CHOISIR MON MÉTIER EN PAYS DE LA LOIRE

fiche formation

EXPERT EN CYBERSÉCURITÉ ET SÉCURITÉ INFORMATIQUE

EPSI - ECOLE DES SCIENCES INFORMATIQUES
44200 NANTES

Informations pratiques

Du 01/9/2023 au 30/6/2025

- en centre : indéfinie heures
- en entreprise : indéfinie heures
- 2 ans temps plein
- 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 : 20300 euros en 2023 (10100 euros la 1re année et 10200 euros la 2e année) - Coût d'inscription : 225 euros en 2023 (uniquement pour la formation à temps plein, 100 euros en 1re année et 125 euros en 2e année) euros -
- Coût de scolarité: euros -

Financements possibles

EPSI - Ecole des Sciences Informatiques

HEP Campus Nantes 16 Boulevard Général de Gaulle
44200 Nantes
02-40-76-60-87
info@nantes-epsi.fr
https://www.epsi.fr/campus/campus-de-nantes/
Statut: Privé hors contrat

Lieu de la formation

EPSI - Ecole des Sciences Informatiques
HEP Campus Nantes 16 Boulevard Général de Gaulle 44200 Nantes
02-40-76-60-87

info@nantes-epsi.fr

- État

Objectif Général

Certification

Objectifs

Compétences visées

- Conception de la stratégie de sécurité du système d'information et conseil à la gouvernance
- Pilotage de projet de déploiement de la stratégie de sécurité informatique et cybersécurité en mobilisant une démarche agile et innovante
- Déploiement d'une architecture fonctionnelle et technique en vue de renforcer la sécurité du S.I et faire face aux cybermenaces

-

Blocs de compétences

> RNCP36924BC01 (CPP Conception de la stratégie de sécurité du système d'information et conseil à la gouvernance)
• Étudier le système d'information d'une structure dans sa globalité, en identifiant les points faibles du système, afin d'évaluer le niveau de sécurité au sein de l'organisation Identifier les enjeux de sécurité, les risques majeurs de sécurité pesant sur l'organisation et vis-à-vis des tiers et sous-traitants et les exigences de conformité légale afin de garantir à l'entreprise d'être en conformité vis à vis de la règlementation française en matière de droit informatique ainsi que la bonne mise en application des normes et certifications du domaine Décliner les axes et les objectifs stratégiques en matière de sécurité informatique et cybersécurité afin de sensibiliser la Direction générale au sujet et lui permettre de vérifier sa bonne correspondance avec la stratégie de développement de l'entreprise Définir la feuille de route stratégique adaptée aux besoins et à la culture de la structure, en lien avec les parties prenantes (informaticiens et les responsables des services) concernés afin de répondre à des objectifs de sécurité métiers et IT stratégiques face à l'augmentation de la cybermenace Définir une stratégie de mise en conformité en lien avec la règlementation RGPD et le droit informatique afin de proposer un descriptif du process de la sécurité tenant compte de ce paramètre et ainsi, faciliter les relations avec les autorités de régulation en cas de contrôle réglementaires (auditeur RGPD et CNIL principalement) Définir les mesures organisationnelles et techniques permettant de minimiser les risques liés à la sécurité du système d'information dans le but d'assurer une protection optimale et appropriée des données de l'entreprise et atteindre ainsi les objectifs de sécurité définis par la gouvernance Définir l'organisation de la cybersécurité en proposant une charte de sécurité informatique de l'organisation afin de sensibiliser régulièrement les équipes et évaluer leurs connaissances en matière de règle de sécurité informatique Concevoir un référentiel SSI de l'organisme (schéma directeur, meilleures pratiques, directives internes…) permettant de formaliser, de justifier les choix, de légitimer les plans d'action et de garantir la cohérence avec le contexte particulier de l'organisme Conseiller l'organisation en proposant des préconisations et des recommandations sur l'amélioration du niveau de sécurité afin de lui permettre une meilleure compréhension des enjeux et risques de cybermenaces et augmenter sa capacité de gestion de crises Informer les directions générales et les directions métiers sur les enjeux de la sécurité informatique, cybersécurité et l'état de la menace afin de les sensibiliser sur l'évolution du contexte de la sécurité et la cybersécurité en utilisant des supports de communication inclusifs Apporter une expertise juridique auprès de la gouvernance en matière de conformité (à une règlementation, à des référentiels d'exigences) afin de fournir

