

Certification PECB - Analyse forensique

RS3717 · RS · Publiée

L'essentiel

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

Certificateur(s)

PECB GROUPE · SIRET : 83397361300015

Partenaires habilités

70 organismes habilités, d'après la liste publiée par France compétences : 70 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
2AB & ASSOCIATES	88031852200013	Former et organiser l'évaluation
AB CONSEILS	53788919800017	Former et organiser l'évaluation
ACG CYBERSECURITY	85024706500012	Former et organiser l'évaluation
ADENIUM-BRG	44195184500086	Former et organiser l'évaluation
ALMOND	43811325000064	Former et organiser l'évaluation
ASTON INSTITUT	49868549400052	Former et organiser l'évaluation
ATOS CONSULTING	41033322300098	Former et organiser l'évaluation
AVOLYS	33354415300146	Former et organiser l'évaluation
BSSI CONSEIL ET AUDIT	52935663600033	Former et organiser l'évaluation
CHAFIK MOHAMED	83145806200013	Former et organiser l'évaluation

Liste complète des 70 partenaires habilités : <https://data.aktaconseil.fr/certifications/rs3717-certification-pecb-analyse-forensique/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

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.

COMPÉTENCES ATTESTÉES

La certification recouvre cinq compétences :

1. Analyser le système d'information d'une organisation publique ou privée en vue de collecter les traces d'une attaque informatique (virus, intrusion, etc.).
2. 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.
3. 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.

4. Planifier et exécuter un plan de réponse à un incident de type cyber-attaque, afin d'assurer la protection des preuves numériques.

5. 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.

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

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

2. 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.

3. 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.

4. Planifier et exécuter un plan de réponse à un incident de type cyber-attaque, afin d'assurer la protection des preuves numériques.

5. 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.

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

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.

Base légale

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

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

En Anglais :

<https://pecb.com/en/>

En Français :

<https://pecb.com/fr/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/3717/>

Demande CPF — formations engagées

Dossiers CPF engagés	1
Montant total engagé	3 041 €
Coût moyen par dossier	3 041 €
Durée moyenne	35 h
Période	01/2020
France compétences	91 %
Reste à charge titulaire	9 %

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