

Microsoft.SC-200.by.Rina.154q

Number: SC-200
Passing Score: 800
Time Limit: 120
File Version: 11.0

Exam Code: SC-200
Exam Name: Microsoft Security Operations Analyst



Case Study 01 - Mitigate threats using Azure Defender

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware Inc. is a renewable company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment

Identity Environment

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

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

Network Environment

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment

The on-premises network contains the computers shown in the following table.

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

Current problems

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes

Litware plans to implement the following changes:

Create and configure Azure Sentinel in the Azure subscription.

Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements

Litware identifies the following business requirements:

The principle of least privilege must be used whenever possible.

Costs must be minimized, as long as all other requirements are met.

Logs collected by Log Analytics must provide a full audit trail of user activities.

All domain controllers must be protected by using Microsoft Defender for Identity.

Azure Information Protection Requirements

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

Microsoft Defender for Endpoint requirements

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

Microsoft Cloud App Security requirements

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

Azure Defender Requirements

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

Azure Sentinel Requirements

Litware must meet the following Azure Sentinel requirements:

Integrate Azure Sentinel and Cloud App Security.

Ensure that a user named admin1 can configure Azure Sentinel playbooks.

Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.

Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.

Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

QUESTION 1

HOTSPOT

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.

Hot Area:

Answer Area

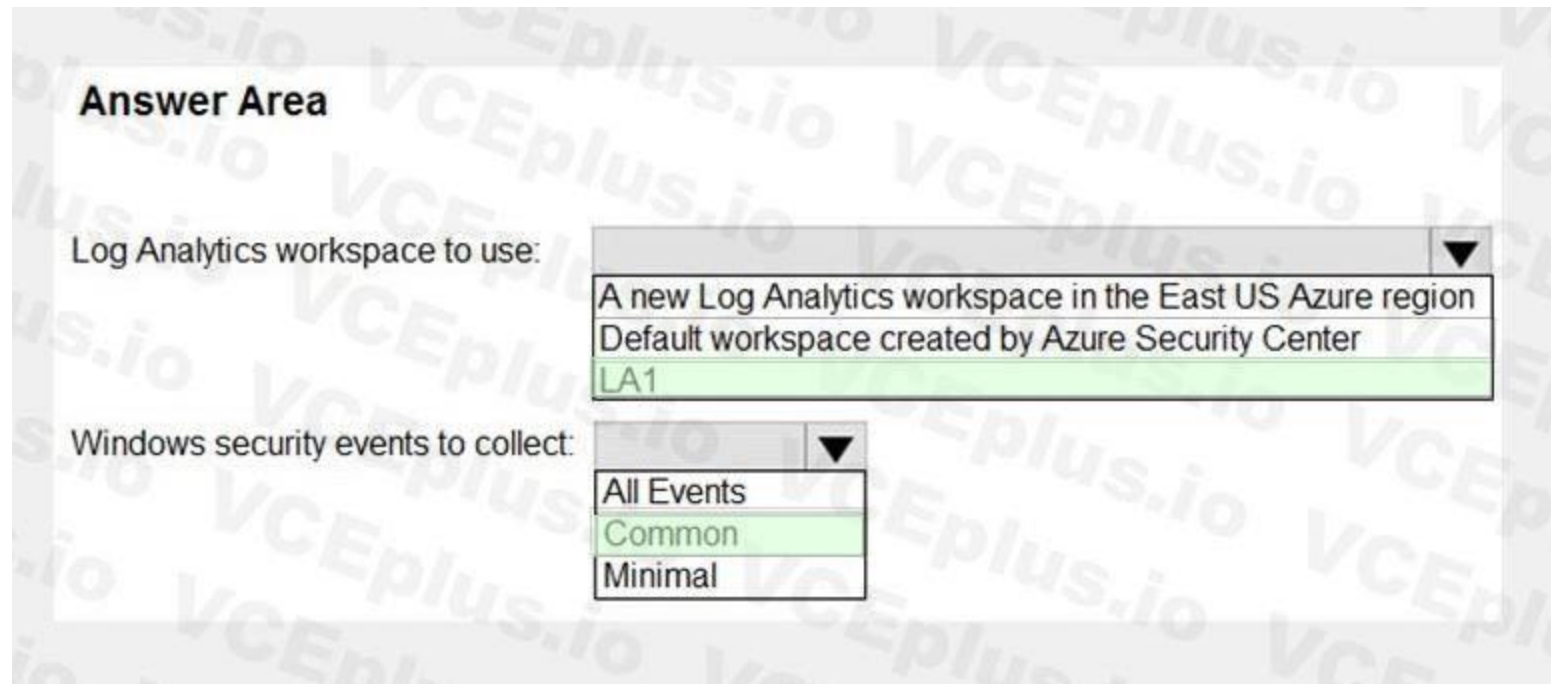
Log Analytics workspace to use:

- 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

Answer Area:



Section:

Explanation:

Case Study 02 - Mitigate threats using Azure Defender

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment

End-User Environment

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for

Microsoft Cloud

App Security-protected applications.

Requirements

Planned Changes

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements

Contoso identifies the following technical requirements:

Receive alerts if an Azure virtual machine is under brute force attack.

Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.

Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.

Develop a procedure to remediate Azure Defender for Key Vault alerts for Contoso in case of external and internal threats. The solution must minimize the impact on legitimate attempts to access the key vault content.

Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

BehaviorAnalytics

| where ActivityType == "FailedLogOn"

| where _____ == True

QUESTION 1

You need to recommend a solution to meet the technical requirements for the Azure virtual machines.

What should you include in the recommendation?

- A. just-in-time (JIT) access
- B. Azure Defender
- C. Azure Firewall
- D. Azure Application Gateway

Correct Answer: B

Section:

Explanation:

Reference:

