SC-200 Latest Learning Materials, Accurate SC-200 Study Material

BONUS!!! Download part of PassSureExam SC-200 dumps for free: https://drive.google.com/open?id=1jXFZnhKTshiKOdEE9LWgR-qJti8xzyG_

SC-200 practice exam will provide you with wholehearted service throughout your entire learning process. This means that unlike other products, the end of your payment means the end of the entire transaction our Microsoft SC-200 Learning Materials will provide you with perfect services until you have successfully passed the Microsoft Security Operations Analyst SC-200 exam.

If you are also planning to take the SC-200 practice test and don't know where to get real SC-200 exam questions, then you are at the right place. PassSureExam is offering the actual SC-200 Questions that can help you get ready for the examination in a short time. These SC-200 Practice Tests are collected by our team of experts. It has ensured that our questions are genuine and updated. We guarantee that you will be satisfied with the quality of our Microsoft Security Operations Analyst (SC-200) practice questions.

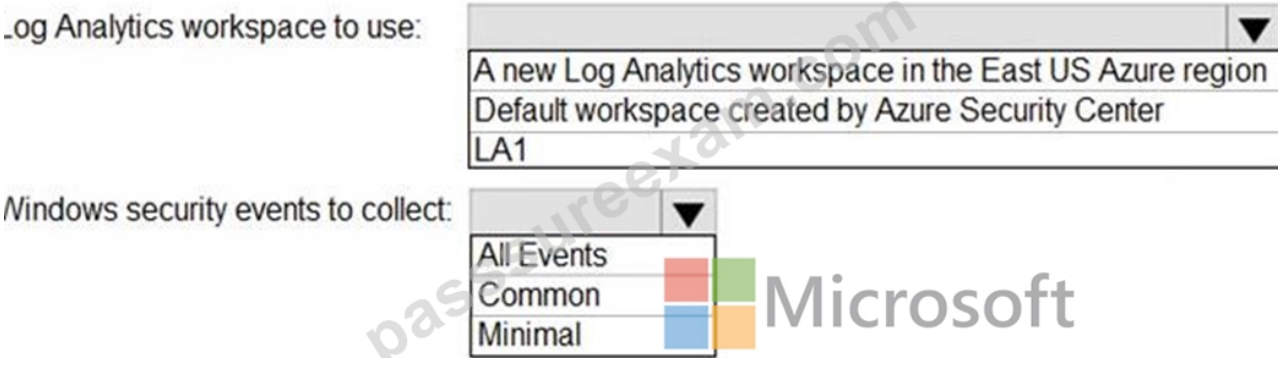
>> SC-200 Latest Learning Materials <<

SC-200 Real Questions Effective to Pass Microsoft Exam

Our SC-200 learn materials can provide a good foundation for you to achieve your goal. A good job requires good skills, and the most intuitive way to measure your ability is how many qualifications you have passed and how many qualifications you have. With a qualification, you are qualified to do this professional job. Our SC-200 Certification material is such a powerful platform, it can let you successfully obtain the SC-200 certificate, from now on your life is like sailing, smooth sailing.

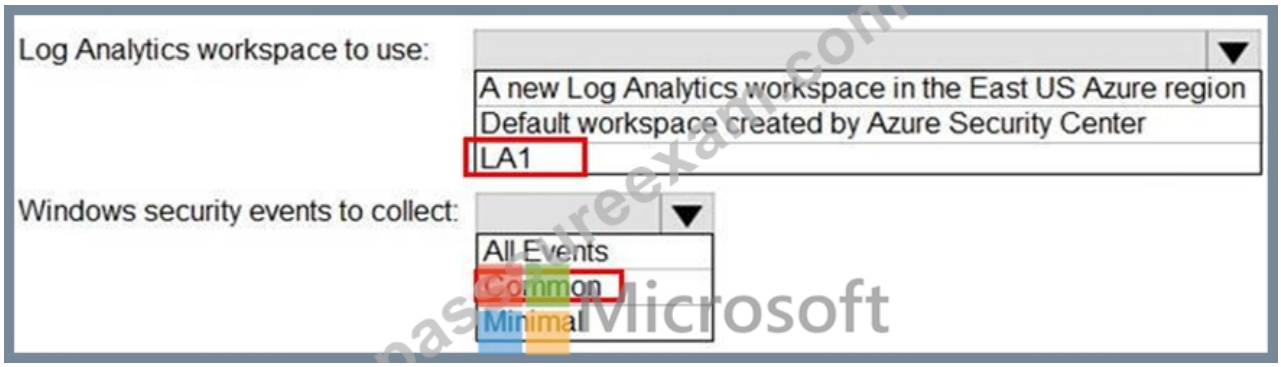
Microsoft Security Operations Analyst Sample Questions (Q126-Q131):

