

# Microsoft Copilot for Security – Sécuriser son SI

1 jour (7 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

**975 € HT** par personne (TVA en vigueur) **Repas inclus en présentiel**

Contenu mis à jour le 25/09/2026. Document téléchargé le 03/10/2026.

## Objectifs

A l'issue de cette formation, vous serez capable de :

- Identifier le rôle de Microsoft Copilot for Security dans l'écosystème Microsoft 365 et Microsoft Security
- Configurer les principaux paramètres d'administration, les accès, les plugins et les connecteurs nécessaires à son exploitation
- Utiliser les prompts, promptbooks et agents pour accompagner l'analyse, l'investigation et la remédiation
- Encadrer l'usage de la solution en tenant compte de la gouvernance, de l'audit, des données manipulées et des limites opérationnelles.

Les compétences visées par cette formation font l'objet d'une évaluation.

## À qui s'adresse cette formation ?

Administrateurs systèmes, administrateurs SSI, ingénieurs en sécurité ou toute personne ayant des fonctions SSI.

### Prérequis

Avoir suivi la formation M365-ADM "Microsoft 365 – Administrer la suite complète" ou avoir les connaissances équivalente. Une expérience confirmée de l'administration d'environnements Microsoft 365 est recommandée.

# Programme

## 1 Pendant votre formation

### Microsoft Copilot for Security – Sécuriser son SI

#### Microsoft Copilot for Security : positionnement et architecture

- Positionnement de Microsoft Copilot for Security dans les usages de cybersécurité et d'administration Microsoft 365
- Fonctionnement des sessions, prompts, agents, promptbooks, plugins et connecteurs
- Préparation de l'environnement : prérequis techniques, permissions, accès et licences
- Notions essentielles de licensing : capacité SCU, provisionnement, consommation et impacts sur l'exploitation
- Intégrations avec Microsoft Defender XDR, Microsoft Sentinel, Microsoft Entra, Microsoft Intune et Microsoft Purview
- Points de vigilance liés aux responsabilités administrateur, à la confidentialité et aux limites d'usage

#### Administrer et configurer Microsoft Copilot for Security

- Accès à l'expérience Copilot for Security et paramétrage initial de la solution
- Sélection et contrôle des plugins Microsoft, partenaires ou personnalisés
- Gestion des rôles, des autorisations et des données accessibles via les connecteurs

#### Exploiter les prompts, promptbooks et agents

- Formulation de demandes efficaces et utilisation de la bibliothèque de prompts
- Utilisation de promptbooks pour l'investigation d'incidents, l'analyse utilisateur, la veille de menace et l'évaluation de vulnérabilités
- Conception d'un promptbook adapté à un processus de sécurité récurrent
- Rôle des agents et articulation avec les prompts, les plugins et les données disponibles
- Adaptation des usages selon les profils : administrateur, analyste SOC, threat intelligence ou IT admin
- Lecture critique des réponses, vérification des sources et prise en compte des limites de l'IA générative
- Structuration des résultats pour faciliter l'analyse, la décision et la remédiation

#### Cas d'usage opérationnels et intégrations de sécurité

- Investigation d'alertes, qualification d'incidents, analyse de scripts suspects et synthèse de menace
- Analyse de posture, priorisation des risques, recommandations de remédiation et restitution exploitable

#### Supervision, audit et gouvernance

- Suivi de l'usage, consultation de l'historique, exploitation des journaux d'audit et encadrement des pratiques d'administration
- Définition de règles d'usage pour les prompts, les agents, les accès et les extensions personnalisées

#### Exemples de travaux pratiques (à titre indicatif)

- Configurer les accès, les paramètres initiaux et les plugins utiles à l'exploitation de Copilot for Security

- Utiliser un promptbook pour conduire une investigation sur un incident ou une menace
- Créer un promptbook réutilisable pour structurer une analyse de sécurité récurrente

## Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

Nous contacter pour en savoir plus →

## Modalités pédagogiques

Formation délivrée en présentiel ou distanciel\* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode\*\* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

\* nous consulter pour la faisabilité en distanciel

\*\* ratio variable selon le cours suivi

### Accessibilité aux personnes en situation de handicap

## Détails de la session

Le 7 décembre 2026 (1 jour / 7 heures)

Mulhouse

Le 7 décembre 2026

Mulhouse

- 7 décembre 2026 ..... 9h00 – 17h00