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

Formation Microsoft SC-100 Cybersecurity Architect

Durée de la formation : 3 jour(s) / 21 heure(s)

OBJECTIFS

A l'issue de la formation le participant sera capable de :
Concevoir une stratégie et une architecture Zero Trust Évaluer les stratégies techniques et les stratégies d’opérations de sécurité des Risques conformité en matière de gouvernance (GRC)
Concevoir la sécurité pour l’infrastructure
Concevoir une stratégie de données et d’applications

PREREQUIS

Avant de suivre ce cours, les étudiants doivent avoir :
Une expérience et des connaissances avancées en matière d’accès et d’identités, de protection des plateformes, d’opérations de sécurité, de sécurisation des données et de sécurisation des applications.
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.

PUBLIC

Cette formation s'adresse aux professionnels de l'informatique ayant une expérience et des connaissances avancées dans un large éventail de domaines d'ingénierie de la sécurité, notamment l'identité et l'accès, la protection des plateformes, les opérations de sécurité, la sécurisation des données et la sécurisation des applications. Ils doivent également avoir une expérience des mises en œuvre hybrides et en nuage.

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

Formation Microsoft SC-100 Cybersecurity Architect

Durée de la formation : 3 jour(s) / 21 heure(s)

PROGRAMME

Générer une stratégie de sécurité globale et une architecture

Découvrez comment générer une stratégie de sécurité globale et une architecture.
Leçons
Introduction
Vue d'ensemble de la Confiance Zéro
Développer des points d'intégration dans une architecture
Développer des exigences de sécurité en fonction des objectifs métier
Translater les exigences de sécurité en fonctionnalités techniques
Concevoir la sécurité pour une stratégie de résilience Concevoir une stratégie de sécurité pour les environnements hybrides et multi-abonnés
Concevoir des stratégies techniques et de gouvernance pour le filtrage et la segmentation du trafic
Comprendre la sécurité des protocoles
Exercice : générer une stratégie de sécurité globale et une architecture
Contrôle des connaissances Récapitulatif
Après avoir terminé ce module, les étudiants seront capables de :
Développer des points d'intégration dans une architecture
Développer des exigences de sécurité en fonction des objectifs métier
Translater les exigences de sécurité en fonctionnalités techniques
Concevoir la sécurité pour une stratégie de résilience Concevoir une stratégie de sécurité pour les environnements hybrides et multi-abonnés
Concevoir des stratégies techniques et de gouvernance pour le filtrage et la segmentation du trafic

Concevoir une stratégie d'opérations de sécurité

Découvrez comment concevoir une stratégie d'opérations de sécurité.
Leçons
Introduction
Comprendre les infrastructures, processus et procédures des opérations de sécurité
Concevoir une stratégie de sécurité de la journalisation et de l'audit
Développer des opérations de sécurité pour les environnements hybrides et multiclouds
Concevoir une stratégie pour Security Information and Event Management (SIEM) et l'orchestration de la sécurité,
Évaluer les workflows de la sécurité
Consulter des stratégies de sécurité pour la gestion des incidents
Évaluer la stratégie d'opérations de sécurité pour partager les renseignements techniques sur les menaces
Analyser les sources pour obtenir des informations sur les menaces et les atténuations
Après avoir terminé ce module, les étudiants seront capables de :
Concevoir une stratégie de sécurité de la journalisation et de l'audit
Développer des opérations de sécurité pour les environnements hybrides et multiclouds.
Concevoir une stratégie pour Security Information and Event Management (SIEM) et l'orchestration de la sécurité,
Évaluer les workflows de la sécurité.
Consulter des stratégies de sécurité pour la gestion des incidents.
Évaluer les opérations de sécurité pour le renseignement technique sur les menaces.
Analyser les sources pour obtenir des informations sur les menaces et les atténuations.

