Bootcamp: Profissional Azure Cloud Computing

Desafio Prático

Módulo 4: Soluções de Segurança, Governança, Compliance e Migração

Enunciado da avaliação

Com o objetivo de avaliar os conhecimentos obtidos, você deverá criar um ambiente com as seguintes premissas:

1. Criar 5 usuários no Azure Active directory com base na tabela abaixo:

Nome	Cargo	País
User1	Gerente de TI	Brasil
User2	Administrador de Rede	Brasil
User3	Diretor de TI	Estados Unidos
User4	Secretario	Estados Unidos
User5	Estagiario	Brasil

2. Dar permissão no Azure AD para que os Usuários Administradores (User1 e User3) tenham permissões de Global Administrator no Azure AD.

3. Dentro da guia segurança do Azure AD, acesse Acesso condicional e crie o local Brasil contendo apenas o Brasil como local.

4. Criar uma política de acesso condicional com os usuários User1 e User3, com as seguintes premissas:

   - Aplicações: Todas
   - Condições: Locais:Brasil
   - Conceder: Permitir Acesso e selecionar Requer autenticação multifator.

- Habilitar a política: Ativado

Obs.: Não esqueça de configurar a política somente para os usuários aqui solicitados.

5. Dentro da guia segurança do Azure AD, acesse o Identity Protection e em seguida, acesse a guia “Política de risco de entrada”.

6. Configure a Política de risco de entrada com as seguintes premissas:

   - Usuários: User1

   - Risco de entrada: Médio e Superior

   - Controles: Ativado

7. Instale o Tor Browser no seu computador (pode desinstalar após a execução deste teste) por meio do site https://www.torproject.org/download/.

8. Usando o Tor Browser, tente acessar o portal do azure usando o usuário User1 e anote o comportamento.

9. Aguarde 10 minutos e, dentro do identity protection, acesse a guia Usuários Arriscados e verifique se existe algum usuário na lista, caso exista, selecione ele e observe as informações fornecidas, em seguida, clique no botão “Ignorar risco dos usuários”.

10. Dentro do portal do Azure, criei um recurso “Azure Sentinel” (será solicitado para criar um workspace, crie um com o nome IGTI-MODULO04 na região East-US).

11. Acesse a guia conectores de dados e localize “Azure Active Directory Identity Protection”, selecione ele, role a barra da blade da direita até o máximo e clique em “Abrir a página do conector”.

12. Na página aberta, em Configuração clique em Conectar.

13. Volte para o Azure Sentinel e clique em “Pastas de Trabalho” (Workbooks) e localize “Logs de Entrada do Azure AD” e, após selecionar ele, clique no botão (do lado direito) em Salvar e OK.

14. Realize ao menos 6 tentativas de acesso ao portal em uma guia privada com os usuários: User3, User4 e User5 com a senha errada.

15. Volte ao Azure Sentinel e vá novamente para a guia “Pastas de Trabalho”, selecione “Minhas pastas de trabalho”, Logs de Entrada do Azure AD e clique em “Ver pasta de trabalho salva”.

16. Verifique os Resultados, caso ainda não tenha nada, aguarde mais um tempo e verifique novamente (como acabamos de criar o log analitics workspace pode levar um tempo até aparecer os primeiros dados, que leva de 1 a 12 horas, após estar tudo ok os resultados são bem rápidos de aparecer).

17. Crie um alerta com as seguintes premissas:

    - Escopo: Sua Assinatura
    - Condição: Create Resource Group
    - Ação: Enviar um SMS para o seu número de celular
    - Nome: New RG

18. Aguarde alguns minutos e, em seguida, crie um grupo de recursos chamado “alerttest”.

19. Apague a Regra de Alerta após receber um alerta via SMS.