MFE-IT
Mes Formations d'Expertise

Référence : SC-5001

Formation Microsoft Sentinel SC-5001

SIEM et opérations de sécurité avancées

Durée : **1 jour** | Volume horaire : **6 h**

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

DESCRIPTION

Cette formation Microsoft Sentinel vous apprend à configurer, exploiter et superviser une plateforme de sécurité SIEM/SOAR moderne dans Azure.

Vous apprendrez à collecter, analyser et corréler des événements de sécurité provenant de sources variées, à écrire des requêtes KQL pour extraire des insights et à créer des règles de détection efficaces.

Le parcours inclut aussi la création de dashboards personnalisés, l'automatisation via des playbooks Azure Logic Apps, et les flux de travail d'un SOC opérationnel. Des ateliers pratiques basés sur des scénarios réels vous permettront d'identifier et de répondre à des menaces de cybersécurité.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, le participant sera capable de :

- Comprendre les fondamentaux de la cybersécurité SIEM/SOAR dans un environnement cloud.
- Maîtriser la configuration, l'administration et la supervision d'Azure Sentinel.
- Collecter, normaliser et analyser des données de sécurité à partir de sources variées.
- Implémenter des règles de détection, des analyses comportementales et des playbooks d'automatisation.
- Développer des dashboards et des rapports exploitables pour la cyberveille opérationnelle.
- Appliquer les bonnes pratiques pour opérer un SOC SIEM/SOAR moderne.

PRÉREQUIS

- Connaissances de base en cybersécurité, réseaux et modèles de menaces.
- Notions de logs, événements système et syntaxe KQL (une introduction est un plus).
- Familiarité avec Microsoft Azure : portail, ressources, RBAC.

Parce que chaque participant est unique, un entretien personnalisé en amont avec notre expert nous permet de concevoir une formation parfaitement alignée avec ses objectifs, son niveau et ses enjeux professionnels.

PUBLIC VISÉ

- Ingénieurs sécurité et analystes SOC.
- Responsables SIEM et architectes sécurité.
- Administrateurs cloud et DevOps impliqués dans la supervision.
- Consultants en cybersécurité souhaitant maîtriser Microsoft Sentinel.

PROGRAMME DÉTAILLÉ

La formation alterne apports théoriques et travaux pratiques (environ 60 % du temps). Les modules sont construits autour d'exercices concrets reprenant les cas d'usage du métier visé.

Introduction à SIEM et SOAR

- Concepts clés SIEM : Security Information and Event Management.
- Principes SOAR : Security Orchestration, Automation and Response.
- Vue d'ensemble des fonctionnalités d'Azure Sentinel.
- Positionnement par rapport aux autres SIEM du marché.

Architecture et collecte des données

- Architecture Sentinel et workspaces Log Analytics.
- Connecteurs de données : Azure, Windows, Linux, firewalls, Microsoft 365, sources tierces.
- Normalisation des logs et formats ASIM.
- Stratégie de rétention et gestion des coûts.

Kusto Query Language (KQL)

- Principes de base du langage KQL.
- Requêtes de recherche, agrégations et visualisation de tendances.
- Optimisation de requêtes pour la performance.
- Bonnes pratiques d'écriture de requêtes analytiques.

Règles d'analyses et détections intelligentes

- Création de règles d'analyse basées sur conditions, tendances et comportements.
- Utilisation de Machine Learning et des templates prédéfinis.
- Tests de faux positifs et faux négatifs.
- Tuning progressif des règles de détection.

Incidents et investigations

- Conception des investigations : indicateurs et pivots.
- Exploration des entités et corrélations entre alertes.
- Traçage des attaques à l'aide de graphes d'investigation.
- Gestion du cycle de vie des incidents.

Playbooks et automatisation

- Présentation des playbooks Azure Logic Apps.
- Exemples concrets : quarantaine, blocage IP, notifications.
- Intégration avec Teams, email, systèmes de ticketing.
- Orchestration de workflows complexes.

Dashboards et reporting

- Création de dashboards personnalisés (Workbooks).
- Publication de rapports pour la compliance et le management.
- Tableaux de bord en temps réel.
- Reporting opérationnel et stratégique.

Scénarios pratiques et SOC workflows

- Détections réelles : phishing, lateral movement, brute force, exfiltration.
- Mise en place d'un processus d'alerte et de réponse SOC.
- Playbooks d'escalade entre niveaux N1/N2/N3.

Bonnes pratiques et sécurité continue

- Gestion des coûts et rétention des logs.
- Protection des données sensibles dans Sentinel.
- Mise à jour périodique des règles et ajustement des playbooks.

MODALITÉS PÉDAGOGIQUES

Format et déroulement

La formation se déroule en distanciel via une classe virtuelle interactive. Elle peut également être réalisée sur le site du client, avec une personnalisation du contenu en fonction des enjeux du projet professionnel.

La répartition théorie / pratique est d'environ 40 % / 60 %. Le programme s'articule autour d'apports théoriques, de démonstrations, de travaux pratiques sur application fil rouge et de phases d'échanges entre participants et formateur.

Format ultra-personnalisé MFE-IT

Chaque session regroupe entre 1 et 3 participants, afin de garantir un suivi individuel très poussé. Un entretien en amont permet d'ajuster le contenu au profil de chacun : niveau, objectifs, contexte professionnel, enjeux.

Les sessions inter-entreprises sont garanties dès 1 seul inscrit (sauf cas de force majeure).

Moyens techniques

La formation est accessible depuis n'importe quel poste disposant d'une connexion Internet haut débit. Avant le démarrage, notre équipe logistique prend contact avec chaque participant pour valider l'environnement technique et présenter la plateforme.

