Smartfuture
Certifications | Training | Technology solutions

Formation & Certification • SC-900

Microsoft Security, Compliance, and Identity Fundamentals

Formation en distanciel (présentiel sur demande). Maîtrisez les concepts d'identité, de sécurité et de conformité et découvrez l'écosystème Microsoft (Entra, Defender, Purview, Priva, Sentinel…).

Distributeur officiel Certiport | Centre d'examen Certiport

Learn • Practice • Certify

Durée	Examen
13.5 h	SC-900
Modalité	**Niveau**
Distanciel	Fondamental

INSCRIPTION / RÉSERVATION

Je m'inscris maintenant

- **Learn** : accès au cours officiel Microsoft Learn aligné sur le plan d'examen SC-900.
- **Practice** : accès à un simulateur d'examen interactif pour s'entraîner dans les conditions réelles.
- **Certify** : voucher officiel de passage d'examen SC-900 inclus.

OBJECTIFS PÉDAGOGIQUES

- Expliquer les notions clés : concepts de sécurité, identité, accès, gouvernance, confidentialité et conformité.
- Décrire les capacités de Microsoft Entra (gestion des identités, accès conditionnel, MFA, protection des identités, gouvernance).
- Présenter les solutions de sécurité Microsoft (Defender, Sentinel) et leurs cas d'usage.
- Présenter les solutions de conformité et de protection des informations (Purview, Priva, eDiscovery, DLP, enregistrements).
- Se préparer efficacement à l'examen SC-900.

PUBLIC CIBLE

- Débutants en sécurité/identité/compliance souhaitant une base solide.
- Fonctions non techniques (vente, avant-vente, gestion, PMO, RH, juristes, conformité).
- Étudiants, personnes en reconversion vers la cybersécurité et la gouvernance des données.

PRÉREQUIS

- Aucun prérequis technique obligatoire.
- Une culture IT générale est un plus.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Décrire les concepts de sécurité, de conformité et d'identité (≈10–15%)

Notions fondamentales de sécurité

- Principes de sécurité (confidentialité, intégrité, disponibilité) et défense en profondeur.
- Stratégie Zero Trust : vérifier explicitement, appliquer le moindre privilège, supposer la compromission.
- Contrôles de sécurité : prévention, détection, investigation, réponse.

Notions d'identité et d'accès

- Identité, authentification (mot de passe, MFA, sans mot de passe), autorisation, RBAC.
- SSO, fédération, protocoles (SAML, OIDC, OAuth 2.0) – concepts et usages.

Notions de conformité et de confidentialité

- Gouvernance, gestion des risques et conformité (GRC) : politiques, contrôles, preuves.
- Confidentialité : principes, demandes des personnes concernées, obligations réglementaires (exemples : RGPD).

Décrire les fonctionnalités de Microsoft Entra (≈20–25%)

Gestion des identités & annuaire cloud

- Présentation de Microsoft Entra ID (ex-Azure AD) : utilisateurs, groupes, unités administratives.
- Synchronisation d'identité (Entra Connect/Cloud Sync), intégration on-prem.
- Authentification : MFA, mot de passe, FIDO2, Windows Hello, authentification sans mot de passe.

Gestion des accès & sécurité d'accès

- Accès conditionnel : signaux (utilisateur, appareil, emplacement, risque), contrôles (MFA, conformité appareil, session).

PROGRAMME DE LA FORMATION – DÉTAILLÉ

- Protection des identités : détection du risque utilisateur/connexion, réponses automatisées.
- RBAC, PIM (Privileged Identity Management) pour les rôles à privilèges avec approbation et durée limitée.

Gouvernance des identités

- Gestion du cycle de vie des identités, packages d'accès, approbations, campagnes de revue d'accès.
- Accès externe & B2B : invités, collaboration sécurisée, listes d'autorisation/interdiction de domaines.

Entra Permissions Management & Workload Identities (vue d'ensemble)

- Gestion des permissions multicloud (CIEM).
- Identités de charges de travail (applications, services) et stratégies d'accès.

Décrire les solutions de sécurité Microsoft (≈35–40%)

- Détection & réponse étendues (XDR) – Microsoft Defender
- Panorama Defender (suite) : Defender for Endpoint, for Office 365, for Identity, for Cloud Apps, Defender for Cloud (CSPM/CWPP).
- Cas d'usage : protection endpoint, investigations, chasse aux menaces, protection email & collaboration, détection d'activités anormales.
- Intégrations et corrélation d'alertes, automatisation (SOAR) avec Logic Apps/Playbooks.

SIEM/SOAR – Microsoft Sentinel

- Principes SIEM/SOAR, connecteurs de données (Microsoft, SaaS, on-prem), normalisation.
- Règles d'analytique, incidents, investigation, notebooks, réponses automatisées.

Protection des identités & accès

- Identity Protection, Accès conditionnel, MFA, PIM – mise en contexte avec la stratégie Zero Trust.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Sécurité des applications & données

- Gestion des applications (catalogue, consentements, autorisations), Cloud Apps – découverte Shadow IT, session control.
- Chiffrement, clés, secrets et gestion (aperçu des approches dans l'écosystème Microsoft).

Sécurité multicloud & posture

- Defender for Cloud : évaluation de posture (CSPM), recommandations, protections des workloads (CWPP), conformité.

Décrire les solutions de conformité, gouvernance et protection de l'information (≈25–30%)

- Microsoft Purview – Protection & Gouvernance des données
- Classification et étiquetage de sensibilité (labels, politiques d'étiquetage automatique/manuelle).
- Protection de l'information (chiffrement, marquage, restrictions), suivi des activités.
- DLP (Data Loss Prevention) : emplacements (Exchange, SharePoint, OneDrive, Teams, endpoints), règles, incidents, rapports.
- Gestion des enregistrements : politiques de rétention, suppressions, dispositions, conservation pour litiges.
- eDiscovery (Standard/Premium) : identification, conservation, collecte, analyse, export.
- Audit : types d'événements, recherche, conservation des logs, scénarios d'enquête.
- Content Search et outils de découverte dans Microsoft 365.

Microsoft Priva – Gestion de la confidentialité

- Découverte des données personnelles, insights de confidentialité, principes de minimisation.
- Gestion des demandes des personnes concernées (DSR), flux de traitement.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Score de conformité & régulations

- Microsoft Compliance Manager : évaluations, contrôles, modèles réglementaires (exemples : RGPD, ISO 27001).
- Gestion des risques internes (aperçu) : politiques, alertes, investigations.

Atelier & mise en pratique (optionnel)

Scénarios guidés

- Configurer un accès conditionnel simple (MFA requis hors réseau de confiance).
- Créer un label de sensibilité Purview et tester un scénario DLP.
- Découvrir les tableaux de bord Defender/Sentinel et simuler une investigation.