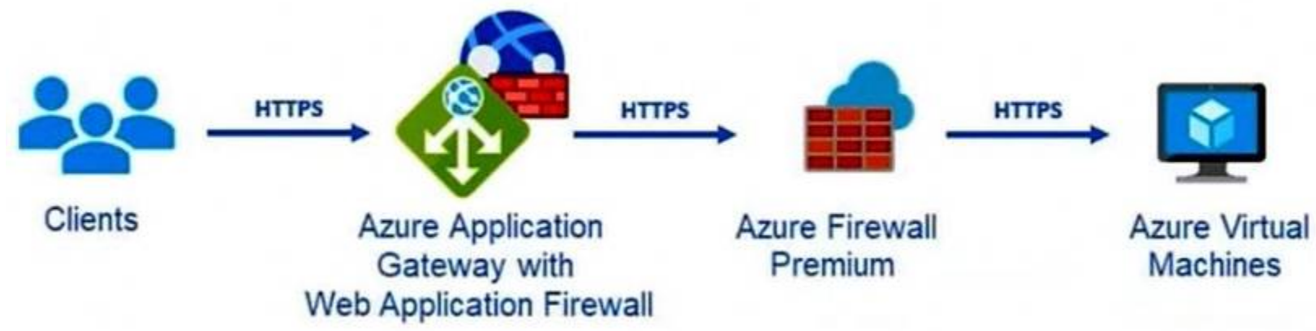
Number: SC-100
Passing Score: 800
Time Limit: 120
File Version: 13.0

Exam Code: SC-100
Exam Name: Microsoft Cybersecurity Architect

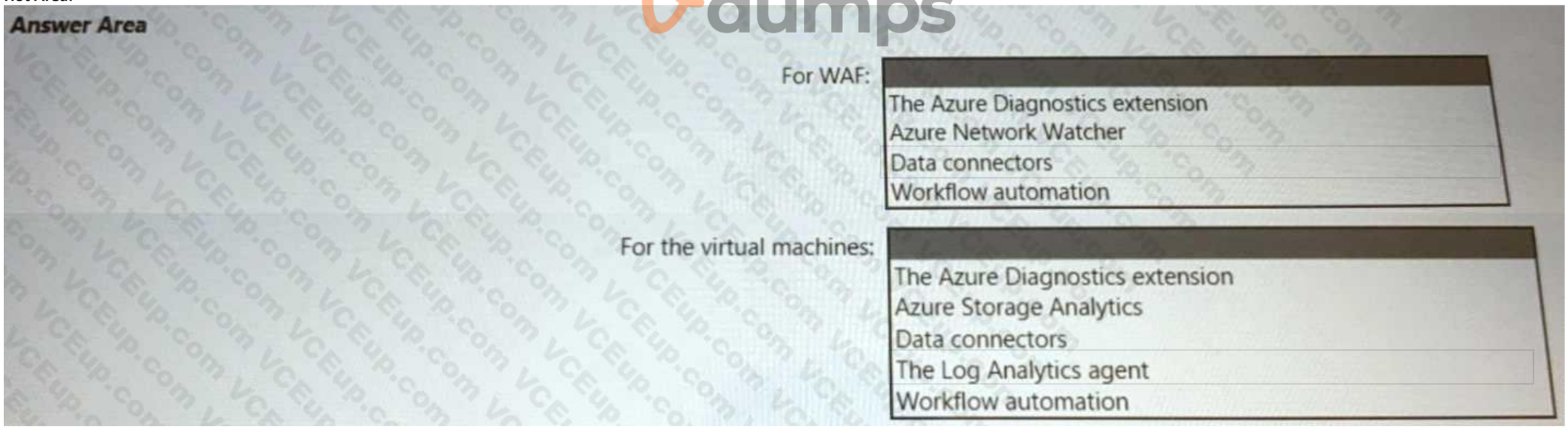
Exam B

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.

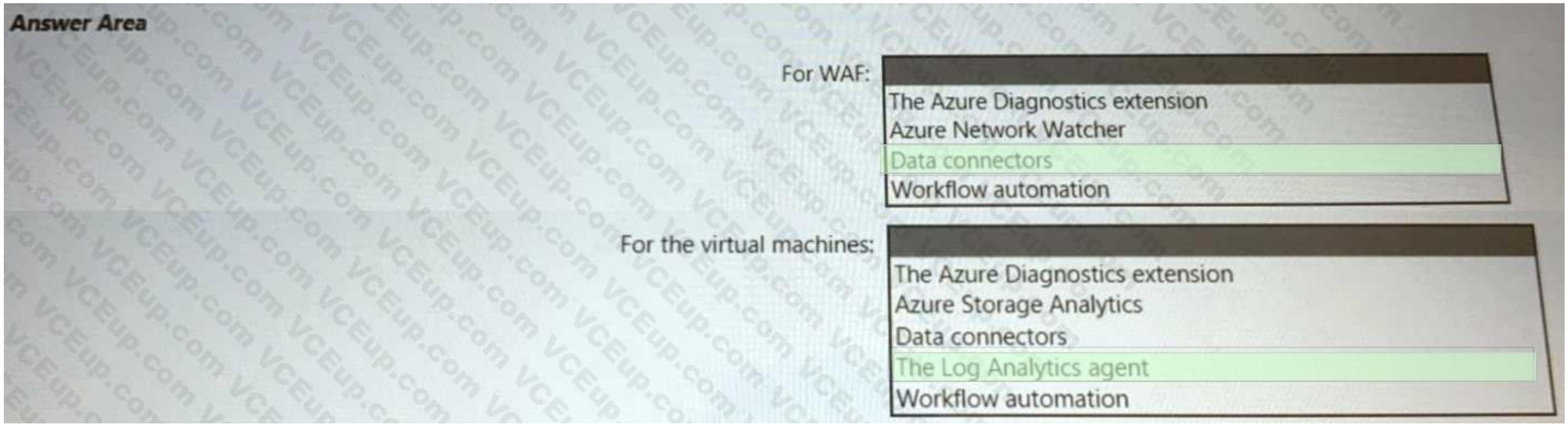


You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-.
• Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
• Use Defender for Cloud to review alerts from the virtual machines.
What should you include in the solution? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Hot Area:



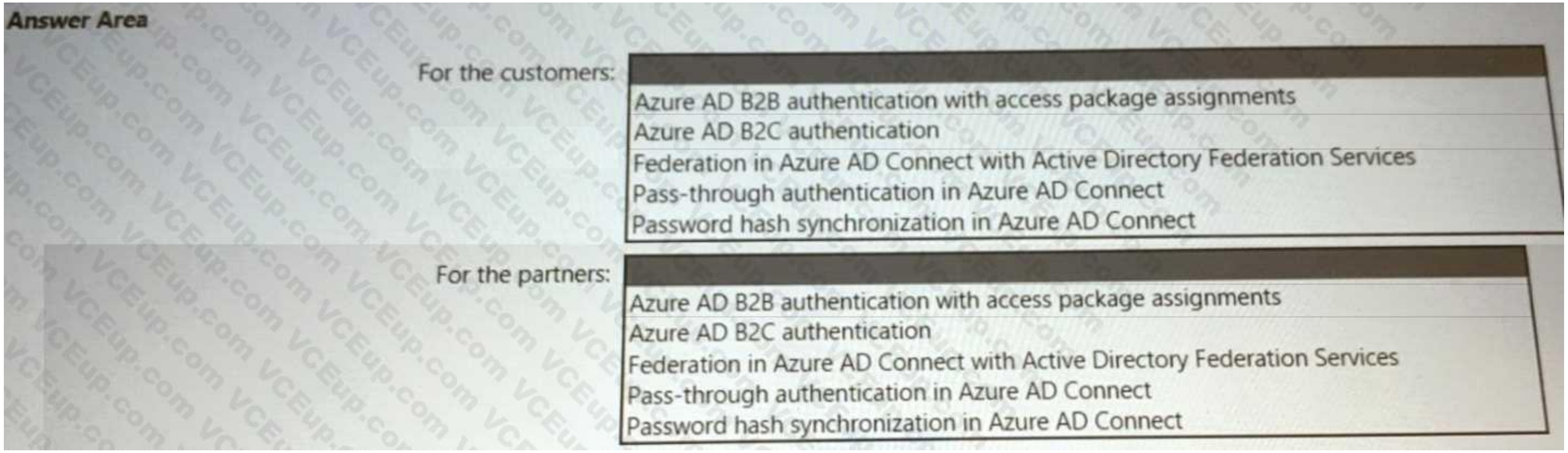
Answer Area:



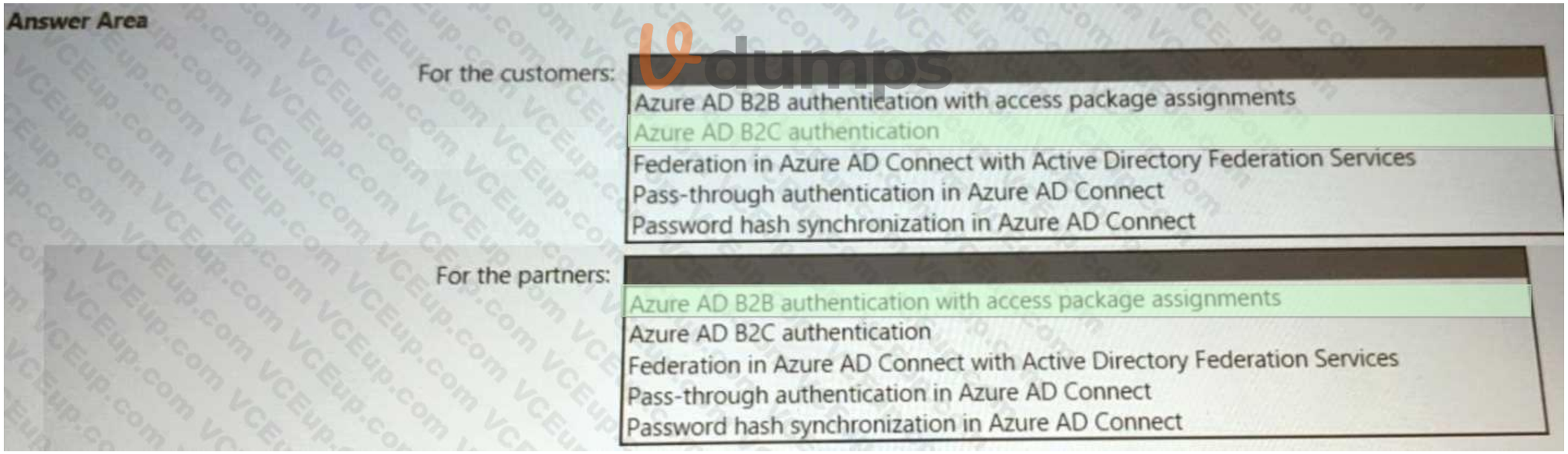
Section:
Explanation:
Box 1: Data connectors -
Microsoft Sentinel connector streams security alerts from Microsoft Defender for Cloud into Microsoft Sentinel. Launch a WAF workbook (see step 7 below)
The WAF workbook works for all Azure Front Door, Application Gateway, and CDN WAFs. Before connecting 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.

QUESTION 2
HOTSPOT
Your company has a Microsoft 365 E5 subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DSV You need to recommend an identity security strategy that meets the following requirements:
• Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website
• 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:



Section:

Explanation:

Box 1 --> https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview

Box 2 -- > https://docs.microsoft.com/en-us/azure/active-directory/external-identities/identity- providers

QUESTION 3

You are designing the security standards for a new Azure environment.
You need to design a privileged identity strategy based on the Zero Trust model.
Which framework should you follow to create the design?

A. Enhanced Security Admin Environment (ESAE)
B. Microsoft Security Development Lifecycle (SDL)
C. Rapid Modernization Plan (RaMP)
D. Microsoft Operational Security Assurance (OSA)

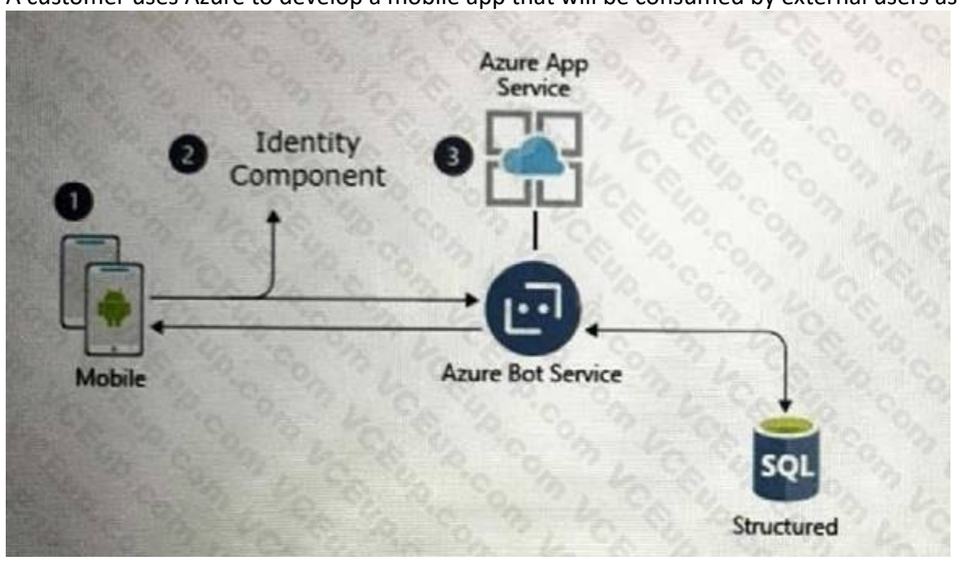
Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan This rapid modernization plan (RAMP) will help you quickly adopt Microsoft's recommended privileged access strategy.

QUESTION 4
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?

A. role-based authorization
B. Azure AD Privileged Identity Management (PIM)
C. resource-based authorization
D. Azure AD Multi-Factor Authentication

Correct Answer: D
Section:
Explanation:
(https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim- configure) https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory- pricing?rtc=1

QUESTION 5
A customer uses Azure to develop a mobile app that will be consumed by external users as shown in the following exhibit.



You need to design an identity strategy for the app. The solution must meet the following requirements:
• Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.
• Be managed separately from the identity store of the customer.
• Support fully customizable branding for each app.
Which service should you recommend to complete the design?

A. Azure Active Directory (Azure AD) B2C
B. Azure Active Directory (Azure AD) B2B
C. Azure AD Connect
D. Azure Active Directory Domain Services (Azure AD DS)

Correct Answer: A
Section:
Explanation:
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-b2c/customize-ui-with-html?pivots=b2c- user-flow

QUESTION 6
A customer has a Microsoft 365 E5 subscription and an Azure subscription.
The customer wants to centrally manage security incidents, analyze log, audit activity, and search for potential threats across all deployed services. You need to recommend a solution for the customer. The solution must minimize costs.
What should you include in the recommendation?

A. Microsoft 365 Defender
B. Microsoft Defender for Cloud
C. Microsoft Defender for Cloud Apps
D. Microsoft Sentinel

Correct Answer: D
Section:

QUESTION 7
You have an Azure subscription that is used as an Azure landing zone for an application. You need to evaluate the security posture of all the workloads in the landing zone. What should you do first?

A. Add Microsoft Sentinel data connectors.
B. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.
C. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.
D. Obtain Azure Active Directory Premium Plan 2 licenses.

Correct Answer: A
Section:

QUESTION 8
Your company plans to move all on-premises virtual machines to Azure. A network engineer proposes the Azure virtual network design shown in the following table.

Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

You need to recommend an Azure Bastion deployment to provide secure remote access to all the virtual machines. Based on the virtual network design, how many Azure Bastion subnets are required?

A. 1
B. 2
C. 3
D. 4
E. 5

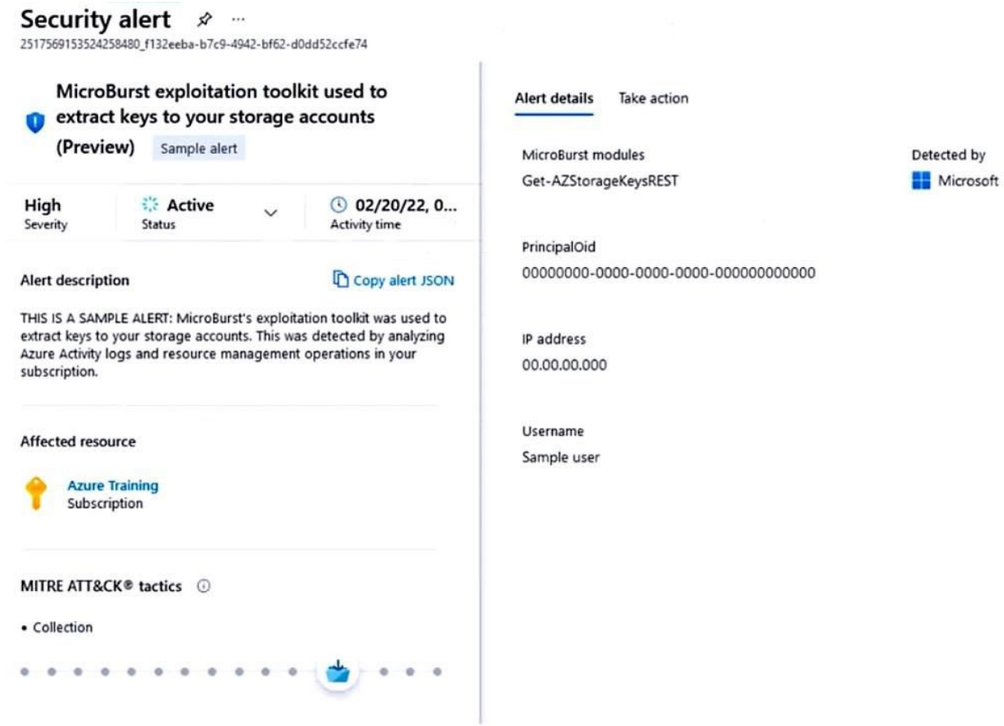
Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/bastion/vnet-peering https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure- bastion

QUESTION 9
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You need to enforce ISO 2700V2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatically. What should you use?

A. the regulatory compliance dashboard in Defender for Cloud
B. Azure Policy
C. Azure Blueprints
D. Azure role-based access control (Azure RBAC)

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/iso27001-shared/control-mapping https://docs.microsoft.com/en-us/azure/defender-for-cloud/release-notes-archive https://docs.microsoft.com/en-us/azure/defender-for-cloud/prevent-misconfigurations

QUESTION 10
You receive a security alert in Microsoft Defender for Cloud as shown in the exhibit. (Click the Exhibit tab.)



After remediating the threat which policy definition should you assign to prevent the threat from reoccurring?

A. Storage account public access should be disallowed
B. Azure Key Vault Managed HSM should have purge protection enabled
C. Storage accounts should prevent shared key access
D. Storage account keys should not be expired

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent

QUESTION 11
Your company is preparing for cloud adoption.
You are designing security for Azure landing zones.
Which two preventative controls can you implement to increase the secure score? Each NOTE: Each correct selection is worth one point.

A. Azure Firewall
B. Azure Web Application Firewall (WAF)
C. Microsoft Defender for Cloud alerts
D. Azure Active Directory (Azure AD Privileged Identity Management (PIM)
E. Microsoft Sentinel

Correct Answer: A, B
Section:
Explanation:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 12
You are designing security for an Azure landing zone. Your company identifies the following compliance and privacy requirements:
• Encrypt cardholder data by using encryption keys managed by the company.
• Encrypt insurance claim files by using encryption keys hosted on-premises.
Which two configurations meet the compliance and privacy requirements? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Store the insurance claim data in Azure Blob storage encrypted by using customer-provided keys.
B. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM
C. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.
D. Store the cardholder data in an Azure SQL database that is encrypted by using Microsoft-managed Keys.

Correct Answer: A, C
Section:
Explanation:
https://azure.microsoft.com/en-us/blog/customer-provided-keys-with-azure-storage-service- encryption/

QUESTION 13
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?

A. Azure Storage Analytics
B. Azure Network Watcher
C. Microsoft Sentinel
D. Azure Policy

Correct Answer: D
Section:
Explanation:
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

QUESTION 14
You have 50 Azure subscriptions.
You need to monitor resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.
NOTE: Each correct selection is worth one point.

A. Assign an initiative to a management group.
B. Assign a policy to each subscription.
C. Assign a policy to a management group.
D. Assign an initiative to each subscription.
E. Assign a blueprint to each subscription.

F. Assign a blueprint to a management group.

Correct Answer: A, F
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview https://docs.microsoft.com/en-us/azure/governance/blueprints/overview https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001 https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

QUESTION 15
Your company has a Microsoft 365 E5 subscription. The company wants to identify and classify data in Microsoft Teams, SharePoint Online, and Exchange Online. You need to recommend a solution to identify documents that contain sensitive information. What should you include in the recommendation?

A. data classification content explorer
B. data loss prevention (DLP)
C. eDiscovery
D. Information Governance

Correct Answer: B
Section:

QUESTION 16
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.

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

Correct Answer: A, C
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user- flow?pivots=b2c-user-flow

QUESTION 17
Your company has a Microsoft 365 E5 subscription.
Users use Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive for sharing and collaborating. The company identifies protected health information (PHI) within stored documents and communications. What should you recommend using to prevent the PHI from being shared outside the company?

A. insider risk management policies
B. data loss prevention (DLP) policies
C. sensitivity label policies
D. retention policies

Correct Answer: C
Section:

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp- policy?view=o365-worldwide

QUESTION 18
You are designing the security standards for containerized applications onboarded to Azure. You are evaluating the use of Microsoft Defender for Containers. In which two environments can you use Defender for Containers to scan for known vulnerabilities?
Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Linux containers deployed to Azure Container Registry
B. Linux containers deployed to Azure Kubernetes Service (AKS)
C. Windows containers deployed to Azure Container Registry
D. Windows containers deployed to Azure Kubernetes Service (AKS)
E. Linux containers deployed to Azure Container Instances

Correct Answer: A, C
Section:
Explanation:
https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas- services/9-specify-security-requirements-for-containers https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction#view-vulnerabilities-for-running-images

QUESTION 19
Your company has an on-premises network and an Azure subscription.
The company does NOT have a Site-to-Site VPN or an ExpressRoute connection to Azure.
You are designing the security standards for Azure App Service web apps. The web apps will access Microsoft SQL Server databases on the network. You need to recommend security standards that will allow the web apps to access the databases. The solution must minimize the number of open internet-accessible endpoints to the on-premises network. What should you include in the recommendation?

A. a private endpoint
B. hybrid connections
C. virtual network NAT gateway integration
D. virtual network integration

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections

QUESTION 20
Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft B65 subscription, and an Azure subscription. The company's on-premises network contains internal web apps that use Kerberos authentication.
Currently, the web apps are accessible only from the network.
You have remote users who have personal devices that run Windows 11.
You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:
• Prevent the remote users from accessing any other resources on the network.
• Support Azure Active Directory (Azure AD) Conditional Access.
• Simplify the end-user experience.
What should you include in the recommendation?

A. Azure AD Application Proxy

B. Azure Virtual WAN
C. Microsoft Tunnel
D. web content filtering in Microsoft Defender for Endpoint

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/learn/modules/configure-azure-ad-application-proxy/2-explore

QUESTION 21
Your company has a third-party security information and event management (SIEM) solution that uses Splunk and Microsoft Sentinel. You plan to integrate Microsoft Sentinel with Splunk. You need to recommend a solution to send security events from Microsoft Sentinel to Splunk. What should you include in the recommendation?

A. Azure Event Hubs
B. Azure Data Factor
C. a Microsoft Sentinel workbook
D. a Microsoft Sentinel data connector

Correct Answer: D
Section:
Explanation:
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with- splunk-via-eventhub/ba-p/2307029

QUESTION 22
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You have an Amazon Web Services (AWS) implementation. You plan to extend the Azure security strategy to the AWS implementation. The solution will NOT use Azure Arc. Which three services can you use to provide security for the AWS resources? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. Azure Active Directory (Azure AD) Conditional Access
C. Microsoft Defender for servers
D. Azure Policy
E. Microsoft Defender for Containers

Correct Answer: B, D, E
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint- solutions-clouds-containers?tabs=aws-eks

QUESTION 23
You have an on-premises network that has several legacy applications. The applications perform LDAP queries against an existing directory service. You are migrating the on-premises infrastructure to a cloud-only infrastructure. You need to recommend an identity solution for the infrastructure that supports the legacy applications. The solution must minimize the administrative effort to maintain the infrastructure. Which identity service should you include in the recommendation?

