

Braindumps SC-200 Pdf & Popular SC-200 Exams

Questions & Answers PDF

Page 1

Microsoft

SC-200 Exam

Microsoft Security Operations Analyst



Thank you for Downloading SC-200 exam PDF Demo

You can Buy Latest SC-200 Full Version Download

<https://www.certkillers.net/Exam/SC-200>

<https://www.certkillers.net>

What's more, part of that Pass4sureCert SC-200 dumps now are free: https://drive.google.com/open?id=1LZk6M4WK_MPDxKV1SJqZanePDol_joVt

The Microsoft Security Operations Analyst (SC-200) practice test software also keeps a record of attempts, keeping users informed about their progress and allowing them to improve themselves. This feature makes it easy for SC-200 desktop-based practice exam software users to focus on their mistakes and overcome them before the original attempt. Overall, the Windows-based Microsoft Security Operations Analyst (SC-200) practice test software has a user-friendly interface that facilitates candidates to prepare for the Microsoft Security Operations Analyst (SC-200) exam without facing technical issues.

The Microsoft SC-200 pdf questions learning material provided to the customers from Pass4sureCert is in three different formats. The first format is PDF format which is printable and portable. It means it can be accessed from tablets, laptops, and smartphones to prepare for the Microsoft Security Operations Analyst exam. The Microsoft SC-200 Pdf Format can be used offline, and candidates can even prepare for it in the classroom or library by printing questions or on their smart devices.

>> **Braindumps SC-200 Pdf** <<

Popular SC-200 Exams, Latest SC-200 Test Format

We provide 3 versions of our Microsoft Security Operations Analyst exam torrent and they include PDF version, PC version, APP online version. Each version's functions and using method are different and you can choose the most convenient version which is suitable for your practical situation. For example, the PDF version is convenient for you to download and print our SC-200 test

torrent and is suitable for browsing learning. If you use the PDF version you can print our SC-200 Guide Torrent on the papers and it is convenient for you to take notes. You learn our SC-200 test torrent at any time and place. The PC version can stimulate the real exam's environment, is stalled on the Windows operating system and runs on the Java environment. You can use it at any time to test your own exam stimulation tests scores and whether you have mastered our SC-200 guide torrent or not.

Microsoft Security Operations Analyst Sample Questions (Q195-Q200):

NEW QUESTION # 195

You need to create an advanced hunting query to investigate the executive team issue.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
| where TimeStamp > ago(2d)
| summarize activityCount = [dropdown] by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

Answer:

Explanation:

```
| where TimeStamp > ago(2d)
| summarize activityCount = [dropdown] by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

Explanation:

```
| where TimeStamp > ago(2d)
| summarize activityCount = [dropdown] by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

NEW QUESTION # 196

You have a Microsoft Sentinel workspace named sws1.

You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.

You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the following requirements:

- * Minimize administrative effort.
- * Use the principle of least privilege.

How should you configure the credentials? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Configure the connector to use:

Role to assign to the credentials:

Answer:

Explanation:

Answer Area

Configure the connector to use:

Role to assign to the credentials:

Explanation:

Answer Area

Configure the connector to use:

Role to assign to the credentials:

NEW QUESTION # 197

You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled. You need to identify all the changes made to sensitivity labels during the past seven days. What should you use?

- A. the Incidents blade of the Microsoft 365 Defender portal
- B. the Explorer settings on the Email & collaboration blade of the Microsoft 365 Defender portal
- C. the Alerts settings on the Data Loss Prevention blade of the Microsoft 365 compliance center
- D. Activity explorer in the Microsoft 365 compliance center

Answer: D

Explanation:

Labeling activities are available in Activity explorer.

For example:

Sensitivity label applied

This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label.

It is captured at the time of save in Office native applications and web applications.

It is captured at the time of occurrence in Azure Information protection add-ins.

Upgrade and downgrade labels actions can also be monitored via the Label event type field and filter.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer-available-events?view=o365-worldwide>

NEW QUESTION # 198

You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

ACTIONS

Answer Area

Create a rule by using the Changes to Amazon VPC settings rule template

From Analytics in Azure Sentinel, create a Microsoft incident creation rule

Add the Amazon Web Services connector

Set the alert logic

From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query

Select a Microsoft security service

Add the Syslog connector



Answer:

Explanation:

Answer Area

Add the Azure Web Services connector

From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query

Set the alert logic

- 1 - Add the Azure Web Services connector
- 2 - From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query
- 3 - Set the alert logic

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom>

NEW QUESTION # 199

HOTSPOT

You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.

How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

```

resources": [
  {
    "type": "Microsoft.Automation" /automations",
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameters('location')]",
    "properties": {
      "description": "[format(variables('description'), '{0}', parameters('subscriptionId'))]",
      "isEnabled": true,
      "actions": [
        {
          "actionType": "LogicApp",
          "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters('appName'))]",
          "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'), parameters('resourceGroupName'), 'Microsoft.Automation' /workflows/triggers', parameters('appName'), 'manual'), '2019-05-01').value]"
        }
      ]
    }
  }
]

```

Answer:

Explanation:

Answer Area



```

resources": [
  {
    "type": "Microsoft.Automation" /automations",
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameters('location')]",
    "properties": {
      "description": "[format(variables('description'), '{0}', parameters('subscriptionId'))]",
      "isEnabled": true,
      "actions": [
        {
          "actionType": "LogicApp",
          "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters('appName'))]",
          "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'), parameters('resourceGroupName'), 'Microsoft.Automation' /workflows/triggers', parameters('appName'), 'manual'), '2019-05-01').value]"
        }
      ]
    }
  }
]

```

Section: [none]

Explanation/Reference:

<https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert>

NEW QUESTION # 200

.....

Our PDF version of SC-200 training materials is legible to read and remember, and support printing request. Software version of

Popular SC-200 Exams: <https://www.pass4surecert.com/Microsoft/SC-200-practice-exam-dumps.html>

Change the large list settings, Specifies IP address of remote site router, Now, make a risk-free investment in training and certification with the help of SC-200 updated study pdf.

Microsoft SC-200 Exam is Easy with Our High-quality Braindumps SC-200 Pdf: Microsoft Security Operations Analyst Surely

Pass4sureCert helps you in many ways to enhance SC-200 your chances of success by improving all the weak portions of your studies.

- P.S. Free & New SC-200 dumps are available on Google Drive shared by Pass4sureCert: https://drive.google.com/open?id=1LZk6M4WK_MPDxKV1SJqZanePDol_joVt