SC-100$^{\text{Q\&As}}$

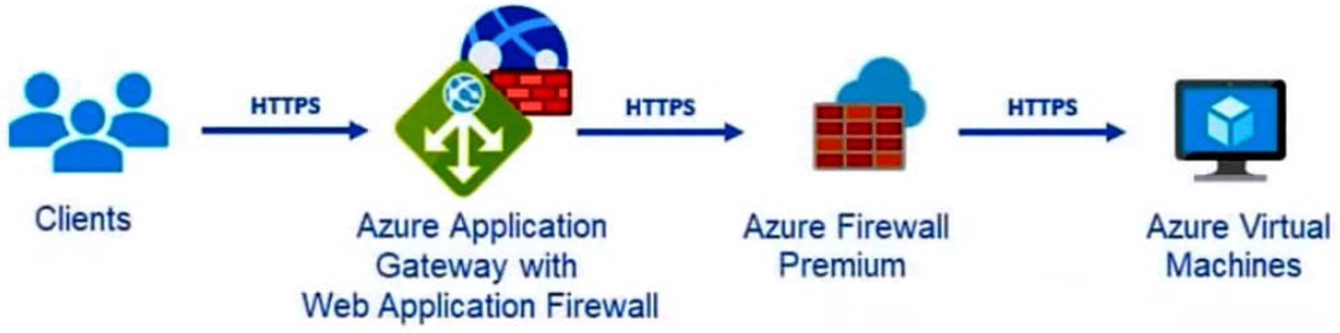
Microsoft Cybersecurity Architect

QUESTION 1

HOTSPOT

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:

1.

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

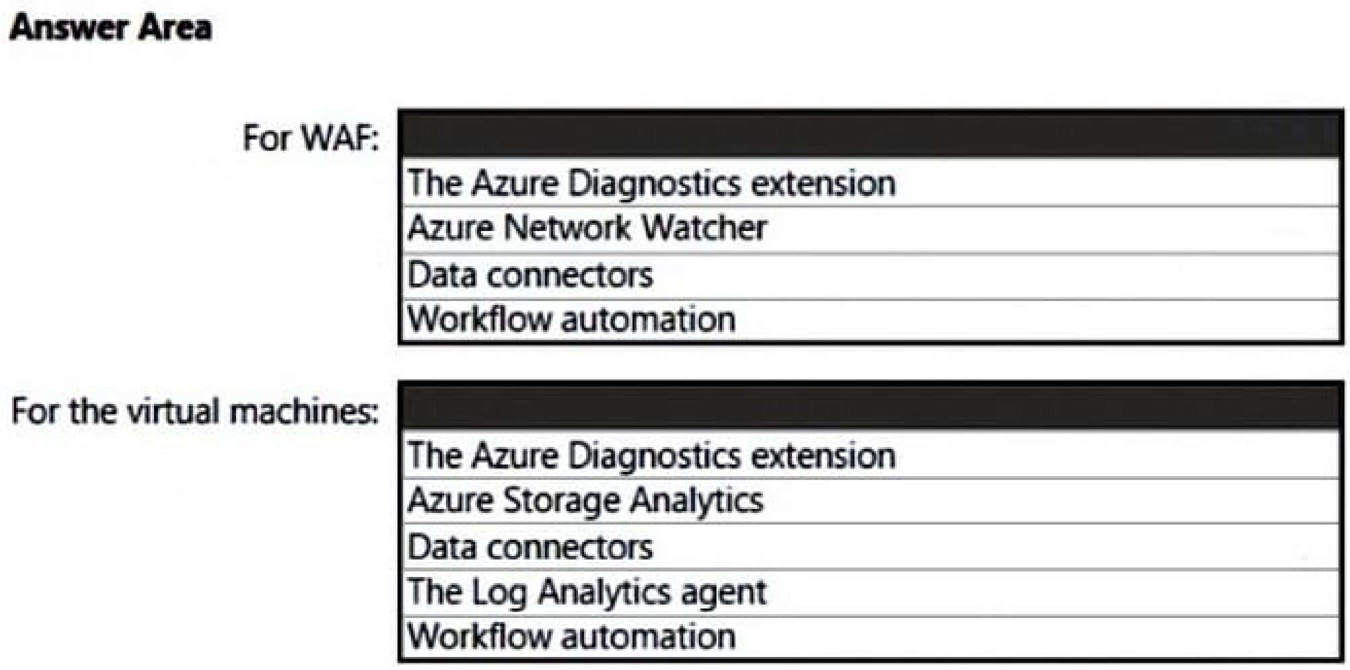
2.

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 area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

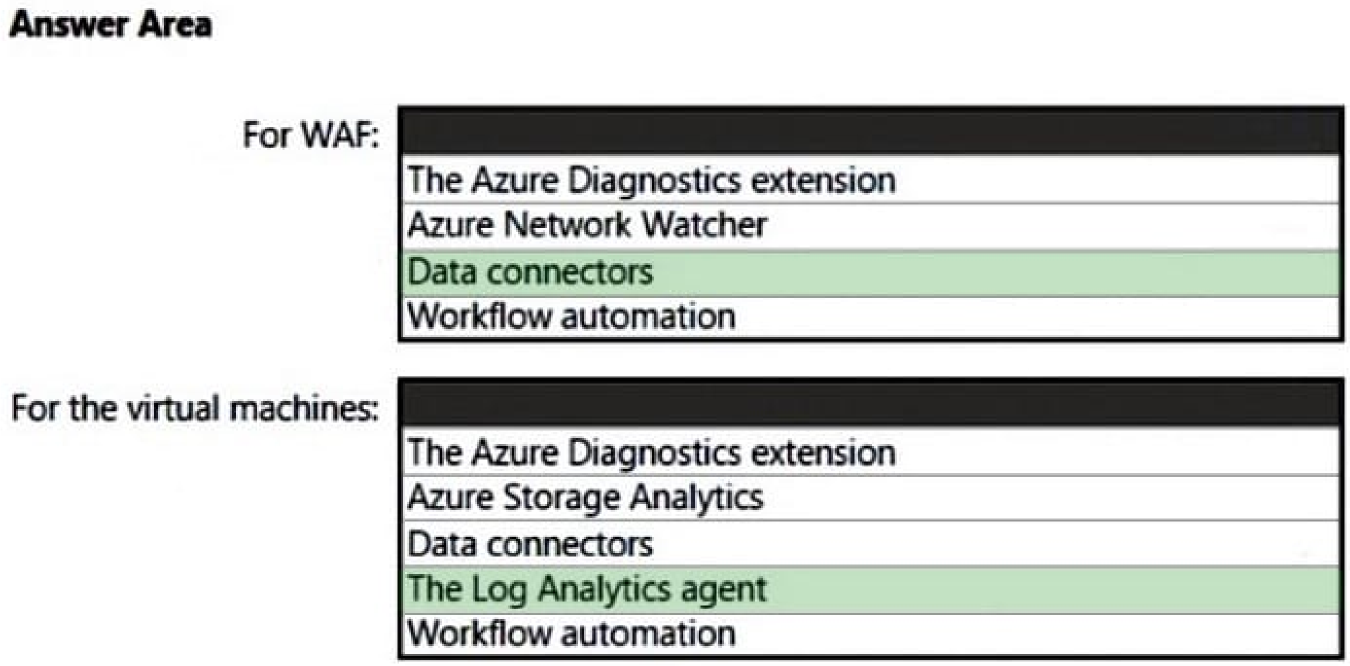
For WAF:

- The Azure Diagnostics extension
- Azure Network Watcher
- Data connectors
- Workflow automation

For the virtual machines:

- The Azure Diagnostics extension
- Azure Storage Analytics
- Data connectors
- The Log Analytics agent
- Workflow automation

Correct Answer:



Answer Area

For WAF:

- The Azure Diagnostics extension
- Azure Network Watcher
- [✓ Data connectors]
- Workflow automation

For the virtual machines:

- The Azure Diagnostics extension
- Azure Storage Analytics
- Data connectors
- [✓ The Log Analytics agent]
- Workflow automation

Box 1: Data connectors

Microsoft Sentinel connector streams security alerts from Microsoft Defender for Cloud into Microsoft Sentinel.

Launch a WAF workbook (see step 7 below)

The WAF workbook works for all Azure Front Door, Application Gateway, and CDN WAFs. Before connecting the data from these resources, log analytics must be enabled on your resource.

To enable log analytics for each resource, go to your individual Azure Front Door, Application Gateway, or CDN resource:

1.

Select Diagnostic settings.

2.

Select + Add diagnostic setting.

3.

In the Diagnostic setting page (details skipped)

4.

On the Azure home page, type Microsoft Sentinel in the search bar and select the Microsoft Sentinel resource.

5.

Select an already active workspace or create a new workspace.

6.

On the left side panel under Configuration select Data Connectors.

7.

Search for Azure web application firewall and select Azure web application firewall (WAF). Select Open connector page on the bottom right.

8.

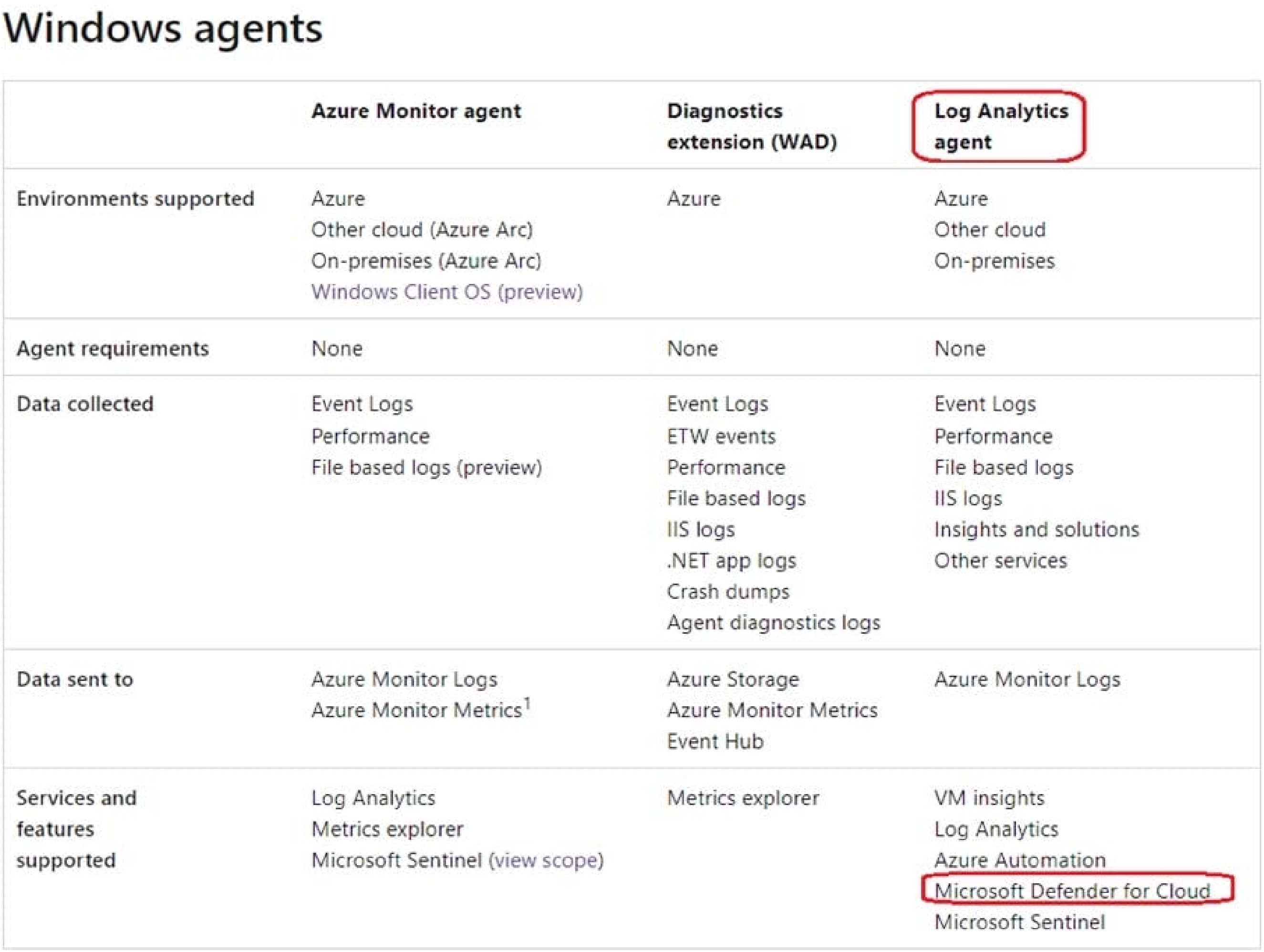
Follow the instructions under Configuration for each WAF resource that you want to have log analytic data for if you haven\\'t done so previously.

9.

Once finished configuring individual WAF resources, select the Next steps tab. Select one of the recommended workbooks. This workbook will use all log analytic data that was enabled previously. A working WAF workbook should now exist for your WAF resources.

Box 2: The Log Analytics agent

Use the Log Analytics agent to integrate with Microsoft Defender for cloud.



Windows agents

	Azure Monitor agent	Diagnostics extension (WAD)	Log Analytics agent
Environments supported	Azure Other cloud (Azure Arc) On-premises (Azure Arc) Windows Client OS (preview)	Azure	Azure Other cloud On-premises
Agent requirements	None	None	None
Data collected	Event Logs Performance File based logs (preview)	Event Logs ETW events Performance File based logs IIS logs .NET app logs Crash dumps Agent diagnostics logs	Event Logs Performance File based logs IIS logs Insights and solutions Other services
Data sent to	Azure Monitor Logs Azure Monitor Metrics[1]	Azure Storage Azure Monitor Metrics Event Hub	Azure Monitor Logs
Services and features supported	Log Analytics Metrics explorer Microsoft Sentinel (view scope)	Metrics explorer	VM insights Log Analytics Azure Automation Microsoft Defender for Cloud Microsoft Sentinel

The Log Analytics agent is required for solutions, VM insights, and other services such as Microsoft Defender for Cloud.

Note: The Log Analytics agent in Azure Monitor can also be used to collect monitoring data from the guest operating system of virtual machines. You may choose to use either or both depending on your requirements.

Azure Log Analytics agent

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

The Azure Log Analytics agent collects telemetry from Windows and Linux virtual machines in any cloud, on-premises machines, and those monitored by System Center Operations Manager and sends collected data to your Log Analytics

workspace in Azure Monitor.

Incorrect:

The Azure Diagnostics extension does not integrate with Microsoft Defender for Cloud.

Reference: https://docs.microsoft.com/en-us/azure/web-application-firewall/waf-sentinel

https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview

QUESTION 2

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using continuous integration and continuous deployment (CI/CD) pipelines.

You need to recommend which types of identities to use for the deployment credentials of the service connection. The solution must follow DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure.

What should you recommend?

