Vendor: Microsoft

Exam Code: SC-100

Exam Name: Microsoft Cybersecurity Architect

Version: DEMO

QUESTION 1
Case Study 1 - Fabrikam, Inc

OverView
Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

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

Azure Environment
Fabrikam has the following Azure resources:
- An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabnkam.com
- A single Azure subscription named Sub1
- A virtual network named Vnetl in the East US Azure region
- A virtual network named Vnet2 in the West Europe Azure region
- An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAR enabled
- A Microsoft Sentinel workspace
- An Azure SQL database named ClaimsDB that contains a table named ClaimDetails
- 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud
- A resource group named TestRG that is used for testing purposes only
- An Azure Virtual Desktop host pool that contains personal assigned session hosts
- All the resources in Sub1 are in either the East US or the West Europe region.

Partners
Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:
- An Azure AD tenant named contoso.onmicrosoft.com
- An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security Group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1. The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

You need to recommend a solution to meet the security requirements for the InfraSec group. What should you use to delegate the access?

A. a subscription
B. a custom role-based access control (RBAC) role
C. a resource group
D. a management group

Answer: B
Explanation:
Scenario: Requirements. Security Requirements include:
Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.
If the Azure built-in roles don't meet the specific needs of your organization, you can create your own custom roles. Just like built-in roles, you can assign custom roles to users, groups, and

service principals at management group (in preview only), subscription, and resource group scopes.

Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

QUESTION 2
Case Study 2 - Litware, inc.

Overview
Litware, inc. is a financial services company that has main offices in New York and San Francisco. litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.
Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

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

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

Planned Changes
Litware plans to implement the following changes:
- Create a management group hierarchy for each Azure AD tenant.
- Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.
- Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

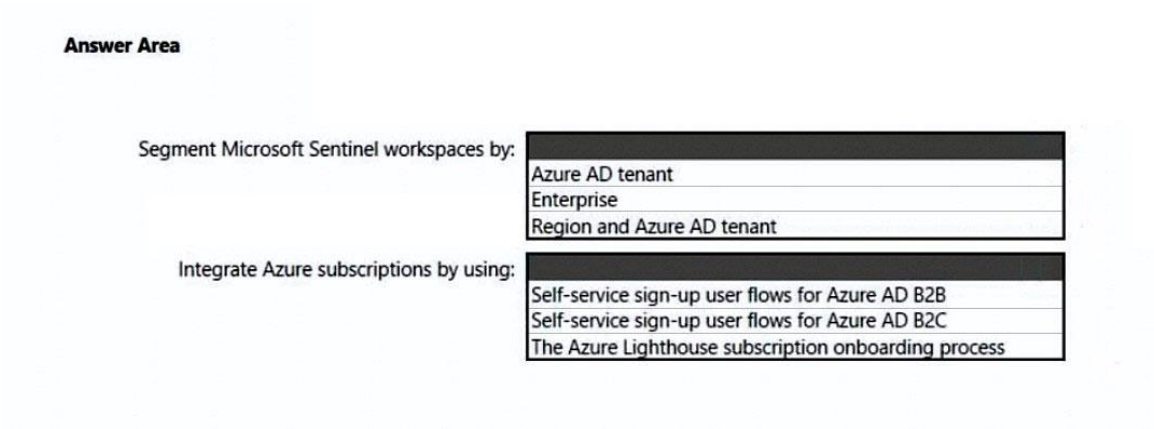
Business Requirements
Litware identifies the following business requirements:
- Minimize any additional on-premises infrastructure.
- Minimize the operational costs associated with administrative overhead.

Hybrid Requirements
Litware identifies the following hybrid cloud requirements:
- Enable the management of on-premises resources from Azure, including the following:
- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.
- Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

