PassQueen
a.k.a dumpsqueen.com

Microsoft Cybersecurity Architect

Microsoft SC-100

Version Demo

Total Demo Questions: 28

Total Premium Questions: 287

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Design solutions that align with security best practices and priorities	19
Topic 2, Design security operations, identity, and compliance capabilities	119
Topic 3, Design security solutions for infrastructure	74
Topic 4, Design security solutions for applications and data	53
Topic 5, Mix Questions	1
Topic 6, Fabrikam, Inc Case Study 1	10
Topic 7, Litware, inc. Case Study 2	11
Total	287

QUESTION NO: 1

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

ANSWER: D

Explanation:

Microsoft Information Protection is the appropriate solution because it provides a unified framework for discovering, classifying, labeling, and protecting sensitive information throughout its lifecycle. Sensitivity labels can be configured to apply encryption and access controls to Microsoft 365 files and emails. The protection remains attached to the content rather than depending solely on its current storage location, so authorized users can continue to access protected content while sharing and collaborating across supported environments.

In a Microsoft 365 E5 environment, administrators can use Microsoft Purview Information Protection capabilities to create and publish sensitivity labels, define encryption settings, apply visual markings, and use automatic or recommended labeling based on sensitive-information types. Users can apply labels in supported Office apps on Windows, macOS, iOS, Android, and the web; organizational policies and supported client capabilities determine the exact labeling experience. Microsoft Information Protection also supports protection for data stored outside Microsoft 365 through sensitivity labels and supported scanners or integrations, helping address on-premises as well as cloud-based data scenarios.

For implementation guidance, see Microsoft Purview Information Protection and Learn about sensitivity labels.

QUESTION NO: 2

Your company uses Microsoft Entra ID P2.

You need to require phishing-resistant multifactor authentication for administrators when they access the Azure portal. The solution must be applied only to privileged administrative roles.

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

NOTE: Each correct selection is worth one point.

A. Create a phishing-resistant authentication strength.

B. Create a Conditional Access policy targeted to privileged directory roles and the Microsoft Azure Management cloud application.

C. Create a Microsoft Entra named location for each administrator.

D. Enable password writeback in Microsoft Entra Connect Sync.

E. Create a device configuration profile in Microsoft Intune.

ANSWER: A B

Explanation:

Create a Microsoft Entra authentication strength that allows phishing-resistant authentication methods. Authentication strengths provide a way to define the authentication methods that satisfy a Conditional Access requirement. A phishing-resistant authentication strength can require methods such as FIDO2 security keys, Windows Hello for Business, or certificate-based authentication, instead of password-based MFA methods that are more susceptible to phishing.

Create a Conditional Access policy targeted to the required directory roles and the Microsoft Azure Management cloud application. The policy can target privileged roles such as Global Administrator, Privileged Role Administrator, and Security Administrator, then require the phishing-resistant authentication strength as a grant control. This applies stronger verification specifically to privileged portal access while avoiding unnecessary impact on non-administrative users. See Authentication strengths and Conditional Access cloud apps, actions, and authentication contexts.

QUESTION NO: 3

You need to recommend a solution to resolve the virtual machine issue. What should you include in the recommendation? (Choose Two)

A. Onboard the virtual machines to Microsoft Defender for Endpoint.

B. Onboard the virtual machines to Azure Arc.

C. Create a device compliance policy in Microsoft Endpoint Manager.

D. Enable the Qualys scanner in Defender for Cloud.

ANSWER: A D

Explanation:

Onboard the virtual machines to Microsoft Defender for Endpoint and enable the Qualys scanner in Defender for Cloud. Defender for Endpoint onboarding establishes the device connection needed for Defender to collect endpoint security telemetry and deliver endpoint detection and response capabilities. For servers, onboarding can be performed through Defender for Cloud integration or other supported deployment methods, allowing the machines to be protected and reported on as managed endpoints.

Enabling the Qualys scanner in Defender for Cloud provides vulnerability assessment coverage for supported virtual machines. The scanner discovers installed software and configuration vulnerabilities and sends assessment results to Defender for Cloud, where they can be reviewed, prioritized, and remediated through recommendations. Together, endpoint onboarding and vulnerability assessment address both endpoint visibility and identification of software vulnerabilities affecting the virtual machines. Microsoft documents Defender for Endpoint server onboarding at Onboard servers to Microsoft Defender for Endpoint and describes vulnerability assessment for machines in Defender for Cloud at Vulnerability assessment solutions in Microsoft Defender for Cloud.

QUESTION NO: 4

You have a Microsoft 365 subscription.

You are designing a user access solution that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend a solution that automatically restricts access to Microsoft Exchange Online. SharePoint Online, and Teams m near-real-lime (NRT) in response to the following Azure AD events:

• A user account is disabled or deleted

• The password of a user is changed or reset.

• All the refresh tokens for a user are revoked

• Multi-factor authentication (MFA) is enabled for a user

Which two features should you include in the recommendation? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. continuous access evaluation

B. a sign-in risk policy

C. Azure AD Privileged Identity Management (PIM)

D. Conditional Access

E. Azure AD Application Proxy

ANSWER: A D

Explanation:

continuous access evaluation is required because it enables Microsoft Entra ID to communicate critical account and session events to supported Microsoft 365 services, including Exchange Online, SharePoint Online, and Teams. When a supported event occurs—such as account disablement, password reset or change, refresh-token revocation, or an MFA-related change—the service can re-evaluate the active session and enforce access changes without waiting for the normal access-token lifetime to expire. This provides the near-real-time session enforcement needed by a Zero Trust design. Microsoft documents the critical event evaluation model and the supported Microsoft 365 workloads in its Continuous access evaluation documentation.

Conditional Access is also part of the recommendation because it is Microsoft Entra ID's Zero Trust policy engine for evaluating and enforcing access requirements. Conditional Access governs the conditions under which identities can access cloud applications and can apply controls such as requiring MFA, compliant devices, or approved client applications. Together with continuous access evaluation, it supports ongoing verification rather than relying only on checks at initial sign-in. The relationship between Conditional Access and continuous access evaluation is described in Microsoft Entra Conditional Access overview.