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



QUESTION 2

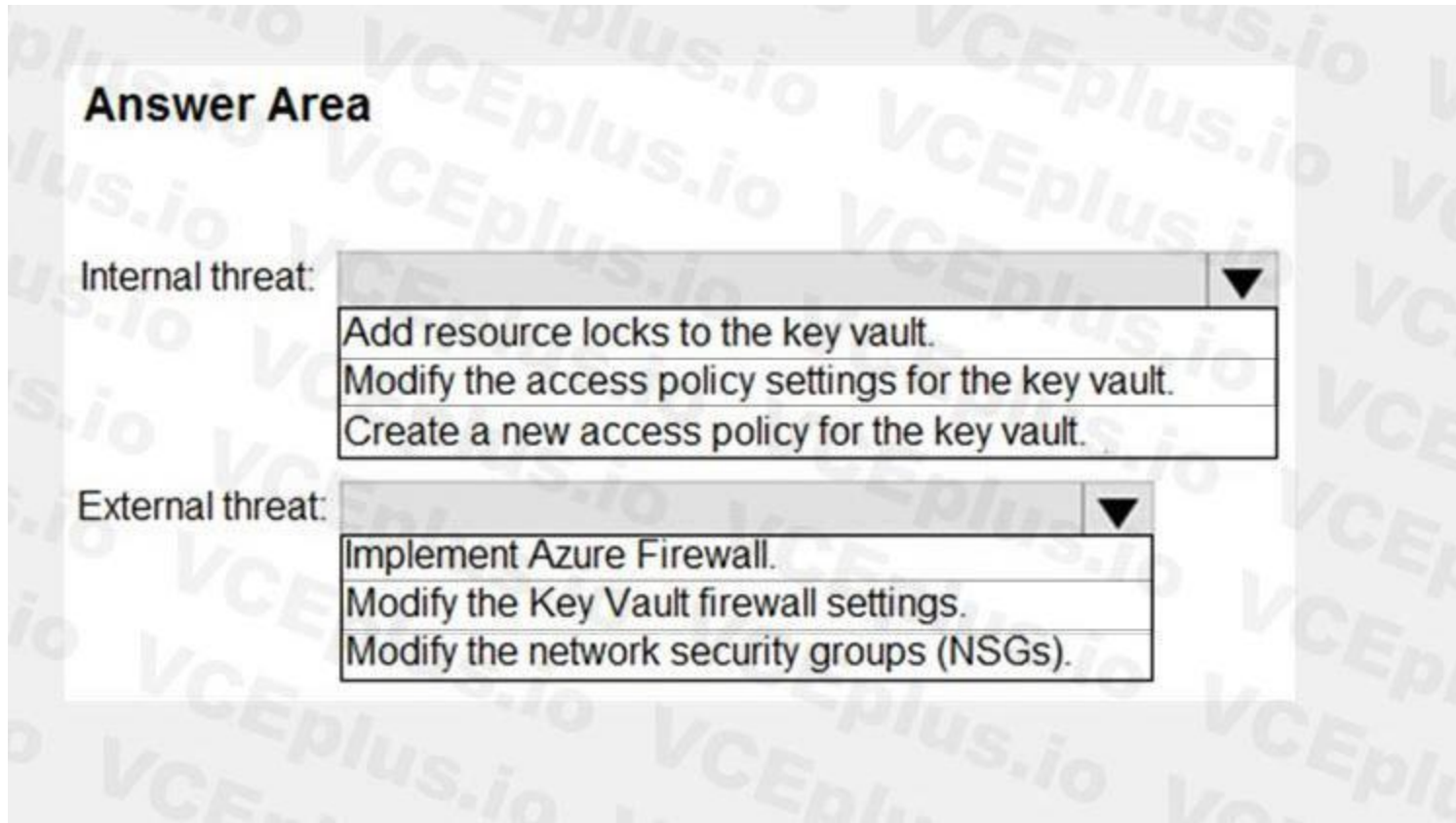
HOTSPOT

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

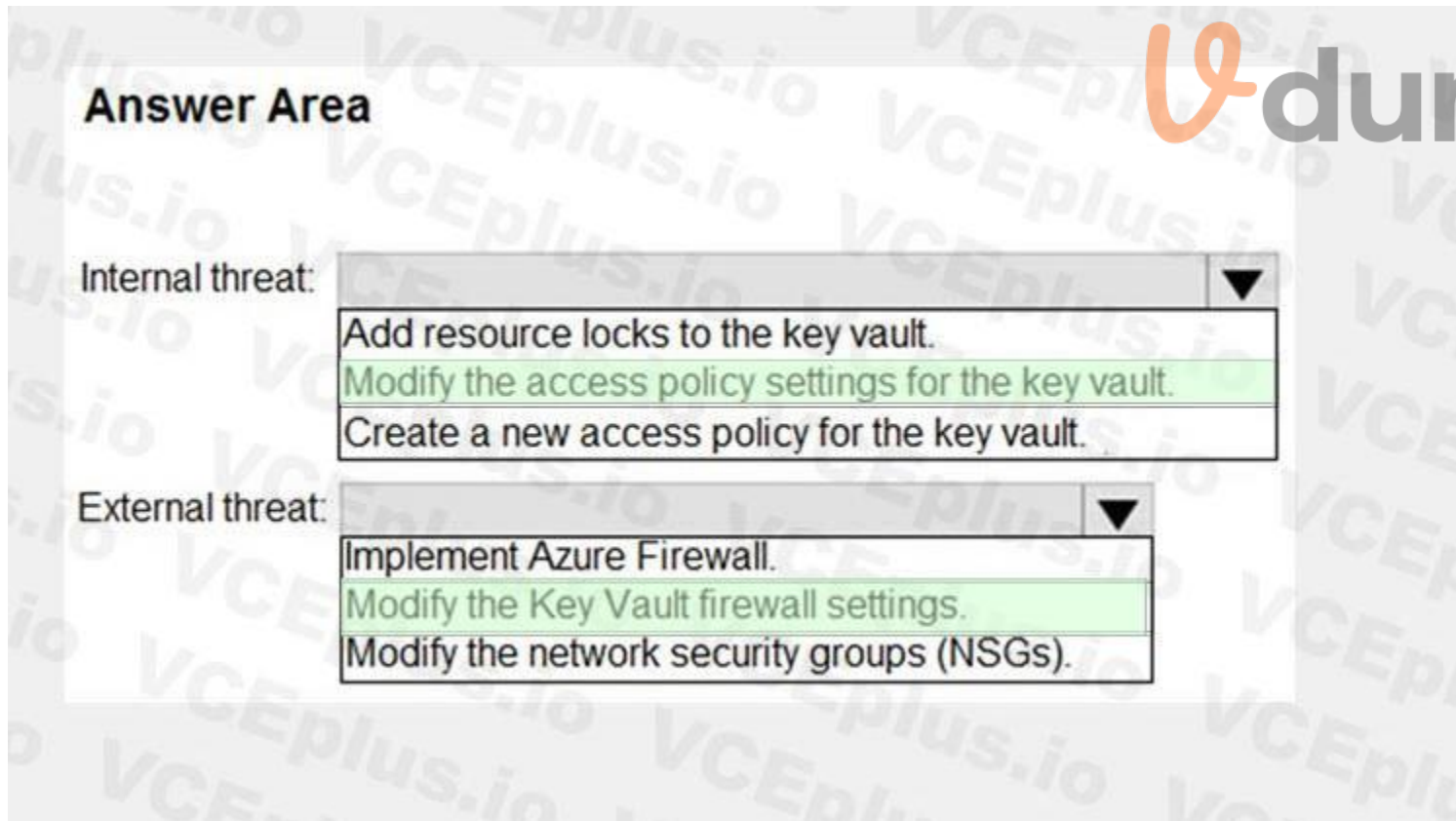
What should you recommend for each threat? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/security-features>

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

03 - Mitigate threats using Azure Defender

QUESTION 1

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

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-azure-defender>

QUESTION 2

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.

Correct Answer: A, C

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center>

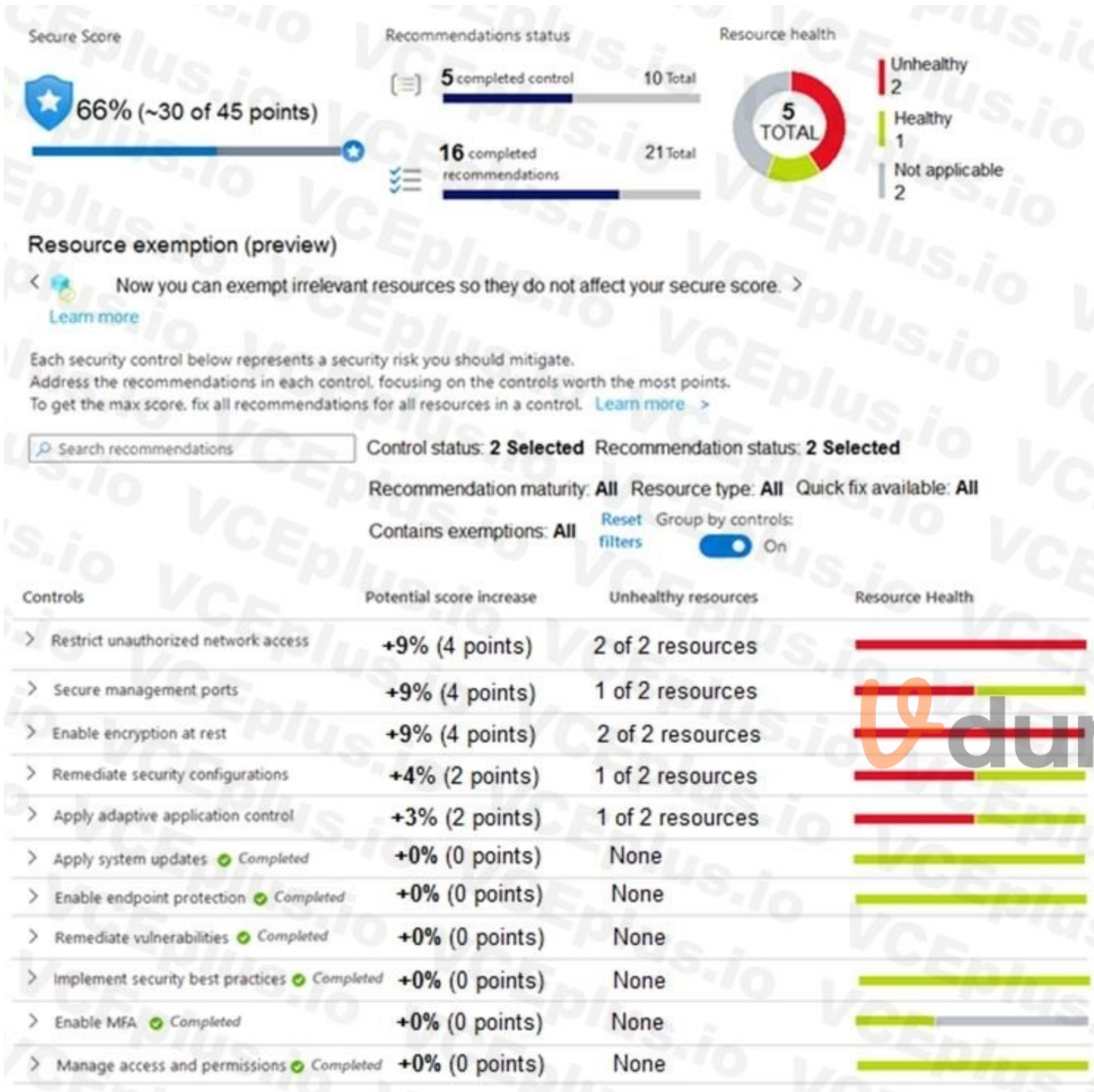
<https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-azure-defender>

