Implémenter des contrôles de sécurité de bout en bout pour les charges de travail cloud et IA

Préparation certification Microsoft AZ-500

DESCRIPTION

Cette formation vous apprend à mettre en œuvre des contrôles de sécurité et une protection contre les menaces, à gérer les identités et les accès, à protéger les données, les applications et les réseaux dans les environnements Cloud et hybrides, au sein d'une infrastructure de bout en bout.

La formation « Azure Security Technologies » (AZ-500) vous accompagnera étape par étape pour sécuriser vos environnements Cloud Azure.

OBJECTIFS PEDAGOGIQUES

A l'issue de cette formation, les participants seront en capacité de :

- Sécuriser l'accès aux ressources à l'aide de Microsoft Entra
- Sécuriser Azure Key Vault avec la défense en profondeur pour les charges de travail cloud et IA
- Appliquer la gouvernance de la sécurité et la conformité réglementaire
- Implémenter la sécurité pour stockage Azure pour l'ingénieur de sécurité cloud et IA
- Implémenter la sécurité pour les bases de données Azure SQL
- Implémenter des contrôles de sécurité réseau dans Azure
- Implémenter la sécurité pour l'IA
- Implémenter la sécurité pour les serveurs et les machines virtuelles
- Sécuriser des services de plateforme d'applications Azure pour l'ingénieur sécurité du cloud et de l'IA
- Gérer la posture de sécurité en utilisant Microsoft Defender pour le cloud
- Implémenter l'activité et la collecte d'événements dans Microsoft Sentinel
- Déployer et exploiter Microsoft Security Copilot

PUBLIC CIBLE

Administrateurs, IT Pro, Responsables sécurité

PRE-REQUIS

Classe à distance
Sécurité

Code :
SC500

Durée :
4 jour(s) (28,00 heures)

Exposés : **60 %**
Cas pratiques : **20 %**
Echanges d'expérience : **20 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 2 970,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

Pour suivre cette formation, vous devez avoir une compréhension et une connaissance :

- Des meilleures pratiques de sécurité et exigences de sécurité de l'industrie telles que la défense en profondeur, l'accès le moins privilégié, le contrôle d'accès basé sur les rôles, l'authentification multifacteur, la responsabilité partagée et le modèle de confiance zéro

- Des protocoles de sécurité tels que les réseaux privés virtuels (VPN), le protocole de sécurité Internet (IPSec), Secure Socket Layer (SSL), les méthodes de cryptage de disque et de données

- Du déploiement de charges de travail Azure.

- Des systèmes d'exploitation Windows et Linux et les langages de script.

Les travaux pratiques de la formation peuvent utiliser PowerShell et l'interface de ligne de commande.

Ce cours ne couvre pas les bases de l'administration Azure, mais le contenu du cours s'appuie sur ces connaissances en ajoutant des informations spécifiques à la sécurité.

Il faut avoir suivi la formation « AZ-900 Azure Fundamentals » et la formation « AZ-104 : Azure Administrator » pour suivre ce cours ou avoir un niveau d'expérience sur Azure équivalent.

Un niveau d'anglais B1 est recommandé, retrouvez les niveaux sur ce lien : Classification des niveaux de langue

METHODE PEDAGOGIQUE

Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique des formateurs, complétés de travaux pratiques et de mises en situation.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

GÉRER ET IMPLÉMENTER DES MÉTHODES D'AUTHENTIFICATION DANS MICROSOFT ENTRA ID

- Décrire les méthodes d'authentification Microsoft Entra ID et les concepts de force d'authentification.
- Configurer l'authentification multifacteur à l'aide de stratégies d'accès conditionnel et d'emplacements nommés.
- Implémenter des méthodes d'authentification sans mot de passe, notamment Windows Hello Entreprise, des clés secrètes et des clés de sécurité FIDO2.
- Configurer la réinitialisation de mot de passe en libre-service pour les utilisateurs dans un environnement hybride.

IMPLÉMENTER ET CONFIGURER PRIVILEGED IDENTITY MANAGEMENT (PIM)

- Expliquer pourquoi la gestion des identités privilégiées et l'accès juste à temps sont essentiels à une stratégie de sécurité zéro confiance.
- Décrire les principales fonctionnalités et les types d'affectation dans Privileged Identity Management (PIM)
- Mettre en œuvre l'accès juste-à-temps pour les rôles Microsoft Entra en utilisant PIM
- Implémenter un accès juste à temps pour les rôles de ressources Azure à l'aide de PIM
- Mettre à l'échelle l'accès juste-à-temps aux groupes en utilisant PIM pour les groupes
- Appliquer des modèles d'accès juste-à-temps aux charges de travail, agents et applications IA
- Appliquer des principes de conception et des bonnes pratiques pour un accès privilégié « juste-à-temps ».