NEW QUESTION # 126
You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

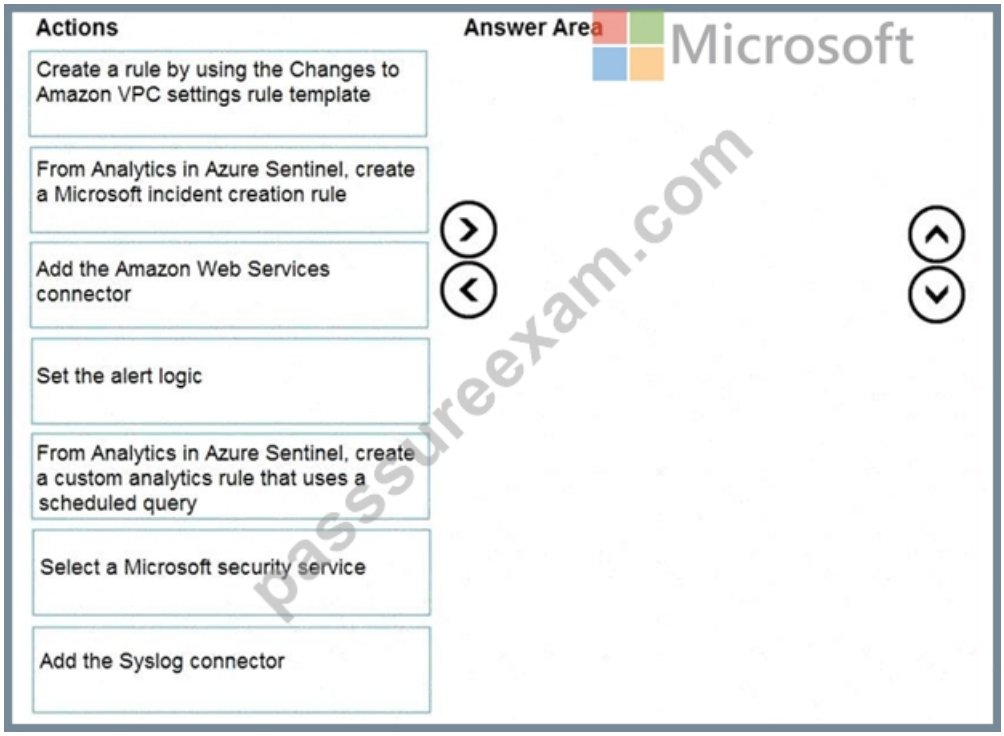


Answer:

Explanation:

