Présentiel/distanciel | Cours Officiel | Formation certifiante

Introduction à la sécurité, à la conformité et à l'identité Microsoft

Objectifs pédagogiques

- Décrire les concepts fondamentaux de sécurité, de conformité et d'identité dans l'écosystème Microsoft
- Décrire les principales fonctionnalités de Microsoft Entra pour l'identité, l'authentification, l'accès et la gouvernance
- Décrire les principales solutions de sécurité Microsoft, notamment Microsoft Defender, Microsoft Sentinel et Microsoft Security Copilot
- Décrire les principales solutions de confidentialité, de protection des données, de conformité et de gouvernance avec Microsoft Priva et Microsoft Purview
- Comprendre comment les solutions Microsoft Azure, Microsoft 365, Microsoft Entra, Microsoft Defender et Microsoft Purview s'articulent dans une approche de bout en bout

Prérequis

- Compréhension générale des concepts de réseau et de cloud computing
- Connaissances générales de l'informatique ou expérience dans un environnement de travail informatique
- Compréhension générale de Microsoft Azure et de Microsoft 365

Certification

Cette formation prépare à l'examen associé à la certification Microsoft Certified: Security, Compliance, and Identity Fundamentals

Public concerné

Cette formation s'adresse aux personnes qui souhaitent découvrir les bases de la sécurité, de la conformité et de l'identité dans les services cloud Microsoft.
Elle concerne un large public, notamment les parties prenantes métier, les professionnels de l'informatique débutants ou expérimentés ainsi que les apprenants qui s'intéressent aux solutions de sécurité, de conformité et d'identité Microsoft.

Bénéfices pour les participants :

- Acquérir une vision d'ensemble claire des offres Microsoft en sécurité, conformité et identité
- Comprendre les concepts essentiels avant d'aller vers des parcours plus spécialisés
- Identifier les grands rôles des solutions Microsoft Entra, Defender, Sentinel, Priva et Purview
- Préparer une première certification de niveau fondamental sur les technologies de sécurité Microsoft

Programme détaillé

Présentation des concepts de sécurité, de conformité et d'identité (1h00)

- Décrire le modèle de responsabilité partagée
- Décrire la défense en profondeur
- Décrire les principes et piliers du modèle Confiance Zéro
- Décrire les concepts de chiffrement et de hachage
- Décrire les concepts de gouvernance, de risque et de conformité
- Décrire l'authentification et l'autorisation
- Décrire l'identité comme nouveau périmètre de sécurité
- Décrire le rôle du fournisseur d'identité
- Décrire les services d'annuaire et le concept de fédération

Présentation de Microsoft Entra (2h00)

- Décrire les fonctionnalités principales de Microsoft Entra ID
- Décrire les types d'identités pris en charge par Microsoft Entra ID
- Décrire le concept d'identité hybride
- Décrire Microsoft Entra External ID
- Décrire les méthodes d'authentification de Microsoft Entra
- Décrire l'authentification multifacteur
- Décrire la réinitialisation de mot de passe en libre-service
- Décrire les fonctionnalités de gestion et de protection des mots de passe
- Décrire l'accès conditionnel et ses avantages
- Décrire l'accès sécurisé global
- Décrire les rôles Microsoft Entra ID et le contrôle d'accès en fonction du rôle
- Décrire la gouvernance des identités dans Microsoft Entra
- Décrire les révisions d'accès
- Décrire la gestion des droits d'utilisation et les conditions d'utilisation
- Décrire Privileged Identity Management
- Décrire Microsoft Entra Identity Protection
- Décrire l'intégration de Microsoft Entra avec Microsoft Security Copilot
- Décrire Microsoft Entra Verified ID

Présentation des solutions de sécurité Microsoft (2h00)

- Décrire Microsoft Security Copilot
- Décrire la terminologie, les usages, les espaces de travail et les assistants de Microsoft Security Copilot
- Décrire les principaux services de sécurité d'infrastructure dans Azure
- Décrire Azure DDoS Protection
- Décrire le Pare-feu Azure
- Décrire le pare-feu d'applications web
- Décrire la segmentation réseau, les réseaux virtuels Azure et les groupes de sécurité réseau
- Décrire Azure Bastion
- Décrire Azure Key Vault
- Décrire Microsoft Defender pour le cloud
- Décrire les initiatives et stratégies de sécurité pour améliorer la posture de sécurité cloud
- Décrire les piliers CSPM, CWPP et DevSecOps dans Microsoft Defender pour le cloud
- Décrire les concepts SIEM et SOAR
- Décrire Microsoft Sentinel et ses capacités de détection, d'investigation et de réponse
- Décrire l'intégration de Microsoft Security Copilot à Microsoft Sentinel
- Décrire Microsoft Defender XDR et ses composants
- Décrire Microsoft Defender for Office 365
- Décrire Microsoft Defender for Endpoint
- Décrire Microsoft Defender for Cloud Apps
- Décrire Microsoft Defender for Identity
- Décrire la gestion des vulnérabilités Microsoft Defender
- Décrire la veille des menaces Microsoft Defender
- Décrire le portail Microsoft Defender
- Décrire l'intégration de Microsoft Defender XDR à Microsoft Security Copilot

Présentation de Microsoft Priva et Microsoft Purview (2h00)

- Décrire le portail d'approbation des services Microsoft
- Décrire les principes de confidentialité de Microsoft
- Décrire Microsoft Priva
- Décrire les solutions de sécurité des données de Microsoft Purview
- Décrire la classification des données
- Décrire les types d'informations sensibles, les classifieurs, l'Explorateur de contenu et l'Explorateur d'activités
- Décrire les étiquettes et stratégies de confidentialité
- Décrire la prévention contre la perte de données
- Décrire Microsoft Purview Insider Risk Management
- Décrire la protection adaptative
- Décrire les solutions de conformité des données de Microsoft Purview
- Décrire Audit et eDiscovery dans Microsoft Purview
- Décrire Compliance Manager et le score de conformité
- Décrire la conformité des communications
- Décrire la gestion du cycle de vie des données, les étiquettes et stratégies de rétention
- Décrire la gestion des enregistrements
- Décrire les solutions de gouvernance des données de Microsoft Purview
- Décrire les avantages de la gouvernance des données
- Décrire Microsoft Purview Data Catalog

Introduction à la sécurité, à la conformité et à l'identité Microsoft

Présentiel/distanciel | Cours Officiel | Formation certifiante

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, 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