CHOISIR MON MÉTIER EN PAYS DE LA LOIRE

fiche formation

EXPERT EN CYBERSÉCURITÉ

NANTES YNOV CAMPUS
44200 NANTES

Informations pratiques

Du 01/9/2024 au 30/6/2026

- en centre : indéfinie heures
- en entreprise : indéfinie heures
- 2 ans temps plein, cours en présentiel
- Temps plein
- Cours de jour

Formation entièrement présentielle

Réunions d'information collective
Non renseigné

Portes ouvertes
Non renseigné

Inscriptions
Fermé

Pré-requis
Niveau d'entrée : Niveau 6 (Licence, Licence pro, BUT, Titres ou équivalents)
Admission sur dossier; Admission sur entretien; Bac + 3

Coûts
- Coûts d'inscription: Coût scolaire : 17500 en 2024 (8750 euros par an. Gratuit en apprentissage) - Coût d'inscription : 500 euros en 2024 euros -
- Coût de scolarité: euros -

Financements possibles
- État

Nantes Ynov Campus

20 Boulevard du Général de Gaulle
CS 46339
44200 Nantes
02-28-44-04-40
contact-nantes@ynov.com
http://www.ynov-nantes.com/
Statut: Privé hors contrat

Lieu de la formation

Nantes Ynov Campus
20 Boulevard du Général de Gaulle
CS 46339 44200 Nantes
02-28-44-04-40

contact-nantes@ynov.com

Objectif Général

Certification

Objectifs

Compétences attestées :

- Définir la stratégie de cybersécurité d'une organisation
- Elaborer et piloter des processus de cybersécurité d'une organisation
- Maintenir la sécurité du système d'information d'une organisation
- Gérer les incidents et crises de cybersécurité d'une organisation :

-

Blocs de compétences

> RNCP37832BC01 (CPP Définir la stratégie de cybersécurité d'une organisation)
• Organiser et animer un système de veille technique et technologique en matière de Sécurité du Système d'Information (SSI) à l'aide de recherches documentaires, de plateformes de partage, de webinars, de participations à des salons, des forums, clubs (CLUSIF, CLUSIR, ...etc.), afin d'être alerté des évolutions techniques, technologiques Organiser et animer un système de veille réglementaire en matière de sécurité du système d'information (SSI) en identifiant les sources de références du secteur de l'organisation afin de garantir la conformité de l'organisation à la réglementation Organiser et animer un système de veille concernant les nouvelles menaces à l'aide de recherche Web, CERT afin d'être prévenu des alertes, vulnérabilités et menaces susceptibles d'impacter l'organisation Traiter les informations recueillies en s'assurant de leur pertinence et véracité afin d'identifier les opportunités d'amélioration et obligations en matière de sécurité des données, des systèmes et des réseaux de l'organisation Identifier les composants techniques et les différentes parties prenantes en étudiant l'écosystème afin d'établir la cartographie des informations, leur portée et les risques afférents Rédiger un état des lieux de l'exposition numérique de l'organisation à l'aide des données publiques disponibles sur internet afin d'identifier les risques en termes de sécurité et d'exigences réglementaires Réaliser une analyse des risques en identifiant les évènements pouvant affecter la sécurité du système d'information et en estimant les conséquences et les impacts potentiels afin de hiérarchiser les risques pouvant affecter le système d'information (SI) Evaluer les besoins métier en consultant les utilisateurs et en identifiant les exigences fonctionnelles afin de déterminer les actions de sécurité à mettre en œuvre Concevoir et rédiger des solutions techniques en étudiant le système d'information (SI) et les procédures informatiques d'une organisation afin de formaliser les objectifs de la stratégie de cybersécurité Définir la politique de sécurité du système d'information (PSSI) en tenant compte de l'analyse de risques, du périmètre et des objectifs stratégiques de sécurité afin de s'assurer que les risques pesant sur le périmètre défini soient bien couverts Identifier les moyens techniques et humains nécessaires à la mise en œuvre de la PSSI en prenant en compte la stratégie de l'organisation en termes de sécurité du SI afin de permettre une évaluation du coût de mise en œuvre de la PSSI Estimer le coût de mise en œuvre de la PSSI en prenant en compte les différentes solutions possibles y compris assurantielles afin de permettre l'organisation de valider le déploiement des solutions Elaborer les plans de sauvegarde, plan de secours informatique (PSI) , plan de reprise d'activité (PRA), plan de continuité d'activité (PCA) en étudiant les processus et scénarios critiques afin de faciliter la résilience du système en cas d'incidents Réaliser un processus de tests des PCA, PRA, PSI et plan de sauvegarde en simulant un incident afin de vérifier la capacité de l'organisation à les mettre en œuvre Estimer les coûts associés à la mise en œuvre des PCA, PRA, PSI en identifiant l'ensemble des postes de dépenses afin d'intégrer ces coûts dans le budget de l'organisation