Pendant toute la formation, le stagiaire bénéficie d'une assistance technique et pédagogique par e-mail, avec un délai de traitement qui n'excède pas 24 heures ouvrées.

Évaluation des acquis

Tout au long de la formation, le formateur évalue la progression des participants au travers de QCM, de mises en situation et de travaux pratiques. Le faible effectif par session rend possible une validation individuelle à la fin de chaque atelier.

À l'issue de la formation, une attestation de validation des acquis est remise à chaque participant, mentionnant les objectifs, la nature, la durée de l'action et les résultats de l'évaluation.

Accessibilité et handicap

MFE-IT est attentif à l'accueil des personnes en situation de handicap. Pour toute demande d'aménagement, un échange avec notre référent handicap permet d'identifier les besoins spécifiques et d'adapter le dispositif de formation. Contact : contact@mfe-it.com.

Assistance post-formation

Pendant le mois qui suit la formation, chaque stagiaire peut solliciter l'aide des formateurs MFE-IT sur des questions de mise en œuvre des connaissances acquises. Une réponse est apportée par e-mail ou par téléphone sous 48 heures ouvrées.

INFORMATIONS PRATIQUES

Prise en compte du handicap

MFE-IT accorde une attention particulière à l'inclusion des personnes en situation de handicap. Afin que la formation se déroule dans les meilleures conditions, nous invitons les participants concernés à nous contacter en amont, par e-mail (contact@mfe-it.com) ou via le formulaire de notre site. Un échange avec notre référente handicap permettra d'identifier ensemble les besoins spécifiques et les aménagements utiles à la réussite du parcours.

Modalités pédagogiques et techniques

Le dispositif pédagogique combine apports théoriques, démonstrations guidées, travaux pratiques sur application fil rouge et temps d'échange entre participants et formateur, selon une répartition voisine de 40 % de théorie et 60 % de pratique.

La formation est accessible à distance depuis n'importe quel lieu disposant d'une connexion Internet haut débit. En amont de la session, nos équipes prennent contact avec chaque stagiaire afin de réaliser une vérification technique et de présenter l'environnement de travail.

Durant toute la durée de l'action, le stagiaire bénéficie d'une assistance technique et pédagogique par e-mail, avec un délai de prise en charge inférieur à 24 heures ouvrées. Un rendez-vous pédagogique individuel avec un formateur peut également être programmé pour approfondir un point précis.

La durée indiquée dans le programme constitue une estimation qui peut évoluer en fonction du profil du participant et de ses attentes, notamment lorsqu'un passage de certification est envisagé.

Moyens mis en œuvre par le formateur

- Des démonstrations structurées en modules et séquences pédagogiques fines, alignées sur le programme détaillé
- Des énoncés et corrigés de travaux pratiques, à réaliser tout au long de la formation
- Un environnement technique prêt à l'emploi pour la réalisation des ateliers pratiques
- Une validation par le formateur des connaissances acquises à l'issue de chaque atelier
- Un ou plusieurs supports numériques faisant office de documents de référence

Validation et sanction de la formation

À l'issue de la formation, une attestation est adressée par e-mail au stagiaire. Elle précise les objectifs, la nature, la durée de l'action ainsi que les résultats de l'évaluation des acquis. Un certificat de réalisation peut également être fourni sur demande.

Type de formation

Action de formation professionnalisante, visant le perfectionnement et l'élargissement des compétences des participants.

Suivi de l'exécution de l'action

L'assiduité des participants est vérifiée par la signature d'une feuille de présence par demi-journée, cosignée par le formateur.

Modalités d'évaluation des acquis

Les participants mettent en pratique les éléments du cours au travers de travaux pratiques réalisés sur poste individuel. La validation des acquis est effectuée par le formateur à l'issue de chaque atelier. Le très faible effectif par session rend possible un suivi individualisé (1 à 3 participants).

À l'issue de la formation, le stagiaire a atteint les objectifs pédagogiques fixés par le programme.

Aide à l'orientation

Pour chaque grande thématique de notre catalogue, nos experts proposent un entretien téléphonique ou en visio afin d'aider les personnes qui le souhaitent à choisir le programme ou le parcours de formation le mieux adapté à leur profil et à leurs objectifs.

Aspects pratiques

Dès l'inscription, nos équipes prennent contact avec les participants pour vérifier la qualité du lien Internet disponible sur le lieu où ils souhaitent se former, ainsi que l'adéquation du matériel (PC portable, webcam, micro-casque).

Avant le démarrage, les participants reçoivent un lien d'accès à la classe virtuelle accompagné de leurs identifiants personnels. Une aide à la prise en main de la solution de visioconférence est également mise à disposition.

Le jour de la formation, les participants rejoignent la salle virtuelle depuis leur navigateur. Ils voient et entendent le formateur ainsi que les autres stagiaires, et peuvent échanger à tout moment. Les ateliers se déroulent dans des conditions proches d'une salle physique, avec possibilité pour le formateur de prendre la main à distance pour accompagner ou vérifier un TP.

Bénéfices pour les participants

- Se former depuis son lieu de travail ou son domicile, sans déplacement
- Bénéficier d'un formateur consultant expert du sujet animé
- Profiter d'un format ultra-personnalisé (1 à 3 participants) favorisant les échanges et la pratique
- Continuer à se former même en cas d'imprévus professionnels ou personnels

Bénéfices pour l'entreprise

- Optimiser le budget formation en limitant les frais de déplacement et d'hébergement
- Offrir des formations de qualité à l'ensemble des collaborateurs, quelle que soit leur localisation
- Réduire les temps d'absence liés aux trajets
- Élargir le choix des formations proposées aux collaborateurs peu mobiles
- Soutenir la montée en compétences des équipes dans tous les contextes