

Certification PECB - Conception et mise en oeuvre des tests d'intrusion

RS3716 · RS · Publiée

L'essentiel

Code(s) NSF	326n
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/rs3716-certification-pecb-conception-et-mise-en-oeuvre-des-tests-d-intrusion/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification garantit que le détenteur a acquis les connaissances, les aptitudes et les compétences nécessaires pour réaliser des tests d'intrusion des systèmes d'information en appliquant les principes, les procédures et les techniques de Pentest (tests d'intrusion). 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 service numérique.

COMPÉTENCES ATTESTÉES

La certification recouvre cinq compétences :

1. Simuler l'attaque d'un système d'information d'entreprise par un utilisateur malintentionné ou un logiciel malveillant, afin de détecter les fragilités de celui-ci.

2. Concevoir et mettre en œuvre une série de tests d'intrusion à même de situer le degré de risque représenté par chacune des fragilités identifiées.
3. Rédiger un rapport de pentest présentant l'ensemble des vulnérabilités exploitables dans les configurations ou la programmation, en vue de la conception par les responsables d'un plan d'amélioration de la sécurité du système d'information cohérent avec l'échelle des risques.
4. Identifier et chiffrer les parades adaptées aux menaces, afin de faciliter la prise de décision et la mise au point du plan de sécurité.
5. Conseiller une entreprise sur les bonnes pratiques en matière de détection et de lutte contre le piratage, afin de faciliter la mise en place des mesures et procédures adéquates.

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

1. Simuler l'attaque d'un système d'information d'entreprise par un utilisateur malintentionné ou un logiciel malveillant, afin de détecter les fragilités de celui-ci.
2. Concevoir et mettre en œuvre une série de tests d'intrusion à même de situer le degré de risque représenté par chacune des fragilités identifiées.
3. Rédiger un rapport de pentest présentant l'ensemble des vulnérabilités exploitables dans les configurations ou la programmation, en vue de la conception par les responsables d'un plan d'amélioration de la sécurité du système d'information cohérent avec l'échelle des risques.
4. Identifier et chiffrer les parades adaptées aux menaces, afin de faciliter la prise de décision et la mise au point du plan de sécurité.
5. Conseiller une entreprise sur les bonnes pratiques en matière de détection et de lutte contre le piratage, afin de faciliter la mise en place des mesures et procédures adéquates.

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Le candidat doit avoir des connaissances fondamentales de la sécurité de l'information, il doit posséder de solides compétences sur les systèmes d'exploitations (Microsoft, Linux).

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/3716/>

Entrées et sorties de formation

Entrées en formation	1
Parcours menés à terme	1
Taux d'achèvement	100 %
Période	03/2022

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	13
Montant total engagé	43 232 €
Coût moyen par dossier	3 326 €
Durée moyenne	125 h
Période	01/2020 – 01/2022
France compétences	73 %
France Travail	14 %
Reste à charge titulaire	7 %
État	6 %

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