[June-2023Braindump2go SC-900 PDF and VCE Dumps SC-900 152Q Free Offered[Q55-Q110

June/2023 Latest Braindump2go SC-900 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindump2go SC-900 Real Exam Questions!QUESTION 55You are considering the use of sensitivity labels in Microsoft 365. Can sensitivity labels can be used to encrypt the contents in documents?A.   YesB.   NoAnswer: AExplanation:When you apply a ?Confidential? label to a document, the label will encrypt the content in the document.Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwideQUESTION 56You are planning on making use of the Azure Bastion service. Can you use the Azure Bastion service to restrict traffic from the Internet onto an Azure virtual machine?A.   YesB.   NoAnswer: BExplanation:You cannot use the Azure Bastion service to restrict traffic into an Azure virtual machine. For this you will need to use Network Security groups. The Azure Bastion service is used to RDP/SSH into an Azure virtual machine via the Azure portal and the browser.Reference: https://docs.microsoft.com/en-us/azure/bastion/bastion-overviewQUESTION 57You are looking at the capabilities of Azure Active Directory. Can you use Azure Active Directory to manage device registrations in Azure Active Directory?A.   YesB.   NoAnswer: AExplanation:https://docs.microsoft.com/en-us/azure/active-directory/devices/overviewQUESTION 58Your company is planning on using Azure Cloud services. Which of the following can be used to ensure that data can be read only by authorized users?A.   EncryptionB.   DeduplicationC.   ArchivingD.   CompressionAnswer: AExplanation:You can ensure data is encrypted. Then only authorized users would have the encryption key. The encryption key can then be used to decrypt and read the data.Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-the-microsoft-cloud-overview?view=o365-worldwideQUESTION 59Your company is planning on using Azure Active Directory for the storage of identities. They want to make use of the self-service password reset feature.Which of the following authentication methods are available for self-service password reset? Choose 3 answers from the options given belowA.   EmailB.   A passport identification numberC.   A picture messageD.   Mobile app notificationE.   Mobile app codeAnswer: ADEExplanation:Below are the authentication methods available for self-service password reset: Mobile app notification Mobile app code Email  Mobile phone Office phone Security questions Reference:https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworksQUESTION 60Your company wants to start making use of Azure. They are looking at different security aspects when it comes to using Azure. Which of the following could be used for the following requirement?- Enforce Multi-Factor authentication based on the sign-in riskA.   Azure AD Identity ManagementB.   Azure Conditional AccessC.   Azure AD RolesD.   Azure AD ConnectAnswer: AExplanation:In Azure AD Identity Protection, you can configure the Sign-in risk policy to allow access and enforce the use of Multi-Factor Authentication.

Reference:https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protectionQUESTION 61 Which of the following is a scalable, cloud-native, security information event management and security orchestration automated response solution?A.   Azure SentinelB.   Azure Security CenterC.   Azure Active DirectoryD.   Azure AD Identity ProtectionAnswer: AExplanation:You can use Azure Sentinel as a scalable, cloud-native, security information event management and security orchestration automated response solution. Azure Sentinel has the capability to ingest data from a variety of sources and performance threat monitoring on that data.Reference:https://docs.microsoft.com/en-us/azure/sentinel/overviewQUESTION 62 Which of the following provides advanced and intelligent protection of Azure and hybrid resources and workloads?A.   Azure DefenderB.   Azure PoliciesC.   Azure BlueprintsD.   Azure Active DirectoryAnswer: AExplanation:With Azure Defender , you can enable intelligent protection of your resources that are defined in Azure and also in your on-premises infrastructure.This is an additional security feature that comes as part of Azure Security Center as shown below
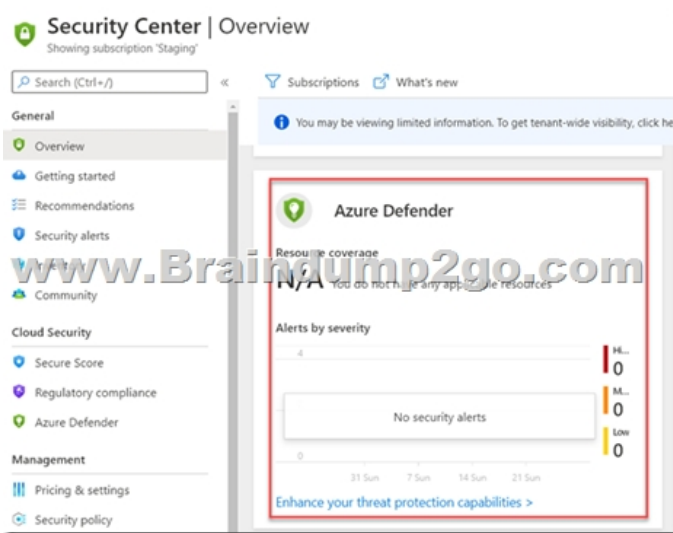
Reference:https://docs.microsoft.com/en-us/azure/security-center/azure-defenderQUESTION 63Which of the following is available for the Azure Application Gateway service that helps to protect web applications from common exploits and vulnerabilities?A.   Azure FirewallB.   Azure Web Application FirewallC.   Azure PolicyD.   Azure Identity ProtectionAnswer: BExplanation:The Azure Web Application Firewall can be used along with the Azure Application Gateway resource to protect web applications from common exploits and vulnerabilities. It can help to protect against attacks such as SQL injection attacks or cross-site scripting attacks.Reference:https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overviewQUESTION 64You are evaluating the different services available in Azure when it comes to security. Which of the following can be accomplished with the use of the Azure Privileged Identity Managed service?A.   Filter traffic to Azure virtual machinesB.   Enable Multi-Factor Authentication for users based on detected sign-in risksC.   Provide just-in-time access to resource roles in AzureD.   Measure the security posture of resources defined in an Azure environmentAnswer: CExplanation:With Azure Privileged Identity Managed , you can provide just-in-time access to Azure AD roles and resource roles. Here users can request for access whenever required. And the access can be granted or denied accordingly.Reference: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configureQUESTION 65You are evaluating the different discovery tools that are available with Microsoft 365. You need to map the tool that can be used for desired requirement below:- Be able to quickly find email in Exchange mailboxesWhich of the following would you use for this requirement?A.   Core eDiscoveryB.   Advanced eDiscoveryC.   Sensitivity labelsD.   Content searchAnswer: DExplanation:The Content search tool can be used to quickly find email in Exchange mailboxes, documents in SharePoint sites and OneDrive locations.Reference:https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-content?view=o365-worldwide QUESTION 66You are evaluating the different discovery tools that are available with Microsoft 365. You need to map the tool that can be used for desired requirement below:- Provide basic capabilities on searching and exporting of content in Microsoft 365Which of the following would you use for this requirement?A.   Core eDiscoveryB.   Privileged Access ManagementC.   Sensitivity labels D.   Content searchAnswer: AExplanation:The Core eDiscovery tool helps you to find and export content in Microsoft 365 and Office 365. You can also use the tool to place an eDiscovery hold on certain content locations.Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwideQUESTION 67In the Microsoft Cloud Adoption Framework for Azure, which two phases are addressed before the Ready phase? Each correct answer presents a complete solution.NOTE: Each correct selection is worth one point.A.   PlanB.   ManageC.   AdoptD.   GovernE. Define StrategyAnswer: AEExplanation:cloud adoption framework: strategy, plan, ready, adopt, govern, manage. https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overviewQUESTION 68What is an example of encryption at rest?A.   encrypting communications by using a site-to-site VPNB.   encrypting a virtual machine diskC.   accessing a website by using an encrypted HTTPS connectionD.   sending an encrypted emailAnswer: BExplanation:Platform as a Service (PaaS) customer's data typically resides in a storage service such as Blob Storage but may also be cached or stored in the application execution environment, such as a virtual machine. To see the encryption at rest options available to you, examine the Data encryption models: supporting services table for the storage and application platforms that you use.QUESTION 69Which Microsoft 365 feature can you use to restrict communication and the sharing of information between members of two departments at your

organization?A. sensitivity label policiesB. Customer LockboxC. information barriersD. Privileged Access Management (PAM)Answer: CExplanation:Information barriers (IBs) are policies that an admin can configure to prevent individuals or groups from communicating with each other. IBs are useful if, for example, one department is handling information that shouldn't be shared with other departments.https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriersQUESTION 70Which three authentication methods does Windows Hello for Business support? Each correct answer presents a complete solution.NOTE: Each correct selection is worth one point.A. fingerprintB. facial recognitionC. PIND. email verificationE. security questionAnswer: ABCExplanation:Windows Hello in Windows 10 enables users to sign in to their device using a PIN. Windows Hello lets your employees use fingerprint or facial recognition as an alternative method to unlocking a device. With Windows Hello, authentication happens when the employee provides his or her unique biometric identifier while accessing the device-specific Windows Hello credentials.