AUTHENTIFIER VOTRE PLUG-IN d'API POUR LES AGENTS DÉCLARATIFS AVEC DES API SÉCURISÉES

- Identifier la façon dont une API est sécurisée
- Concevoir un moyen sécurisé d'intégrer un plug-in d'API pour Microsoft 365 Copilot avec une API

- Intégrer un plug-in d'API à une API sécurisée avec une clé API
- Intégrer un plug-in d'API à une API sécurisée avec OAuth2
- Exécuter le plug-in d'API dans Microsoft 365 Copilot pour valider les résultats

CONFIGURER ET SÉCURISER LES AZURE KEY VAULT

- Déployer Azure Key Vault avec des contrôles de sécurité appliqués au moment de la création
- Configurer le contrôle d'accès en fonction du rôle et le privilège juste-à-temps pour les opérations de Key Vault
- Sécuriser l'accès réseau de Key Vault à l'aide de règles de pare-feu, de points de terminaison de service de réseau virtuel et de points de terminaison privés

GÉRER LES CLÉS ET LES SECRETS DANS AZURE KEY VAULT

- Créer et gérer des clés cryptographiques, y compris les scénarios protégés par HSM et BYOK
- Configurer des stratégies de rotation de clés automatisées pour réduire le risque d'exposition aux chiffrements
- Créer une rotation des secrets sans temps d'arrêt à l'aide des identifiants doubles et des schémas de rotation automatisés

GÉRER LES CERTIFICATS ET SURVEILLER LES AZURE KEY VAULT

- Gérer l'émission, le renouvellement et le cycle de vie des certificats par le biais des autorités de certification intégrées
- Configurer les actions relatives à la durée de vie de Key Vault et les contacts pour le certificat pour le renouvellement et la notification automatique
- Activer la journalisation des diagnostics de Key Vault pour soutenir les enquêtes de sécurité et répondre aux exigences de conformité.

PROTÉGER AZURE KEY VAULT AVEC MICROSOFT DEFENDER FOR CLOUD

- Utiliser l'analyse sans agent de CSPM Defender pour découvrir les secrets exposés sur les machines virtuelles et les déploiements cloud.
- Activer Microsoft Defender pour Key Vault et identifier ses fonctionnalités de détection des menaces
- Étudier et répondre aux alertes de sécurité de Microsoft Defender pour Key Vault

APPLIQUER LA GOUVERNANCE AVEC DES AZURE POLICY ET DES VERROUS DE RESSOURCES

- Attribuer des définitions et des initiatives de Azure Policy intégrées pour appliquer des configurations de sécurité dans l'étendue de l'abonnement et du groupe d'administration
- Créer des définitions de Azure Policy personnalisées avec des tâches de correction pour appliquer des contrôles que les définitions intégrées ne couvrent pas
- Configurer Azure verrous de ressources pour empêcher la suppression ou la modification des ressources critiques

CONFIGURER LES CONTRÔLES DE SÉCURITÉ ET CORRIGER LES RECOMMANDATIONS DANS DEFENDER FOR CLOUD

- Configurer les paramètres d'environnement et les normes de sécurité de Defender for Cloud au niveau du périmètre du groupe d'administration
- Déployer des contrôles de sécurité pour corriger les recommandations à grande échelle à l'aide de correctifs, de règles de gouvernance, de tâches de correction de stratégie et d'exemptions

ÉVALUER LA CONFORMITÉ RÉGLEMENTAIRE DANS DEFENDER FOR CLOUD

- Expliquer comment fonctionnent les normes de conformité, les contrôles et les évaluations dans Defender for Cloud, y compris le rôle du benchmark de sécurité Microsoft Cloud
- Naviguer dans le tableau de bord de conformité réglementaire pour identifier et examiner les contrôles de conformité défaillants
- Attribuer des normes de conformité réglementaires aux abonnements Azure et gérer l'étendue de conformité dans le portail Azure
- Générer des rapports de conformité et communiquez le statut en utilisant les téléchargements d'audit, les classeurs de conformité et le Gestionnaire de conformité Microsoft Purview.

GÉRER ET AJUSTER LA TAILLE DES ATTRIBUTIONS DE RÔLES RBAC POUR LES PRIVILEGES MINIMAUX

- Attribuer des rôles Azure intégrés à l'étendue appropriée à l'aide de principes de privilège minimum
- Créer des rôles Azure personnalisés et des rôles Microsoft Entra pour les opérations que les rôles intégrés ne couvrent pas au niveau d'autorisation approprié

- Identifier les attributions de rôles surprivilegiées et corrigez-les à l'aide de Defender for Cloud CSPM, CIEM (Cloud Infrastructure Entitlement Management) et Microsoft Entra examens d'accès

