QUESTION 61
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:
https://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal

QUESTION 62
You are responsible for responding to Azure Defender for Key Vault alerts.
During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.
What should you configure to mitigate the threat?

A. Key Vault firewalls and virtual networks
B. Azure Active Directory (Azure AD) permissions
C. role-based access control (RBAC) for the key vault
D. the access policy settings of the key vault

Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/key-vault/general/network-security

QUESTION 63
You have an Azure subscription that contains a Log Analytics workspace.
You need to enable just-in-time (JIT) VM access and network detections for Azure resources.
Where should you enable Azure Defender?

A. at the subscription level
B. at the workspace level
C. at the resource level

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/security-center/enable-azure-defender

QUESTION 64
You use Azure Defender.
You have an Azure Storage account that contains sensitive information.
You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Azure Security Center, enable workflow automation.
B. Create an Azure logic app that has a manual trigger.
C. Create an Azure logic app that has an Azure Security Center alert trigger.
D. Create an Azure logic app that has an HTTP trigger.
E. From Azure Active Directory (Azure AD), add an app registration.

Answer: AC
Explanation:
https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

QUESTION 65
You recently deployed Azure Sentinel.
You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.
You need to ensure that the Fusion rule can generate alerts.
What should you do?

A. Disable, and then enable the rule.
B. Add data connectors
C. Create a new machine learning analytics rule.
D. Add a hunting bookmark.

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

QUESTION 66
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:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION 67
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 Azure Sentinel to a workspace.
D. Create a data connector in Azure Sentinel.

Answer: C
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

QUESTION 68
You create a custom analytics rule to detect threats in Azure Sentinel.
You discover that the rule fails intermittently.
What are two possible causes of the failures? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. The rule query takes too long to run and times out.
B. The target workspace was deleted.
C. Permissions to the data sources of the rule query were modified.
D. There are connectivity issues between the data sources and Log Analytics

Answer: AD
Explanation:
Incorrect Answers:
B: This would cause it to fail every time, not just intermittently.
C: This would cause it to fail every time, not just intermittently.

QUESTION 69
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 scheduled query rule for a data connector.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

QUESTION 70
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:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

QUESTION 71
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 Microsoft incident creation rule for a data connector.
Does this meet the goal?

A. Yes
B. No

Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

QUESTION 72
Hotspot Question
You are informed of an increase in malicious email being received by users.
You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.
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

```
let MaliciousEmails = [EmailAttachementInfo | EmailEvents | IdentityLogonEvents]
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join ( [EmailAttachementInfo | EmailEvents | IdentityLogonEvents]
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [select 20 | take 20 | top 20]
```

Answer:

Answer Area

```
let MaliciousEmails = [EmailAttachementInfo | EmailEvents | IdentityLogonEvents]
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join ( [EmailAttachementInfo | EmailEvents | IdentityLogonEvents]
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [select 20 | take 20 | top 20]
```

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

QUESTION 73
Hotspot Question
You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.
You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will

be based on the match of the SHA256 hash.
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
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Answer:

Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-

worldwide

QUESTION 74
Hotspot Question
You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.
How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

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

- Microsoft.Automation
- Microsoft.Logic
- Microsoft.Security

Answer:

Answer Area

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

Microsoft.Automation
Microsoft.Logic
Microsoft.Security

Microsoft.Automation
Microsoft.Logic
Microsoft.Security

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

QUESTION 75
Drag and Drop Question
Your company deploys Azure Sentinel.
You plan to delegate the administration of Azure Sentinel to various groups.
You need to delegate the following tasks:
- Create and run playbooks
- Create workbooks and analytic rules.

The solution must use the principle of least privilege.
Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. 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.

Answer Area

Azure Sentinel Contributor
Azure Sentinel Responder
Azure Sentinel Reader
Logic App Contributor

Create and run playbooks: [ ]
Create workbooks and analytic rules: [ ]

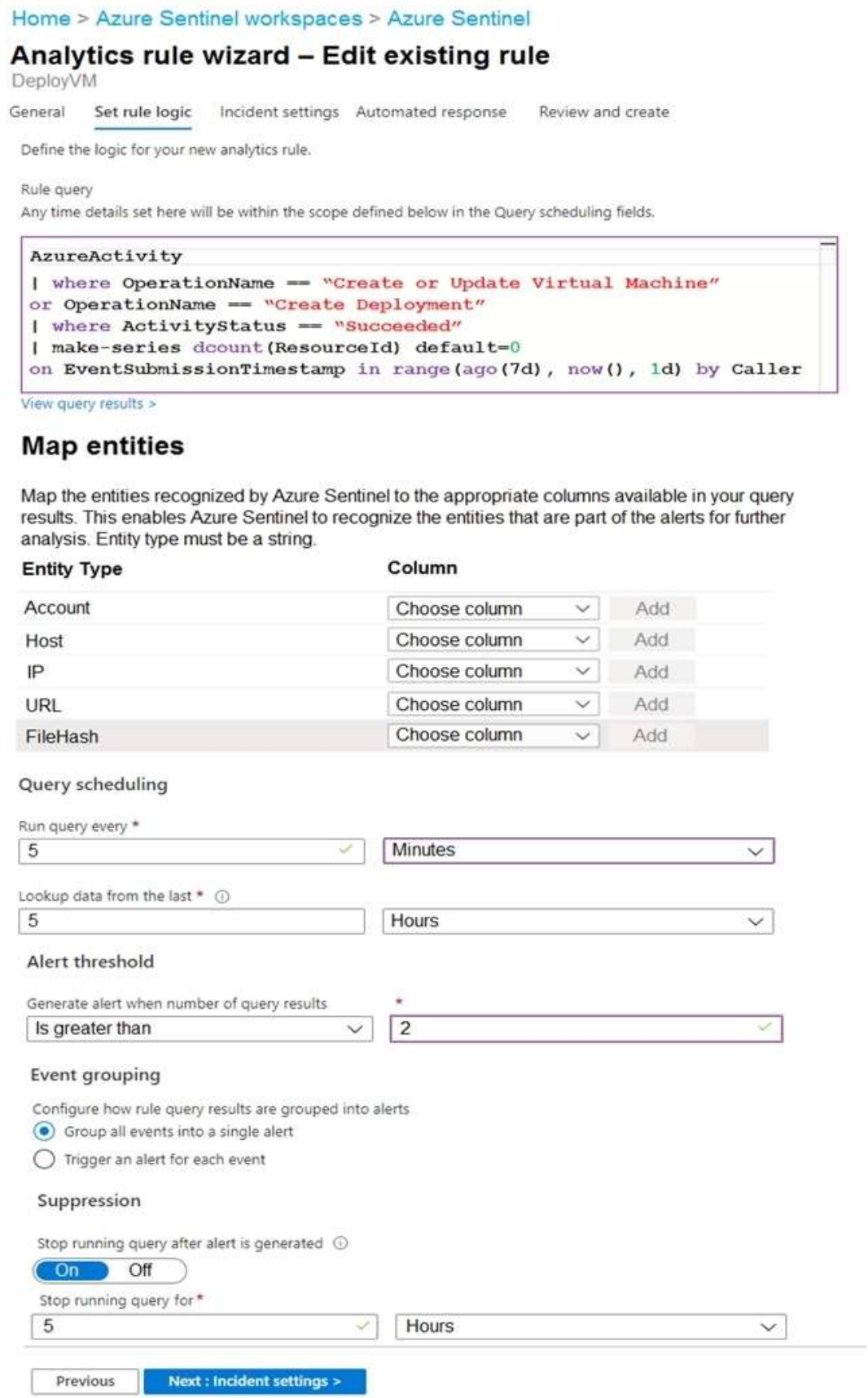
Answer:

Answer Area

Azure Sentinel Responder	Create and run playbooks:	Logic App Contributor
Azure Sentinel Reader	Create workbooks and analytic rules:	Azure Sentinel Contributor

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

QUESTION 76
Hotspot Question
You use Azure Sentinel to monitor irregular Azure activity.
You create custom analytics rules to detect threats as shown in the following exhibit.



You do NOT define any incident settings as part of the rule definition.
Use the drop-down menus to select the answer choice that completes each statement based on the information

presented in the graphic.
NOTE: Each correct selection is worth one point.

Answer Area

If a user deploys three Azure virtual machines simultaneously, how many times will you receive **[answer choice]** in the next five hours.

- 0 alerts
- 1 alert
- 2 alerts
- 3 alerts

If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive **[answer choice]**.

- 0 alerts
- 1 alert
- 2 alerts
- 3 alerts

Answer:

Answer Area

If a user deploys three Azure virtual machines simultaneously, how many times will you receive **[answer choice]** in the next five hours.

- 0 alerts
- **1 alert**
- 2 alerts
- 3 alerts

If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive **[answer choice]**.

- 0 alerts
- **1 alert**
- 2 alerts
- 3 alerts

Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom