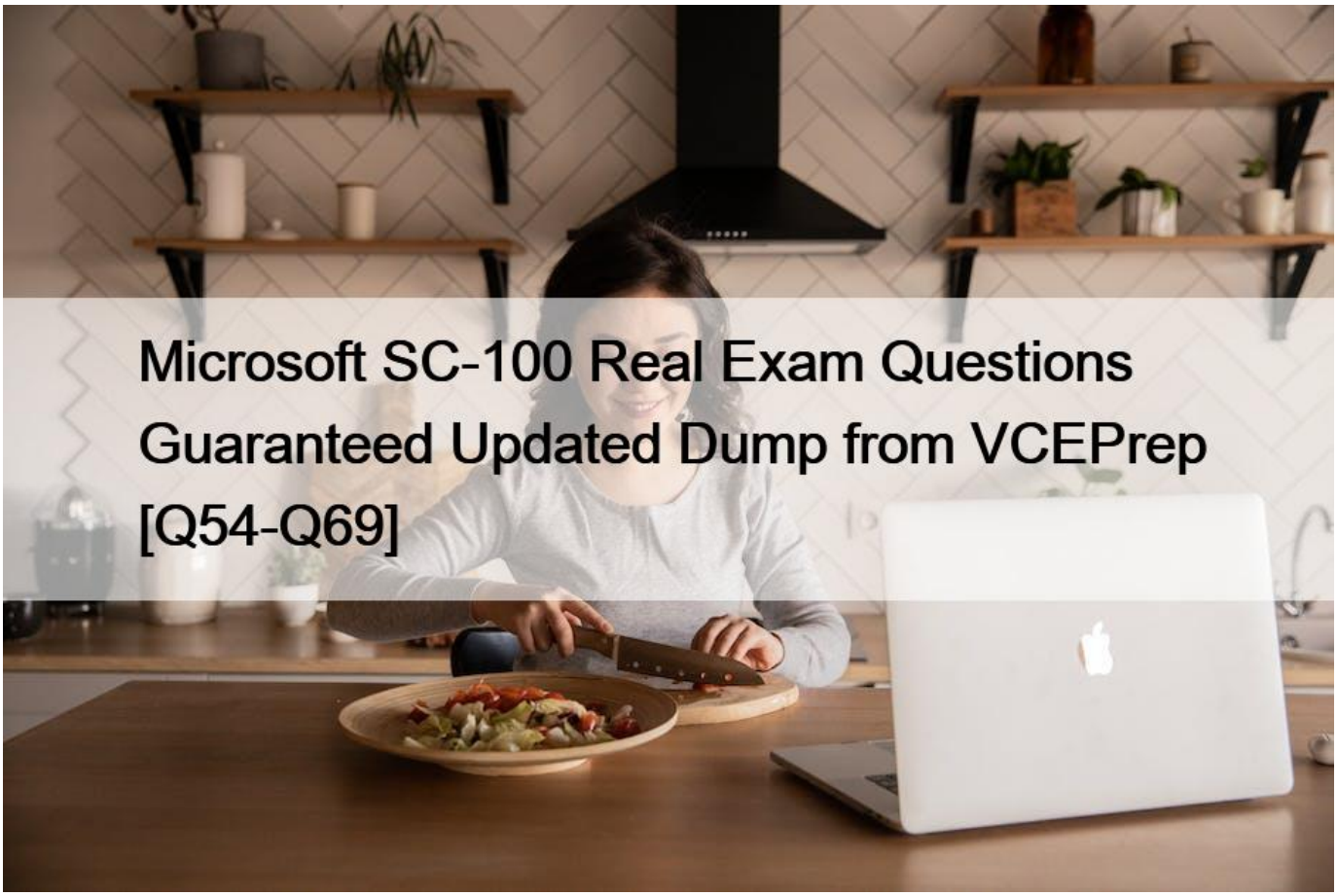
Microsoft SC-100 Real Exam Questions Guaranteed Updated Dump from VCEPrep [Q54-Q69



Microsoft SC-100 Real Exam Questions Guaranteed Updated Dump from VCEPrep
Verified Pass SC-100 Exam in First Attempt Guaranteed

Q54. Your company finalizes the adoption of Azure and is implementing Microsoft Defender for Cloud.

You receive the following recommendations in Defender for Cloud

* Access to storage accounts with firewall and virtual network configurations should be restricted,

* Storage accounts should restrict network access using virtual network rules.

* Storage account should use a private link connection.

* Storage account public access should be disallowed.

You need to recommend a service to mitigate identified risks that relate to the recommendations. What should you recommend?
* Azure Storage Analytics

* Azure Network Watcher
* Microsoft Sentinel
* Azure Policy

https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept
https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline

Q55. Your company has Microsoft 365 E5 licenses and Azure subscriptions.

The company plans to automatically label sensitive data stored in the following locations:

* Microsoft SharePoint Online

* Microsoft Exchange Online

* Microsoft Teams

You need to recommend a strategy to identify and protect sensitive data.

Which scope should you recommend for the sensitivity label policies? To answer, drag the appropriate scopes to the correct locations. Each scope may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Topic 1, Litware, inc.

Existing Environment

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD D%) forest named Utvvare.com and is linked to 20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Planned Changes

Litware plans to implement the following changes:

* Create a management group hierarchy for each Azure AD tenant.

* Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

* Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Business Requirements

Litware identifies the following business requirements:

* Minimize any additional on-premises infrastructure.

* Minimize the operational costs associated with administrative overhead.

Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

* Enable the management of on-premises resources from Azure, including the following:

* Use Azure Policy for enforcement and compliance evaluation.

* Provide change tracking and asset inventory.

* Implement patch management.

* Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAK) capabilities of Microsoft Sentinel. The company wants to centralize Security Operations Center (SOQ by using Microsoft Sentinel.

Identity Requirements

Litware identifies the following identity requirements:

* Detect brute force attacks that directly target AD DS user accounts.

* Implement leaked credential detection in the Azure AD tenant of Litware.

* Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.

* Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for.

* The management of group properties, membership, and licensing

* The management of user properties, passwords, and licensing

* The delegation of user management based on business units.

Regulatory Compliance Requirements

Litware identifies the following regulatory compliance requirements:

* insure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.

* Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.

* Use the principle of least privilege.

Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:

* Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.

* Provide a secure score scoped to the landing zone.

* Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.

* Minimize the possibility of data exfiltration.

* Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:

* Be created in a dedicated subscription.

* Use a DNS namespace of litware.com.

Application Security Requirements

Litware identifies the following application security requirements:

* Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.

* Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

Q56. Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C.

The application will be deployed as an App Service web app. You need to recommend a solution to the application development team to secure the application from identity related attacks. Which two configurations should you recommend? Each correct answer

presents part of the solution. NOTE: Each correct selection is worth one point.

* Azure AD Conditional Access integration with user flows and custom policies
* Azure AD workbooks to monitor risk detections
* custom resource owner password credentials (ROPC) flows in Azure AD B2C
* access packages in Identity Governance
* smart account lockout in Azure AD B2C

Q57. You need to recommend a solution to meet the compliance requirements.

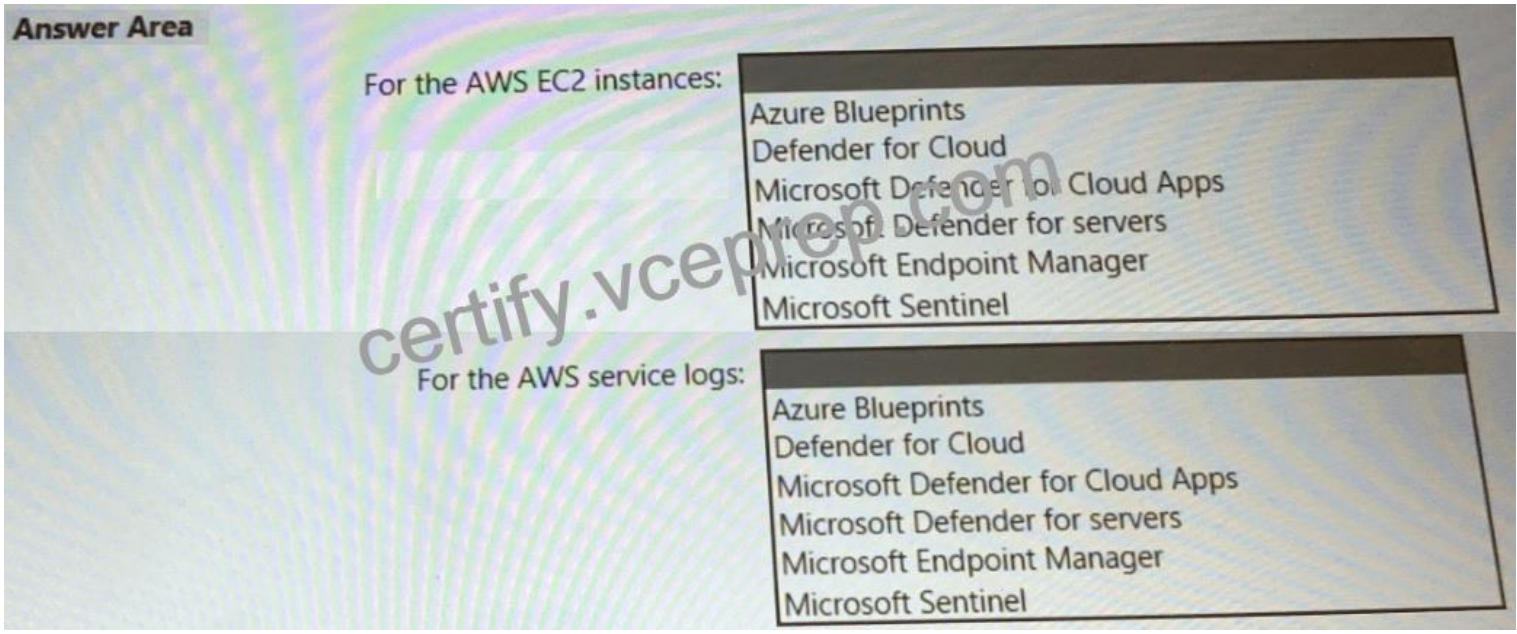
What should you recommend? To answer, select the appropriate options in the answer area.