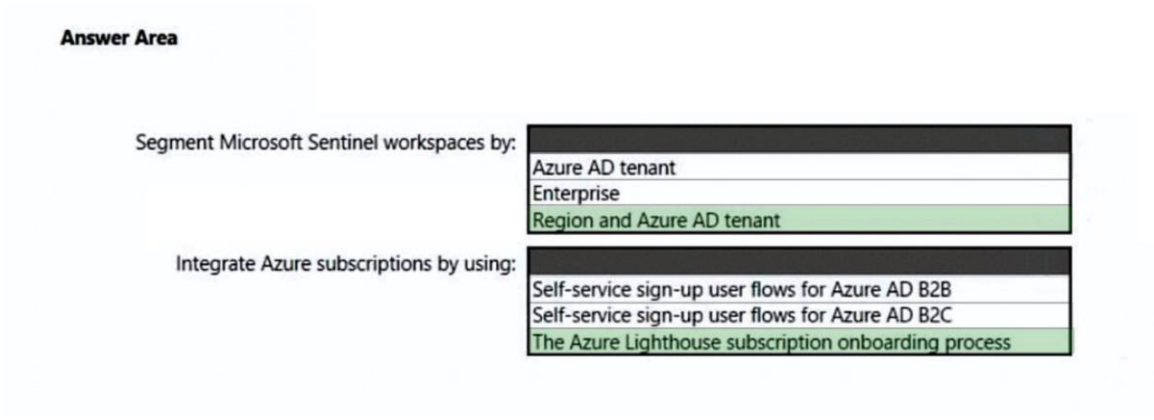
Hotspot Question

You need to recommend a SIEM and SOAR strategy that meets the hybrid requirements, the Microsoft Sentinel requirements, and the regulatory compliance 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:
Box 1: Region and Azure AD tenant
Relevant information from Microsoft is on this Best Practices page for workspace architecture:
https://docs.microsoft.com/en-us/azure/sentinel/best-practices-workspace-architecture#region-considerations

Box 2: Azure Lighthouse subscription onboarding process
You can use Azure Lighthouse to extend all cross-workspace activities across tenant boundaries, allowing users in your managing tenant to work on Microsoft
Sentinel workspaces across all tenants.
Azure Lighthouse enables you to see and manage Azure resources from different tenancies, in the one place, with the power of delegated administration. That tenancy may be a customer (for example, if you're a managed services provider with a support contract arrangement in place), or a separate Azure environment for legal or financial reasons (like franchisee groups or Enterprises with large brand groups).

QUESTION 3
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: DE
Explanation:
Bastion provides secure remote access.
It uses RDP/SSH session is over TLS on port 443.
Note: Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.
Lock down inbound traffic to your Azure Virtual Machines with Microsoft Defender for Cloud's just-in-time (JIT) virtual machine (VM) access feature. This reduces exposure to attacks while providing easy access when you need to connect to a VM.
Meets the requirement: Only provide permission to connect the virtual machines when required

Reference:
https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.2
https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

QUESTION 4
You have Windows 11 devices and Microsoft 365 E5 licenses.
You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites.
What should you include in the recommendation?

A. Microsoft Endpoint Manager
B. Compliance Manager
C. Microsoft Defender for Cloud Apps
D. Microsoft Defender for Endpoint

Answer: D
Explanation:
Web content filtering is part of the Web protection capabilities in Microsoft Defender for Endpoint. It enables your organization to track and regulate access to websites based on their content categories. Many of these websites, while not malicious, might be problematic because of compliance regulations, bandwidth usage, or other concerns.

Note: Turn on web content filtering
From the left-hand navigation in Microsoft 365 Defender portal, select Settings > Endpoints > General > Advanced Features. Scroll down until you see the entry for Web content filtering.
Switch the toggle to On and Save preferences.
Configure web content filtering policies
Web content filtering policies specify which site categories are blocked on which device groups.
To manage the policies, go to Settings > Endpoints > Web content filtering (under Rules).

