Présentiel/distanciel Cours Officiel Formation certifiante

Architecte cybersécurité Microsoft

Objectifs pédagogiques

- Concevoir des solutions de cybersécurité alignées sur Zero Trust, les bonnes pratiques Microsoft et les priorités métier
- Concevoir des capacités de sécurité pour les opérations, l'identité, les accès privilégiés et la conformité
- Concevoir des solutions de sécurité pour les applications, les données et les usages Microsoft 365
- Concevoir des solutions de sécurité pour l'infrastructure, les environnements hybrides, multicloud et les endpoints
- Évaluer des architectures de sécurité à l'aide de cadres comme MCRA, MCSB, CAF et WAF

Prérequis

- Expérience avancée et connaissances approfondies en identité et accès, protection de plateforme, opérations de sécurité, sécurisation des données et sécurisation des applications
- Expérience des environnements hybrides et cloud
- Bonne connaissance des technologies Microsoft de sécurité et d'identité
- Une certification préalable dans le portefeuille sécurité, conformité et identité est recommandée
- Il est fortement recommandé d'avoir suivi l'une ou plusieurs des formations suivantes :
- Se défendre contre les cybermenaces avec la plateforme d'opérations de sécurité Microsoft
- Administrateur des identités et des accès Microsoft
- Sécurisation avancée des environnements Microsoft Azure et protection des ressources cloud

Certification

Cette formation prépare à l'examen Architecte en cybersécurité Microsoft, qui associé à l'examen Associé Ingénieur en Sécurité Azure ou l'examen Administrateur d'Identité et d'Accès Associé ou l'examen Analyste des opérations de sécurité Associé permet d'obtenir la certification Microsoft Certified : Cybersecurity Architect Expert

Public concerné

Cette formation s'adresse aux ingénieurs sécurité cloud expérimentés et aux architectes sécurité souhaitant concevoir et faire évoluer des solutions de cybersécurité à l'échelle de l'entreprise avec les technologies Microsoft.
Elle concerne les professionnels amenés à transformer des exigences métier, sécurité, conformité et résilience en architectures de sécurité couvrant l'identité, les opérations de sécurité, les applications, les données et l'infrastructure.

Bénéfices pour les participants :

- Structurer une vision d'architecture cybersécurité cohérente à l'échelle de l'entreprise
- Relier les exigences de sécurité, conformité, résilience et gouvernance aux capacités Microsoft adaptées
- Renforcer la capacité à concevoir des architectures sécurité hybrides, multicloud et orientées Zero Trust
- Préparer un positionnement de niveau architecte sur les technologies Microsoft de sécurité

Présentiel/distanciel | Cours Officiel | Formation certifiante

Programme détaillé

Introduction à Zero Trust et aux référentiels de bonnes pratiques (1h30)

- Décrire les anti-patterns de sécurité et le rôle des bonnes pratiques
- Décrire le concept Zero Trust et ses piliers technologiques
- Décrire le cadre d'adoption Zero Trust et l'approche de modernisation rapide

Concevoir des solutions alignées sur le Cloud Adoption Framework et le Well-Architected Framework (1h30)

- Comprendre le Cloud Adoption Framework et la méthodologie Secure
- Comprendre les Azure Landing Zones et leurs zones de conception
- Comprendre le Well-Architected Framework et ses principes de conception de sécurité
- Évaluer et concevoir des stratégies de sécurité et de gouvernance basées sur CAF et WAF
- Concevoir un processus DevSecOps aligné sur les bonnes pratiques du CAF
- Concevoir une stratégie d'adoption sécurisée de l'IA

Concevoir des solutions alignées sur la Microsoft Cybersecurity Reference Architecture et le Microsoft Cloud Security Benchmark (1h30)

