Oidaneos
Immeuble Le Sommet 42 rue Ferdinand Forest
97122 Baie-mahault
Email : start@oidaneos.com
Tel : +590690649318

Certification Cybersécurité DROM - Piloter et animer la sécurité informatique

Le parcours de formation vise à permettre aux candidats à la certification d'acquérir les connaissances, savoir-faire et compétences nécessaires au pilotage à l'animation de la sécurité informatique.
Jusqu'à 217.00 heures de formation

Profils des apprenants

- Professionnels titulaires d'une certification de niveau 5 ou 6 dans le domaine de l'informatique, dont la cybersécurité n'est pas la seule fonction (techniciens systèmes et réseaux, assistance technique dans les ESN, différents profils de la DSI).

Prérequis

- Justifier d'un diplôme ou d'une certification de niveau 5 (par exemple : BTS Services Informatiques aux Organisations, BTS Systèmes numériques, DUT informatique, Licence Professionnelle métiers de l'Informatique, BUT Informatique, Titres à Finalité Professionnelle, CQP dont le CQP Administrateur Systèmes et Réseaux, etc.)
- ou
- Justifier d'une expérience acquise au sein de la Direction des systèmes d'information d'une entreprise ou d'une ESN (Entreprise de Services du Numérique),

Accessibilité et délais d'accès

Accessibilité aux personnes handicapées : contacter le référent handicap à start@oidaneos.com ou whatsapp +590690649318
2 semaines

Objectifs pédagogiques

- Mettre en place d'une stratégie de cybersécurité à partir d'une analyse du risque
- Sécuriser des réseaux, des protocoles, des terminaux et des serveurs
- Animer et évaluer la mise en œuvre d'une stratégie de cybersécurité

Contenu de la formation

- Bloc 1 – Fondamentaux de la cybersécurité
  - Expliquer les concepts et acteurs de la cybersécurité
  - Identifier les risques, menaces et enjeux pour l'organisation
  - Reconnaître les cyberattaques et leurs vecteurs
  - Appliquer les normes et réglementations clés (ISO, RGPD)
- Bloc 2 – Supervision et suivi du SI
  - Décrire le rôle des IDS, IPS et UTM
  - Identifier les incidents et leur criticité
  - Reconnaître les actifs sensibles du SI
  - Interpréter les tableaux de bord et journaux
- Bloc 3 – Gestion et remédiation des incidents
  - Mettre en œuvre un processus de gestion d'incident
  - Exploiter les informations issues du SIRT et des outils de supervision
  - Réagir face à un incident : détection, classification, réponse
  - Analyser les causes racines et appliquer les procédures de traitement

Oidaneos
Immeuble Le Sommet 42 rue Ferdinand Forest
97122 Baie-mahault
Email : start@oidaneos.com
Tel : +590690649318

- Bloc 4 – Gestion de crise, veille et sensibilisation
    - Analyser et documenter une crise de cybersécurité
    - Réaliser un retour d'expérience (RETEX)
    - Sensibiliser les utilisateurs aux bonnes pratiques
    - Concevoir et diffuser des supports de communication adaptés
    - Contribuer à la veille cyber et partager les informations pertinentes

Organisation de la formation

Équipe pédagogique
L'équipe pédagogique du centre de formation est composée de professionnels qualifiés et expérimentés dans leur domaine d'expertise. Ils sont passionnés par l'enseignement et engagés à offrir des programmes de formation de haute qualité pour aider les étudiants à atteindre leurs objectifs professionnels.

Ressources pédagogiques et techniques
- Modules Théoriques : Guides complets et articles
- Vidéos et Tutoriels : Supports vidéo
- Plateforme Interactive : Accès à une plateforme LMS pour des démonstrations et exercices pratiques.
- Bibliographie Recommandée : Livres et articles essentiels sélectionnés pour approfondir la compréhension.
- Supports de Cours Interactifs : Supports multimédias interactifs pour une compréhension visuelle.

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation
- Étapes de Suivi : Tableau de bord pour suivre la progression, réunions régulières et feedback continu.
- Évaluation Formative : Quiz périodiques, revues par les pairs et soutien individuel.
- Projets Pratiques et Études de Cas : Évaluation des projets et analyses d'études de cas pour une application pratique.
- Feedback des Formateurs et des Pairs : Retours détaillés des formateurs, échanges entre pairs pour un apprentissage collaboratif.
- Évaluation Sommative : Examen final et présentation des projets devant un comité d'évaluation.
- Réajustement du Programme : Collecte de feedback à mi-parcours et adaptation du contenu en fonction des évaluations finales.
- Attestation : Délivrance de certification aux participants réussissant, avec collecte de retours pour améliorations futures.

Modalités de certification

À l'issue du parcours, le participant sera capable de :
- Mettre en place d'une stratégie de cybersécurité à partir d'une analyse du risque
- Sécuriser des réseaux, des protocoles, des terminaux et des serveurs
- Animer et évaluer la mise en œuvre d'une stratégie de cybersécurité

L'apprenant peut suivre un ou plusieurs modules sans viser la certification. Une attestation de formation sera délivrée pour chaque module suivi.

Organisme certificateur : OPCO Atlas
La certification est délivrée sous réserve de la validation des 10 compétences définies dans le référentiel.

Soutenance orale (35 min) : Présentation de plusieurs situations vécues en contexte professionnel ou formatif (20 min) suivi d'un entretien avec le jury (15 min)
Plus d'informations CAMPUS Atlas :
https://campus.opco-atlas.fr/modules/piloter-animer-securite-informatique-/715

Financement de la formation

Prix : 22100.00

Oidaneos
Immeuble Le Sommet 42 rue Ferdinand Forest
97122 Baie-mahault
Email : start@oidaneos.com
Tel : +590690649318

Qualité et indicateurs de résultats

OIDANEOS est un organisme certifié Qualiopi pour ses actions de formation.
Les indicateurs de résultats relatifs à cette certification IA seront publiés après les premières sessions (taux de réussite, taux de satisfaction, taux d'insertion professionnelle).
À titre indicatif, les formations dispensées par OIDANEOS en 2024–2025 présentent un taux de satisfaction supérieur à 90 %.