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering

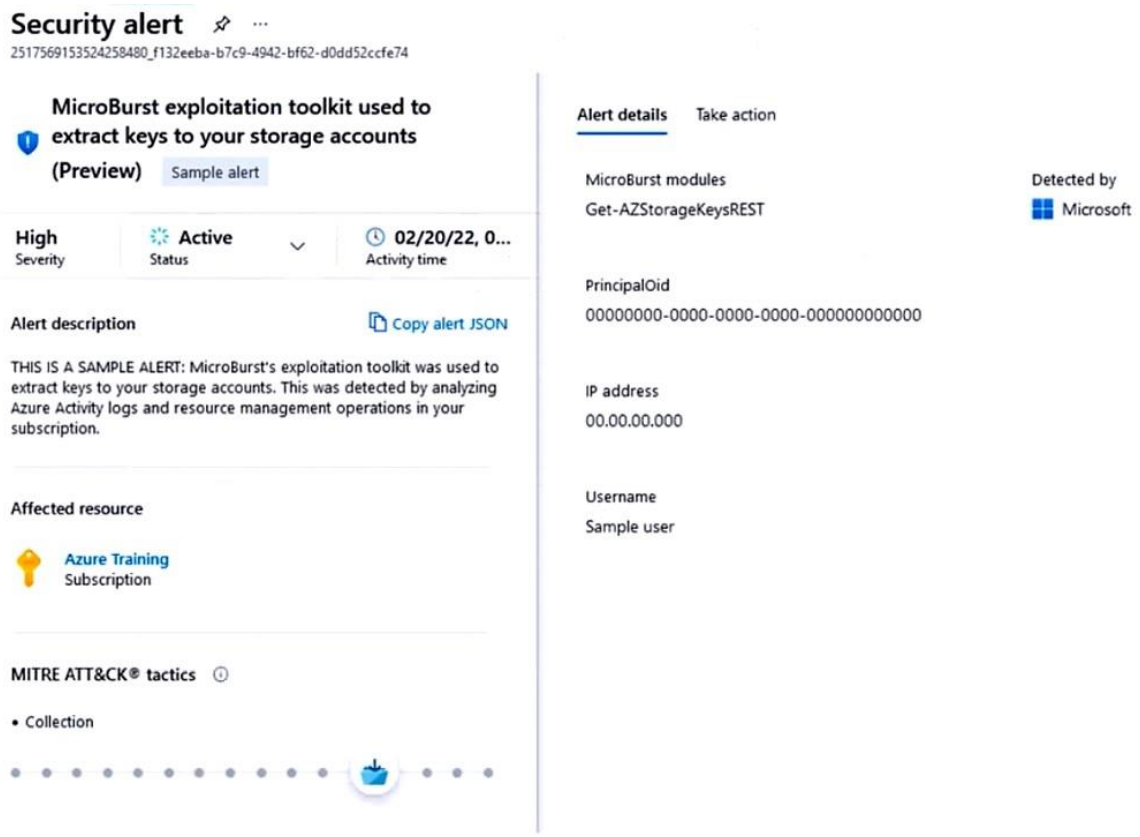
QUESTION 5
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You need to enforce ISO 2700V2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatical.
What should you use?

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

Answer: B
Explanation:
Control mapping of the ISO 27001 Shared Services blueprint sample
The following mappings are to the ISO 27001:2013 controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an Azure Policy initiative.
Open Policy in the Azure portal and select the Definitions page. Then, find and select the [Preview] Audit ISO 27001:2013 controls and deploy specific VM
Extensions to support audit requirements built-in policy initiative.
Note: Security Center can now auto provision the Azure Policy's Guest Configuration extension (in preview)
Azure Policy can audit settings inside a machine, both for machines running in Azure and Arc connected machines. The validation is performed by the Guest
Configuration extension and client.
With this update, you can now set Security Center to automatically provision this extension to all supported machines.
Enforcing a secure configuration, based on a specific recommendation, is offered in two modes:
Using the Deny effect of Azure Policy, you can stop unhealthy resources from being created
Using the Enforce option, you can take advantage of Azure Policy's DeployIfNotExist effect and automatically remediate non-compliant resources upon creation

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 6
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

Answer: A
Explanation:
Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data, but may also present a security risk. It's important to manage anonymous access judiciously and to understand how to evaluate anonymous access to your data. Operational complexity, human error, or malicious attack against data that is publicly accessible can result in costly data breaches. Microsoft recommends that you enable anonymous access only when necessary for your application scenario.
Note: Attackers have been crawling for public containers using tools such as MicroBurst.
Exploiting Anonymous Blob Access
Now, there are thousands of articles explaining how this can be abused and how to search for insecure storage in Azure. One of the easiest way is to use
MicroBurst, provide the storage account name to search for, and it'll check if the containers exists based on a wordlist saved in the Misc/permutations.txt

Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent
https://hackingthe.cloud/azure/anonymous-blob-access/

QUESTION 7
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.

Answer: BC
Explanation:
Azure Key Vault Managed HSM (Hardware Security Module) is a fully managed, highly available, single-tenant, standards-compliant cloud service that enables you to safeguard cryptographic keys for your cloud applications, using FIPS 140-2 Level 3 validated HSMs.
You can generate HSM-protected keys in your on-premise HSM and import them securely into Managed HSM.

Reference:
https://docs.microsoft.com/en-us/azure/key-vault/managed-hsm/overview

QUESTION 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: AB
Explanation:
This question is to increase secure score. Here is a long reference page from Microsoft of security recommendations that can increase your secure score. Sentinel & PIM are not on it. The explanation makes a great point about alerts not being preventive, which is a key aspect of the required solution.
https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference

QUESTION 9

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

Answer: A
Explanation:
Content explorer. This tab provides visibility into the amount and types of sensitive data in an organization. It also enables users to filter by label or sensitivity type. Doing so displays a detailed view of locations where the sensitive data is stored. It provides admins with the ability to:
- index the sensitive documents that are stored within supported Microsoft 365 workloads.
- identify the sensitive information they're storing.

https://docs.microsoft.com/en-us/learn/modules/implement-data-classification-of-sensitive-information/6-view-sensitive-data-content-explorer-activity-explorer

QUESTION 10
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

Answer: AB
Explanation:
Defender for Containers assists you with the three core aspects of container security:
Environment hardening - Defender for Containers protects your Kubernetes clusters whether they're running on Azure Kubernetes Service, Kubernetes on-premises/IaaS, or Amazon EKS. Defender for Containers continuously assesses clusters to provide visibility into misconfigurations and guidelines to help mitigate identified threats.
Vulnerability assessment - Vulnerability assessment and management tools for images stored in ACR registries and running in Azure Kubernetes Service.
Run-time threat protection for nodes and clusters - Threat protection for clusters and Linux nodes generates security alerts for suspicious activities.

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 11

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

Answer: ABE
Explanation:
PIM is supported: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/aws/aws-azure-ad-security#advanced-azure-ad-identity-management-with-aws-accounts
To enable the Defender for Servers plan Azure Arc for servers installed on your EC2 instances (https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings)
Azure Policy not supported. But the CSPM part of Defender for Cloud is. So you could deploy CIS Benchmark for AWS.

QUESTION 12
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls.

Solution: You recommend enabling adaptive network hardening.

Does this meet the goal?

A. Yes
B. No

Answer: A
Explanation:
Keep in mind the instructions "Some question sets might have more than one correct solution" and familiarize yourself with the Azure Security Benchmark V3 report.
Two correct answers are JIT and Adaptive Network Hardening.

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

QUESTION 13
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You 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

Answer: B
Explanation:
Instead: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Restrict access to a specific Azure Front Door instance
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.

Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions
https://docs.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services

QUESTION 14
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

Answer: C
Explanation:
The Threat Modeling Tool is a core element of the Microsoft Security Development Lifecycle (SDL). It allows software architects to identify and mitigate potential security issues early, when they are relatively easy and cost-effective to resolve. As a result, it greatly reduces the total cost of development. Also, we designed the tool with non-security experts in mind, making threat modeling easier for all developers by providing clear guidance on creating and analyzing threat models.
https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool

QUESTION 15
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

Answer: B
Explanation:
Roughly 20% of all Internet traffic comes from bad bots. They do things like scraping, scanning, and looking for vulnerabilities in your web application. When these bots are stopped at the Web Application Firewall (WAF), they can't attack you. They also can't use up your resources and services, such as your backends and other underlying infrastructure.
You can enable a managed bot protection rule set for your WAF to block or log requests from known malicious IP addresses. The IP addresses are sourced from the Microsoft Threat Intelligence feed. Intelligent Security Graph powers Microsoft threat intelligence and is used by multiple services including Microsoft Defender for Cloud.
https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection-overview

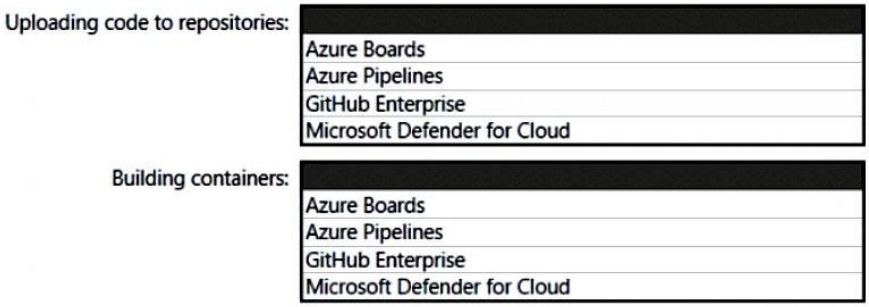
QUESTION 16
Hotspot Question

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.
```

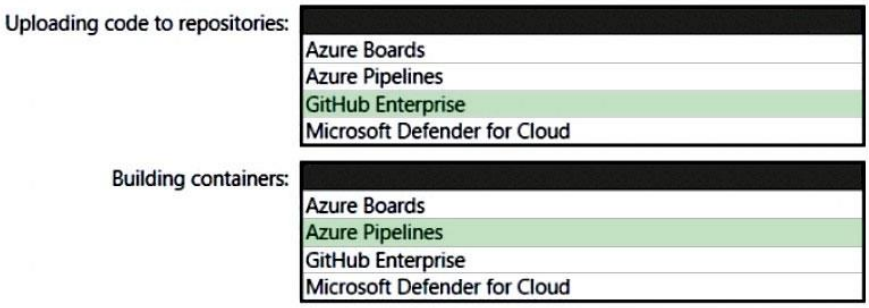
Where should you integrate code scanning for each phase? To answer, select the appropriate options in the answer area.

Answer Area



Answer:

Answer Area



Explanation:
Box 1: GitHub Enterprise
A GitHub Advanced Security license provides the following additional features:
Code scanning - Search for potential security vulnerabilities and coding errors in your code.
Secret scanning - Detect secrets, for example keys and tokens, that have been checked into the repository. If push protection is enabled, also detects secrets when they are pushed to your repository.
Etc.
Code scanning is a feature that you use to analyze the code in a GitHub repository to find security vulnerabilities and coding errors. Any problems identified by the analysis are shown in GitHub Enterprise Cloud.

Box 2: Azure Pipelines
Building Containers with Azure DevOps using DevTest Pattern with Azure Pipelines
The pattern enabled as to build container for development, testing and releasing the container for further reuse (production ready).
Azure Pipelines integrates metadata tracing into your container images, including commit hashes and issue numbers from Azure Boards, so that you can inspect your applications with confidence.

Incorrect:

* Not Azure Boards: Azure Boards provides software development teams with the interactive and customizable tools they need to manage their software projects.
It provides a rich set of capabilities including native support for Agile, Scrum, and Kanban processes, calendar views, configurable dashboards, and integrated reporting.
* Not Microsoft Defender for Cloud
Microsoft Defender for Containers is the cloud-native solution that is used to secure your containers so you can improve, monitor, and maintain the security of your clusters, containers, and their applications.
You cannot use Microsoft Defender for Cloud to scan code, it scans images.

Reference:
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 17
You have a Microsoft 365 E5 subscription.
You need to recommend a solution to add a watermark to email attachments that contain sensitive data. What should you include in the recommendation?

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

Answer: C
Explanation:
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.

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

QUESTION 18
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

Answer: A
Explanation:
The Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in NIST SP 800-53 Rev. 5.
The following mappings are to the NIST SP 800-53 Rev. 5 controls. Use the navigation on the right to jump directly to a specific compliance domain. Many of the controls are implemented with an Azure Policy initiative definition. To review the complete initiative definition, open Policy in the Azure portal and select the
Definitions page. Then, find and select the NIST SP 800-53 Rev. 5 Regulatory Compliance built-in initiative definition.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-53-r5

QUESTION 19
Your company uses loT flow valves at remote water treatment facilities. The devices are monitored by network sensors that are supplied by different vendors. Each vendor uses different public clouds.
You want to consolidate monitoring and enhance security.
You need to recommend a multi-cloud connectivity method that will allow the devices to be protected by Microsoft Defender for loT.
Your solution requires predictable throughput.
Which recommendation should your solution include?

A. Use Bicep to create an Azure ExpressRoute circuit.
B. Set up a private endpoint using the Azure portal.
C. Define a Point-to-Site (P2S) VPN gateway connection.
D. Create a Private Link service with an ARM template.

Answer: A
Explanation
You should recommend using Bicep to create an Azure ExpressRoute circuit. Microsoft Defender for loT can be used to monitor security for Internet of Things (loT) devices. To connect devices from multiple public clouds while ensuring predictable throughput, you should use Azure ExpressRoute. Azure ExpressRoute lets you extend your on-premises and other-cloud networks into the Microsoft cloud over a secure, private connection.
You can create hybrid applications and architectures that include both cloud and on-premises services, and you can use ExpressRoute to bypass the public internet and improve network performance. Bicep is a human-readable language that can be used to deploy Azure resources.
You should not recommend defining a Point-to-Site (P2S) Virtual Private Network (VPN) gateway connection. P2S VPN connections are designed to connect a single endpoint to an Azure virtual network.
You should not recommend creating a Private Link service with an ARM template. A Private Link service is a link to one of your services or resources hosted in Azure.
You should not recommend setting up a private endpoint using the Azure portal. An Azure private endpoint is a network interface that connects you privately and securely to a service powered by Azure Private Link.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**