SC-100 Dumps

Microsoft Cybersecurity Architect

https://www.certleader.com/SC-100-dumps.html

NEW QUESTION 1
- (Exam Topic 1)
You need to recommend a solution to meet the security requirements for the virtual machines. What should you include in the recommendation?

A. an Azure Bastion host
B. a network security group (NSG)
C. just-in-time (JIT) VM access
D. Azure Virtual Desktop

Answer: A

NEW QUESTION 2
- (Exam Topic 2)
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 Area

Segment Microsoft Sentinel workspaces by:	Azure AD tenant
	Enterprise
	Region and Azure AD tenant

Integrate Azure subscriptions by using:	Self-service sign-up user flows for Azure AD B2B
	Self-service sign-up user flows for Azure AD B2C
	The Azure Lighthouse subscription onboarding process

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Segment Microsoft Sentinel workspaces by:	Azure AD tenant
	Enterprise
	Region and Azure AD tenant

Integrate Azure subscriptions by using:	**Self-service sign-up user flows for Azure AD B2B**
	Self-service sign-up user flows for Azure AD B2C
	The Azure Lighthouse subscription onboarding process

NEW QUESTION 3
- (Exam Topic 2)
You need to recommend a multi-tenant and hybrid security solution that meets to the business requirements and the hybrid requirements. What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
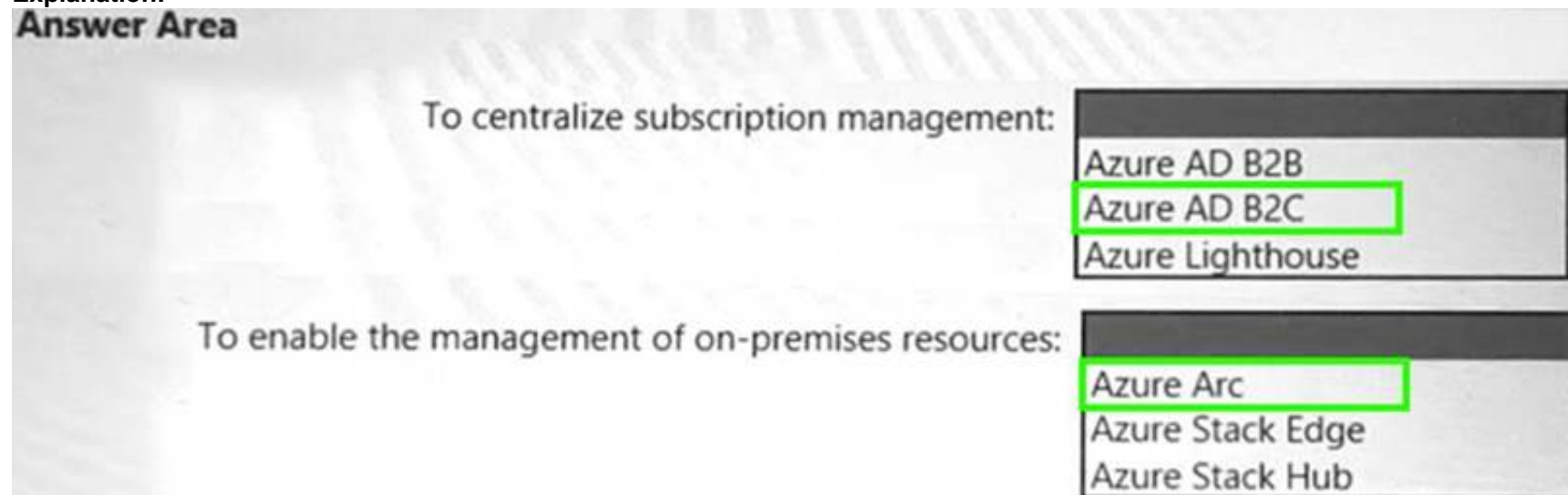
Answer Area

To centralize subscription management:	Azure AD B2B
	Azure AD B2C
	Azure Lighthouse

To enable the management of on-premises resources:	Azure Arc
	Azure Stack Edge
	Azure Stack Hub

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

To centralize subscription management:
- Azure AD B2B
- Azure AD B2C
- Azure Lighthouse

To enable the management of on-premises resources:
- Azure Arc
- Azure Stack Edge
- Azure Stack Hub

NEW QUESTION 4
- (Exam Topic 3)
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: DE

NEW QUESTION 5
- (Exam Topic 3)
You have Microsoft Defender for Cloud assigned to Azure management groups. You have a Microsoft Sentinel deployment.
During the triage of alerts, you require additional information about the security events, including suggestions for remediation. Which two components can you use to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: A

NEW QUESTION 6
- (Exam Topic 3)
You have an Azure subscription that is used as an Azure landing zone for an application. You need to evaluate the security posture of all the workloads in the landing zone. What should you do first?

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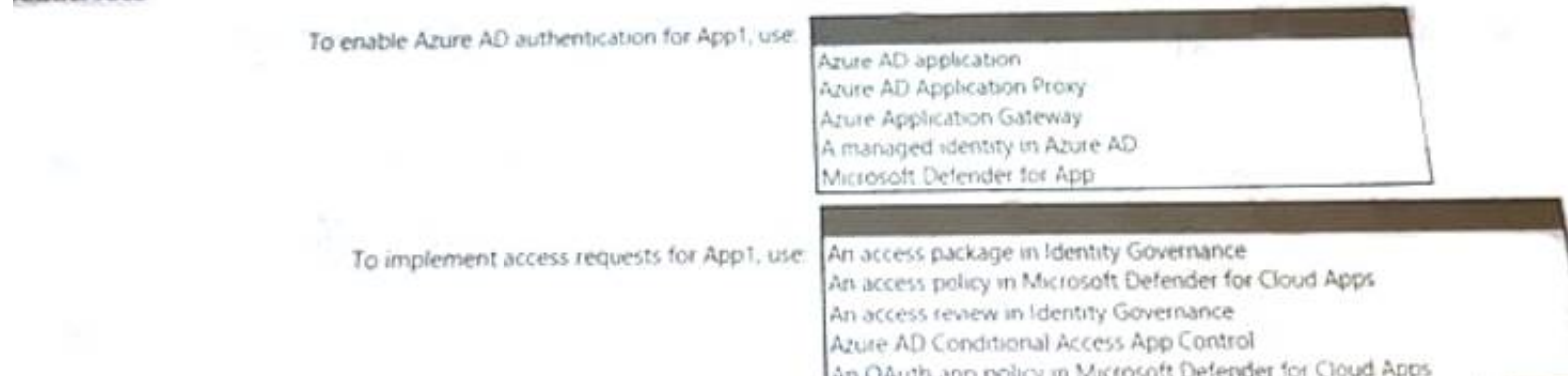
Answer: A

NEW QUESTION 7
- (Exam Topic 3)
You are creating the security recommendations for an Azure App Service web app named App1. App1 has the following specifications:
• Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
• Users will authenticate by using Azure Active Directory (Azure AD) user accounts. You need to recommend an access security architecture for App1.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
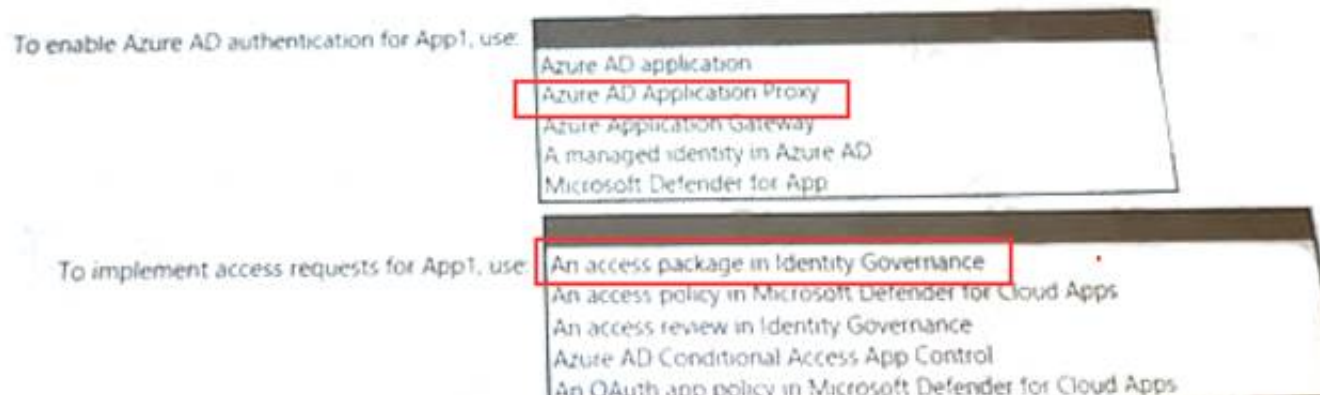
Answer Area

To enable Azure AD authentication for App1, use:
- Azure AD application
- Azure AD Application Proxy
- Azure Application Gateway
- A managed identity in Azure AD
- Microsoft Defender for App

To implement access requests for App1, use:
- An access package in Identity Governance
- An access policy in Microsoft Defender for Cloud Apps
- An access review in Identity Governance
- Azure AD Conditional Access App Control
- An OAuth app policy in Microsoft Defender for Cloud Apps

A. Mastered

B. Not Mastered

Answer: A

Explanation:
Answer Area

To enable Azure AD authentication for App1, use:
- Azure AD application
- **Azure AD Application Proxy**
- Azure Application Gateway
- A managed identity in Azure AD
- Microsoft Defender for App

To implement access requests for App1, use:
- **An access package in Identity Governance**
- An access policy in Microsoft Defender for Cloud Apps
- An access review in Identity Governance
- Azure AD Conditional Access App Control
- An OAuth app policy in Microsoft Defender for Cloud Apps

NEW QUESTION 8
- (Exam Topic 3)
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: BE

NEW QUESTION 9
- (Exam Topic 3)
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government. You need to review the current subscription for NIST 800-53 compliance. What should you do first?
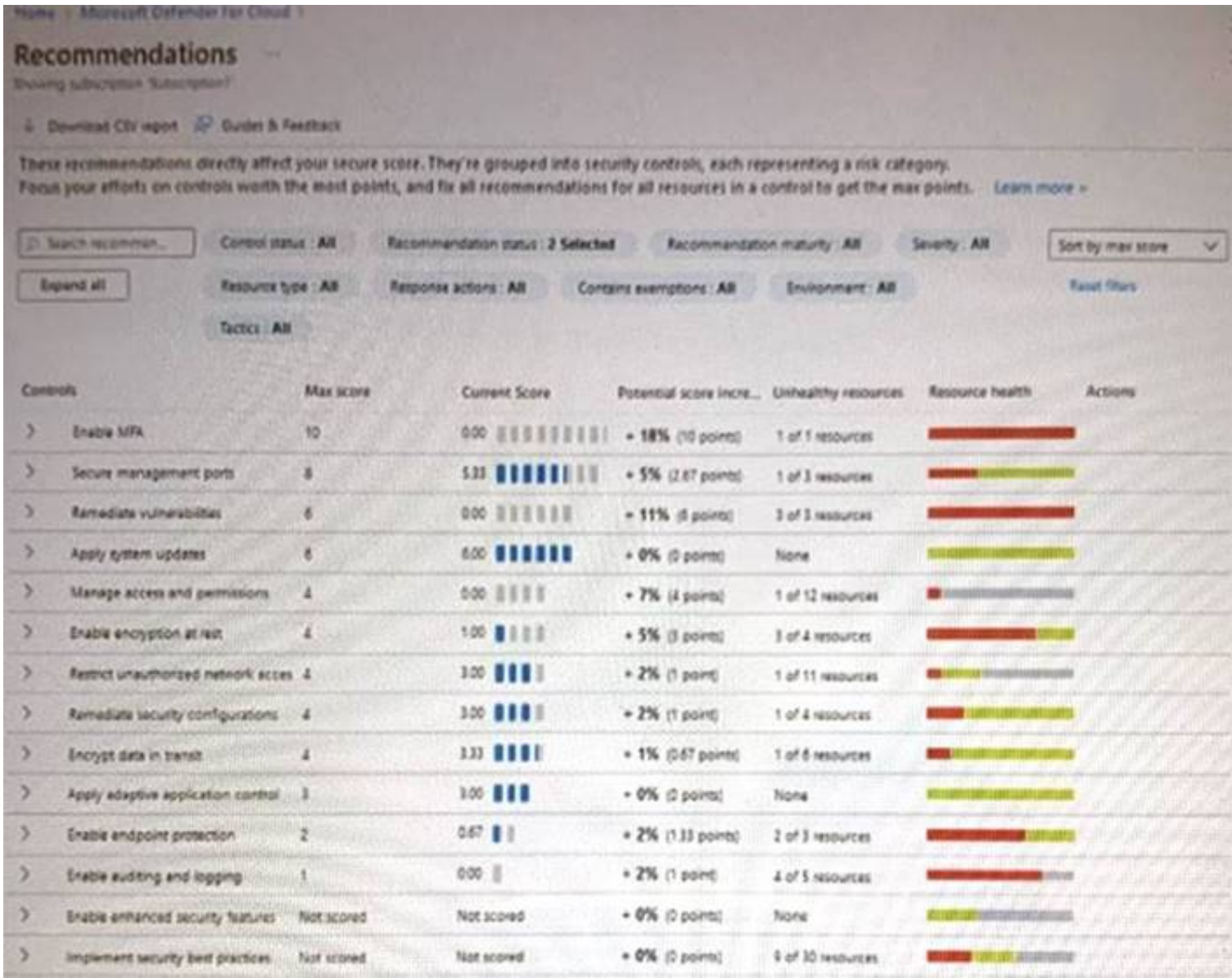
A. From Defender for Cloud, review the Azure security baseline for audit report.
B. From Defender for Cloud, add a regulatory compliance standard.
C. From Defender for Cloud, enable Defender for Cloud plans.
D. From Defender for Cloud, review the secure score recommendations.

Answer: D

NEW QUESTION 10
- (Exam Topic 3)
You open Microsoft Defender for Cloud as shown in the following exhibit.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 10
- (Exam Topic 3)
A customer has a Microsoft 365 E5 subscription and an Azure subscription.
The customer wants to centrally manage security incidents, analyze log, audit activity, and hunt for potential threats across all deployed services.
You need to recommend a solution for the customer. The solution must minimize costs. What should you include in the recommendation?

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

Answer: D

NEW QUESTION 15
- (Exam Topic 3)
A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.

All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.

The customer plans to deploy Microsoft Sentinel.

