Question: 288 CertyIQ

HOTSPOT
-
You have a Microsoft 365 tenant.
Sometimes, users use external, third-party applications that require limited access to the Microsoft 365 data of the respective user. The users register the applications in Azure AD.
You need to receive an alert if a registered application gains read and write access to the users' email.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

LIVEWORKSHEETS

Answer Area

Tool to use:

- Azure AD Identity Protection
- Identity Governance
- Microsoft Defender for Cloud Apps
- Microsoft Endpoint Manager

Policy type to create:

- App discovery
- App protection
- Conditional access
- OAuth app
- Sign-in risk
- User risk

LIVEWORKSHEETS

Question: 289

CertyIQ

Case Study -
Overview -
ADatum Corporation is a consulting company in Montreal.
ADatum recently acquired a Vancouver-based company named Litware, Inc.
Existing Environment. ADatum Environment
The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.
ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.
ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.
The tenant contains the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

The tenant contains the groups shown in the following table.

LIVEWORKSHEETS

The tenant contains the groups shown in the following table.

Name	Type	Membership type	Owner	Members
IT_Group1	Security	Assigned	*None*	All users in the IT department
AdatumUsers	Security	Assigned	*None*	User1, User2

Existing Environment. Litware Environment
Litware has an AD DS forest named litware.com
Existing Environment. Problem Statements
ADatum identifies the following issues:
•Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
•A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
•When you attempt to assign the Device Administrators role to IT_Group1, the group does NOT appear in the selection list.
•Anyone in the organization can invite guest users, including other guests and non-administrators.
•The helpdesk spends too much time resetting user passwords.
•Users currently use only passwords for authentication.

LIVEWORKSHEETS

Requirements. Planned Changes -
ADatum plans to implement the following changes:
•Configure self-service password reset (SSPR).
•Configure multi-factor authentication (MFA) for all users.
•Configure an access review for an access package named Package1.
•Require admin approval for application access to organizational data.
•Sync the AD DS users and groups of litware.com with the Azure AD tenant.
•Ensure that only users that are assigned specific admin roles can invite guest users.
•Increase the maximum number of devices that can be joined or registered to Azure AD to 10.
Requirements. Technical Requirements
ADatum identifies the following technical requirements:
•Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
•Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
•Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
- Email
- Phone
- Security questions
- The Microsoft Authenticator app
•Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
•The principle of least privilege must be used.
You need implement the planned changes for application access to organizational data.
What should you configure?

A.authentication methods

B.the User consent settings

C.access packages

D.an application proxy

LIVEWORKSHEETS

Question: 317

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
VM1	Virtual machine
App1	Azure App Service web app
Managed1	Managed identity
Managed2	Managed identity

You create a Microsoft Entra user named User1.

Which identities can you add to VM1 and App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

LIVEWORKSHEETS

VM1:

- User1 only
- Managed2 only
- Managed1 and Managed2 only
- Managed2 and User1 only
- Managed1, Managed2, and User1

App1:

- User1 only
- Managed2 only
- Managed2 and User1 only
- A system-assigned managed identity only
- A system-assigned managed identity and Managed2 only
- A system-assigned managed identity, Managed2, and User1

LIVEWORKSHEETS