ARRIOPH
Academy

FORMATIONS & CERTIFICATIONS

FORMATION MICROSOFT SECURITY & COMPLIANCE

Microsoft Cybersecurity Architect Expert

Microsoft Partner

www.academy.arrioph.com

À Propos de la formation

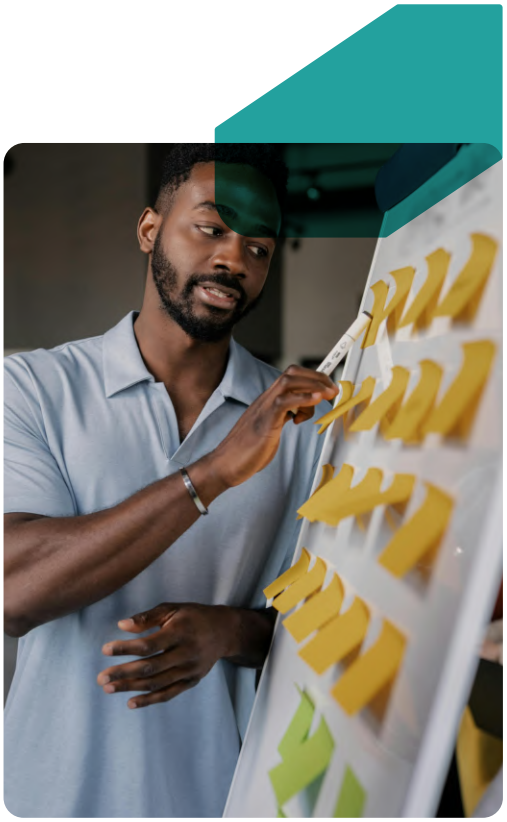
Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour concevoir et à évaluer des stratégies de cybersécurité dans les domaines suivants : Confiance zéro, gouvernance, risque et conformité (GRC), opérations de sécurité (SecOps), et données et applications.
Les participants apprendront également à concevoir et à architecturer des solutions en utilisant les principes de confiance zéro et à spécifier les exigences de sécurité pour l'infrastructure du cloud dans différents modèles de services (SaaS, PaaS, IaaS).

Profil du public

Cette formation s'adresse aux professionnels de l'informatique ayant une expérience et des connaissances avancées dans un large éventail de domaines d'ingénierie de la sécurité, notamment l'identité et l'accès, la protection des plateformes, les opérations de sécurité, la sécurisation des données et la sécurisation des applications.
Ils doivent également avoir une expérience des mises en œuvre hybrides et en cloud.

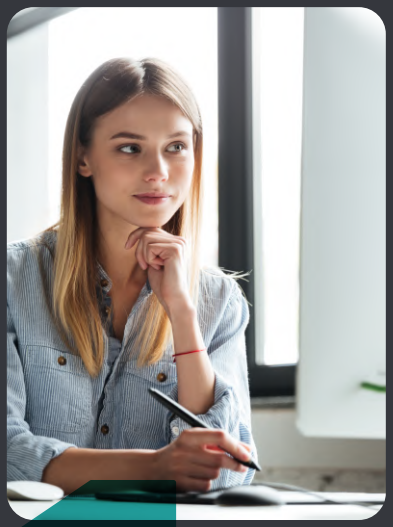
Objectifs de cette formation

A l'issue de la formation, les participants seront capables de :



- Concevoir une stratégie et une architecture de confiance zéro
- Évaluer les stratégies techniques de gouvernance, de risque et de conformité (GRC) et les stratégies de sécurité opérationnelle
- Concevoir la sécurité de l'infrastructure
- Concevoir une stratégie pour les données et les applications

Pré-requis de la formation



Avant de suivre cette formation, les participants doivent avoir une expérience et connaissances avancées en matière d'identité et d'accès, de protection des plateformes, d'opérations de sécurité, de sécurisation des données et de sécurisation des applications.

Programme détaillé de la formation

01 Construire une stratégie et une architecture de sécurité globale

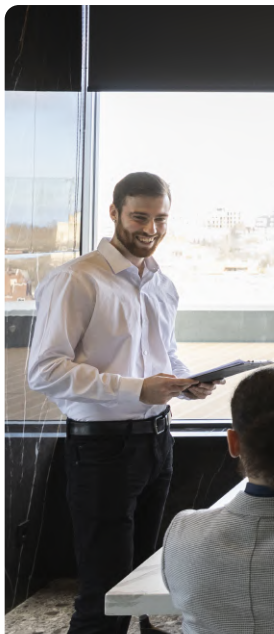
- Aperçu de la confiance zéro
- Développer des points d'intégration dans une architecture
- Développer des exigences de sécurité basées sur des objectifs commerciaux
- Traduire les exigences de sécurité en capacités techniques
- Concevoir la sécurité pour une stratégie de résilience
- Concevoir une stratégie de sécurité pour les environnements hybrides et multi-tenant
- Concevoir des stratégies techniques et de gouvernance pour le filtrage et la segmentation du trafic
- Comprendre la sécurité des protocoles

02 Concevoir une stratégie d'opérations de sécurité

- Comprendre les cadres, processus et procédures des opérations de sécurité
- Concevoir une stratégie de sécurité en matière de journalisation et d'audit
- Développer des opérations de sécurité pour les environnements hybrides et multi-clouds
- Concevoir une stratégie pour la gestion des informations et des événements de sécurité (SIEM) et l'orchestration de la sécurité
- Évaluer les flux de travail de sécurité
- Examiner les stratégies de sécurité pour la gestion des incidents
- Évaluer la stratégie des opérations de sécurité pour le partage des renseignements techniques sur les menaces
- Surveiller les sources de renseignements sur les menaces et les mesures d'atténuation.

03 Concevoir une stratégie de sécurité des identités

- Sécuriser l'accès aux ressources du cloud
- Recommandation d'un magasin d'identité pour la sécurité
- Recommandation de stratégies d'authentification et d'autorisation sécurisées
- Accès conditionnel sécurisé
- Conception d'une stratégie d'attribution et de délégation de rôles
- Définir la gouvernance des identités pour les contrôles d'accès et la gestion des droits
- Conception d'une stratégie de sécurité pour l'accès des rôles privilégiés à l'infrastructure
- Concevoir une stratégie de sécurité pour les activités privilégiées
- Comprendre la sécurité des protocoles



04 Évaluer une stratégie de conformité réglementaire

- Interpréter les exigences de conformité et leurs capacités techniques
- Évaluer la conformité de l'infrastructure en utilisant Microsoft Defender for Cloud
- Interpréter les scores de conformité et recommander des actions pour résoudre les problèmes ou améliorer la sécurité
- Concevoir et valider la mise en œuvre de la politique Azure
- Conception pour les exigences de résidence des données
- Traduire les exigences de confidentialité en exigences pour les solutions de sécurité

05 Évaluer la posture de sécurité et recommander des stratégies techniques pour gérer les risques

- Évaluer la posture de sécurité à l'aide de repères
- Évaluer la posture de sécurité à l'aide de Microsoft Defender for Cloud
- Évaluer les postures de sécurité à l'aide de Secure Scores
- Évaluer l'hygiène de sécurité des charges de travail dans le Cloud
- Concevoir la sécurité d'une Azure Landing Zone
- Interpréter les renseignements sur les menaces techniques et recommander des mesures d'atténuation des risques
- Recommander des capacités ou des contrôles de sécurité pour atténuer les risques identifiés.

06 Comprendre les meilleures pratiques d'architecture et la façon dont elles évoluent avec le cloud

- Planifier et mettre en œuvre une stratégie de sécurité au sein des équipes
- Établir une stratégie et un processus pour une évolution proactive et continue de la stratégie de sécurité
- Comprendre les protocoles réseau et les meilleures pratiques de segmentation du réseau et de filtrage du trafic

07

Concevoir une stratégie pour sécuriser les points d'extrémité des serveurs et des clients

- Définir les lignes de base de la sécurité pour les points d'extrémité des serveurs et des clients
- Définir les exigences de sécurité pour les serveurs
- Spécifier les exigences de sécurité pour les appareils mobiles et les clients
- Préciser les exigences en matière de sécurisation des services de domaine Active Directory
- Conception d'une stratégie de gestion des secrets, des clés et des certificats
- Concevoir une stratégie d'accès à distance sécurisé
- Comprendre les cadres, processus et procédures des opérations de sécurité
- Comprendre les procédures d'investigation approfondie par type de ressources