aux dirigeants des entreprises les règles et les bonnes pratiques à applique faces aux nouvelles exigences en matière de conformité règlementaire
• Mise en situation professionnelle reconstituée (MSPR) Analyse et conseil d'une politique de sécurité informatique d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur Phase I- Préparation tutorée de la MSPR par équipe de 3 max - Durée de préparation : 21 h Phase II-Production écrite individuelle à réaliser Phase III -Soutenance orale devant un jury de professionnel Durée : 45 mn - 15 min de présentation de la réalisation en groupe - 10 min d'entretien individuel (questions en lien avec les compétences)
> RNCP36924BC02 (CPP Pilotage de projet de déploiement de la stratégie de sécurité informatique et cybersécurité en mobilisant une démarche agile et innovante)
• Identifier l'ensemble des étapes de réalisation du système d'information pour organiser le projet en tâches et livrables en répartissant les activités en fonction des ressources humaines, techniques et financières à mobiliser Concevoir les cahiers des charges technique et fonctionnel d'un projet de développement S.I. à l'aide des besoins utilisateurs collectés afin de cadrer le développement? Piloter les prestataires extérieurs éventuels gérant les ressources informatiques d'un système d'information existant listées dans la cartographie établie afin de sécuriser la mise en œuvre technique Établir des tableaux de bord de suivi de performance (qualitative et quantitative) de l'ensemble des ressources allouées à chaque étape-projet pour anticiper, visualiser et corriger les écarts en temps réel afin de limiter les contraintes de ressources et les retards Gérer un projet agile en utilisant les méthodes et outils adaptés à ce mode de fonctionnement pour tester, modifier et procéder par itération afin de réduire les délais de remise des projets de développement S.I. Conduire une équipe projet en diffusant les fondamentaux de l'agilité?: adaptation, flexibilité et amélioration continue au sein de l'équipe afin d'être en mesure d'absorber les changements de priorité qui peuvent intervenir dans un contexte de forte contrainte de temps et d'incertitudes Proposer des solutions innovantes afin de favoriser les interactions et l'inclusion au sein de l'équipe et d'anticiper des conflits de travail liés aux malentendus multiculturels et des profils en situation d'handicap Accompagner l'équipe dans l'appropriation du travail à distance ou du télétravail en proposant des solutions managériales afin de favoriser la motivation et la résilience et permettre ainsi de préserver équilibre entre vie professionnelle/vie privée dans un souci de productivité et de bien-être Concevoir un processus de communication inclusif régulier au sein de l'équipe afin de synchroniser les activités quotidiennes et mettre en place un fil de discussion à l'aide d'outils numériques Communiquer avec l'équipe en adoptant les modes de communication adéquats selon les cultures et la langue des collaborateurs afin de garantir l'intégration de tous les membres de l'équipe Animer des réunions à distance afin de maintenir une dynamique de groupe et renforcer l'esprit d'équipe des membres en télétravail et/ou à distance Concevoir un processus de partage d'information afin de faciliter la collaboration entre les membres (tous profils confondus) en télétravail et/ou à distance en utilisant des outils numériques
• Mise en situation professionnelle reconstituée (MSPR) Gestion d'un projet de mis en place d'une stratégie de sécurité et cybersécurité pour une structure proposée par le certificateur Phase I- Préparation tutorée de la MSPR par équipe de 3 max - Durée de préparation : 21 h Phase II-Production écrite individuelle à réaliser Phase III -Soutenance orale devant un jury de professionnel Durée : 45 mn - 15 min de présentation de la réalisation en groupe - 10 min d'entretien individuel (questions en lien avec les compétences)
> RNCP36924BC03 (CPP Déploiement d'une architecture fonctionnelle et technique en vue de renforcer la sécurité du S.I et faire face aux cybermenaces)
• Assurer la mise en place des structures organisationnelles des plans d'actions de sécurité au sein des entités afin de garantir la protection de données et le niveau de sécurité du système d'information Paramétrer les mesures organisationnelles permettant la surveillance de la sécurité globale d'une organisation (des événements de sécurité, l'appréciation des incidents de sécurité et la réaction face aux attaques) afin d'assurer la mise en place d'un SOC (Security Operation Center) Déployer les mesures organisationnelles de sécurité en se basant sur la stratégie de sécurité informatique de l'organisation afin d'assurer le fonctionnement opérationnel et les maintenir à l'état de l'art Déployer des architectures et ou des solutions de sécurité de la couche matériels et logiciels de l'entreprise permettant de garantir l'évolutivité et la haute-disponibilité du système d'information Piloter la procédure de paramétrage des politiques (habilitations) et configuration des droits d'accès appliqués sur son périmètre et vis-à-vis des tiers et des sous-traitants afin de garantir une utilisation sécurisée des moyens informatiques mis à disposition des utilisateurs finaux Contribuer au pilotage de la mise en œuvre des outils et des solutions de sécurité autour des données de l'organisation et leur sauvegarde en fournissant une assistance technique et méthodologiques aux équipes informatiques afin de s'assurer de la pertinence des solutions/ outils choisis et participer lui-même à la bonne mise en place de la stratégie Assurer le déploiement du programme et des initiatives cybersécurité dans l'ensemble des entités tout en respectant la cohérence globale et la coordination entre ces différentes entités afin que chaque entité s'approprie les nouvelles solutions/plateformes techniques et les services en cybersécurité