You need to recommend configurations to meet the following requirements:

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

• Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.

Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

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

Answer: A

NEW QUESTION 19
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DSV You need to recommend an identity security strategy that meets the following requirements:

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

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

The solution must minimize the need to deploy additional infrastructure components. What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 24
- (Exam Topic 3)
Your company is migrating data to Azure. The data contains Personally Identifiable Information (PII). The company plans to use Microsoft Information Protection for the PII data store in Azure. You need to recommend a solution to discover PII data at risk in the Azure resources.

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To connect the Azure data sources to Microsoft Information Protection:

- Azure Purview
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

To connect the Azure data sources to Microsoft Information Protection:

- Azure Purview
- Endpoint data loss prevention
- **Microsoft Defender for Cloud Apps**
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- **Azure Monitor**
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

NEW QUESTION 25
- (Exam Topic 3)
Your company has an on-premise network in Seattle and an Azure subscription. The on-premises network contains a Remote Desktop server.
The company contracts a third-party development firm from France to develop and deploy resources to the virtual machines hosted in the Azure subscription.
Currently, the firm establishes an RDP connection to the Remote Desktop server. From the Remote Desktop connection, the firm can access the virtual machines hosted in Azure by using custom administrative tools installed on the Remote Desktop server. All the traffic to the Remote Desktop server is captured by a firewall, and the firewall only allows specific connections from France to the server.
You need to recommend a modern security solution based on the Zero Trust model. The solution must minimize latency tor developers.
Which three actions should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: BDE

