SC-900Q&As

Microsoft Security Compliance and Identity Fundamentals

Pass Microsoft SC-900 Exam with 100% Guarantee

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

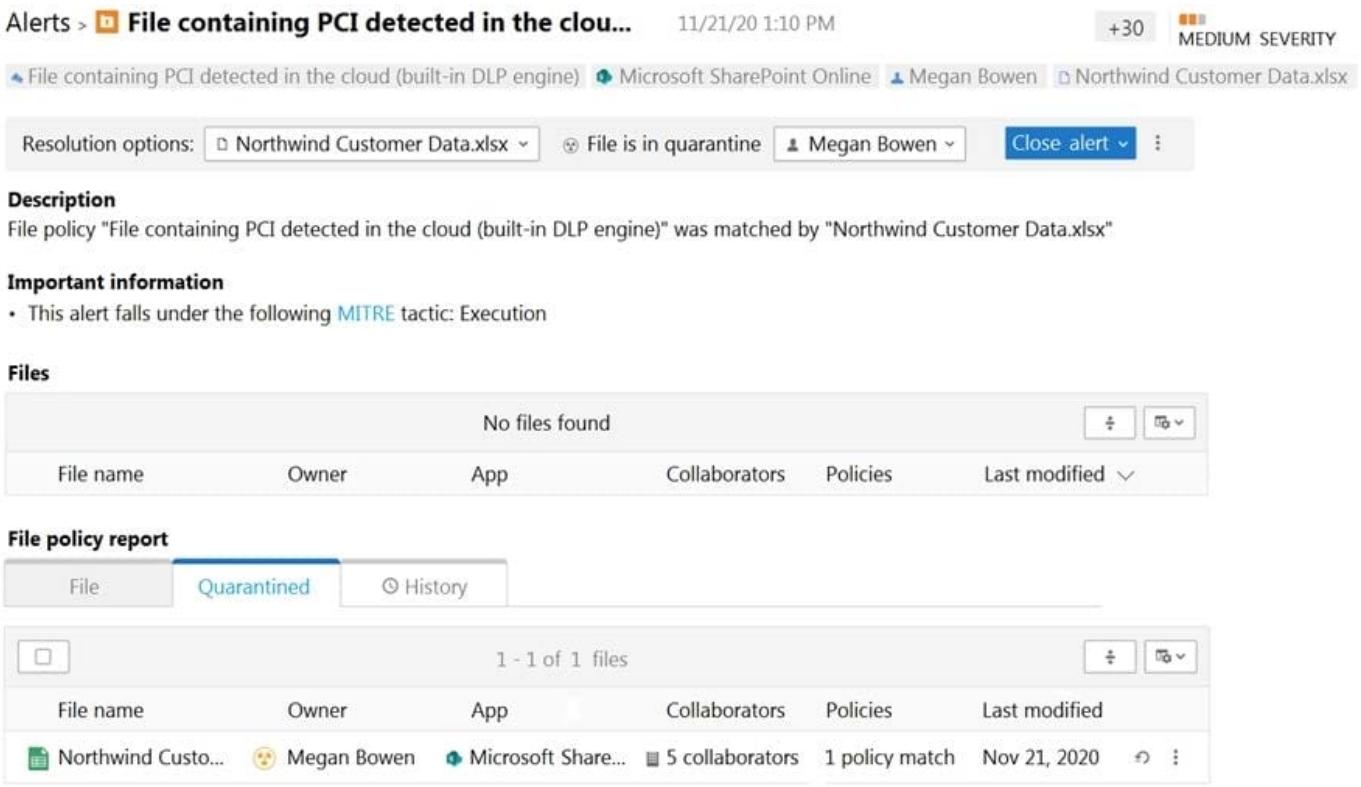
https://www.passapply.com/sc-900.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A user reports that she can no longer access a Microsoft Excel file named Northwind Customer Data.xlsx. From the Cloud App Security portal, you discover the alert shown in the exhibit.



You restore the file from quarantine.

You need to prevent files that match the policy from being quarantined. Files that match the policy must generate an alert.

What should you do?

A. Modify the policy template.

B. Assign the Global reader role to the file owners.

C. Exclude file matching by using a regular expression.

D. Update the governance action.

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies#create-a-new-file-policy

QUESTION 2

Which compliance feature should you use to identify documents that are employee resumes?