A. Azure Active Directory Domain Services (Azure AD DS)
B. Azure Active Directory (Azure AD) B2C
C. Azure Active Directory (Azure AD)
D. Active Directory Domain Services (AD DS)

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview

QUESTION 24
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 adaptive network hardening. Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:

QUESTION 25
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 onboarding all virtual machines to Microsoft Defender for Endpoint.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 26
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance. You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance. Solution: You recommend configuring gateway-required virtual network integration.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a- specific-azure-front-door-instance

QUESTION 27
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance. You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance. Solution: You recommend access restrictions to allow traffic from the backend IP address of the Front Door instance. Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 28
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance. You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance. Solution: You recommend access restrictions that allow traffic from the Front Door service tags.
Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a- specific-azure-front-door-instance

QUESTION 29
You are creating an application lifecycle management process based on the Microsoft Security Development Lifecycle (SDL). You need to recommend a security standard for onboarding applications to Azure. The standard will include recommendations for application design, development, and deployment What should you include during the application design phase?

A. static application security testing (SAST) by using SonarQube
B. dynamic application security testing (DAST) by using Veracode
C. threat modeling by using the Microsoft Threat Modeling Tool
D. software decomposition by using Microsoft Visual Studio Enterprise

Correct Answer: C
Section:
Explanation:
https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

QUESTION 30
Your company is developing a new Azure App Service web app. You are providing design assistance to verify the security of the web app. You need to recommend a solution to test the web app for vulnerabilities such as insecure server configurations, cross-site scripting (XSS), and SQL injection. What should you include in the recommendation?

A. interactive application security testing (IAST)
B. static application security testing (SAST)
C. runtime application se/f-protection (RASP)
D. dynamic application security testing (DAST)

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/security/develop/secure-develop#test-your-application-in- an-operating-state

QUESTION 31

Your company plans to deploy several Azure App Service web apps. The web apps will be deployed to the West Europe Azure region. The web apps will be accessed only by customers in Europe and the United States. You need to recommend a solution to prevent malicious bots from scanning the web apps for vulnerabilities. The solution must minimize the attach surface. What should you include in the recommendation?

A. Azure Firewall Premium
B. Azure Application Gateway Web Application Firewall (WAF)
C. network security groups (NSGs)
D. Azure Traffic Manager and application security groups

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection

QUESTION 32
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?

A. Microsoft Defender for Cloud Apps
B. insider risk management
C. Microsoft Information Protection
D. Azure Purview

Correct Answer: C
Section:
Explanation:
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.

QUESTION 33
Your company has a hybrid cloud infrastructure.
The company plans to hire several temporary employees within a brief period. The temporary employees will need to access applications and data on the company' premises network. The company's security policy prevents the use of personal devices for accessing company data and applications. You need to recommend a solution to provide the temporary employee with access to company resources. The solution must be able to scale on demand. What should you include in the recommendation?

A. Migrate the on-premises applications to cloud-based applications.
B. Redesign the VPN infrastructure by adopting a split tunnel configuration.
C. Deploy Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access.
D. Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual- desktop https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft- defender-for-cloud-apps/ba-p/2835842

QUESTION 34
You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases. All resources are backed up multiple times a day by using Azure Backup. You are developing a strategy to protect against ransomware attacks.
You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successful\ ransonvware attack. Which two controls should you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Use Azure Monitor notifications when backup configurations change.
B. Require PINs for critical operations.
C. Perform offline backups to Azure Data Box.
D. Encrypt backups by using customer-managed keys (CMKs).
E. Enable soft delete for backups.

Correct Answer: A, B
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against- ransomware'You need to recommend which CONTROLS must be enabled to ENSURE that Azure Backup can be used to RESTORE the resources in the event of a successful ransomware attack.' Whilst helpful for auditing purposes and detection of a malicious attack, monitoring configuration changes and alerting after a change is made does not represent a CONTROL which ENSURES Azure Backup can be used to RESTORE the resources.

QUESTION 35
Your company develops several applications that are accessed as custom enterprise applications in Azure Active Directory (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. device compliance policies in Microsoft Endpoint Manager
D. Azure AD Conditional Access policies
E. user risk policies in Azure AD Identity Protection

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional- access-policy-location https://docs.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules

QUESTION 36
Your company has a Microsoft 365 subscription and uses Microsoft Defender for Identity. You are informed about incidents that relate to compromised identities. You need to recommend a solution to expose several accounts for attackers to exploit. When the attackers attempt to exploit the accounts, an alert must be triggered. Which Defender for Identity feature should you include in the recommendation?

A. standalone sensors
B. honeytoken entity tags
C. sensitivity labels
D. custom user tags

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeytoken- activityThe Sensitive tag is used to identify high value assets.(user / devices / groups)Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert. and Defender for Identity considers Exchange servers as high-value assets and automatically tags them as Sensitive

QUESTION 37
You have a Microsoft 365 E5 subscription and an Azure subscription. You are designing a Microsoft Sentinel 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
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview

QUESTION 38
Your company has an on-premise network in Seattle and an Azure subscription. The on-premises network contains a Remote Desktop server. The company contracts a third-party development firm from France to develop and deploy resources to the virtual machines hosted in the Azure subscription. Currently, the firm establishes an RDP connection to the Remote Desktop server. From the Remote Desktop connection, the firm can access the virtual machines hosted in Azure by using custom administrative tools installed on the Remote Desktop server. All the traffic to the Remote Desktop server is captured by a firewall, and the firewall only allows specific connections from France to the server. You need to recommend a modern security solution based on the Zero Trust model. The solution must minimize latency tor developers. Which three actions should you recommend? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.
B. Implement Azure Firewall to restrict host pool outbound access.
C. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.
D. Migrate from the Remote Desktop server to Azure Virtual Desktop.
E. Deploy a Remote Desktop server to an Azure region located in France.

Correct Answer: B, C, D
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop

QUESTION 39
Your company is moving all on-premises workloads to Azure and Microsoft 365. Vou need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:
• Minimizes manual intervention by security operation analysts
• Supports Waging alerts within Microsoft Teams channels
What should you include in the strategy?

A. data connectors
B. playbooks
C. workbooks
D. KQL

Correct Answer: B

Section:
Explanation:

QUESTION 40
Your company plans to provision blob storage by using an Azure Storage account The blob storage will be accessible from 20 application sewers on the internet. You need to recommend a solution to ensure that only the application servers can access the storage account. What should you recommend using to secure the blob storage?

A. service tags in network security groups (NSGs)
B. managed rule sets in Azure Web Application Firewall (WAF) policies
C. inbound rules in network security groups (NSGs)
D. firewall rules for the storage account
E. inbound rules in Azure Firewall

Correct Answer: D
Section:

QUESTION 41
Your company has a Microsoft 365 E5 subscription.
The company plans to deploy 45 mobile self-service kiosks that will run Windows
10. You need to provide recommendations to secure the kiosks. The solution must meet the following requirements:
• Ensure that only authorized applications can run on the kiosks.
• Regularly harden the kiosks against new threats.
Which two actions should you include in the recommendations? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Onboard the kiosks to Azure Monitor.
B. Implement Privileged Access Workstation (PAW) for the kiosks.
C. Implement Automated Investigation and Remediation (AIR) in Microsoft Defender for Endpoint.
D. Implement threat and vulnerability management in Microsoft Defender for Endpoint.
E. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint.

Correct Answer: D, E
Section:
Explanation:
(https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability- management/defender-vulnerability-management?view=o365-worldwide)

QUESTION 42
Your company has an office in Seattle.
The company has two Azure virtual machine scale sets hosted on different virtual networks.
The company plans to contract developers in India.
You need to recommend a solution provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal. The solution must meet the following requirements:
• Prevent exposing the public IP addresses of the virtual machines.
• Provide the ability to connect without using a VPN.
• Minimize costs.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Deploy Azure Bastion to one virtual network.

B. Deploy Azure Bastion to each virtual network.
C. Enable just-in-time VM access on the virtual machines.
D. Create a hub and spoke network by using virtual network peering.
E. Create NAT rules and network rules in Azure Firewall.

Correct Answer: A, D
Section:
Explanation:
https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure- bastion

QUESTION 43
Your company is developing a modern application that will run as an Azure App Service web app. You plan to perform threat modeling to identify potential security issues by using the Microsoft Threat Modeling Tool. Which type of diagram should you create?

A. dataflow
B. system flow
C. process flow
D. network flow

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational- data-flow-diagram-elements/1b-elements https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started? source=recommendations

QUESTION 44
Your company is moving a big data solution to Azure.
The company plans to use the following storage workloads:
• Azure Storage blob containers
• Azure Data Lake Storage Gen2
• Azure Storage file shares
• Azure Disk Storage
Which two storage workloads support authentication by using Azure Active Directory (Azure AD)?
Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Azure Disk Storage
B. Azure Storage blob containers
C. Azure Storage file shares
D. Azure Data Lake Storage Gen2

Correct Answer: B, D
Section:

QUESTION 45
You are evaluating an Azure environment for compliance.
You need to design an Azure Policy implementation that can be used to evaluate compliance without changing any resources. Which effect should you use in Azure Policy?

A. Deny

B. Disabled
C. Modify
D. Append

Correct Answer: B
Section:
Explanation:
Before looking to manage new or updated resources with your new policy definition, it's best to see how it evaluates a limited subset of existing resources, such as a test resource group. Use the enforcement mode Disabled (DoNotEnforce) on your policy assignment to prevent the effect from triggering or activity log entries from being created. https://docs.microsoft.com/en-us/azure/governance/policy/concepts/evaluate-impact

QUESTION 46
Your company has devices that run either Windows 10, Windows 11, or Windows Server.
You are in the process of improving the security posture of the devices.
You plan to use security baselines from the Microsoft Security Compliance Toolkit.
What should you recommend using to compare the baselines to the current device configurations?

A. Microsoft Intune
B. Policy Analyzer
C. Local Group Policy Object (LGPO)
D. Windows Autopilot

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security- configuration-framework/security-compliance-toolkit-10

QUESTION 47
A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications. The customer discovers that several endpoints are infected with malware.
The customer suspends access attempts from the infected endpoints.
The malware is removed from the end point.
Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Endpoint reports the endpoints as compliant.
B. Microsoft Intune reports the endpoints as compliant.
C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.
D. The client access tokens are refreshed.

Correct Answer: B, D
Section:

QUESTION 48

A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription. All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.

The customer plans to deploy Microsoft Sentinel.

You need to recommend configurations to meet the following requirements:

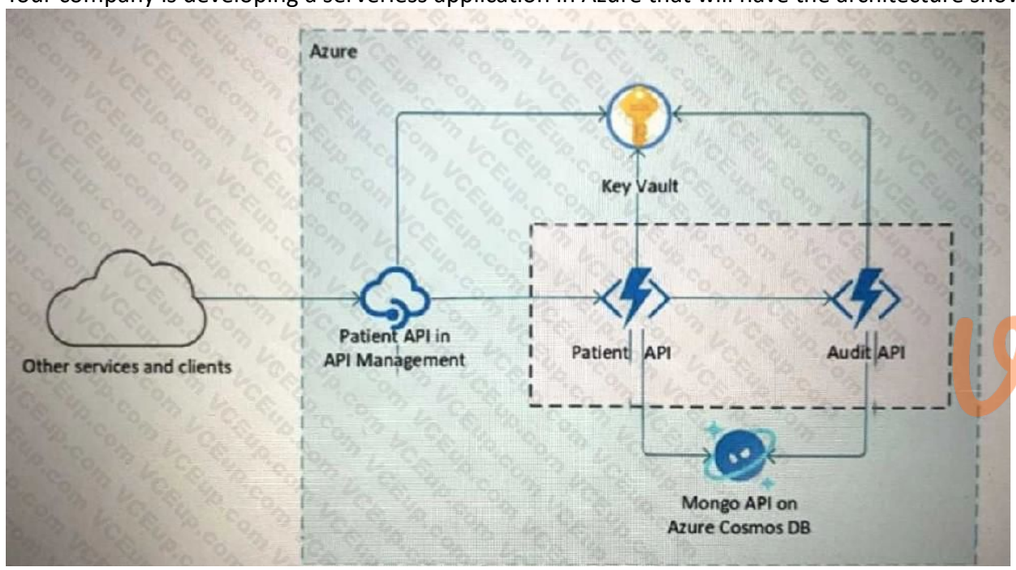
- Ensure that the security operations team can access the security logs and the operation logs.

• Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network. Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Configure Azure Active Directory (Azure AD) Conditional Access policies.
B. Use the Azure Monitor agent with the multi-homing configuration.
C. Implement resource-based role-based access control (RBAC) in Microsoft Sentinel.
D. Create a custom collector that uses the Log Analytics agent.

Correct Answer: B, C
Section:

QUESTION 49
Your company is developing a serverless application in Azure that will have the architecture shown in the following exhibit.



You need to recommend a solution to isolate the compute components on an Azure virtual network.
What should you include in the recommendation?

A. Azure Active Directory (Azure AD) enterprise applications
B. an Azure App Service Environment (ASE)
C. Azure service endpoints
D. an Azure Active Directory (Azure AD) application proxy

Correct Answer: B
Section:
Explanation:
App Service environments (ASEs) are appropriate for application workloads that require: Very high scale,Isolation and secure network access,High memory utilization.This capability can host your: Windows web apps,Linux web apps Docker containers,Mobile apps Functionshttps://docs.microsoft.com/en-us/azure/app-service/environment/overview

QUESTION 50
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. sensitivity label policies
C. retention label policies
D. eDiscovery cases

Correct Answer: A, B
Section:
Explanation:
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.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.
https://motionwave.com.au/keeping-your-confidential-data-secure-with-microsoft-office-365/ https://docs.microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect- information?view=o365-worldwide#sensitivity-labels

QUESTION 51
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?

A. eDiscovery
B. retention policies
C. Compliance Manager
D. Microsoft Information Protection

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

QUESTION 52

You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance. You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance. Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID. Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access- to-my-backend-to-only-azure-front-door-

QUESTION 53
Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.

You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model. Solution: You recommend creating private endpoints for the web app and the database layer. Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section:
Explanation:
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints

QUESTION 54
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 just-in-time (JIT) VM access on all virtual machines.
Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 55
Your on-premises network contains an e-commerce web app that was developed in Angular and Node.js. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.

You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model. Solution: You recommend implementing Azure Front Door with Azure Web Application Firewall (WAF). Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
ttps://www.varonis.com/blog/securing-access-azure-webapps

QUESTION 56
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 discovery anomaly detection policies in Microsoft Defender for Cloud Apps
B. adaptive application controls in Defender for Cloud
C. Azure Security Benchmark compliance controls m Defender for Cloud
D. app protection policies in Microsoft Endpoint Manager

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference#compute- recommendations

QUESTION 57
A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription. All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.
The customer plans to deploy Microsoft Sentinel.
You need to recommend configurations to meet the following requirements:
• Ensure that the security operations team can access the security logs and the operation logs.
• Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network. Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Azure Active Directory (Azure AD) Conditional Access policies
B. a custom collector that uses the Log Analytics agent
C. resource-based role-based access control (RBAC)
D. the Azure Monitor agent

Correct Answer: C, D
Section:
Explanation:

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent

QUESTION 58

Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.


Client Browser
Azure App Service Web App
Azure Cosmos DB
Azure Cognitive Search

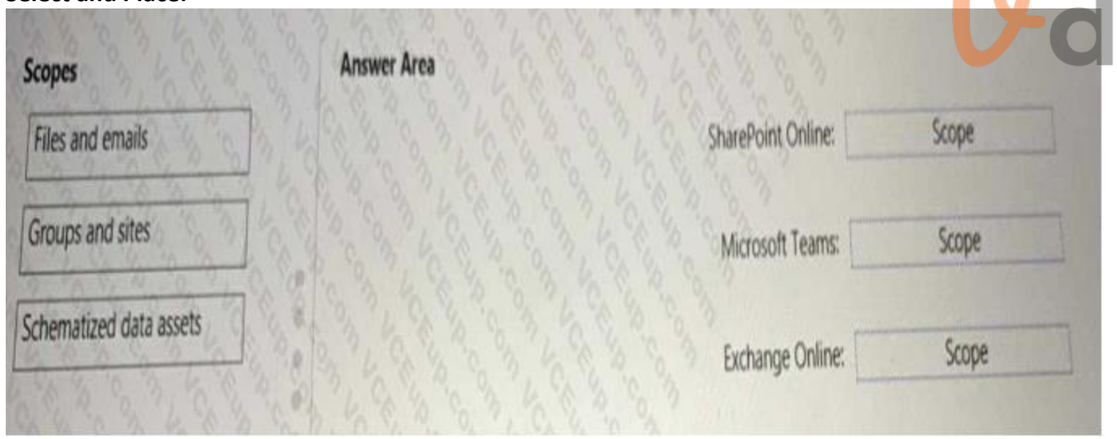
You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model. Solution: You recommend implementing Azure Key Vault to store credentials.

A. Yes
B. No

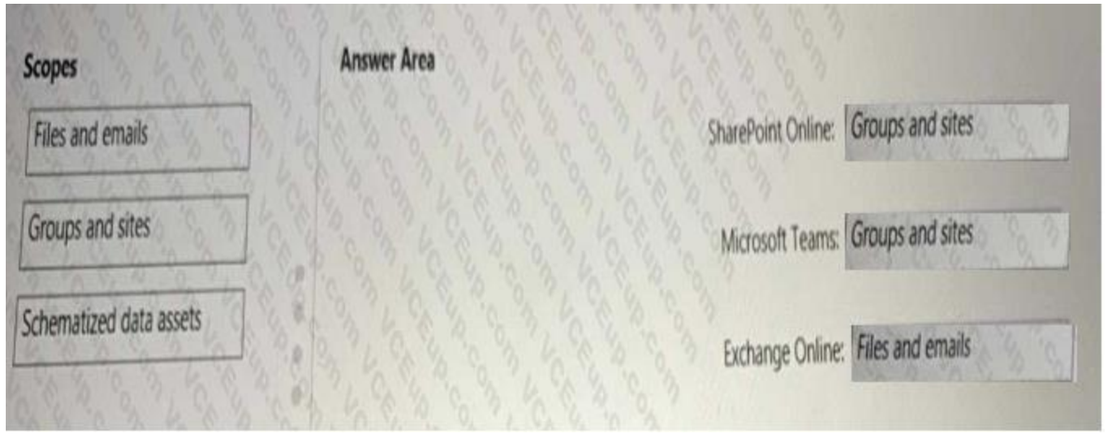
Correct Answer: B
Section:
Explanation:
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

QUESTION 59
DRAG DROP
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.

Select and Place:



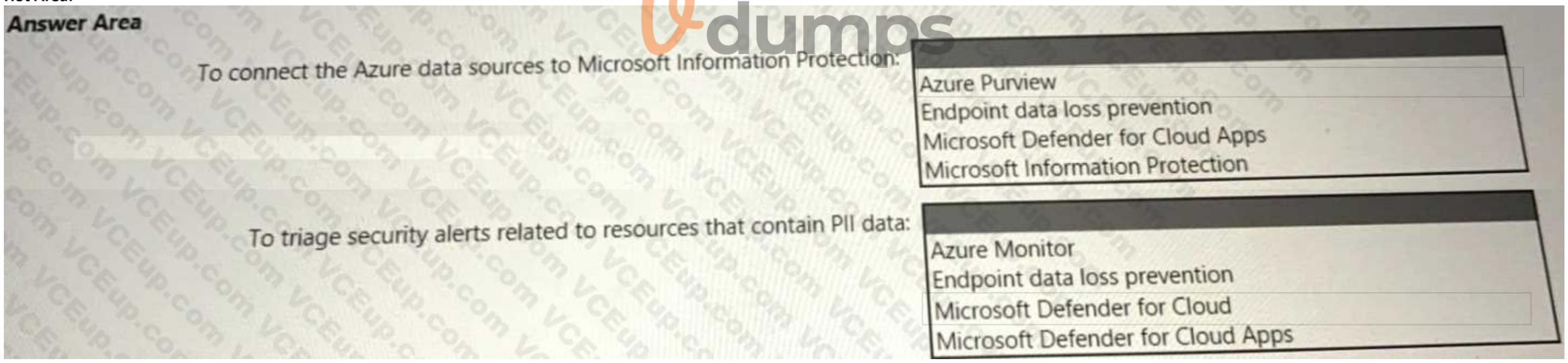
Correct Answer:



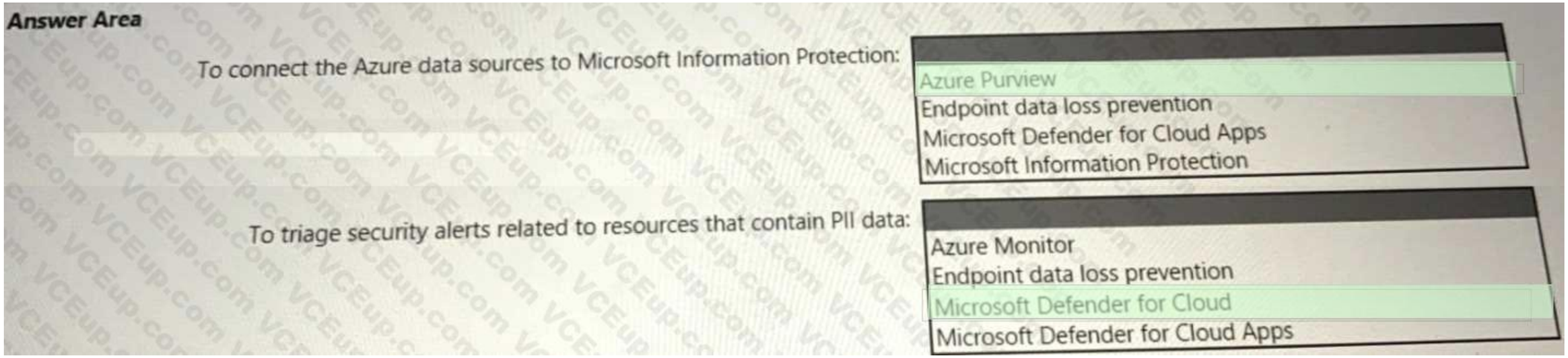
Section:
Explanation:
Box 1: Groups and sites Box 2: Groups and sites Box 3: Files and emails – https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365- worldwide Go to label scopes

QUESTION 60
HOTSPOT
Your company is migrating data to Azure. The data contains Personally Identifiable Information (Pll). The company plans to use Microsoft Information Protection for the Pll data store in Azure. You need to recommend a solution to discover Pll data at risk in the Azure resources. 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:



Section:

Explanation:

Box 1: Azure Purview -

Microsoft Purview is a unified data governance service that helps you manage and govern your on-premises, multi-cloud, and software-as-a-service (SaaS) data. Microsoft Purview allows you to:

Create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Enable data curators to manage and secure your data estate.

Empower data consumers to find valuable, trustworthy data.

Box 2: Microsoft Defender for Cloud

Microsoft Purview provides rich insights into the sensitivity of your data. This makes it valuable to security teams using Microsoft Defender for Cloud to manage the organization's security posture and protect against threats to their workloads. Data resources remain a popular target for malicious actors, making it crucial for security teams to identify, prioritize, and secure sensitive data resources across their cloud environments. The integration with Microsoft Purview expands visibility into the data layer, enabling security teams to prioritize resources that contain sensitive data. References:

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

https://docs.microsoft.com/en-us/azure/purview/how-to-integrate-with-azure-security-products

QUESTION 61

HOTSPOT

Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation. You need to recommend a security posture management solution for the following components:

- Azure loT Edge devices
- AWS EC2 instances

Which services 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 IoT Edge devices:

- Azure Arc
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Defender for IoT

For the AWS EC2 instances:

- Azure Arc only
- Microsoft Defender for Cloud and Azure Arc
- Microsoft Defender for Cloud Apps only
- Microsoft Defender for Cloud only
- Microsoft Defender for Endpoint and Azure Arc
- Microsoft Defender for Endpoint only

Answer Area:

Answer Area

For the IoT Edge devices:

- Azure Arc
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Defender for IoT

For the AWS EC2 instances:

- Azure Arc only
- Microsoft Defender for Cloud and Azure Arc
- Microsoft Defender for Cloud Apps only
- Microsoft Defender for Cloud only
- Microsoft Defender for Endpoint and Azure Arc
- Microsoft Defender for Endpoint only

Section:

Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/architecture
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env- settings https://docs.microsoft.com/en-us/azure/azure-arc/servers/overview#supported-cloud-operations

QUESTION 62
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance.
What should you do first?

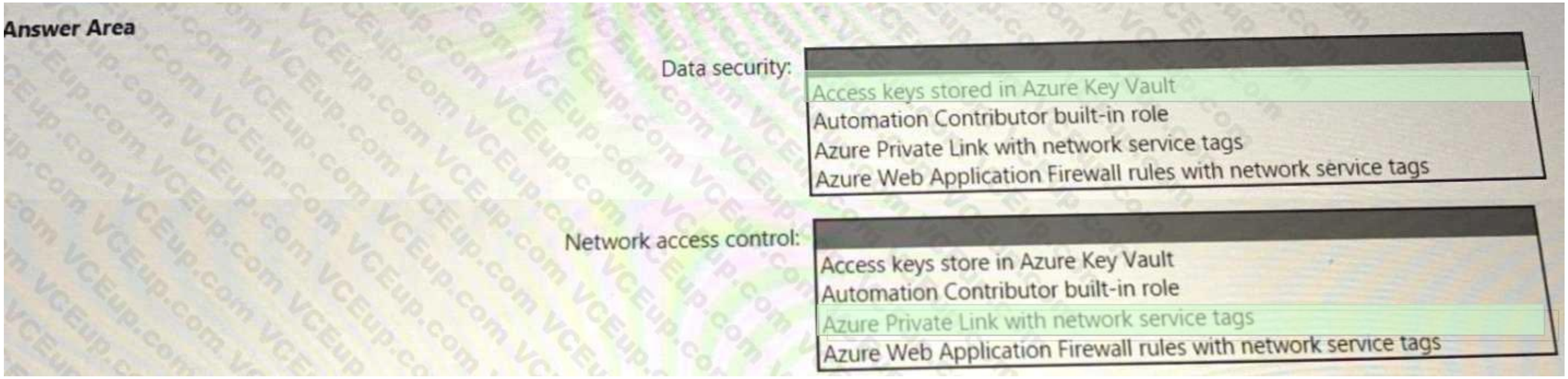
A. From Azure Policy, assign a built-in initiative that has a scope of the subscription.
B. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.
C. From Defender for Cloud, review the Azure security baseline for audit report.
D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

Correct Answer: A
Section:

QUESTION 63
HOTSPOT
You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2. You need to recommend a solution to secure the components of the copy process.
What should you include in the recommendation for each component? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area:



Section:
Explanation:
Data Security : Access Keys stored in Azure Key Vault
Network access control : Azure Private Link with network service tags

QUESTION 64
HOTSPOT
You have a hybrid cloud infrastructure.
You plan to deploy the Azure applications shown in the following table.

Name	Type	Requirement
App1	An Azure App Service web app accessed from Windows 11 devices on the on-premises network	Protect against attacks that use cross-site scripting (XSS).
App2	An Azure App Service web app accessed from mobile devices	Allow users to authenticate to App2 by using their LinkedIn account.

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

App1:

App2:

App1:
Azure AD B2B authentication with Conditional Access
Azure AD B2C custom policies with Conditional Access
Azure Application Gateway Web Application Firewall policies
Azure Firewall
Azure VPN Gateway with network security group rules
Azure VPN Point-to-Site connections

App2:
Azure AD B2B authentication with Conditional Access
Azure AD B2C custom policies with Conditional Access
Azure Application Gateway Web Application Firewall policies
Azure Firewall
Azure VPN Gateway with network security group rules
Azure VPN Point-to-Site connections

Answer Area:

Answer Area

App1:

- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

App2:

- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

Section:
Explanation:

QUESTION 65
HOTSPOT
You are designing an auditing solution for Azure landing zones that will contain the following components:
• SQL audit logs for Azure SQL databases
• Windows Security logs from Azure virtual machines
• Azure App Service audit logs from App Service web apps
You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:
• Log all privileged access.
• Retain logs for at least 365 days.
• Minimize costs.
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.

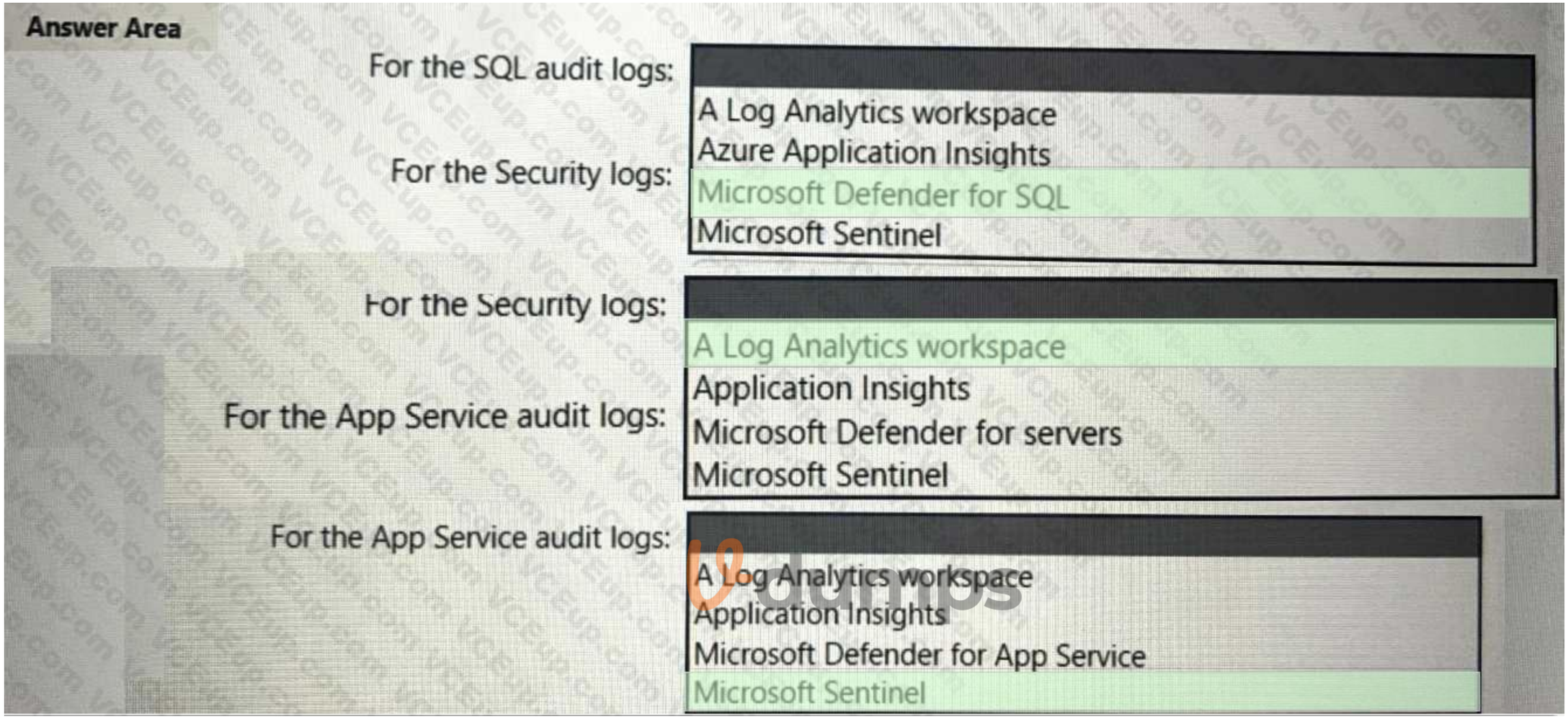
Hot Area:

Answer Area

For the SQL audit logs:	A Log Analytics workspace Azure Application Insights Microsoft Defender for SQL Microsoft Sentinel
For the Security logs:	A Log Analytics workspace Application Insights Microsoft Defender for servers Microsoft Sentinel
For the App Service audit logs:	A Log Analytics workspace Application Insights Microsoft Defender for App Service Microsoft Sentinel

Answer Area:

Answer Area



Section:
Explanation:

QUESTION 66
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?

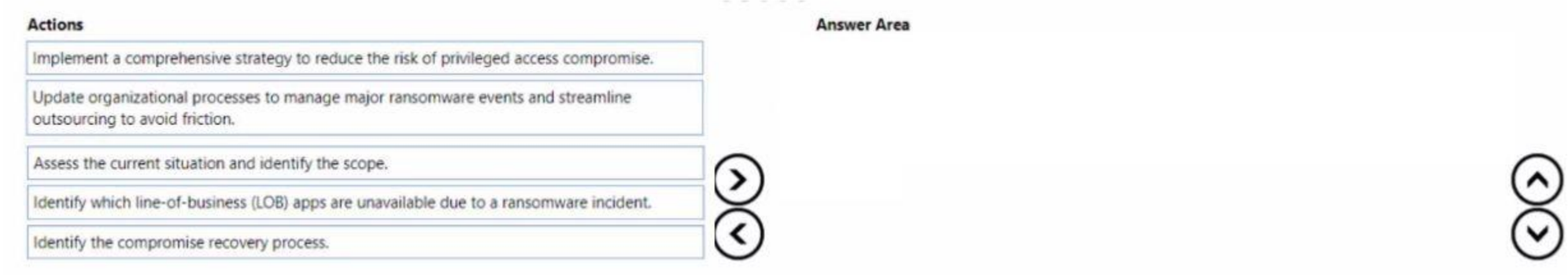
A. an Azure AD user account that has a password stored in Azure Key Vault
B. a group managed service account (gMSA)
C. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management {PIM)
D. a managed identity in Azure

Correct Answer: D
Section:

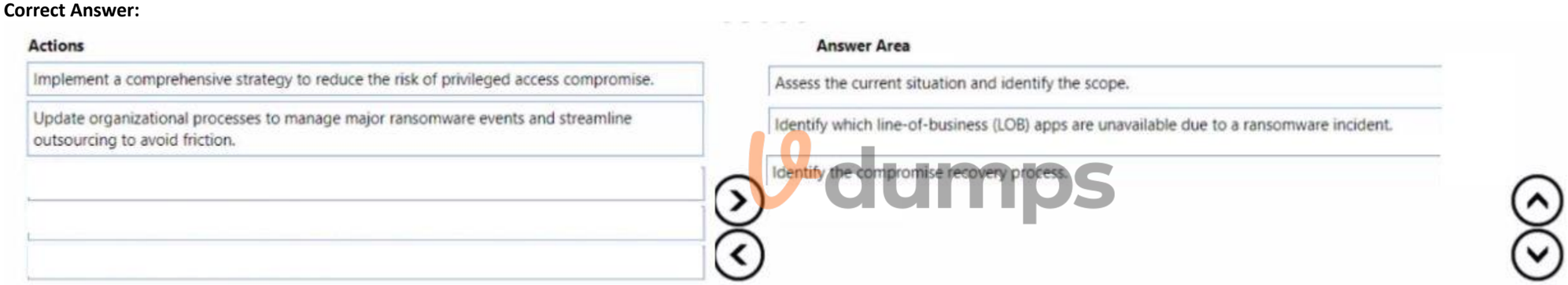
QUESTION 67

DRAG DROP
Your company wants to optimize ransomware incident investigations.
You need to recommend a plan to investigate ransomware incidents based on the Microsoft Detection and Response Team (DART) approach.
Which three actions should you recommend performing in sequence in the plan? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Section:
Explanation:
Assess teh current situation and identity the scope.
Identity which line-of-business (LOB) apps are unavailable due to ransomware incident.
Identity the compromise recovery process.

