SC-200 Q&As

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/sc-200.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.

You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.

Which two actions should you perform? Each correct answer present part of the solution.

NOTE: Each correct selection is worth one point.

A. Create custom rule based on the Office 365 connector templates.

B. Create a Microsoft incident creation rule based on Azure Security Center.

C. Create a Microsoft Cloud App Security connector.

D. Create an Azure AD Identity Protection connector.

Correct Answer: AB

QUESTION 2

You have a Microsoft Sentinel workspace.

You receive multiple alerts for failed sign in attempts to an account.

You identify that the alerts are false positives.

You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements:

1.

Ensure that failed sign-in alerts are generated for other accounts.

2.

Minimize administrative effort What should do?

A. Create an automation rule.

B. Create a watchlist.

C. Modify the analytics rule.

D. Add an activity template to the entity behavior.

Correct Answer: A

There are two methods for avoiding false positives:

Automation rules create exceptions without modifying analytics rules.

Scheduled analytics rules modifications permit more detailed and permanent exceptions.

Automation rules

Can apply to several analytics rules.

Keep an audit trail. Exceptions prevent incident creation, but alerts are still recorded for audit purposes.

Are often generated by analysts.

Allow applying exceptions for a limited time. For example, maintenance work might trigger false positives that outside the maintenance timeframe would be true incidents.

Incorrect:

Not A: Analytics rules modifications

Allow advanced boolean expressions and subnet-based exceptions.

Let you use watchlists to centralize exception management.

Typically require implementation by Security Operations Center (SOC) engineers.

Are the most flexible and complete false positive solution, but are more complex

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/false-positives

QUESTION 3

DRAG DROP

A company wants to analyze by using Microsoft 365 Apps.

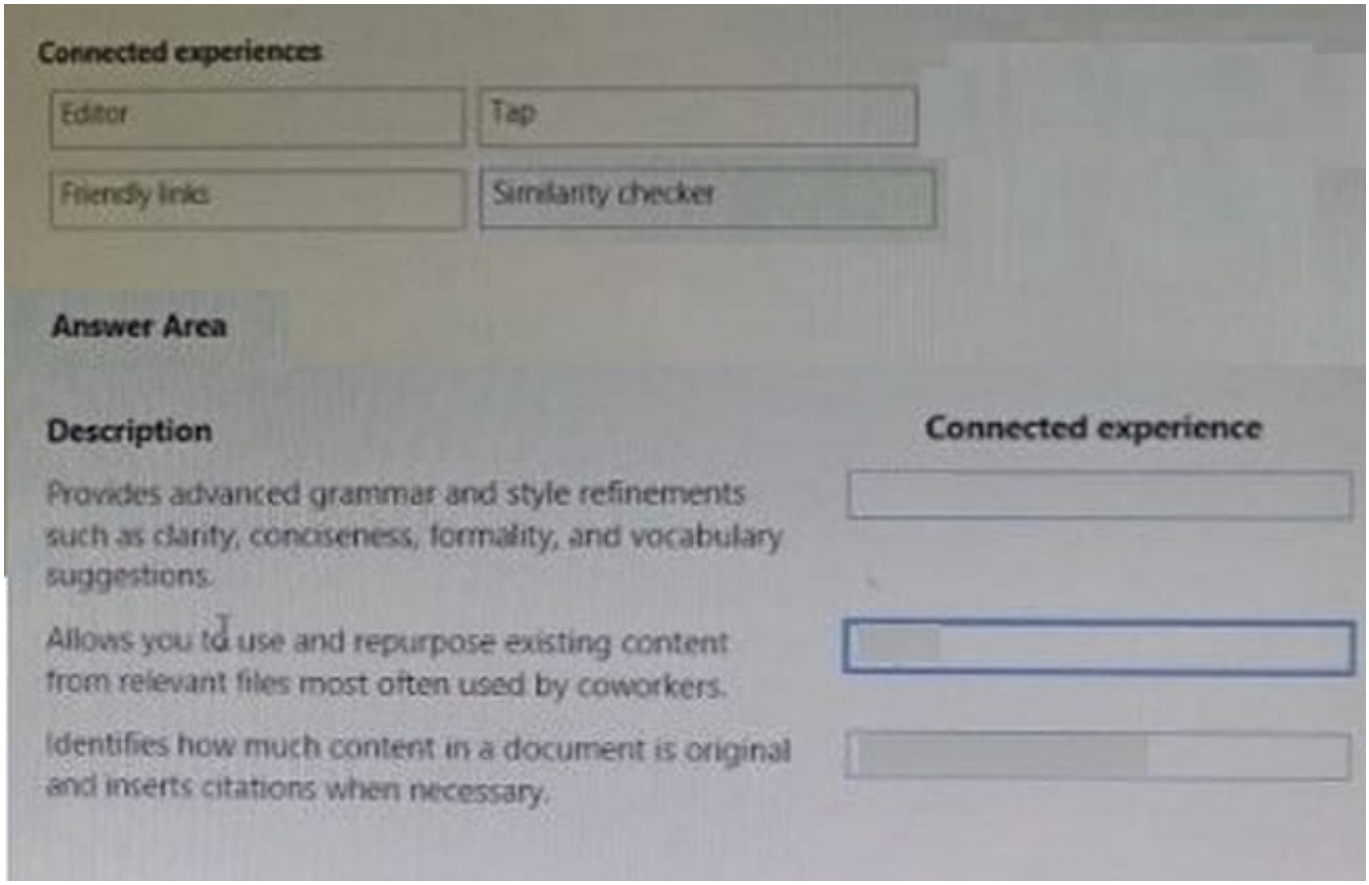
You need to describe the connected experiences the company can use.

Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the

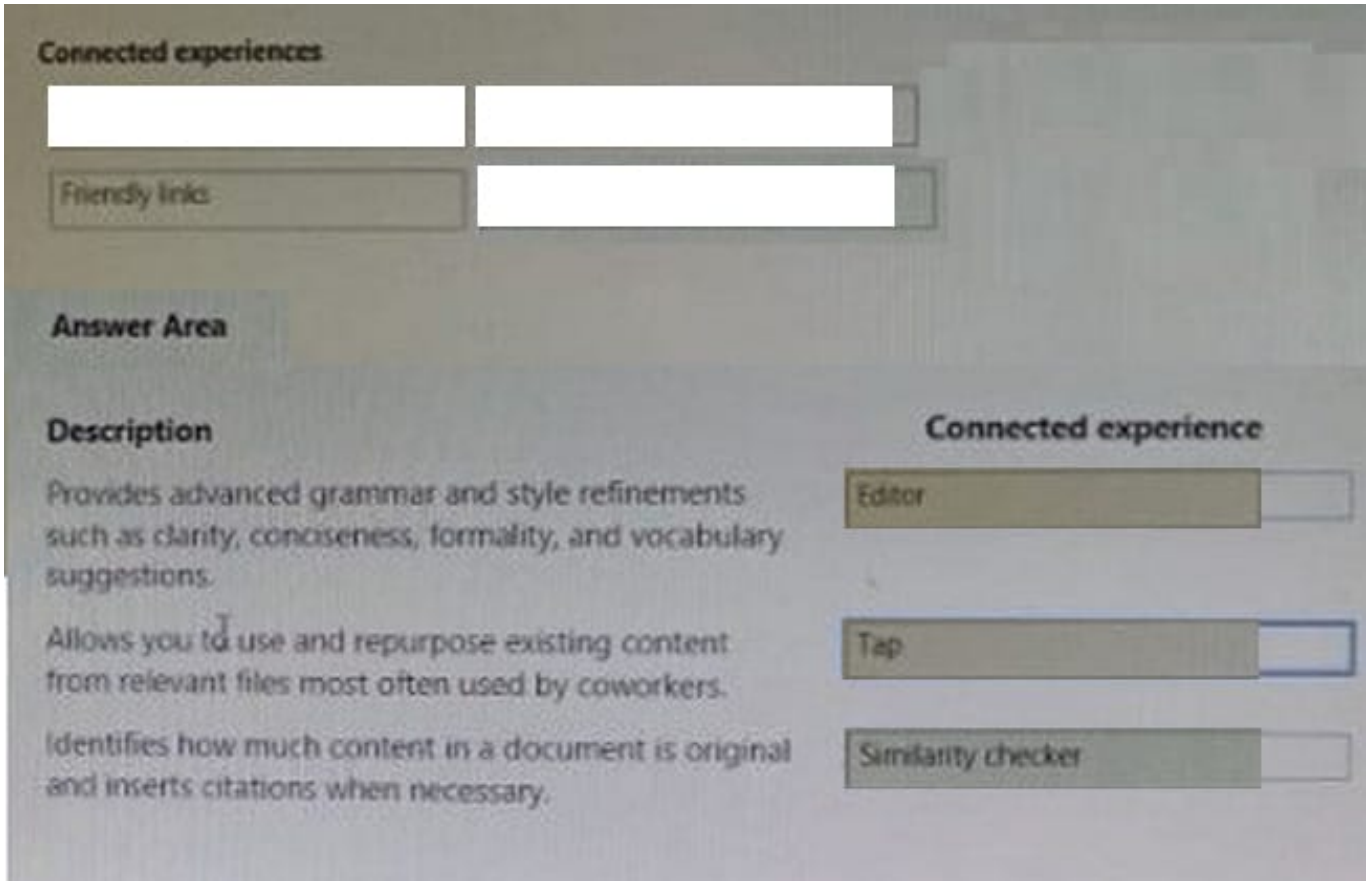
split between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



QUESTION 4

Your company deploys the following services:

1.

Microsoft Defender for Identity

2.

Microsoft Defender for Endpoint

3.

Microsoft Defender for Office 365

You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Microsoft Defender for Endpoint. The solution must use the principle

of least privilege.

Which two roles should assign to the analyst? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. the Compliance Data Administrator in Azure Active Directory (Azure AD)

B. the Active remediation actions role in Microsoft Defender for Endpoint

C. the Security Administrator role in Azure Active Directory (Azure AD)

D. the Security Reader role in Azure Active Directory (Azure AD)

Correct Answer: BD

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide

QUESTION 5

The custom analytics rule which can detect threats in Azure Sentinel stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED. What is the problem?

A. The number of alerts exceeded 10,000 within two minutes.

B. There are connectivity issues between the data sources and Log Analytics.

C. The rule query takes too long to run and times out.

D. Permissions to one of the data sources of the rule query were modified.

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom