03 20 61 95 06
formation@access-it.fr

Formation Microsoft SC-200 Analyste des opérations de sécurité

Durée de la formation : 4 jour(s)

OBJECTIFS

A l'issue de la formation, l'apprenant sera capable de :
Expliquer comment Microsoft Defender pour Endpoint peut remédier aux risques dans votre environnement
Créer un environnement Microsoft Defender pour Endpoint
Configurer les règles de réduction de la surface d'attaque sur les appareils Windows 10
Effectuer des actions sur un appareil à l'aide de Microsoft Defender pour Endpoint
Examiner les domaines et les adresses IP dans Microsoft Defender pour Endpoint
Examiner les comptes d'utilisateurs et configurer les paramètres d'alerte dans Microsoft Defender pour Endpoint
Comprendre comment effectuer une recherche avancée dans Microsoft 365 Defender
Gérer les incidents dans Microsoft 365 Defender
Expliquer comment Microsoft Defender for Identity peut remédier aux risques dans votre environnement
Examiner les alertes DLP dans Microsoft Cloud App Security
Configurer l'approvisionnement automatique dans Azure Defender
Comprendre comment corriger les alertes dans Azure Defender
Construire des instructions KQL
Pouvoir filtrer les recherches en fonction de l'heure de l'événement, de la gravité, du domaine et d'autres données pertinentes à l'aide de KQL
Comprendre comment extraire des données de champs de chaîne non structurés à l'aide de KQL
Gérer un espace de travail Azure Sentinel
Apprendre à utiliser KQL pour accéder à la liste de surveillance dans Azure Sentinel
Gérer les indicateurs de menace dans Azure Sentinel
Connecter les machines virtuelles Azure Windows à Azure Sentinel
Configurer l'agent Log Analytics pour collecter les événements Sysmon
Créer de nouvelles règles et requêtes d'analyse à l'aide de l'assistant de règle d'analyse
Pouvoir utiliser des requêtes pour rechercher les menaces

PREREQUIS

Compréhension de base de Microsoft 365
Compréhension fondamentale des produits de sécurité, de conformité et d'identité Microsoft
Compréhension intermédiaire de Windows 10
Familiarité avec les services Azure, en particulier les bases de données Azure SQL et le stockage Azure
Connaissance des machines virtuelles Azure et des réseaux virtuels
Compréhension de base des concepts de script
Un entretien en amont avec notre expert permet de prendre en compte le profil de chaque participant (niveau, objectifs et résultats attendus, contexte professionnel, enjeux...) et d'adapter le contenu de la formation si besoin
Cette formation ne peut être financée que dans le cadre d'un projet d'entreprise (prise en charge entreprise ou OPCO). Les dossiers à financement personnel et CPF ne sont pas pris en compte.

03 20 61 95 06
formation@access-it.fr

Formation Microsoft SC-200 Analyste des opérations de sécurité

Durée de la formation : 4 jour(s)

PUBLIC

Analystes sécurité
Ingénieurs sécurité

03 20 61 95 06
formation@access-it.fr

Formation Microsoft SC-200 Analyste des opérations de sécurité

Durée de la formation : 4 jour(s)

PROGRAMME

ATTÉNUER LES MENACES À L'AIDE DE MICROSOFT DEFENDER POUR ENDPOINT

Se protéger contre les menaces avec Microsoft Defender pour Endpoint
Déployer l'environnement Microsoft Defender pour Endpoint
Mettre en oeuvre les améliorations de la sécurité de Windows 10 avec Microsoft Defender pour Endpoint
Gérer les alertes et les incidents dans Microsoft Defender pour Endpoint
Effectuer des enquêtes sur les appareils dans Microsoft Defender pour Endpoint
Effectuer des actions sur un appareil à l'aide de Microsoft Defender pour Endpoint
Effectuer des enquêtes sur les preuves et les entités à l'aide de Microsoft Defender pour Endpoint
Configurer et gérer l'automatisation à l'aide de Microsoft Defender pour Endpoint
Configurer les alertes et les détections dans Microsoft Defender pour Endpoint
Utiliser la gestion des menaces et des vulnérabilités dans Microsoft Defender pour Endpoint

ATTÉNUER LES MENACES À L'AIDE DE MICROSOFT 365 DEFENDER

Introduction à la protection contre les menaces avec Microsoft 365
Atténuer les incidents à l'aide de Microsoft 365 Defender
Protéger les identités avec Azure AD Identity Protection
Remédier aux risques avec Microsoft Defender pour Office 365
Protéger son environnement avec Microsoft Defender for Identity
Sécuriser ses applications et services cloud avec Microsoft Cloud App Security
Répondre aux alertes de prévention de la perte de données à l'aide de Microsoft 365
Gérer les risques internes dans Microsoft 365

ATTÉNUER LES MENACES À L'AIDE D'AZURE DEFENDER

Planifier les protections de la charge de travail cloud à l'aide d'Azure Defender
Expliquer les protections des charges de travail cloud dans Azure Defender
Connecter les actifs Azure à Azure Defender
Connecter des ressources non-Azure à Azure Defender
Corriger les alertes de sécurité à l'aide d'Azure Defender

CRÉER DES REQUÊTES POUR AZURE SENTINEL À L'AIDE DU LANGAGE DE REQUÊTE KUSTO (KQL)

Construire des instructions KQL pour Azure Sentinel
Analyser les résultats des requêtes à l'aide de KQL
Créer des instructions multi-tables à l'aide de KQL
Travailler avec des données dans Azure Sentinel à l'aide du langage de requête Kusto

CONFIGURER VOTRE ENVIRONNEMENT AZURE SENTINEL

Introduction à Azure Sentinel
Créer et gérer des espaces de travail Azure Sentinel
Requête des journaux dans Azure Sentinel
Utiliser des listes de surveillance dans Azure Sentinel
Utiliser l'intelligence des menaces dans Azure Sentinel

03 20 61 95 06
formation@access-it.fr

Formation Microsoft SC-200 Analyste des opérations de sécurité

Durée de la formation : 4 jour(s)

CONNECTER LES JOURNAUX À AZURE SENTINEL

Connecter les données à Azure Sentinel à l'aide de connecteurs de données
Connecter les services Microsoft à Azure Sentinel
Connecter Microsoft 365 Defender à Azure Sentinel
Connecter les hôtes Windows à Azure Sentinel
Connecter les journaux du format d'événement commun à Azure Sentinel
Connecter les sources de données Syslog à Azure Sentinel
Connecter les indicateurs de menace à Azure Sentinel

CRÉER DES DÉTECTIONS ET EFFECTUER DES INVESTIGATIONS À L'AIDE D'AZURE SENTINEL

Détection des menaces avec l'analyse Azure Sentinel
Réponse aux menaces avec les playbooks Azure Sentinel
Gestion des incidents de sécurité dans Azure Sentinel
Utiliser l'analyse du comportement des entités dans Azure Sentinel
Interroger, visualiser et surveiller les données dans Azure Sentinel

EFFECTUER UNE RECHERCHE DE MENACES DANS AZURE SENTINEL

Chasse aux menaces avec Azure Sentinel
Traquer les menaces à l'aide de blocs-notes dans Azure Sentinel

03 20 61 95 06
formation@access-it.fr

Formation Microsoft SC-200 Analyste des opérations de sécurité

Durée de la formation : 4 jour(s)

Prise en compte du handicap
Pour les personnes en situation de handicap, afin de nous permettre d'organiser le déroulement de la formation dans les meilleures conditions possibles, contactez-nous via notre formulaire de contact ou par mail (formation@access-it.fr) ou par téléphone (0320619506). Un entretien avec notre référente handicap pourra être programmé afin d'identifier les besoins et aménagements nécessaires.

Modalités et moyens Pédagogiques, techniques et d'encadrement mis en œuvre
Répartition théorie/pratique : 45%/55%. Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques s'articulant autour d'une application fil rouge, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.
Formation accessible à distance de n'importe où et n'importe quand, via un ordinateur type PC disposant d'une connexion à Internet à haut débit (ADSL ou plus).
Pour assurer un démarrage dans les meilleures conditions au premier jour de la formation, notre service logistique se met systématiquement en relation, en amont, avec vous afin de réaliser un test de validation technique et de vous présenter l'environnement de formation.
Pendant toute la durée de la formation, le stagiaire dispose d'une assistance technique et pédagogique illimitée, par e-mail, avec un délai de prise en compte et de traitement qui n'excède pas 24h. En complément, le stagiaire peut planifier un rendez-vous pédagogique avec un formateur expert afin d'échanger sur des éléments de la formation.
La durée de la formation affichée sur cette page est une durée estimée qui peut varier en fonction du profil du stagiaire et de ses objectifs (notamment s'il souhaite valider sa formation par le passage d'un examen de certification).
Durant la formation, le formateur prévoit :
Des démonstrations organisées en modules et en séquences découpées le plus finement possible, en suivant le programme pédagogique détaillé sur cette page ;
Des énoncés et corrigés de travaux pratiques à réaliser tout au long de la formation ;
Des travaux pratiques sont proposés ; la plateforme prévoit l'environnement technique nécessaire à la réalisation de l'ensemble des travaux pratiques ;
Le formateur valide les connaissances acquises après chaque TP ;
Il est proposé un ou plusieurs livres numériques faisant office d'ouvrage(s) de référence sur le thème de la formation.

Validation et sanction de la formation
Une attestation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation sera remise au stagiaire à l'issue de sa formation par courrier électronique.
A la demande, il sera délivré un certificat de réalisation.

Type de formation
Professionnalisante ayant pour objectif le perfectionnement, l'élargissement des compétences

Moyens permettant de suivre l'exécution de l'action
Le contrôle de la présence des stagiaires sera assuré par la vérification de l'assiduité des participants. Le stagiaire signera une feuille de présence par demi-journée de formation. Celle-ci sera également signée par le formateur.

Modalité d'évaluation des acquis
Durant la formation, le participant est amené à mettre en pratique les éléments du cours par la réalisation de travaux pratiques réalisés sur PC.
La validation des acquis du stagiaire est faite par le formateur à la fin de chaque atelier. Cette validation individuelle est possible du fait du faible nombre de participants par session de formation (6 personnes maximum).
A la fin de la formation, le stagiaire a donc atteint les objectifs fixés par la formation.
En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par l'éditeur en passant un examen de certification.
Access it étant centre d'examen ENI, les examens peuvent être réalisés sur demande à distance ou dans nos locaux de Villeneuve d'Ascq.
Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification

Assistance Post-Formation
Toute personne ayant suivi une formation avec Access it bénéficie d'une assistance post-formation d'une durée de 1 mois. Ce nouveau service d'accompagnement permet aux stagiaires rencontrant des difficultés dans la mise en oeuvre des connaissances acquises de solliciter l'aide de nos formateurs sur des aspects relatifs aux programmes de formation suivis. Pour en bénéficier, il suffit de se rendre sur la page contact de notre site web et de remplir le formulaire. Une réponse est apportée par mail ou par téléphone dans un délai de 48 heures.

Centre d'Examen
Notre centre de formation agréé Qualiopi bénéficie de l'agrément d'ENI et ICDL pour les certifications informatiques. C'est pour nos clients la garantie de pouvoir suivre des formations préparant à des certifications professionnelles.

Aide à l'orientation
Pour chacune des grandes thématiques couvertes par notre offre de formation, nous proposons via nos spécialistes un rendez-vous physique ou téléphonique qui via un diagnostic permettra aux personnes souhaitant être accompagnées dans le choix d'un programme ou dans la définition d'un parcours de formation une orientation vers les programmes les plus adaptés à leurs besoins et à leur niveau.

Aspects Pratiques
Dès leur inscription, les participants sont contactés par nos services qui s'assurent que les débits internet constatés sur le lieu depuis lequel ils souhaitent se former sont suffisants pour suivre la formation dans des conditions optimales.
À l'occasion de cet appel, nos experts s'assurent également qu'ils disposent du matériel nécessaire pour suivre la formation (PC Portable, webcam, Micro-casque..).
Avant le début de la formation, les participants reçoivent un lien leur permettant d'accéder à la classe virtuelle et leurs identifiants personnels de connexion. Un aide à l'utilisation de la solution de visioconférence utilisée leur est également proposée.
Le jour de la formation, ils se connectent à la classe virtuelle depuis leur navigateur internet. Ils voient et entendent le formateur ainsi que les autres participants et peuvent à tout moment communiquer avec eux.
Ils participent aux échanges et réalisent les ateliers dans les mêmes conditions que s'ils étaient en salle. Grâce à nos outils de prise en main à distance, les formateurs peuvent à tout moment prendre la main sur leurs postes pour les aider ou vérifier leurs TP.
Tout au long de la formation, les participants peuvent bénéficier de l'assistance immédiate de nos experts en composant le numéro qui leur a été communiqué avant la formation.
Des bilans intermédiaires ont lieu en présence des participants du formateur et du référent pédagogique d'Access it afin de vérifier l'état d'avancement de la session, les difficultés rencontrées et permettre d'éventuels actions correctives.

Bénéfices pour les participants
Se former depuis leur lieu de travail ou leur domicile,
Accéder sans se déplacer à la qualité d'une formation délivrée par un formateur consultant ayant une expérience probante sur le sujet animé.
Bénéficier à distance de la richesse d'une formation interentreprises : échanges avec le formateur et les autres participants, partages d'expériences, ateliers pratiques...
Pouvoir se former en toutes circonstances et notamment en cas d'imprévus.

Bénéfices pour l'entreprise
Optimiser ses budgets en limitant les frais de déplacement et d'hébergement.
Proposer à tous ses collaborateurs, quelle que soit leur situation géographique, des formations de qualité (en Inter comme en Intra).
Limiter les temps de déplacement.
Proposer davantage de choix dans les formations à des collaborateurs peu mobiles.
Assurer la montée en compétences de ses collaborateurs quelles que soient les circonstances