

Durée : 1 jour soit 7 heures

Référence : SC-900T00



Public visé :

Cette formation est destinée à toutes les personnes qui souhaitent se familiariser avec les principes fondamentaux de la sécurité, de la conformité et de l'identité (SCI) dans les services Microsoft basés dans le Cloud et associés.

Ce cours est destiné aux informaticiens qui souhaitent se préparer et passer la certification SC-900T00.



Pré-requis :

Pour suivre cette formation, les apprenants doivent :

- Avoir une compréhension générale des concepts de réseautage et de Cloud Computing.
- Connaissances générales en informatique ou toute expérience générale de travail dans un environnement informatique.
- Compréhension générale de Microsoft Azure et Microsoft 365.



Objectifs pédagogiques :

A l'issue de la formation, les apprenants auront acquis les compétences suivantes :

- Décrire les concepts de base de la sécurité, de la conformité et de l'identité.
- Décrire les concepts et les capacités des solutions de gestion des identités et des accès Microsoft.
- Décrire les capacités des solutions de sécurité Microsoft.
- Décrire les fonctionnalités de gestion de la conformité dans Microsoft.



Compétences acquises à l'issue de la formation :

- Comprendre et expliquer les concepts fondamentaux de la sécurité, de la conformité et de l'identité dans un environnement Microsoft Cloud.
- Maîtriser les principes de sécurité et de conformité appliqués aux solutions Microsoft.
- Expliquer le rôle et les fonctionnalités d'Azure Active Directory (Azure AD) dans la gestion des identités, de l'authentification et des accès.
- Décrire les principales solutions de sécurité de Microsoft Azure et Microsoft 365.
- Présenter les capacités des outils de protection contre les menaces, tels qu'Azure Sentinel et Microsoft Defender.
- Expliquer les stratégies de conformité et les outils Microsoft 365 et Azure permettant de protéger les informations et de gérer la gouvernance.
- Identifier les fonctionnalités d'audit et de gestion des risques pour assurer la surveillance et l'analyse des menaces et des conformités.



Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure. La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz. L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration. En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Note relative au programme : Les ateliers, démonstrations, travaux pratiques et scénarios présentés dans ce programme sont fournis à titre d'exemples illustratifs et ne sont pas exhaustifs. Afin de garantir une adéquation permanente avec les évolutions technologiques, le contenu pédagogique ainsi que les environnements de travaux pratiques (TP) sont susceptibles d'être adaptés, ajustés ou mis à jour au cours du temps.



Moyens et supports pédagogiques :

Cadre présentiel

Salles de formation équipées et accessibles aux personnes à mobilité réduite.

- Un poste de travail par participant

IFORM : Agence de Balma : 16 avenue Charles de Gaulle, bâtiment 13, 31130 Balma

Siège social : Mbe 308 46 rue André Vasseur 31200 TOULOUSE

Tél : 05 61 34 39 80 • SIRET : 431 421 742 00096 • APE : 6202A



- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel

Session dispensée via notre solution iClassRoom s'appuyant sur Microsoft Teams.

- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique



Modalités d'évaluation et de suivi :

Avant

Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice), qui valide la base de connaissances nécessaires.

Les stagiaires disposent également, depuis leur extranet, d'un **outil d'auto-positionnement** leur permettant d'évaluer leur niveau de maîtrise des compétences visées par la formation. Cette auto-évaluation est réalisée avant le démarrage de la formation à l'aide d'un curseur de positionnement allant du niveau le plus faible au niveau le plus élevé.

Pendant

Après chaque module théorique, un ou plusieurs ateliers pratiques permettent de valider progressivement l'acquisition des connaissances. Un quiz peut accompagner les ateliers pratiques afin de mesurer la compréhension des notions abordées.

Après

À l'issue de la formation, les stagiaires réalisent une nouvelle **auto-évaluation** sur les mêmes compétences que celles évaluées avant la formation. Cette comparaison permet de mesurer leur perception de la progression réalisée et de visualiser les compétences développées au cours de la formation.

Lorsque le programme de formation le prévoit, un examen de certification est organisé conformément aux modalités définies par l'éditeur ou le centre de certification (TOSA, Pearson VUE, ENI, PeopleCert...).

Le formateur réalise également une **évaluation individuelle des compétences** de chaque stagiaire sur l'ensemble des compétences visées par la formation. Pour chacune d'elles, il indique si la compétence est :

- Acquis ;
- En cours d'acquisition ;
- Non acquise.

Lorsque la compétence est évaluée comme **en cours d'acquisition** ou **non acquise**, le formateur formule des observations précisant les difficultés rencontrées ainsi que les actions ou recommandations permettant au stagiaire de poursuivre sa montée en compétences.

Enfin

Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation de formation.



Informations sur l'accessibilité :

Nos formations sont, dans la mesure du possible, conçues pour être accessibles à toutes et à tous. Afin de garantir les meilleures conditions d'accueil et d'apprentissage pour les personnes en situation de handicap, nous vous invitons à contacter notre référente handicap certifiée :

Céline SOLATGES – 05 61 34 39 80 – csolatges@iform.fr

Nous vous remercions de bien vouloir nous communiquer toute information utile à ce sujet en amont de la formation, afin de mettre en place les adaptations nécessaires et d'assurer un accompagnement optimal.

Pour en savoir plus sur les dispositifs d'accompagnement existants, vous pouvez consulter les sites suivants :

- [AGEFIPH](#)
- [FIPHFP](#)

- MDPH de votre département

Description / Contenu

Module 1 : Décrire les concepts de base de la sécurité, de la conformité et de l'identité.

- Décrire les concepts et méthodologies de sécurité.
- Décrire les principes de sécurité et de conformité de Microsoft.

- Décrire les capacités de gouvernance des ressources dans Azure

Module 2 : Décrire les concepts et les capacités des solutions de gestion des identités et des accès Microsoft

- Décrire les concepts d'identité
- Décrire les services de base et les types d'identité d'Azure AD
- Décrire les capacités d'authentification d'Azure AD
- Décrire les capacités de gestion des accès d'Azure AD
- Décrire les capacités de protection des identités et de gouvernance d'Azure AD

Module 3 : Décrire les capacités des solutions de sécurité Microsoft

- Décrire les fonctionnalités de sécurité de base dans Azure
- Décrire les capacités de gestion de la sécurité d'Azure
- Décrire les capacités de sécurité d'Azure Sentinel
- Décrire les capacités de protection contre les menaces de Microsoft 365
- Décrire les capacités de gestion de la sécurité de Microsoft 365
- Décrire la sécurité des points de terminaison avec Microsoft Intune
- Résumé du module

Module 4 : Décrire les capacités des solutions de conformité Microsoft

- Décrire les capacités de gestion de la conformité dans Microsoft
- Décrire les capacités de protection des informations et de gouvernance de Microsoft 365
- Décrire les capacités de risque d'initié dans Microsoft 365
- Décrire les capacités de découverte électronique de Microsoft 365
- Décrire les capacités d'audit de Microsoft 365