PROTÉGER LES DONNÉES DE SAUVEGARDE AVEC DES FONCTIONNALITÉS DE SÉCURITÉ SAUVEGARDE AZURE

- Configurer la suppression temporaire et l'immuabilité du coffre-fort pour protéger les points de récupération de sauvegarde contre la suppression
- Implémenter une autorisation multi-utilisateur à l'aide de Resource Guard pour empêcher les opérations de sauvegarde critiques non autorisées

IMPLÉMENTER DES CONTRÔLES DE SÉCURITÉ DANS L'INFRASTRUCTURE EN TANT QUE CODE

- Configurer Microsoft Defender pour DevOps pour analyser des modèles de Bicep et ARM dans GitHub Actions et Azure Pipelines
- Appliquer Azure Policy dans un flux de travail de stratégie en tant que code pour assurer la conformité en matière de sécurité lors du déploiement de l'IaC

DÉCRIRE LES SERVICES DE STOCKAGE AZURE

- Comparer les services de stockage Azure
- Décrire les niveaux de stockage
- Décrire les options de redondance
- Décrire les options de compte de stockage et les types de stockage
- Identifier les options de déplacement de fichiers, notamment AzCopy, l'Explorateur Stockage Azure et Azure File Sync
- Décrire les options de migration, notamment Azure Migrate et Azure Data Box

IMPLÉMENTER LA SÉCURITÉ ET GÉRER L'ACCES POUR STOCKAGE AZURE

- Configurer les paramètres de sécurité du compte de stockage, notamment le transfert sécurisé, le protocole TLS (Transport Layer Security) et les contrôles d'accès anonymes
- Sélectionner un modèle d'autorisation approprié pour différents scénarios d'accès, notamment l'identité managée pour les charges de travail de l'agent IA
- Créer et gérer des stratégies d'accès stockées pour contrôler le

cycle de vie des jetons SAP
- Désactiver l'autorisation de clé partagée et appliquer la conformité à l'aide de Azure Policy

CONFIGURER LA SÉCURITÉ RÉSEAU POUR STOCKAGE AZURE

- Décrire comment stockage Azure règles de pare-feu limitent l'accès via le point de terminaison public
- Créer des règles de réseau virtuel et des règles de réseau IP pour les sources approuvées
- Configurer des règles d'instance de ressource pour les services IA et PaaS Azure
- Ajouter des exceptions de service approuvé pour les services de plateforme Azure
- Implémenter des points de terminaison privés pour une connectivité de stockage entièrement privée

IMPLÉMENTER MICROSOFT DEFENDER POUR LE STOCKAGE

- Décrire les trois piliers de détection de Microsoft Defender pour le stockage et comment ils diffèrent du plan classique
- Activer Defender pour le stockage au niveau de l'abonnement et des ressources à l'aide d'un déploiement piloté par des stratégies
- Configurer l'analyse des programmes malveillants avec des limites mensuelles de Go pour le contrôle des coûts
- Configurer la détection des menaces de données sensibles
- Configurer les notifications d'alerte et vérifier que les sorties Defender atteignent l'équipe de sécurité appropriée

CONFIGURER LA SÉCURITÉ AU NIVEAU DE LA PLATEFORME POUR AZURE SQL

- Configurer l'authentification Microsoft Entra ID et désactiver l'authentification SQL sur Azure SQL
- Implémenter l'isolation réseau pour Azure SQL à l'aide de points de terminaison privés et de règles de pare-feu
- Activer le chiffrement transparent des données et configurer des clés gérées par le client pour les charges de travail réglementées
- Appliquer le masquage des données dynamiques et la sécurité au niveau des lignes pour restreindre l'accès aux données sensibles

CONFIGURER L'AUDIT POUR AZURE SQL DATABASE ET SQL MANAGED

INSTANCE

- Décrire Azure SQL fonctionnalités d'audit et sélectionner les groupes d'actions d'audit appropriés
- Configurer les destinations du journal d'audit pour Azure SQL Database
- Configurer l'audit pour SQL Managed Instance
- Concevoir une stratégie d'audit conforme à l'aide de plusieurs destinations de journal

IMPLÉMENTER MICROSOFT DEFENDER POUR LES BASES DE DONNÉES

- Décrire Microsoft Defender pour les plans de bases de données et les fonctionnalités de détection des menaces
- Activer Defender pour les bases de données Azure SQL au niveau de l'étendue de l'abonnement
- Activer Defender pour les bases de données relationnelles open source
- Configurer l'évaluation des vulnérabilités pour établir des bases de référence de sécurité pour Azure SQL
- Configurer le routage des alertes pour fournir des détections de Defender à l'équipe des opérations de sécurité