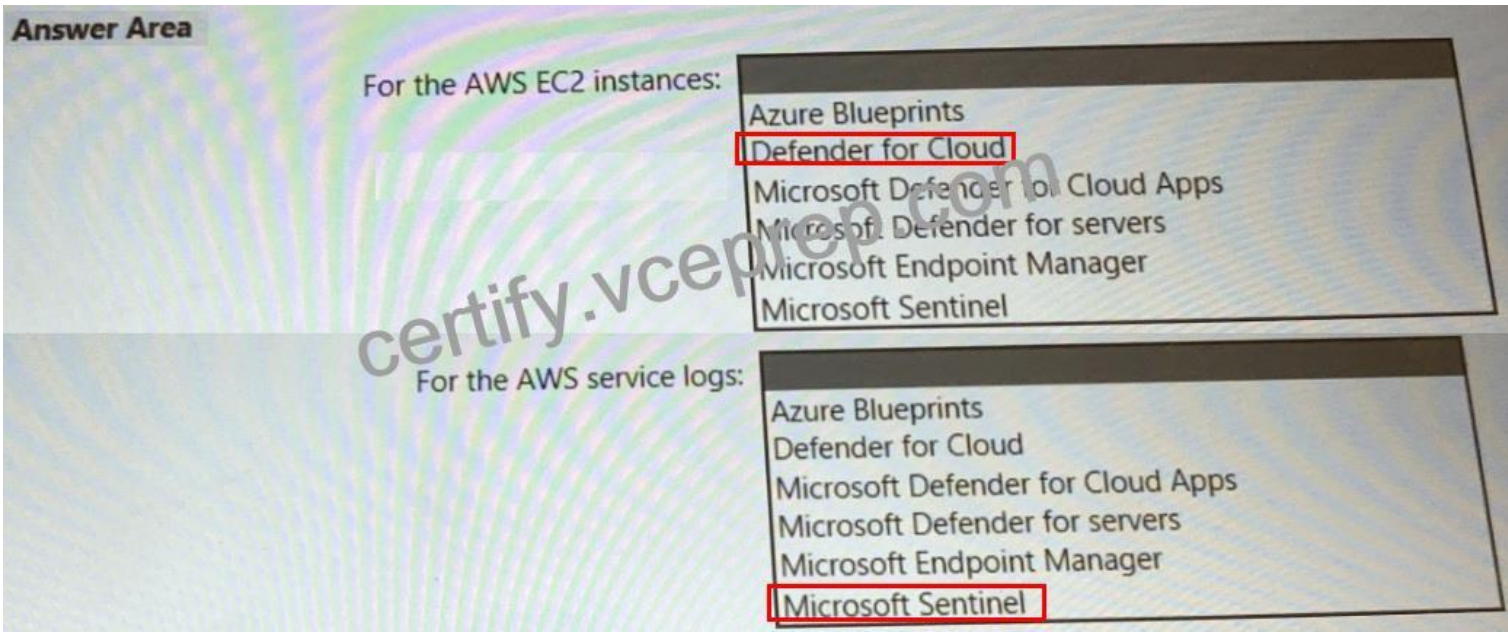
NOTE: Each correct selection is worth one point.

Q58. You need to recommend a solution to meet the AWS requirements.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.





Q59. You need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table. The solution must meet the Contoso developer requirements.

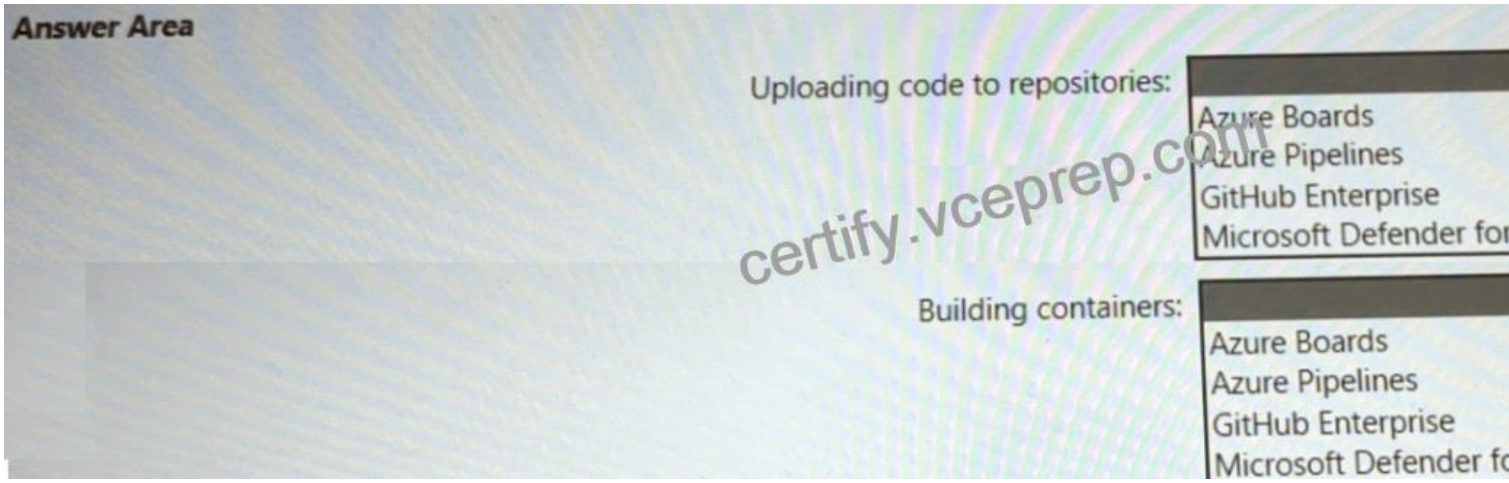
What should you include in the recommendation?
* Transparent Data Encryption (TDE)
* Always Encrypted
* row-level security (RLS)
* dynamic data masking
* data classification

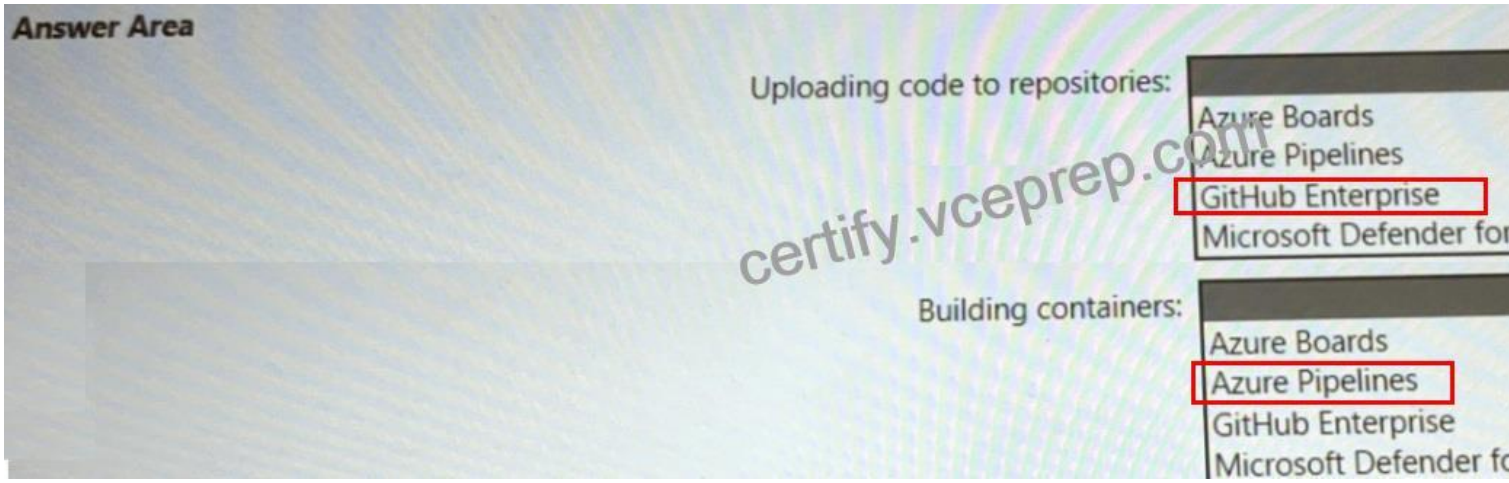
Q60. Your company has an Azure App Service plan that is used to deploy containerized web apps. You are designing a secure DevOps strategy for deploying the web apps to the App Service plan. You need to recommend a strategy to integrate code scanning

tools into a secure software development lifecycle. The code must be scanned during the following two phases:

Uploading the code to repositories Building containers

Where should you integrate code scanning for each phase? To answer, select the appropriate options in the answer area.





Q61. Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.

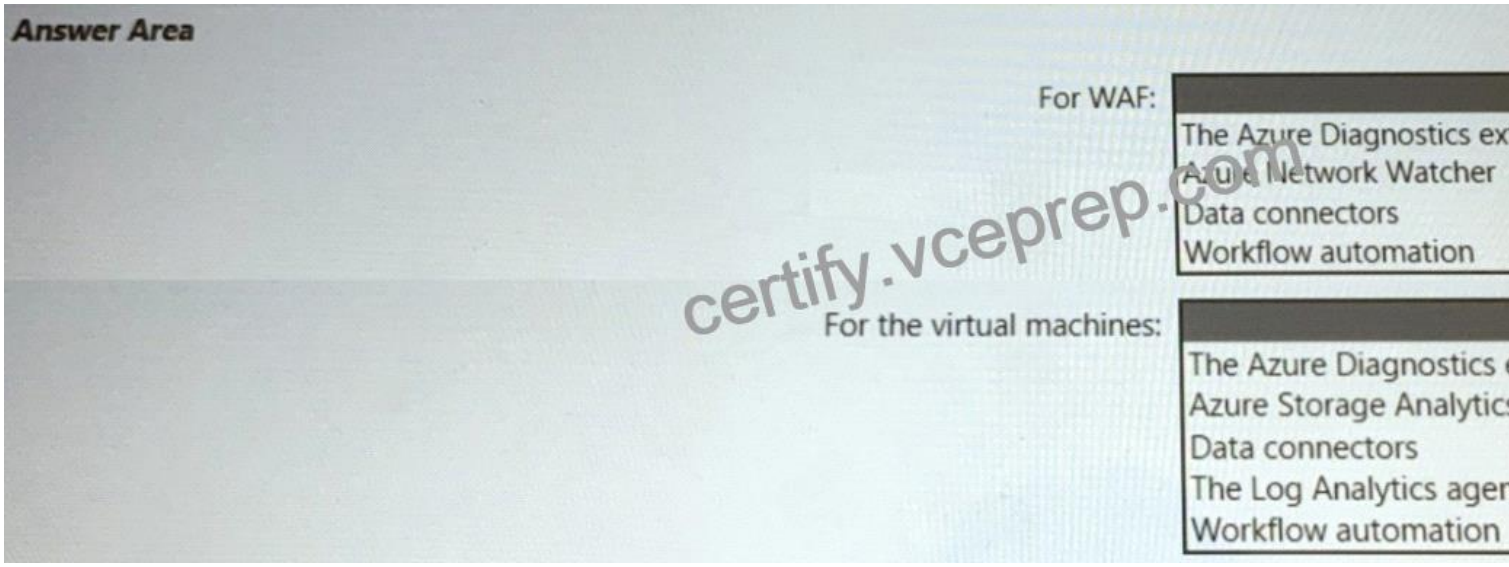
You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-.

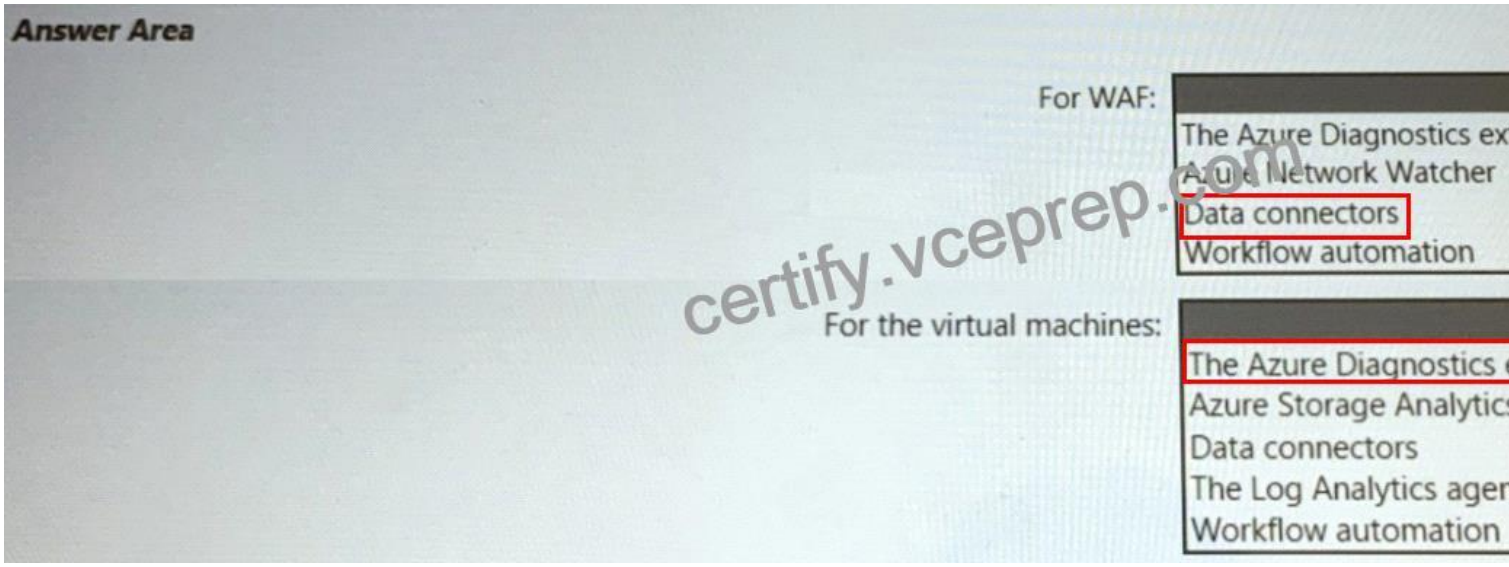
* Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.

* Use Defender for Cloud to review alerts from the virtual machines.

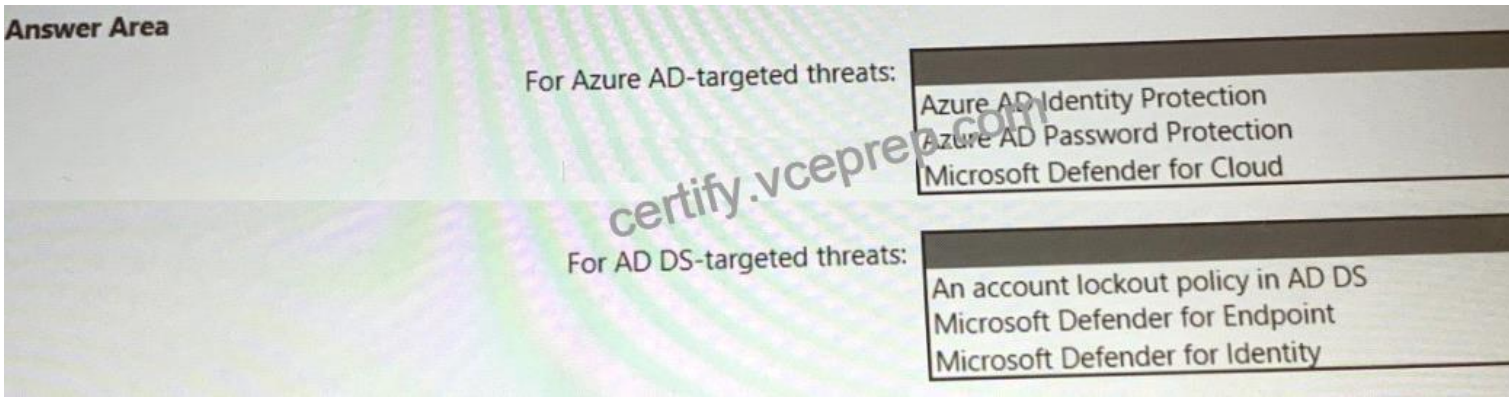
What should you include in the solution? To answer, select the appropriate options in the answer are

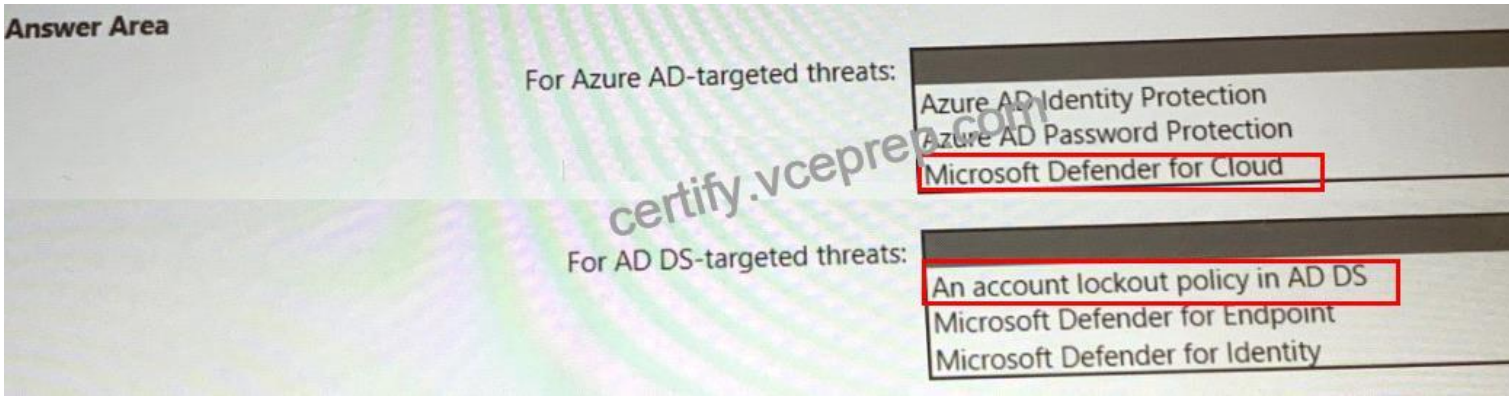
a. NOTE: Each correct selection is worth one point.