NEW QUESTION 27
- (Exam Topic 3)
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure.
You plan to deploy Azure virtual machines that will run Windows Server.
You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.
How should you recommend enabling each capability? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

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

NEW QUESTION 29
- (Exam Topic 3)
You have a hybrid cloud infrastructure.
You plan to deploy the Azure applications shown in the following table.

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

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

Answer Area

App1:
App2:
- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
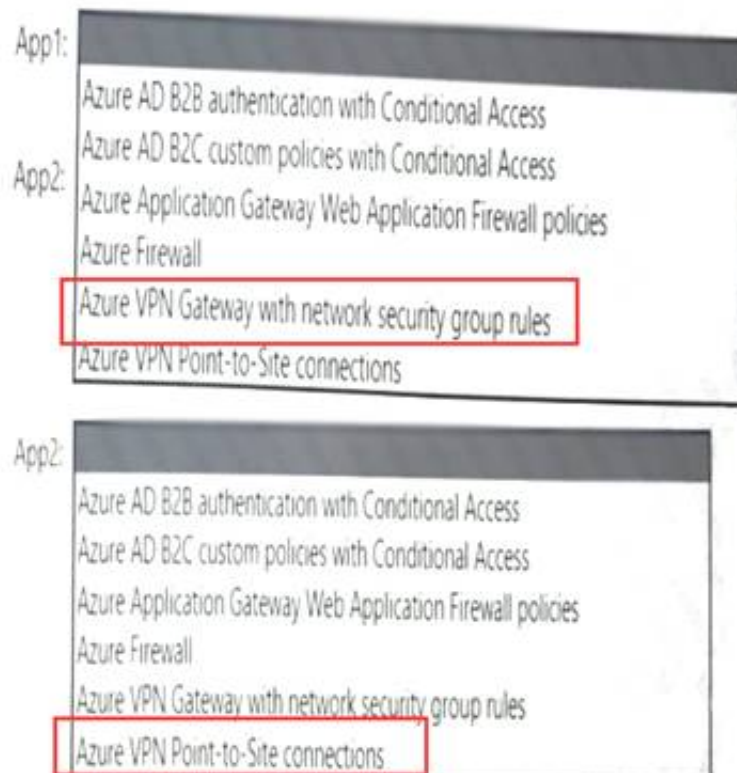- Azure VPN Point-to-Site connections

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 30
- (Exam Topic 3)
Your company is developing a modern application that will run as an Azure App Service web app. You plan to perform threat modeling to identify potential security issues by using the Microsoft Threat Modeling Tool.
Which type of diagram should you create?

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

Answer: C

NEW QUESTION 34
- (Exam Topic 3)
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.
You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.
Which security control should you recommend?

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

Answer: A

NEW QUESTION 37
- (Exam Topic 3)
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

NEW QUESTION 40
- (Exam Topic 3)
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions that allow traffic from the Front Door service tags. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 42
- (Exam Topic 3)
You are designing an auditing solution for Azure landing zones that will contain the following components:
• SQL audit logs for Azure SQL databases
• Windows Security logs from Azure virtual machines
• Azure App Service audit logs from App Service web apps
You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:
• Log all privileged access.
• Retain logs for at least 365 days.
• Minimize costs.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

For the SQL audit logs:
- A Log Analytics workspace
- Azure Application Insights
- Microsoft Defender for SQL
- Microsoft Sentinel

For the Security logs:

For the Security logs:
- A Log Analytics workspace
- Application Insights
- Microsoft Defender for servers
- Microsoft Sentinel

For the App Service audit logs:

For the App Service audit logs:
- A Log Analytics workspace
- Application Insights
- Microsoft Defender for App Service
- Microsoft Sentinel

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

For the SQL audit logs:
- A Log Analytics workspace
- Azure Application Insights
- **Microsoft Defender for SQL**
- Microsoft Sentinel

For the Security logs:

For the Security logs:
- **A Log Analytics workspace**
- Application Insights
- Microsoft Defender for servers
- Microsoft Sentinel

For the App Service audit logs:

For the App Service audit logs:
- A Log Analytics workspace
- Application Insights
- Microsoft Defender for App Service
- **Microsoft Sentinel**

NEW QUESTION 46
- (Exam Topic 3)
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions to allow traffic from the backend IP address of the Front Door instance.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 49
- (Exam Topic 3)
Azure subscription that uses Azure Storage.
The company plans to share specific blobs with vendors. You need to recommend a solution to provide the vendors with secure access to specific blobs without exposing the blobs publicly. The access must be
t\me-Vim\ted. What should you include in the recommendation?

A. Create shared access signatures (SAS).

B. Share the connection string of the access key.
C. Configure private link connections.
D. Configure encryption by using customer-managed keys (CMKs)

Answer: D

NEW QUESTION 50
- (Exam Topic 3)
Your company is developing a new Azure App Service web app. You are providing design assistance to verify the security of the web app.
You need to recommend a solution to test the web app for vulnerabilities such as insecure server configurations, cross-site scripting (XSS), and SQL injection.
What should you include in the recommendation?

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

Answer: A

NEW QUESTION 51
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.
You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort. What should you include in the recommendation?

A. Azure Monitor webhooks
B. Azure Logics Apps
C. Azure Event Hubs
D. Azure Functions apps

Answer: D

NEW QUESTION 54
- (Exam Topic 3)
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?
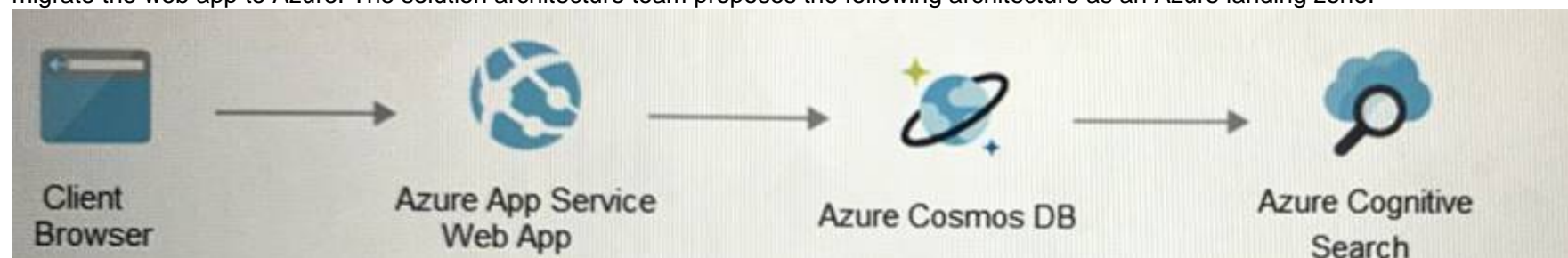
A. insider risk management policies
B. data loss prevention (DLP) policies
C. sensitivity label policies
D. retention policies

Answer: A

NEW QUESTION 59
- (Exam Topic 3)
Your on-premises network contains an e-commerce web app that was developed in Angular and Node.js. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.

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

A. Yes
B. No

Answer: A

NEW QUESTION 61
- (Exam Topic 3)
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: D

NEW QUESTION 63
- (Exam Topic 3)
Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation. You need to recommend a security posture management solution for the following components:
• Azure loT Edge devices
• AWS EC2 instances
Which services should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

For the loT Edge devices:

For the AWS EC2 instances:

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

For the AWS EC2 instances:

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

For the loT Edge devices:

For the AWS EC2 instances:

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

For the AWS EC2 instances:

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

NEW QUESTION 67
- (Exam Topic 3)
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: A

NEW QUESTION 71
......

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SC-100 Exam with Our Prep Materials Via below:

https://www.certleader.com/SC-100-dumps.html