Expert en cybersécurité (MS)

Mastère Spécialisé® Cybersécurité

Certifiante | Formation continue

Réf. : 25172946F — Mise à jour : 4 septembre 2026

Organisme responsable : **SUPELEC**

Présentation de la formation

Objectifs

Analyser des enjeux liés à la sécurité du SI en vue de gérer les risques associés en termes technique, économique et juridique en s'appuyant sur une étude du contexte.

- Identifier les biens essentiels et supports ainsi que procédures d'exploitation de l'organisation en vue de déterminer les risques afférents en recensant les biens au sein du périmètre de l'étude ainsi que leurs relations fonctionnelles.
- Évaluer la vraisemblance d'un scénario de menace en mettant en regard le potentiel des sources de menaces considérées, l'exposition à ces menaces et la facilité d'exploitation des vulnérabilités identifiées afin d'estimer la plausibilité de celui-ci et déterminer la nature de la réponse à apporter.
- Évaluer les coûts liés à la sécurité en mettant en regard les coûts d'un incident de sécurité, d'une mesure préventive et d'une remédiation en vue de déterminer la nature de la réponse à apporter.
- Restituer l'analyse de risque et des moyens de remédiation auprès d'un donneur d'ordre (autorité, chef de projet, chef DSI...) dans le domaine de la SSI en réalisant un rapport et une présentation orale adaptés aux parties prenantes concernées (dont les personnes en situations de handicap) afin de sensibiliser les parties prenantes et d'arbitrer les réponses à apporter au regard de l'analyse établie.
- Évaluer la pertinence d'une mesure technique de sécurité en mettant en regard le contexte technique, légal et organisationnel afin d'apporter une réponse adaptée au regard des risques identifiés.
- Proposer une articulation de moyens techniques et organisationnels répondant aux enjeux de l'analyse de risques en définissant des procédures d'exploitation et d'utilisation des équipements informatiques dans le respect des contraintes SSI en vue de répondre de manière adaptée aux exigences issues de l'analyse de risque
- Identifier le contexte légal en s'appuyant sur les référentiels standards (droits, obligations, normes et standards) de la sécurité concernant la protection des données et services numériques afin de mesurer les périmètres de responsabilité en matière de sécurité informatique.
- Déployer les différents équipements et protocoles employés dans une architecture sécurisée en vue de garantir le juste niveau de sécurité en s'appuyant sur l'état de l'art.
- Rendre compte auprès des équipes techniques (SI, Security Operations center (SOC), Computer Emergency Response Team (CERT)...) des mesures mises en œuvre dans le domaine de la SSI au travers de communications écrites et orales en s'adaptant à l'audience et aux potentiels profils singuliers (situation de handicap, interculturalité, ...) afin de garantir l'appropriation, par les parties prenantes, d'un vocabulaire et d'une connaissance partagée des processus mis en œuvre.
- ...

Certifications préparées et métiers visés

Niveau d'entrée	Niveau de sortie
Aucun prérequis	**Niveau Master, ingénieur - Bac +5 et plus**

Liste des certifications

Expert en cybersécurité (MS)

Code RNCP : 39837

Métiers associés

M1802 — Expertise et support en systèmes d'information

Dates et lieux de formation

N° session	Modalité	Lieu	Du	Au
2022107S	Présentiel	CESSON-SEVIGNE	02/09/2025	31/12/2026
2377608S	Présentiel	CESSON-SEVIGNE	03/09/2026	31/12/2027

Source : GREF Bretagne #25172946F