Durée : 1 jour soit 7 heures

Référence : SC-5004

Public visé :

Profils et métiers visés :

- Analyste sécurité ou analyste SOC chargé de traiter les incidents et les alertes (modules 1, 5 et 6).
- Administrateur sécurité chargé de déployer et configurer Defender for Endpoint (modules 2 à 4).
- Administrateur systèmes ou administrateur de postes de travail impliqué dans la sécurité des terminaux (déduction).
- Ingénieur, consultant ou intégrateur en sécurité Microsoft (déduction).
- *Ne conviennent pas :* les profils non techniques, ni les personnes qui cherchent une vue d'ensemble de toute la gamme Defender XDR (messagerie, identités, applications cloud). Ces produits ne sont pas traités.

Niveau attendu : intermédiaire. La formation suppose des bases en sécurité et en administration de postes. Elle ne demande aucune expérience préalable de Defender for Endpoint, puisqu'elle en couvre le déploiement.

Pré-requis :

Prérequis indispensables

- **Connaissances fondamentales en cybersécurité** : types de menaces et d'attaques courantes, notions d'alerte, d'incident et de correction. La formation entre directement dans l'investigation, sans module d'introduction à la sécurité.
- **Bonne pratique de l'administration de postes de travail Windows** dans un environnement d'entreprise. Elle est nécessaire pour intégrer les appareils, examiner un appareil et comprendre les actions de correction.
- **Notions de base sur Microsoft Entra ID et l'environnement Microsoft 365** (comptes, rôles d'administration). Elles servent pour la gestion des accès et des rôles RBAC, ainsi que pour lire les journaux de connexion Entra.

Prérequis recommandés (non obligatoires)

- Avoir des notions de KQL, utiles pour tirer parti de la découverte de la chasse avancée.
- Connaître dans les grandes lignes les solutions de sécurité Microsoft, au niveau « fondamentaux ». La référence SC-900 est ma suggestion : le document ne la cite pas.
- Savoir comment on déploie des outils sur un parc de postes (stratégies de groupe, solution de gestion des appareils). Le document ne précise pas les méthodes d'intégration utilisées : cette recommandation est une déduction.
- Savoir lire l'anglais technique, *si les supports ou les labs sont en anglais.*

Objectifs pédagogiques :

À l'issue de la formation, les participants seront en mesure de :

- **Utiliser et configurer** le portail Microsoft Defender.
- **Déployer** Microsoft Defender for Endpoint : créer l'environnement, vérifier la compatibilité des systèmes d'exploitation, intégrer les appareils, définir les rôles RBAC et les groupes d'appareils.
- **Configurer** les notifications d'alerte, les règles de suppression d'alertes et les indicateurs.
- **Configurer** l'investigation et la correction automatisées, ainsi que le blocage des appareils à risque.
- **Gérer et examiner** les incidents et les alertes, puis **suivre** les investigations automatisées dans le centre de notifications.
- **Examiner** un appareil à partir de l'inventaire et de la découverte d'appareils, et **décrire** le principe du blocage basé sur le comportement.
- **Identifier** les autres ressources d'analyse du portail : chasse avancée (découverte), journaux de connexion Microsoft Entra, Microsoft Secure Score, rapports, agent Threat Intelligence Briefing de Security Copilot.

Compétences acquises à l'issue de la formation :

- Être capable de déployer l'environnement Microsoft Defender for Endpoint : créer l'environnement, vérifier la compatibilité des systèmes d'exploitation, intégrer les appareils, gérer les accès (rôles RBAC), organiser les groupes d'appareils et configurer le portail Microsoft Defender.
- Être capable de paramétrer la détection et la réponse automatisée dans Defender for Endpoint : notifications d'alerte, suppression d'alertes, indicateurs, investigation et correction automatisées, paramètres de chargement de fichiers et de

dossiers, blocage des appareils à risque.
- Être capable d'examiner et de traiter les incidents et les alertes dans le portail Microsoft Defender : trier et examiner les incidents et les alertes, analyser un appareil (inventaire, page de l'appareil, découverte d'appareils), suivre les investigations automatisées dans le centre de notifications, puis prendre les mesures d'atténuation.

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

La formation Administrateur de la sécurité de l'information vous permet de mettre en œuvre l'environnement Microsoft Defender for Endpoint afin de gérer les appareils, mener des investigations sur les points de terminaison, gérer les incidents dans Defender XDR et utiliser la chasse avancée avec Kusto Query Language (KQL) pour détecter des menaces spécifiques.

Module 1 : Atténuer les incidents avec Microsoft Defender

- Utiliser le portail Microsoft Defender
- Gérer les incidents
- Examiner les incidents
- Gérer et examiner les alertes
- Gérer les investigations automatisées
- Utiliser le centre de notifications
- Explorer la chasse avancée
- Examiner les journaux de connexion Microsoft Entra
- Comprendre Microsoft Secure Score
- Analyser les menaces avec l'agent Threat Intelligence Briefing de Security Copilot
- Analyser les rapports
- Configurer le portail Microsoft Defender

Module 2 : Déployer l'environnement Microsoft Defender for Endpoint

- Créer votre environnement
- Comprendre la compatibilité et les fonctionnalités des systèmes d'exploitation Intégrer les appareils
- Gérer les accès
- Créer et gérer les rôles pour le contrôle d'accès en fonction du rôle
- Configurer les groupes d'appareils
- Configurer les fonctionnalités avancées de l'environnement

Module 3 : Configurer les alertes et les détections dans Microsoft Defender for Endpoint

- Configurer les fonctionnalités avancées
- Configurer les notifications d'alerte
- Gérer la suppression des alertes
- Gérer les indicateurs

Module 4 : Configurer et gérer l'automatisation avec Microsoft Defender for Endpoint

- Configurer les fonctionnalités avancées
- Gérer les paramètres de chargement et de dossier pour l'automatisation
- Configurer les fonctionnalités d'investigation et de correction automatisées
- Bloquer les appareils à risque

Module 5 : Mener des investigations sur les appareils dans Microsoft Defender for Endpoint

- Utiliser la liste d'inventaire des appareils
- Examiner un appareil Utiliser le blocage basé sur le comportement
- Détecter les appareils à l'aide de la découverte d'appareils

Module 6 : Exercices pratiques : se défendre contre les cybermenaces avec Microsoft Defender XDR

- Configurer l'environnement Microsoft Defender XDR
- Déployer Microsoft Defender for Endpoint
- Atténuer les attaques avec Microsoft Defender for Endpoint