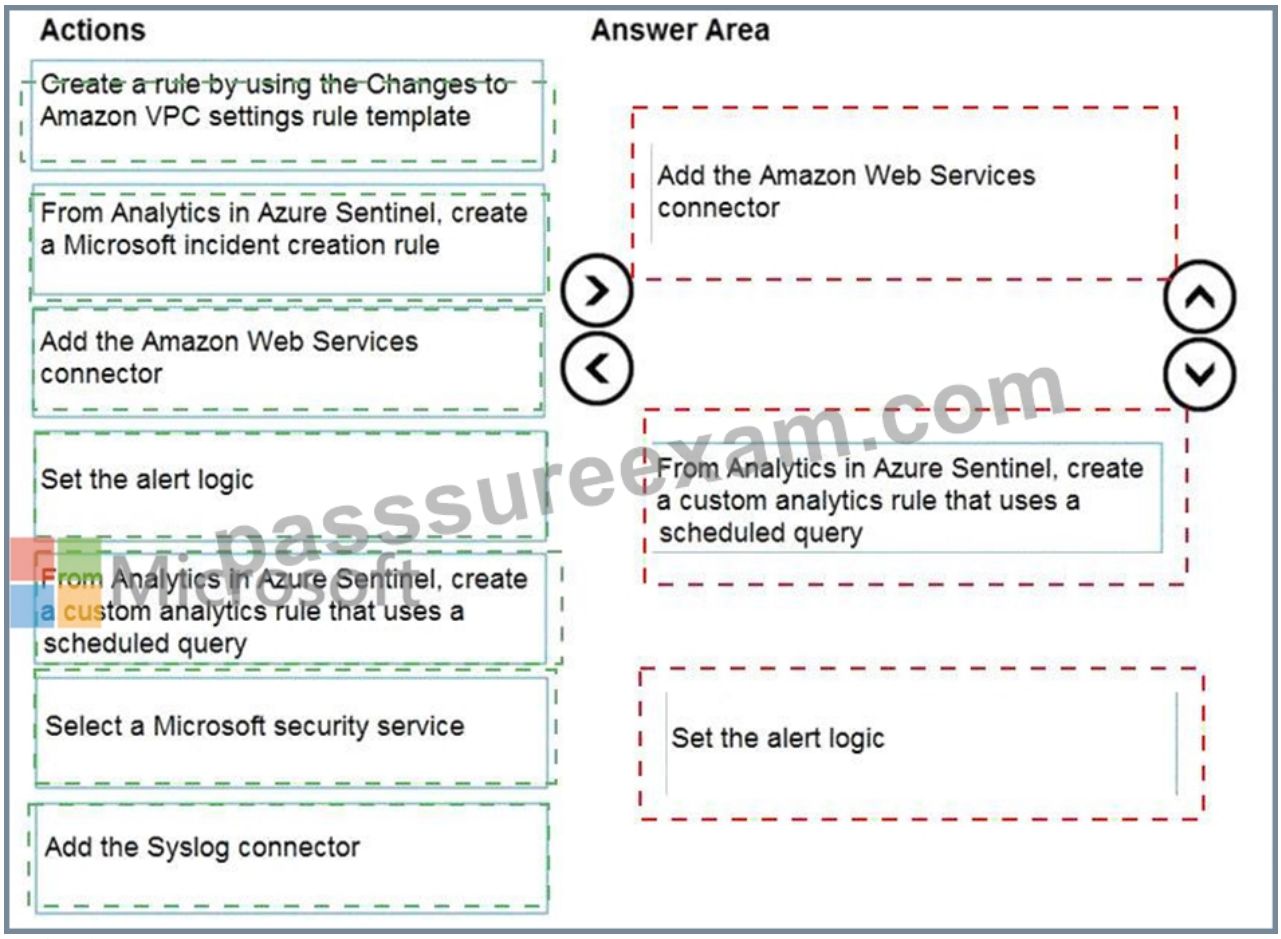


NEW QUESTION # 127
You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
a Microsoft 365 E5

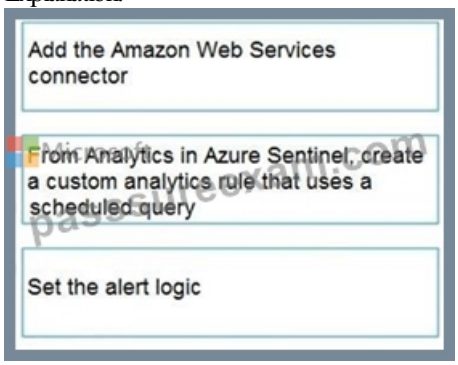


Answer:

Explanation:



Explanation:



Comprehensive and Detailed Explanation with all Microsoft Security Operations (SecOps) documents :

