# SC-900 Q&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**

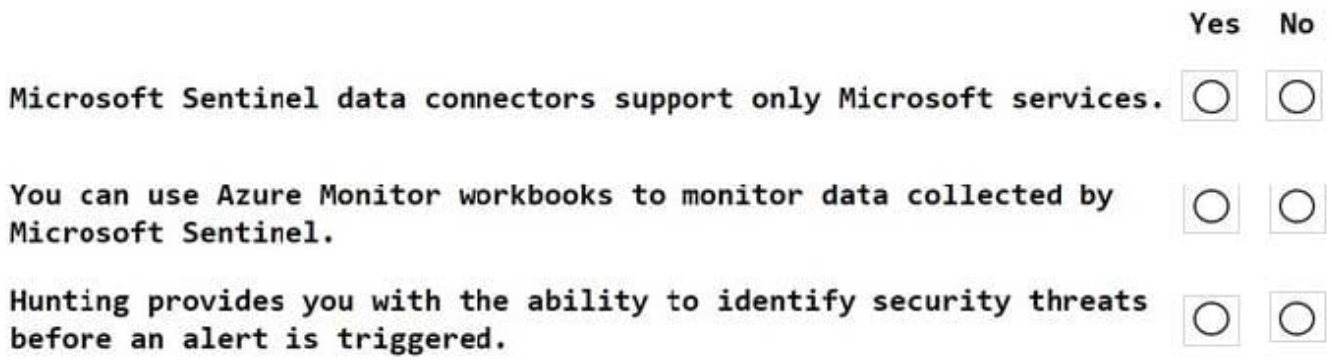
100% Passing Guarantee
100% Money Back Assurance

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

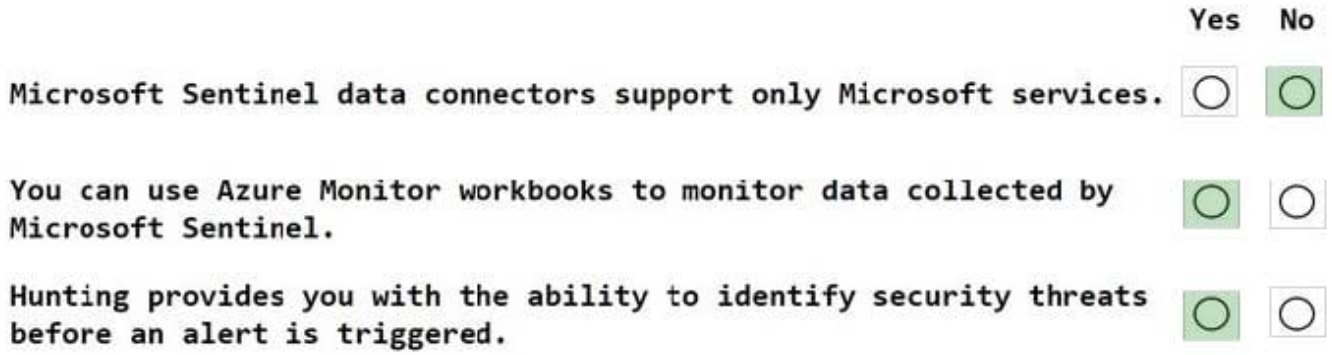
**QUESTION 1**

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:




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

**QUESTION 2**

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:

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| Network security groups (NSGs) can deny inbound traffic from the internet. | ○ | ○ |
| Network security groups (NSGs) can deny outbound traffic to the internet. | ○ | ○ |
| Network security groups (NSGs) can filter traffic based on IP address, protocol, and port. | ○ | ○ |

Correct Answer:

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| Network security groups (NSGs) can deny inbound traffic from the internet. | ○ | ○ |
| Network security groups (NSGs) can deny outbound traffic to the internet. | ○ | ○ |
| Network security groups (NSGs) can filter traffic based on IP address, protocol, and port. | ○ | ○ |

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

**QUESTION 3**

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:

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| Microsoft Purview provides sensitive data classification. | ○ | ○ |
| Microsoft Sentinel is a data lifecycle management solution. | ○ | ○ |
| Microsoft Purview can only discover data that is stored in Azure. | ○ | ○ |

Correct Answer:

## Answer Area

| Statements | Yes | No |
|---|---|---|
| Microsoft Purview provides sensitive data classification. | ○ | ○ |
| Microsoft Sentinel is a data lifecycle management solution. | ○ | ○ |
| Microsoft Purview can only discover data that is stored in Azure. | ○ | ○ |

Box 1: Yes

Microsoft Purview allows you to apply sensitivity labels to assets, enabling you to classify and protect your data.

Box 2: Yes

Microsoft Sentinel content is Security Information and Event Management (SIEM) content that enables customers to ingest data, monitor, alert, hunt, investigate, respond, and connect with different products, platforms, and services in

Microsoft Sentinel.

Content sources for Microsoft Sentinel content and solutions

Each piece of content or solution has one of the following content sources:

Content hub - Content or solutions deployed by the content hub that support lifecycle management

Custom - Content or solutions you\\'ve customized in your workspace

Gallery content- Content or solutions from the gallery that don\\'t support lifecycle management

Repositories - Content or solutions from a repository connected to your workspace

Box 3: No

Microsoft Purview provides a unified data governance solution to help manage and govern your on-premises, multicloud, and software as a service (SaaS) data.