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterpriseQUESTION 71What feature in Microsoft Defender for Endpoint provides the first line of defense against cyberthreats by reducing the attack surface?A. automated remediationB. automated investigationC. advanced huntingD. network protectionAnswer: D Explanation:Network protection helps protect devices from Internet-based events. Network protection is an attack surface reduction capability.Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?view=o365-worldwideQUESTION 72Which two types of resources can be protected by using Azure Firewall? Each correct answer presents a complete solution.NOTE: Each correct selection is worth one point.A. Azure virtual machinesB. Azure Active Directory (Azure AD) usersC. Microsoft Exchange Online inboxesD. Azure virtual networksE. Microsoft SharePoint Online sitesAnswer: ADExplanation:Firewall is really not directly protecting the Virtual Networks though DDOS would have been ideal for VNETS. https://docs.microsoft.com/en-us/azure/firewall/overviewQUESTION 73You plan to implement a security strategy and place multiple layers of defense throughout a network infrastructure.Which security methodology does this represent?A. threat modeling B. identity as the security perimeterC. defense in depthD. the shared responsibility modelAnswer: CExplanation:Data, Application, Compute, Network, Perimeter, Identity and Access and Physical. Of this physical is more of cloud provider responsibility.https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/2-what-is-defense-in-depth QUESTION 74What can you use to scan email attachments and forward the attachments to recipients only if the attachments are free from malware?A. Microsoft Defender for Office 365B. Microsoft Defender AntivirusC. Microsoft Defender for IdentityD. Microsoft Defender for EndpointAnswer: AExplanation:

https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description QUESTION 75Which feature provides the extended detection and response (XDR) capability of Azure Sentinel?A. integration with the Microsoft 365 compliance centerB. support for threat huntingC. integration with Microsoft 365 DefenderD. support for Azure Monitor WorkbooksAnswer: CExplanation:The Microsoft 365 Defender connector for Azure Sentinel (preview) sends all Microsoft 365 Defender incidents and alerts information to Azure Sentinel and keeps the incidents synchronized.Once you add the connector, Microsoft 365 Defender incidents - which include all associated alerts, entities, and relevant information received from Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Office 365, and Microsoft Cloud App Security?are streamed to Azure Sentinel as security information and event management (SIEM) data, providing you with context to perform triage and incident response with Azure Sentinel.Once in Azure Sentinel, incidents remain bi-directionally synchronized with Microsoft 365 Defender, allowing you to take advantage of the benefits of both the Microsoft 365 Defender portal and Azure Sentinel in the Azure portal for incident investigation and response.

https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender-integration-with-azure-sentinel?view=o365-worldwideQUESTION 76What can you use to provide threat detection for Azure SQL Managed Instance?A. Microsoft Secure ScoreB. application security groupsC. Azure DefenderD. Azure BastionAnswer: CExplanation:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introductionQUESTION 77Which Azure Active Directory (Azure AD) feature can you use to restrict Microsoft Intune-managed devices from accessing corporate resources?A. network security groups (NSGs)B. Azure AD Privileged Identity Management (PIM)C. conditional access policiesD. resource locksAnswer: CQUESTION 78Which Microsoft 365 feature can you use to restrict users from sending email messages that contain lists of customers and their associated credit card numbers?A. retention policiesB. data loss prevention (DLP) policiesC. conditional access policiesD. information barriersAnswer: BExplanation:

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwideQUESTION 79In a Core

eDiscovery workflow, what should you do before you can search for content?A.   Create an eDiscovery hold.B.   Run Express Analysis.C.   Configure attorney-client privilege detection.D.   Export and download results.Answer: AExplanation: https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwideQUESTION 80 Which Microsoft portal provides information about how Microsoft manages privacy, compliance, and security?A.   Microsoft Service Trust PortalB.   Compliance ManagerC.   Microsoft 365 compliance centerD.   Microsoft SupportAnswer: AExplanation: The Microsoft Service Trust Portal provides a variety of content, tools, and other resources about Microsoft security, privacy, and compliance practices.

https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwideQUESTION 81What can you protect by using the information protection solution in the Microsoft 365 compliance center?A.   computers from zero-day exploitsB.   users from phishing attemptsC.   files from malware and virusesD.   sensitive data from being exposed to unauthorized usersAnswer: DExplanation:

https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwideQUESTION 82What can you specify in Microsoft 365 sensitivity labels?A.   how long files must be preservedB.   when to archive an email messageC. which watermark to add to filesD.   where to store filesAnswer: CExplanation:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwideQUESTION 102You have an Azure subscription.You need to implement approval-based, time-bound role activation.What should you use?A.   Windows Hello for BusinessB.   Azure Active Directory (Azure AD) Identity ProtectionC.   access reviews in Azure Active Directory (Azure AD) D.   Azure Active Directory (Azure AD) Privileged Identity Management (PIM)Answer: DExplanation:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configureQUESTION 103Hotspot QuestionFor each of the following statements, select Yes if the statement is true. Otherwise, select No.NOTE: Each correct selection is worth one point.

Answer:

 Explanation:https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfaQUESTION 104When security defaults are enabled for an Azure Active Directory (Azure AD) tenant, which two requirements are enforced? Each correct answer presents a complete solution.NOTE: Each correct selection is worth one point.A.   All users must authenticate from a registered device.B.   Administrators must always use Azure Multi-Factor Authentication (MFA).C.   Azure Multi-Factor Authentication (MFA) registration is required for all users.D.   All users must authenticate by using passwordless sign-in.E.   All users must authenticate by using Windows Hello.Answer: BCExplanation:Security defaults make it easy to protect your organization with the following preconfigured security settings: Requiring all users to register for Azure AD Multi-Factor Authentication. Requiring administrators to do multi-factor authentication. Blocking legacy authentication protocols. Requiring users to do multi-factor authentication when necessary. Protecting privileged activities like access to the Azure portal.Reference: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaultsQUESTION 105 Which type of identity is created when you register an application with Active Directory (Azure AD)?A.   a user accountB.   a user-assigned managed identityC.   a system-assigned managed identityD.   a service principalAnswer: DExplanation:When you

register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.Reference:https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal QUESTION 106Which three tasks can be performed by using Azure Active Directory (Azure AD) Identity Protection? Each correct answer presents a complete solution.NOTE: Each correct selection is worth one point.A.   Configure external access for partner organizations.B.   Export risk detection to third-party utilities.C.   Automate the detection and remediation of identity based-risks. D.   Investigate risks that relate to user authentication.E.   Create and automatically assign sensitivity labels to data.Answer: CDE Explanation:Identity Protection allows organizations to accomplish three key tasks:- Automate the detection and remediation of identity-based risks.- Investigate risks using data in the portal.- Export risk detection data to other tools.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protectionQUESTION 107You have a Microsoft 365 E3 subscription.You plan to audit user activity by using the unified audit log and Basic Audit.For how long will the audit records be retained?A.   15 daysB.   30 daysC.   90 daysD.   180 daysAnswer: CExplanation:Microsoft 365 unified auditing helps to track activities performed in the different Microsoft 365 services by both users and admins. Basic auditing is enabled by default for most Microsoft 365 organizations. In the Basic audit, audit records are retained and searchable for the last 90 days.

https://o365reports.com/2021/07/07/microsoft-365-retrieve-audit-log-for-1-year-for-all-subscriptions/QUESTION 108To which type of resource can Azure Bastion provide secure access?A.   Azure FilesB.   Azure SQL Managed InstancesC.   Azure virtual machinesD.   Azure App ServiceAnswer: CExplanation:Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.Reference:

https://docs.microsoft.com/en-us/azure/bastion/bastion-overviewQUESTION 109What are three uses of Microsoft Cloud App Security? Each correct answer presents a complete solution.NOTE: Each correct selection is worth one point.A.   to discover and control the use of shadow ITB.   to provide secure connections to Azure virtual machinesC.   to protect sensitive information hosted anywhere in the cloudD.   to provide pass-through authentication to on-premises applicationsE.   to prevent data leaks to noncompliant apps and limit access to regulated dataAnswer: ACEExplanation:

https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-appsQUESTION 110Hotspot QuestionFor each of the following statements, select Yes if the statement is true. Otherwise, select No.NOTE: Each correct selection is worth one point.

Answer:

Explanation:Box 1: NoPhishing scams are external threats.Box 2: YesInsider risk management is a compliance solution in Microsoft 365.Box 3: YesInsider risk management helps minimize internal risks from users. These include: Leaks of sensitive data and data spillage Confidentiality violations Intellectual property (IP) theft Fraud Insider trading Regulatory compliance violations Reference:https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center?view=o365-worldwideResources From:1.2023 Latest Braindump2go SC-900 Exam Dumps (PDF & VCE) Free Share: https://www.braindump2go.com/sc-900.html2.2023 Latest Braindump2go SC-900 PDF and SC-900 VCE Dumps Free Share: https://drive.google.com/drive/folders/1lBjx9vxksSKq1-ok4CmD-HBgZND4cDno?usp=sharing3.2023 Free Braindump2go SC-900

Exam Questions Download:https://www.braindump2go.com/free-online-pdf/SC-900-PDF-Dumps(55-110).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!