



Microsoft

Exam Questions SC-200

Microsoft Security Operations Analyst

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

HOTSPOT - (Topic 1)

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

What should you recommend for each threat? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

NEW QUESTION 2

- (Topic 1)

You need to remediate active attacks to meet the technical requirements. What should you include in the solution?

- A. Azure Automation runbooks
- B. Azure Logic Apps
- C. Azure FunctionsD Azure Sentinel livestreams

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks>

NEW QUESTION 3

- (Topic 1)

You need to complete the query for failed sign-ins to meet the technical requirements. Where can you find the column name to complete the where clause?

- A. Security alerts in Azure Security Center
- B. Activity log in Azure
- C. Azure Advisor
- D. the query windows of the Log Analytics workspace

Answer: D

NEW QUESTION 4

HOTSPOT - (Topic 2)

You need to implement Microsoft Defender for Cloud to meet the Microsoft Defender for Cloud 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 Area

Log Analytics workspace to use: ▼
A new Log Analytics workspace in the East US Azure region
Default workspace created by Azure Security Center
LA1

Windows security events to collect: ▼
All Events
Common
Minimal

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Log Analytics workspace to use: ▼
A new Log Analytics workspace in the East US Azure region
Default workspace created by Azure Security Center
LA1

Windows security events to collect: ▼
All Events
Common
Minimal

NEW QUESTION 5

HOTSPOT - (Topic 2)

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.

Log Analytics workspace to use: ▼
A new Log Analytics workspace in the East US Azure region
Default workspace created by Azure Security Center
LA1

Windows security events to collect: ▼
All Events
Common
Minimal

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Log Analytics workspace to use: ▼
A new Log Analytics workspace in the East US Azure region
Default workspace created by Azure Security Center
LA1

Windows security events to collect: ▼
All Events
Common
Minimal

NEW QUESTION 6

HOTSPOT - (Topic 2)

You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

In the Cloud App Security portal:

	▼
Add a security extension	
Configure app connectors	
Configure log collectors	

From Azure Sentinel in the Azure portal:

	▼
Add a data connector	
Add a workbook	
Configure the Logs settings	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

In the Cloud App Security portal:

	▼
Add a security extension	
Configure app connectors	
Configure log collectors	

From Azure Sentinel in the Azure portal:

	▼
Add a data connector	
Add a workbook	
Configure the Logs settings	

NEW QUESTION 7

HOTSPOT - (Topic 2)

You need to configure the Microsoft Sentinel integration to meet the Microsoft Sentinel requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

In the Microsoft Defender for Cloud Apps portal:

Add a security extension	▼
Add a security extension	
Configure app connectors	
Configure log collectors	

From Microsoft Sentinel in the Azure portal:

Add a data connector	▼
Add a data connector	
Add a workbook	
Configure the Logs settings	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

In the Microsoft Defender for Cloud Apps portal:

Add a security extension	▼
Add a security extension	
Configure app connectors	
Configure log collectors	

From Microsoft Sentinel in the Azure portal:

Add a data connector	▼
Add a data connector	
Add a workbook	
Configure the Logs settings	

NEW QUESTION 8

- (Topic 2)

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements. Which role should you assign?

- A. Automation Operator
- B. Automation Runbook Operator
- C. Azure Sentinel Contributor
- D. Logic App Contributor

Answer: C

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/roles>

NEW QUESTION 9

HOTSPOT - (Topic 3)

You need to implement the query for Workbook1 and Webapp1. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Data source to query: JSON

On Webapp1: Enable Cross-Origin Resource Sharing (CORS)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Data source to query: JSON

On Webapp1: Enable Cross-Origin Resource Sharing (CORS)

NEW QUESTION 10

- (Topic 3)

You need to configure event monitoring for Server1. The solution must meet the Microsoft Sentinel requirements. What should you create first?

- A. a Microsoft Sentinel automation rule
- B. a Microsoft Sentinel scheduled query rule
- C. a Data Collection Rule (DCR)
- D. an Azure Event Grid topic

Answer: C

NEW QUESTION 10

HOTSPOT - (Topic 3)

You need to implement the Microsoft Sentinel NRT rule for monitoring the designated break glass account. The solution must meet the Microsoft Sentinel requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area

SigninLogs

join kind=inner GetWatchlist ('breakglass_account')

on \$left.UserPrincipalName == \$right.SearchKey

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 12

HOTSPOT - (Topic 3)

You need to monitor the password resets. The solution must meet the Microsoft Sentinel requirements.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

In the identity environment, implement:

- Azure AD Password Protection
- Azure AD Password Protection
- Microsoft Defender for Identity
- Smart lockout

In Microsoft Sentinel, configure:

- The Windows Security Events via AMA connector
- A Microsoft security rule
- The Windows Security Events via AMA connector
- User and Entity Behavior Analytics (UEBA)

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

In the identity environment, implement:

- Azure AD Password Protection
- Azure AD Password Protection
- Microsoft Defender for Identity
- Smart lockout

In Microsoft Sentinel, configure:

- The Windows Security Events via AMA connector
- A Microsoft security rule
- The Windows Security Events via AMA connector
- User and Entity Behavior Analytics (UEBA)

NEW QUESTION 15

- (Topic 4)

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel. You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?

- A. Azure Sentinel Responder
- B. Logic App Contributor
- C. Azure Sentinel Contributor
- D. Azure Sentinel Reader

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

NEW QUESTION 16

- (Topic 4)

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Security solutions
- B. Security policy
- C. Pricing & settings

- D. Security alerts
- E. Azure Defender

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

NEW QUESTION 19

- (Topic 4)

You implement Safe Attachments policies in Microsoft Defender for Office 365.

Users report that email messages containing attachments take longer than expected to be received.

You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.

What should you configure in the Safe Attachments policies?

- A. Dynamic Delivery
- B. Replace
- C. Block and Enable redirect
- D. Monitor and Enable redirect

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide>

NEW QUESTION 24

- (Topic 4)

You have an Azure subscription that contains an Azure logic app named app1 and a Microsoft Sentinel workspace that has an Azure AD connector. You need to ensure that app1 launches when Microsoft Sentinel detects an Azure AD-generated alert. What should you create first?

- A. a repository connection
- B. a watchlist
- C. an analytics rule
- D. an automation rule

Answer: D

NEW QUESTION 25

HOTSPOT - (Topic 4)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.

You are notified that the account of User1 is compromised.

You need to review the alerts triggered on the devices to which User1 signed in.

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

NOTE: Each correct selection is worth one point.

DeviceInfo

```
| where LoggedOnUsers contains 'user1'
| distinct DeviceId
|  kind=inner AlertEvidence on DeviceId
| 

|         |
|---------|
| extend  |
| join    |
| project |


| project AlertId
| join AlertInfo on AlertId
|  AlertId, Timestamp, Title, Severity, Category
| 

|           |
|-----------|
| project   |
| summarize |
| take      |


```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: join An inner join.

This query uses kind=inner to specify an inner-join, which prevents deduplication of left side values for DeviceId.

This query uses the DeviceInfo table to check if a potentially compromised user (<account-name>) has logged on to any devices and then lists the alerts that have been triggered on those devices.

DeviceInfo

```
//Query for devices that the potentially compromised account has logged onto
```

```
| where LoggedOnUsers contains '<account-name>'
```

```
| distinct DeviceId
```

```
//Crosscheck devices against alert records in AlertEvidence and AlertInfo tables
```

```
| join kind=inner AlertEvidence on DeviceId
```

```
| project AlertId
```

```
//List all alerts on devices that user has logged on to
```

```
| join AlertInfo on AlertId
```

```
| project AlertId, Timestamp, Title, Severity, Category
```

```
DeviceInfo LoggedOnUsers AlertEvidence "project AlertID" Box 2: project
```

NEW QUESTION 27

- (Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a hunting bookmark. Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center>

NEW QUESTION 29

- (Topic 4)

You have a Microsoft 365 subscription. The subscription uses Microsoft 365 Defender and has data loss prevention (DLP) policies that have aggregated alerts configured.

