Identification du module

Numéro de module	680	
Titre	Contrôler la sécurité de l'infrastructure informatique	
Compétence	Contrôler, dans le cadre d'un mandat, la sécurité des systèmes, des réseaux et des applications d'une organisation au moyen de méthodes et d'outils appropriés, consigner et présenter les résultats des tests de façon concluante et recommander des mesures pour corriger les failles identifiées.	
Objectifs opérationnels	1	Clarifier et définir avec le mandant les objectifs, le périmètre et les conditions cadres de l'audit de sécurité de tout ou partie de l'infrastructure informatique.
	2	Sélectionner des méthodes de tests de sécurité appropriées en fonction des objectifs et du rapport coûts/utilité.
	3	Vérifier la conformité légale et contractuelle des tests de sécurité planifiés et engager, si nécessaire, des mesures correctives.
	4	Choisir, en tenant compte des objectifs et de la méthodologie de test, des techniques et des outils appropriés pour procéder aux tests et aux audits de sécurité.
	5	Exécuter les tests de sécurité et consigner la procédure et les résultats des tests de façon continue et exhaustive.
	6	Analyser et évaluer les résultats des tests et rédiger un rapport d'audit avec des mesures pour corriger les vulnérabilités.
Domaine de compétence	Security/Risk Management	
Objet	Mandat d'audit de sécurité portant sur l'infrastructure ICT d'une organisation dotée de systèmes, de réseaux et d'applications.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	680
Titre	Contrôler la sécurité de l'infrastructure informatique
Compétence	Contrôler, dans le cadre d'un mandat, la sécurité des systèmes, des réseaux et des applications d'une organisation au moyen de méthodes et d'outils appropriés, consigner et présenter les résultats des tests de façon concluante et recommander des mesures pour corriger les failles identifiées.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître des méthodologies et des standards pertinents pour procéder à des contrôles de sécurité (p.ex. OSSTMM, normes BSI pour les tests d'intrusion [BSI Leitfaden für Penetrationstests], Penetration Testing Execution Standard [PTES], méthodologie de l'OWASP pour la réalisation de tests de pénétration d'applications WEB, Technical Guide to Information Security Testing and Assessment du NIST, CIS Controls, ISO/CEI 2700x).
	1.2	Connaître l'infrastructure informatique et le paysage système du mandant et pouvoir expliquer les possibilités de limitation du périmètre d'un audit de sécurité (p.ex. complet, limité, ciblé).
	1.3	Connaître les conditions cadres organisationnelles et techniques pertinentes applicables aux audits de sécurité (p.ex. identification de tous les systèmes et collaborateurs concernés, durée d'exécution, risques relevant de la responsabilité en cas de pannes et de dommages, accès aux réseaux et à l'infrastructure).
	1.4	Connaître des aspects éthiques pertinents dans le cadre des audits de sécurité (p.ex. utilisation de techniques d'ingénierie sociale, exploitation de vulnérabilités identifiées).
2	2.1	Connaître les possibilités et les limites des scans de vulnérabilité et de l'exploitation (exploiting).
	2.2	Connaître les possibilités et les limites des tests d'intrusion et pouvoir expliquer leurs caractéristiques quant à la perspective (en mode boîte noire, boîte grise ou boîte blanche), au système cible, à la procédure (visible, invisible), à la position de l'attaquant (interne, externe) et à l'agressivité.
	2.3	Connaître les possibilités et les limites des audits et revues techniques (p.ex. audit de sécurité, audit de processus, audit de conformité) et pouvoir expliquer l'objet de l'audit en tant qu'élément de différenciation.
	2.4	Connaître les possibilités et les limites des techniques d'ingénierie sociale.
	2.5	Connaître le modèle et le but des simulations par équipe rouge (red teaming) et par équipe bleue (blue teaming) dans le contexte des tests de sécurité.
3	3.1	Connaître les aspects de droit pénal pertinents en matière de tests de sécurité (p.ex. soustraction de données, accès indu à un système informatique, détérioration de données, utilisation frauduleuse d'un ordinateur) et l'importance du consentement contractuel du mandant.

Connaissances opérationnelles nécessaires

	3.2	Connaître les dispositions légales relatives à la protection des données et au droit d'auteur (licences) dans le contexte des tests de sécurité (p.ex. traitement de données à caractère personnel, modifications non autorisées du code de programme) et pouvoir expliquer les possibilités permettant de garan-tir le respect des prescriptions en la matière.
	3.3	Connaître les risques juridiques civils pertinents dans le contexte des tests de sécurité (p.ex. pannes et endommagements de systèmes, perte et détérioration de données) et pouvoir expliquer les possibilités permettant de prévenir les dommages, les coûts consécutifs ainsi que les demandes de dommages et intérêts.
	3.4	Connaître les principaux contenus d'un contrat de service portant sur des tests de sécurité (p.ex. but, type de tests et technique utilisée, obligation de confidentialité, devoir de diligence, protection des données, demande de dommages et intérêts et exclusion de la responsabilité, notification aux personnes concernées) et pouvoir expliquer leur finalité.
4	4.1	Connaître des techniques manuelles de vérification de la sécurité (p.ex. étude de documents, enquêtes et entretiens, renseignement de sources ouvertes ou Open Source Intelligence [OSINT], piratage manuel et vérification manuelle des exploits, audit physique des contrôles d'accès).
	4.2	Connaître des outils appropriés pour procéder à un audit de sécurité assisté par ordinateur et pouvoir expliquer la finalité de leur utilisation (p.ex. test de stress, scan de vulnérabilités, exploitation, déverrouillage, sniffing, spoofing, rétro-ingénierie).
5	5.1	Connaître les principaux contenus d'un protocole de test compréhensible et traçable (p.ex. identification, timbre horodateur et calendrier, activité, motivation, outils et paramètres, résultats, pièces justificatives).
	5.2	Connaître des possibilités de sauvegarde des pièces justificatives issues des tests de sécurité (p.ex. enregistrement du trafic réseau, captures d'écran, photographies, fichiers log et fichiers journaux des outils).
6	6.1	Connaître diverses causes de vulnérabilités (p.ex. directives de sécurité lacunaires ou non appliquées, failles dans l'architecture de sécurité ou dans la configuration, failles dans la gestion des incidents ou des correctifs).
	6.2	Connaître des modèles courants d'évaluation de la criticité des vulnérabilités (p.ex. Common Vulnera-bility Scoring System [CVSS], OWASP Risk Rating Methodology, schéma de classification des vulnérabilités selon le BSI)
	6.3	Connaître les principaux contenus d'un catalogue de mesures structuré (p.ex. mesure, évaluation, priorité, compétences, évaluation des ressources et estimation des coûts, vérification).
	6.4	Connaître les principaux contenus d'un rapport d'audit (p.ex. synthèse, contexte, objet d'investigation, méthodes, résultats, constats, catalogue des mesures, recommandation avec justification).

Version du module	1.0
Créé le	11.02.2021