A. a managed identity in Azure

B. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management (PIM)

C. a group managed service account (gMSA)

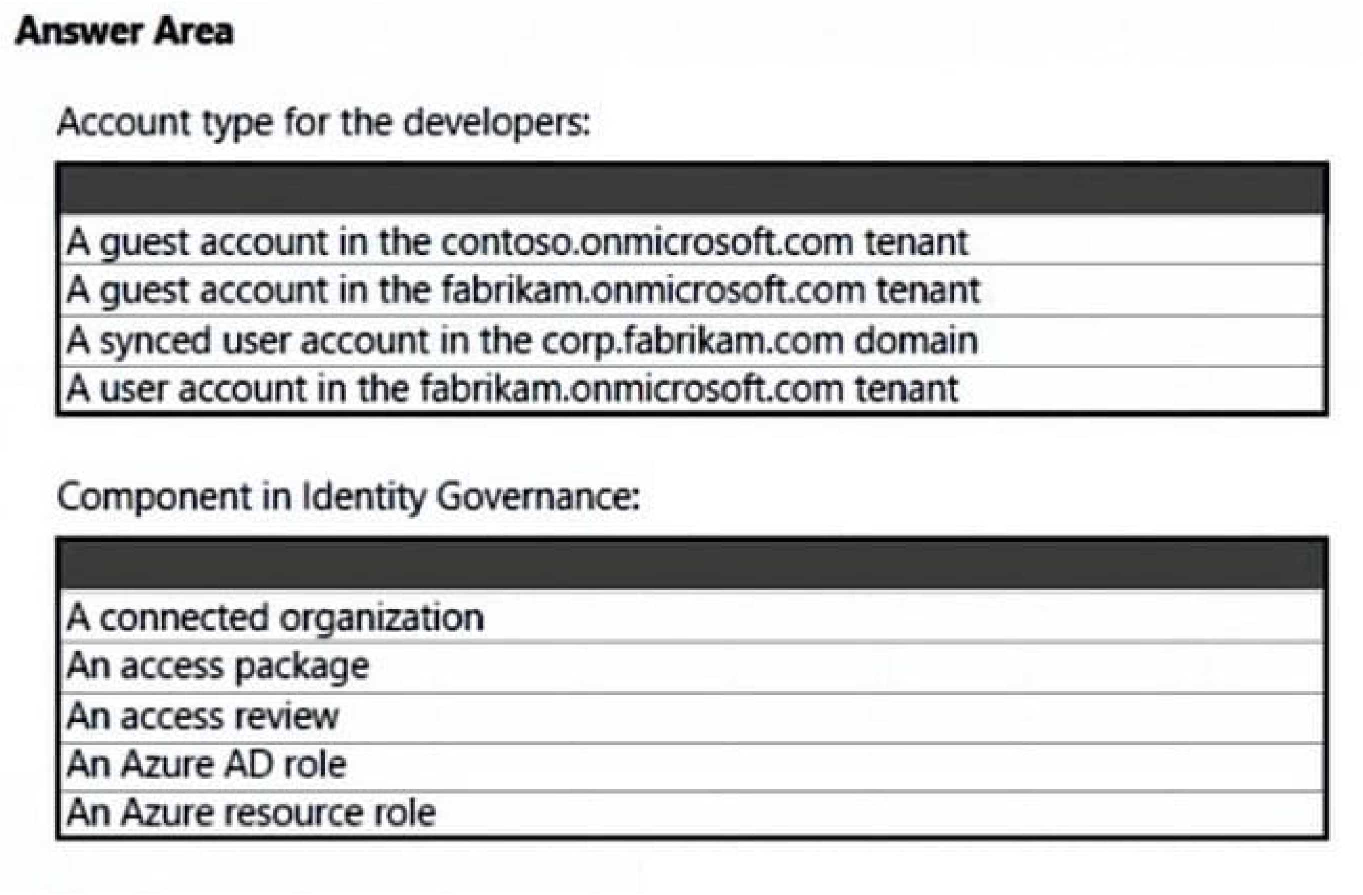
D. an Azure AD user account that has a password stored in Azure Key Vault

Correct Answer: D

QUESTION 3

What should you create in Azure AD to meet the Contoso developer requirements?

Hot Area:



Answer Area

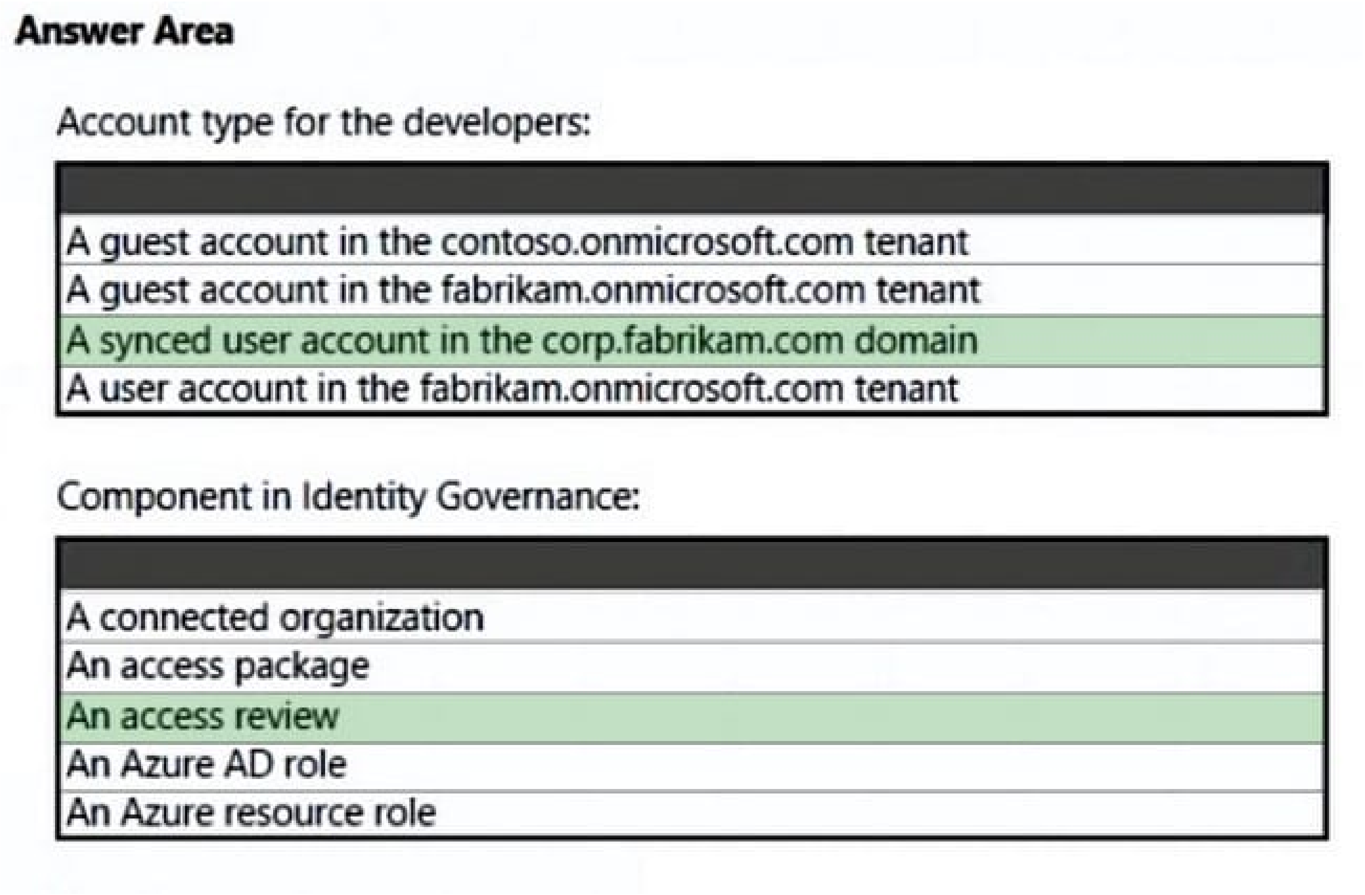
Account type for the developers:

A guest account in the contoso.onmicrosoft.com tenant
A guest account in the fabrikam.onmicrosoft.com tenant
A synced user account in the corp.fabrikam.com domain
A user account in the fabrikam.onmicrosoft.com tenant

Component in Identity Governance:

A connected organization
An access package
An access review
An Azure AD role
An Azure resource role

Correct Answer:



Answer Area

Account type for the developers:

A guest account in the contoso.onmicrosoft.com tenant
A guest account in the fabrikam.onmicrosoft.com tenant
A synced user account in the corp.fabrikam.com domain
A user account in the fabrikam.onmicrosoft.com tenant

Component in Identity Governance:

A connected organization
An access package
An access review
An Azure AD role
An Azure resource role

Box 1: A synced user account

Need to use a synched user account.

Incorrect:

*

Not A user account in the fabrikam.onmicrosoft.com tenant

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

*

Guest accounts would not meet the requirements.

Note: 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 ContosoDevelopers 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.

Contoso Developers 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 Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Box 2: An access review

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

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User\\'s access can be reviewed on a regular basis to make sure only

the right people have continued access.

Access review is part of Azure AD Identity governance.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/synchronization

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

QUESTION 4

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator

authorizes the application.

Which security control should you recommend?

A. app registrations in Azure AD

B. application control policies in Microsoft Defender for Endpoint

C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

D. Azure AD Conditional Access App Control policies

Correct Answer: B

Explanation:

Windows Defender Application Control is designed to protect devices against malware and other untrusted software. It prevents malicious code from running by ensuring that only approved code, that you know, can be run.

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC.

Incorrect:

Not C: A Cloud Discovery anomaly detection policy enables you to set up and configure continuous monitoring of unusual increases in cloud application usage. Increases in downloaded data, uploaded data, transactions, and users are

considered for each cloud application. Each increase is compared to the normal usage pattern of the application as learned from past usage. The most extreme increases trigger security alerts.

Reference:

https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager

QUESTION 5

You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server and 50 virtual machines that run Linux.

You need to perform vulnerability assessments on the virtual machines. The solution must meet the following requirements:

Identify missing updates and insecure configurations. Use the Qualys engine.

What should you use?

A. Microsoft Defender for Servers

B. Microsoft Defender Threat Intelligence (Defender TI)

C. Microsoft Defender for Endpoint

D. Microsoft Defender External Attack Surface Management (Defender EASM)

Correct Answer: A

Explanation:

The vulnerability scanner included with Microsoft Defender for Cloud is powered by Qualys. Qualys\\' scanner is one of the leading tools for real-time identification of vulnerabilities. It\\'s only available with Microsoft Defender for Servers.

Note: Enable vulnerability scanning with the integrated Qualys scanner

A core component of every cyber risk and security program is the identification and analysis of vulnerabilities. Defender for Cloud regularly checks your connected machines to ensure they\\'re running vulnerability assessment tools.

When a machine is found that doesn\\'t have a vulnerability assessment solution deployed, Defender for Cloud generates the security recommendation: Machines should have a vulnerability assessment solution. Use this recommendation to

deploy the vulnerability assessment solution to your Azure virtual machines and your Azure Arc-enabled hybrid machines.

Defender for Cloud includes vulnerability scanning for your machines. You don\\'t need a Qualys license or even a Qualys account - everything\\'s handled seamlessly inside Defender for Cloud.

Reference:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm

QUESTION 6

You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.

You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort. What should you include in the recommendation?

A. Azure Monitor webhooks

B. Azure Logics Apps

C. Azure Event Hubs

D. Azure Functions apps

Correct Answer: B

The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance.Note: Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems. With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.

QUESTION 7

For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cloud Security Benchmark.

What are three best practices for identity management based on the Azure Security Benchmark? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Manage application identities securely and automatically.

B. Manage the lifecycle of identities and entitlements

C. Protect identity and authentication systems.

D. Enable threat detection for identity and access management.

E. Use a centralized identity and authentication system.

Correct Answer: ACE

QUESTION 8

Your company develops several applications that are accessed as custom enterprise applications in Azure AD.

You need to recommend a solution to prevent users on a specific list of countries from connecting to the applications.

What should you include in the recommendation?

A. activity policies in Microsoft Defender for Cloud Apps

B. sign-in risk policies in Azure AD Identity Protection

C. Azure AD Conditional Access policies

D. device compliance policies in Microsoft Endpoint Manager

E. user risk policies in Azure AD Identity Protection

Correct Answer: A

Microsoft Defender for Cloud Apps Activity policies.

Activity policies allow you to enforce a wide range of automated processes using the app provider\\'s APIs. These policies enable you to monitor specific activities carried out by various users, or follow unexpectedly high rates of one certain

type of activity.

After you set an activity detection policy, it starts to generate alerts - alerts are only generated on activities that occur after you create the policy.

Each policy is composed of the following parts:

Activity filters – Enable you to create granular conditions based on metadata.

Activity match parameters – Enable you to set a threshold for the number of times an activity repeats to be considered to match the policy.

Actions – The policy provides a set of governance actions that can be automatically applied when violations are detected.

Incorrect:

Not C: Azure AD Conditional Access policies applies to users, not to applications.

Note: Blocking user logins by location can be an added layer of security to your environment. The following process will use Azure Active Directory conditional access to block access based on geographical location. For example, you are

positive that nobody in your organization should be trying to login to select cloud applications from specific countries.

Reference: https://docs.microsoft.com/en-us/defender-cloud-apps/user-activity-policies
https://cloudcompanyapps.com/2019/04/18/block-users-by-location-in-azure-o365/

QUESTION 9

HOTSPOT

Your company has a Microsoft 365 E5 subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DS).

You need to recommend an identity security strategy that meets the following requirements:

1.

Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website

2.

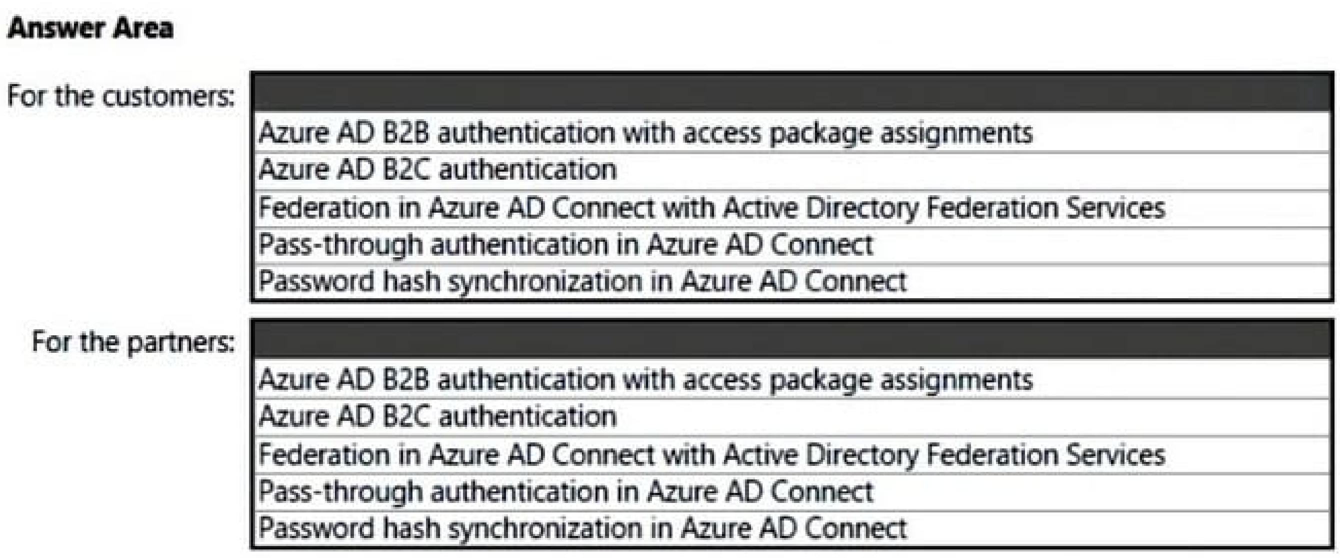
Ensures that partner companies can access Microsoft SharePoint Online sites for the project to which they are assigned

The solution must minimize the need to deploy additional infrastructure components.

