Microsoft Azure :
Les meilleures pratiques

WorkshopPLUS

Optimisez votre investissement dans Microsoft Azure et augmentez votre sécurité pour l'accès aux applications et aux données

Public concerné :

Cet atelier est destiné aux organisations utilisant Microsoft Azure et souhaitant comprendre et explorer les fonctionnalités de sécurité disponibles.

Introduction

Aujourd'hui, les entreprises doivent se concentrer sur la création de solutions sécurisées dans le cloud qui apportent de la valeur à leurs clients, partenaires et actionnaires. Le cloud computing offre la possibilité de transférer une partie des coûts, des risques et des efforts de gestion d'une infrastructure informatique à un fournisseur indépendant et expérimenté.

Microsoft possède une expérience de plusieurs décennies dans la création de logiciels d'entreprise et l'exploitation de certains des plus grands services en ligne au monde. Microsoft a tiré parti de cette expérience pour mettre en œuvre et améliorer continuellement les pratiques de développement de logiciels, de gestion opérationnelle et d'atténuation des menaces qui sont essentielles pour renforcer la protection des services et des données dans le cloud.

L'atelier Azure Security offre aux participants une vaste connaissance et une bonne compréhension des principales fonctionnalités de sécurité disponibles dans Azure.

Principales caractéristiques et avantages

Chaque module présente un niveau d'explication technique concernant les fonctionnalités de sécurité Azure et des meilleures pratiques recommandées. Les labs permettent aux participants de construire leur environnement Azure depuis le début, tout en leur permettant de se concentrer sur les fonctionnalités de sécurité décrites dans chaque module. Azure Resource Manager et Azure Service Manager sont utilisés au cours des travaux pratiques pour illustrer leurs différences.

Plus-values techniques

Après avoir suivi cette formation, vous aurez gagné en connaissance sur les fonctionnalités disponibles de sécurité dans Azure et cela vous aidera à vous décider de ce qui vous convient pour sécuriser votre environnement au mieux, en fonction des principes fondamentaux de Microsoft suivants :

- Sécurité : Notre priorité est de protéger vos données avec une technologie, des processus et un cryptage de pointe.

- Confidentialité et contrôle : Vous contrôlez la confidentialité de vos données, qui y a accès et où elles résident.
- Conformité : Nous offrirons toujours le plus grand portefeuille de normes de conformité et de certifications dans l'industrie.
- Transparence : Vous aurez toujours une visibilité complète de l'emplacement de vos données et de leur gestion.

Programme

Ce workshop se déroule sur trois jours complets. Les stagiaires doivent anticiper les horaires de début et de fin pour l'ensemble des journées. Partir avant la fin de chaque cours n'est pas recommandé.

Délivré par des ingénieurs Microsoft expérimentés, l'atelier Azure Security vous aide à comprendre et à implémenter les fonctions de sécurité sur Azure.

Module 01 : Introduction à la Sécurité dans Azure Microsoft : Ce module présente les technologies de sécurité disponibles sur Microsoft Azure, un aperçu de l'architecture Cybersecurity de Microsoft et explique comment tirer parti du Cloud pour améliorer la protection, la détection et la réponse aux menaces.

Module 02 : Sécurisation du réseau : Ce module présente les composants disponibles pour sécuriser les communications réseau dans Azure. Vous apprendrez à utiliser les groupes de sécurité réseau (NSG) pour créer des règles (ACL) de contrôle d'accès en autorisant ou en refusant la communication entre les composants, ainsi que la sécurisation de la communication entre vos locaux et Azure.

Module 03 : Identité dans le Cloud et Accès : Ce module présente le concept «L'identité est le nouveau périmètre» et décrit les événements de risque et les vulnérabilités potentielles affectant les identités de votre organisation, ainsi que les fonctionnalités de sécurité d'Azure, telles que les contrôles de sécurité disponibles dans Microsoft Azure Active Directory (Azure AD), Le proxy d'application Azure AD, la gestion des identités privilégiées (PIM) et Cloud App Security.

Module 04 : Chiffrement et protection des données : Ce module présente le coffre-fort de clés Azure (Key Vault) et divers scénarios utilisant l'encryption et la protection des données dans Azure. Cela inclut le cryptage des données au repos, en transit et en cours d'utilisation, en authentifiant uniquement les utilisateurs autorisés au niveau de la base de données ou de l'application, et en limitant l'accès des utilisateurs au sous-ensemble approprié de données.

Module 05 : Gestion des menaces : Dans ce module, vous apprendrez l'importance du déploiement de tout type de solution antimalware pour les machines virtuelles dans Azure. Vous découvrirez l'architecture Microsoft Antimalware, les scénarios de déploiement à l'aide de PowerShell et du portail Azure.

Module 06 : Sécurité Web dans Azure : Ce module couvre les menaces courantes des applications Web et les fonctionnalités qu'Azure a pour gérer et accéder en toute sécurité aux applications Web.

Module 07 : Monitoring d'Azure, journalisation et génération de rapports : Ce module couvre les mécanismes de surveillance continue et d'audit des activités pour aider à la détection des menaces potentielles et fournir un enregistrement

Prérequis :

- Connaissance des composants d'infrastructure Microsoft (Active Directory, Windows Server / Client)
- Compréhension des différences entre ASM et ARM
- Connaissances dans le déploiement de ressources dans les deux modèles à l'aide du Portail et de PowerShell
- Connaissance des modèles ARM

Plus-values techniques :

- Sécurité des données et Conformité
- Protection des identités
- Sécurisation des accès à Azure
- Sécurité des applications Web
- Audit et Monitoring

des événements critiques en cas de violation. Ces fonctionnalités de sécurité sont équilibrées par la capacité à implémenter rapidement les fonctionnalités et à réduire les risques de sécurité sans compromettre la productivité des développeurs ou l'expérience des clients.