2026 High-quality New SC-200 Study Guide | Microsoft Security Operations Analyst 100% Free Lab Questions

2025 Latest ExamCost SC-200 PDF Dumps and SC-200 Exam Engine Free Share: https://drive.google.com/open?id=1pQgeE3X33fZpWXphBO5TkjB6UcEq8272

In order to make your exam easier for every candidate, our SC-200 exam prep is capable of making you test history and review performance, and then you can find your obstacles and overcome them. In addition, once you have used this type of SC-200 exam question online for one time, next time you can practice in an offline environment. The SC-200 test torrent also offer a variety of learning modes for users to choose from, which can be used for multiple clients of computers and mobile phones to study online, as well as to print and print data for offline consolidation. Therefore, for your convenience, more choices are provided for you, we are pleased to suggest you to choose our SC-200 Exam Question for your exam.

To earn the Microsoft Security Operations Analyst certification, individuals must pass the SC-200 Exam. SC-200 exam is a rigorous and comprehensive assessment of an individual's knowledge and skills in Microsoft security technologies. It requires a deep understanding of Microsoft Defender for Endpoint, Azure Sentinel, Microsoft Cloud App Security, and other Microsoft security tools.

>> New SC-200 Study Guide <<

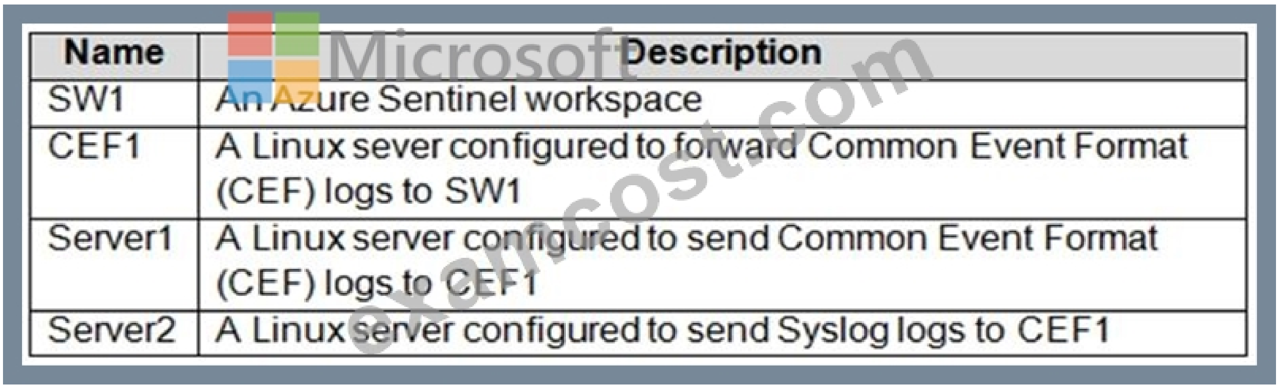
Lab Microsoft SC-200 Questions, Test SC-200 Questions Pdf

Please don't worry about the purchase process because it's really simple for you. The first step is to select the SC-200 test guide, choose your favorite version, the contents of different versionof our SC-200 exam questions are the same, but different in their ways of using. We have three different versions for you to choose: PDF, Soft and APP versions. The second step: fill in with your email and make sure it is correct, because we send our SC-200 learn tool to you through the email. Later, if there is an update, our system will automatically send you the latest SC-200 version.

Microsoft SC-200 Exam covers a variety of topics, including threat protection, incident response, and governance, risk, and compliance (GRC). Professionals who pass the exam are equipped with the skills to identify and respond to security threats, develop and implement security policies and procedures, and ensure compliance with industry regulations. Microsoft Security Operations Analyst certification is an essential credential for security analysts who are looking to advance their careers and demonstrate their expertise to potential employers.

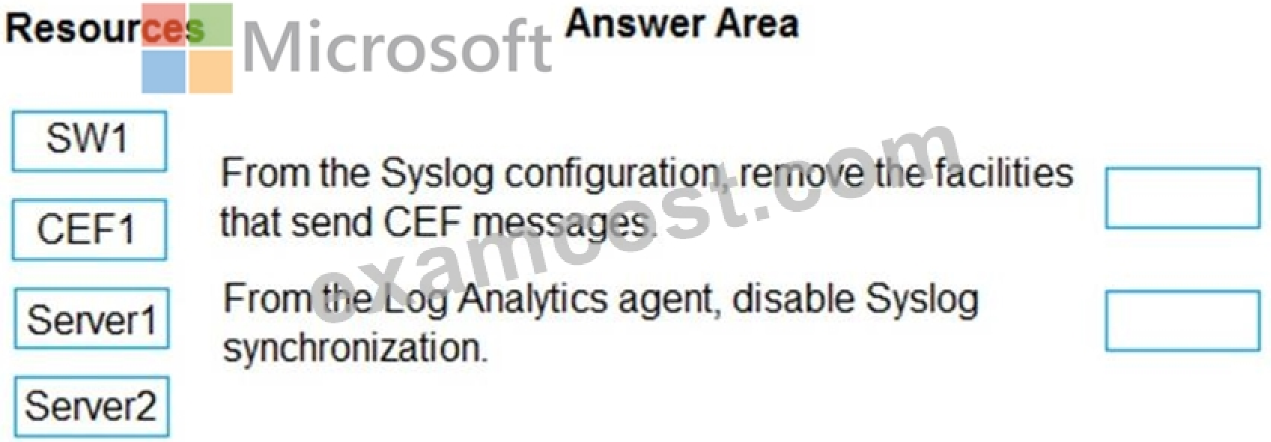
Microsoft Security Operations Analyst Sample Questions (Q285-Q290):

NEW QUESTION # 285
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.



Resources

SW1

CEF1

Server1

Server2

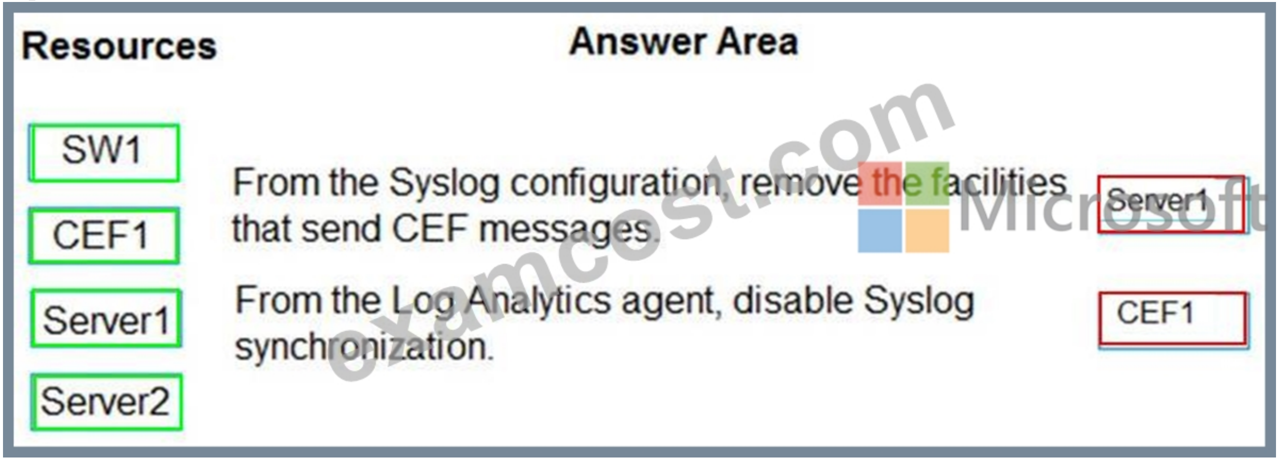
Answer Area

From the Syslog configuration, remove the facilities that send CEF messages.

From the Log Analytics agent, disable Syslog synchronization.

Answer:

Explanation:



Resources

SW1

CEF1

Server1

Server2

Answer Area

From the Syslog configuration, remove the facilities that send CEF messages. Server1

From the Log Analytics agent, disable Syslog synchronization. CEF1

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

NEW QUESTION # 286
You have an Azure subscription that contains a user named User1.
User1 is assigned an Azure Active Directory Premium Plan 2 license
You need to identify whether the identity of User1 was compromised during the last 90 days.
What should you use?

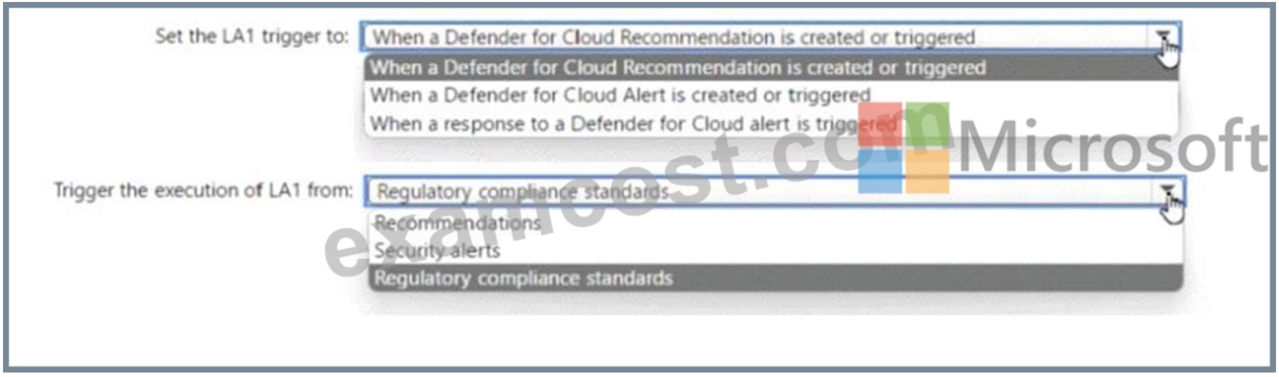
- A. the risk detections report
- B. Identity Secure Score recommendations

- C. the risky sign-ins report
- D. the risky users report

Answer: D

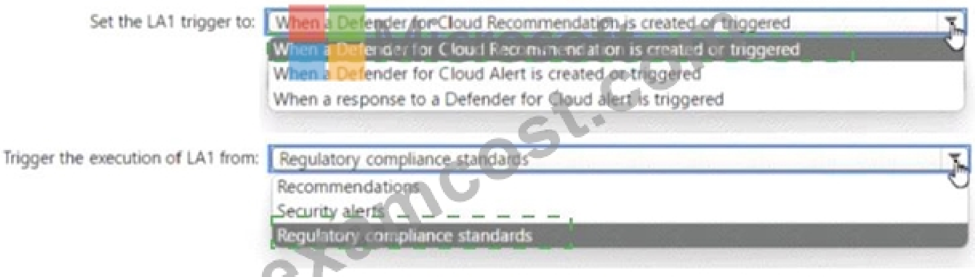
Explanation:
The Risky users report in Microsoft Entra ID Protection provides visibility into users whose identities might have been compromised. It shows risk levels, risk states, and when risk detections occurred - allowing you to investigate activity for the last 90 days.
The Risk detections report lists individual risk events but not overall user risk status, while risky sign-ins report only sign-in attempts, not the cumulative user risk.
Thus, to determine whether User1's identity was compromised during the last 90 days, use the risky users report.

NEW QUESTION # 287
You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You create an Azure logic app named LA1.
You plan to use LA1 to automatically remediate security risks detected in Defenders for Cloud.
You need to test LA1 in Defender for Cloud.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

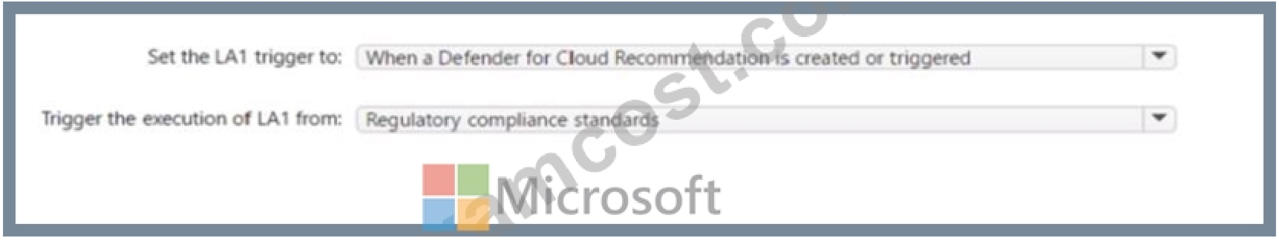

Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Alert is created or triggered
When a response to a Defender for Cloud alert is triggered
Trigger the execution of LA1 from: Regulatory compliance standards
Recommendations
Security alerts
Regulatory compliance standards

Answer:

Explanation:

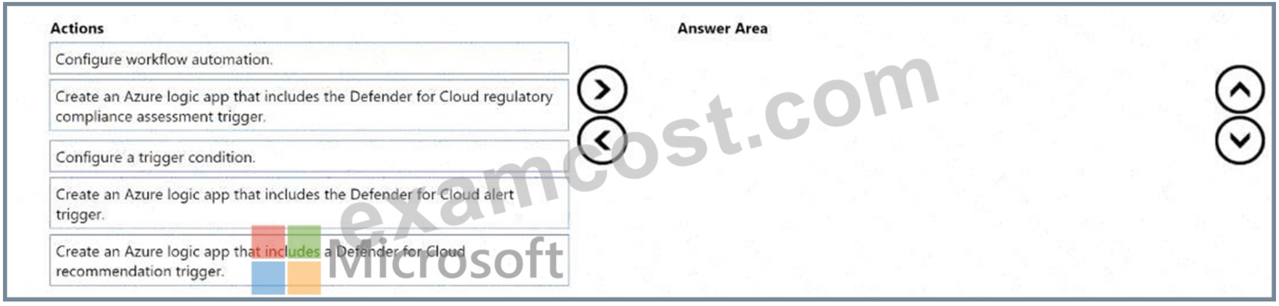

Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Alert is created or triggered
When a response to a Defender for Cloud alert is triggered
Trigger the execution of LA1 from: Regulatory compliance standards
Recommendations
Security alerts
Regulatory compliance standards

Explanation


Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered
Trigger the execution of LA1 from: Regulatory compliance standards

NEW QUESTION # 288
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to create a workflow that will send a Microsoft Teams message to the IT department of your company when a new Microsoft Secure Score action is generated.
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.



Configure workflow automation.

Create an Azure logic app that includes the Defender for Cloud regulatory compliance assessment trigger.

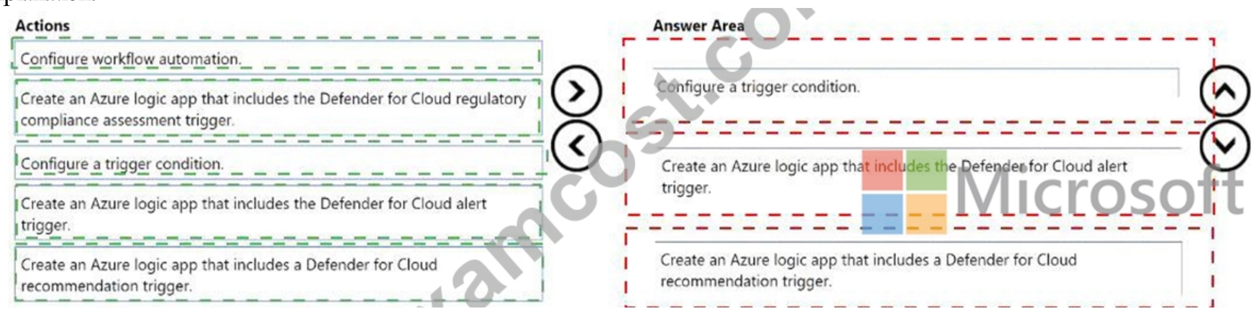
Configure a trigger condition.

Create an Azure logic app that includes the Defender for Cloud alert trigger.

Create an Azure logic app that includes a Defender for Cloud recommendation trigger.

Answer:

Explanation:



Configure workflow automation.

Create an Azure logic app that includes the Defender for Cloud regulatory compliance assessment trigger.

Configure a trigger condition.

Create an Azure logic app that includes the Defender for Cloud alert trigger.