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.

Hot Area:



Answer Area

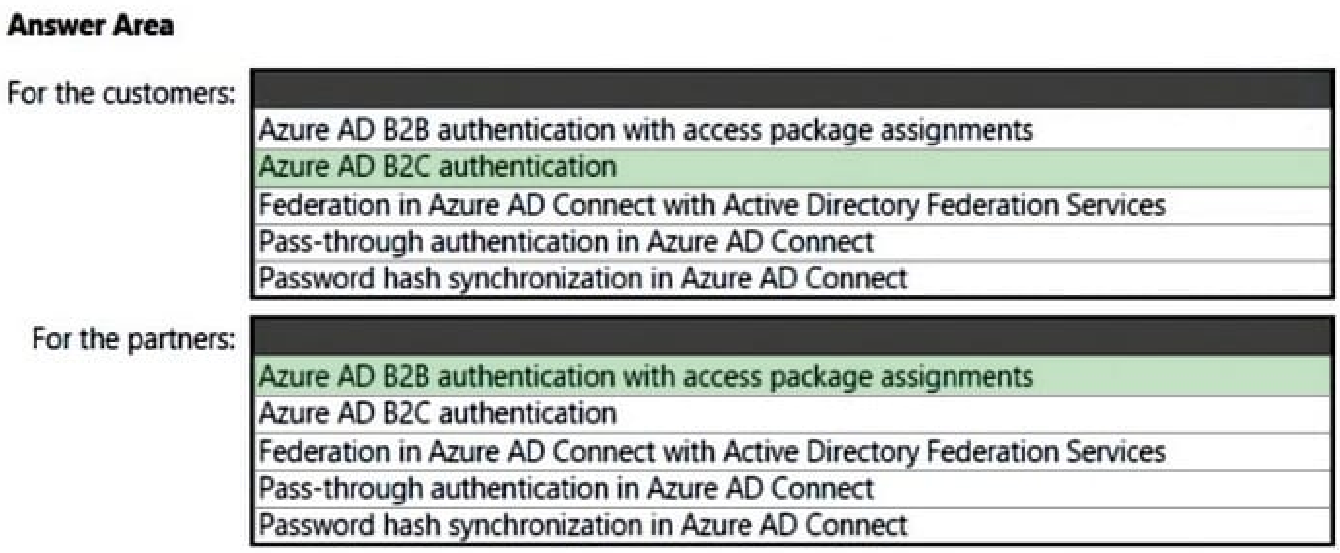
For the customers:

- Azure AD B2B authentication with access package assignments
- Azure AD B2C authentication
- Federation in Azure AD Connect with Active Directory Federation Services
- Pass-through authentication in Azure AD Connect
- Password hash synchronization in Azure AD Connect

For the partners:

- Azure AD B2B authentication with access package assignments
- Azure AD B2C authentication
- Federation in Azure AD Connect with Active Directory Federation Services
- Pass-through authentication in Azure AD Connect
- Password hash synchronization in Azure AD Connect

Correct Answer:



Answer Area

For the customers:

- Azure AD B2B authentication with access package assignments
- [✓ Azure AD B2C authentication]
- Federation in Azure AD Connect with Active Directory Federation Services
- Pass-through authentication in Azure AD Connect
- Password hash synchronization in Azure AD Connect

For the partners:

- [✓ Azure AD B2B authentication with access package assignments]
- Azure AD B2C authentication
- Federation in Azure AD Connect with Active Directory Federation Services
- Pass-through authentication in Azure AD Connect
- Password hash synchronization in Azure AD Connect

Box 1: Azure AD B2C authentication

Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website.

You can set up sign-up and sign-in with a Facebook account using Azure Active Directory B2C.

Box 2: Azure AD B2B authentication with access package assignments

Govern access for external users in Azure AD entitlement management

Azure AD entitlement management uses Azure AD business-to-business (B2B) to share access so you can collaborate with people outside your organization. With Azure AD B2B, external users authenticate to their home directory, but have a

representation in your directory. The representation in your directory enables the user to be assigned access to your resources.

Incorrect:

Not: Password hash synchronization in Azure AD connect

The partners are not integrated with AD DS.

Reference: https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users

https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-integration

QUESTION 10

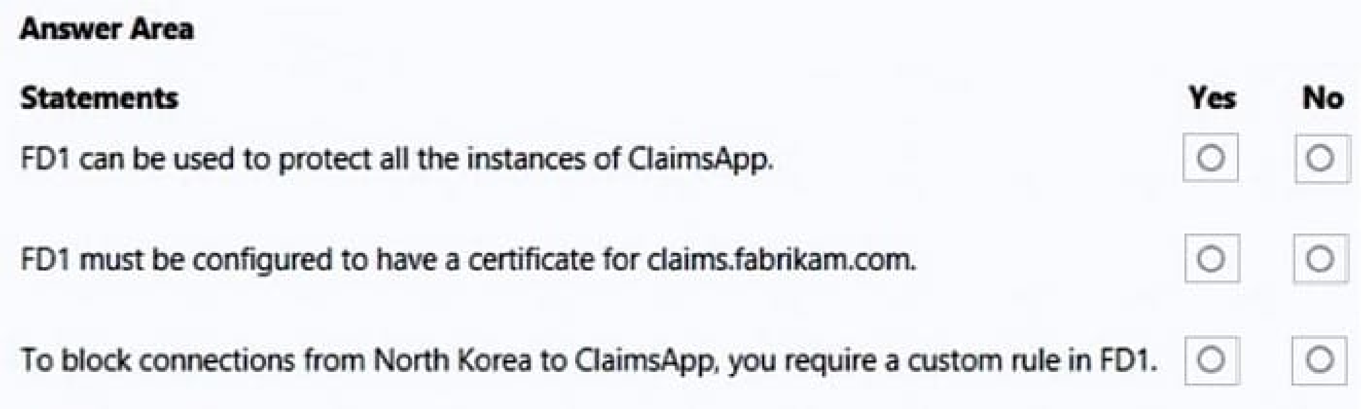
HOTSPOT

You are evaluating the security of ClaimsApp.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

