Programme de cours
Améliorer les opérations de sécurité à l'aide de Microsoft Security Copilot

Durée : 1 jour soit 7 heures | Référence : SC-5006

Public visé :

Cette formation s'adresse principalement à des professionnels de la sécurité informatique, plus précisément ceux ayant déjà une expérience pratique dans les opérations de sécurité et la réponse aux incidents. Le public cible inclut donc les administrateurs de sécurité, les analystes de sécurité, les ingénieurs en sécurité ou tout autre professionnel impliqué dans la gestion et la sécurisation des infrastructures informatiques, avec une connaissance préalable des services et produits de sécurité Microsoft.

Pré-requis :

- Connaissance pratique des opérations de sécurité et de la réponse aux incidents
- Connaissance pratique des services et produits de sécurité Microsoft

Objectifs pédagogiques :

- Comprendre la place de l'IA générative dans le développement de l'intelligence artificielle
- Comprendre les modèles de langage et leur rôle dans les applications intelligentes
- Décrire des exemples de co-pilotes et de bons prompts
- Décrire ce qu'est Microsoft Security Copilot
- Expliquer la terminologie de Microsoft Security Copilot
- Décrire comment Microsoft Security Copilot traite les demandes de prompts
- Décrire les éléments d'un prompt efficace
- Expliquer comment activer Microsoft Security Copilot
- Décrire les fonctionnalités disponibles dans l'expérience autonome de Copilot
- Décrire les plugins disponibles dans Copilot
- Décrire les guides de prompts personnalisés
- Décrire les connexions à la base de connaissances
- Décrire Copilot dans Microsoft Defender XDR
- Décrire Copilot dans Microsoft Purview
- Décrire Copilot dans Microsoft Entra
- Décrire Copilot dans Microsoft Intune
- Décrire Copilot dans Microsoft Defender pour le Cloud
- Configurer Microsoft Security Copilot
- Utiliser les sources dans Copilot
- Créer une séquence de prompts personnalisée
- Utiliser les fonctionnalités de Copilot dans Defender XDR
- Utiliser les fonctionnalités de Copilot dans Microsoft Purview

Compétences acquises à l'issue de la formation :

- Comprendre l'IA générative et son rôle dans l'amélioration des opérations de sécurité
- Maîtriser l'utilisation des modèles de langage et des co-pilotes pour améliorer la sécurité
- Appliquer les bonnes pratiques pour créer des prompts efficaces dans Microsoft Security Copilot
- Activer et configurer Microsoft Security Copilot pour une utilisation optimale
- Explorer et utiliser les fonctionnalités de Microsoft Security Copilot dans un environnement de sécurité autonome
- Intégrer Microsoft Security Copilot avec les services Microsoft de sécurité (Defender XDR, Purview, Entra, Intune, Defender pour le Cloud)
- Utiliser les plugins et guides de prompts personnalisés dans Microsoft Security Copilot
- Configurer et exploiter des séquences de prompts personnalisées pour des cas d'utilisation spécifiques

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
- 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 :

- Acquise ;
- 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 : Bases de l'IA générative

- Qu'est-ce que l'IA générative ?
- Qu'est-ce qu'un modèle de langage ?
- Utilisation des modèles de langage
- Qu'est-ce qu'un co-pilote ?
- Microsoft Copilot
- Considérations pour les prompts de Copilot
- Extension et développement des co-pilotes
- Exercice – Explorer Microsoft Copilot

Module 2 : Décrire la sécurité de Microsoft Copilot

- Se familiariser avec Microsoft Security Copilot
- Décrire la terminologie de Microsoft Security Copilot
- Expliquer comment Microsoft Security Copilot traite les demandes de prompts
- Décrire les éléments d'un prompt efficace
- Expliquer comment activer Microsoft Security Copilot

Module 3 : Décrire les fonctionnalités de base de Microsoft Security Copilot

- Décrire les fonctionnalités disponibles dans l'expérience autonome de Microsoft Security Copilot
- Décrire les fonctionnalités disponibles dans une session d'expérience autonome
- Décrire les plugins Microsoft disponibles dans Microsoft Security Copilot
- Décrire les plugins non-Microsoft pris en charge par Microsoft Security Copilot
- Décrire les guides de prompts personnalisés
- Décrire les connexions à la base de connaissances

Module 4 : Décrire les expériences intégrées de Microsoft Security Copilot

- Décrire Copilot dans Microsoft Defender XDR
- Copilot dans Microsoft Purview
- Copilot dans Microsoft Entra
- Copilot dans Microsoft Intune
- Copilot dans Microsoft Defender pour le Cloud (Aperçu)

Module 5 : Explorer les cas d'utilisation de Microsoft Security Copilot

- Découvrir l'expérience de première utilisation
- Découvrir l'expérience autonome
- Configurer le plugin Microsoft Sentinel
- Activer un plugin personnalisé
- Découvrir les téléchargements de fichiers via une base de connaissances
- Créer une séquence de prompts personnalisée
- Explorer les fonctionnalités de Copilot dans Microsoft Defender XDR
- Explorer les fonctionnalités de Copilot dans Microsoft Purview