

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

RS6803 · RS · Publiée

L'essentiel

Code(s) NSF	326
Formacode(s)	31006
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	01/10/2024
Date d'échéance	01/10/2027

Certificateur(s)

SIMPLON.CO · SIRET : 79279132900016

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le Global Risk Report du World Economic Forum 2023 place la cybercriminalité et la cyberinsécurité comme le 8ème risque mondial majeur à 2 et à 10 ans. De nombreux facteurs, conséquence notamment de la révolution numérique, ont fait augmenter la surface d'attaque ainsi que le volume de données potentiellement corruptibles, provoquant une augmentation sans précédent de la cybercriminalité ces dernières années.

Face à ce phénomène, une prise en compte prépondérante de ses enjeux à la fois au niveau national et international s'impose, avec un durcissement de la réglementation et une volonté renforcée de contrôle et de coopération.

L'exploitation des vulnérabilités est la porte d'entrée numéro 1 des attaquants. Ainsi, la première étape pour assurer un système de sécurité des systèmes d'information robustes est d'être en mesure d'analyser les risques afin de mettre en place des mécanismes de surveillance idoines.

La clé pour limiter les cyberattaques dommageables et atténuer les pertes est de surveiller pour détecter une attaque dès ses premiers stades.

Cette certification vise à apporter des compétences complémentaires aux techniciens, administrateurs, architectes et ingénieurs réseaux, en première ligne pour protéger les systèmes et les données dont ils assurent la maintenance et la sécurité.

COMPÉTENCES ATTESTÉES

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.

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.

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 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.

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.

Secteur d'activité et type d'emploi

RÉGLEMENTATIONS D'ACTIVITÉ

Si l'activité n'est pas réglementée en tant que telle, elle s'exerce dans le respect de standards et de réglementations applicables en matière de sécurité informatique.

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue

PRÉREQUIS À L'ENTRÉE EN FORMATION

Justifier d'une expérience professionnelle d'1 an minimum en tant que technicien ou administrateur système et réseau ou assimilé.

COMPOSITION DU JURY — FORMATION CONTINUE

Le jury est composé de deux professionnels du domaine, dont un externe à l'organisme certificateur.

Base légale

Date de décision	01/10/2024
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	01/10/2027
Date de dernière délivrance possible	01/04/2028

Liens avec d'autres certifications

ANCIENNES VERSIONS

RS5020

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/6803/>