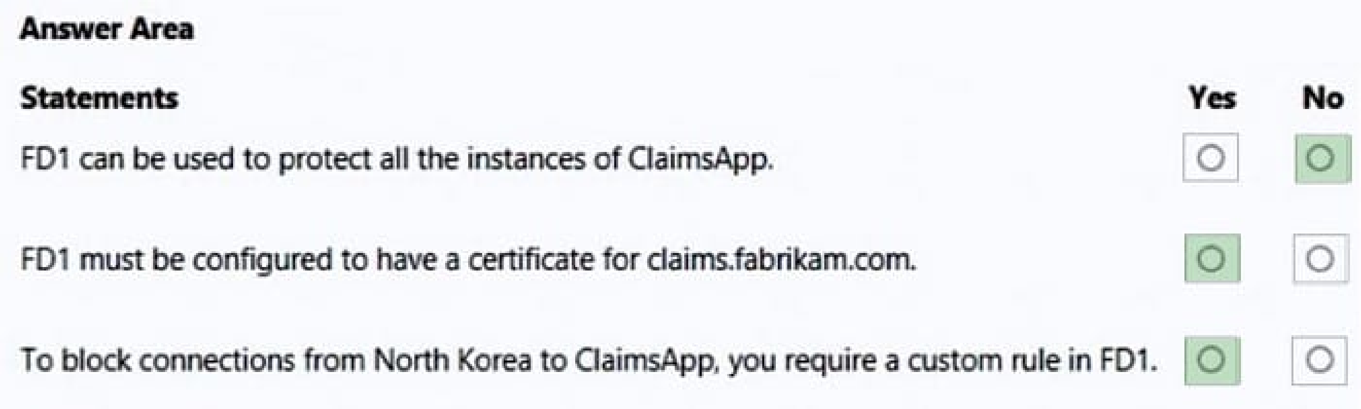
Hot Area:



Answer Area

Statements	Yes	No
FD1 can be used to protect all the instances of ClaimsApp.	○	○
FD1 must be configured to have a certificate for claims.fabrikam.com.	○	○
To block connections from North Korea to ClaimsApp, you require a custom rule in FD1.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
FD1 can be used to protect all the instances of ClaimsApp.	○	●
FD1 must be configured to have a certificate for claims.fabrikam.com.	●	○
To block connections from North Korea to ClaimsApp, you require a custom rule in FD1.	●	○

Box 1: No Box 2: Yes

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

Need certificate for HTTPS.

TLS/SSL certificates

To enable the HTTPS protocol for securely delivering content on a Front Door custom domain, you must use a TLS/SSL certificate. You can choose to use a certificate that is managed by Azure Front Door or use your own certificate.

Box 3: Yes

By default, Azure Front Door will respond to all user requests regardless of the location where the request is coming from. In some scenarios, you may want to restrict the access to your web application by countries/regions. The Web

application firewall (WAF) service in Front Door enables you to define a policy using custom access rules for a specific path on your endpoint to either allow or block access from specified countries/regions.

Note: Requirements. Security Requirements

Fabrikam identifies the following security requirements:

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

Reference: https://techcommunity.microsoft.com/t5/azure-architecture-blog/permit-access-only-from-azure-front-door-to-azure-app-service-as/ba-p/2000173

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https#tlsssl-certificates

QUESTION 11

You have an Azure subscription.

Your company has a governance requirement that resources must be created in the West Europe or North Europe Azure regions.

What should you recommend using to enforce the governance requirement?

A. Azure management groups

B. custom Azure roles

C. Azure Policy assignments

D. regulatory compliance standards in Microsoft Defender for Cloud

Correct Answer: C

Explanation:

Azure Policy helps to enforce organizational standards and to assess compliance at-scale.

Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management. Policy definitions for these common use cases are already available in your Azure

environment as built-ins to help you get started.

Specifically, some useful governance actions you can enforce with Azure Policy include:

Ensuring your team deploys Azure resources only to allowed regions

Enforcing the consistent application of taxonomic tags

Requiring resources to send diagnostic logs to a Log Analytics workspace

Note: Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources. The

assignment applies to all resources within the Resource Manager scope of that assignment.

Reference:

https://learn.microsoft.com/en-us/azure/governance/policy/overview

QUESTION 12

You have a Microsoft 365 E5 subscription.

You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents.

You need to recommend a solution to prevent Personally Identifiable Information (Pll) from being shared.

Which two components should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. data loss prevention (DLP) policies

B. retention label policies

C. eDiscovery cases

D. sensitivity label policies

Correct Answer: AD

A: Data loss prevention in Office 365. Data loss prevention (DLP) helps you protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your

organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically

protect sensitive information across Office 365.

D: Sensitivity labels

Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization\\'s data without hindering the productivity of users and their ability to collaborate.

Plan for integration into a broader information protection scheme. On top of coexistence with OME, sensitivity labels can be used along-side capabilities like Microsoft Purview Data Loss Prevention (DLP) and Microsoft Defender for Cloud

Apps.

Incorrect:

Not B: Retention labels help you retain what you need and delete what you don\\'t at the item level (document or email). They are also used to declare an item as a record as part of a records management solution for your Microsoft 365 data.

Not C: eDiscovery cases in eDiscovery (Standard) and eDiscovery (Premium) let you associate specific searches and exports with a specific investigation. You can also assign members to a case to control who can access the case and view

the contents of the case. Place content locations on legal hold.

Reference: https://motionwave.com.au/keeping-your-confidential-data-secure-with-microsoft-office-365/ https://docs.mic rosoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?view=o365-worldwide#sensitivity-labels

QUESTION 13

DRAG DROP

You have a Microsoft 365 subscription.

You need to recommend a security solution to monitor the following activities:

1.

User accounts that were potentially compromised

2.

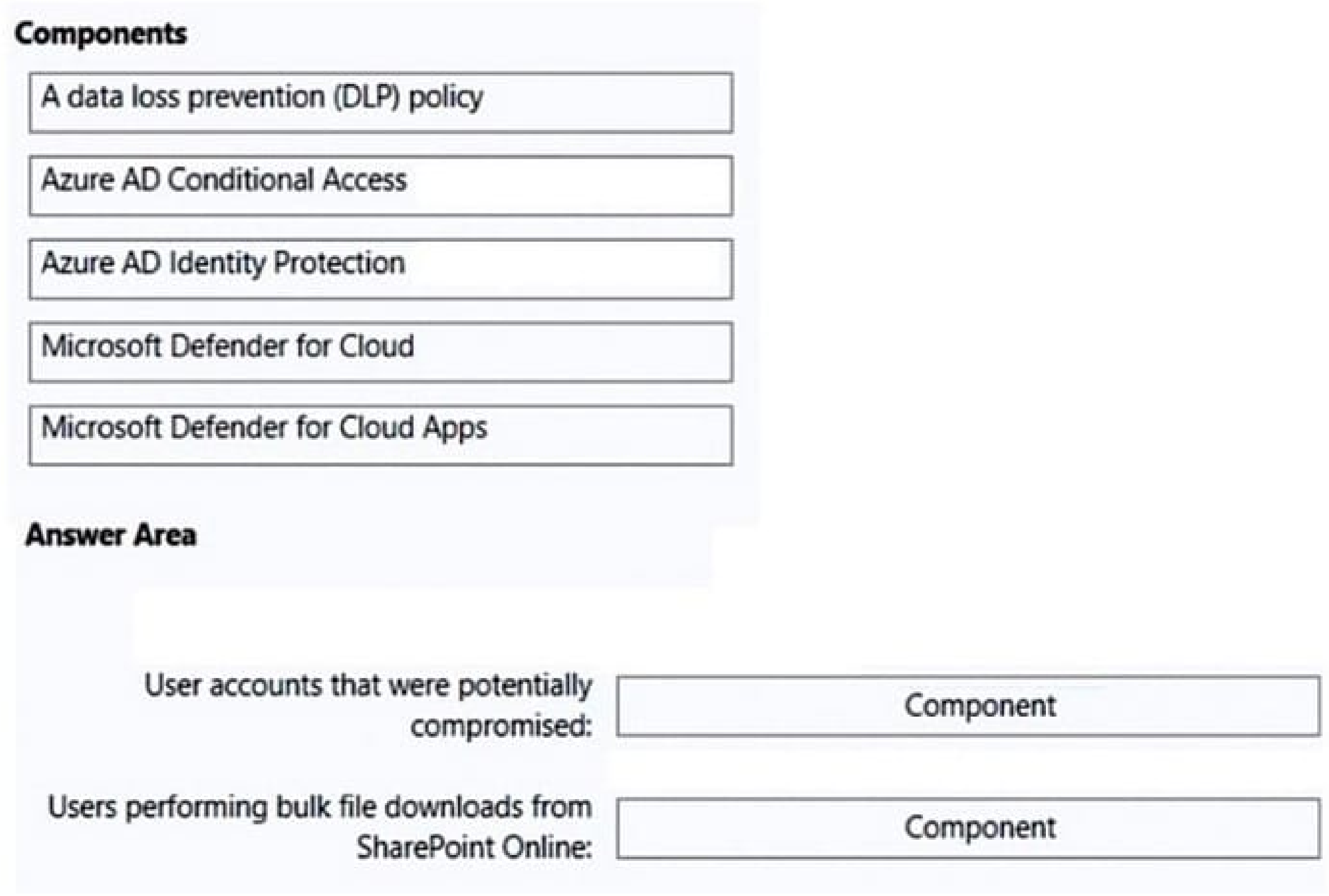
Users performing bulk file downloads from Microsoft SharePoint Online

What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component 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.

Select and Place:



Components

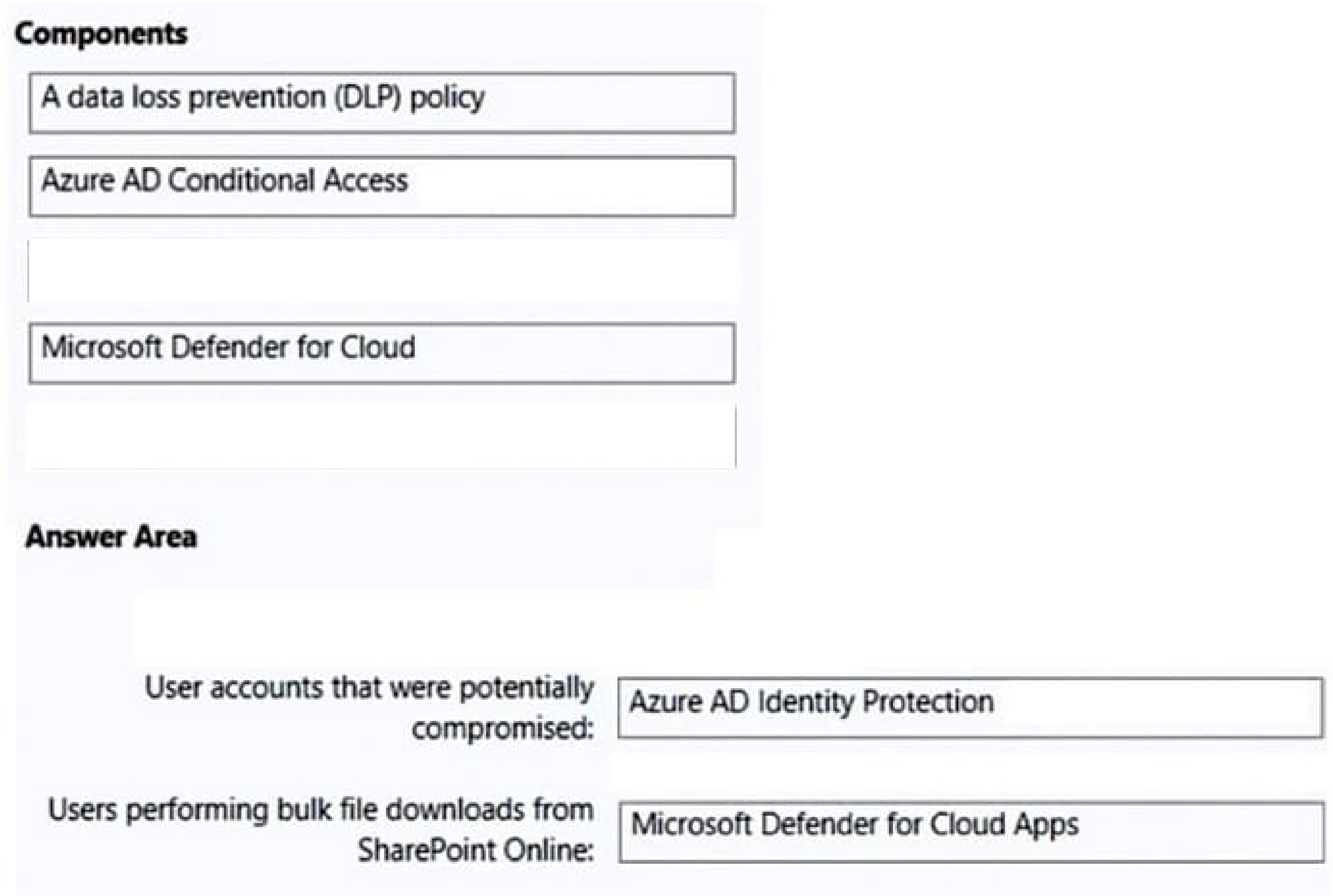
- A data loss prevention (DLP) policy
- Azure AD Conditional Access
- Azure AD Identity Protection
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Answer Area

User accounts that were potentially compromised: Component

Users performing bulk file downloads from SharePoint Online: Component

Correct Answer:



Components

A data loss prevention (DLP) policy

Azure AD Conditional Access

Microsoft Defender for Cloud

Answer Area

User accounts that were potentially compromised: Azure AD Identity Protection

Users performing bulk file downloads from SharePoint Online: Microsoft Defender for Cloud Apps

Box 1: Azure Active Directory (Azure AD) Identity Protection

Risk detections in Azure AD Identity Protection include any identified suspicious actions related to user accounts in the directory. Risk detections (both user and sign-in linked) contribute to the overall user risk score that is found in the Risky

Users report.

Identity Protection provides organizations access to powerful resources to see and respond quickly to these suspicious actions.

Note:

Premium sign-in risk detections include:

*

Token Issuer Anomaly - This risk detection indicates the SAML token issuer for the associated SAML token is potentially compromised. The claims included in the token are unusual or match known attacker patterns.

*

Suspicious inbox manipulation rules - This detection is discovered by Microsoft Defender for Cloud Apps. This detection profiles your environment and triggers alerts when suspicious rules that delete or move messages or folders are set on a user\\'s inbox. This detection may indicate that the user\\'s account is compromised, that messages are being intentionally hidden, and that the mailbox is being used to distribute spam or malware in your organization.

*

Etc.

Incorrect:

Not: Microsoft 365 Defender for Cloud

Part of your incident investigation can include user accounts. You can see the details of user accounts identified in the alerts of an incident in the Microsoft 365 Defender portal from Incidents and alerts > incident > Users.

Box 2: Microsoft 365 Defender for App

Defender for Cloud apps detect mass download (data exfiltration) policy

Detect when a certain user accesses or downloads a massive number of files in a short period of time.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks
https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exfiltration
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users

QUESTION 14

HOTSPOT

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure.

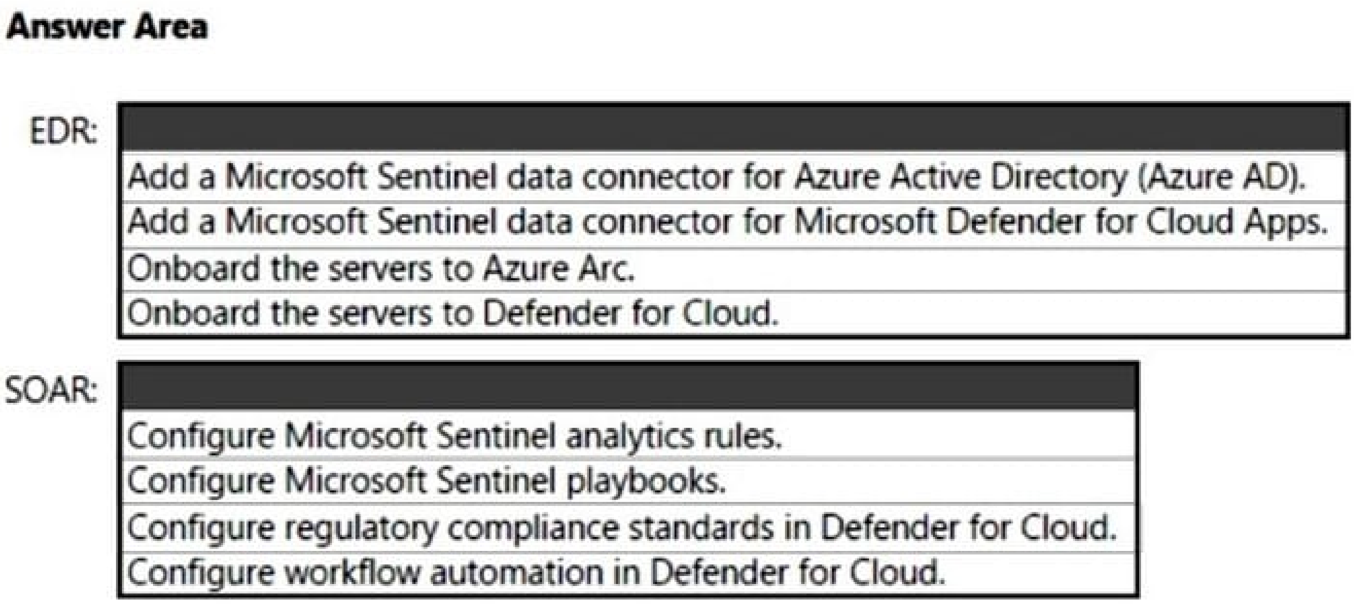
You plan to deploy Azure virtual machines that will run Windows Server.

You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.

How should you recommend enabling each capability? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

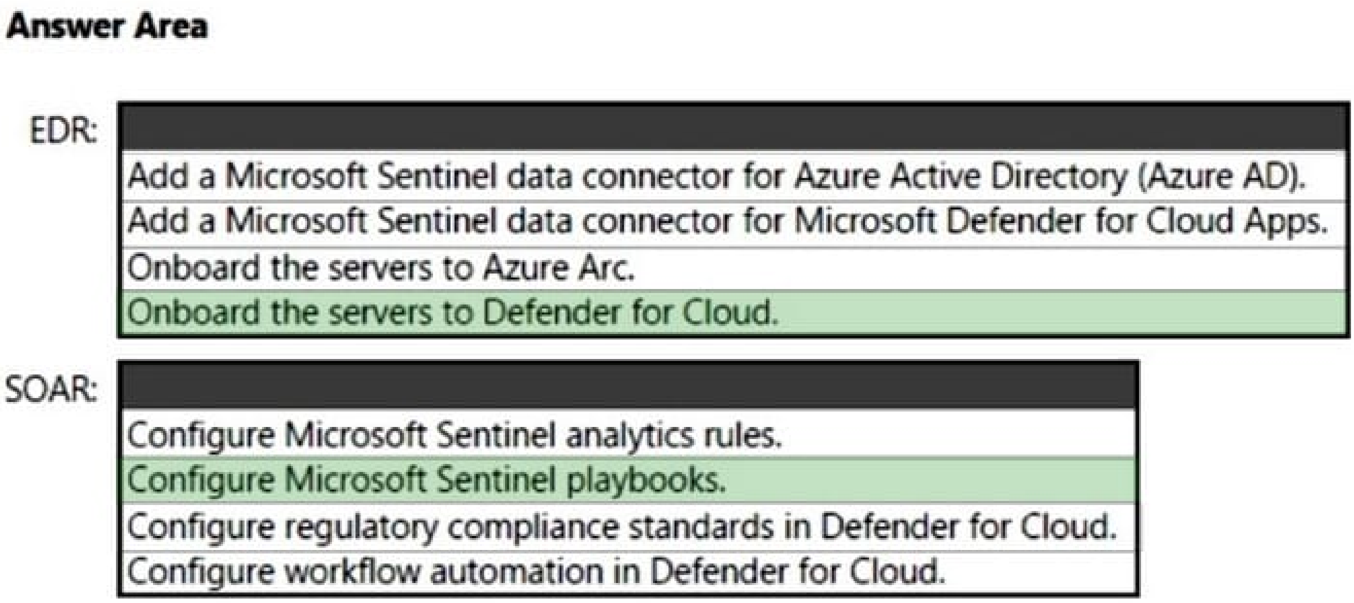
EDR:

Add a Microsoft Sentinel data connector for Azure Active Directory (Azure AD).
Add a Microsoft Sentinel data connector for Microsoft Defender for Cloud Apps.
Onboard the servers to Azure Arc.
Onboard the servers to Defender for Cloud.

SOAR:

Configure Microsoft Sentinel analytics rules.
Configure Microsoft Sentinel playbooks.
Configure regulatory compliance standards in Defender for Cloud.
Configure workflow automation in Defender for Cloud.

Correct Answer:



Answer Area

EDR:

Add a Microsoft Sentinel data connector for Azure Active Directory (Azure AD).
Add a Microsoft Sentinel data connector for Microsoft Defender for Cloud Apps.
Onboard the servers to Azure Arc.
Onboard the servers to Defender for Cloud.

SOAR:

Configure Microsoft Sentinel analytics rules.
Configure Microsoft Sentinel playbooks.
Configure regulatory compliance standards in Defender for Cloud.
Configure workflow automation in Defender for Cloud.

Box 1: Onboard the servers to Defender for Cloud.

Extended detection and response (XDR) is a new approach defined by industry analysts that are designed to deliver intelligent, automated, and integrated security across domains to help defenders connect seemingly disparate alerts and get

ahead of attackers.

As part of this announcement, we are unifying all XDR technologies under the Microsoft Defender brand. The new Microsoft Defender is the most comprehensive XDR in the market today and prevents, detects, and responds to threats across

identities, endpoints, applications, email, IoT, infrastructure, and cloud platforms.

Box 2: Configure Microsoft Sentinel playbooks.

As a SOAR platform, its primary purposes are to automate any recurring and predictable enrichment, response and remediation tasks that are the responsibility of Security Operations Centers (SOC/SecOps). Leveraging SOAR frees up time

and resources for more in-depth investigation of and hunting for advanced threats. Automation takes a few different forms in Microsoft Sentinel, from automation rules that centrally manage the automation of incident handling and response to

playbooks that run predetermined sequences of actions to provide robust and flexible advanced automation to your threat response tasks.

Reference: https://www.microsoft.com/security/blog/2020/09/22/microsoft-unified-siem-xdr-modernize-security-operations/

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/become-a-microsoft-sentinel-automation-ninja/ba-p/3563377

QUESTION 15

You have a Microsoft 365 E5 subscription and an Azure subscription.

You are designing a Microsoft deployment.

You need to recommend a solution for the security operations team. The solution must include custom views and a dashboard for analyzing security events.

What should you recommend using in Microsoft Sentinel?

A. playbooks

B. workbooks

C. notebooks

D. threat intelligence

Correct Answer: B

After you connected your data sources to Microsoft Sentinel, you get instant visualization and analysis of data so that you can know what\\'s happening across all your connected data sources. Microsoft Sentinel gives you workbooks that provide you with the full power of tools already available in Azure as well as tables and charts that are built in to provide you with analytics for your logs and queries. You can either use built-in workbooks or create a new workbook easily, from scratch or based on an existing workbook.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/get-visibility