

Analyser les incidents de sécurité informatique

RS6806 · 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.

Analyser les incidents de cybersécurité et leur niveau de criticité, ainsi que les rapporter de la façon la plus précise possible, est clé pour maintenir des systèmes d'information en fonctionnement.

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. Détecter les activités suspectes depuis la console d'un système de gestion des événements et des informations de sécurité (SIEM), en analysant les événements collectés afin de signaler les incidents de sécurité redoutés.

C2. Analyser une activité suspecte, en déterminant sa véracité et son niveau de gravité afin de déterminer la nature et le niveau de réponse à appliquer.

C3. Identifier les tactiques, les techniques et l'objectif d'une attaque, en relevant son point de départ et les indicateurs de compromission pour appuyer la stratégie de réponse à un incident de sécurité.

C4. Rédiger un rapport d'incident en respectant la politique de réponse à incident de sécurité afin de soutenir l'effort de réponse et de remédiation du système d'information.

C5. Etablir un système de veille professionnelle 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 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

RS5021

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/6806/>