• Mise en situation professionnelle réelle ou fictive avec rendus de livrables
> RNCP37832BC02 (CPP Elaborer et piloter des processus de cybersécurité d'une organisation)
• Décliner la Politique de sécurité du système d'information (PSSI) en actions et/ou règles de sécurité adaptées à la cible en prenant en compte l'état actuel du système d'information (SI) afin de déterminer les impacts sur l'organisation Elaborer le plan d'actions en priorisant les actions selon les enjeux de sécurité identifiés et en évaluant leurs coûts afin d'éclairer la prise de décision Rédiger le corpus documentaire en tenant compte de la Politique de sécurité du système d'information (PSSI) afin d'encadrer l'utilisation /l'usage du système d'information (SI) Concevoir une architecture sécurisée en utilisant les méthodes et solutions connues afin de garantir la sécurité du système d'information (SI) Rationaliser les identités et les accès à l'aide de différents dispositifs de contrôle et d'alerte (électronique, physique et informatique) afin d'éviter les diffusions d'informations indues Mettre en place les solutions potentielles de sécurité (VPN, chiffrement de portable, protection de fichiers, ...) en identifiant les besoins (classification et usage) afin de renforcer la protection des informations contre les accès indus et risques de divulgation accidentelle ou malveillante Intégrer la sécurité dans l'organisation en appliquant les prérequis, les normes et les bonnes pratiques en matière de sécurisation du système d'information (SI) en vigueur, a?n de garantir un niveau de sécurité en adéquation avec la Politique de sécurité du système d'information (PSSI) Définir un processus de validation des changements en évaluant la demande de changement, en analysant son impact et en accompagnant les parties prenantes aux changements afin de garantir la sécurité du système d'information (SI) dans le déploiement des projets Elaborer les spécifications fonctionnelles d'un projet de sécurité en tenant compte de l'exposition au risque, des ressources nécessaires et de la politique de sécurité du système d'information (PSSI) afin de définir les spécifications techniques Planifier un projet de sécurité du système d'information (SI) en tenant compte des ressources humaines, matérielles, financières nécessaires à l'exécution du projet afin de définir l'ordonnancement détaillé des tâches, clarifier les responsabilités des différents acteurs et assurer une bonne coordination Piloter l'avancement d'un projet après avoir défini les outils de suivi adaptés, en assurant un suivi régulier de l'avancée, en communiquant sur les indicateurs clés afin de garantir la performance du projet dans le respect des délais, de la qualité et des coûts Réaliser une campagne de tests conformément au cahier de recettes afin de s'assurer que le projet réponde aux attentes et spécifications définies Rédiger la documentation projet en tenant compte des spécificités du projet et son impact dans l'organisation du système d'information (SI) afin de permettre la livraison du projet
• Mise en situation professionnelle réelle ou fictive avec rendus de livrables et soutenance orale devant jury
> RNCP37832BC03 (CPP Maintenir la sécurité du système d'information d'une organisation)
• Elaborer une politique de sensibilisation aux risques de cybersécurité en impliquant tous les collaborateurs afin de prévenir les incidents de cybersécurité au sein de l'organisation Déployer la politique de sensibilisation aux risques de cybersécurité en élaborant des supports et des méthodes de formation a?n d'aider les utilisateurs du système d'information (SI) à s'approprier la culture de cybersécurité mise en place Mettre en place une politique de contrôle et de surveillance continue en tenant compte des menaces identifiées et de la PSSI afin de s'assurer de l'efficacité des mesures de protection Identifier, en étudiant le contexte du système d'information, les paramètres à connaitre et mesurer, qui permettent soit par leur valeur absolue, soit par leur variation d'évaluer le niveau de sécurité du système d'information Mettre en place une surveillance et un contrôle à l'aide de dispositifs de sécurité et d'outils de supervision afin de s'assurer du fonctionnement continu et efficace des dispositifs de sécurité mis en place Documenter les vulnérabilités détectées par les moyens techniques de surveillance en analysant les risques associés afin de décrire les mesures à prendre Corriger les vulnérabilités identifiées en élaborant un plan d'actions approprié afin de restaurer la sécurité du système concerné Définir le plan d'audit en délimitant le périmètre à étudier et en prenant en compte les points critiques a?n de s'assurer de la bonne application des politiques et procédures de sécurité Rédiger un rapport d'audit en précisant la démarche suivie, les actions entreprises les vulnérabilités détectées afin afin d'établir un plan de remédiation Suivre la mise en œuvre des actions correctives en véri?ant leur e?cacité a?n d'augmenter la sécurité de l'organisation
• Mise en situation professionnelle réelle ou fictive avec rendus de livrables et soutenance orale devant jury
> RNCP37832BC04 (CPP Gérer les incidents et crises de cybersécurité d'une organisation :)
• Identifier les incidents de sécurité détectés à l'aide des outils de supervision au sein d'un Security Operations Center (SOC) afin de permettre leur analyse Réaliser une analyse forensique de l'incident en collectant les preuves afin de permettre la présentation d'une synthèse destinée aux décideurs Utiliser des moyens d'atténuation, de réparation ou de récupération du système d'information (SI), en utilisant des outils dédiés afin d'assurer la continuité du bon fonctionnement du SI et la préservation des données Réaliser un protocole de tests afin de vérifier que les moyens et solutions techniques mis en œuvre permettent de corriger une faille informatique Mettre en œuvre le plan de restauration du SI en utilisant des solutions techniques afin de restaurer toutes les capacités ou les Services du système d'information (SI) Donner des instructions et un plan d'actions détaillé pour répondre aux intrusions en maintenant la communication avec les équipes et la

direction afin de piloter la gestion de crise Définir un plan de communication de crise en identifiant les parties prenantes à informer et les canaux de communication à utiliser afin de réagir de manière efficace en cas de crise Présenter une synthèse de l'incident à partir des éléments présents dans le rapport d'analyse forensique afin de faire valider les adaptations des procédures du système d'information (SI) à déployer
• Mise en situation professionnelle réelle ou fictive avec rendus de livrables

Résultats attendus

voir la fiche sur le site de l'ONISEP

Niveau d'entrée

Niveau 6 (Licence, Licence pro, BUT, Titres ou équivalents)

Organisation pédagogique

> Modalité d'enseignement :
• Formation entièrement présentielle

En savoir plus

Source : Onisep traitée par le Cariforef - 223431 - Code établissement : 51594