Reference:

https://docs.microsoft.com/en-us/azure/purview/create-sensitivity-label

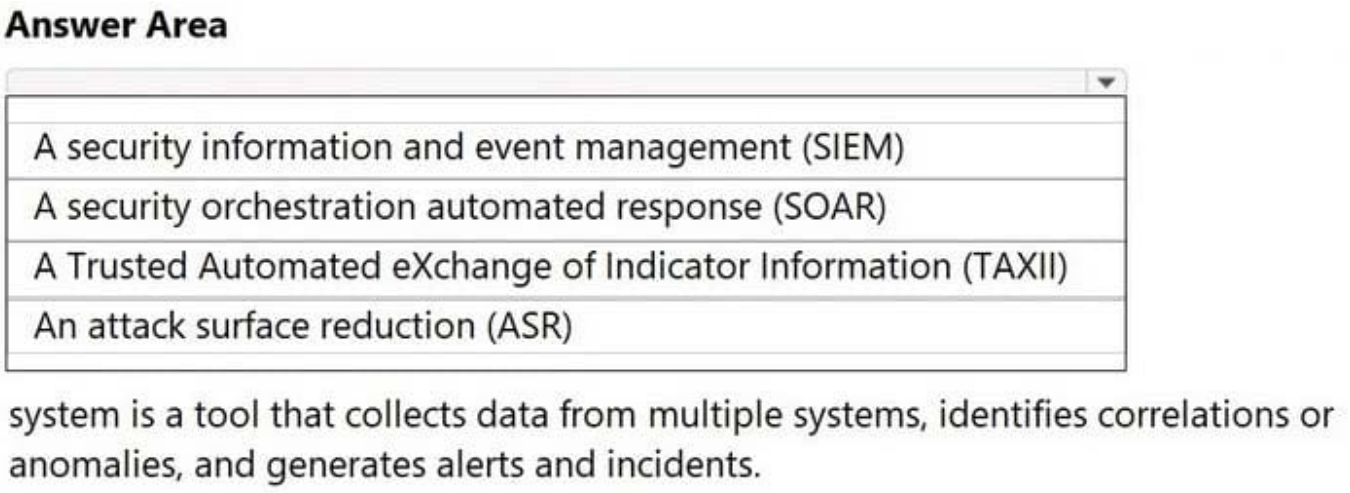
https://docs.microsoft.com/en-us/azure/sentinel/sentinel-solutions

**QUESTION 4**

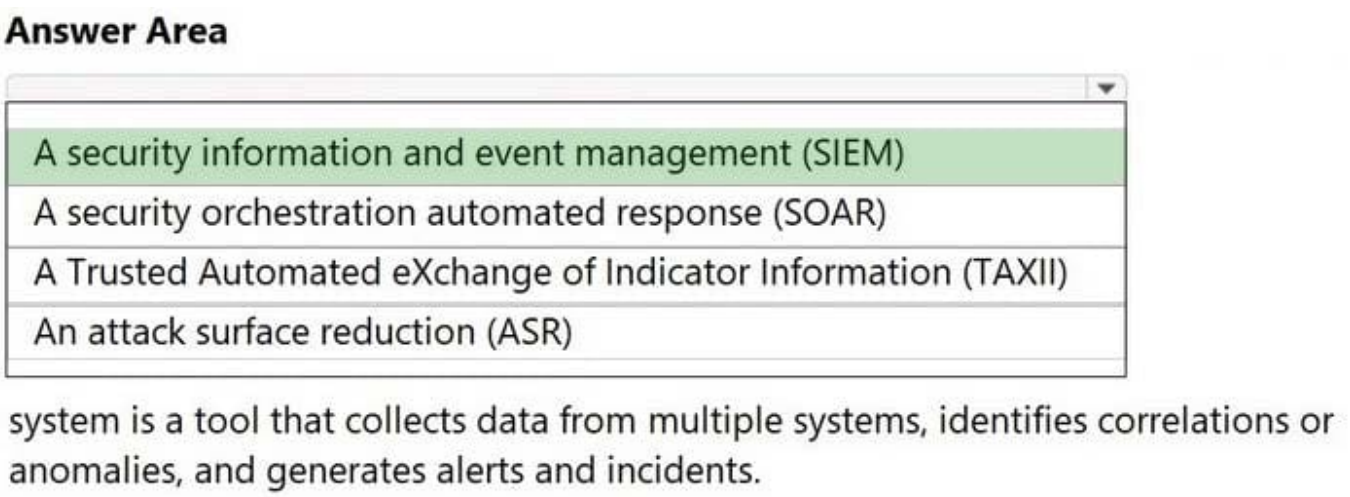
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:




Correct Answer:




**QUESTION 5**

What do you use to provide real-time integration between Azure Sentinel and another security source?

A. Azure AD Connect

B. a Log Analytics workspace

C. Azure Information Protection

D. a connector

Correct Answer: D

To on-board Azure Sentinel, you first need to connect to your security sources. Azure Sentinel comes with a number of connectors for Microsoft solutions, including Microsoft 365 Defender solutions, and Microsoft 365 sources, including Office 365, Azure AD, Microsoft Defender for Identity, and Microsoft Cloud App Security, etc.

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