QUESTION NO: 5

You have an Azure subscription that contains multiple network security groups (NSGs), multiple virtual machines, and an Azure Bastion host named bastion1.

Several NSGs contain rules that allow direct RDP access to the virtual machines by bypassing bastion!

You need to ensure that the virtual machines can be accessed only by using bastion! The solution must prevent the use of NSG rules to bypass bastion1.

What should you include in the solution?

A. Azure Virtual Network Manager connectivity configurations

B. Azure Virtual Network Manager security admin rules

C. Azure Firewall application rules

D. Azure Firewall network rules

ANSWER: B

Explanation:

Azure Virtual Network Manager security admin rules are the appropriate control because they provide centrally managed network-security policy that is evaluated before network security group rules. Security admin rules can enforce a deny policy for direct Remote Desktop Protocol traffic to the virtual-machine subnets while allowing the traffic path required from the Azure Bastion subnet. This makes the intended Bastion-mediated administration path enforceable across multiple virtual networks and NSGs.

A key benefit is that security admin rules have higher precedence than NSG rules. Therefore, an NSG rule created or modified later cannot reopen direct RDP access that the centrally deployed admin rule denies. The security architect can deploy the policy through an Azure Virtual Network Manager security admin configuration to the appropriate network groups and regions, providing consistent governance at scale. The rules should be designed with appropriate source and destination prefixes so that Bastion-to-VM management traffic remains permitted while inbound RDP paths that bypass the Bastion host are denied. Microsoft documents the precedence and behavior of security admin rules in Security admin rules in Azure Virtual Network Manager and describes Azure Bastion's secure RDP and SSH connectivity model in What is Azure Bastion?.

QUESTION NO: 6

You are designing a new Azure environment based on the security best practices of the Microsoft Cloud Adoption Framework for Azure. The environment will contain one subscription for shared infrastructure components and three separate subscriptions for applications.

You need to recommend a deployment solution that includes network security groups (NSGs) Azure Key Vault, and Azure Bastion. The solution must minimize deployment effort and follow security best practices of the Microsoft Cloud Adoption Framework for Azure.

What should you include in the recommendation?

A. the Azure landing zone accelerator

B. the Azure Well-Architected Framework

C. Azure Security Benchmark v3

D. Azure Advisor

ANSWER: A

Explanation:

The Azure landing zone accelerator is correct because it provides an opinionated, deployable implementation of Azure landing zone architecture aligned with the Microsoft Cloud Adoption Framework. It is designed to establish a secure, governed foundation for workloads while reducing the effort needed to build common platform capabilities manually. The accelerator can deploy an enterprise-scale management-group and subscription hierarchy that separates shared platform services from application workloads, which fits the stated shared-infrastructure subscription and separate application subscriptions.

Its reference architecture and implementation artifacts include core networking and security capabilities appropriate for an Azure environment, including network security groups, Azure Bastion, and Azure Key Vault. It also applies governance and security guardrails through Azure Policy, identity integration, resource organization, and standardized configuration. Using the accelerator enables consistent implementation of these controls across subscriptions and supports subsequent workload onboarding without repeatedly designing the foundational platform. This directly meets the requirement to follow Cloud Adoption Framework security practices while minimizing deployment effort through reusable, Microsoft-provided architecture and deployment automation. See the Azure landing zones guidance and the Azure landing zone implementation options.

QUESTION NO: 7

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

ANSWER: A

Explanation:

Azure AD Application Proxy is the appropriate recommendation because it provides secure remote access to specific on-premises web applications without granting users broad network-level connectivity. A connector installed in the internal network establishes an outbound connection to the cloud service, so users access only the applications explicitly published through the proxy. This satisfies the requirement to avoid exposing or enabling access to other internal resources.

Application Proxy integrates with Azure AD, now Microsoft Entra ID, for preauthentication. Consequently, Conditional Access policies can be evaluated before a user reaches the published application. For example, the organization can require multifactor authentication, enforce sign-in risk policies, or apply other access conditions appropriate for personally owned Windows devices.

It also improves the user experience through single sign-on. For applications that use Integrated Windows Authentication with Kerberos, Application Proxy can use Kerberos constrained delegation to authenticate the user to the on-premises application after Entra ID authentication. Users therefore sign in through their cloud identity and can access the authorized web app without a traditional VPN connection or direct exposure to the internal network. See Microsoft Entra Application Proxy overview and Configure single sign-on with Kerberos constrained delegation.

QUESTION NO: 8

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

ANSWER: A B

Explanation:

Azure Firewall and Azure Web Application Firewall (WAF) are preventative network-security controls that help protect Azure landing zones by blocking unauthorized or malicious traffic before it reaches protected workloads. Azure Firewall provides centrally managed, stateful network filtering for Azure virtual networks. It can enforce network and application rules, apply threat-intelligence filtering, and control outbound as well as inbound traffic paths. This supports a landing-zone design in which network security is consistently governed across subscriptions and workloads.

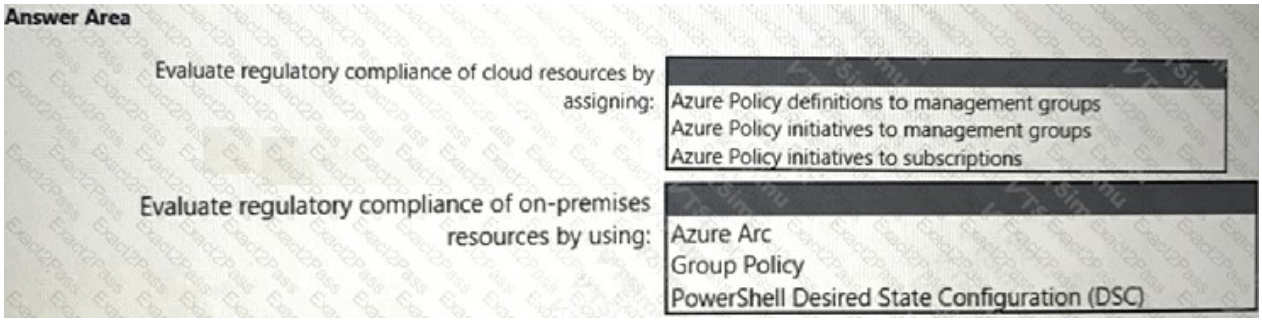
Azure Web Application Firewall (WAF) is a preventative control for HTTP/S applications. When deployed with services such as Azure Application Gateway or Azure Front Door, it inspects web requests and blocks common web exploits and malicious patterns before they reach the web application. Its managed rule sets provide protection against common attack techniques, including those covered by OWASP rules. Implementing and correctly configuring these controls helps remediate applicable Microsoft Defender for Cloud recommendations, which contributes to the Defender for Cloud secure score. Secure score measures the security posture improvements achieved by addressing recommended actions and is organized around security controls. See Secure score security controls and What is Azure Firewall?.