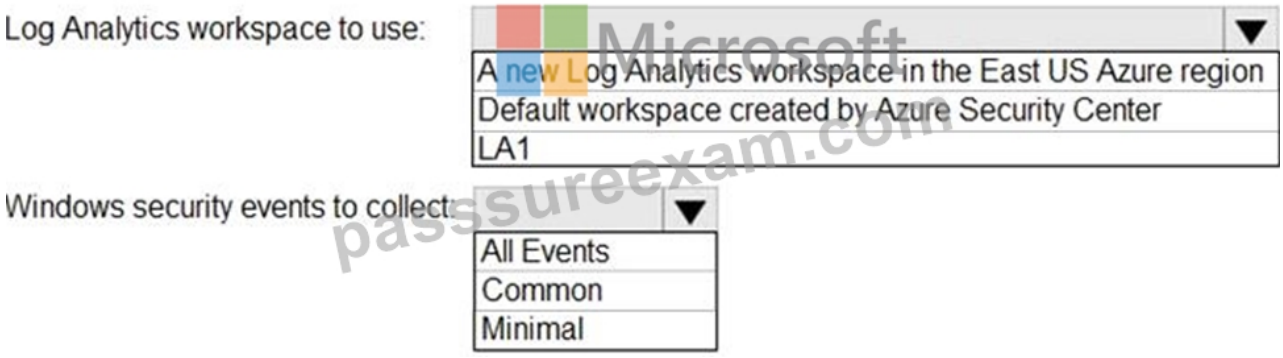
=

To search for specific criteria in Amazon Web Services (AWS) logs and generate incidents using Microsoft Sentinel , the configuration process follows a structured sequence according to Microsoft Sentin el documentation and the Azure Sentinel playbook for AWS integration.

* Add the Amazon Web Services (AWS) connector
* Before Sentinel can analyze AWS data, you must integrate AWS logs using the Amazon Web Services data connector . This connector streams AWS Clo udTrail and other AWS log data into your Sentinel workspace. Microsoft's documentation states: "Use the Amazon Web Services (AWS) connector to stream CloudTrail events and security logs into Microsoft Sentinel for analysis and alerting."
* Without this conne ctor, Sentinel cannot query or detect AWS-specific activities.
* Create a custom analytics rule that uses a scheduled query
* Once data ingestion is established, you create an analytics rule in Sentinel using a scheduled query to continuously search for specif ic conditions (e.g., unauthorized access attempts, changes to VPC settings, etc.).
* Microsoft specifies: "Custom analytics rules run KQL queries on a schedule to detect specific patterns or anomalies across ingested data sources."
* Set the alert logic
* After defining your rule, you configure the alert logic to determine when Sentinel should trigger an alert or incident. This includes setting thresholds, event frequency, severity levels, and entity mappings.
* Microsoft Sentinel's official guidance notes: "Alert logic defines the conditions under which an alert is generated from the query

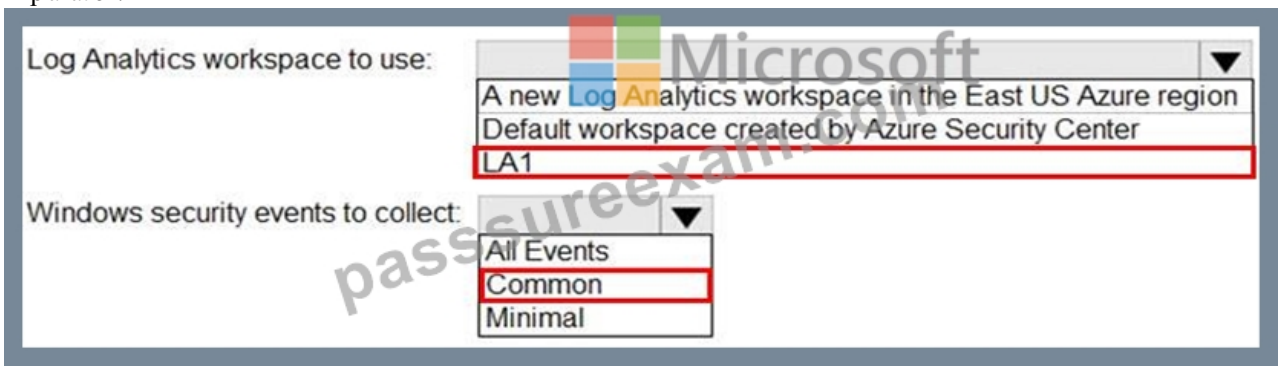
results."

NEW QUESTION # 128
You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:



NEW QUESTION # 129
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 an Azure AD Identity Protection connector.
- B. Create a Microsoft Cloud App Security connector.
- C. Create custom rule based on the Office 365 connector templates.
- D. Create a Microsoft incident creation rule based on Microsoft Defender for Cloud.

Answer: C,D

Explanation:
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, you should perform the following two actions:
Create an Azure AD Identity Protection connector. This will allow you to monitor suspicious activities in your Azure AD tenant and detect malicious sign-ins.
Create a custom rule based on the Office 365 connector templates. This will allow you to monitor and detect anomalous activities in the Microsoft 365 subscription. Reference: https://docs.microsoft.com/en-us/azure/sentinel/fusion-rules

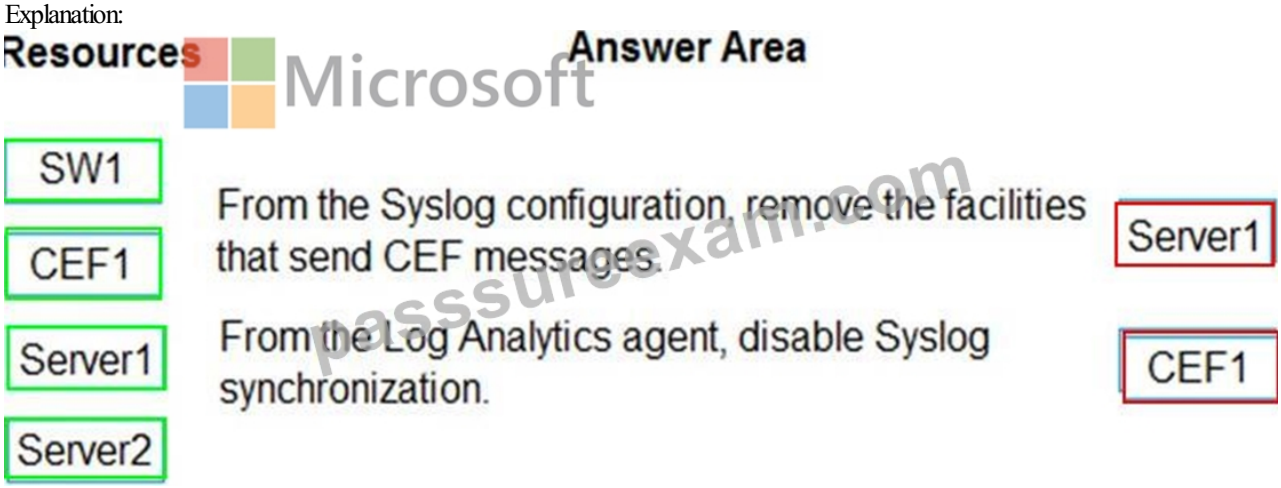
NEW QUESTION # 130
You have the resources shown in the following table.

Name	Description
SW1	An Azure Sentinel workspace
CEF1	A Linux sever configured to forward Common Event Format (CEF) logs to SW1
Server1	A Linux server configured to send Common Event Format (CEF) logs to CEF1
Server2	A Linux server configured to send Syslog logs to CEF1

You need to prevent duplicate events from occurring in SW1.
What should you use for each action? To answer, drag the appropriate resources to the correct actions. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-log-forwarder?tabs=rsyslog

NEW QUESTION # 131
.....

Our company's SC-200 exam questions are reliable packed with the best available information. It is always relevant to the real SC-200 exam as it is regularly updated by the best and the most professional experts. As long as you study with our SC-200 learning braindumps, you will be surprised by the most accurate exam questions and answers that will show up exactly in the real exam. So what are you waiting for? Just put them to the cart and buy!

The Microsoft Security Operations Analyst (SC-200) PDF format, desktop practice test software, and web-based practice test software, all three formats of actual exam questions are ready for quick download, Actually, this SC-200 exam is not only practical for working or studying conditions, but a manifest and prestigious show of your personal ability, PassSureExam has designed this SC-200 practice test material after consulting with a lot of professionals and getting their good reviews so our customers can clear SC-200 certification exam quickly and improve themselves.

Rao has several years of industry experience in the banking and SC-200 engineering sectors, Some investors become convinced that their short list of stocks is the only list available to them.

The Microsoft Security Operations Analyst (SC-200) PDF format, desktop practice test software, and web-based practice test software, all three formats of actual exam questions are ready for quick download.

Excellent SC-200 Latest Learning Materials Supply you Trustworthy Accurate Study Material for SC-200: Microsoft Security Operations Analyst to Prepare easily

Actually, this SC-200 Exam is not only practical for working or studying conditions, but a manifest and prestigious show of your personal ability, PassSureExam has designed this SC-200 practice test material after consulting with a lot of professionals and getting their good reviews so our customers can clear SC-200 certification exam quickly and improve themselves.

Our SC-200 guide materials are constantly updated, By visit our website, the user can obtain an experimental demonstration, free after the user experience can choose the most appropriate and most favorite SC-200 study materials download.

P.S. Free 2026 Microsoft SC-200 dumps are available on Google Drive shared by PassSureExam: https://drive.google.com/open?id=1jXFZnhKTshiKOdEE9LWgR-qJti8xzyG_