Concevoir une stratégie de sécurité des identités

Découvrez comment concevoir une stratégie de sécurité des identités.
Leçons
Introduction

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

Formation Microsoft SC-100 Cybersecurity Architect

Durée de la formation : 3 jour(s) / 21 heure(s)

Sécuriser l’accès aux ressources cloud
Recommander un magasin d’identités pour la sécurité Recommander des stratégies d’authentification sécurisée et d’autorisation de sécurité Sécuriser l’accès conditionnel
Concevoir une stratégie pour l’attribution de rôle et la délégation
Définir la gouvernance des identités pour les révisions d’accès et la gestion des droits d’utilisation
Concevoir une stratégie de sécurité pour l’accès des rôles privilégiés à l’infrastructure
Concevoir une stratégie de sécurité pour des activités privilégiées
Comprendre la sécurité des protocoles
Après avoir terminé ce module, les étudiants seront capables de :
Recommander un magasin d’identités pour la sécurité.
Recommander des stratégies d’authentification sécurisée et d’autorisation de sécurité.
Sécuriser l’accès conditionnel.
Concever une stratégie pour l’attribution de rôle et la délégation.
Définisser la gouvernance des identités pour les révisions d’accès et la gestion des droits d’utilisation.
Concever une stratégie de sécurité pour l’accès des rôles privilégiés à l’infrastructure.
Concever une stratégie de sécurité pour des accès privilégiés.

Evaluer la posture de sécurité et recommander des stratégies techniques pour gérer les risques

Découvrez comment évaluer une stratégie de conformité réglementaire.
Leçons
Introduction
Interpréter les exigences de conformité et leurs fonctionnalités techniques
Évaluer la conformité de l’infrastructure à l’aide de Microsoft Defender pour le cloud
Interpréter les scores de conformité et recommander des actions pour résoudre les problèmes ou améliorer la sécurité
Concevoir et valider l’implémentation de Azure Policy Conception pour les exigences de résidence des données
Traduire les exigences de confidentialité en exigences pour les solutions de sécurité
Après avoir terminé ce module, les étudiants seront capables de :
Interpréter les exigences de conformité et leurs fonctionnalités techniques
Évaluer la conformité de l’infrastructure à l’aide de Microsoft Defender pour le cloud
Interpréter les scores de conformité et recommander des actions pour résoudre les problèmes ou améliorer la sécurité
Concevoir et valider l’implémentation de Azure Policy Conception pour les exigences de résidence des données
Traduire les exigences de confidentialité en exigences pour les solutions de sécurité

Evaluer une stratégie de conformité réglementaire

Découvrez comment évaluer une stratégie de conformité réglementaire.
Leçons
Introduction
Interpréter les exigences de conformité et leurs fonctionnalités techniques
Évaluer la conformité de l’infrastructure à l’aide de Microsoft Defender pour le cloud
Interpréter les scores de conformité et recommander des actions pour résoudre les problèmes ou améliorer la sécurité
Concevoir et valider l’implémentation de Azure Policy Conception pour les exigences de résidence des données
Traduire les exigences de confidentialité en exigences pour les solutions de sécurité
Après avoir terminé ce module, les étudiants seront capables de :
Interpréter les exigences de conformité et leurs fonctionnalités techniques
Évaluer la conformité de l’infrastructure à l’aide de Microsoft Defender pour le cloud
Interpréter les scores de conformité et recommander des actions pour résoudre les problèmes ou améliorer la sécurité
Concevoir et valider l’implémentation de Azure Policy Conception pour les exigences de résidence des données

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

Formation Microsoft SC-100 Cybersecurity Architect

Durée de la formation : 3 jour(s) / 21 heure(s)

Traduire les exigences de confidentialité en exigences pour les solutions de sécurité

Comprendre les meilleures pratiques relatives à l’architecture et comment elles changent avec le cloud

Découvrez comment les meilleures pratiques relatives à l’architecture et comment elles changent avec le cloud.
Leçons
Introduction
Planifier et implémenter une stratégie de sécurité entre les équipes
Établir une stratégie et un processus pour une évolution proactive et continue d’une stratégie de sécurité
Comprendre les protocoles réseau et les meilleures pratiques pour la segmentation du réseau et le filtrage du trafic
Après avoir terminé ce module, les étudiants seront capables de :
Décrire les meilleures pratiques pour la segmentation du réseau et le filtrage du trafic.
Planifier et implémenter une stratégie de sécurité entre les équipes.
Établir une stratégie et un processus pour une évolution proactive et continue d’une stratégie de sécurité.

Concevoir une stratégie pour sécuriser les points de terminaison serveur et client

Découvrez comment concevoir une stratégie pour sécuriser les points de terminaison serveur et client.
Leçons
Introduction
Spécifier des lignes de base de sécurité pour les points de terminaison serveur et client
Spécifier les exigences de sécurité pour les serveurs Spécifier les exigences de sécurité pour les appareils mobiles et les clients
Spécifier les exigences pour la sécurisation de Active Directory Domain Services
Concevoir une stratégie pour gérer les secrets, les clés et les certificats
Concevoir une stratégie pour sécuriser l’accès à distance
Comprendre les infrastructures, processus et procédures des opérations de sécurité
Comprendre les procédures forensiques approfondies par type de ressource
Après avoir terminé ce module, les étudiants seront capables de :
Spécifier des lignes de base de sécurité pour les points de terminaison serveur et client
Spécifier les exigences de sécurité pour les serveurs Spécifier les exigences de sécurité pour les appareils mobiles et les clients
Spécifier les exigences pour la sécurisation de Active Directory Domain Services
Concevoir une stratégie pour gérer les secrets, les clés et les certificats
Concevoir une stratégie pour sécuriser l’accès à distance
Comprendre les infrastructures, processus et procédures des opérations de sécurité
Comprendre les procédures forensiques approfondies par type de ressource

Concevoir une stratégie de sécurisation des services PaaS, IaaS et SaaS

Découvrez comment concevoir une stratégie de sécurisation des services PaaS, IaaS et SaaS.
Leçons
Introduction
Spécifier des lignes de base de sécurité pour les services PaaS
Spécifier des lignes de base de sécurité pour les services IaaS
Spécifier des lignes de base de sécurité pour les services SaaS
Spécifier les exigences de sécurité pour les charges de travail IoT
Spécifier les exigences de sécurité pour les charges de travail données
Spécifier les exigences de sécurité pour les charges de travail web

Formation Microsoft SC-100 Cybersecurity Architect

Durée de la formation : 3 jour(s) / 21 heure(s)

Spécifier les exigences de sécurité pour les charges de travail de stockage
Spécifier les exigences de sécurité pour les conteneurs Spécifier les exigences de sécurité pour l'orchestration des conteneurs
Après avoir terminé ce module, les étudiants seront capables de :
Spécifier des lignes de base de sécurité pour les services PaaS, SaaS et IaaS
Spécifier les exigences de sécurité pour les charges de travail IoT, données, stockage et web
Spécifier les exigences de sécurité pour les conteneurs et l'orchestration des conteneurs

Spécifier les exigences de sécurité pour les applications

Découvrez comment spécifier les exigences de sécurité pour les applications.
Leçons
Introduction
Comprendre la modélisation des menaces sur les applications
Spécifier des priorités pour atténuer les menaces sur les applications
Spécifier une norme de sécurité pour l'intégration d'une nouvelle application
Spécifier une stratégie de sécurité pour les applications et les API
Après avoir terminé ce module, les étudiants seront capables de :
Spécifier des priorités pour atténuer les menaces sur les applications
Spécifier une norme de sécurité pour l'intégration d'une nouvelle application
Spécifier une stratégie de sécurité pour les applications et les API

Concevoir une stratégie de sécurisation des données

Découvrez comment concevoir une stratégie de sécurisation des données.
Leçons
Introduction
Classer par ordre de priorité l'atténuation des menaces sur les données
Concevoir une stratégie pour identifier et protéger les données sensibles
Spécifier une norme de chiffrement pour les données au repos et en mouvement
Après avoir terminé ce module, les étudiants seront capables de :
Classer par ordre de priorité l'atténuation des menaces sur les données
Concevoir une stratégie pour identifier et protéger les données sensibles
Spécifier une norme de chiffrement pour les données au repos et en mouvement

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

Formation Microsoft SC-100 Cybersecurity Architect

Durée de la formation : 3 jour(s) / 21 heure(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