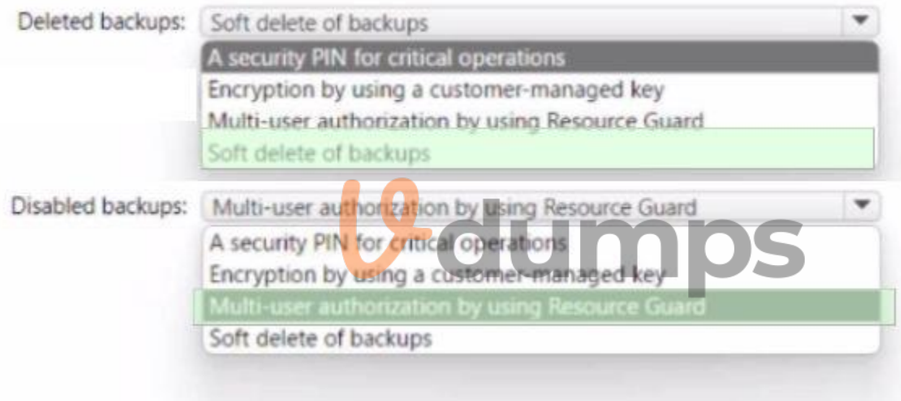
QUESTION 68
HOTSPOT
You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. AJI the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.
You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks:
* A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers
* A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers
What should you use for each risk? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point

Hot Area:

Answer Area

Answer Area:

Answer Area



Section:
Explanation:

QUESTION 69
For of an Azure deployment you are designing a security architecture based on the Microsoft Cloud Security Benchmark. You need to recommend a best practice for implementing service accounts for Azure API management What should you include in the recommendation?

A. device registrations in Azure AD
B. application registrations m Azure AD
C. Azure service principals with certificate credentials
D. Azure service principals with usernames and passwords
E. managed identities in Azure

Correct Answer: E
Section:

QUESTION 70
HOTSPOT

You have a Microsoft 365 subscription that is protected by using Microsoft 365 Defender
You are designing a security operations strategy that will use Microsoft Sentinel to monitor events from Microsoft 365 and Microsoft 365 Defender
You need to recommend a solution to meet the following requirements:
* Integrate Microsoft Sentinel with a third-party security vendor to access information about known malware
* Automatically generate incidents when the IP address of a command-and control server is detected in the events
What should you configure in Microsoft Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area:

Section:
Explanation:

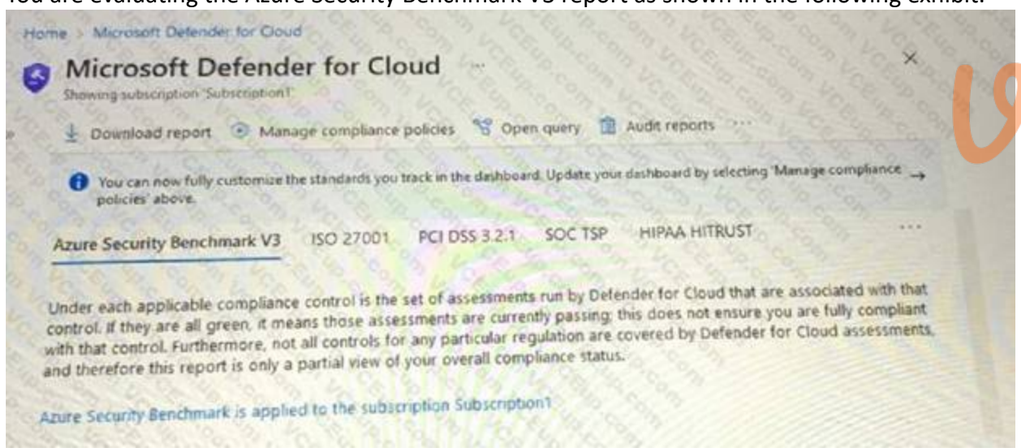
QUESTION 71
Your company has a Microsoft 365 E5 subscription.
The Chief Compliance Officer plans to enhance privacy management in the working environment.

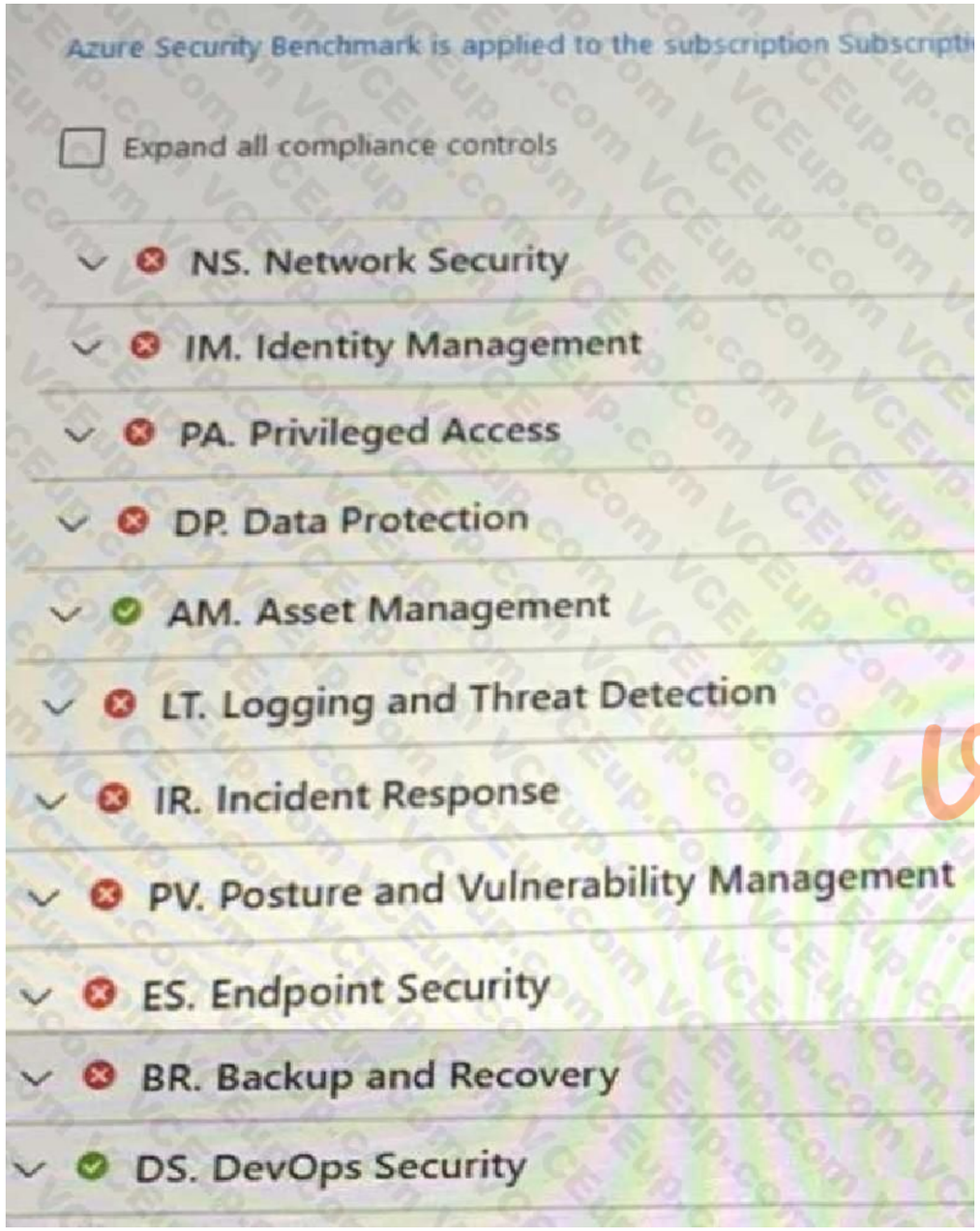
You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:
• Identify unused personal data and empower users to make smart data handling decisions.
• Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.
• Provide users with recommendations to mitigate privacy risks.
What should you include in the recommendation?

A. Microsoft Viva Insights
B. Advanced eDiscovery
C. Privacy Risk Management in Microsoft Priva
D. communication compliance in insider risk management

Correct Answer: C
Section:
Explanation:
Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you: Detect overexposed personal data so that users can secure it.Spot and limit transfers of personal data across departments or regional borders.Help users identify and reduce the amount of unused personal data that you store.https://www.microsoft.com/en-us/security/business/privacy/microsoft-priva-risk-management

QUESTION 72
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report as shown in the following exhibit.





You need to verify whether Microsoft Defender for servers is installed on all the virtual machines that run Windows. Which compliance control should you evaluate?

A. Data Protection
B. Incident Response
C. Posture and Vulnerability Management
D. Asset Management
E. Endpoint Security

Correct Answer: E

Section:

QUESTION 73
A customer is deploying Docker images to 10 Azure Kubernetes Service (AKS) resources across four Azure subscriptions. You are evaluating the security posture of the customer. You discover that the AKS resources are excluded from the secure score recommendations. You need to produce accurate recommendations and update the secure score. Which two actions should you recommend in Microsoft Defender for Cloud? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Configure auto provisioning.
B. Assign regulatory compliance policies.
C. Review the inventory.
D. Add a workflow automation.
E. Enable Defender plans.

Correct Answer: A, E
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance- packages https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

QUESTION 74
You have Microsoft Defender for Cloud assigned to Azure management groups.
You have a Microsoft Sentinel deployment.
During the triage of alerts, you require additional information about the security events, including suggestions for remediation. Which two components can you use to achieve the goal? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. workload protections in Defender for Cloud
B. threat intelligence reports in Defender for Cloud
C. Microsoft Sentinel notebooks
D. Microsoft Sentinel threat intelligence workbooks

Correct Answer: B, D
Section:
Explanation:
A: Workbooks provide insights about your threat intelligence
Workbooks provide powerful interactive dashboards that give you insights into all aspects of Microsoft Sentinel, and threat intelligence is no exception. You can use the built-in Threat Intelligence workbook to visualize key information about your threat intelligence, and you can easily customize the workbook according to your business needs. You can even create new dashboards combining many different data sources so you can visualize your data in unique ways. Since Microsoft Sentinel workbooks are based on Azure Monitor workbooks, there is already extensive documentation available, and many more templates. C: What is a threat intelligence report?
Defender for Cloud's threat protection works by monitoring security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to identify threats.
Defender for Cloud has three types of threat reports, which can vary according to the attack. The reports available are:
Activity Group Report: provides deep dives into attackers, their objectives, and tactics.
Campaign Report: focuses on details of specific attack campaigns.
Threat Summary Report: covers all of the items in the previous two reports.
This type of information is useful during the incident response process, where there's an ongoing investigation to understand the source of the attack, the attacker's motivations, and what to do to mitigate this issue in the future. Incorrect:
Not B: When to use Jupyter notebooks
While many common tasks can be carried out in the portal, Jupyter extends the scope of what you can do with this data. For example, use notebooks to:
Perform analytics that aren't provided out-of-the box in Microsoft Sentinel, such as some Python machine learning features Create data visualizations that aren't provided out-of-the box in Microsoft Sentinel, such as custom timelines and process trees Integrate data sources outside of Microsoft Sentinel, such as an on-premises data set.

Not D: Defender for Cloud offers security alerts that are powered by Microsoft Threat Intelligence. It also includes a range of advanced, intelligent, protections for your workloads. The workload protections are provided through Microsoft Defender plans specific to the types of resources in your subscriptions. For example, you can enable Microsoft Defender for Storage to get alerted about suspicious activities related to your Azure Storage accounts.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports https://docs.microsoft.com/en-us/azure/sentinel/notebooks

QUESTION 75
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. Azure Active Directory (Azure AD) Conditional Access App Control policies
B. OAuth app policies in Microsoft Defender for Cloud Apps
C. app protection policies in Microsoft Endpoint Manager
D. application control policies in Microsoft Defender for Endpoint

Correct Answer: D
Section:
Explanation:
<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender- application-control/select-types-of-rules-to-create#windows-defender-application-control-policy>- rules

QUESTION 76
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud. The company signs a contract with the United States government. You need to review the current subscription for NIST 800-53 compliance. What should you do first?

A. From Defender for Cloud, review the Azure security baseline for audit report.
B. From Defender for Cloud, add a regulatory compliance standard.
C. From Defender for Cloud, enable Defender for Cloud plans.
D. From Defender for Cloud, review the secure score recommendations.

Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance- packages#what-regulatory-compliance-standards-are-available-in-defender-for-cloud

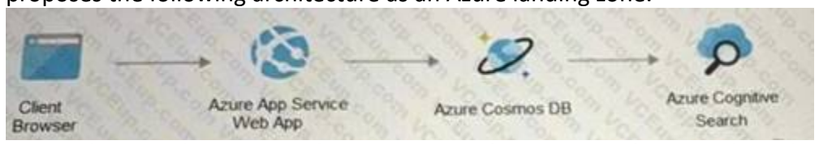
QUESTION 77
You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload protections dashboard. You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution 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
Section:

Explanation:
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 78
Your on-premises network contains an e-commerce web app that was developed in Angular and Node.js. The web app uses a MongoDB database You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model. Solution: You recommend implementing Azure Application Gateway with Azure Web Application Firewall (WAF). Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

QUESTION 79
You need to recommend a strategy for routing internet-bound traffic from the landing zones. The solution must meet the landing zone requirements. What should you recommend as part of the landing zone deployment?

A. service chaining
B. local network gateways
C. forced tunneling
D. a VNet-to-VNet connection

Correct Answer: A
Section:

QUESTION 80
You have an Azure subscription that contains a Microsoft Sentinel workspace.
Your on-premises network contains firewalls that support forwarding event logs m the Common Event Format (CEF). There is no built-in Microsoft Sentinel connector for the firewalls
You need to recommend a solution to ingest events from the firewalls into Microsoft Sentinel.
What should you include m the recommendation?

A. an Azure logic app
B. an on-premises Syslog server
C. an on-premises data gateway
D. Azure Data Factory

Correct Answer: B
Section:

QUESTION 81
You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AO credentials. You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials. What should you include in the recommendation?

A. an Azure AD enterprise application
B. a retying party trust in Active Directory Federation Services (AD FS)
C. Azure AD Application Proxy
D. Azure AD B2C

Correct Answer: A
Section:

QUESTION 82
You are designing a ransomware response plan that follows Microsoft Security Best Practices.
You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files.
What should you include in the recommendation?

A. Microsoft Defender for Endpoint
B. Windows Defender Device Guard
C. protected folders
D. Azure Files
E. BitLocker Drive Encryption (BitLocker)

Correct Answer: C
Section:
Explanation:

QUESTION 83
Your company has the virtual machine infrastructure shown in the following table.

Operation system	Location	Number of virtual machines	Hypervisor
Linux	On-premises	100	VMWare vSphere
Windows Server	On-premises	100	Hyper-V

The company plans to use Microsoft Azure Backup Server (MABS) to back up the virtual machines to Azure. You need to provide recommendations to increase the resiliency of the backup strategy to mitigate attacks such as ransomware. What should you include in the recommendation?

A. Use geo-redundant storage (GRS).
B. Use customer-managed keys (CMKs) for encryption.
C. Require PINs to disable backups.
D. Implement Azure Site Recovery replication.

Correct Answer: C
Section:

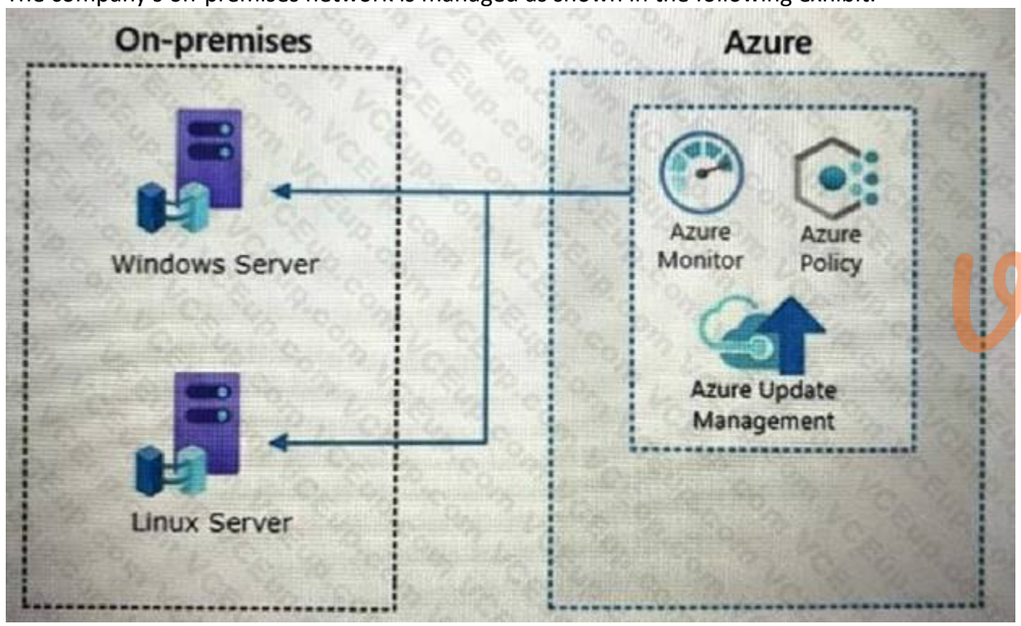
QUESTION 84
You have a customer that has a Microsoft 365 subscription and an Azure subscription.

The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure. You need to design a security solution to assess whether all the devices meet the customer's compliance rules. What should you include in the solution?

A. Microsoft Information Protection
B. Microsoft Defender for Endpoint
C. Microsoft Sentinel
D. Microsoft Endpoint Manager

Correct Answer: D
Section:

QUESTION 85
Your company has a hybrid cloud infrastructure.
Data and applications are moved regularly between cloud environments.
The company's on-premises network is managed as shown in the following exhibit.



You are designing security operations to support the hybrid cloud infrastructure. The solution must meet the following requirements: Govern virtual machines and servers across multiple environments.Enforce standards for all the resources across all the environment across the Azure policy.Which two components should you recommend for the on-premises network? Each correct answer presents part of the solution.

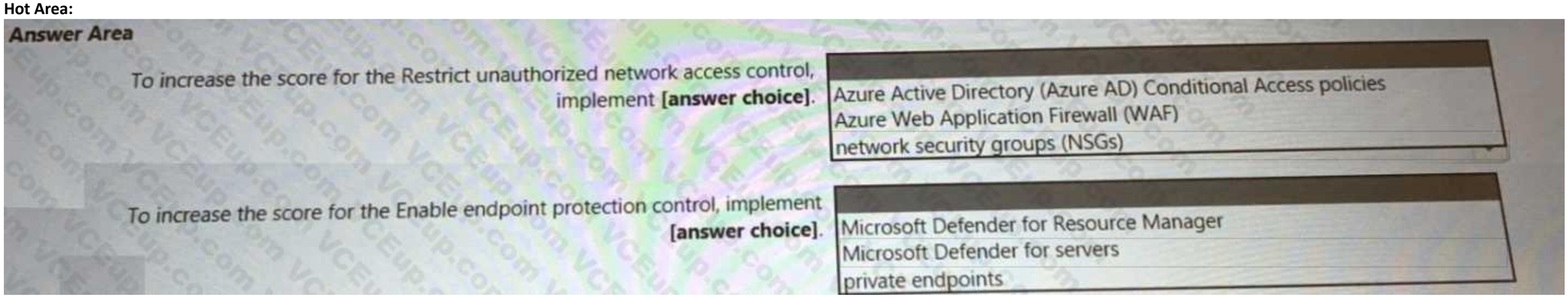
A. Azure VPN Gateway
B. guest configuration in Azure Policy
C. on-premises data gateway
D. Azure Bastion
E. Azure Arc

Correct Answer: B, E
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/governance/machine-configuration/overview

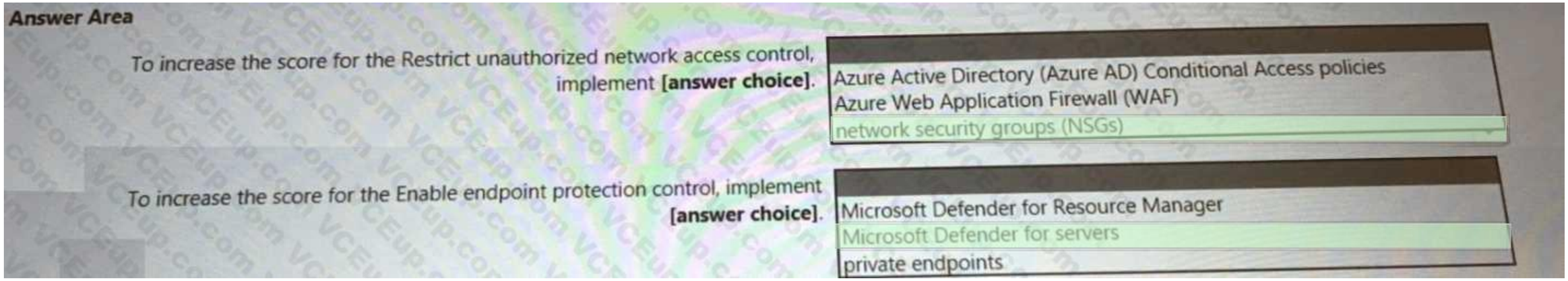
QUESTION 86
HOTSPOT
You open Microsoft Defender for Cloud as shown in the following exhibit.

Use the drop-down menus to select the answer choice that complete each statements based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

Selection 1: NSG

https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/security-control-restrict-unauthorized-network-access/ba-p/1593833 Selection 2: Microsoft Defender for servers

Enable endpoint protection - Defender for Cloud checks your organization's endpoints for active threat detection and response solutions such as Microsoft Defender for Endpoint or any of the major solutions shown in this list.

When an Endpoint Detection and Response (EDR) solution isn't found, you can use these recommendations to deploy Microsoft Defender for Endpoint (included as part of Microsoft Defender for servers). Incorrect:

Not Microsoft Defender for Resource Manager:

Microsoft Defender for Resource Manager does not handle endpoint protection.

Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they're performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Defender for Cloud runs advanced security analytics to detect threats and alerts you about suspicious activity.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

QUESTION 87

HOTSPOT

You have a Microsoft 365 E5 subscription and an Azure subscripts You need to evaluate the existing environment to increase the overall security posture for the following components:

- Windows 11 devices managed by Microsoft Intune
- Azure Storage accounts
- Azure virtual machines

What should you use to evaluate the components? To answer, select the appropriate options in the answer area.

Hot Area:

Answer Area

Windows 11 devices:

- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

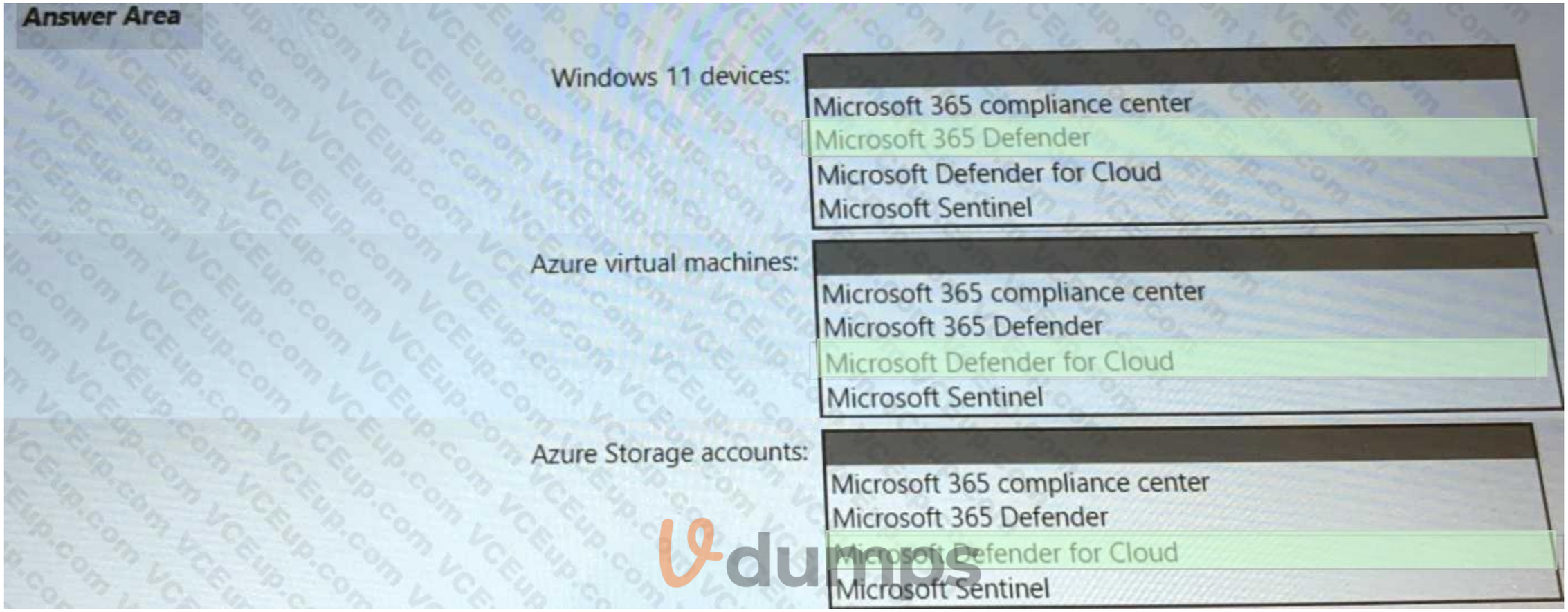
Azure virtual machines:

- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Azure Storage accounts:

- Microsoft 365 compliance center
- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Sentinel

Answer Area:



Section:

Explanation:

Selection 1: Microsoft 365 Defender (Microsoft Defender for Endpoint is part of it).

Selection 2: Microsoft Defender for Cloud.

Selection 3: Microsoft Defender for Cloud.https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas- services/8-specify-security-requirements-for-storage-workloads

QUESTION 88

HOTSPOT

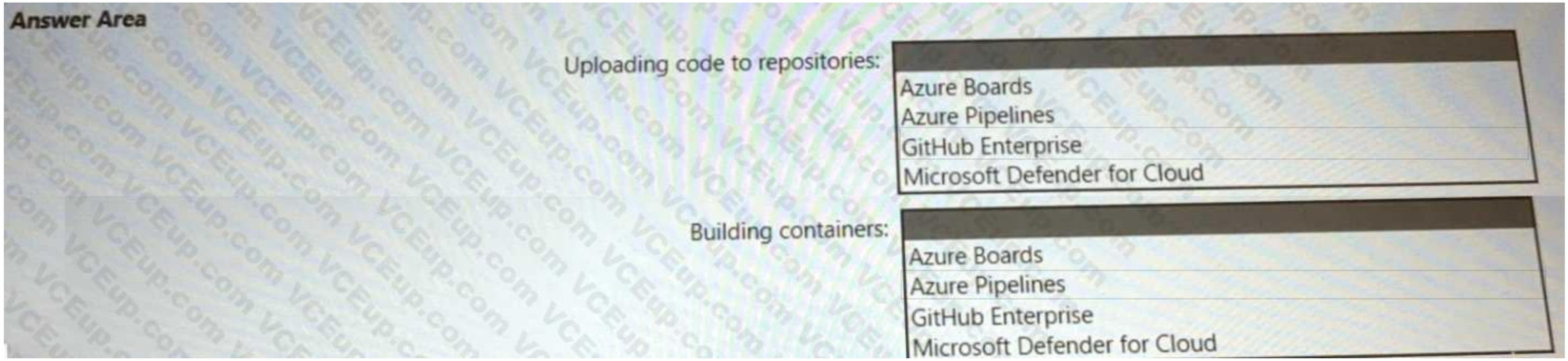
Your company has an Azure App Service plan that is used to deploy containerized web apps. You are designing a secure DevOps strategy for deploying the web apps to the App Service plan. You need to recommend a strategy to integrate code scanning tools into a secure software development lifecycle.

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.

Hot Area:



Answer Area:

Section:

Explanation:

https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about- github-advanced-security https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific- samples/azdo-container-dev-test-release/

QUESTION 89

HOTSPOT

You are creating the security recommendations for an Azure App Service web app named App1.

App1 has the following specifications:

- Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
- Users will authenticate by using Azure Active Directory (Azure AD) user accounts.

You need to recommend an access security architecture for App1.

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.

Hot Area:

To enable Azure AD authentication for App1, use:

Azure AD application
Azure AD Application Proxy
Azure Application Gateway
A managed identity in Azure AD
Microsoft Defender for App

To implement access requests for App1, use:

An access package in Identity Governance
An access policy in Microsoft Defender for Cloud Apps
An access review in Identity Governance
Azure AD Conditional Access App Control
An OAuth app policy in Microsoft Defender for Cloud Apps

Answer Area:

To enable Azure AD authentication for App1, use:

Azure AD application
Azure AD Application Proxy
Azure Application Gateway
A managed identity in Azure AD
Microsoft Defender for App

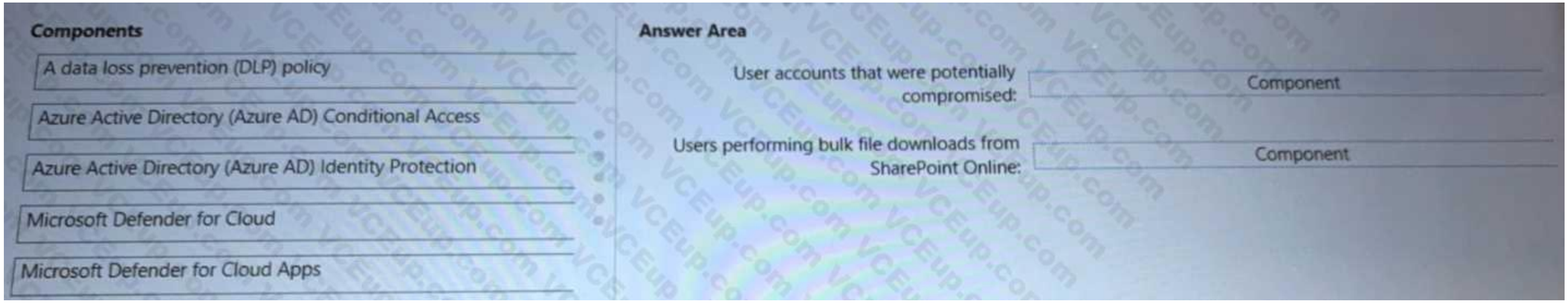
To implement access requests for App1, use:

An access package in Identity Governance
An access policy in Microsoft Defender for Cloud Apps
An access review in Identity Governance
Azure AD Conditional Access App Control
An OAuth app policy in Microsoft Defender for Cloud Apps

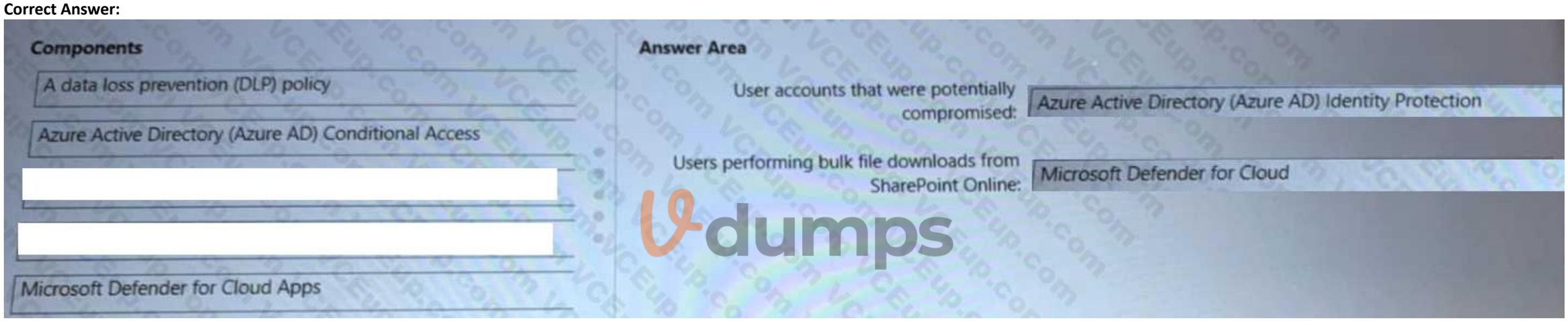
Section:
Explanation:
Azure AD application
(https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management) An access package in identity governance
(https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create)

QUESTION 90
DRAG DROP
You have a Microsoft 365 subscription
You need to recommend a security solution to monitor the following activities:
• User accounts that were potentially compromised
• 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:



Correct Answer:



Section:
Explanation:
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 91
You have a Microsoft 365 subscription.
You need to design a solution to block file downloads from Microsoft SharePoint Online by authenticated users on unmanaged devices.
Which two services should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Cloud Apps
B. Azure AD Application Proxy
C. Azure Data Catalog
D. Azure AD Conditional Access
E. Microsoft Purview Information Protection

Correct Answer: A, D
Section:

QUESTION 92
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. regulatory compliance standards in Microsoft Defender for Cloud
B. custom Azure roles
C. Azure Policy assignments
D. Azure management groups

Correct Answer: C
Section:

QUESTION 93
You have a Microsoft 365 tenant.
Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant. You need to design a security strategy to meet the following requirements:
* Users must be able to request access to App1 by using a self-service request.
* When users request access to App1, they must be prompted to provide additional information about their request.
* Every three months, managers must verify that the users still require access to Appl.
What should you include in the design?

A. Azure AD Application Proxy
B. connected apps in Microsoft Defender for Cloud Apps
C. Microsoft Entra Identity Governance
D. access policies in Microsoft Defender for Cloud Apps

Correct Answer: C
Section:

QUESTION 94
DRAG DROP
You have a hybrid Azure AD tenant that has pass-through authentication enabled.
You are designing an identity security strategy.
You need to minimize the impact of brute force password attacks and leaked credentials of hybrid identities.
What should you include in the design? To answer, drag the appropriate features to the correct requirements. Each feature 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:

Features

Azure AD Password Protection

Extranet Smart Lockout (ESL)

Password hash synchronization

Answer Area

For brute force password attacks:

For leaked credentials:

Correct Answer:

Features

Password hash synchronization

Answer Area

For brute force password attacks: Azure AD Password Protection

For leaked credentials: Extranet Smart Lockout (ESL)

Section:

Explanation:

QUESTION 95

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online.

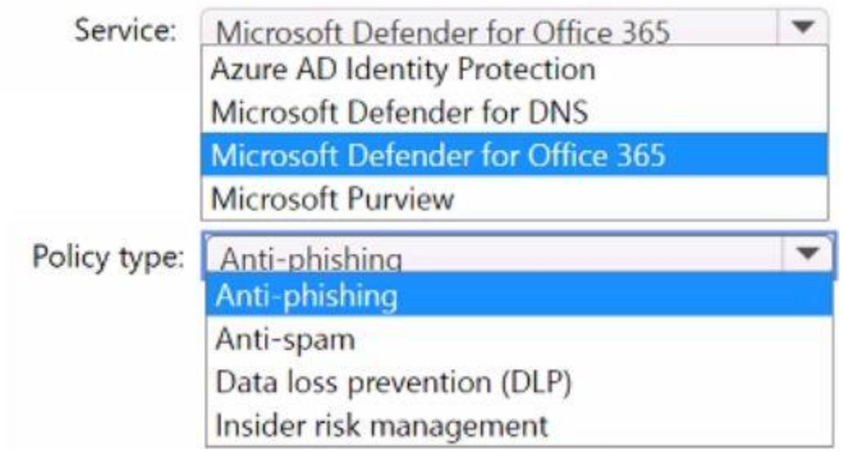
You need to recommend a solution to prevent malicious actors from impersonating the email addresses of internal senders.

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.

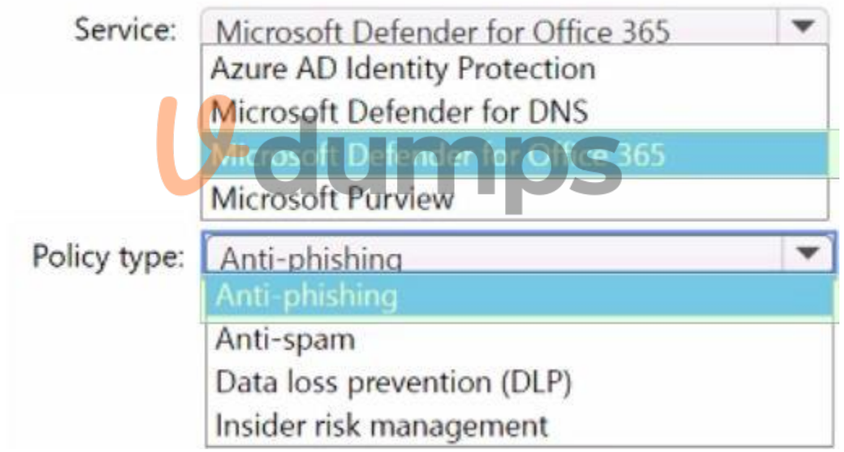
Hot Area:

Answer Area



Answer Area:

Answer Area



Section:
Explanation: