

Analyser les incidents de sécurité détectés

RS5021 · RS · Publiée

L'essentiel

Code(s) NSF	326
Formacode(s)	31006
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	10/10/2019
Date d'échéance	10/10/2024

Certificateur(s)

SIMPLON.CO · SIRET : 79279132900016

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
DATASCIENTEST	83145006900024	Former et organiser l'évaluation
ORSYS	48276116000019	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

OBJECTIFS :

La certification a pour objectif de certifier que le candidat est en mesure de mobiliser ses compétences lors de :

- L'élaboration de l'analyse des événements de sécurité
- L'analyse et gestion des incidents de sécurité
- L'élaboration et mise en oeuvre d'une stratégie de veille technologique pour optimiser la gestion des risques

CONTEXTE :

Valeur ajoutée pour les individus

- La certification "Analyser les incidents de sécurité détectés" permet aux personnes formées d'acquérir et de valoriser des compétences en forte demande sur le marché de l'emploi.
- Par ailleurs, l'enjeu de la cybersécurité étant commun à l'ensemble des secteurs d'activités (ex : Électronique / Électricité, Informatique / Télécoms, Métallurgie / Travail du métal, Études et conseils, Machines et équipements / Automobile...), cette certification permet de garantir la mobilité professionnelle des personnes formées.
- Cela permet ainsi aux individus de sécuriser leur parcours professionnel et de maintenir leur employabilité.

Valeur ajoutée pour les entités utilisatrices

- Ces dernières années ont marqué un tournant dans la gestion de la cybersécurité par les entreprises. Le nombre croissant de cyberattaques et l'intensification de la réglementation liée à la protection des données les ont obligées à faire de la cybersécurité une composante à part entière de leur organisation.
- Ainsi, dans un monde de plus en plus connecté, la cybersécurité est devenue une préoccupation majeure des entreprises, tous secteurs confondus. Il apparaît aujourd'hui nécessaire pour les organisations de former et/ou recruter des collaborateurs capables de piloter la gestion des incidents de sécurité détectés sur un système d'information.

COMPÉTENCES ATTESTÉES

Les compétences constituant la certification visent à exercer les activités suivantes :

- C1. Analyser les événements collectés afin de détecter des incidents de sécurité à partir des règles préalablement définies
- C2. Qualifier un incident de sécurité détecté sur la base d'une analyse des impacts sur l'organisation de manière à apporter une réponse adaptée
- C3. Identifier les tactiques et techniques d'attaques ainsi que les objectifs de l'attaquant de manière à proposer des préconisations adaptées au mode opératoire utilisé
- C4. Rédiger un rapport d'alerte sous la forme d'un compte rendu d'incident à destination du commanditaire afin de préconiser des mesures de remédiation en vue du traitement de l'incident de sécurité
- C5. Concevoir un système de veille technologique permettant de collecter, classier, analyser et diffuser l'information liés à la cybersécurité aux différents acteurs de l'organisation/du commanditaire afin d'améliorer la sécurité du SI du commanditaire.

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue, Candidature individuelle, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Justifier d'une expérience professionnelle d'un an minimum en tant que technicien systèmes et réseaux ou assimilé.

COMPOSITION DU JURY — FORMATION CONTINUE, CANDIDATURE INDIVIDUELLE, VAE

Un jury composé de 3 personnes, dont au moins un professionnel.

Base légale

Date de décision	10/10/2019
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	10/10/2024

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)

RS6806

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

www.simplon.co

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/5021/>

Entrées et sorties de formation

Entrées en formation	61
Parcours menés à terme	60
Taux d'achèvement	98 %
Période	01/2023 – 07/2025

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	70
Montant total engagé	232 412 €
Coût moyen par dossier	3 320 €
Durée moyenne	369 h
Période	11/2022 – 09/2024
France compétences	74 %
France Travail	16 %
Entreprise	8 %
Reste à charge titulaire	1 %
OPCO	1 %
Compte d'engagement citoyen	0 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.