You need to identify the impacted entities in an aggregated alert.

What should you review in the DIP alert management dashboard of the Microsoft Purview compliance portal?

A. the Details tab of the alert

B. Management log

C. the Sensitive Info Types tab of the alert

D. the Events tab of the alert

Answer: B

NEW QUESTION 31

- (Topic 4)

You have an Azure subscription that contains a Microsoft Sentinel workspace. The workspace contains a Microsoft Defender for Cloud data connector. You need to customize which details will be included when an alert is created for a specific event. What should you do?

A. Modify the properties of the connector.

B. Create a Data Collection Rule (DCR).

C. Create a scheduled query rule.

D. Enable User and Entity Behavior Analytics (UEBA)

Answer: D

NEW QUESTION 32

- (Topic 4)

You have a Microsoft 365 tenant that uses Microsoft Exchange Online and Microsoft Defender for Office 365.

What should you use to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user?

A. the Threat Protection Status report in Microsoft Defender for Office 365

B. the mailbox audit log in Exchange

C. the Safe Attachments file types report in Microsoft Defender for Office 365

D. the mail flow report in Exchange

Answer: A

Explanation:

To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections).

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide>

NEW QUESTION 34

HOTSPOT - (Topic 4)

You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application. You need to hide Azure Defender alerts for the storage account.

Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Entity type:

IP address
Azure Resource
Host
User account

Field:

Name
Resource Id
Address
Command line

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Entity type:

IP address
Azure Resource
Host
User account

Field:

Name
Resource Id
Address
Command line

NEW QUESTION 35

- (Topic 4)

You have the resources shown in the following Table.

Name	Type	Description	Location
Server1	Server	File server that runs Windows Server	On-premises
Server2	Virtual machine	Application server that runs Linux	Amazon Web Services (AWS)
Server3	Virtual machine	Domain controller that runs Windows Server	Azure
Server4	Server	Domain controller that runs Windows Server	On-premises

You have an Azure subscription that uses Microsoft Defender for Cloud. You need to enable Microsoft Defender IoT Servers on each resource. Which resources will require the installation of the Azure Arc agent?

- A. Server 3 only
- B. Server1 and Server4 only
- C. Server 1, Server2, and Server4 only
- D. Server 1, Server2, Server3, and Server4

Answer: B

NEW QUESTION 38

- (Topic 4)

You have a Microsoft Sentinel workspace that has user and Entity Behavior Analytics (UEBA) enabled for Signin Logs. You need to ensure that failed interactive sign-ins are detected. The solution must minimize administrative effort. What should you use?

- A. a scheduled alert query
- B. a UEBA activity template
- C. the Activity Log data connector
- D. a hunting query

Answer: B

NEW QUESTION 43

- (Topic 4)

Your company has an on-premises network that uses Microsoft Defender for Identity. The Microsoft Secure Score for the company includes a security assessment associated with unsecure Kerberos delegation. You need remediate the security risk. What should you do?

- A. Install the Local Administrator Password Solution (LAPS) extension on the computers listed as exposed entities.
- B. Modify the properties of the computer objects listed as exposed entities.
- C. Disable legacy protocols on the computers listed as exposed entities.
- D. Enforce LDAP signing on the computers listed as exposed entities.

Answer: B

Explanation:

To remediate the security risk associated with unsecure Kerberos delegation, you should modify the properties of the computer objects listed as exposed entities. Specifically, you should set the Kerberos delegation settings to either 'Trust this computer for delegation to any service' or 'Trust this computer for delegation to specified services only'. This will ensure that the computer is not allowed to use Kerberos delegation to access other computers on the network. Reference: <https://docs.microsoft.com/en-us/windows/security/identity-protection/microsoft-defender-for-identity/configure-kerberos-delegation>

NEW QUESTION 47

- (Topic 4)

You have two Azure subscriptions that use Microsoft Defender for Cloud. You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort. What should you do in the Azure portal?

- A. Create an Azure Policy assignment.
- B. Modify the Workload protections settings in Defender for Cloud.
- C. Create an alert rule in Azure Monitor.
- D. Modify the alert settings in Defender for Cloud.

Answer: D

Explanation:

You can use alerts suppression rules to suppress false positives or other unwanted security alerts from Defender for Cloud.

Note: To create a rule directly in the Azure portal:

* 1. From Defender for Cloud's security alerts page:

Select the specific alert you don't want to see anymore, and from the details pane, select Take action.

Or, select the suppression rules link at the top of the page, and from the suppression rules page select Create new suppression rule:

* 2. In the new suppression rule pane, enter the details of your new rule.

Your rule can dismiss the alert on all resources so you don't get any alerts like this one in the future.

Your rule can dismiss the alert on specific criteria - when it relates to a specific IP address, process name, user account, Azure resource, or location.

* 3. Enter details of the rule.

* 4. Save the rule.

Reference: <https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules>

NEW QUESTION 48

- (Topic 4)

You have a custom Microsoft Sentinel workbook named Workbooks.

You need to add a grid to Workbook1. The solution must ensure that the grid contains a maximum of 100 rows.

What should you do?

- A. In the query editor interface, configure Settings.
- B. In the query editor interface, select Advanced Editor
- C. In the grid query, include the project operator.
- D. In the grid query, include the take operator.

Answer: B

NEW QUESTION 50

- (Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud. You have a GitHub account named Account1 that contains 10 repositories.

You need to ensure that Defender for Cloud can assess the repositories in Account1. What should you do first in the Microsoft Defender for Cloud portal?

- A. Add an environment.
- B. Enable security policies.
- C. Enable integrations.
- D. Enable a plan.

Answer: A

NEW QUESTION 55

- (Topic 4)

You have a Microsoft Sentinel workspace.

You need to prevent a built-in Advance Security information Model (ASIM) parse from being updated automatically.

What are two ways to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Redeploy the built-in parse and specify a CallerContext parameter of any and a SourceSpecificParse parameter of any.
- B. Create a hunting query that references the built-in parse.
- C. Redeploy the built-in parse and specify a CallerContext parameter of built-in.
- D. Build a custom unify parse and include the build- parse version
- E. Create an analytics rule that includes the built-in parse

Answer: AD

NEW QUESTION 57

- (Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a resource group named RG1. RG1. You need to configure just in time (JIT)

VM access for the virtual machines in RG1. The solution must meet the following

- Limit the maximum request time to two hours.
- Limit protocol access to Remote Desktop Protocol (RDP) only.
- Minimize administrative effort. What should you use?

- A. Azure AD Privileged Identity Management (PIM)
- B. Azure Policy
- C. Azure Front Door
- D. Azure Bastion

Answer: A

NEW QUESTION 61

- (Topic 4)

You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC).

What should you use?

- A. notebooks in Azure Sentinel
- B. Microsoft Cloud App Security
- C. Azure Monitor
- D. hunting queries in Azure Sentinel

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

NEW QUESTION 65

HOTSPOT - (Topic 4)

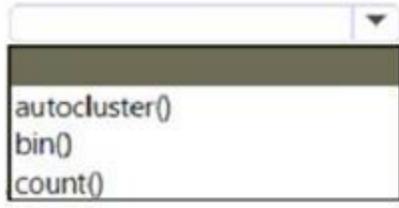
You have a Microsoft Sentinel workspace named sws1.

You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts. The solution must exclude users that list storage keys for a single storage account.