Q62. You need to recommend a strategy for securing the litware.com forest. The solution must meet the identity requirements. What should you include in the recommendation? To answer, select the appropriate options in the answer are a. NOTE; Each correct selection is worth one point.





Q63. Your company has an on-premises network, an Azure subscription, and a Microsoft 365 E5 subscription. The company uses the following devices:

* Computers that run either Windows 10 or Windows 11

* Tablets and phones that run either Android or iOS

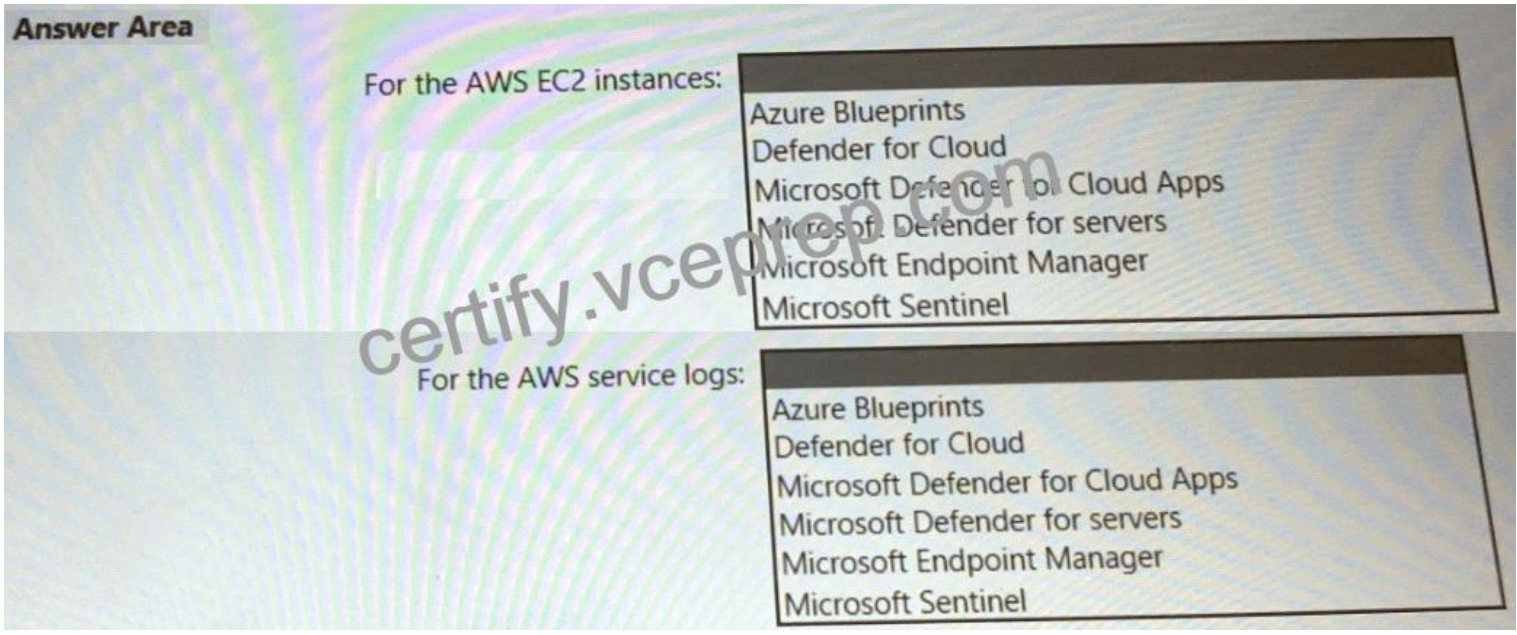
You need to recommend a solution to classify and encrypt sensitive Microsoft Office 365 data regardless of where the data is stored.
What should you include in the recommendation?
* eDiscovery
* retention policies
* Compliance Manager
* Microsoft Information Protection
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection

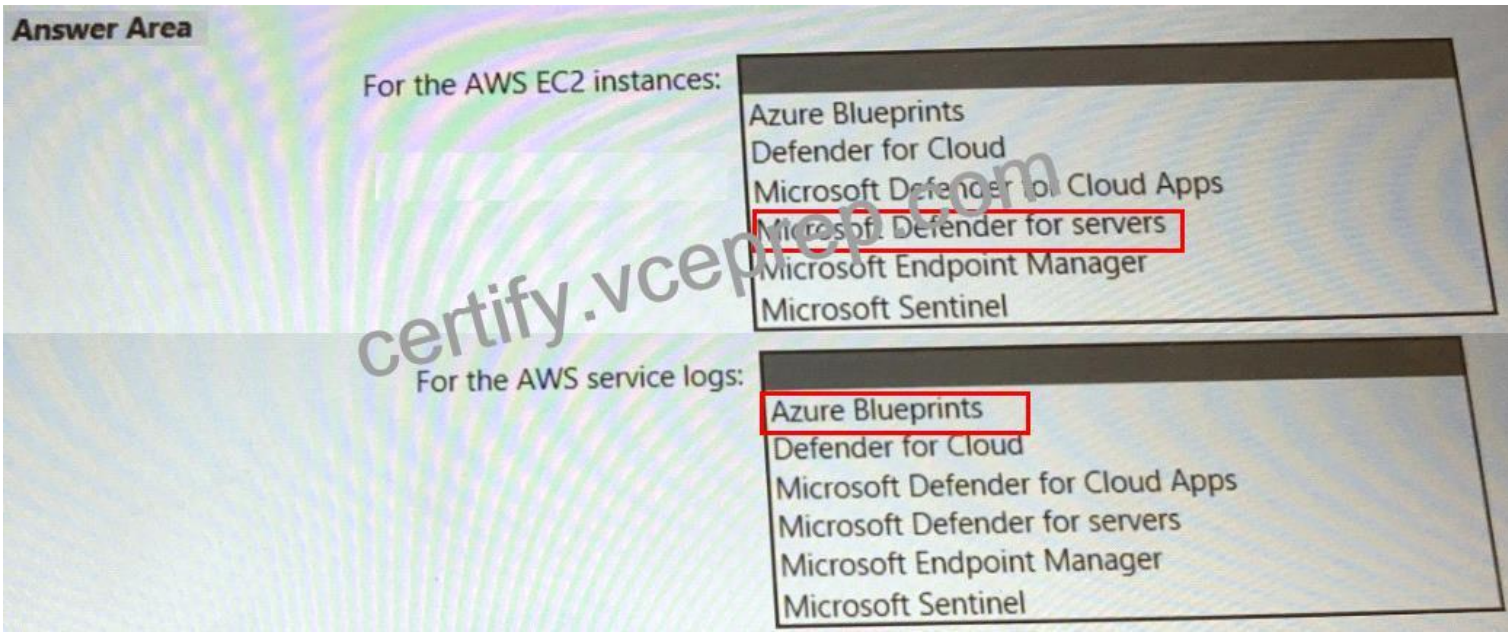
https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

