LES TECHNOLOGIES DE SÉCURITÉ SUR MICROSOFT AZURE – TH-500

Programme *(Mis à jour le 27/10/2023)*

Sécuriser les solutions Azure avec Microsoft Entra ID

- Configurer Azure AD et Azure AD Domain Services pour la sécurité
- Créer des utilisateurs et des groupes qui permettent une utilisation sécurisée de votre locataire
- Utiliser MFA pour protéger les identités des utilisateurs
- Configurer les options de sécurité avec mot de passe

Implémenter l'identité hybride

- Déployer Microsoft Entra Connect
- Choisir et configurer l'option d'authentification la mieux adaptée à vos besoins de sécurité
- Configurer la récupération du mot de passe

Déployer la protection des identités Entra ID

- Déployer et configurer la protection des identités
- Configurer MFA pour les utilisateurs, les groupes et les applications
- Créer des politiques d'accès conditionnel pour garantir votre sécurité
- Créer et suivre un processus de révision d'accès

Configurer la gestion des identités privilégiées Microsoft Entra

- Décrire Zero Trust et son impact sur la sécurité
- Configurer et déployer des rôles à l'aide de Privileged Identity Management (PIM)
- Évaluer l'utilité de chaque paramètre PIM en ce qui concerne vos objectifs de sécurité

Concevoir une stratégie de gouvernance d'entreprise

- Expliquer le modèle de responsabilité partagée et son impact sur votre configuration de sécurité
- Créer des stratégies Azure pour protéger vos solutions
- Configurer et déployer l'accès aux services à l'aide de RBAC

Implémenter la sécurité du périmètre

- Définir la défense en profondeur
- Protéger votre environnement des attaques par déni de service
- Sécuriser vos solutions à l'aide de pare-feu et de VPN
- Explorer votre configuration de sécurité de périmètre de bout en bout en fonction de votre posture de sécurité

Configurer la sécurité réseau

- Déployer et configurer des groupes de sécurité réseau pour protéger vos solutions Azure
- Configurer et verrouiller les points de terminaison de service et les liaisons privées
- Sécuriser vos applications avec Application Gateway, web app Firewall et Front Door
- Configurer ExpressRoute pour contribuer à protéger votre trafic

Configurer et gérer la sécurité des ordinateurs hôtes

Référence

THCI3164

Durée

4 jours / 28 heures

Prix HT / stagiaire

2850€

Objectifs pédagogiques

- Sécuriser les solutions Azure avec Microsoft Entra ID
- Implémenter l'identité hybride
- Déployer la protection Microsoft Entra ID
- Configurer la gestion des identités privilégiées Microsoft Entra ID
- Concevoir une stratégie de gouvernance d'entreprise
- Implémenter la sécurité du périmètre
- Configurer la sécurité réseau
- Configurer et gérer la sécurité des ordinateurs hôtes
- Activer la sécurité des conteneurs
- Déployer et sécuriser Azure Key Vault
- Mettre en œuvre la sécurité du stockage
- Configurer et gérer la sécurité de la base de données SQL
- Configurer et gérer Azure Monitor
- Activer et gérer Microsoft Defender pour le cloud
- Configurer et surveiller Microsoft Sentinel

Niveau requis

- Il faut avoir suivi la formation « Azure Fundamentals » et impérativement la formation «Azure Administrator », ou avoir un niveau d'expérience sur Azure équivalent, pour comprendre le contenu du cours.
- Avoir des connaissances de base en langue anglaise car le support de cours, l'examen sont en langue anglaise et les ateliers seront réalisés sur des VM en anglais
- Des systèmes d'exploitation Windows et Linux et les langages de script.

Public concerné

- Administrateur et responsable de solutions traditionnelles ayant des 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.

- Configurer et déployer Endpoint Protection
- Déployer une stratégie d'accès privilégié pour les appareils et les stations de travail privilégiées
- Sécuriser vos machines virtuelles et y accéder
- Déployer Windows Defender
- Pratiquer la sécurité par couche en examinant et en implémentant Security
- Center et les security Benchmarks

Activer la sécurité des conteneurs

- Définir les outils de sécurité disponibles pour les conteneurs dans Azure
- Configurer les paramètres de sécurité pour les conteneurs et les services Kubernetes
- Verrouiller les ressources réseau, de stockage et d'identité connectées à vos conteneurs
- Déployer RBAC pour contrôler l'accès aux conteneurs

Déployer et sécuriser Azure Key Vault

- Définir ce qu'est un coffre de clés et comment il protège les certificats et les secrets
- Déployer et configurer Azure Key Vault
- Sécuriser l'accès et l'administration de votre coffre de clés
- Stocker les clés et les secrets dans votre coffre de clés
- Explorer la sécurité des clés, comme la rotation des clés et la sauvegarde/récupération

Configurer les fonctionnalités de sécurité des applications

- Inscrire une application dans Azure à l'aide de l'inscription d'application
- Sélectionner et configurer les utilisateurs de Microsoft Entra pouvant accéder à chaque application
- Configurer et déployer des certificats d'application web

Implémenter la sécurité du stockage

- Définir la souveraineté des données et comment les obtenir dans Azure
- Configurer l'accès au Stockage Azure de manière sécurisée et gérée
- Chiffrer vos données pendant qu'elles sont au repos et en transit
- Appliquer des règles pour de conservation des données

Configurer et gérer la sécurité de la base de données SQL

- Configurer les utilisateurs et les applications qui ont accès à vos bases de données SQL
- Bloquer l'accès à vos serveurs à l'aide de pare-feu
- Découvrir, classer et auditer l'utilisation de vos données
- Chiffrer et protéger vos données pendant qu'elles sont stockées dans la base de données.

Configurer et gérer Azure Monitor

- Configurer et surveiller Azure Monitor
- Définir les métriques et les journaux que vous souhaitez suivre pour vos applications Azure
- Connecter les sources de données et configurer Log Analytics
- Créer et surveiller les alertes associées à la sécurité de vos solutions

Activer et gérer Microsoft Defender pour le cloud

- Définir les types les plus courants de cyberattaques
- Configurer Microsoft Defender pour le cloud en fonction de votre posture de sécurité
- Examiner le score de sécurité et l'élever
- Verrouiller vos solutions à l'aide de la protection de charge de travail de Microsoft Defender pour le cloud
- Activer l'accès juste-à-temps et d'autres fonctionnalités de sécurité

Configurer et surveiller Microsoft Sentinel

- Expliquer ce qu'est Microsoft Sentinel et comment l'utiliser

- Déployer Microsoft Sentinel
- Connecter des données à Microsoft Sentinel, comme Azure Logs, Microsoft Entra ID et autres
- Suivre les incidents à l’aide de classeurs, de playbooks et de techniques de chasse