dans une organisation Assurer la mise en place d'un service de détection des incidents de sécurité SOC (Security Opération center) au sein de l'organisation afin d'évaluer le niveau de vulnérabilité et détecter des activités suspectes en prenant compte des exigences réglementaires Conduire des plans d'action sur la détection et la réaction aux incidents, en fournissant des informations pertinentes aux équipes afin d'assurer l'efficacité des outils de détection déployés dans le SOC Analyser des données brutes issues de différentes sources (dark web, renseignement open source, média sociaux, CERT) en utilisant la data science afin d'étudier l'évolution des modes opératoires des hackers et ajuster ensuite sa stratégie de cybersécurité Renforcer les capacités de détection des activités malveillantes menaçant le système d'information en utilisant des solutions IA afin de réduire le risque des cybers attaques et rendre plus performant le SI de l'entreprise Proposer des nouvelles approches innovantes basées sur l'IA en s'appuyant sur une veille technologique et industrielle concernant les nouveaux produits et process métiers mobilisant de l'IA afin d'améliorer la procédure de prévention d'intrusion de l'organisation et réinterroger son dispositif interne en initiant la mise en place d'un processus d'amélioration continue efficace
• Mise en situation professionnelle reconstituée (MSPR) Déploiement d'une architecture ou solution de sécurité / cybersécurité d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur Phase I- Préparation tutorée de la MSPR par équipe de 3 max - Durée de préparation : 28 h Phase II - Production écrite individuelle à réaliser Phase III -Soutenance orale sous forme d'une démonstration technique devant un jury de professionnel Durée : 45 mn - 15 min de présentation de la réalisation en groupe - 10 min de démonstration technique et entretien individuel (questions en lien avec les compétences)
> RNCP36924BC04 (CPP Supervision, audit et gestion de la sécurité informatique et des cyberattaques)
• Définir les plans d'audits et de contrôles au sein de l'organisation afin d'évaluer la bonne application, l'efficacité et la conformité des politiques et procédures de sécurité de l'entreprise Mener des contrôles permanents et/ou périodiques de sécurité, notamment sur la base de revues documentaires, de collecte de preuves, d'accès aux consoles et aux rapports des outils de sécurité ou de l'utilisation d'outils automatisés de contrôle de conformité afin de mettre à jour le niveau de la sécurité du SI de l'entreprise Rédiger des rapports intégrant une analyse des vulnérabilités et écarts constatés ainsi que les recommandations permettant de remédier aux risques découlant des vulnérabilités découvertes et d'informer la direction générale de l'avancement du ou des projets de déploiement Informer les équipes en charge de la sécurité des nouvelles menaces importantes et recommander des mesures tactiques pour les contrer en se basant sur sa veille technologique et son étude du marché afin d'impliquer l'ensemble des acteurs de l'entreprise et en particulier les directions métiers et ainsi favoriser la prévention des risques Analyser les risques de sécurité liés à l'introduction des nouvelles technologies en se basant sur une méthode d'analyse de risque optimisé afin d'atténuer les impacts sur le niveau de sécurité informatique d'une entreprise Assurer un appui opérationnel à la gestion de la cyber- crise avec les experts techniques, en cas d'incidents de sécurité majeurs, en coordonnant les équipes, afin d'agir de traiter tout actes malveillants impactant l'entreprise et mieux prévenir la cyber menace Assurer la formation et l'entraînement des acteurs métiers et support susceptible d'intervenir en cas de crise de cybersécurité afin d'améliorer la capacité de l'organisation à réagir à une attaque Animer la cellule de crise décisionnelle et les cellules de crise opérationnelles en impliquant chaque membre de l'équipe afin de s'assurer de leur capacité à agir et à traiter la crise de cybersécurité Piloter les actions de sensibilisation à la sécurité des SI et de conduite du changement auprès des utilisateurs en organisant des formations internes et externes dans le domaine de la sécurité des S.I afin de faire gagner en compétences les équipes internes en matière de cyber prévention et à terme faciliter la mise en place des nouveaux processus
• Mise en situation professionnelle reconstituée (MSPR) Audit, supervision et gestion de la sécurité informatique et des cyberattaques d'une structure à partir d'une situation réelle ou reconstituée proposée par le certificateur Phase II - Production écrite individuelle à réaliser Phase III -Soutenance orale devant un jury de professionnel Durée : 30 mn - 15 min de présentation de la réalisation en groupe - 15 min d'entretien individuel (questions en lien avec les compétences)

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 - 192216 - Code établissement : 36654