08

Concevoir une stratégie pour sécuriser les services PaaS, IaaS et SaaS

- Définir des lignes de base de sécurité pour les services PaaS
- Spécifier les lignes de base de sécurité pour les services IaaS
- Spécifier les lignes de base de sécurité pour les services SaaS
- Spécifier les exigences de sécurité pour les charges de travail IoT
- Spécifier les exigences de sécurité pour les charges de travail de données
- Spécifier les exigences de sécurité pour les charges de travail Web
- Spécifier les exigences de sécurité pour les charges de travail de stockage
- Spécifier les exigences de sécurité pour les conteneurs
- Spécifier les exigences de sécurité pour l'orchestration des conteneurs
- Spécifier les exigences de sécurité pour les applications

09

Comprendre la modélisation des menaces pour les applications

- Définir les priorités pour atténuer les menaces pesant sur les applications
- Définir une norme de sécurité pour l'intégration d'une nouvelle application
- Définir une stratégie de sécurité pour les applications et les API

10

Concevoir une stratégie de sécurisation des données

- Établir des priorités pour atténuer les menaces pesant sur les données
- Concevoir une stratégie pour identifier et protéger les données sensibles
- Définir une norme de chiffrement pour les données au repos et en mouvement

Les plus de cette formation

- Les formateurs/consultants spécialistes Microsoft apportent leurs conseils et leur expérience.

- Ce cours prépare à la certification Microsoft Certified : Cybersecurity Architect Expert Certification après réussite de l'examen SC-100

- La qualité d'une formation officielle Microsoft (support de cours numérique en anglais).

- Votre formateur :
  - Est un consultant formateur certfiié Microsoft
  - Possède plusieurs années d'expérience sur l'environnement Dynamics
  - En veille permanente pour suivre son évolution.

Modalités

- Durée de la formation : 4 jour (28h)
- Tarif : 2900 € HT
- Référence : MSSC100
- Disponible en Classe en présentiel et à distance
- Formation éligible au Action Collective OPCO
- ARRIOPH est certifiée Qualiopi au titre de ses actions de formation

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

OPCO Atlas
Soutenir les compétences

Préparation à la certification SC-100 (En option)

- Les certifications vous donnent un avantage professionnel en fournissant des preuves de maîtrise des compétences reconnues dans le monde entier, démontrant vos capacités et votre volonté d'adopter de nouvelles technologies.
- L'architecte en cybersécurité de Microsoft possède une expertise en matière de conception et d'évolution de la stratégie de cybersécurité afin de protéger la mission et les processus commerciaux d'une organisation dans tous les aspects de l'architecture d'entreprise.
- L'architecte de cybersécurité conçoit une stratégie et une architecture Confiance nulle, notamment des stratégies de sécurité pour les données, les applications, la gestion des accès, l'identité et l'infrastructure.
- L'architecte de cybersécurité évalue également les stratégies techniques de GRC (Conformité aux risques de gouvernance) et les stratégies d'opérations de sécurité.
- L'architecte de cybersécurité collabore continuellement avec les dirigeants et les professionnels en matière de sécurité informatique et de confidentialité, ainsi que d'autres rôles organisationnels, afin de planifier et d'implémenter une stratégie de cybersécurité répondant aux besoins d'une organisation.
- Un candidat à cet examen doit avoir une expérience et des connaissances avancées dans un vaste éventail de domaines de l'ingénierie de la sécurité, notamment l'identité et l'accès, la protection des plateformes, les opérations de sécurité, la sécurisation des données et la sécurisation des applications.
  Ils doivent également être familiarisés avec les implémentations hybrides et cloud.

Les compétences mesurées:

- Concevoir une stratégie et une architecture Confiance zéro (30 - 35%)
- Évaluer les stratégies techniques de GRC (gouvernance, risque et conformité) et les stratégies d'opérations de sécurité (10 - 15%)
- Concevoir la sécurité pour l'infrastructure (10 - 15%)
- Concevoir une stratégie pour les données et les applications (15 - 20%)
- Recommander les bonnes pratiques et priorités en matière de sécurité (20 - 25%)

ARRIOPH Academy

FORMATIONS & CERTIFICATIONS

Nous contacter

P : +33 1 89 27 27 81

E : academy@arrioph.com

34 Av. des Champs-Élysées
75008 Paris