QUESTION 3

HOTSPOT

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.)





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.



Hot Area:

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"/>

Answer Area:

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input checked="" type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input checked="" 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 checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833>

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770>

QUESTION 4

HOTSPOT

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.

Hot Area:



Answer Area

Entity type:

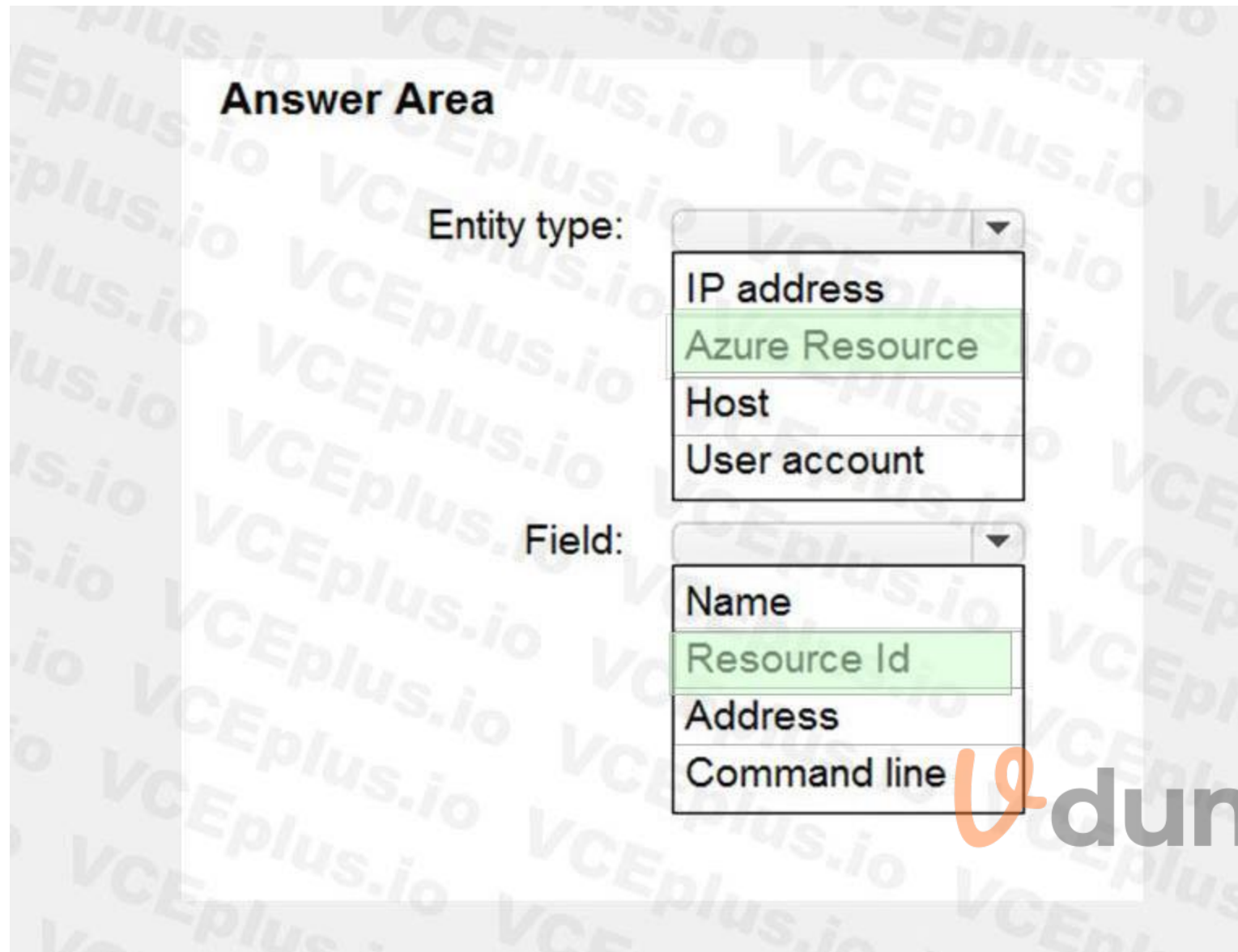
▼
IP address
Azure Resource
Host
User account

Field:

▼
Name
Resource Id
Address
Command line

 **Vdumps**

Answer Area:



Section:

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920>

QUESTION 5

You create an Azure subscription.

You enable Azure Defender for the subscription.

You need to use Azure Defender to protect on-premises computers.

What should you do on the on-premises computers?

- A. Install the Log Analytics agent.
- B. Install the Dependency agent.
- C. Configure the Hybrid Runbook Worker role.
- D. Install the Connected Machine agent.

Correct Answer: A

Section:

Explanation:

Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.

Data is collected using:

The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.

Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.

Reference:

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

QUESTION 6

A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.

The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center.

You need to ensure that the security administrator receives email alerts for all the activities.

What should you configure in the Security Center settings?

- A. the severity level of email notifications
- B. a cloud connector
- C. the Azure Defender plans
- D. the integration settings for Threat detection

Correct Answer: A

Section:

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/microsoft-365-defender/get-email-notifications-on-new-incidents-from-microsoft-365/ba-p/2012518>

QUESTION 7

DRAG DROP

You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.

You need to hide the alerts automatically in Security Center.

Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

Select and Place:

Actions

Select **Pricing & settings**.

Select **Security alerts**.

Select **IP** as the entity type and specify the IP address.

Select **Azure Resource** as the entity type and specify the ID.

Select **Suppression rules**, and then select **Create new suppression rule**.

Select **Security policy**.

Answer area



Correct Answer:

Actions

Select **Pricing & settings**.

Select **IP** as the entity type and specify the IP address.

Select **Security policy**.

Answer area

Select **Security alerts**.

Select **Suppression rules**, and then select **Create new suppression rule**.

Select **Azure Resource** as the entity type and specify the ID.



Section:

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920>

QUESTION 8

DRAG DROP

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

Enable and disable Azure Defender.

Apply security recommendations to resource.

The solution must use the principle of least privilege.

Which Azure Security Center 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.

Select and Place:

Roles	Answer Area
Security Admin	Enable and disable Azure Defender: <input type="text" value="Role"/>
Resource Group Owner	Apply security recommendations to a resource: <input type="text" value="Role"/>
Subscription Contributor	
Subscription Owner	

Correct Answer:

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

Section:

Explanation:

Reference:

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

QUESTION 9

DRAG DROP

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.

Select and Place:

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



Correct Answer:

Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Advanced hunting, search for `cveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

Answer Area

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

Select **Security recommendations**.

Create the remediation request.



Vdumps

Section:

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271>

QUESTION 10

HOTSPOT

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 Azure Security Center.

You need to test LA1 in Security Center.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Set the LA1 trigger to:

▼
When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

▼
Recommendations
Workflow automation
Security alerts

Answer Area:

Answer Area

Set the LA1 trigger to:

▼
When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

▼
Recommendations
Workflow automation
Security alerts



Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run>

QUESTION 11

DRAG DROP

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

You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration. 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.

Select and Place:

Actions

- Change the alert severity threshold for emails to **Medium**.
- Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
- Enable Azure Defender for the subscription.
- Change the alert severity threshold for emails to **Low**.
- Run the executable file and specify the appropriate arguments.
- Rename the executable file as AlertTest.exe.

Answer Area

Navigation icons: left arrow, right arrow, up arrow, down arrow.

Correct Answer:

Actions

- Change the alert severity threshold for emails to **Medium**.
-
-
- Change the alert severity threshold for emails to **Low**.
-
- Rename the executable file as AlertTest.exe.

Answer Area

- Enable Azure Defender for the subscription.
- 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.

Navigation icons: left arrow, right arrow, up arrow, down arrow.

Section:

Explanation:

Reference:



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

QUESTION 12

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

Correct Answer: B

Section:

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>

QUESTION 13

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

- A. Modify the access control settings for the key vault.
- B. Enable the Key Vault firewall.
- C. Create an application security group.
- D. Modify the access policy for the key vault.

Correct Answer: B

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usaQe>

QUESTION 14

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 Sec Admin in 1.

You need to ensure that SecAdmin 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 SecAdmin?

- 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

Correct Answer: C

Section:

QUESTION 15

You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. `cp /bin/echo ./asc_alerttest_662jfi039n`

B. `./alerttest testing eicar pipe`

C. `cp /bin/echo ./alerttest`

D. `./asc_alerttest_662jfi039n testing eicar pipe`

Correct Answer: A, D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-alertr-validation#simulate-alerts-on-your-azure-vms-linux->

QUESTION 16

You create an Azure subscription named sub1.

In sub1, you create a Log Analytics workspace named workspace*!.

You enable Azure Security Center and configure Security Center to use workspace*!.

You need to collect security event logs from the Azure virtual machines that report to workspace 1.

What should you do?

A. From Security Center, enable data collection

B. In sub*!, register a provider.

C. From Security Center, create a Workflow automation.

D. In workspace*!, create a workbook.

Correct Answer: A

Section:

Explanation:

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

QUESTION 17

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

Correct Answer: C

Section:

Explanation:

Reference:

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

QUESTION 18

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

Correct Answer: B

Section:

Explanation:

Reference:

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



QUESTION 19

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 Mitigate the threat section.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

Explanation:

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

QUESTION 20

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

Correct Answer: C

Section:

Explanation:

Reference:

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

QUESTION 21

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

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/network-security>

QUESTION 22

DRAG DROP

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.

Select and Place:



Actions

- 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.

Answer Area

Navigation icons: Left arrow, Right arrow, Up arrow, Down arrow.

Correct Answer:

Actions

-
-
-
-
-

Answer Area

- 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.

Navigation icons: Left arrow, Right arrow, Up arrow, Down arrow.

Section:

Explanation:

Reference:

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

QUESTION 23

HOTSPOT

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

How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

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]"  
        }  
      ]  
    }  
  },  
],
```

Answer Area:

Answer Area

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



Section:

Explanation:

Reference:

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

QUESTION 24

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.

Correct Answer: B

Section:

Explanation:

Reference:

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

QUESTION 25

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.

Correct Answer: B

Section:

Explanation:

Reference:

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

QUESTION 26

HOTSPOT

You have an Azure subscription that uses Azure Defender.

You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.

You need to create an Azure policy that will perform threat remediation automatically.

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.

Hot Area:

Answer Area

Set available effects to:

	▼
Append	
DeployIfNotExists	
EnforceRegoPolicy	

To perform remediation use:

	▼
An Azure Automation runbook that has a webhook	
An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered	
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered	

Answer Area:



Answer Area

Set available effects to:

	▼
Append	
DeployIfNotExists	
EnforceRegoPolicy	

To perform remediation use:

	▼
An Azure Automation runbook that has a webhook	
An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered	
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered	

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects>

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

Case Study 01 - Mitigate threats using Azure Sentinel**Case study**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment**End-User Environment**

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for

Microsoft Cloud

App Security-protected applications.

Requirements**Planned Changes**

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements

Contoso identifies the following technical requirements:

Receive alerts if an Azure virtual machine is under brute force attack.

Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.

Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.

Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure AD applications.

Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

BehaviorAnalytics

```
| where ActivityType == "FailedLogOn"
```

```
| where _____ == True
```

QUESTION 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 Functions
- D. Azure Sentinel livestreams

Correct Answer: B

Section:

Explanation:

Reference:

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

QUESTION 2

HOTSPOT

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)
```

| summarize activityCount =
ActionType, AccountDisplayName

| where activityCount > 5

avg()
count()
sum()

by FolderPath, FileName,

Answer Area:

Answer Area

```
| where TimeStamp > ago(2d)
| summarize activityCount =
ActionType, AccountDisplayName
| where activityCount > 5
```

by FolderPath, FileName,

avg()
count()
sum()

Section:

Explanation:

QUESTION 3

HOTSPOT

You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical 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.

Hot Area:



Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

0
1
2
3

Query element required to correlate data between tenants:

extend
project
workspace

Answer Area:

Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

0
1
2
3

Query element required to correlate data between tenants:

extend
project
workspace



Section:

Explanation:

Reference:

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

QUESTION 4

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

Correct Answer: D

Section:

Explanation:

Case Study 02 - Mitigate threats using Azure Sentinel

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware Inc. is a renewable company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment

Identity Environment

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

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

Network Environment

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment

The on-premises network contains the computers shown in the following table.

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

Current problems

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes

Litware plans to implement the following changes:

Create and configure Azure Sentinel in the Azure subscription.

Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements

Litware identifies the following business requirements:

The principle of least privilege must be used whenever possible.

Costs must be minimized, as long as all other requirements are met.

Logs collected by Log Analytics must provide a full audit trail of user activities.

All domain controllers must be protected by using Microsoft Defender for Identity.

Azure Information Protection Requirements

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

Microsoft Defender for Endpoint requirements

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

Microsoft Cloud App Security requirements

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

Azure Defender Requirements

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

Azure Sentinel Requirements

Litware must meet the following Azure Sentinel requirements:

Integrate Azure Sentinel and Cloud App Security.

Ensure that a user named admin1 can configure Azure Sentinel playbooks.

Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.

Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.

Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

QUESTION 1

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 Run book Operator
- C. Azure Sentinel Contributor
- D. Logic App Contributor

Correct Answer: C

Section:

Explanation:

Reference:

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

QUESTION 2

You need to create the test rule to meet the Azure Sentinel requirements.

What should you do when you create the rule?

- A. From Set rule logic, turn off suppression.
- B. From Analytics rule details, configure the tactics.
- C. From Set rule logic, map the entities.
- D. From Analytics rule details, configure the severity.

Correct Answer: C

Section:

Explanation:

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

QUESTION 3

DRAG DROP

You need to add notes to the events to meet the Azure Sentinel requirements.

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

Select and Place:

Actions

- Add a bookmark and map an entity.
- From Azure Monitor, run a Log Analytics query.
- Add the query to favorites.
- Select a query result.
- From the Azure Sentinel workspace, run a Log Analytics query.

Answer Area



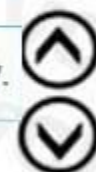
Correct Answer:

Actions

-
- From Azure Monitor, run a Log Analytics query.
- Add the query to favorites.
-
-

Answer Area

- From the Azure Sentinel workspace, run a Log Analytics query.
- Select a query result.
- Add a bookmark and map an entity.



Section:

Explanation:

Reference:

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

QUESTION 4

HOTSPOT

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.

Hot Area:

Answer Area

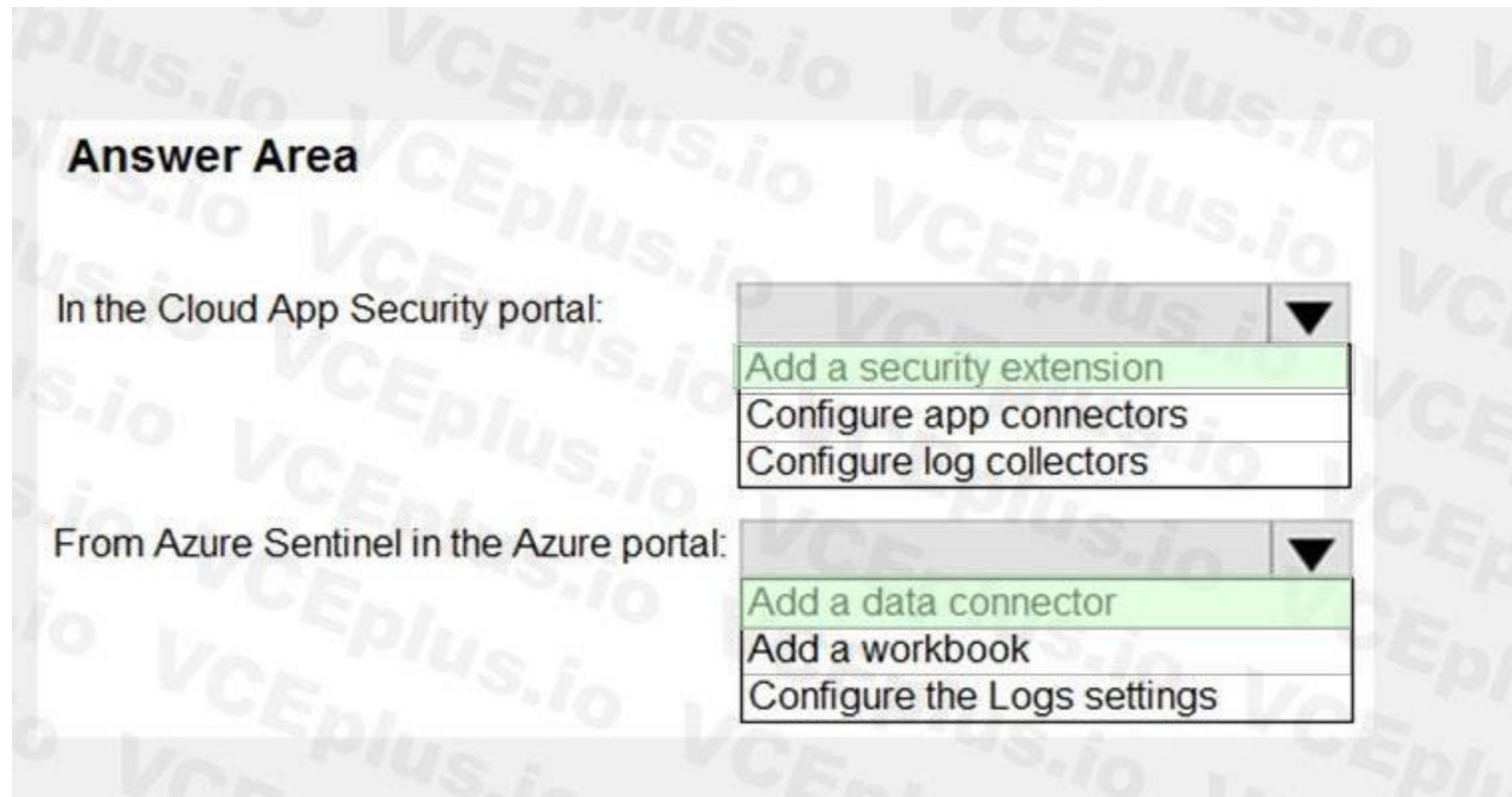
In the Cloud App Security portal:

- 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

Answer Area:



Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel>

QUESTION 5

HOTSPOT

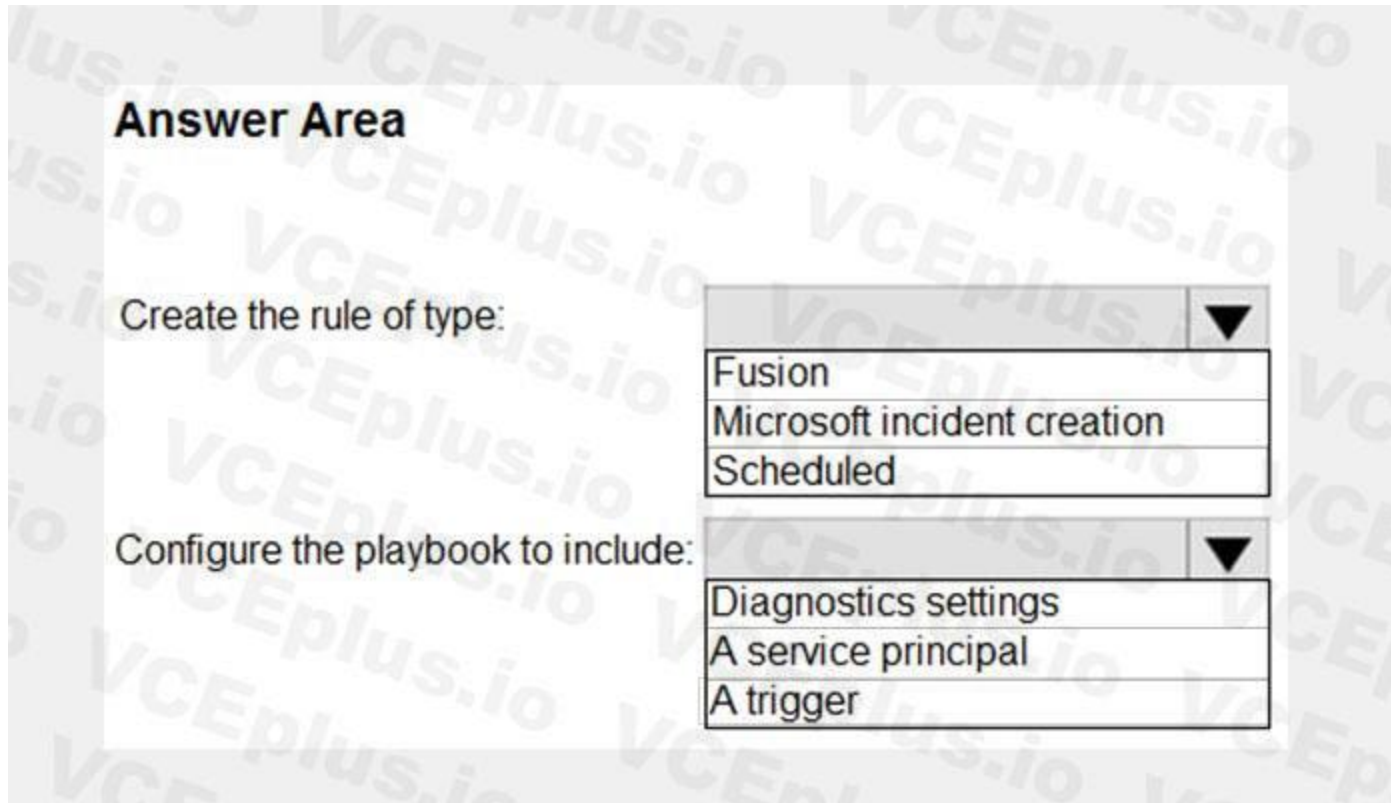
You need to create the analytics rule to meet the Azure Sentinel requirements.