- Comprendre la Microsoft Cybersecurity Reference Architecture
- Comprendre le Microsoft Cloud Security Benchmark
- Concevoir des solutions alignées sur les bonnes pratiques de capacités et de contrôles
- Concevoir des solutions de protection contre les attaques internes, externes et supply chain
- Concevoir des solutions IA alignées sur MCSBv2

Concevoir une stratégie de résilience face au ransomware et aux cybermenaces courantes (0h30)

- Comprendre les cybermenaces courantes et leurs vecteurs d'attaque
- Concevoir des solutions de résilience et d'atténuation face au ransomware
- Concevoir des solutions de continuité d'activité et de reprise d'activité
- Évaluer des solutions de gestion des mises à jour de sécurité

Concevoir des solutions pour la conformité réglementaire (0h15)

- Interpréter les exigences réglementaires et les traduire en contrôles de sécurité
- Concevoir des solutions de conformité avec Microsoft Purview
- Concevoir des solutions de confidentialité avec Microsoft Priva
- Concevoir des solutions Azure Policy pour la sécurité et la conformité
- Évaluer les standards et benchmarks avec Microsoft Defender for Cloud

Concevoir des solutions de gestion des identités et des accès (1h15)

- Concevoir une solution d'accès aux ressources SaaS, PaaS, IaaS, hybrides et multicloud
- Concevoir une solution Microsoft Entra ID dans des environnements hybrides et multicloud
- Concevoir une solution pour les identités externes
- Concevoir des stratégies modernes d'authentification et d'autorisation
- Valider l'alignement des stratégies Conditional Access avec Zero Trust
- Spécifier les exigences de sécurisation d'Active Directory Domain Services
- Concevoir une solution de gestion des secrets, clés et certificats

Concevoir des solutions pour sécuriser les accès privilégiés (1h15)

- Comprendre les principes des accès privilégiés sécurisés
- Concevoir une solution d'attribution et de délégation des rôles privilégiés avec l'enterprise access model
- Évaluer la sécurité et la gouvernance avec Microsoft Entra ID
- Concevoir une solution de sécurisation de l'administration des tenants
- Concevoir une solution de cloud infrastructure entitlement management
- Évaluer une solution de revues d'accès
- Concevoir une solution de poste d'administration privilégié avec accès distant sécurisé

Concevoir des solutions pour les opérations de sécurité (1h15)

- Décrire le rôle des opérations de sécurité
- Concevoir la supervision pour les environnements hybrides et multicloud
- Concevoir des solutions de journalisation et d'audit centralisés
- Concevoir des solutions de détection et de réponse intégrant XDR et SIEM
- Concevoir une solution SOAR
- Concevoir et évaluer des workflows de sécurité
- Évaluer la couverture de détection avec MITRE ATT&CK

Étude de cas interactive : Moderniser l'identité et la sécurité des données (1h00)

- Analyse d'un scénario d'architecture sécurité
- Évaluation des choix de conformité, identité et protection des données
- Comparaison et justification des solutions retenues

Étude de cas interactive : Moderniser le contrôle d'accès utilisateur et la résilience face aux menaces (1h00)

- Analyse d'un scénario d'architecture sécurité
- Évaluation des choix d'accès, de résilience et d'opérations de

sécurité
- Comparaison et justification des solutions retenues

Concevoir des solutions de sécurité pour Microsoft 365 (2h00)
- Évaluer la posture de sécurité des workloads de productivité et de collaboration
- Évaluer la protection assurée par Defender for Office 365 et Defender for Cloud Apps
- Évaluer la protection et la gestion des terminaux avec Microsoft Intune
- Évaluer la sécurisation des données Microsoft 365 avec Microsoft Purview
- Évaluer les contrôles de sécurité et de conformité pour les données utilisées par Microsoft 365 Copilot

Concevoir des solutions de sécurité pour les applications (2h00)
- Concevoir des standards et pratiques de sécurisation du développement applicatif
- Concevoir une stratégie cycle de vie complète pour la sécurité applicative
- Évaluer la posture de sécurité d'un portefeuille applicatif existant
- Évaluer les menaces applicatives par le threat modeling
- Sécuriser l'accès des workload identities
- Concevoir une solution de gestion et de sécurité des API
- Concevoir une solution d'accès sécurisé aux applications

Concevoir des solutions de sécurité pour les données de l'organisation (2h00)
- Évaluer des solutions de découverte et de classification des données avec Microsoft Purview
- Définir les priorités de réduction des menaces pesant sur les données
- Évaluer des solutions de chiffrement avec Azure Key Vault et l'infrastructure encryption
- Concevoir une solution de sécurité pour les données dans les workloads Azure
- Concevoir la sécurité des données utilisées dans les workloads IA
- Concevoir une solution de sécurité pour Azure Storage
- Concevoir une solution intégrant Defender for SQL et Defender for Storage

Étude de cas interactive : Sécuriser les applications et les données (1h30)
- Analyse d'un scénario d'architecture sécurité
- Évaluation des choix de sécurisation des applications et des données
- Comparaison et justification des solutions retenues

Spécifier les exigences de sécurité pour l'infrastructure cloud (1h30)
- Spécifier les baselines de sécurité pour les services SaaS, PaaS et IaaS
- Spécifier les exigences de sécurité pour les workloads IoT
- Spécifier les exigences de sécurité pour les workloads web
- Spécifier les exigences de sécurité pour les conteneurs et l'orchestration
- Spécifier les exigences de sécurité pour les services et workloads IA

Concevoir des solutions de gestion de la posture de sécurité en environnements hybrides et multicloud (1h30)
- Évaluer la posture de sécurité avec Microsoft Defender for Cloud, MCSB et Secure Score
- Sélectionner les solutions de cloud workload protection dans Defender for Cloud
- Concevoir une solution d'intégration hybride et multicloud avec Azure Arc
- Concevoir une solution avec Microsoft Defender External Attack Surface Management
- Spécifier les exigences de posture management avec Microsoft Security Exposure Management

Concevoir des solutions de sécurité pour les serveurs et les terminaux (1h30)
- Spécifier les exigences de sécurité pour les serveurs
- Spécifier les exigences de sécurité pour les appareils mobiles et les clients
- Spécifier les exigences de sécurité pour les objets IoT et systèmes embarqués
- Évaluer des solutions de sécurisation OT et ICS avec Microsoft Defender for IoT
- Spécifier les baselines de sécurité pour les serveurs et clients
- Concevoir une solution d'accès distant sécurisé
- Évaluer Windows Local Administrator Password Solution

Concevoir des solutions de sécurité réseau et de Security Service Edge (1h30)
- Évaluer des conceptions réseau alignées sur les exigences et bonnes pratiques de sécurité
- Évaluer des solutions utilisant Microsoft Entra Internet Access
- Évaluer des solutions utilisant Microsoft Entra Private Access

Étude de cas interactive : Sécuriser les terminaux et l'infrastructure (1h30)
- Analyse d'un scénario d'architecture sécurité
- Évaluation des choix de sécurisation des endpoints, de l'infrastructure et du réseau
- Comparaison et justification des solutions retenues

Documentation

Travaux pratiques et/ou Labo en anglais

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, le formateur évalue chaque stagiaire sur l'atteinte des objectifs pédagogiques de la formation selon quatre niveaux (non évalué, non acquis, en cours d'acquisition, acquis). Cette évaluation repose sur une modalité choisie par le formateur en cohérence avec la formation : QCM, exercices pratiques réalisés pendant la formation, évaluation finale de synthèse, quiz interactif de validation, étude de cas, mise en situation, analyse de l'auto-évaluation, autres modalités adaptées.
Pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification. Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes (ex : ITIL, DPO, ...), le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.
Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés.
Il est présent auprès des stagiaires pendant toute la durée de la formation.

Accessibilité de la formation