Q64. You need to recommend a solution to meet the AWS requirements.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.





Topic 1, Fabrikam, Inc

On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Azure Environment

Fabrikam has the following Azure resources:

* An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabnkam.com

* A single Azure subscription named Sub1

* A virtual network named Vnetl in the East US Azure region

* A virtual network named Vnet2 in the West Europe Azure region

* An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAR enabled

* A Microsoft Sentinel workspace

* An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

* 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud

* A resource group named TestRG that is used for testing purposes only

* An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Partners

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure-.

* An Azure AD tenant named contoso.onmicrosoft.com

* An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security Group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

Compliance Event

Fabrikam deploys the following compliance environment:

* Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.

* Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.

* Qualys is used as the standard vulnerability assessment tool for servers.

Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation-. Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

ClaimApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specification

* ClaimsApp will be deployed to Azure App Service instances that connect to Vnetl and Vnet2.

* Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

* ClaimsApp will access data in ClaimsDB.

* ClaimsDB must be accessible only from Azure virtual networks.

* The app services permission for ClaimsApp must be assigned to ClaimsDB.

Application Development Requirements

Fabrikam identifies the following requirements for application development:

* Azure DevTest labs will be used by developers for testing.

* All the application code must be stored in GitHub Enterprise.

* Azure Pipelines will be used to manage application deployments.

* All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text. Scanning must be done at the time the code is pushed to a repository.

Security Requirement

Fabrikam identifies the following security requirements:

* Internet-accessible applications must prevent connections that originate in North Korea.

* Only members of a group named InfraSec must be allowed to configure network security groups (NSGs} and instances of Azure Firewall, VJM. And Front Door in Sub1.

* Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

AWS Requirements

Fabrikam identifies the following security requirements for the data hosted in ContosoAWSV.

* Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

* Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Contoso Developer Requirements

Fabrikam identifies the following requirements for the Contoso developers;

* Every month, the membership of the ContosoDevelopers group must be verified.

* The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

* The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Compliance Requirement

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPPA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Q65. You have a customer that has a Microsoft 365 subscription and uses the Free edition of Azure Active Directory (Azure AD) The customer plans to obtain an Azure subscription and provision several Azure resources.

You need to evaluate the customer’s security environment.

What will necessitate an upgrade from the Azure AD Free edition to the Premium edition?
* role-based authorization
* Azure AD Privileged Identity Management (PIM)
* resource-based authorization
* Azure AD Multi-Factor Authentication

Q66. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls.

Solution: You recommend enabling the VMAccess extension on all virtual machines.

