DUMPSQUEEN

Microsoft Cybersecurity Architect

Microsoft SC-100

Version Demo

Total Demo Questions: 10

Total Premium Questions: 130

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Fabrikam, Inc Case Study 1	9
Topic 2, Litware, inc. Case Study 2	9
Topic 3, Mix Questions	112
Total	130

QUESTION NO: 1

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: B D

Explanation:

https://docs.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports https://docs.microsoft.com/en-us/azure/sentinel/notebooks

QUESTION NO: 2 - (DRAG DROP)

You have a Microsoft 365 subscription

You need to recommend a security solution to monitor the following activities:

• User accounts that were potentially compromised

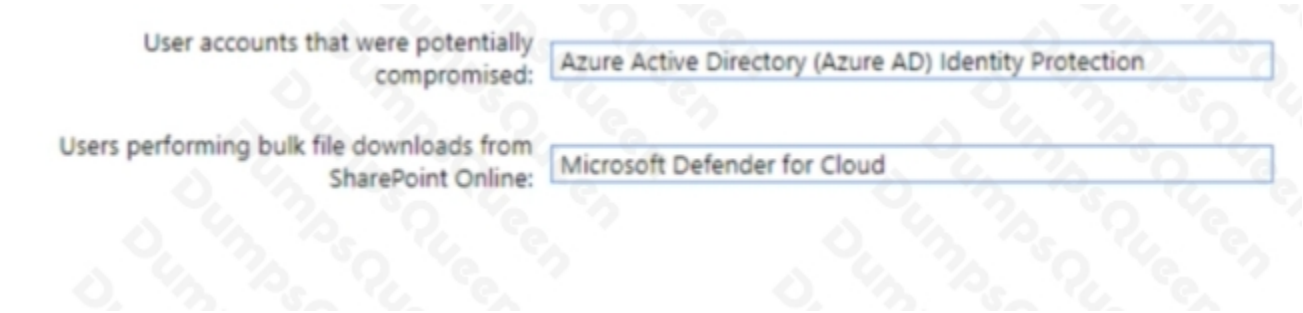
• Users performing bulk file downloads from Microsoft SharePoint Online

What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each Correct selection is worth one Point.

ANSWER:

Explanation:



https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exfiltration

https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users

QUESTION NO: 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

QUESTION NO: 4

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:

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

QUESTION NO: 5

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:

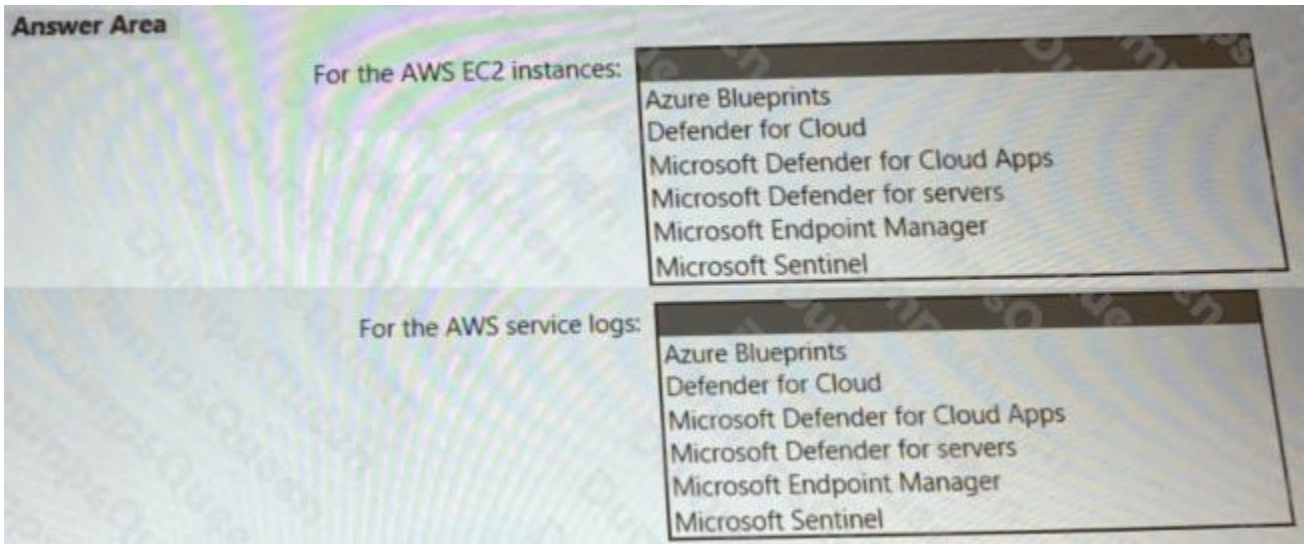
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-mde-phase-3?view=o365-worldwide

QUESTION NO: 6 - (HOTSPOT)

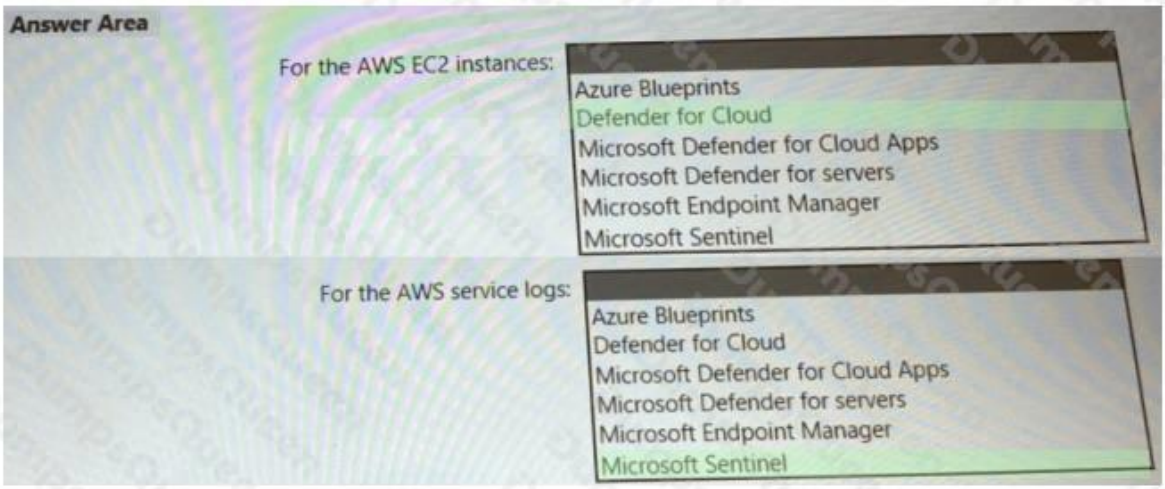
You need to recommend a solution to meet the AWS requirements.

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:



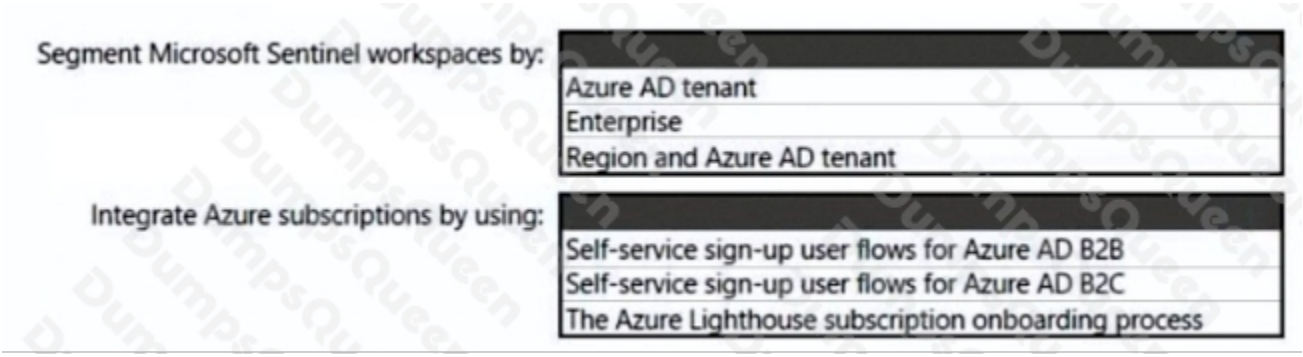
Explanation:

QUESTION NO: 7 - (HOTSPOT)

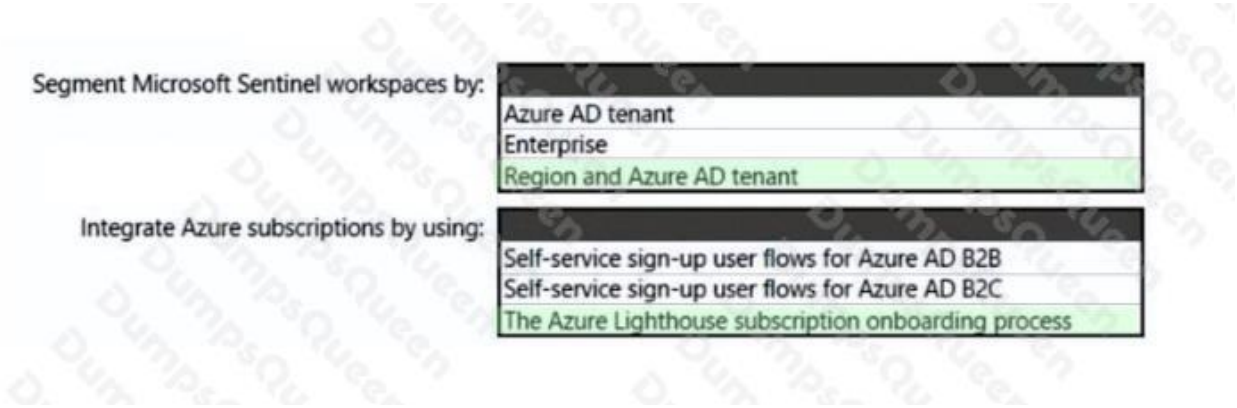
You need to recommend a SIEM and SOAR strategy that meets the hybrid requirements, the Microsoft Sentinel requirements, and the regulatory compliance requirements.

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

NOTE: Each correct selection is worth one point.



ANSWER:



Explanation:

Segment Microsoft Sentinel workspaces by: Region and Azure AD tenant

Lighthouse subscription

QUESTION NO: 8

You are designing the encryption standards for data at rest for an Azure resource

You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.

Solution: For blob containers in Azure Storage, you recommend encryption that uses Microsoft-managed keys within an encryption scope.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

QUESTION NO: 9

You need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table. The solution must meet the Contoso developer requirements.

What should you include in the recommendation?

A. Transparent Data Encryption (TDE)

B. Always Encrypted

C. row-level security (RLS)

D. dynamic data masking

E. data classification

ANSWER: B

Explanation:

https://docs.microsoft.com/en-us/learn/modules/protect-data-transit-rest/4-explain-object-encryption-secure-enclaves

QUESTION NO: 10

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