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 OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
    AzureActivity
    | where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
    | where ActivityStatusValue == "Succeeded"
    | project ExpectedIpAddress=CallerIpAddress, Caller
    | evaluate
        
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
    by OperationNameValue, Caller, CallerIpAddress
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: AzureActivity

The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:

Box 2: autocluster()

Example: description: |

'Listing of storage keys is an interesting operation in Azure which might expose additional secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this type, it would be interesting to see if the account performing this activity or the source IP address from which it is being done is anomalous.

The query below generates known clusters of ip address per caller, notice that users which only had single operations do not appear in this list as we cannot learn from it their normal activity (only based on a single event). The activities for listing storage account keys is correlated with this learned clusters of expected activities and activity which is not expected is returned.'

AzureActivity

```
| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner ( AzureActivity
| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| project ExpectedIpAddress=CallerIpAddress, Caller
| evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
by OperationNameValue, Caller, CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress
```

NEW QUESTION 70

- (Topic 4)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender. You plan to create a hunting query from Microsoft Defender.

You need to create a custom tracked query that will be used to assess the threat status of the subscription.

From the Microsoft 365 Defender portal, which page should you use to create the query?

- A. Policies & rules
- B. Explorer
- C. Threat analytics
- D. Advanced Hunting

Answer: D

NEW QUESTION 71

DRAG DROP - (Topic 4)

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

- Enable and disable advanced features of Microsoft Defender for Cloud.
- Apply security recommendations to a resource. The solution must use the principle of least privilege.

Which Microsoft Defender for Cloud role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role 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.

Roles	Answer Area
Resource Group Owner	Enable and disable advanced features of Microsoft Defender for Cloud: <input type="text"/>
Security Admin	Apply security recommendations to a resource: <input type="text"/>
Subscription Contributor	
Subscription Owner	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Roles	Answer Area
Resource Group Owner	Enable and disable advanced features of Microsoft Defender for Cloud: <input type="text" value="Security Admin"/>
Security Admin	Apply security recommendations to a resource: <input type="text" value="Subscription Contributor"/>
Subscription Contributor	
Subscription Owner	

NEW QUESTION 75

HOTSPOT - (Topic 4)

You need to create a query for a workbook. The query must meet the following requirements:

- ? List all incidents by incident number.
- ? Only include the most recent log for each incident.

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

NOTE: Each correct selection is worth one point.

`SecurityIncident`

		(LastModifiedTime,*) by IncidentNumber
project	arg_max	
sort	limit	
summarize	top	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

`SecurityIncident`

		(LastModifiedTime,*) by IncidentNumber
project	arg_max	
sort	limit	
summarize	top	

NEW QUESTION 76

HOTSPOT - (Topic 4)

You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1. You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel 1 and configure UEBA to use data collected from Active Directory Domain Services (AD OS).

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To the AD DS domain controllers, deploy:

- The Azure Connected Machine agent
- Microsoft Defender for Identity sensors
- The Azure Connected Machine agent**
- The Azure Monitor agent

For Sentinel1, configure:

- The Audit Logs data source
- The Audit Logs data source**
- The Security Events data source
- The Signin Logs data source

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

To the AD DS domain controllers, deploy:

- The Azure Connected Machine agent
- Microsoft Defender for Identity sensors
- The Azure Connected Machine agent**
- The Azure Monitor agent

For Sentinel1, configure:

- The Audit Logs data source
- The Audit Logs data source**
- The Security Events data source
- The Signin Logs data source

NEW QUESTION 78

HOTSPOT - (Topic 4)

You have an Azure subscription that contains an Microsoft Sentinel workspace.

You need to create a hunting query using Kusto Query Language (KQL) that meets the following requirements:

- Identifies an anomalous number of changes to the rules of a network security group (NSG) made by the same security principal
- Automatically associates the security principal with an Microsoft Sentinel entity

How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

```

AuditLogs
AzureActivity
AzureDiagnostics
in~ ("Microsoft.Network/networkSecurityGroups/securityRules/write")
e == "Succeeded"
| make-series dcount(ResourceId) default=0 on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
| extend timestamp = todatetime(EventSubmissionTimestamp[0])
AccountCustomEntity = Caller
| extend
| parse-where
| where
    
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```

AuditLogs
AzureActivity
AzureDiagnostics
in~ ("Microsoft.Network/networkSecurityGroups/securityRules/write")
e == "Succeeded"
| make-series dcount(ResourceId) default=0 on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
| extend timestamp = todatetime(EventSubmissionTimestamp[0])
AccountCustomEntity = Caller
| extend |
| parse-where
| where
    
```

NEW QUESTION 81

HOTSPOT - (Topic 4)

You have an Azure subscription that contains a guest user named User1 and a Microsoft Sentinel workspace named workspace1.

You need to ensure that User1 can triage Microsoft Sentinel incidents in workspace1. The

solution must use the principle of least privilege.

Which roles should you assign to User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Azure role:

- Microsoft Sentinel Contributor
- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Contributor
- Microsoft Sentinel Responder

Azure AD role:

- Attribute assignment reader
- Directory readers
- Global reader

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure role:

- Microsoft Sentinel Contributor
- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Contributor
- Microsoft Sentinel Responder

Azure AD role:

- Attribute assignment reader
- Directory readers
- Global reader

NEW QUESTION 85

- (Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1. You need to identify which blobs were deleted. What should you review?

- A. the activity logs of storage1
- B. the Azure Storage Analytics logs
- C. the alert details
- D. the related entities of the alert

Answer: A

Explanation:

To identify which blobs were deleted, you should review the activity logs of the storage account. The activity logs contain information about all the operations that have taken place in the storage account, including delete operations. These logs can be accessed in the Azure portal by navigating to the storage account, selecting "Activity log" under the "Monitoring" section, and filtering by the appropriate time range. You can also use Azure Monitor and Log Analytics to query and analyze the activity logs data. References:

- ? <https://docs.microsoft.com/en-us/azure/storage/common/storage-activity-logs>
- ? <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-azure-storage>

NEW QUESTION 88

- (Topic 4)

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You need to configure the continuous export of high-severity alerts to enable their retrieval from a third-party security information and event management (SIEM) solution.

To which service should you export the alerts?

- A. Azure Cosmos DB
- B. Azure Event Grid
- C. Azure Event Hubs
- D. Azure Data Lake

Answer: C

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal>

NEW QUESTION 89

- (Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have Linux virtual machines on Amazon Web Services (AWS). You deploy Azure Defender and enable auto-provisioning.

You need to monitor the virtual machines by using Azure Defender.

Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivot=azure-arc>

NEW QUESTION 92

- (Topic 4)

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.

You need to identify which Office VBA macros might be affected.

Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`
- B. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`
- C. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`
- D. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: BC

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction>

NEW QUESTION 96

- (Topic 4)

You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region. You need to ensure that you can use scheduled analytics rules in the existing Azure

Sentinel deployment to generate alerts based on queries to LogsWest. What should you do first?

- A. Deploy Azure Data Catalog to the West US Azure region.
- B. Modify the workspace settings of the existing Azure Sentinel deployment
- C. Add Microsoft Sentinel to a workspace.
- D. Create a data connector in Azure Sentinel.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants>

NEW QUESTION 99

- (Topic 4)

You create an Azure subscription named sub1.

In sub1, you create a Log Analytics workspace named workspace1.

You enable Azure Security Center and configure Security Center to use workspace1.

You need to ensure that Security Center processes events from the Azure virtual machines that report to workspace1.

What should you do?

- A. In workspace1, install a solution.
- B. In sub1, register a provider.
- C. From Security Center, create a Workflow automation.
- D. In workspace1, create a workbook.