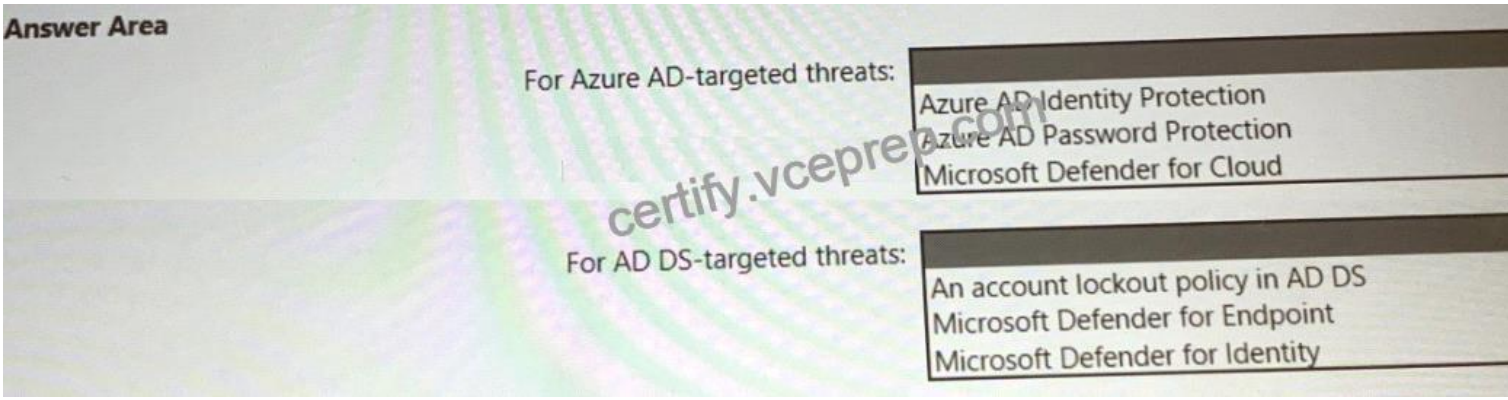
Does this meet the goal?
* Yes
* No

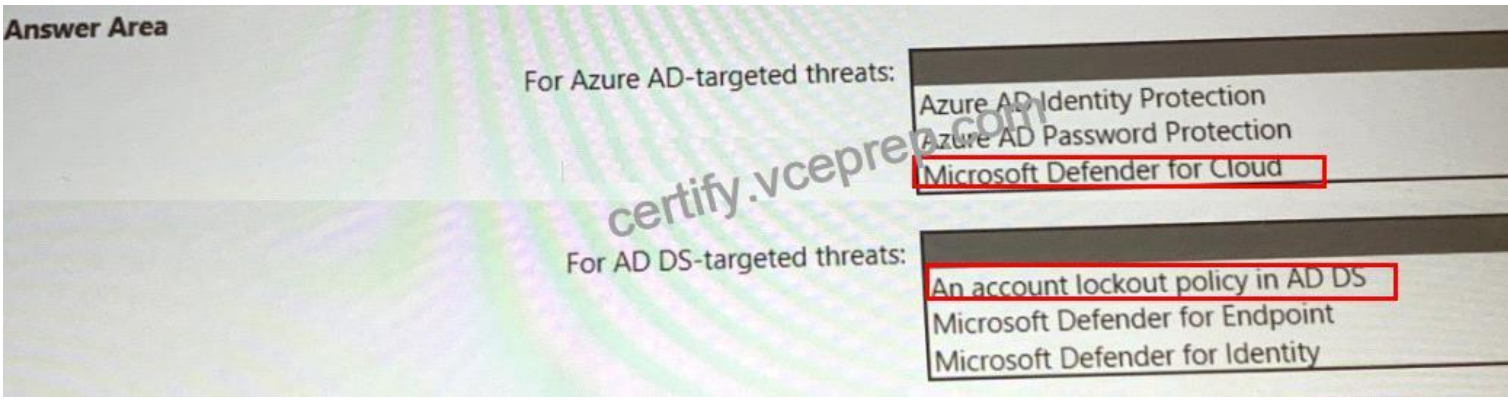
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-standing-access-for-user-accounts-and-permissions Adaptive Network Hardening: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify-network-security-configuration

Q67. You need to recommend a strategy for securing the litware.com forest. The solution must meet the identity requirements. What

should you include in the recommendation? To answer, select the appropriate options in the answer are

a. NOTE; Each correct selection is worth one point.





Topic 2, Fabrikam, Inc

On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Azure Environment

Fabrikam has the following Azure resources:

* An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabnkam.com

* A single Azure subscription named Sub1

* A virtual network named Vnetl in the East US Azure region

* A virtual network named Vnet2 in the West Europe Azure region

* An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAR enabled

* A Microsoft Sentinel workspace

* An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

* 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud

* A resource group named TestRG that is used for testing purposes only

* An Azure Virtual Desktop host pool that contains personal assigned session hosts

All the resources in Sub1 are in either the East US or the West Europe region.

Partners

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure-.

* An Azure AD tenant named contoso.onmicrosoft.com

* An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam

Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security Group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

Compliance Event

Fabrikam deploys the following compliance environment:

* Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.

* Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.

* Qualys is used as the standard vulnerability assessment tool for servers.

Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation-. Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

ClaimApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specification

* ClaimsApp will be deployed to Azure App Service instances that connect to Vnetl and Vnet2.

* Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

* ClaimsApp will access data in ClaimsDB.

* ClaimsDB must be accessible only from Azure virtual networks.

* The app services permission for ClaimsApp must be assigned to ClaimsDB.

Application Development Requirements

Fabrikam identifies the following requirements for application development:

* Azure DevTest labs will be used by developers for testing.

* All the application code must be stored in GitHub Enterprise.

* Azure Pipelines will be used to manage application deployments.

* All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text. Scanning must be done at the time the code is pushed to a repository.

Security Requirement

Fabrikam identifies the following security requirements:

* Internet-accessible applications must prevent connections that originate in North Korea.

* Only members of a group named InfraSec must be allowed to configure network security groups (NSGs} and instances of Azure Firewall, VJM. And Front Door in Sub1.

* Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

AWS Requirements

Fabrikam identifies the following security requirements for the data hosted in ContosoAWSV.

* Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

* Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Contoso Developer Requirements

Fabrikam identifies the following requirements for the Contoso developers;

* Every month, the membership of the ContosoDevelopers group must be verified.

* The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

* The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Compliance Requirement

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPPA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Q68. You have a Microsoft 365 E5 subscription.

You need to recommend a solution to add a watermark to email attachments that contain sensitive dat a. What should you include in the recommendation?

* Microsoft Defender for Cloud Apps
* insider risk management
* Microsoft Information Protection
* Azure Purview

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide You can use sensitivity labels to: Provide protection settings that include encryption and content markings. For example, apply a “Confidential” label to a document or email, and that label encrypts the content and applies a “Confidential” watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content. Protect content in Office apps across different platforms and devices. Supported by Word, Excel, PowerPoint, and Outlook on the Office desktop apps and Office on the web. Supported on Windows, macOS, iOS, and Android. Protect content in third-party apps and services by using Microsoft Defender for Cloud Apps. With Defender for Cloud Apps, you can detect, classify, label, and protect content in third-party apps and services, such as SalesForce, Box, or DropBox, even if the third-party app or service does not read or support sensitivity labels.

Q69. You need to recommend a solution to meet the compliance requirements.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Download Real Microsoft SC-100 Exam Dumps Test Engine Exam Questions:
https://www.vceprep.com/SC-100-latest-vce-prep.html]