SEGMENTER ET ISOLER LES CHARGES DE TRAVAIL AZURE A L'AIDE DE CONTRÔLES DE SÉCURITÉ RÉSEAU

- Évaluer une topologie de réseau virtuel pour identifier les risques de mouvement latéral et les lacunes de segmentation du réseau
- Configurer des règles NSG pour appliquer l'accès au moindre privilège entre les charges de travail Azure
- Utiliser les ASG pour simplifier et maintenir les ensembles de règles NSG pour les charges de travail regroupées
- Configurer les règles d'administration de sécurité d'Azure Virtual Network Manager pour appliquer des politiques de sécurité réseau à l'échelle de l'organisation
- Vérifier les règles de sécurité réseau effectives à l'aide de diagnostics Network Watcher

CENTRALISER ET APPLIQUER L'INSPECTION DU TRAFIC A L'AIDE DE PARE-FEU AZURE

- Déterminer quand Pare-feu Azure est nécessaire pour résoudre les menaces que le filtrage du groupe de sécurité réseau (NSG) ne peut pas atténuer
- Configurer les collections de règles de pare-feu Azure et la stratégie de pare-feu pour contrôler et inspecter le trafic réseau

- Déployer Pare-feu Azure sur un hub Virtual WAN pour centraliser l'inspection du trafic hub-spoke et de branche

SÉCURISER LA CONNECTIVITÉ DISTANTE ET HYBRIDE A L'AIDE DE PASSERELLES VPN ET D'ACCES PRIVE MICROSOFT ENTRA

- Identifier les risques de sécurité dans les configurations de passerelle VPN pour les connexions de site à site et de point à site
- Configurer les paramètres de passerelle VPN pour réduire la surface d'attaque par le biais d'une authentification et d'un chiffrement plus forts
- Déployer Accès privé Microsoft Entra pour appliquer l'accès au niveau de l'application Confiance nulle pour les utilisateurs distants

ÉLIMINER L'EXPOSITION DU RÉSEAU PUBLIC AUX SERVICES PaaS AZURE

- Évaluer la surface d'attaque créée par les points de terminaison de service PaaS publics dans un environnement Azure
- Configurer des points de terminaison privés pour acheminer l'accès à Azure services PaaS et IA sur un réseau privé
- Configurer Azure Private Link service pour exposer des services internes sans créer de point de terminaison public
- Appliquer l'adoption du point de terminaison privé à grande échelle à l'aide de Azure Policy et de Defender for Cloud

ACCES SÉCURISÉ POUR L'IDENTITÉ DE L'AGENT DE MICROSOFT ENTRA

- Mapper la façon dont les agents IA s'authentifient et identifient où l'accès conditionnel s'applique
- Configurer des stratégies d'accès conditionnel limitées aux identités d'agent
- Contrôler l'accès aux agents et gérer les événements de cycle de vie des identités de l'agent

ANALYSER LES RISQUES LIÉS AUX IDENTITÉS IA A L'AIDE DE MICROSOFT DEFENDER XDR

- Découvrir des agents IA dans Microsoft Defender XDR à l'aide de l'inventaire des agents IA
- Évaluer le rayon de l'explosion des identités des agents en examinant les permissions, les sources de connaissances et la configuration des plans
- Analyser les chemins d'accès aux attaques susceptibles d'entraîner un accès non autorisé si une identité d'agent est

compromise

ACTIVER LA PROTECTION EN TEMPS RÉEL POUR LES AGENTS COPILOT STUDIO

- Décrire les fonctionnalités de protection de l'agent IA disponibles dans Microsoft Defender for Cloud Apps
- Activer la protection en temps réel pour les agents Copilot Studio dans le portail Microsoft Defender
- Vérifier que les résultats de la protection de l'agent apparaissent dans l'inventaire Microsoft Defender XDR, dans les alertes et dans la fonctionnalité Advanced Hunting.

CONFIGURER LA SÉCURITÉ DE LA PASSERELLE AI DANS MICROSOFT FOUNDRY

- Examiner l'architecture de la passerelle IA et expliquez comment elle sécurise le trafic du modèle IA
- Créer et configurer une instance de passerelle AI dans Microsoft Foundry
- Appliquer des contrôles d'accès et une surveillance pour sécuriser et auditer l'utilisation de la passerelle AI

CONFIGURER ET GÉRER DES GARDE-FOUS DANS MICROSOFT FOUNDRY

- Expliquer comment les garde-fous sécurisent les interactions de modèle dans Microsoft Foundry
- Décrire les contrôles de sécurité tels que les filtres de contenu, les listes de blocage et les boucliers d'invite
- Configurer et valider des garde-fous personnalisés pour différents types de charge de travail
- Évaluer l'efficacité du garde-fou et affiner les configurations pour l'assurance continue

PROTÉGER LES CHARGES DE TRAVAIL IA AVEC MICROSOFT DEFENDER POUR CLOUD

- Activer et configurer le plan des charges de travail IA dans Microsoft Defender pour cloud
- Examiner les aperçus des ressources IA dans le tableau de bord de sécurité des données et de l'IA
- Évaluer et améliorer la posture d'IA avec Cloud Security Posture Management (CSPM)
- Détecter et répondre aux menaces d'exécution à l'aide de la protection de la charge de travail

- Détecter et répondre aux menaces d'exécution à l'aide de la protection de la charge de travail cloud (CWP)

ACTIVER DEFENDER POUR LES SERVICES D'IA PROTECTION DES CHARGES DE TRAVAIL DANS MICROSOFT DEFENDER FOR CLOUD

- Activer le plan de Defender pour les services d'IA et configurer ses composants pour un abonnement Azure
- Examiner les alertes de protection contre les menaces IA dans le portail Defender
- Surveiller la posture de sécurité de l'IA à l'aide du tableau de bord de sécurité des données et de l'IA dans Microsoft Defender for Cloud

GÉRER LES AGENTS A L'AIDE DE MICROSOFT AGENT 365

- Activer et accéder à l'interface de gestion Microsoft Agent 365 dans le Microsoft 365 admin center
- Inscrire des agents et appliquer des contrôles d'accès pour appliquer des stratégies d'organisation
- Surveiller l'activité de l'agent et appliquer des contrôles de gouvernance à l'aide de Microsoft Agent 365

IDENTIFIER LES RISQUES LIÉS AUX DONNÉES IA A L'AIDE DE GESTION DE LA POSTURE DE SÉCURITÉ DES DONNÉES MICROSOFT PURVIEW

- Configurer Gestion de la posture de sécurité des données Microsoft Purview (DSPM) pour l'IA
- Évaluer les risques de surexposition des données de SharePoint qui affectent les données fondamentales de l'IA.
- Identifier les risques de données sensibles dans les interactions des applications Copilot et IA
- Interpréter DSPM pour les tableaux de bord IA et hiérarchiser les actions de correction

IMPLÉMENTER LE CHIFFREMENT DE DISQUE POUR LES MACHINES VIRTUELLES AZURE

- Comparer Azure options de chiffrement de disque managé et sélectionner l'approche appropriée pour les machines virtuelles nouvelles et existantes
- Configurer le chiffrement sur l'hôte avec des clés gérées par le client à l'aide d'un jeu de chiffrement de disque et de Azure Key Vault
- Appliquer le chiffrement de disque confidentiel aux machines virtuelles confidentielles

- Appliquer la conformité du chiffrement de disque à l'aide de Azure Policy

CONFIGURER LES FONCTIONNALITÉS DE SÉCURITÉ DE LANCEMENT APPROUVÉES POUR LES MACHINES VIRTUELLES AZURE

- Identifier la façon dont le lancement approuvé protège contre les menaces au niveau du démarrage à l'aide du démarrage sécurisé, vTPM et de la surveillance de l'intégrité
- Activer le lancement approuvé et configurer ses composants de sécurité sur les machines virtuelles Azure nouvelles et existantes
- Mettre à niveau des machines virtuelles Gen1 existantes vers Gen2 avec lancement approuvé activé
- Imposer l'adoption de Trusted Launch à l'aide des stratégies Azure intégrées

PLANIFIER ET IMPLÉMENTER AZURE BASTION

- Sélectionner la référence SKU Azure Bastion appropriée en fonction de la mise à l'échelle, de la fonctionnalité et des exigences de coût
- Déployer et configurer des Azure Bastion dans un réseau virtuel Azure
- Se connecter à des machines virtuelles Azure via Azure Bastion à l'aide du portail et des méthodes clientes natives
- Configurer des fonctionnalités Bastion avancées, notamment la prise en charge native du client, les liens partageables et l'enregistrement de session

GÉRER LA SÉCURITÉ DES SERVEURS HYBRIDES AVEC ARC

- Configurer RBAC et les listes d'autorisation/de blocage pour protéger les serveurs avec Arc contre l'installation d'une extension non autorisée
- Affecter et gérer des Azure Policy pour les serveurs avec Arc afin d'appliquer des bases de référence de sécurité
- Surveiller la posture de sécurité des serveurs inscrits à Arc dans Microsoft Defender for Cloud
- Appliquer des stratégies de configuration de machine aux serveurs inscrits à Arc

IMPLÉMENTER MICROSOFT DEFENDER POUR LES SERVEURS

- Sélectionner Defender pour les serveurs Plan 1 ou Plan 2 en fonction des fonctionnalités requises et intégrer des machines

virtuelles Azure et des serveurs connectés à Arc
- Configurer l'analyse des vulnérabilités à l'aide de Defender Vulnerability Management sans agent et basée sur l'agent
- Gérer l'intégration de Microsoft Defender for Endpoint et configurer l'analyse sans agent et la surveillance de l'intégrité des fichiers