QUESTION NO: 9 - (HOTSPOT)

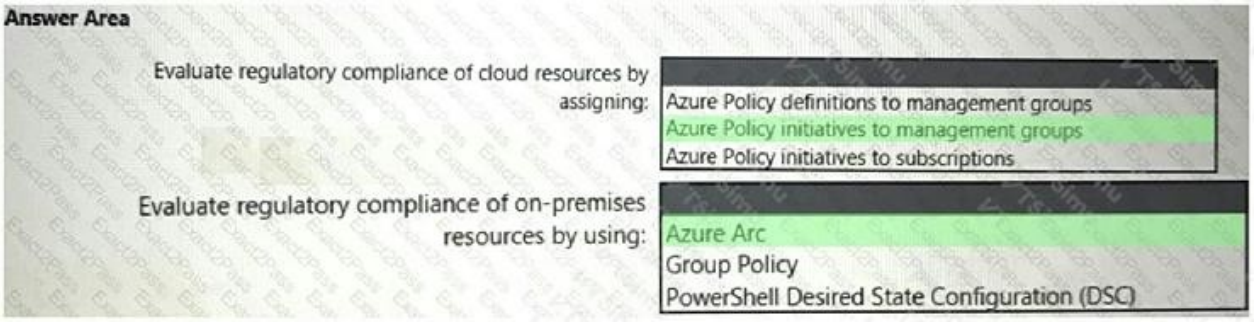
You need to recommend a solution to evaluate regulatory compliance across the entire managed environment. The solution must meet the regulatory compliance requirements and the business requirements.

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

NOTE: Each correct selection is worth one point.



ANSWER:



Explanation:

For cloud resources, assign **Azure Policy initiatives to management groups**. An initiative is a collection of related Azure Policy definitions that can represent an entire regulatory or industry compliance standard, rather than a single isolated control. Assigning the initiative at the management-group level gives the organization a scalable governance boundary: the assignment is inherited by subscriptions beneath that management group, allowing compliance posture to be evaluated consistently across the managed cloud estate. Azure Policy also records compliance results for the resources evaluated by the policies in the initiative, which supports centralized reporting and ongoing assessment against the required standard. Microsoft documents that initiatives simplify assigning and managing groups of related policies and that management groups provide a scope above subscriptions for governance assignments. See Azure Policy initiative definitions and What are Azure management groups?.

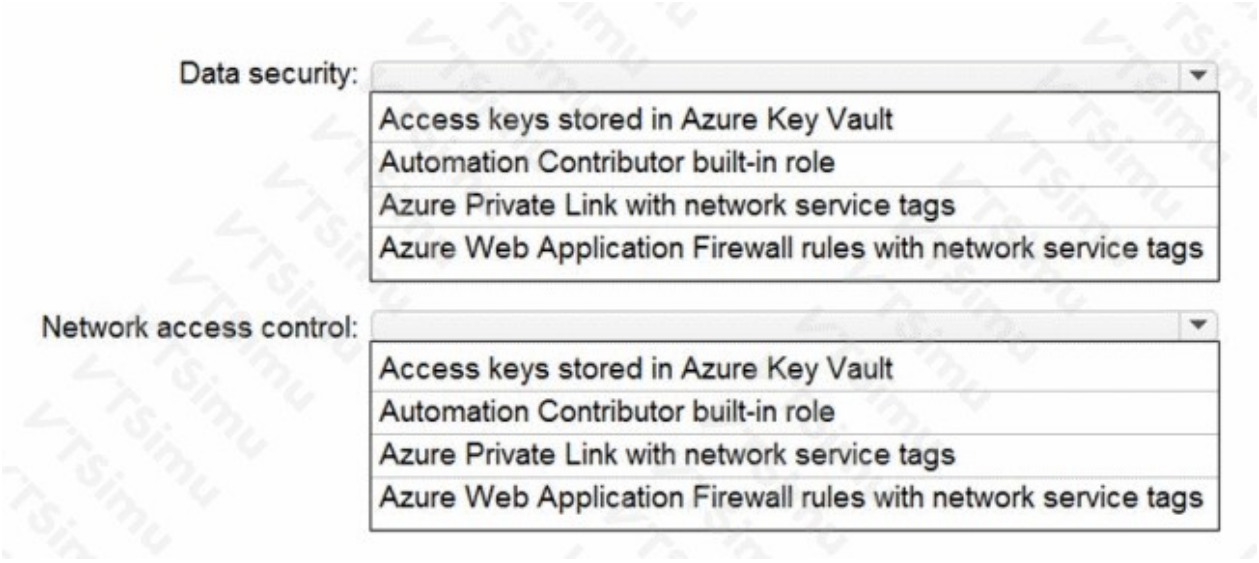
For on-premises resources, use **Azure Arc**. Azure Arc connects servers outside Azure, including on-premises servers, to Azure Resource Manager so they can be organized and governed alongside Azure resources. Once the servers are Arc-enabled, Azure Policy can assess the applicable machine configuration and regulatory controls, and the resulting compliance state is available through Azure governance tooling. This extends the same centralized compliance approach beyond native Azure resources while preserving a single control plane for the entire managed environment. Microsoft's Azure Arc-enabled servers overview describes how Arc brings non-Azure machines under Azure management, and the Azure Policy machine configuration overview explains policy-based compliance assessment for machine settings.

QUESTION NO: 10 - (HOTSPOT)

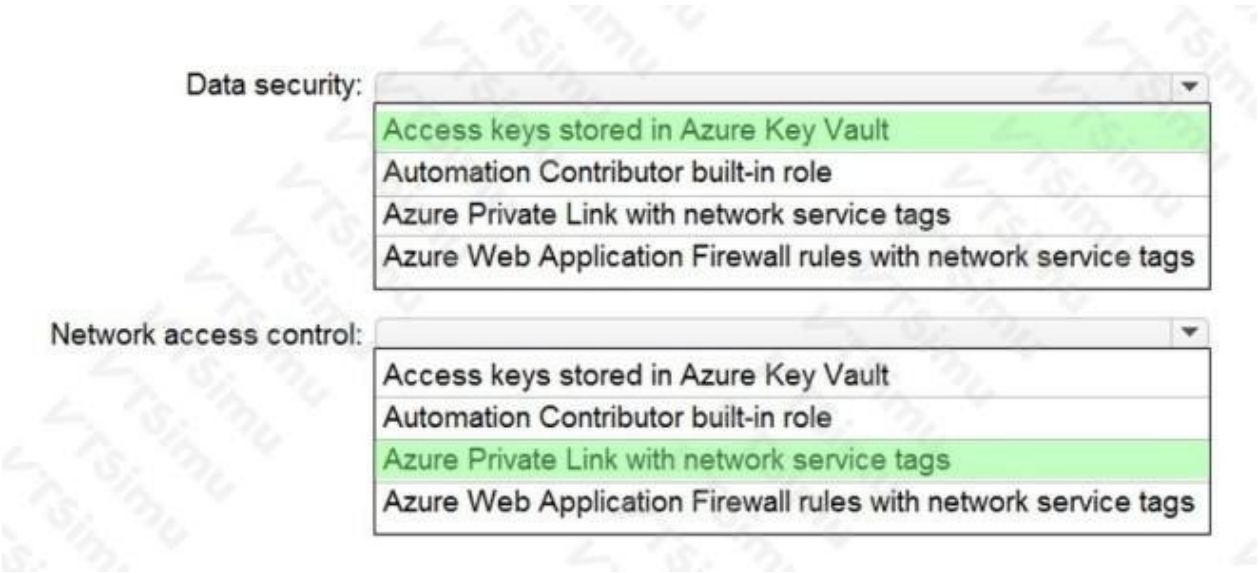
You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.

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.



ANSWER:



Explanation:

The copy process needs protection for both its authentication material and its connectivity path. Store the Azure Data Lake Storage Gen2 access keys in Azure Key Vault so that the runbook does not contain storage secrets directly in its code, variables, or other less controlled locations. Azure Key Vault is designed to safeguard secrets, apply access controls, support auditing, and let an authorized automation process retrieve a secret when it runs. This creates a more secure lifecycle for the credentials used to authenticate the data copy operation. Microsoft's Azure Automation security guidance specifically recommends using Azure Key Vault to protect sensitive information such as credentials and keys used by runbooks. See Azure Automation security guidelines: Data security.

For network access control, use Azure Private Link with network service tags. Private Link provides private connectivity to supported Azure services through a private endpoint, allowing traffic to remain on the Microsoft backbone rather than traversing the public internet. Network service tags simplify defining and maintaining the associated network security rules because Microsoft manages the underlying address prefixes for the tagged Azure service. Together, these controls support

a restricted, intentional communication path for the automation workload and the services involved in the copy process. Private Endpoint and Private Link are described in Azure Private Endpoint overview, while service tags are documented in Virtual network service tags overview.

QUESTION NO: 11

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

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

NOTE: Each correct selection is worth one point.

A. Manage application identities securely and automatically.

B. Manage the lifecycle of identities and entitlements

C. Protect identity and authentication systems.

D. Enable threat detection for identity and access management.

E. Use a centralized identity and authentication system.

ANSWER: C D E

Explanation:

Protect identity and authentication systems, **Enable threat detection for identity and access management**, and **Use a centralized identity and authentication system** are core identity-management practices in the Microsoft Cloud Security Benchmark. A centralized identity system, typically Microsoft Entra ID, provides a consistent control plane for users, administrators, applications, authentication methods, and access policies across cloud resources. This centralization supports consistent application of Conditional Access, multifactor authentication, and least-privilege access.

Identity and authentication services are security-critical infrastructure because compromise of identities can give an attacker broad access to cloud resources. Their protection therefore includes strong authentication controls, secure administrative access, and resilient identity-service configuration. Continuous identity threat detection complements those preventive measures by identifying anomalous sign-ins, risky users, suspicious credential use, and other indicators of identity compromise so that security teams can investigate and respond quickly. Together, these practices implement the benchmark's emphasis on establishing a trusted identity foundation and detecting threats affecting that foundation. See Microsoft Cloud Security Benchmark identity-management controls and Microsoft Entra monitoring and health guidance.

QUESTION NO: 12

You have an Azure subscription that is linked to a Microsoft Entra tenant.

You plan deploy an enterprise application named Appl. App1 requires LDAP to look up attributes related to Microsoft Entra users.

You need to recommend a solution to support the LDAP requirement.

What should you recommend?

A. Configure a Conditional Access policy that has a trusted network location.

B. Deploy Microsoft Entra Domain Services.

C. Deploy Microsoft Entra Private Access.

D. Implement pass-through authentication.

ANSWER: B

Explanation:

Deploy Microsoft Entra Domain Services. Microsoft Entra Domain Services provides managed domain services for a Microsoft Entra tenant, including LDAP support, Kerberos and NTLM authentication, and domain join capabilities. It creates a managed Microsoft Entra Domain Services domain and synchronizes applicable user, group, and credential information from the tenant, enabling applications that depend on traditional directory protocols to query directory attributes without requiring the organization to deploy, operate, patch, or manage domain controllers. For an enterprise application whose stated requirement is LDAP-based lookup of attributes associated with Microsoft Entra users, this service supplies the compatible LDAP directory endpoint and managed domain infrastructure needed by the application. Secure LDAP can also be enabled when the application needs LDAP over TLS, and network security controls can limit access to the managed domain. This approach is specifically designed to support legacy or directory-aware workloads that cannot use modern Microsoft Entra ID APIs or authentication protocols directly. For implementation details and supported managed domain capabilities, see Microsoft Entra Domain Services overview and Configure secure LDAP for Microsoft Entra Domain Services.

QUESTION NO: 13 - (SIMULATION)

You have an Azure subscription that contains Azure App Service web apps. The apps have the following characteristics:

• The apps are deployed by using continuous integration and continuous deployment (CI/CD) pipelines in Azure DevOps.

• The apps are deployed to a test environment first, and then to a production environment.

• The source code for the apps is stored in Azure Repos.

You plan to implement DevSecOps controls based on the Microsoft Cloud Adoption Framework for Azure. You need to recommend testing controls to meet the following requirements:

• All the source code must be tested for security vulnerabilities in Azure Repos before deploying the apps.

• Once the apps are deployed to the test environment they must be tested for security vulnerabilities.

Which testing method should you recommend for each stage? To answer, select the options in the answer area.

NOTE: Each correct answer is worth one point.



ANSWER: See the explanation for the answer

Explanation:

Select:

Reasoning: SAST analyzes source code without requiring the application to be running, so it is the appropriate control for identifying vulnerabilities in Azure Repos before deployment. DAST tests a running application externally, making it appropriate after deployment to the test environment.

QUESTION NO: 14

You have an Azure subscription that contains several virtual networks and Azure private endpoints for Azure Storage accounts.

You need to recommend a DNS solution that ensures that clients in the virtual networks resolve the private endpoint names to their private IP addresses.

What should you include in the recommendation?

A. an Azure Private DNS zone

B. an Azure public DNS zone

C. an Azure Traffic Manager profile

D. a network security group (NSG)

ANSWER: A

Explanation:

An Azure Private DNS zone is the appropriate recommendation. Private endpoints require DNS resolution of the service hostname to the private IP address assigned to the endpoint. For Azure Blob Storage, a private DNS zone such as `privatelink.blob.core.windows.net` contains the private endpoint DNS records.

By linking the private DNS zone to the virtual networks, workloads can use the standard Azure Storage hostname while DNS resolution returns the private endpoint address. This keeps traffic on private connectivity and avoids clients resolving the service name to its public endpoint. For hybrid environments, on-premises DNS can forward the relevant private-link zones to Azure DNS Private Resolver or another supported DNS-forwarding design. See Azure private endpoint DNS configuration.

QUESTION NO: 15

You have a Microsoft Entra tenant named contoso.com and use Microsoft Intune. Each user in contoso.com has a Microsoft Entra ID P1 license and a Windows 11 device that has the Global Secure Access client deployed.

You plan to deploy the following configuration of Microsoft Entra Internet Access:

• Enable a baseline profile.

• Create a security profile named Profile` that has a priority of 300 and contains a single web content filtering policy named WCFPolicy configure WCFPolicy1 as follows:

o Set Action to allow.

o Include a single rule that has a fully qualified domain name (FQDN) destination of ‘. adatum.com.

• Link Profile1 to a Conditional Access policy named CAPolicy1, apply CAPolicy1 to all users, and grant access unless a user ' s device is noncompliant

You need to evaluate the impact of the planned deployment on traffic to the following resources:

•

•

Which two traffic scenarios will occur? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point

A. Traffic to https://www.fabrikam.com will be allowed from all the devices.

B. Traffic to https://www.adatum.com:8433 will be blocked from all the devices.

C. Traffic to https://www.adatumxom:8433 will be allowed from all the devices.

D. Traffic to https://www.fabrikam.com will be allowed from compliant devices only.

E. Traffic to https://www.adatum.com:8433 will be allowed from compliant devices only.

F. Traffic to https://www.fabrikam.com will be blocked from noncompliant devices only.

ANSWER: A E

Explanation:

Traffic to `https://www.fabrikam.com` will be allowed from all the devices because the configured web content filtering rule is scoped specifically to the `.adatum.com` domain destination. Traffic that does not match that destination is handled by the enabled baseline profile. The baseline profile provides the default processing path for Internet Access traffic when a higher-priority applicable security profile does not govern that destination.

Traffic to `https://www.adatum.com:8433` will be allowed from compliant devices only because the allow rule in the higher-priority security profile matches the Adatum destination, and that profile is associated with the Conditional Access policy. The policy targets all users and requires the device to be compliant. Consequently, users on compliant Intune-managed devices meet the grant requirement and can use the profile's allow rule for the Adatum destination. This design combines destination-specific filtering in Microsoft Entra Internet Access with device-compliance enforcement through Conditional Access. Microsoft documents web content filtering rules and their use in Internet Access security profiles at Web content filtering in Global Secure Access. For the Conditional Access device-compliance grant requirement, see Require device compliance with Conditional Access.

QUESTION NO: 16

You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (O/CD) workflows for the deployment of applications to Azure. You need to recommend what to include in dynamic application security testing (DAST) based on the principles of the Microsoft Cloud Adoption Framework for Azure. What should you recommend?

A. unit testing

B. penetration testing

C. dependency testing

D. threat modeling

ANSWER: B

Explanation:

penetration testing is the appropriate recommendation for dynamic application security testing (DAST). DAST assesses an application while it is executing, typically by interacting with its exposed interfaces in a test or preproduction environment. This approach can identify exploitable runtime weaknesses in areas such as authentication, authorization, input handling, session management, API endpoints, and web-server configuration. Penetration testing uses the same externally observable behavior and attack paths that a malicious actor could use, making it a practical dynamic validation activity within a secure CI/CD process.

The Microsoft Cloud Adoption Framework guidance for securing workloads emphasizes integrating security practices throughout development and release processes, including testing deployed applications for vulnerabilities before production release. Automated dynamic scans can be incorporated into Azure Pipelines, while appropriately authorized penetration-testing activities provide deeper validation for significant releases or internet-facing workloads. Testing must be scoped and performed against resources you own or are authorized to assess, following Azure's penetration-testing rules of engagement. This supports a DevSecOps model by providing actionable findings that teams can remediate and retest before deployment. See Secure DevOps in the Cloud Adoption Framework and Microsoft cloud penetration testing rules of engagement.

QUESTION NO: 17

You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:

• Prevent the need to enable ports 3389 and 22 from the internet.

• Only provide permission to connect the virtual machines when required.

• Ensure that administrators use the Azure portal to connect to the virtual machines.

Which two actions should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM) roles as virtual machine contributors.

B. Configure Azure VPN Gateway.

C. Enable Just Enough Administration (JEA).

D. Enable just-in-time (JIT) VM access.

E. Configure Azure Bastion.

ANSWER: D E

Explanation:

Enable just-in-time (JIT) VM access provides time-bound, approved access to a virtual machine's management ports. When an administrator requests access, JIT can temporarily create the required network security rule for a defined duration and then removes that access when the period expires. This satisfies the requirement that remote-connectivity permission is granted only when it is needed, rather than leaving management access continuously available. JIT access is a Microsoft Defender for Cloud capability and can be governed through Azure RBAC permissions and approval workflows where appropriate.

Configure Azure Bastion provides browser-based RDP and SSH connectivity from the Azure portal to virtual machines. Bastion is deployed into the virtual network and acts as the managed connection point, so the target virtual machines do not require public IP addresses or direct exposure of inbound TCP 3389 or TCP 22 to the internet. Administrators initiate their sessions through the portal, meeting the specified connection experience while retaining network isolation for the virtual machines.

Using JIT VM access together with Azure Bastion applies least privilege to remote administration and provides a portal-based path for secure management. Microsoft documents JIT behavior in Enable just-in-time VM access and Bastion's portal-based RDP/SSH architecture in What is Azure Bastion?.

QUESTION NO: 18

You are designing a Microsoft Sentinel solution.

When a high-severity incident is created, the solution must enrich the incident by using an external threat intelligence service and send the results to a Microsoft Teams channel automatically.

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

NOTE: Each correct selection is worth one point.

A. a Microsoft Sentinel automation rule

B. a Microsoft Sentinel playbook

C. a Microsoft Sentinel workbook

D. a Microsoft Sentinel watchlist

E. an Azure Policy initiative

ANSWER: A B

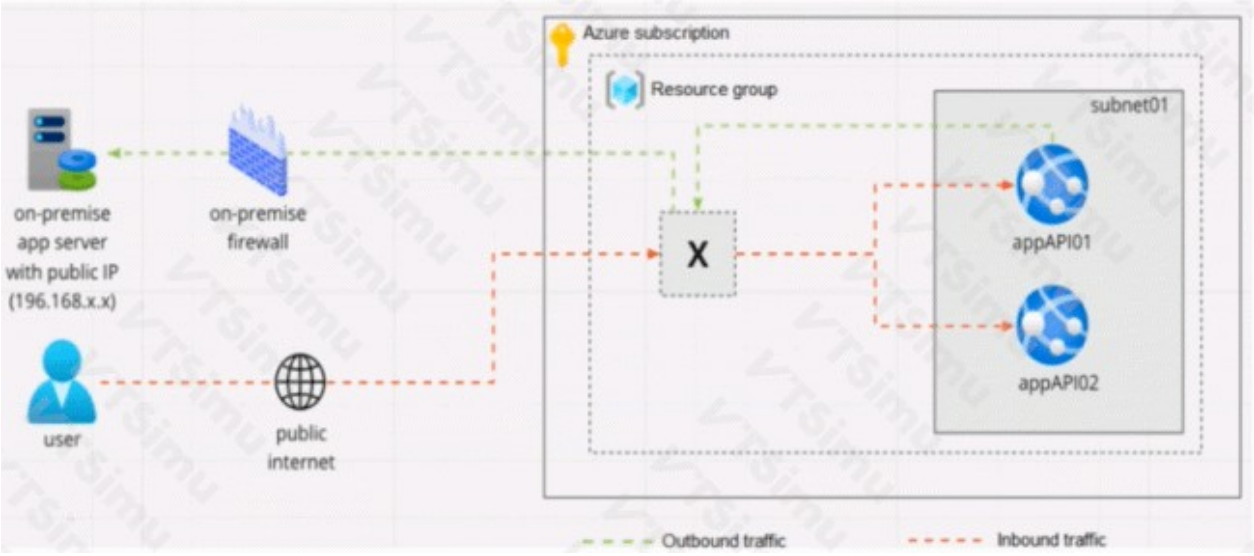
Explanation:

A Microsoft Sentinel automation rule is required to define when automated response occurs. Automation rules can evaluate incident properties, such as severity, status, analytics rule name, or tags, and can trigger a playbook when the defined conditions are met. In this scenario, the rule can trigger only when a high-severity incident is created.

A Microsoft Sentinel playbook is required to perform the response actions. Playbooks are based on Azure Logic Apps and can use connectors and workflows to call an external threat intelligence service, add enrichment results to the incident, and post a notification to a Microsoft Teams channel. Together, the automation rule supplies the incident-based trigger and the playbook orchestrates the enrichment and notification actions. See Automate threat response with automation rules and Automate threat responses with playbooks.

QUESTION NO: 19

Your company is designing an application architecture for Azure App Service Environment (ASE) web apps as shown in the exhibit. (Click the Exhibit tab.)



Communication between the on-premises network and Azure uses an ExpressRoute connection.

You need to recommend a solution to ensure that the web apps can communicate with the on-premises application server. The solution must minimize the number of public IP addresses that are allowed to access the on-premises network.

What should you include in the recommendation?

A. Azure Traffic Manager with priority traffic-routing methods

B. Azure Application Gateway v2 with user-defined routes (UDRs).

C. Azure Front Door with Azure Web Application Firewall (WAF)

D. Azure Firewall with policy rule sets

ANSWER: D

Explanation:

Azure Firewall with policy rule sets is the appropriate centralized egress-control solution for this requirement. Azure Firewall can be deployed in the virtual network path used by the App Service Environment and configured with network rules that permit the required traffic from the web-app environment to the on-premises application server. Routing can direct this traffic

through the firewall, including for connectivity that traverses ExpressRoute. This provides a single, governed inspection and policy-enforcement point rather than requiring the on-premises environment to manage access for numerous individual application-related addresses.

For flows that require public source-address allowlisting, Azure Firewall performs source network address translation (SNAT) by using its assigned public IP address or addresses. The on-premises firewall can therefore allow only the small, known set of Azure Firewall public IP addresses. Firewall policy rule sets centralize the network-access rules and support consistent management of permitted destinations, ports, and protocols. The firewall's SNAT behavior and its public IP configuration make it suitable for reducing the public address exposure that must be maintained on the on-premises side. For implementation details, see Azure Firewall overview and Azure Firewall SNAT private IP address ranges.

QUESTION NO: 20 - (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.



ANSWER:

Explanation:

A DART-based ransomware investigation should begin by assessing the current situation and identifying the scope. This creates the factual baseline for the response: the team needs to understand what is known about the incident, which systems or identities may be involved, what evidence is available, and how broadly the activity may have spread. Establishing scope early helps incident responders organize investigation work, preserve relevant evidence, and coordinate containment and recovery decisions using a shared understanding of the incident.

After that initial assessment, the organization should identify which line-of-business (LOB) applications are unavailable because of the ransomware incident. Ransomware response is not only a technical exercise; it must also identify operational impact. Mapping unavailable applications helps the response team understand which critical business services have been disrupted, prioritize restoration work according to business requirements, and communicate an accurate impact picture to business stakeholders.

With the scope and business impact understood, the next step is to identify the compromise recovery process. Recovery must address the underlying compromise in addition to restoring systems or data. A defined process coordinates the activities required to return the environment to a trusted state, including recovery planning, validation, and safe restoration sequencing. Microsoft's ransomware guidance emphasizes investigating the full incident, determining the business impact, and conducting recovery in a controlled way. See Microsoft incident response playbooks and Microsoft ransomware and extortion incident response playbook.

QUESTION NO: 21

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

ANSWER: A E

Explanation:

Azure AD Conditional Access integration with user flows and custom policies provides a policy-based control plane for the application's customer identities. When Conditional Access is enabled for Azure AD B2C user flows or incorporated into custom policies, the organization can evaluate sign-in risk and require an appropriate action, such as multifactor authentication or blocking access. This helps protect the invoicing application when a sign-in has indicators associated with compromised credentials or other risky authentication activity. Conditional Access is therefore a direct identity-security control that can be applied as part of the B2C authentication journey.

Smart account lockout in Azure AD B2C protects user accounts from password-spray and repeated password-guessing attempts. It distinguishes familiar from unfamiliar sign-in behavior and uses progressive lockout behavior to limit repeated failed sign-ins, reducing the effectiveness of automated credential attacks while helping legitimate users avoid unnecessary lockouts. Together, Conditional Access-based risk controls and smart lockout address both risky authentication events and brute-force credential attacks at the identity provider layer, before an attacker can obtain a valid session for the web application. Microsoft documents these B2C threat-management capabilities at Threat management in Azure AD B2C and describes policy integration at Conditional Access in Azure AD B2C user flows.

QUESTION NO: 22

You have two Azure subscriptions named Sub1 and Sub2 that contain the vaults shown in the following table.

Name	Type	Location	Subscription
RSVault1	Recovery Services vault	East US	Sub1
BackupVault1	Azure Backup vault	East US	Sub2
RSVault2	Recovery Services vault	West US	Sub2
BackupVault2	Azure Backup vault	West US	Sub1

You need to design a multi-user authorization (MUA) solution for security operations on the vaults. The solution must meet the following requirements:

• RSVault1 and RSVault2 must require MUA for disabling soft delete, removing MUA protection, and disabling immutability.

• BackupVault1 and BackupVault2 must require MUA for disabling soft delete and removing MUA protection.

What is the minimum number of Resource Guard resources required?

A. 1

B. 2

C. 3

D. 4

ANSWER: C

Explanation:

3 is the minimum number of Resource Guard resources. Azure Backup multi-user authorization is implemented by associating a vault with a Resource Guard and selecting the critical operations that require authorization from the Resource Guard's security boundary. A single Resource Guard can protect more than one vault, including both Recovery Services vaults and Backup vaults, provided that the vaults meet the Resource Guard association requirements. The protected operations can include disabling soft delete, removing multi-user authorization protection, and—where applicable to a Recovery Services vault—disabling immutability.

Resource Guards are regional resources: a Resource Guard can protect vaults only in its own Azure region. The vault placement shown in the table requires coverage in three distinct regions. Therefore, the vaults in each region can share one appropriately located Resource Guard, with the required critical operations enabled for the associated vaults. This design supplies the required MUA protection while avoiding unnecessary Resource Guard deployments. Microsoft also recommends placing a Resource Guard in a separate subscription from the vaults it protects to preserve the intended separation of duties and reduce the risk that a vault administrator can remove the protection unilaterally.

See Multi-user authorization in Azure Backup and Azure Backup security and access control.

QUESTION NO: 23

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

ANSWER: C D

Explanation:

resource-based role-based access control (RBAC) is appropriate for separating the teams' log access. Azure role assignments can be scoped to the relevant resource groups, resources, or Log Analytics workspace. This lets the security operations team receive the permissions required to investigate across the security and operational data estate, while the IT operations team can be assigned access only to the resources and operational-log scope for which it is responsible. Access to Log Analytics data can use resource-context authorization, which evaluates a user's Azure permissions for the resource that produced the records. This supports least privilege while preserving the ability to investigate operational events. See Manage access to Log Analytics workspaces.

the Azure Monitor agent can collect Windows event logs from the perimeter servers through data collection rules and send them to the Log Analytics workspace used by Microsoft Sentinel. For on-premises machines, the servers can be Azure Arc-enabled and configured to use approved proxy or private connectivity rather than making a direct internet connection. The agent supports collecting Windows Event Logs and other monitoring data, providing the operational telemetry needed by the IT operations team and the broader visibility required by security operations. For implementation details, see Azure Monitor agent overview.

QUESTION NO: 24

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

ANSWER: D

Explanation:

Azure Policy is the appropriate service because it provides centralized governance and enforcement for Azure resource configurations, including Azure Storage security settings. Microsoft Defender for Cloud assesses resources against security recommendations and can identify storage accounts that permit overly broad network access, lack private endpoints, or allow public access. Azure Policy mitigates these identified risks by assigning built-in policy definitions or initiatives at the management-group, subscription, or resource-group scope.

For example, policies can audit or deny storage-account configurations that allow public network access, require private endpoint connections, require restrictive network rules, or prevent public blob access. Using a *Deny* effect prevents noncompliant configurations from being created or updated, while *Audit* identifies existing noncompliant resources. Where supported, remediation tasks can help bring existing resources into compliance. Defender for Cloud integrates policy compliance results into its recommendations and secure score, allowing the organization to continuously measure and improve its security posture. This makes Azure Policy the governance control that turns the stated recommendations into enforceable configuration requirements across the Azure environment.

See Azure Policy overview and Review security recommendations in Microsoft Defender for Cloud.

QUESTION NO: 25

You are designing a Microsoft Sentinel solution for a security operations center.

The solution must automatically respond when a high-severity incident is created. It must disable a user account and notify the incident response team by email.

Which two components should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Create an automation rule that invokes a playbook for high-severity incidents.

B. Create a Microsoft Sentinel playbook by using Azure Logic Apps.

C. Create a Microsoft Sentinel workbook.

D. Configure a data collection rule.

E. Create a Log Analytics workspace table.

ANSWER: A B

Explanation:

Create an automation rule to trigger automated response when an incident that meets the required criteria is created. Automation rules in Microsoft Sentinel can evaluate incident properties, such as severity, and invoke a playbook. This provides a consistent way to start the response process for high-severity incidents.

Create a Microsoft Sentinel playbook that uses Azure Logic Apps. A playbook can invoke Microsoft Graph-based actions to disable the affected user account and use an email connector to notify the incident response team. Playbooks provide orchestration across Microsoft Sentinel, Microsoft Entra ID, and communication services, enabling repeatable response actions. See Automate threat response with automation rules in Microsoft Sentinel and Automate threat responses with playbooks in Microsoft Sentinel.

QUESTION NO: 26

Your on-premises network contains an Active Directory Domain Services (AD DS) domain and a hybrid deployment between a Microsoft Exchange Server 2019 organization and an Exchange Online tenant. The AD DS domain contains a group named Group1. Group1 is a member of the Organization Management role group for the Exchange deployment.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender.

You have an Azure subscription that uses Microsoft Sentinel.

You need to recommend a solution to ensure that Group1 is marked as a sensitive group and that any changes made to Group1 raises an alert in Microsoft Sentinel. The solution must minimize administrative effort.

What should you include in the recommendation?

A. Microsoft Entra ID Protection

B. Microsoft Defender for Identity

C. Microsoft Defender for Office 365

D. Microsoft Entra Privileged Identity Management (PIM)

ANSWER: B

Explanation:

Microsoft Defender for Identity is the appropriate recommendation because it monitors on-premises Active Directory Domain Services activity and includes built-in security monitoring for sensitive groups. Groups can be designated as sensitive within Defender for Identity, allowing changes to their membership and other relevant directory activity to be treated as high-value events. This is especially suitable for Group1 because membership in the Exchange Organization Management role group provides substantial administrative privileges in the Exchange environment.

Defender for Identity generates security alerts for suspicious or sensitive Active Directory changes and integrates with Microsoft Sentinel through the Microsoft Defender XDR data connector. Enabling this connector sends Defender for Identity incidents and alerts to Sentinel, where they can be investigated, correlated with other security telemetry, and used in analytics rules or automation. This approach avoids creating and maintaining custom Windows event collection, custom parsing, and bespoke Sentinel detections solely to identify group changes, thereby minimizing administrative effort. Microsoft documents sensitive account and group monitoring in Defender for Identity and the Sentinel integration for Microsoft Defender XDR at Manage sensitive accounts in Microsoft Defender for Identity and Connect Microsoft Defender XDR to Microsoft Sentinel.

QUESTION NO: 27

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

ANSWER: B

Explanation:

Data loss prevention (DLP) policies are the appropriate control because they are designed to identify sensitive information and prevent inappropriate sharing of that information across Microsoft 365 workloads. A Microsoft Purview DLP policy can use the built-in U.S. Health Insurance Act (HIPAA) sensitive information type, or a customized sensitive information type, to detect PHI in Exchange Online email, SharePoint Online and OneDrive documents, and Teams messages and files. The policy can then enforce protective actions when a user attempts to share matched content with people outside the organization. For example, it can block external email recipients, restrict external sharing of files, block Teams messages containing PHI from being sent externally, and present policy tips that educate users at the point of action. DLP policies can be scoped to selected users, groups, sites, accounts, and locations, allowing the organization to apply PHI controls where required while minimizing operational impact. Microsoft 365 E5 provides the necessary Microsoft Purview capabilities to create, test, tune, and enforce these policies. Administrators should initially run the policy in simulation or test mode, review detections, and then enable blocking actions after validating the rule conditions. See Learn about Microsoft Purview Data Loss Prevention and Create and deploy data loss prevention policies.

QUESTION NO: 28

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. Create a blueprint definition at a management group and assign it to the subscriptions.

ANSWER: A F

Explanation:

Assigning an initiative to a management group provides the most direct, scalable Azure Policy approach. The built-in ISO 27001:2013 initiative groups the relevant policy definitions into one policy set, and a management-group assignment is inherited by all subscriptions beneath that management group. Consequently, changes to the initiative's monitored policy-definition list can be managed centrally rather than repeated across 50 individual subscriptions. This supports a consistent compliance posture and consolidated compliance reporting at scale. Microsoft describes initiatives as collections of policy definitions that simplify assigning and managing related policies, while management groups provide a scope above subscriptions for applying governance consistently. See Azure Policy initiative definitions and Management groups in Azure.

Creating a blueprint definition at a management group and assigning it to the subscriptions also centralizes the governance artifact and its included policy assignments. A blueprint can package policy assignments with other governed resources and settings, allowing the standardized ISO-oriented configuration to be maintained in one blueprint definition and versioned for use by the governed subscriptions. This provides a centrally managed alternative when the organization requires a broader, repeatable governance package in addition to policy monitoring.