A. pre-trained classifiers

B. Content explorer

C. Activity explorer

D. eDiscovery

Correct Answer: A

Microsoft Information Protection - Trainable Classifiers

Leverage user-friendly, pre-trained or trainable Machine Learning classifiers to identify various types of content in your organization.

Microsoft provides a list of classifiers which are pre-trained (based on sample documents like Legal, Finance, Manufacturing, Supply Chain etc.) and use Machine Learning to identify the classification of the documents in user-configured

target locations.

Incorrect:

Not B: How is activity explorer helpful to a compliance administrator?

Activity explorer provides a historical view of activities on your labeled content. The activity information is collected from the Microsoft 365 unified audit logs, transformed, and made available in the Activity explorer UI.

Creating a custom trainable classifier first involves giving it samples that are human picked and positively match the category.

Not C: Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases.

Not D: Content explorer shows a current snapshot of the items that have a sensitivity label, a retention label or have been classified as a sensitive information type in your organization.

Reference: https://www.infotechtion.com/post/microsoft-trainable-classifiers

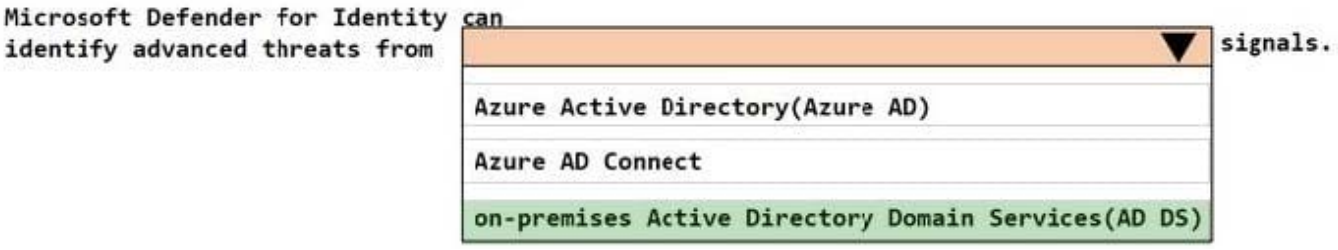
QUESTION 3

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

Correct Answer:



Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

QUESTION 4

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point

Hot Area:

Correct Answer:

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	◯	◯
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	◯	◯
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	◯	◯

Box 1: Yes

From Microsoft Defender for cloud you can enable Microsoft Defender for Storage to get alerted about suspicious activities related to your storage resources.

Note: Microsoft Defender for Storage is an Azure-native layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit your storage accounts.

Defender for Storage continually analyzes the telemetry stream generated by the Azure Blob Storage and Azure Files services. When potentially malicious activities are detected, security alerts are generated. These alerts are displayed in

Microsoft Defender for Cloud, together with the details of the suspicious activity along with the relevant investigation steps, remediation actions, and security recommendations.

Box 2: No Box 3: Yes

Microsoft Defender for Cloud is a solution for cloud security posture management (CSPM) and cloud workload protection (CWP) that finds weak spots across your cloud configuration, helps strengthen the overall security posture of your environment, and can protect workloads across multicloud and hybrid environments from evolving threats.

Microsoft Defender for Servers is one of the plans provided by Microsoft Defender for Cloud\\'s enhanced security features. Defender for Servers protects your Windows and Linux machines in Azure, AWS, GCP, and on-premises.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction

QUESTION 5

HOTSPOT For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point

Hot Area:

	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	○	○
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	○	○
Hunting provides you with the ability to identify security threats before an alert is triggered.	○	○

Correct Answer:

	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	○	●
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	●	○
Hunting provides you with the ability to identify security threats before an alert is triggered.	●	○

Box 1: No

Microsoft Sentinel data connectors are available for non-Microsoft services like Amazon Web Services.

Box 2: Yes

Once you have connected your data sources to Microsoft Sentinel, you can visualize and monitor the data using the Microsoft Sentinel adoption of Azure Monitor Workbooks, which provides versatility in creating custom dashboards. While the

Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to create interactive reports with Azure Monitor Workbooks. Microsoft Sentinel allows you to create custom workbooks across your data, and also

comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

Box 3: Yes

To help security analysts look proactively for new anomalies that weren\\'t detected by your security apps or even by your scheduled analytics rules, Microsoft Sentinel\\'s built-in hunting queries guide you into asking the right questions to find

issues in the data you already have on your network.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/data-connectors-reference

https://docs.microsoft.com/en-us/azure/sentinel/monitor-your-data

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