ACTIVER ET APPLIQUER L'ACCES JUSTE-A-TEMPS AUX MACHINES VIRTUELLES

- Examiner comment l'accès juste-à-temps aux machines virtuelles réduit la surface d'attaque sur les ports de gestion
- Activer JIT et configurer des stratégies d'accès par port sur des machines virtuelles Azure
- Demander et approuver l'accès JIT et vérifier l'activité d'accès
- Appliquer l'adoption du JIT dans un patrimoine de machines virtuelles à l'aide de Azure Policy

APPLIQUER LA CONFIGURATION DE SÉCURITÉ DES MACHINES VIRTUELLES AVEC AZURE MACHINE CONFIGURATION

- Découvrir comment Azure Configuration de l'ordinateur audite et applique les paramètres au niveau du système d'exploitation à l'aide de Azure Policy
- Déployer l'extension Azure Machine Configuration et configurer les prérequis requis
- Affecter des stratégies de base de référence de sécurité Windows et Linux intégrées dans les modes d'audit et d'application
- Créer et publier une configuration d'ordinateur personnalisée pour les exigences spécifiques à l'organisation

DÉTECTER LES RISQUES LIÉS AUX CONTENEURS A L'AIDE DE MICROSOFT DEFENDER POUR LES CONTENEURS

- Décrire les piliers d'architecture et de protection de Microsoft Defender pour conteneurs
- Activer et configurer le plan Defender pour conteneurs dans Microsoft Defender for Cloud
- Évaluer les résultats de l'analyse des vulnérabilités des images de conteneur issues de l'analyse effectuée par Azure Container Registry (ACR)
- Interpréter les alertes de menaces au moment de l'exécution et les recommandations de posture de sécurité pour les clusters AKS

IMPLÉMENTER DES CONTRÔLES DE SÉCURITÉ POUR AZURE KUBERNETES SERVICE

- Configurer Microsoft Entra ID intégration et RBAC pour l'authentification et l'autorisation du serveur d'API AKS
- Implémenter des contrôles de sécurité réseau, notamment des clusters privés, des plages d'adresses IP autorisées et des stratégies réseau
- Appliquer l'identité de charge de travail et les identités managées afin d'éliminer la gestion des identifiants pour les charges de travail AKS
- Appliquer les normes de sécurité des pods et les restrictions d'accès aux conteneurs

IMPLÉMENTER DES CONTRÔLES DE SÉCURITÉ POUR AZURE CONTAINER REGISTRY, CONTAINER INSTANCES ET CONTAINER APPS

- Implémenter des contrôles d'accès et une isolation réseau pour Azure Container Registry
- Configurer des contrôles de sécurité pour les charges de travail Azure Container Instances
- Appliquer des contrôles d'entrée, une identité managée et une gestion des secrets pour Azure Container Apps

IMPLÉMENTER DES CONTRÔLES DE SÉCURITÉ POUR LES APPLICATIONS DE FONCTION AZURE ET LES APPLICATIONS LOGIQUES

- Configurer des contrôles d'authentification et d'autorisation pour les applications de fonction Azure
- Implémenter des contrôles d'accès réseau pour les applications de fonction, notamment l'intégration de réseau virtuel et les points de terminaison privés
- Appliquer l'identité managée, la sécurité du connecteur et l'isolation réseau pour les applications logiques Azure

IMPLÉMENTER DES CONTRÔLES DE SÉCURITÉ POUR AZURE APP SERVICES ET WEB APPLICATION FIREWALL

- Implémenter des contrôles d'authentification, d'identité managée et de réseau pour Azure App Service
- Configurer les stratégies de pare-feu d'applications web, y compris les ensembles de règles gérés et les règles personnalisées
- Intégrer Web Application Firewall avec App Service pour assurer une protection en périphérie

IMPLÉMENTER LA SÉCURITÉ DU BACK-END D'API A L'AIDE DE GESTION DES API AZURE

- Configurer les stratégies d'authentification et d'autorisation des API, notamment la validation JWT et OAuth 2.0 avec Microsoft Entra ID
- Implémenter des contrôles de sécurité réseau, notamment le filtrage IP, la limitation de débit et l'intégration de réseau virtuel pour gestion des API
- Appliquer la sécurité des connexions back-end à l'aide de l'authentification par certificat client et du protocole TLS mutuel
- Configurer la passerelle AI dans Gestion des API pour sécuriser et régir les points de terminaison de modèle IA

CONNECTER DES ENVIRONNEMENTS HYBRIDES ET MULTICLOUDS A MICROSOFT DEFENDER FOR CLOUD

- Expliquer le modèle de connectivité multicloud dans Defender for Cloud, notamment le fonctionnement de l'authentification fédérée pour les connecteurs AWS et GCP
- Planifier une stratégie de connecteur pour les environnements hybrides et multiclouds, notamment l'étendue, l'intervalle d'analyse et les autorisations requises par type d'environnement
- Connecter des machines locales à des Defender for Cloud à l'aide de serveurs compatibles avec Azure Arc
- Connecter des comptes AWS à Defender for Cloud à l'aide du connecteur cloud natif et du modèle CloudFormation
- Connecter des projets GCP à Defender for Cloud à l'aide du connecteur cloud natif et du script de déploiement GCloud
- Vérifier l'intégrité de la connectivité multicloud et confirmer les surfaces de couverture CSPM et CWPP dans les environnements connectés

IDENTIFIER LES RISQUES DE SÉCURITÉ A L'AIDE DE LA GESTION DE LA POSTURE DE SÉCURITÉ CLOUD

- Différencier les fonctionnalités fondamentales des plans CSPM et CSPM Defender, y compris les fonctionnalités de gestion de la posture de sécurité basées sur l'IA.
- Interpréter le score de sécurité cloud et les recommandations de sécurité à l'aide du modèle de hiérarchisation basé sur les risques dans le portail Microsoft Defender
- Identifier les chemins d'attaque exploitables en externe, y compris ceux ciblant des charges de travail IA, à l'aide de l'analyse des chemins d'attaque
- Exécuter des requêtes basées sur des graphiques dans Cloud

Security Explorer pour détecter de manière proactive les risques de sécurité dans les environnements Azure

DÉCOUVRIR DES RESSOURCES ET DES VULNÉRABILITÉS NON PROTÉGÉES A L'AIDE DE MICROSOFT DEFENDER EXTERNAL ATTACK SURFACE MANAGEMENT

- Explorer les caractéristiques et fonctionnalités d'EASM, notamment les types de ressources, les états des ressources, et la façon dont l'analyse externe diffère des autres outils Defender.
- Configurer la découverte de ressources à l'aide de semences pour identifier l'infrastructure et les connexions de ressources accessibles sur Internet inconnues
- Utiliser des tableaux de bord EASM pour hiérarchiser les vulnérabilités et les risques d'hygiène de sécurité sur votre surface d'attaque
- Intégrer les résultats EASM à CSPM Defender pour analyser les chemins d'attaque à partir de ressources exposées sur Internet

ÉVALUER LA CONFORMITÉ RÉGLEMENTAIRE DANS DEFENDER FOR CLOUD

- Expliquer comment fonctionnent les normes de conformité, les contrôles et les évaluations dans Defender for Cloud, y compris le rôle du benchmark de sécurité Microsoft Cloud
- Naviguer dans le tableau de bord de conformité réglementaire pour identifier et examiner les contrôles de conformité défaillants
- Attribuer des normes de conformité réglementaires aux abonnements Azure et gérer l'étendue de conformité dans le portail Azure
- Générer des rapports de conformité et communiquez le statut en utilisant les téléchargements d'audit, les classeurs de conformité et le Gestionnaire de conformité Microsoft Purview.

ACTIVER ET CONFIGURER DES PLANS DE PROTECTION DES CHARGES DE TRAVAIL DANS MICROSOFT DEFENDER FOR CLOUD

- Identifier les plans CWPP disponibles dans Defender for Cloud et expliquez quelles charges de travail protègent chaque plan, y compris les Defender pour les services d'IA et les Defender pour les API
- Activer les plans de protection des charges de travail au niveau de l'abonnement à l'aide des paramètres d'environnement dans le portail Azure
- Configurer Defender pour les serveurs (Plan 1 et Plan 2) et

Defender pour les sous-paramètres de stockage pour vos besoins en matière de protection
- Déployer des plans de protection à grande échelle à l'aide de groupes d'administration et de Azure Policy, et vérifier la couverture du plan à l'aide du classeur Couverture

CONFIGURER LES PARAMETRES DE GESTION DES VULNÉRABILITÉS MICROSOFT DEFENDER POUR LES MACHINES VIRTUELLES AZURE

- Gérer des vulnérabilités Microsoft Defender s'intègre à Defender pour les serveurs Plan 1 et Plan 2 afin de fournir une analyse des vulnérabilités sans agent pour les machines virtuelles Azure
- Configurer le balayage des vulnérabilités pour les machines virtuelles Azure au niveau de l'abonnement et de la portée de la machine à l'aide des paramètres de Defender for Cloud.
- Passer en revue les résultats des vulnérabilités, interprétez les données CVE et de gravité, puis créer des règles de désactivation pour gérer les risques acceptés dans le portail Defender
- Appliquer les capacités premium de Defender pour Serveurs Plan 2, notamment l'évaluation des bases de référence de sécurité et le blocage des applications, pour renforcer la posture de sécurité des machines virtuelles.

