Identification du module

Numéro de module	685	
Titre	Assurer la gestion des vulnérabilités et des correctifs	
Compétence	Identifier et prioriser les failles des systèmes, des réseaux et des applications d'une organisation et les traiter dans le cadre de la gestion des vulnérabilités et des correctifs.	
Objectifs opérationnels	1	Surveiller en continu les développements actuels concernant les vulnérabilités dans le fonctionnement opérationnel.
	2	Vérifier de façon proactive la sécurité de l'infrastructure informatique d'une organisation quant aux vulnérabilités devenues connues.
	3	Evaluer la criticité des vulnérabilités identifiées et fixer les priorités dans leur traitement.
	4	Vérifier la disponibilité d'un correctif afin de supprimer une vulnérabilité et définir, si nécessaire, des mesures alternatives.
	5	Vérifier au moyen de tests appropriés la fonction et l'efficacité des correctifs avant la mise en production.
	6	Planifier et coordonner avec les divisions ICT la distribution des correctifs de sécurité sur l'environnement productif et garantir l'actualisation des informations de configuration.
	7	Vérifier et évaluer périodiquement la performance et l'efficacité de la gestion des vulnérabilités et des correctifs et proposer, si nécessaire, des mesures d'amélioration.
Domaine de compétence	Service Management	
Objet	Organisation dotée d'une infrastructure informatique complexe ainsi que de structures et de processus définis pour la gestion des vulnérabilités et des correctifs.	
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	685
Titre	Assurer la gestion des vulnérabilités et des correctifs
Compétence	Identifier et prioriser les failles des systèmes, des réseaux et des applications d'une organisation et les traiter dans le cadre de la gestion des vulnérabilités et des correctifs.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître des déclencheurs possibles (triggers) pour la détection des vulnérabilités dans le fonctionnement opérationnel d'une organisation (gestion des incidents de sécurité, tests de sécurité périodiques, Cyber Threat Intelligence [CTI], avis et rapports de sécurité des fabricants).
	1.2	Connaître diverses sources contenant des informations actuelles sur les vulnérabilités (p. ex. Common Vulnerabilities and Exposures [CVE], avis et rapports de sécurité de fabricants et de prestataires tiers, listes d'adresses électroniques, organisations CERT, catalogue des menaces MELANI, ENISA et BSI).
2	2.1	Connaître l'infrastructure informatique et le paysage système d'une organisation et pouvoir expliquer la pertinence des interdépendances entre les systèmes dans le contexte de la gestion des vulnérabilités et des correctifs.
	2.2	Connaître des normes et directives courantes en matière de durcissement des systèmes, des réseaux et des applications (p. ex. CIS Benchmarks, Microsoft Security Baselines, STIG de la DISA, guides de durcissement de la sécurité spécifiques à des produits) et pouvoir expliquer en quoi le durcissement des systèmes est important dans le cadre de la gestion des vulnérabilités.
	2.3	Connaître des outils appropriés pour détecter des vulnérabilités dans les systèmes, les réseaux et les applications (p. ex. OpenVAS, Nessus, Metasploit, IronWASP, outils spécifiques à des fabricants).
3	3.1	Connaître des modèles courants d'évaluation de la criticité des vulnérabilités (p. ex. Common Vulnerability Scoring System [CVSS], schéma de classification des vulnérabilités selon le BSI).
	3.2	Connaître des facteurs d'influence déterminants dans la priorisation des vulnérabilités (p. ex. inventaire et classification des valeurs [assets], exposition des systèmes menacés, répercussions possibles d'une vulnérabilité, disponibilité d'exploits).
4	4.1	Connaître divers types de releases logiciels (p. ex. mise à niveau, mise à jour, service pack, correctif, hotfix) et pouvoir expliquer leurs différences en termes de portée, de finalité, de degré de maturité, de versionnage (numéros de version) et de déploiement.
	4.2	Connaître l'importance d'une réaction en temps réel dans la gestion des correctifs et pouvoir expliquer les caractéristiques d'exploits zero-day et d'attaques zero-day ainsi que les menaces que ceux-ci représentent.

Connaissances opérationnelles nécessaires

	4.3	Connaître des mesures alternatives aux correctifs afin de réduire le potentiel de menace d'une vulnérabilité (p. ex. renoncement à un produit ou produit alternatif, déplacement d'un système menacé dans un segment de réseau avec un besoin de protection plus élevé, séparation temporaire ou déconnexion).
5	5.1	Connaître des raisons de tester des mises à jour et des correctifs avant le déploiement (p. ex. dépendances dans la suite des correctifs, temps requis et interruptions éventuelles, dépendances résultant de la configuration système, interdépendances avec d'autres systèmes, preuve de l'efficacité).
	5.2	Connaître les exigences à remplir par un environnement de test idéal (p. ex. séparation de l'environnement productif, image exacte [miroir] de l'environnement productif en ce qui concerne les conditions système, les logiciels, la configuration et les données) et pouvoir expliquer d'autres procédures en cas d'indisponibilité d'un environnement de test.
	5.3	Connaître des méthodes et des techniques pour tester des correctifs (p. ex. tests de fonctionnement manuels, contrôle des fichiers log ou fichiers journaux, tests de régression automatisés, vérification de l'efficacité au moyen de scripts d'exploits).
6	6.1	Connaître les divisions ICT et les processus d'une organisation et pouvoir indiquer leurs compétences et leurs besoins lors du déploiement des mises à jour et des correctifs (p. ex. Change Management, Release and Deployment Management, Service Asset and Configuration Management, Service Operations, Service Level Management).
	6.2	Connaître diverses stratégies de distribution des mises à jour et des correctifs (p. ex. séquentielle, parallèle, big bang) et pouvoir expliquer les facteurs déterminants dans le choix d'une stratégie.
	6.3	Connaître des aspects déterminants de la planification des mises à jour et des correctifs (p. ex. temps requis, interruptions, annonce, sauvegarde des données, scénario d'urgence et scénario de retour en arrière [fallback]).
	6.4	Connaître les possibilités et les limites des outils servant à la distribution automatisée des mises à jour et des correctifs.
	6.5	Connaître l'importance de la gestion de configuration et l'utilité d'une base de données de gestion de configuration (CMDB) et pouvoir expliquer les principaux éléments d'information d'un configuration item (CI) dans la CMDB.
7	7.1	Connaître des valeurs statistiques et des indicateurs clés de performance (CPI) pertinents dans le contexte de la gestion des vulnérabilités et des correctifs.
	7.2	Connaître des méthodes et des techniques appropriées de synthèse et de présentation des informations (p. ex. tableaux de fréquence et histogrammes, agrégation au moyen de tableaux croisés et de tableaux croisés dynamiques, diagrammes de corrélation, analyse de séries temporelles et analyse des tendances).
	7.3	Connaître les directives de l'entreprise en matière d'amélioration continue et pouvoir expliquer les besoins en informations relatifs à la gestion des vulnérabilités et des correctifs spécifiques aux parties prenantes concernées (p. ex. management, CISO, SOC, CERT, divisions ICT, fournisseurs et fabricants).

Connaissances opérationnelles nécessaires

Version du module	1.0
Créé le	11.02.2021