Adenium (Paris)
- Business & Decision (Paris)

Compétences évaluées

Evaluation de la totalité des cinq compétences constitutives de la certification :

Analyser le système d'information d'une organisation publique ou privée en vue de collecter les traces d'une attaque informatique (virus, intrusion, etc.).
Exploiter les traces d'une attaque informatique afin de reconstituer le parcours de l'attaquant, d'identifier les informations exfiltrées et de comprendre les vulnérabilités exploitées.
Appliquer des techniques et protocoles d'investigations numériques respectant les procédures légales, en vue de produire des preuves numériques dans le cadre d'une action en justice.
Planifier et exécuter un plan de réponse à un incident de type cyber-attaque, afin d'assurer la protection des preuves numériques.
Rédiger le rapport enregistrant les étapes d'une investigation numérique, afin de garantir que les preuves sont issues de manière irrévocable d'une information numérique.

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

Pas de niveaux

- Devoteam (Paris – Bruxelles – Luxembourg)
- Econocom Digital Security (Paris)
- Fidens (Paris – Lyon)
- Global Knowledge (Rueil Malmaison)
- HTS Experts (Valencienne)
- It-Gnosis (Paris)
- Orsys (Paris–Bruxelles–Luxembourg–Genève)
- Provadys (Paris)
- SCASSI (Toulouse – Paris – Madrid)
- Sekoia (Paris)
- Sodifrance (Rennes - Nantes)
- Sysdream (Paris)
- Wipro (Paris)

La validité est Temporaire

La certification est valable 3 années.
Possibilité de certification partielle : non
Matérialisation officielle de la certification :
Remise d'un certificat de compétences PECB sous accréditation IAS (ISO 17024)

Plus d'informations

Statistiques

50 certificats de compétences sont délivrés en moyenne annuelle.

Autres sources d'information

En Anglais :

https://pecb.com/en/

En Français :

https://pecb.com/fr/

https://pecb.com/fr/education-and-certification-for-individuals/iso-iec-27035