CRÉER ET GÉRER DES ESPACES DE TRAVAIL MICROSOFT SENTINEL

- Décrire l'architecture de l'espace de travail Microsoft Sentinel
- Intégrer un espace de travail Microsoft Sentinel à Microsoft Defender
- Gérer un espace de travail Microsoft Sentinel dans Microsoft Defender

GÉRER LE CONTENU DANS MICROSOFT SENTINEL

- Installer une solution de hub de contenu dans Microsoft Sentinel
- Connecter un dépôt GitHub à Microsoft Sentinel

CONNECTER DES SERVICES MICROSOFT A MICROSOFT SENTINEL

- Connecter les connecteurs de service Microsoft
- Expliquer comment les connecteurs décrétent automatiquement des incidents dans Microsoft Sentinel

CONNECTER DES SOURCES DE DONNÉES SYSLOG A MICROSOFT SENTINEL

- Décrire la règle de collecte de données de l'agent Azure Monitor pour Syslog
- Installer et configurer l'extension Agent Linux Azure Monitor avec la règle de collecte de données Syslog
- Exécuter les scripts de déploiement et de connexion d'Azure Arc Linux
- Vérifier que les données de journal Syslog sont disponibles dans Microsoft Sentinel
- Créer un analyseur en utilisant KQL dans Microsoft Sentinel

CONNECTER DES JOURNAUX COMMON EVENT FORMAT A MICROSOFT SENTINEL

- Expliquer les options de déploiement du connecteur Common Event Format dans Microsoft Sentinel
- Exécuter le script de déploiement pour le connecteur Common Event Format

CONNECTER DES HÔTES WINDOWS A MICROSOFT SENTINEL

- Connecter les machines virtuelles Windows Azure à Microsoft Sentinel
- Connecter des hôtes Windows non Azure à Microsoft Sentinel
- Installer et configurer un connecteur de données pour collecter des événements Sysmon

IMPLÉMENTER DES REGLES D'AUTOMATISATION ET DES PLAYBOOKS DANS MICROSOFT SENTINEL

- Expliquer la différence entre les règles d'automatisation et les playbooks dans Microsoft Sentinel
- Créer des règles d'automatisation pour automatiser les tâches de gestion des incidents
- Configurer et activer un playbook prédéfini à partir du hub de contenu Microsoft Sentinel
- Créer un playbook Logic Apps personnalisé et le connecter à une règle d'automatisation

GÉRER LE STOCKAGE DES DONNÉES ET INTERROGER LES JOURNAUX D'AUDIT DANS MICROSOFT SENTINEL

- Créer des tables de journal personnalisées dans un espace de travail Microsoft Sentinel pour stocker des données ingérées

non standard
- Configurer les niveaux de rétention des données et les stratégies d'archivage pour les tables Microsoft Sentinel
- Connecter Microsoft Purview Audit en tant que source de données dans Microsoft Sentinel
- Interroger les journaux d'audit Purview dans le portail Microsoft Defender XDR

DÉCRIRE SÉCURITÉ MICROSOFT COPILOT

- Décrire ce qu'est Copilote de sécurité Microsoft.
- Décrire la terminologie de Microsoft Sécurité Copilot.
- Décrire comment le Copilote de sécurité Microsoft traite les requêtes de commande.
- Décrire les éléments d'une invite efficace
- Décrire comment activer Microsoft Security Copilot.

CONFIGURER DES ESPACES DE TRAVAIL POUR MICROSOFT SECURITY COPILOT

- Planifier un déploiement d'espace de travail en évaluant la capacité, la résidence des données et les exigences de rôle
- Créer un espace de travail Security Copilot avec les SCUs appropriés, la sélection géographique et les paramètres de partage de données
- Attribuer et gérer des rôles et des autorisations dans un espace de travail
- Configurer les paramètres et plug-ins du propriétaire au niveau de l'espace de travail
- Affecter des espaces de travail pour les agents de Microsoft Security Copilot intégrés
- Surveiller et ajuster l'utilisation de la capacité de l'espace de travail

GÉRER LES PLUG-INS ET LES AGENTS DANS MICROSOFT SECURITY COPILOT

- Configurer les paramètres de plug-in pour régir qui peut ajouter et gérer des plug-ins personnalisés au niveau de l'étendue de l'utilisateur et de l'organisation
- Restreindre l'accès au plug-in préinstallé pour gérer la disponibilité dans les expériences incorporées et autonomes
- Découvrir et configurer des agents développés par Microsoft à l'aide de la bibliothèque d'agents Security Copilot.
- Acquérir et configurer des agents développés par un partenaire à l'aide du Magasin de sécurité, y compris le flux de travail

d'approbation de l'administrateur global.
- Gérer les agents en contrôlant l'état d'exécution, en modifiant la configuration et en conservant la mémoire de l'agent

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com