Référence: SC-200

MFE-IT

Formation Microsoft 365 et Azure SC-200

Maîtrisez l'analyse et la réponse aux menaces dans Microsoft 365 et Azure

---

Durée: 4 jours | 28 h

Distanciel · Sessions garanties dès 1 inscrit · 60 % de pratique

DESCRIPTION

Cette formation Microsoft 365 vous donne les compétences pour assurer les missions d'un analyste en opérations de sécurité : détection proactive, investigation, réponse aux incidents et sécurisation de l'environnement hybride Microsoft.

Face à la montée des cybermenaces, Microsoft a intégré des outils puissants (Defender, Sentinel, Purview…) pour détecter, analyser et contenir les attaques. Le rôle de l'analyste en sécurité n'a jamais été aussi central.

OBJECTIFS PÉDAGOGIQUES

À l'issue de cette formation, les participants seront capables de :

- Comprendre les rôles et responsabilités d'un analyste SOC sur Microsoft.
- Déployer et configurer Microsoft Defender pour Endpoint, Identity, Office 365 et Cloud Apps.
- Utiliser Microsoft Sentinel pour collecter, corréler et investiguer des alertes.
- Réaliser des investigations guidées, définir des règles de détection (KQL), gérer les incidents.
- Créer des playbooks automatisés pour la réponse aux menaces.

PRÉREQUIS

- Connaissance des fondamentaux de Microsoft 365 / Azure.
- Notions de sécurité informatique, SIEM, incidents ou journalisation.

> Parce que chaque participant est unique, un entretien personnalisé est systématiquement organisé en amont avec notre expert afin de concevoir un programme parfaitement aligné sur ses objectifs, son niveau et ses enjeux professionnels.

PUBLIC VISÉ

Analystes SOC, administrateurs Microsoft 365/Azure, consultants ou toute personne souhaitant monter en compétence sur la défense active dans les environnements Microsoft.

PROGRAMME DÉTAILLÉ

> La formation alterne apports théoriques et pratique (environ 60 % du temps). Les modules s'articulent autour d'exercices concrets basés sur des cas d'usage métier réels.

Module 1 – Introduction à la cybersécurité Microsoft et rôle d'un analyste SOC

- Panorama des outils de sécurité Microsoft.
- Rôles Blue Team, MITRE ATT&CK.
- Architecture de surveillance.

Module 2 – Microsoft Defender for Endpoint et Identity

- Déploiement, configuration, alertes.
- Détection comportementale, investigation locale.
- Remédiation automatisée.

Module 3 – Microsoft Defender for Office 365 et Cloud Apps

- Analyse de Defender for Office 365 et Cloud Apps (MCAS).
- Politiques DLP.
- Alertes d'accès et comportement utilisateur.

Module 4 – Microsoft Sentinel (SIEM/SOAR)

- Architecture et connecteurs de données.
- Analyse KQL, investigation, carnet d'investigation.
- Gestion des incidents.

Module 5 – Automatiser la réponse aux menaces

- Playbooks avec Logic Apps.
- Enrichissement automatique, réponse pilotée par règles.
- Scénarios d'automatisation.

MODALITÉS PÉDAGOGIQUES

Format et déroulement

La formation est dispensée à distance via une classe virtuelle interactive. Elle peut également être réalisée sur site, avec un contenu personnalisé selon les besoins de votre projet professionnel. La répartition théorie/pratique est d'environ 40 %/60 %.

Format ultra-personnalisé MFE-IT

Chaque session accueille de 1 à 3 participants, garantissant un accompagnement très individualisé. Un entretien préalable permet d'adapter le contenu au profil de chacun. Les sessions inter-entreprises sont garanties dès 1 inscrit (sauf cas de force majeure).

Évaluation des compétences

Tout au long de la formation, le formateur évalue la progression des participants par des QCM, des mises en situation et des travaux pratiques. À la fin, une attestation de validation des acquis est remise à chaque participant.

Suivi post-formation

Pendant un mois après la formation, chaque participant peut contacter les formateurs MFE-IT pour toute question sur la mise en œuvre des acquis. Une réponse est apportée par e-mail ou téléphone sous 48 heures ouvrées.

Accessibilité

MFE-IT s'engage à accueillir les personnes en situation de handicap. Contact : contact@mfe-it.com.

INFORMATIONS PRATIQUES

Ressources formateur

- Démonstrations structurées alignées sur le programme détaillé
- Énoncés d'exercices et corrigés tout au long de la formation
- Un environnement technique prêt à l'emploi pour les ateliers pratiques
- Validation des acquis par le formateur à la fin de chaque atelier
- Documents de référence numériques

Certification et validation

À l'issue de la formation, une attestation est envoyée par e-mail précisant les objectifs, la nature, la durée et les résultats de l'évaluation. Un certificat de réalisation peut également être fourni sur demande.

Bénéfices pour les participants

- Se former depuis son lieu de travail ou son domicile, sans déplacement
- Bénéficier d'un formateur-consultant expert du sujet
- Profiter d'un format ultra-personnalisé (1 à 3 participants)
- Poursuivre la formation même en cas d'imprévu

Bénéfices pour l’organisation

- Optimiser le budget formation en réduisant déplacements et hébergements
- Offrir une formation de qualité à tous les collaborateurs, où qu’ils soient
- Réduire le temps d’absence lié aux déplacements
- Accompagner la montée en compétences des équipes dans tous les contextes