MS-101$^{Q\&As}$

Microsoft 365 Mobility and Security

Pass Microsoft MS-101 Exam with 100% Guarantee

QUESTION 1

You have a Microsoft 365 E5 tenant.

You plan to deploy a monitoring solution that meets the following requirements:

1.

Captures Microsoft Teams channel messages that contain threatening or violent language.

2.

Alerts a reviewer when a threatening or violent message is identified. What should you include in the solution?

A. Data Subject Requests (DSRs)

B. Insider risk management policies

C. Communication compliance policies

D. Audit log retention policies

Correct Answer: C

QUESTION 2

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft 365 Defender.

Which Microsoft service source will appear on the Incidents page of the Microsoft 365 Defender portal?

A. Azure Information Protection

B. Azure Arc

C. Microsoft Sentinel

D. Microsoft Defender for Identity

Correct Answer: D

Explanation:

Microsoft 365 Defender incidents include all their alerts, entities, and other relevant information, and they group together, and are enriched by, alerts from Microsoft 365 Defender\\'s component services Microsoft Defender for Endpoint,

Microsoft Defender for Identity, Microsoft Defender for Office 365, and Microsoft Defender for Cloud Apps, as well as alerts from other services such as Microsoft Purview Data Loss Prevention (DLP).

Incorrect:

Not B: Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.

Not C: Microsoft Sentinel\\'s Microsoft 365 Defender connector with incident integration allows you to stream all Microsoft 365 Defender incidents and alerts into Microsoft Sentinel, and keeps the incidents synchronized between both portals.

Microsoft 365 Defender incidents include all their alerts, entities, and other relevant information, and they group together, and are enriched by, alerts from Microsoft 365 Defender\\'s component services Microsoft Defender for Endpoint,

Microsoft Defender for Identity, Microsoft Defender for Office 365, and Microsoft Defender for Cloud Apps, as well as alerts from other services such as Microsoft Purview Data Loss Prevention (DLP).

The connector also lets you stream advanced hunting events from all of the above components into Microsoft Sentinel, allowing you to copy those Defender components\\' advanced hunting queries into Microsoft Sentinel, enrich Sentinel alerts

with the Defender components\\' raw event data to provide additional insights, and store the logs with increased retention in Log Analytics.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/connect-microsoft-365-defender

QUESTION 3

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.

Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You upgrade Server1 to Windows Server 2019.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

QUESTION 4

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 deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You configure the Mobility (MDM and MAM) settings.

Does this meet the goal?