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

NEW QUESTION 101

DRAG DROP - (Topic 4)

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

- Enable Security Health Analytics.
- From Azure Security Center, add cloud connectors.
- Configure the GCP Security Command Center.
- Create a dedicated service account and a private key.
- Enable the GCP Security Command Center API.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Answer Area

- Enable Security Health Analytics.
- From Azure Security Center, add cloud connectors.
- Configure the GCP Security Command Center.
- Create a dedicated service account and a private key.
- Enable the GCP Security Command Center API.

- Configure the GCP Security Command Center.
- Enable Security Health Analytics.
- Enable the GCP Security Command Center API.
- Create a dedicated service account and a private key.
- From Azure Security Center, add cloud connectors.



NEW QUESTION 102

- (Topic 4)

You use Azure Sentinel.

You need to use a built-in role to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

- A. Azure Sentinel Contributor
- B. Security Administrator
- C. Azure Sentinel Responder
- D. Logic App Contributor

Answer: C

Explanation:

Azure Sentinel Contributor can create and edit workbooks, analytics rules, and other Azure Sentinel resources.

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

NEW QUESTION 107

- (Topic 4)

You have 50 Microsoft Sentinel workspaces.

You need to view all the incidents from all the workspaces on a single page in the Azure portal. The solution must minimize administrative effort.

Which page should you use in the Azure portal?

- A. Microsoft Sentinel - Incidents
- B. Microsoft Sentinel - Workbooks
- C. Microsoft Sentinel
- D. Log Analytics workspaces

Answer: D

NEW QUESTION 110

- (Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add each account as a Sensitive account. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

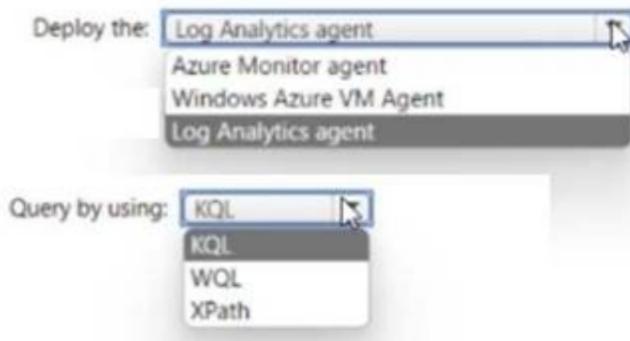
<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

NEW QUESTION 114

HOTSPOT - (Topic 4)

You need to meet the Microsoft Sentinel requirements for collecting Windows Security event logs. What should you do? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.

Answer Area

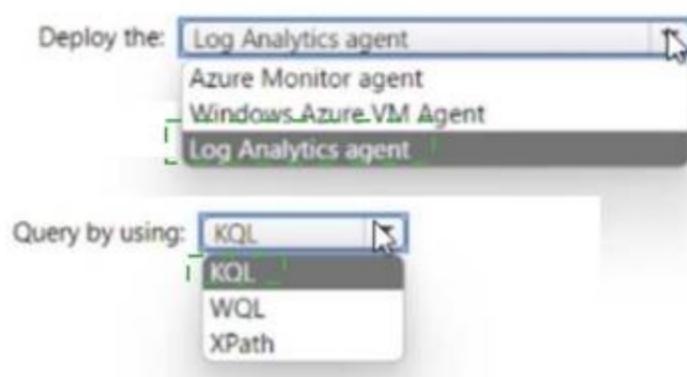


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 116

- (Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Entity tags, you add the accounts as Honeytoken accounts. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

NEW QUESTION 117

- (Topic 4)

You have an Azure subscription that use Microsoft Defender for Cloud and contains a user named User1.

You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Security operator
- B. Security Admin
- C. Owner
- D. Contributor

Answer: B

NEW QUESTION 120

HOTSPOT - (Topic 4)

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Resource exemption (preview)

Now you can exempt irrelevant resources so they do not affect your secure score. [Learn more](#)

Each security control below represents a security risk you should mitigate. Address the recommendations in each control, focusing on the controls worth the most points. To get the max score, fix all recommendations for all resources in a control. [Learn more](#)

Search recommendations:

Control status: **2 Selected** Recommendation status: **2 Selected**

Recommendation maturity: **All** Resource type: **All** Quick fix available: **All**

Contains exemptions: **All** [Reset filters](#) Group by controls: On

Controls	Potential score increase	Unhealthy resources	Resource Health
> Restrict unauthorized network access	+9% (4 points)	2 of 2 resources	
> Secure management ports	+9% (4 points)	1 of 2 resources	
> Enable encryption at rest	+9% (4 points)	2 of 2 resources	
> Remediate security configurations	+4% (2 points)	1 of 2 resources	
> Apply adaptive application control	+3% (2 points)	1 of 2 resources	
> Apply system updates Completed	+0% (0 points)	None	
> Enable endpoint protection Completed	+0% (0 points)	None	
> Remediate vulnerabilities Completed	+0% (0 points)	None	
> Implement security best practices Completed	+0% (0 points)	None	
> Enable MFA Completed	+0% (0 points)	None	
> Manage access and permissions Completed	+0% (0 points)	None	

Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)

Home > Policy

Policy - Compliance

Search (Ctrl+F)

Assign policy Assign initiative Refresh

Scope: Microsoft Azure Type: All definition types Compliance state: All compliance states Search: Filter by name or id...

Overall resource compliance: **100%**

Resources by compliance state: 0 (0 - Compliant, 0 - Exempt, 1 - Non-compliant, 0 - Conflicting)

Non-compliant initiatives: 0 out of 0

Non-compliant policies: 0 out of 0

Name Scope Compliance Resource compliance

No assignments to display within the given scope Non-Compliant Resources Non-compliant policies

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

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

NEW QUESTION 125

- (Topic 4)

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart. What should you include in the query?

- A. extend
- B. bin
- C. makeset
- D. workspace

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries>

NEW QUESTION 128

HOTSPOT - (Topic 4)

You have a Microsoft Sentinel workspace

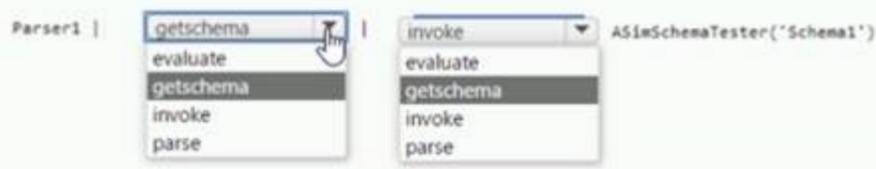
You develop a custom Advanced Security information Model (ASIM) parser named Parser1 that produces a schema named Schema1.

You need to validate Schema1.

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

NOTE: Each correct selection is worth one point.

Answer Area

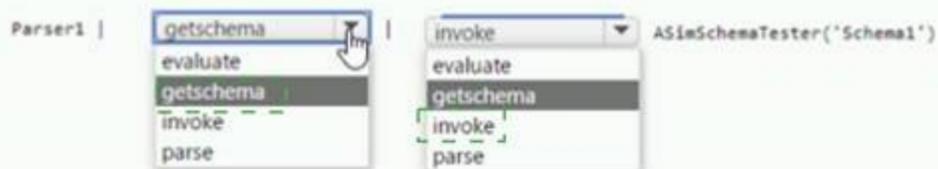


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 133

HOTSPOT - (Topic 4)

You need to assign role-based access control (RBAQ roles to Group1 and Group2 to meet The Microsoft Defender for Cloud requirements and the business requirements Which role should you assign to each group? To answer, select the appropriate options in the answer area NOTE Each correct selection is worth one point.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 134

- (Topic 4)

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add a playbook.
- B. Associate a playbook to an incident.
- C. Enable Entity behavior analytics.
- D. Create a workbook.
- E. Enable the Fusion rule.

Answer: AB

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

NEW QUESTION 135

- (Topic 4)

You have an Azure subscription that uses resource type for Cloud. You need to filter the security alerts view to show the following alerts:

- Unusual user accessed a key vault
- Log on from an unusual location
- Impossible travel activity Which severity should you use?

- A. Informational
- B. Low
- C. Medium
- D. High

Answer: C

NEW QUESTION 136

HOTSPOT - (Topic 4)

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.

You need to identify all the interactive authentication attempts by the users in the finance department of your company.

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

NOTE: Each correct selection is worth one point.

Answer Area

```

IdentityQueryEvents
BehaviorAnalytics
IdentityInfo
IdentityQueryEvents
| where Department == 'Finance'
| project-rename objid = AccountObjectId
| join AuditLogs on $left.objid == $right.AccountObjectId
AuditLogs
IdentityLogonEvents
SigninLogs
    
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

```

IdentityQueryEvents
BehaviorAnalytics
IdentityInfo
IdentityQueryEvents
| where Department == 'Finance'
| project-rename objid = AccountObjectId
| join AuditLogs on $left.objid == $right.AccountObjectId
AuditLogs
IdentityLogonEvents
SigninLogs
    
```

NEW QUESTION 138

- (Topic 4)

You have a Microsoft Sentinel workspace named Workspaces

You need to exclude a built-in, source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser.

What should you create in Workspace1?

- A. a workbook
- B. a hunting query
- C. a watchlist
- D. an analytic rule

Answer: D

Explanation:

To exclude a built-in, source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser, you should create an analytic rule in the Microsoft Sentinel workspace. An analytic rule allows you to customize the behavior of the unified ASIM parser and exclude specific source-specific parsers from being used.

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-analytic-rule>

NEW QUESTION 139

- (Topic 4)

You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.

You are troubleshooting an issue on the virtual machines.

In Security Center, you need to view the alerts generated by the virtual machines during the last five days.

What should you do?

- A. Change the rule expiration date of the suppression rule.
- B. Change the state of the suppression rule to Disabled.
- C. Modify the filter for the Security alerts page.
- D. View the Windows event logs on the virtual machines.

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules>

NEW QUESTION 143

DRAG DROP - (Topic 4)

You create a new Azure subscription and start collecting logs for Azure Monitor.

You need to validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server.

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

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions	Answer Area
Enable Microsoft Defender for Cloud's enhanced security features for the subscription.	<div style="display: flex; align-items: center; justify-content: center;"> <div style="margin-right: 20px;"> ➤ ➤ </div> <div style="margin-right: 20px;"> ⬅ ⬅ </div> <div style="margin-right: 20px;"> ⬆ ⬆ </div> <div style="margin-right: 20px;"> ⬆ ⬆ </div> </div>
Change the alert severity threshold for emails to Medium .	
Rename the executable file as AlertTest.exe.	
Change the alert severity threshold for emails to Low .	
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.	
Run the executable file and specify the appropriate arguments.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server, you should perform the following three actions in sequence:

? Copy an executable file on a virtual machine and rename the file as

ASC_AlertTest_662jfi039N.exe

? Run the executable file and specify the appropriate arguments

? Enable Microsoft Defender for Cloud's enhanced security features for the subscription.

These actions will simulate a malicious activity on the virtual machine and generate an alert in Defender for Cloud. You can then verify the alert details and response recommendations in the Azure portal. For more information, see Alert validation - Microsoft Defender for Cloud.

NEW QUESTION 146

DRAG DROP - (Topic 4)

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

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
From Device Inventory, search for the CVE.	<div style="display: flex; align-items: center; justify-content: center;"> <div style="margin-right: 20px;"> ⬅ ⬅ </div> <div style="margin-right: 20px;"> ➤ ➤ </div> <div style="margin-right: 20px;"> ⬆ ⬆ </div> <div style="margin-right: 20px;"> ⬆ ⬆ </div> </div>
Open the Threat Protection report.	
From Threat & Vulnerability Management, select Weaknesses , and search for the CVE.	
From Advanced hunting, search for <code>cveId</code> in the <code>DeviceTvmSoftwareInventoryVulnerabilitites</code> table.	
Create the remediation request.	
Select Security recommendations .	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

- From Device Inventory, search for the CVE.
- Open the Threat Protection report.
- From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.
- From Advanced hunting, search for `cveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.
- Create the remediation request.
- Select **Security recommendations**.

Answer Area

- From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.
- Select **Security recommendations**.
- Create the remediation request.

NEW QUESTION 151

- (Topic 4)

You have an Azure subscription that contains a virtual machine named VM1 and uses Azure Defender. Azure Defender has automatic provisioning enabled. You need to create a custom alert suppression rule that will suppress false positive alerts for suspicious use of PowerShell on VM1. What should you do first?

- A. From Azure Security Center, add a workflow automation.
- B. On VM1, run the `Get-MPThreatCatalog` cmdlet.
- C. On VM1 trigger a PowerShell alert.
- D. From Azure Security Center, export the alerts to a Log Analytics workspace.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide>

NEW QUESTION 156

- (Topic 4)

You have an Azure subscription that contains an Microsoft Sentinel workspace. You need to create a playbook that will run automatically in response to an Microsoft Sentinel alert. What should you create first?

- A. a trigger in Azure Functions
- B. an Azure logic app
- C. a hunting query in Microsoft Sentinel
- D. an automation rule in Microsoft Sentinel

Answer: D

NEW QUESTION 161

HOTSPOT - (Topic 4)

You have an Azure subscription.

You plan to implement an Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.

You need to configure storage for the workspace. The solution must meet the following requirements:

- Minimize costs for daily ingested data.
- Maximize the data retention period without incurring extra costs.

What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.

Minimize costs for daily ingested data:

- Use a commitment tier.
- Apply a daily cap.
- Use a commitment tier.
- Use the Pay-As-You-Go (PAYG) model.

Maximize the data retention period without incurring extra costs:

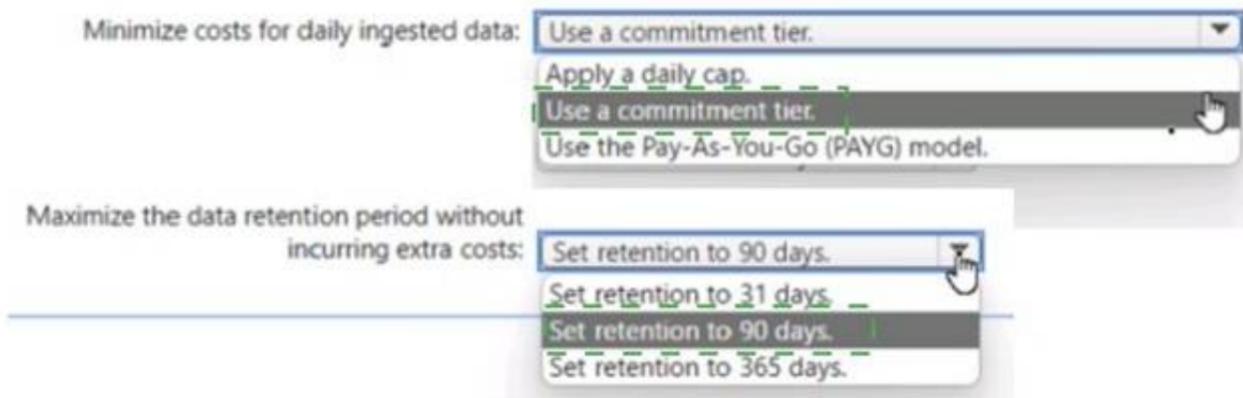
- Set retention to 90 days.
- Set retention to 31 days.
- Set retention to 90 days.
- Set retention to 365 days.

A. Mastered

B. Not Mastered

Answer: A

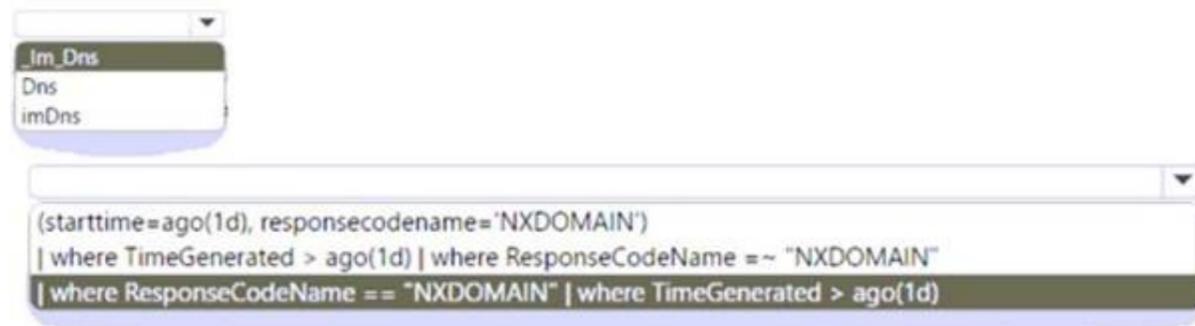
Explanation:



NEW QUESTION 165

HOTSPOT - (Topic 4)

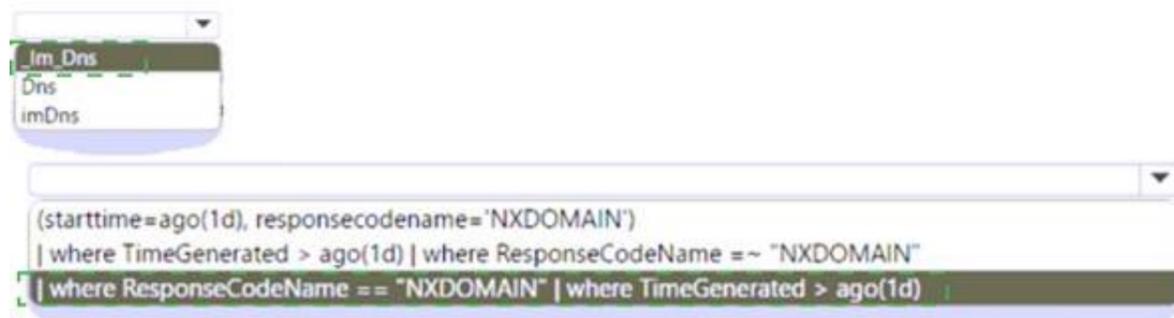
You have a Microsoft Sentinel workspace named Workspaces You configure Workspace1 to collect DNS events and deploy the Advanced Security information Model (ASIM) unifying parser for the DNS schema. You need to query the ASIM DNS schema to list all the DNS events from the last 24 hours that have a response code of 'NXDOMAIN' and were aggregated by the source IP address in 15-minute intervals. The solution must maximize query performance. How should you complete the query? To answer, select the appropriate options in the answer area
 NOTE: Each correct selection is worth one point.



A. Mastered
 B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 166

- (Topic 4)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender. You need to identify all the entities affected by an incident. Which tab should you use in the Microsoft 365 Defender portal?

A. Investigations
 B. Devices
 C. Evidence and Response
 D. Alerts

Answer: C

Explanation:

The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident. Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents>

NEW QUESTION 169

- (Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the 'Mitigate the threat' option.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

NEW QUESTION 170

- (Topic 4)

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.

Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Enable Entity behavior analytics.

B. Associate a playbook to the analytics rule that triggered the incident.

C. Enable the Fusion rule.

D. Add a playbook.

E. Create a workbook.

Answer: AB

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/enable-entity-behavior-analytics> <https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks>

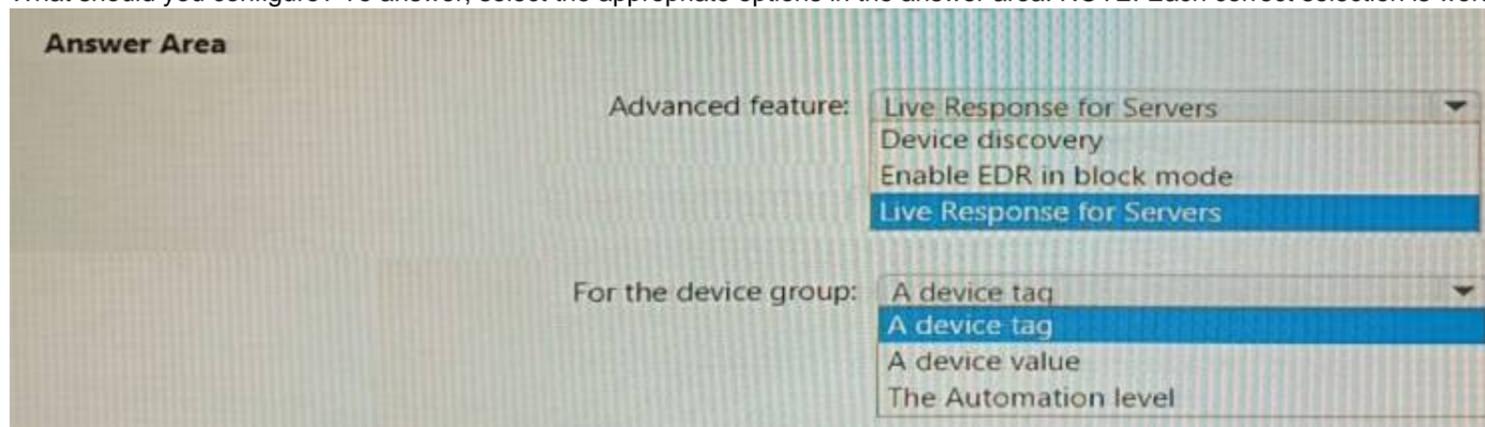
NEW QUESTION 173

HOTSPOT - (Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender for Endpoint.

You need to ensure that you can initiate remote shell connections to Windows servers by using the Microsoft 365 Defender portal.

What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

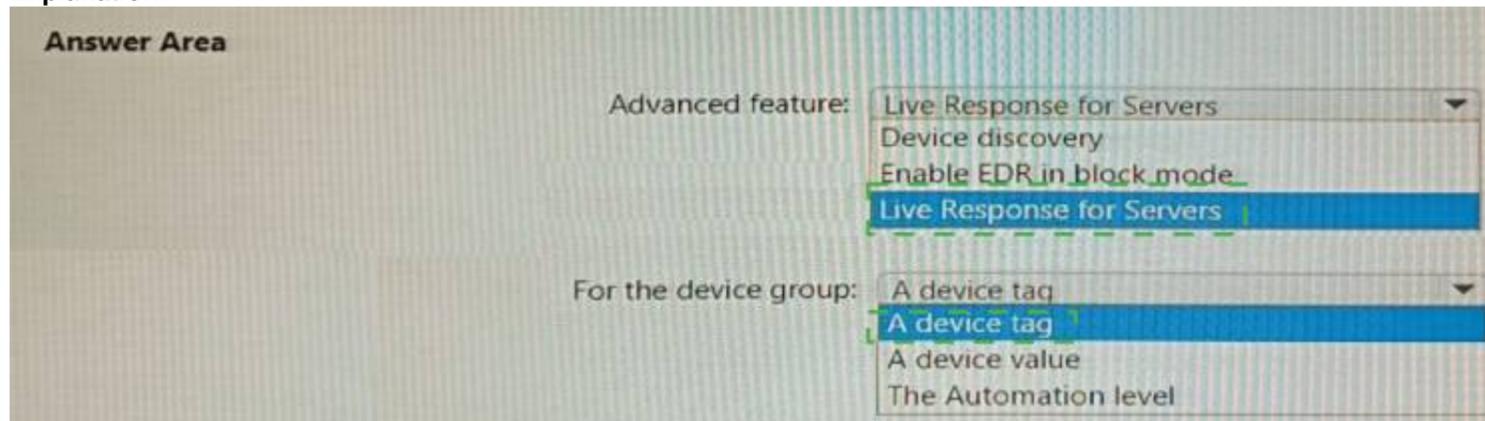


A. Mastered

B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 174

- (Topic 4)

You receive a security bulletin about a potential attack that uses an image file.

You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.

Which indicator type should you use?

- A. a URL/domain indicator that has Action set to Alert only
- B. a URL/domain indicator that has Action set to Alert and block
- C. a file hash indicator that has Action set to Alert and block
- D. a certificate indicator that has Action set to Alert and block

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide>

NEW QUESTION 176

- (Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

NEW QUESTION 180

- (Topic 4)

You are configuring Microsoft Cloud App Security.

You have a custom threat detection policy based on the IP address ranges of your company's United States-based offices.

You receive many alerts related to impossible travel and sign-ins from risky IP addresses. You determine that 99% of the alerts are legitimate sign-ins from your corporate offices. You need to prevent alerts for legitimate sign-ins from known locations.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Override automatic data enrichment.
- B. Add the IP addresses to the corporate address range category.
- C. Increase the sensitivity level of the impossible travel anomaly detection policy.
- D. Add the IP addresses to the other address range category and add a tag.
- E. Create an activity policy that has an exclusion for the IP addresses.

Answer: AD

NEW QUESTION 182

- (Topic 4)

You have a Microsoft Sentinel workspace named workspace1 that contains custom Kusto queries.

You need to create a Python-based Jupyter notebook that will create visuals. The visuals will display the results of the queries and be pinned to a dashboard. The solution must minimize development effort.

What should you use to create the visuals?

- A. plotly
- B. TensorFlow
- C. msticpy
- D. matplotlib

Answer: C

Explanation:

msticpy is a library for InfoSec investigation and hunting in Jupyter Notebooks. It includes functionality to: query log data from multiple sources. enrich the data with Threat Intelligence, geolocations and Azure resource data. extract Indicators of Activity (IoA) from logs and unpack encoded data.

MSTICPy reduces the amount of code that customers need to write for Microsoft Sentinel, and provides:

Data query capabilities, against Microsoft Sentinel tables, Microsoft Defender for Endpoint, Splunk, and other data sources.

Threat intelligence lookups with TI providers, such as VirusTotal and AlienVault OTX. Enrichment functions like geolocation of IP addresses, Indicator of Compromise (IoC) extraction, and WhoIs lookups.

Visualization tools using event timelines, process trees, and geo mapping.

Advanced analyses, such as time series decomposition, anomaly detection, and clustering.

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started> <https://msticpy.readthedocs.io/en/latest/>

NEW QUESTION 184

HOTSPOT - (Topic 4)

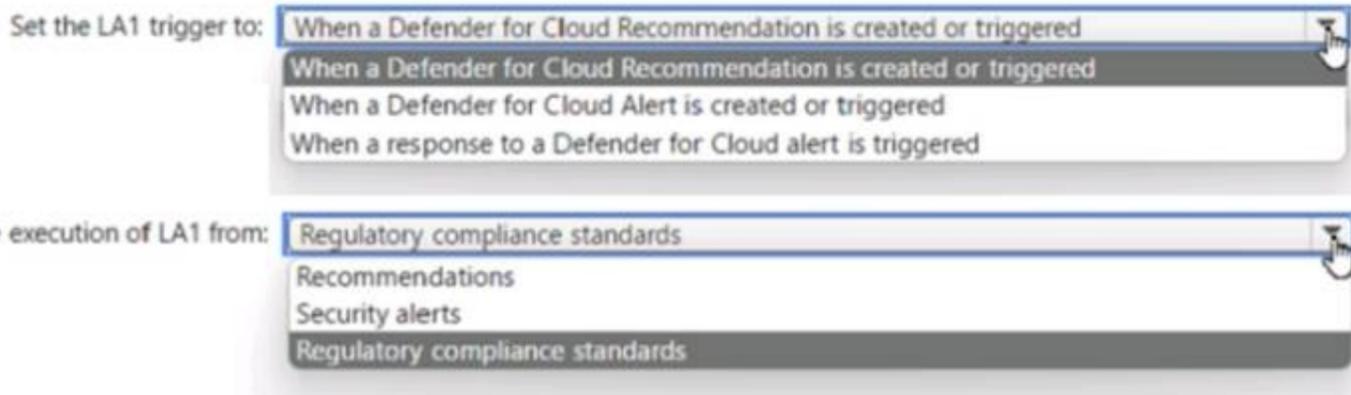
You have an Azure subscription that has Azure Defender enabled for all supported resource types.

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.

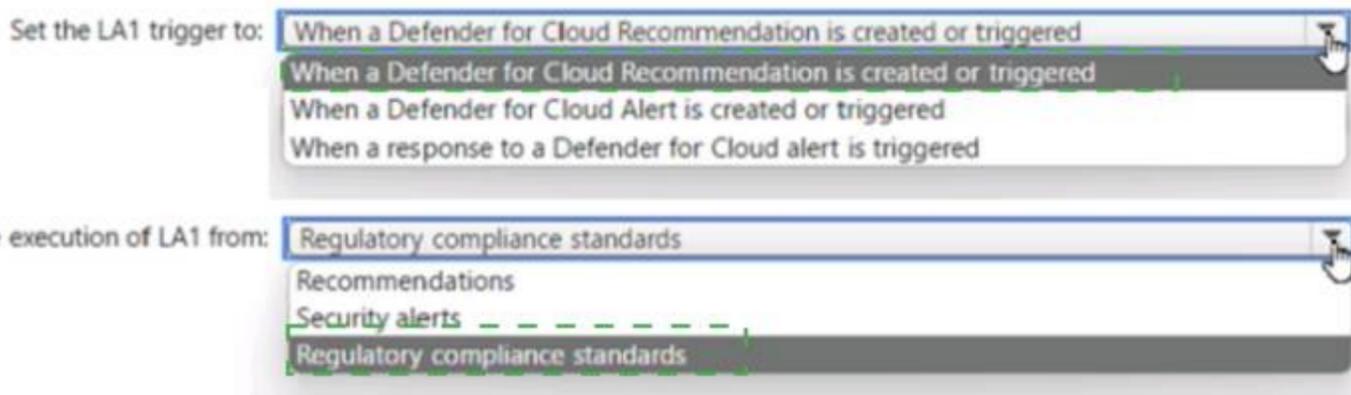
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 189

- (Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Azure Identity Protection, you configure the sign-in risk policy. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

NEW QUESTION 192

- (Topic 4)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender A remediation action for an automated investigation quarantines a file across multiple devices. You need to mark the file as safe and remove the file from quarantine on the devices. What should you use in the Microsoft 365 Defender portal?

- A. From Threat tracker, review the queries.
- B. From the History tab in the Action center, revert the actions.
- C. From the investigation page, review the AIR processes.
- D. From Quarantine from the Review page, modify the rules.

Answer: B

NEW QUESTION 196

- (Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the

stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You use Azure Security Center. You receive a security alert in Security Center. You need to view recommendations to resolve the alert in Security Center. Solution: From Regulatory compliance, you download the report. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

NEW QUESTION 197

- (Topic 4)
 You have an Azure Sentinel workspace. You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Answer: D

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand>

NEW QUESTION 199

- (Topic 4)
 You have a Microsoft Sentinel playbook that is triggered by using the Azure Activity connector. You need to create a new near-real-time (NRT) analytics rule that will use the playbook. What should you configure for the rule?

- A. the Incident automation settings
- B. entity mapping
- C. the query rule
- D. the Alert automation settings

Answer: B

NEW QUESTION 204

HOTSPOT - (Topic 4)
 You have an Azure subscription that uses Microsoft Sentinel and contains a user named User1. You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in Azure AD. The solution must use The principle of least privilege. Which roles should you assign to User1? To answer select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Azure AD role: Security administrator
 Global administrator
 Identity Governance Administrator
 Security administrator
 Security operator

Azure role: Microsoft Sentinel Contributor
 Microsoft Sentinel Automation Contributor
 Microsoft Sentinel Contributor
 Security Admin
 Security Assessment Contributor

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 209

- (Topic 4)

A company uses Azure Sentinel.

You need to create an automated threat response. What should you use?

- A. a data connector
- B. a playbook
- C. a workbook
- D. a Microsoft incident creation rule

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

NEW QUESTION 211

- (Topic 4)

You have a Microsoft Sentinel workspace that contains the following incident. Brute force attack against Azure Portal analytics rule has been triggered.

You need to identify the geolocation information that corresponds to the incident. What should you do?

- A. From Overview, review the Potential malicious events map.
- B. From Incidents, review the details of the iPCustomEntity entity associated with the incident.
- C. From Incidents, review the details of the AccouncCuscomEntity entity associated with the incident.
- D. From Investigation, review insights on the incident entity.

Answer: A

Explanation:

Potential malicious events: When traffic is detected from sources that are known to be malicious, Microsoft Sentinel alerts you on the map. If you see orange, it is inbound traffic: someone is trying to access your organization from a known malicious IP address. If you see Outbound (red) activity, it means that data from your network is being streamed out of your organization to a known malicious IP address.

NEW QUESTION 212

HOTSPOT - (Topic 4)

You have a Microsoft 365 E5 subscription.

You need to create a hunting query that will return every email that contains an attachment named Document.pdf. The query must meet the following requirements:

- Only show emails sent during the last hour.
- Optimize query performance.

How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

EmailAttachmentInfo

```
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

| where Subject == "Document Attachment" and FileName == "Document.pdf"

```
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

EmailAttachmentInfo

```
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

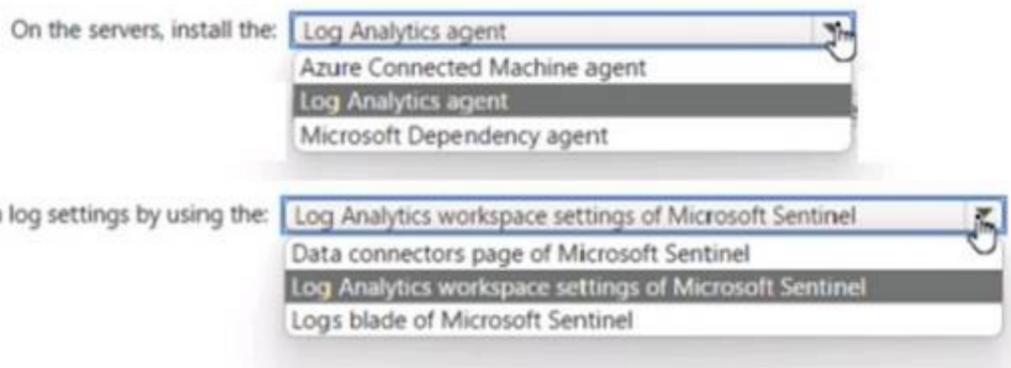
| where Subject == "Document Attachment" and FileName == "Document.pdf"

```
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

NEW QUESTION 213

HOTSPOT - (Topic 4)

Your on-premises network contains 100 servers that run Windows Server. You have an Azure subscription that uses Microsoft Sentinel. You need to upload custom logs from the on-premises servers to Microsoft Sentinel. What should you do? To answer, select the appropriate options in the answer area.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To upload custom logs from the on-premises servers to Microsoft Sentinel, you should install the Log Analytics agent on each of the 100 servers. The Log Analytics agent is a lightweight agent that runs on the server and allows it to connect to the cloud-based Microsoft Defender Security Center. Once installed, the agent will allow the Microsoft Sentinel service to collect and analyze the custom log data from the servers.

NEW QUESTION 216

HOTSPOT - (Topic 4)

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



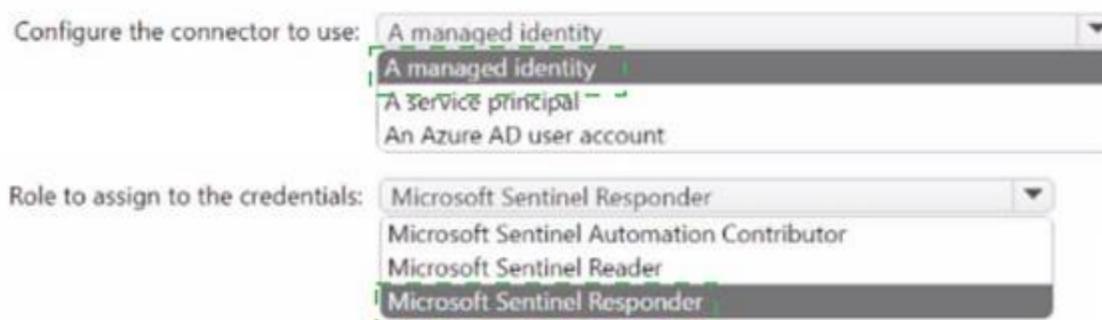
- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 218

- (Topic 4)

You use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center. What should you do?

- A. From Security alerts, select the alert, select Take Action, and then expand the Prevent future attacks section.
- B. From Security alerts, select Take Action, and then expand the Mitigate the threat section.
- C. From Regulatory compliance, download the report.
- D. From Recommendations, download the CSV report.

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

NEW QUESTION 219

- (Topic 4)

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You have a virtual machine named Server1 that runs Windows Server 2022 and is hosted in Amazon Web Services (AWS).

You need to collect logs and resolve vulnerabilities for Server1 by using Defender for Cloud.

What should you install first on Server1?

- A. the Microsoft Monitoring Agent
- B. the Azure Arc agent
- C. the Azure Monitor agent
- D. the Azure Pipelines agent

Answer: C

NEW QUESTION 222

- (Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint

You need to identify any devices that triggered a malware alert and collect evidence related to the alert. The solution must ensure that you can use the results to initiate device isolation for the affected devices.

What should you use in the Microsoft 365 Defender portal?

- A. Incidents
- B. Investigations
- C. Advanced hunting
- D. Remediation

Answer: A

NEW QUESTION 227

- (Topic 4)

You have a Microsoft 365 subscription that uses Azure Defender. You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege. Which role should you assign to SecAdmin1?

- A. the Security Reader role for the subscription
- B. the Contributor for the subscription
- C. the Contributor role for RG1
- D. the Owner role for RG1

Answer: C

NEW QUESTION 231

- (Topic 4)

You have a third-party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.

What should you do to route events to the SIEM solution?

- A. Create an Azure Sentinel workspace that has a Security Events connector.
- B. Configure the Diagnostics settings in Azure AD to stream to an event hub.
- C. Create an Azure Sentinel workspace that has an Azure Active Directory connector.
- D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring>

NEW QUESTION 232

.....

Relate Links

100% Pass Your SC-200 Exam with ExamBible Prep Materials

<https://www.exambible.com/SC-200-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>