KA SOLUTION
WWW.KASOLUTION.COM.BR

Curso Oficial da Microsoft

(AZ-500) Microsoft Azure Security Technologies

Microsoft Azure Security Technologies (AZ-500)
Curso Oficial Microsoft

Este curso fornece aos Profissionais de Segurança de TI o conhecimento e as habilidades necessárias para implementar controles de segurança, manter a postura de segurança de uma organização e identificar e corrigir vulnerabilidades. Este curso inclui também segurança para identidade e acesso, proteção de plataforma, dados e aplicativos e operações de segurança.

Carga Horária: 4 dias /8 noites

Depois de concluir este curso, os alunos serão capazes de:

- Implementar estratégias de governança corporativa, incluindo controle de acesso baseado em função, políticas do Azure e bloqueios de recursos.
- Implemente uma infraestrutura do Azure AD incluindo usuários, grupos e autenticação multifator.
- Implementar o Azure AD Identity Protection, incluindo políticas de risco, acesso condicional e revisões de acesso.
- Implementar o Azure AD Privileged Identity Management incluindo funções do Azure AD e recursos do Azure.
- Implementar o Azure AD Connect incluindo métodos de autenticação e sincronização de diretório local.
- Implementar estratégias de segurança de perímetro, incluindo Firewall do Azure.
- Implementar estratégias de segurança de rede, incluindo grupos de segurança de rede e grupos de segurança de aplicativos.
- Implementar estratégias de segurança de host, incluindo proteção de endpoint, gerenciamento de acesso remoto, gerenciamento de atualização e criptografia de disco.
- Implementar estratégias de segurança de contêiner, incluindo instâncias de contêiner do Azure, Azure Container Registry e Azure Kubernetes.
- Implementar o Azure Key Vault incluindo certificados, chaves e segredos.
- Implementar estratégias de segurança de aplicativo, incluindo registro de aplicativo, identidades gerenciadas e terminais de serviço.
- Implementar estratégias de segurança de armazenamento, incluindo assinaturas de acesso compartilhado, políticas de retenção de blob e autenticação de arquivos do Azure.
- Implementar estratégias de segurança de banco de dados, incluindo autenticação, classificação de dados, mascaramento dinâmico de dados e sempre criptografados.
- Implementar o Azure Monitor incluindo fontes conectadas, análise de log e alertas.
- Implementar a Central de Segurança do Azure, incluindo políticas, recomendações e acesso just in time à máquina virtual.
- Implementar o Azure Sentinel incluindo pastas de trabalho, incidentes e manuais.

Módulo 1: Gerenciar Identidade e Acesso

Este módulo cobre o Azure Active Directory, Proteção de Identidade do Azure, Enterprise Governance, Azure AD PIM e Identidade Híbrida.

Lições

- Azure Active Directory.
- Proteção de identidade do Azure.
- Governança Corporativa.
- Azure AD Privileged Identity Management.
- Identidade Híbrida.

Laboratórios:

- Controle de Acesso Baseado em Funções.
- Política Azure.
- Bloqueios do Gerenciador de Recursos.
- MFA, Acesso Condicional e Proteção de Identidade AAD.
- Azure AD Privileged Identity Management.
- Implementar Sincronização de Diretório.

Depois de concluir este módulo, os alunos serão capazes de:

- Implementar estratégias de governança corporativa, incluindo controle de acesso baseado em função, políticas do Azure e bloqueios de recursos.
- Implemente uma infraestrutura do Azure AD incluindo usuários, grupos e autenticação multifator.
- Implementar o Azure AD Identity Protection incluindo políticas de risco, acesso condicional e revisões de acesso.
- Implementar o Azure AD Privileged Identity Management incluindo funções do Azure AD e recursos do Azure.
- Implementar o Azure AD Connect incluindo métodos de autenticação e sincronização de diretório local.

Módulo 2: Implementar Proteção de Plataforma

Este módulo cobre perímetro, rede, host e segurança de contêiner.

Lições

- Segurança de Perímetro.
- Segurança de Rede.
- Segurança de Host.
- Segurança de Contêiner.

Laboratórios:

- Grupos de segurança de rede e grupos de segurança de aplicativos.
- Firewall do Azure.
- Configurando e protegendo ACR e AKS.

Depois de concluir este módulo, os alunos serão capazes de:

- Implementar estratégias de segurança de perímetro, incluindo Firewall do Azure.
- Implementar estratégias de segurança de rede, incluindo grupos de segurança de rede e grupos de segurança de aplicativos.
- Implementar estratégias de segurança de host, incluindo proteção de endpoint, gerenciamento de acesso remoto, gerenciamento de atualização e criptografia de disco.
- Implementar estratégias de segurança de contêiner, incluindo instâncias de contêiner do Azure, Azure Container Registry e Azure Kubernetes.

Módulo 3: Dados e Aplicativos Seguros

Este módulo cobre o Azure Key Vault, segurança de aplicativos, segurança de armazenamento e segurança de banco de dados SQL.

Lições

- Azure Key Vault.
- Segurança do Aplicativo.
- Segurança de Armazenamento.
- Segurança de Banco de Dados SQL.

Laboratórios:

- Key Vault (implementação de dados seguros configurando o Always Encrypted).
- Protegendo o Banco de Dados SQL do Azure.
- Endpoints de serviço e armazenamento seguro.

Depois de concluir este módulo, os alunos serão capazes de:

- Implementar o Azure Key Vault incluindo certificados, chaves e segredos.
- Implementar estratégias de segurança de aplicativo, incluindo registro de aplicativo, identidades gerenciadas e terminais de serviço.
- Implementar estratégias de segurança de armazenamento, incluindo assinaturas de acesso compartilhado, políticas de retenção de blob e autenticação de arquivos do Azure.
- Implementar estratégias de segurança de banco de dados, incluindo autenticação, classificação de dados, mascaramento dinâmico de dados e sempre criptografados.

Módulo 4: Gerenciar Operações de Segurança

Este módulo cobre o Azure Monitor, o Azure Security Center e o Azure Sentinel.

Lições

- Azure Monitor.
- Centro de Segurança Azure.
- Azure Sentinel.

Laboratórios:

- Azure Monitor.
- Central de Segurança do Azure.
- Azure Sentinel.

Depois de concluir este módulo, os alunos serão capazes de:

- Implementar o Azure Monitor incluindo fontes conectadas, análise de log e alertas.
- Implementar a Central de Segurança do Azure, incluindo políticas, recomendações e acesso “just in time” à máquina virtual.
- Implementar o Azure Sentinel incluindo pastas de trabalho, incidentes e manuais.