Référentiel de certification et d'évaluation

Surveiller un système d'information sur des critères de sécurité informatique

Mars 2024

REFERENTIEL DE COMPETENCES *Identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *Définit les critères et les modalités d'évaluation des acquis*	
	MODALITES D'EVALUATION	**CRITÈRES D'ÉVALUATION**
C1. Identifier les risques liés à un système d'information en analysant l'architecture, les actifs et les usages du système à surveiller, en appliquant une méthode standard, afin d'évaluer leur potentialité et leur impact.	**E1. Mise en situation professionnelle (C1, C2, C3, C4)** L'évaluation se fait dans un contexte de projet de sécurisation d'un système d'information, réel ou fictif, avec une politique de sécurité établie. Le candidat est partie prenante du projet de sécurisation avec un rôle d'expert technique garant de la méthodologie à suivre. L'évaluation porte sur les étapes de surveillance et de la mise en œuvre d'une veille professionnelle en cybersécurité. Livrable : - rapport professionnel individuel,	- Une méthode (ou *framework*) d'analyse de risque standard est appliquée et respectée (EBIOS, NIST), - Le système d'information (SI) cible est cartographié : composants, services, flux et usages métiers, - Les incidents redoutés sont listés, catégorisés et évalués en suivant le cadre méthodologique choisi, - À chaque incident redouté est associé un degré de risque, - Le degré de risque prend en compte

	Évaluation : - correction du rapport professionnel, - soutenance orale individuelle.	la vraisemblance d'un incident et son impact sur l'activité métier.
C2. Élaborer une stratégie de traitement des risques à partir des niveaux de risque évalués en suivant une méthode standard, afin de sélectionner des mesures appropriées pour chaque risque évalué.		- Une méthode (ou *framework*) de gestion des risques est appliquée et respectée (EBIOS, NIST, ISO 27005...), - Les traitements (ou l'absence de traitement) des risques proposés respectent le cadre de la méthode choisie, - Les risques sont réévalués suite aux traitements proposés, - Les risques résiduels sont identifiés et évalués.
C3. Intégrer une sonde à un système de gestion des événements et des informations de sécurité (SIEM*), en configurant le collecteur, les règles de filtre et la console de visualisation, dans le		- L'objectif de surveillance est rappelé, - Un environnement bac-à-sable est configuré et reproduit la partie du système d'information visée par la

respect de la réglementation en vigueur sur la gestion des données, pour enrichir ses capacités de surveillance, en accord avec la stratégie de traitement des risques.		collecte d'événements, - La solution technique est intégrée et testée dans l'environnement bac-à-sable, - Les règles de filtre sont adaptées à l'objectif de surveillance, - La console est configurée pour alerter et rendre compte des traces des incidents. - Dans le cas où la sonde collecte des données personnelles : - Un registre des traitements de données personnelles est présenté et il intègre l'ensemble des traitements de données personnelles impliqués dans le projet. - Les procédures de tri de

		données personnelles pour la mise en conformité de l'application avec le RGPD sont rédigées. - Les procédures de tri détaillent les traitements de conformité (automatisés ou non) à appliquer ainsi que leur fréquence d'exécution.
C4. Etablir un système de veille professionnel en cybersécurité, en identifiant des sources de confiance, en les agrégeant à l'aide d'un outil dédié, en analysant les informations recueillies et en les partageant avec les parties prenantes du projet de sécurisation afin d'ajuster son système de défense, en continu, aux actualités et aux mises à jour critiques.		- Un objectif de veille est fixé, - Un cadre méthodologique et opérationnel (outils, supports, espaces d'échanges...) est défini pour la veille, - Des sources d'autorités sont choisies en priorité (OpenCVE, Cert-fr, Cert-eu...), elles sont identifiées et leur fiabilité évaluée, - Les opportunités de réinvestissement

		des informations et données collectées dans le cadre d'un projet de sécurisation d'un SI sont rappelées.

Glossaire

- **SIEM (S*ecurity Information and Event Management* ou système de gestion des informations et des événements de sécurité)** : un système dédié à la surveillance des systèmes et réseaux informatiques. Un SIEM permet la collecte des données relatives aux activités informatiques sur les systèmes et réseaux sous surveillance, leur normalisation, leur agrégation, la recherche de corrélation, le reporting, l'archivage, le rejeu des événements.