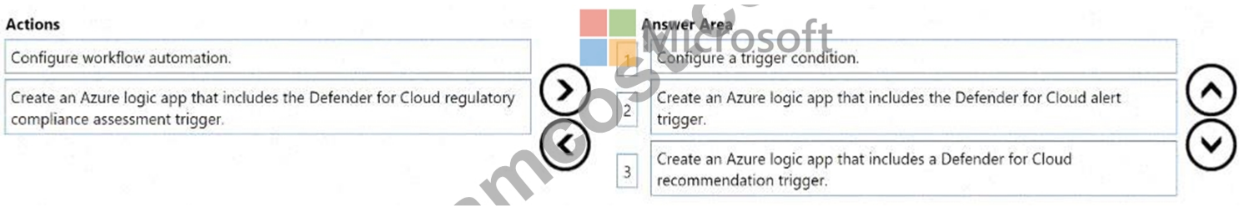
Create an Azure logic app that includes a Defender for Cloud recommendation trigger.

Configure a trigger condition.

Create an Azure logic app that includes the Defender for Cloud alert trigger.

Create an Azure logic app that includes a Defender for Cloud recommendation trigger.

Explanation:



Configure workflow automation.

Create an Azure logic app that includes the Defender for Cloud regulatory compliance assessment trigger.

1 Configure a trigger condition.

2 Create an Azure logic app that includes the Defender for Cloud alert trigger.

3 Create an Azure logic app that includes a Defender for Cloud recommendation trigger.

When you need to send a Microsoft Teams message (or perform any automated response) in Microsoft Defender for Cloud based on a new Microsoft Secure Score action, you must use workflow automation integrated with Azure Logic Apps.

Here's the correct sequence of actions, step by step:

* The Secure Score is part of Defender for Cloud's Regulatory Compliance section.

* To react to new Secure Score recommendations or actions, the Logic App must use the "When a Defender for Cloud regulatory compliance assessment is created or triggered" trigger.

* This ensures that the automation is initiated whenever a new Secure Score change occurs.

* According to Microsoft documentation:

"To automate Secure Score or compliance actions, select the 'Regulatory compliance assessment trigger' in Logic Apps. It triggers workflows when a new compliance or Secure Score recommendation is created or updated."

* Next, you configure the condition that specifies which Secure Score events should trigger the workflow.

* For example, you can set conditions such as:

* "If the assessment type = Secure Score," or

* "If compliance status = Failed."

* This filtering ensures that only relevant events (new Secure Score actions) will activate the workflow and prevent unnecessary Teams notifications.

* Finally, in Defender for Cloud, you configure workflow automation to link the Logic App to the event stream.

* From the Defender for Cloud portal, navigate to Workflow automation # Add automation # Choose trigger and Logic App.

* Select the created Logic App as the target and define the scope (e.g., all subscriptions or resource groups).

* This connects Defender for Cloud to the Logic App so that when a new Secure Score event occurs, the app automatically sends the Microsoft Teams message.

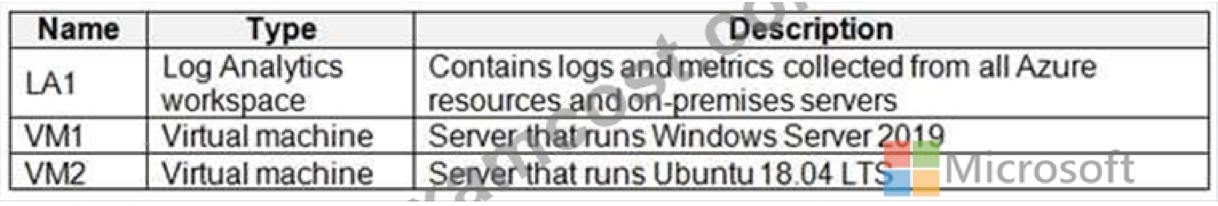
NEW QUESTION # 289

The issue for which team can be resolved by using Microsoft Defender for Office 365?

- A. marketing
- B. executive
- C. sales
- D. security

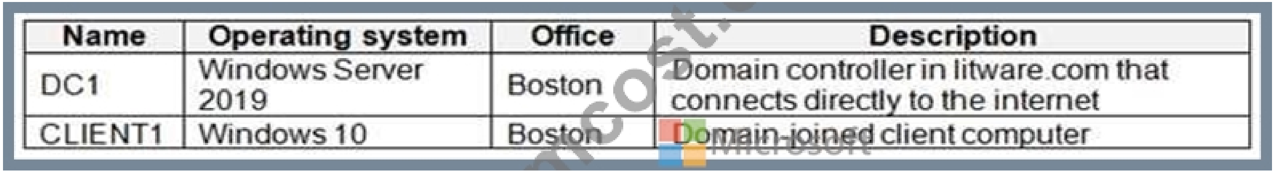
Answer: A

Explanation:
Explanation/Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide
Mitigate threats using Microsoft 365 Defender
Testlet 2
Case study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Litware Inc. is a renewable company.
Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.
Existing Environment
Identity Environment
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.
Microsoft 365 Environment
Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.
Azure Environment
Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.



Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment
Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.
On-premises Environment
The on-premises network contains the computers shown in the following table.



Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems
Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.
Planned Changes
Litware plans to implement the following changes:
* Create and configure Azure Sentinel in the Azure subscription.
* Validate Azure Sentinel functionality by using Azure AD test user accounts.
Business Requirements

Litware identifies the following business requirements:
* The principle of least privilege must be used whenever possible.
* Costs must be minimized, as long as all other requirements are met.
* Logs collected by Log Analytics must provide a full audit trail of user activities.
* All domain controllers must be protected by using Microsoft Defender for Identity.

Azure Information Protection Requirements

All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection - Data discovery dashboard.

Microsoft Defender for Endpoint requirements

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Microsoft Cloud App Security requirements

Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements

All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements

Litware must meet the following Azure Sentinel requirements:
* Integrate Azure Sentinel and Cloud App Security.
* Ensure that a user named admin1 can configure Azure Sentinel playbooks.
* Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
* Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
* Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

NEW QUESTION # 290

......

Lab SC-200 Questions: https://www.examcost.com/SC-200-practice-exam.html

- Microsoft certification SC-200 exam targeted training □ The page for free download of { SC-200 } on □ www.examcollectionpass.com □ will open immediately □Reliable SC-200 Dumps Sheet
- SC-200 Pass4sure □ Training SC-200 Solutions □ SC-200 Reliable Exam Tips □ Search for ▸ SC-200 ◂ and easily obtain a free download on ⇒ www.pdfvce.com ⇐ □SC-200 Reliable Dumps Ebook
- SC-200 Valid Test Test □ Training SC-200 Solutions □ SC-200 Sure Pass □ Search for 「SC-200」 and easily obtain a free download on 【 www.prep4away.com 】 □SC-200 Sure Pass
- Latest updated Microsoft New SC-200 Study Guide With Interarctive Test Engine - Valid Lab SC-200 Questions □ Open website （ www.pdfvce.com ） and search for ▸ SC-200 ◂ for free download □Test SC-200 Passing Score
- Get Marvelous New SC-200 Study Guide and First-grade Lab SC-200 Questions □ Simply search for □ SC-200 □ for free download on 「www.practicevce.com」 □SC-200 Pass Guarantee
- SC-200 Valid Braindumps □ Practice SC-200 Tests □ SC-200 Sure Pass □ Search for □ SC-200 □ and download it for free on ⇒ www.pdfvce.com ⇐ website □Certification SC-200 Test Answers
- SC-200 Reliable Exam Tips □ SC-200 Valid Test Test □ Test SC-200 Simulator Fee □ The page for free download of " SC-200 " on ➽ www.prep4sures.top □ will open immediately □SC-200 Pass Guarantee
- Practice SC-200 Tests □ Test SC-200 Passing Score □ Reliable SC-200 Dumps Sheet □ Simply search for □ SC-200 □ for free download on ➥ www.pdfvce.com □ □SC-200 Reliable Dumps Ebook
- Training SC-200 Solutions □ Training SC-200 Solutions □ SC-200 Valid Test Test □ Search for ➤ SC-200 □ on ▸ www.dumpsquestion.com ◂ immediately to obtain a free download □SC-200 Reliable Dumps Ebook
- SC-200 Answers Real Questions □ Reliable SC-200 Real Test □ SC-200 Valid Test Test □ Go to website ▹ www.pdfvce.com ◃ open and search for □ SC-200 □ to download for free □SC-200 Pass4sure
- Microsoft certification SC-200 exam targeted training □ Simply search for ▹ SC-200 ◃ for free download on 「www.vce4dumps.com」 □Guaranteed SC-200 Success
- coursewoo.com, aartisticbakes.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, actek.in, myportal.utt.edu.tt,

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes