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

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 : **62.02B**, **62.02A**
Code(s) NSF : **326n**
Code(s) ROME : **I1401**, **M1801**, **M1805**
Formacode : **31006**

Date de création de la certification : **01/06/2018**
Mots clés : **Pentest**, **Test d'intrusion**, **Hacking**, **Cybersécurité**

Identification

Identifiant : **3716**
Version du : **16/10/2018**

Références

Consensus, reconnaissance ou recommandation :
Formalisé :
- **Analyse du marché et des acteurs de la filière industrielle française de sécurité**

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 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.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- Aucun

Descriptif général des compétences constituant la certification

La certification recouvre cinq compétences :

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.
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.

Public visé par la certification

Tous publics

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.
Identifier et chiffrer les parades adaptées aux menaces, afin de faciliter la prise de décision et la mise au point du plan de sécurité.
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.

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 en matière de protection des donées personnelles. 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 permet aux individus de :

Disposer des compétences nécessaires à la conception et à la mise en oeuvre de tests d'intrusion sur différents types de systèmes d'information.
Appartenir au réseau de formateurs et certifiés PECB sollicités pour leurs compétences auprès des clients à l'international.
Répondre aux exigences de postes correspondant à ces caractéristiques: RSSI, Consultant en sécurité des systèmes d'information.

Pour l'entité utilisatrice

La certification permet aux entités utilisatrices de :

Faciliter la gestion des compétences et le recrutement en s'appuyant sur une certification reconnue.
Favoriser la collaboration inter-organisationnelle en partageant un langage et des processus communs.
Garantir aux parties prenantes de l'organisation un certain standard de qualité.
Le maintien dans le temps de la certification garantit la transférabilité des compétences d'une entité utilisatrice à une autre.

Evaluation / certification

Pré-requis

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.

Compétences évaluées

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

Centre(s) de passage/certification

- Adenium (Paris)
- Business & Decision (Paris)
- Devoteam (Paris – Bruxelles – Luxembourg)
- Econocom Digital Security (Paris)
- Fidens (Paris – Lyon)

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.
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.
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.
Identifier et chiffrer les parades adaptées aux menaces, afin de faciliter la prise de décision et la mise au point du plan de sécurité.
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.

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

Pas de niveaux

- 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 ans.
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

25 certificats délivrés (moyenne annuelle estimée).

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