A. Yes

B. No

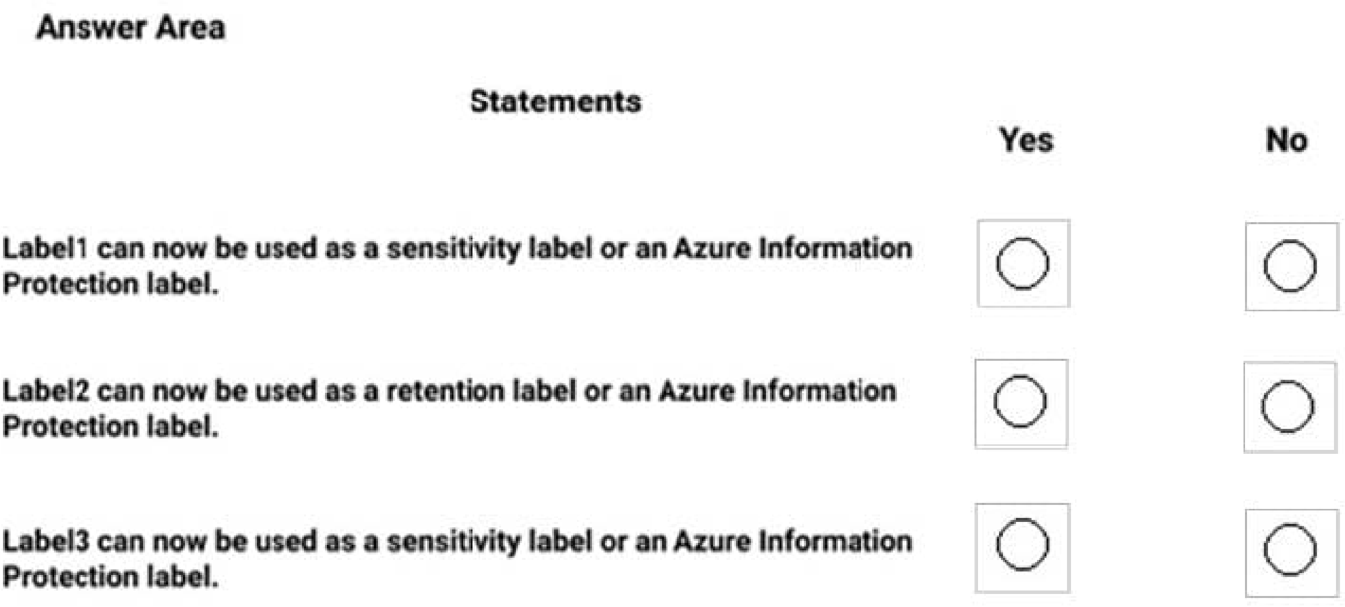
Correct Answer: B

QUESTION 5

HOTSPOT

You have Microsoft 365 subscription.

You create an alert policy as shown in the following exhibit.

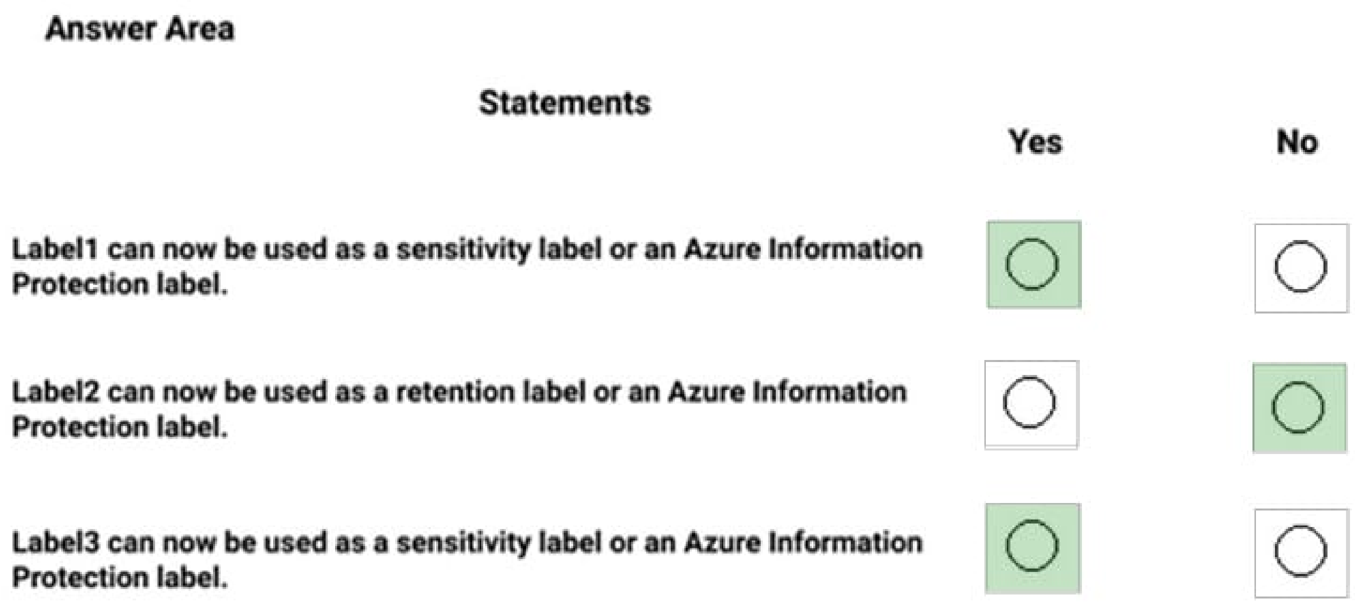


Answer Area

Statements	Yes	No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	○	○
Label2 can now be used as a retention label or an Azure Information Protection label.	○	○
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	○	○

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

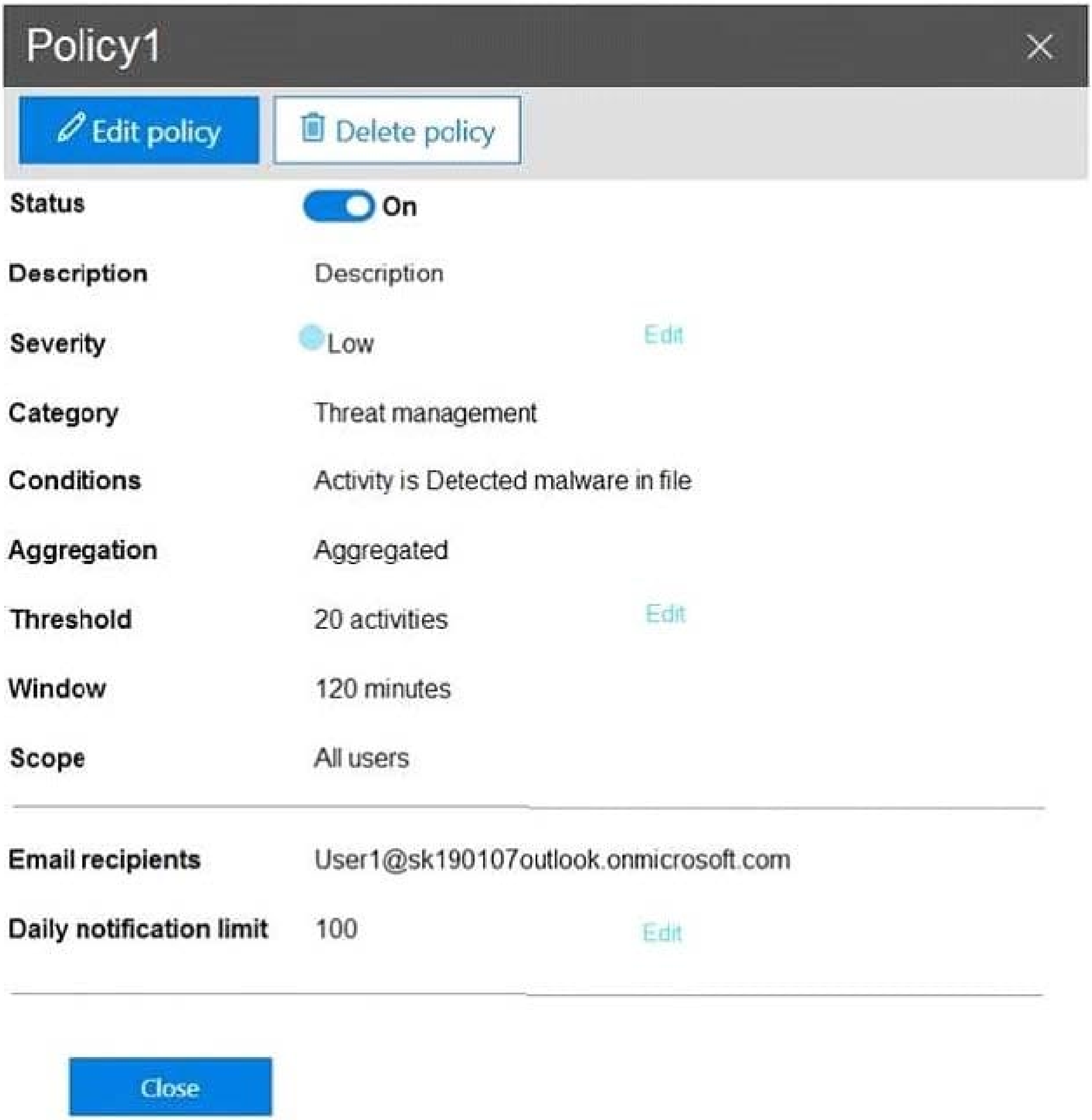
Hot Area:



Answer Area

Statements	Yes	No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	[✓ ○]	○
Label2 can now be used as a retention label or an Azure Information Protection label.	○	[✓ ○]
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	[✓ ○]	○

Correct Answer:



Status	On
Description	Description
Severity	Low
Category	Threat management
Conditions	Activity is Detected malware in file
Aggregation	Aggregated
Threshold	20 activities
Window	120 minutes
Scope	All users
Email recipients	User1@sk190107outlook.onmicrosoft.com
Daily notification limit	100

Note: The Aggregation settings has a 120 minute window

Latest MS-101 Dumps MS-101 VCE Dumps MS-101 Exam Questions