Architecte en cybersécurité Microsoft

Réf : SC100

OBJECTIFS DE LA FORMATION

Être capable de concevoir une stratégie et une architecture Confiance zéro
Savoir évaluer les stratégies techniques et les stratégies d'opérations de sécurité des Risques conformité en matière de gouvernance (GRC)
Comprendre comment concevoir la sécurité pour l'infrastructure
Apprendre à concevoir une stratégie de données et d'applications

PROGRAMME

GÉNÉRER UNE STRATÉGIE DE SÉCURITÉ GLOBALE ET UNE ARCHITECTURE
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
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

CONCEVOIR UNE STRATÉGIE D'OPÉRATIONS DE SÉCURITÉ
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

CONCEVOIR UNE STRATÉGIE DE SÉCURITÉ DES IDENTITÉS
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

ÉVALUER UNE STRATÉGIE DE CONFORMITÉ RÉGLEMENTAIRE
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
Translater les exigences de confidentialité en exigences pour les solutions de sécurité

ÉVALUER LA POSTURE DE SÉCURITÉ ET RECOMMANDER DES STRATÉGIES TECHNIQUES POUR GÉRER LES RISQUES
Évaluer les postures de sécurité à l'aide de points de référence
Évaluer les postures de sécurité à l'aide de

La formation est accessible aux personnes à mobilité réduite et toute demande d'adaptation peut être étudiée en amont de la formation en fonction du besoin des personnes. Nous contacter pour plus d'informations

Lieu : Site de Metz : JCD FORMATION - 193 rue Metman - 57070 METZ - 03 87 37 97 70
Site de Pompey : KAPEDIA – 132 Rue Léonard de Vinci – 54340 POMPEY – 03 83 49 80 80

4 jours soit 28h

Voir calendrier

2690 HT / participant

Public / Prérequis

Public :
Ingénieurs de sécurité cloud expérimentés

Prérequis
Posséder une expérience et des connaissances avancées en matière d'accès et d'identités, de protection des plates-formes, d'opérations de sécurité, de sécurisation des données et des applications.
Être familiarisé avec les implémentations hybrides et cloud.
Il est conseillé d'avoir passé une certification dans les domaines de la sécurité, de la conformité et de l'identité (par exemple AZ-500, SC-200 ou SC-300)

Méthodes et Moyens pédagogiques

Alternance continuelle entre apport de connaissances et manipulation des outils. Fourniture de documents et supports de cours qui restent la propriété des stagiaires.

Salles équipées : vidéoprojecteur, paperboard, ordinateur individuel, support de cours papier ou électronique, outils de prise de note

Validation

Attestation de stage

Profil intervenant

Professionnel et expert en informatique

Suivi et Évaluation de l'action

Compte rendu de fin de formation et analyse interne

Questionnaire « évaluation de la formation » rempli par le stagiaire.

Document mis à jour le 21/03/2023

Architecte en cybersécurité Microsoft

Réf : SC100

OBJECTIFS DE LA FORMATION

Être capable de concevoir une stratégie et une architecture Confiance zéro
Savoir évaluer les stratégies techniques et les stratégies d'opérations de sécurité des Risques conformité en
matière de gouvernance (GRC)
Comprendre comment concevoir la sécurité pour l'infrastructure
Apprendre à concevoir une stratégie de données et d'applications

PROGRAMME

Microsoft Defender pour le cloud
Évaluer les postures de sécurité à l'aide du niveau de sécurité
Évaluer l'hygiène de sécurité des charges de travail cloud
Conception de la sécurité d'une zone d'atterrissage Azure
Interpréter les renseignements techniques sur les menaces et recommander des atténuations des risques
Recommander des fonctionnalités de sécurité ou des contrôles pour atténuer les risques identifiés

COMPRENDRE LES MEILLEURES PRATIQUES RELATIVES À L'ARCHITECTURE ET COMMENT ELLES CHANGENT AVEC LE CLOUD
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

CONCEVOIR UNE STRATÉGIE POUR SÉCURISER LES POINTS DE TERMINAISON SERVEUR ET CLIENT
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
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
Spécifier des lignes de base de sécurité pour les services PaaS, IaaS et SaaS
Déterminer les exigences de sécurité pour les charges de travail IoT
Spécifier les exigences de sécurité pour les charges de travail données
Définir les exigences de sécurité pour les charges de travail web
Désigner les exigences de sécurité pour les charges de travail de stockage
Définir les exigences de sécurité pour les conteneurs
Spécifier les exigences de sécurité pour l'orchestration des conteneurs

SPÉCIFIER LES EXIGENCES DE SÉCURITÉ POUR LES APPLICATIONS
Comprendre la modélisation des menaces sur les applications
Spécifier des priorités pour atténuer les menaces sur les applications
Définir une norme de sécurité pour l'intégration d'une nouvelle application
Désigner une stratégie de sécurité pour les applications et les API

CONCEVOIR UNE STRATÉGIE DE SÉCURISATION DES DONNÉES
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

4 jours soit 28h

Voir calendrier

2690 HT / participant

Public / Prérequis

Public :
Ingénieurs de sécurité cloud expérimentés

Prérequis
Posséder une expérience et des connaissances avancées en matière d'accès et d'identités, de protection des plates-formes, d'opérations de sécurité, de sécurisation des données et des applications.
Être familiarisé avec les implémentations hybrides et cloud.
Il est conseillé d'avoir passé une certification dans les domaines de la sécurité, de la conformité et de l'identité (par exemple AZ-500, SC-200 ou SC-300)

Méthodes et Moyens pédagogiques

Alternance continuelle entre apport de connaissances et manipulation des outils. Fourniture de documents et supports de cours qui restent la propriété des stagiaires.

Salles équipées : vidéoprojecteur, paperboard, ordinateur individuel, support de cours papier ou électronique, outils de prise de note

Validation

Attestation de stage

Profil intervenant

Professionnel et expert en informatique

Suivi et Évaluation de l'action

Compte rendu de fin de formation et analyse interne

Questionnaire « évaluation de la formation » rempli par le stagiaire.

La formation est accessible aux personnes à mobilité réduite et toute demande d'adaptation peut être étudiée en amont de la formation en fonction du besoin des personnes. Nous contacter pour plus d'informations

Lieu : Site de Metz : JCD FORMATION - 193 rue Metman - 57070 METZ - 03 87 37 97 70
Site de Pompey : KAPEDIA – 132 Rue Léonard de Vinci – 54340 POMPEY – 03 83 49 80 80

Document mis à jour le 21/03/2023