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

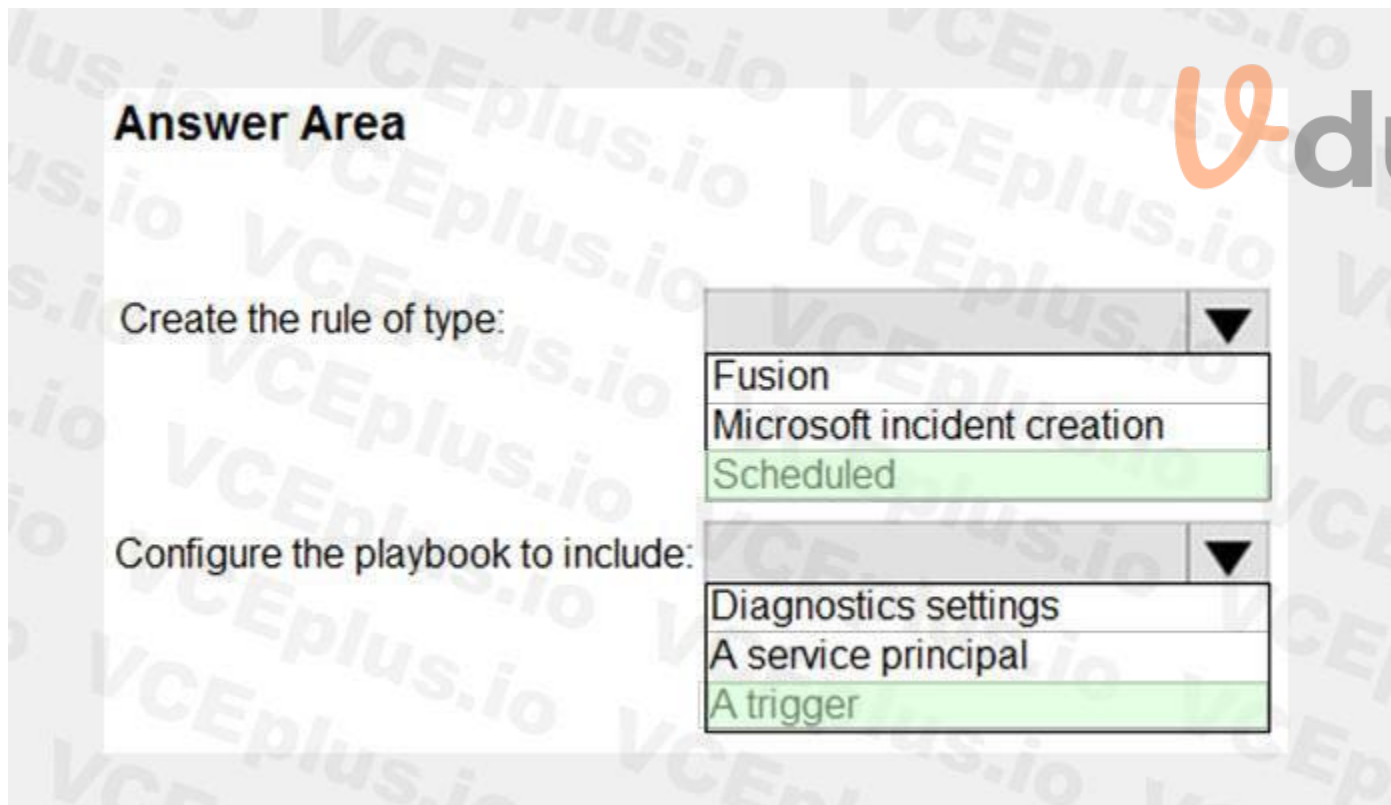
NOTE: Each correct selection is worth one point.

Hot Area:





Answer Area:



 **vdumps**

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#set-automated-responses-and-create-the-rule>

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

QUESTION 6

You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements. Which two configurations should you modify? Each correct answer present part of the solution.
NOTE: Each correct selection is worth one point.

- A. the Onboarding settings from Device management in Microsoft Defender Security Center
- B. Cloud App Security anomaly detection policies
- C. Advanced features from Settings in Microsoft Defender Security Center
- D. the Cloud Discovery settings in Cloud App Security

Correct Answer: C, D

Section:

Explanation:

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

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/mde-govern>

QUESTION 7

You need to restrict cloud apps running on CUENT1 to meet the Microsoft Defender for Endpoint requirements. Which two configurations should you modify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. the Cloud Discovery settings in Microsoft Defender for Cloud Apps
- B. the Onboarding settings from Device management in Settings in Microsoft 365 Defender portal
- C. Microsoft Defender for Cloud Apps anomaly detection policies
- D. Advanced features from the Endpoints Settings in the Microsoft 365 Defender portal

Correct Answer: A, D

Section:

QUESTION 8

HOTSPOT

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.

Hot Area:

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

Answer Area:

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

Section:

Explanation:

QUESTION 9

HOTSPOT

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.

Hot Area:

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	

Answer Area:

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	

Section:

Explanation:

Exam F

QUESTION 1

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.

Correct Answer: B

Section:

Explanation:

QUESTION 2

HOTSPOT

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.

Hot Area:

```
(starttime=ago(1d), responsecodename='NXDOMAIN')
| where TimeGenerated > ago(1d) | where ResponseCodeName == "NXDOMAIN"
| where ResponseCodeName == "NXDOMAIN" | where TimeGenerated > ago(1d)
```

Answer Area:

```
(starttime=ago(1d), responsecodename='NXDOMAIN')
| where TimeGenerated > ago(1d) | where ResponseCodeName == "NXDOMAIN"
| where ResponseCodeName == "NXDOMAIN" | where TimeGenerated > ago(1d)
```

Section:

Explanation:

QUESTION 3

HOTSPOT

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.

Hot Area:

```
AuditLogs |> in ("Microsoft.Network/networkSecurityGroups/securityRules/write")
AzureActivity |> where Status == "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
```

Answer Area:

```
AuditLogs |> in ("Microsoft.Network/networkSecurityGroups/securityRules/write")
AzureActivity |> where Status == "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
```



Section:

Explanation:

QUESTION 4

You have an Azure subscription that uses Microsoft Sentinel.

You detect a new threat by using a hunting query.

You need to ensure that Microsoft Sentinel automatically detects the threat. The solution must minimize administrative effort.

What should you do?

- A. Create a playbook.
- B. Create a watchlist.
- C. Create an analytics rule.
- D. Add the query to a workbook.

Correct Answer: A

Section:

Explanation:

QUESTION 5

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

Correct Answer: A

Section:

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.

Reference:

<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>

QUESTION 6

HOTSPOT

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

List all incidents by incident number.

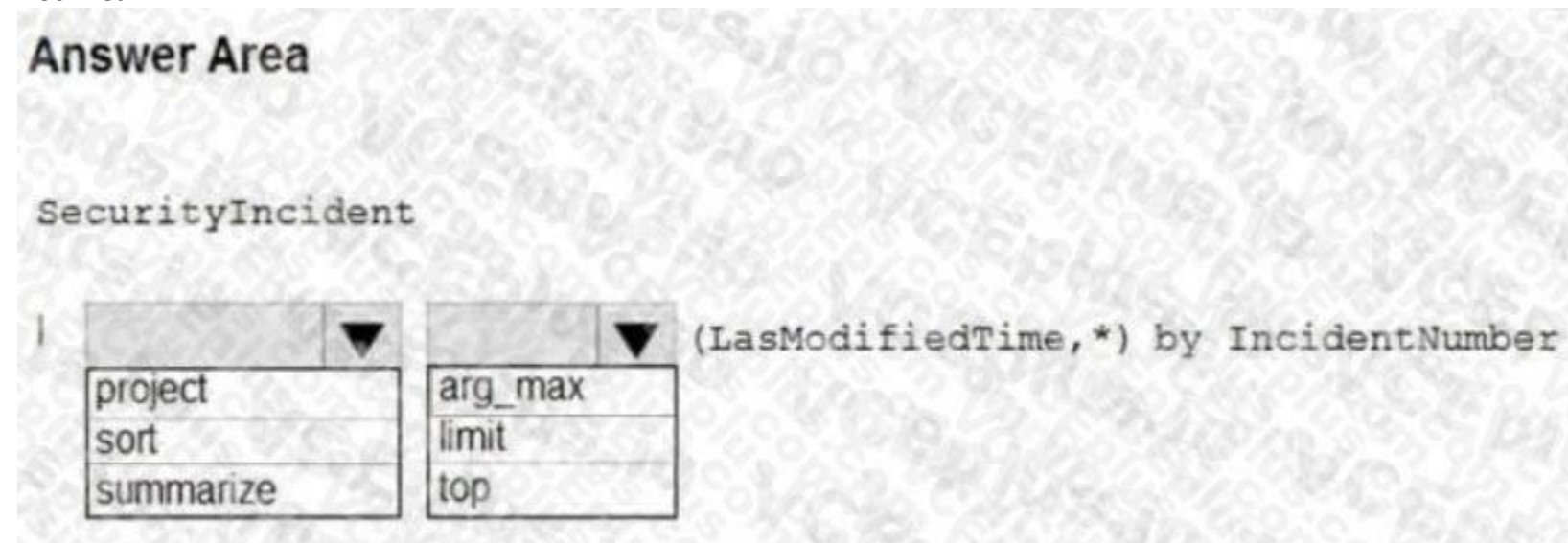
Only include the most recent log for each incident.

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

NOTE: Each correct selection is worth one point.

 Vdumps

Hot Area:



Answer Area

SecurityIncident

| [project] (LasModifiedTime, *) by IncidentNumber

project	arg_max
sort	limit
summarize	top

Answer Area:

Answer Area

SecurityIncident

| (LasModifiedTime, *) by IncidentNumber

project	arg_max
sort	limit
summarize	top

Section:

Explanation:

Reference:

<https://www.drware.com/whats-new-soc-operational-metrics-now-available-in-sentinel/>

QUESTION 7

DRAG DROP

You have the resources shown in the following table.

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

You need to prevent duplicate events from occurring in SW1.

What should you use for each action? To answer, drag the appropriate resources to the correct actions. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Resources	Answer Area
SW1	From the Syslog configuration, remove the facilities that send CEF messages.
CEF1	
Server1	From the Log Analytics agent, disable Syslog synchronization.
Server2	

Correct Answer:

Resources	Answer Area
SW1	From the Syslog configuration, remove the facilities that send CEF messages.
	From the Log Analytics agent, disable Syslog synchronization.
Server2	

Section:

Explanation:

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

QUESTION 8

DRAG DROP

You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.

You plan to deploy Azure Defender.

You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

User	Task
User1	<ul style="list-style-type: none"> • Assign initiatives • Edit security policies • Enable automatic provisioning
User2	<ul style="list-style-type: none"> • View alerts and recommendations • Apply security recommendations • Dismiss alerts

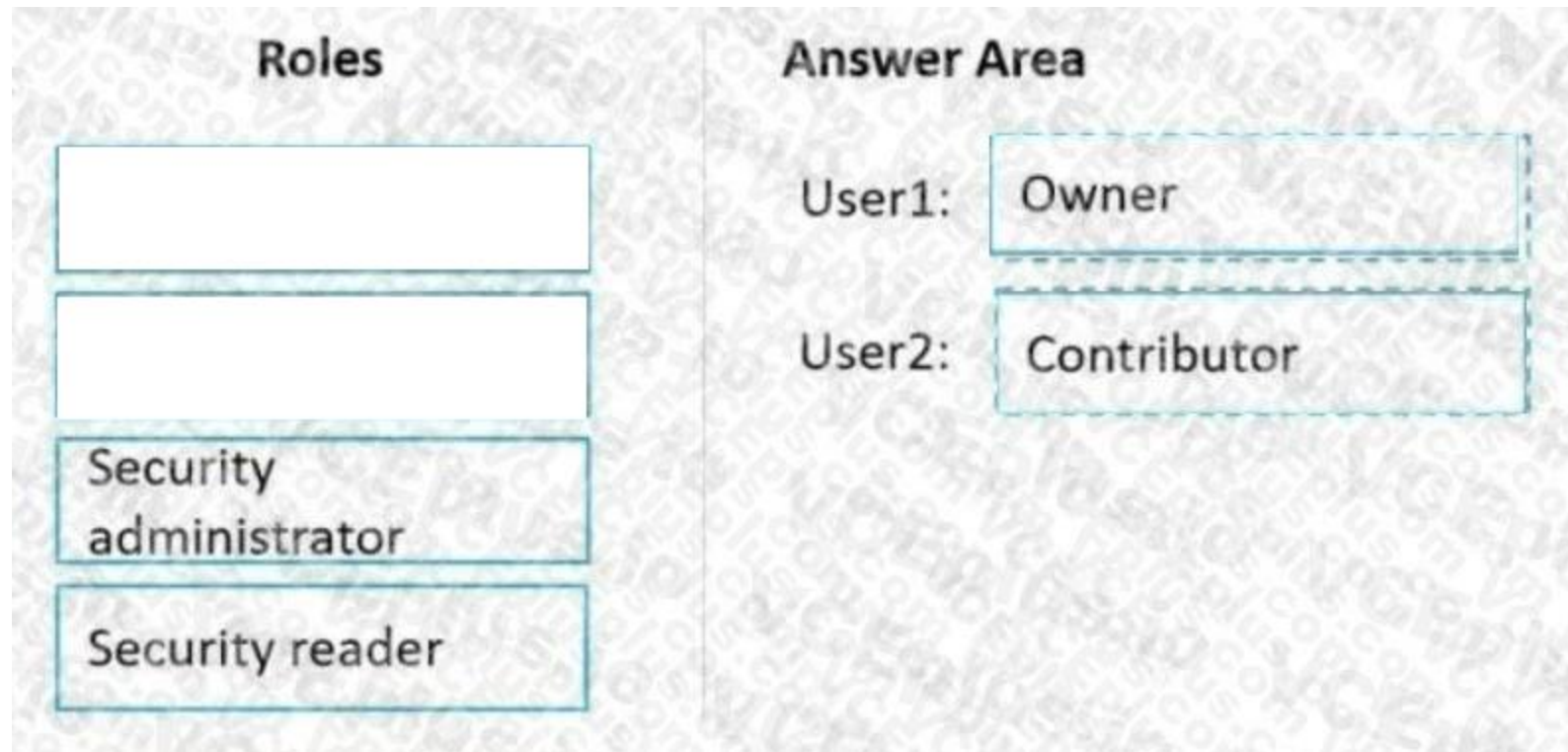
The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. 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.

Select and Place:

The interface shows a list of roles on the left and an answer area on the right. The roles are Contributor, Owner, Security administrator, and Security reader. The answer area has two rows: User1: and User2:.

Correct Answer:



Section:

Explanation:

Box 1: Owner

Only the Owner can assign initiatives.

Box 2: Contributor

Only the Contributor or the Owner can apply security recommendations.

Reference:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions>



QUESTION 9

HOTSPOT

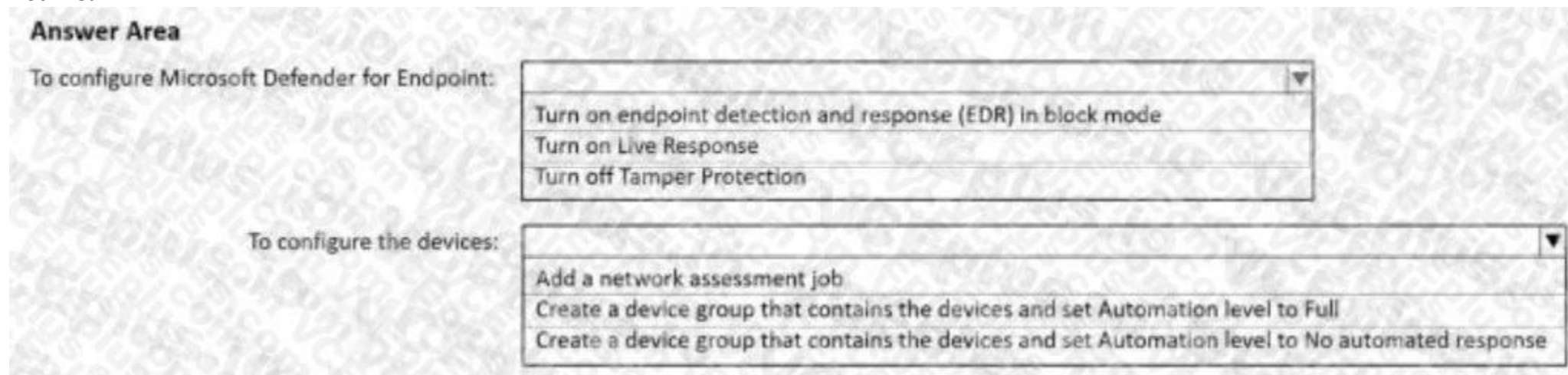
You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.

You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.

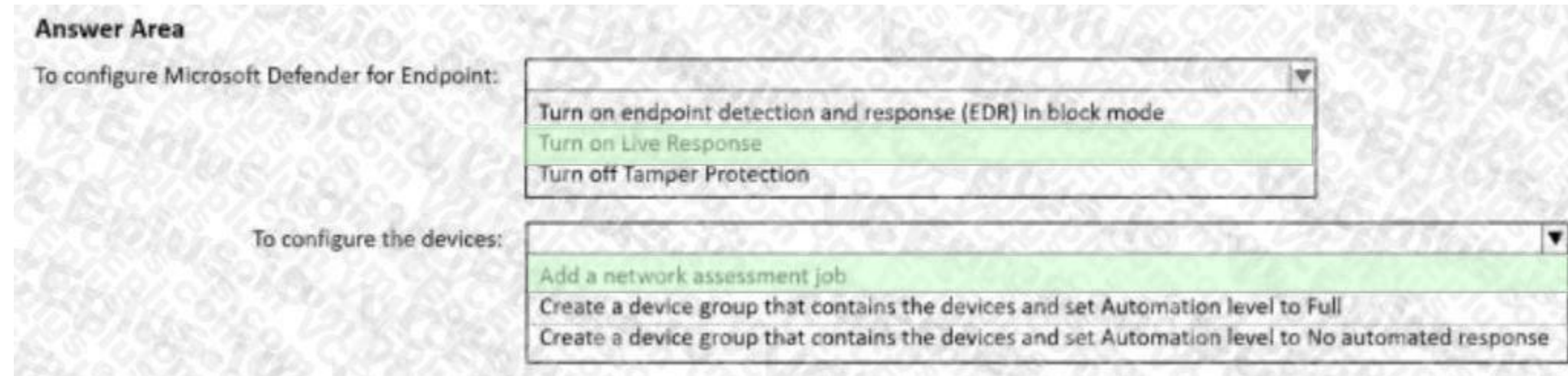
What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

Box 1: Turn on Live Response

Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.

Box: 2

Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide> <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-devices?view=o365worldwide>

QUESTION 10

You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online.

You delete users from the subscription.

You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted.

What should you use?

- A. a file policy in Microsoft Defender for Cloud Apps
- B. an access review policy
- C. an alert policy in Microsoft Defender for Office 365
- D. an insider risk policy

Correct Answer: C

Section:

Explanation:

Alert policies let you categorize the alerts that are triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and decide whether to receive email notifications when alerts are triggered.

Default alert policies include:

Unusual external user file activity - Generates an alert when an unusually large number of activities are performed on files in SharePoint or OneDrive by users outside of your organization. This includes activities such as accessing files, downloading files, and deleting files. This policy has a High severity setting.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies>

QUESTION 11

You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.

You need to identify all the changes made to sensitivity labels during the past seven days.

What should you use?

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

Correct Answer: C

Section:

Explanation:

Labeling activities are available in Activity explorer.

For example:

Sensitivity label applied

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

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

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

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

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

QUESTION 12

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

Correct Answer: C

Section:

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>

QUESTION 13

You have five on-premises Linux servers.

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to use Defender for Cloud to protect the Linux servers.

What should you install on the servers first?

- A. the Dependency agent
- B. the Log Analytics agent
- C. the Azure Connected Machine agent
- D. the Guest Configuration extension

Correct Answer: B

Section:



Explanation:

Defender for Cloud depends on the Log Analytics agent.

Use the Log Analytics agent if you need to:

* Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure * Etc.

Reference:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage>

<https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#log-analytics-agent>

QUESTION 14

You have an Azure subscription that uses Microsoft Sentinel.

You need to minimize the administrative effort required to respond to the incidents and remediate the security threats detected by Microsoft Sentinel.

Which two features should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Microsoft Sentinel bookmarks
- B. Azure Automation runbooks
- C. Microsoft Sentinel automation rules
- D. Microsoft Sentinel playbooks
- E. Azure Functions apps

Correct Answer: C, E

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threatsplaybook?tabs=LAC>

**QUESTION 15**

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

Correct Answer: C

Section:

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/>

QUESTION 16

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 AccountCustomEntity entity associated with the incident.
- D. From Investigation, review insights on the incident entity.

Correct Answer: A

Section:

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.

QUESTION 17

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.

Correct Answer: D

Section:

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>

QUESTION 18

DRAG DROP

You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2. You plan to deploy Azure Defender. You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

User	Task
User1	<ul style="list-style-type: none">• Assign initiatives• Edit security policies• Enable automatic provisioning
User2	<ul style="list-style-type: none">• View alerts and recommendations• Apply security recommendations• Dismiss alerts

The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. 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.

Select and Place:

The screenshot shows an interactive role assignment interface. On the left, under the heading "Roles", there are four role boxes: Contributor, Owner, Security administrator, and Security reader. On the right, under the heading "Answer Area", there are two user labels: User1 and User2. Dashed blue boxes indicate that the Security administrator role is being assigned to User1 and the Security reader role is being assigned to User2. A large watermark "Vdumps" is overlaid on the interface.

Correct Answer:

Roles	Answer Area
	User1: <input type="text" value="Owner"/>
	User2: <input type="text" value="Contributor"/>
<input type="text" value="Security administrator"/>	
<input type="text" value="Security reader"/>	

Section:

Explanation:

Box 1: Owner

Only the Owner can assign initiatives.

Box 2: Contributor

Only the Contributor or the Owner can apply security recommendations.

Reference:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions>



QUESTION 19

HOTSPOT

You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.

You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.

What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

To configure Microsoft Defender for Endpoint:

<input type="checkbox"/>	Turn on endpoint detection and response (EDR) in block mode
<input type="checkbox"/>	Turn on Live Response
<input type="checkbox"/>	Turn off Tamper Protection

To configure the devices:

<input type="checkbox"/>	Add a network assessment job
<input type="checkbox"/>	Create a device group that contains the devices and set Automation level to Full
<input type="checkbox"/>	Create a device group that contains the devices and set Automation level to No automated response

Answer Area:

To configure Microsoft Defender for Endpoint:

Turn on endpoint detection and response (EDR) in block mode
Turn on Live Response
Turn off Tamper Protection

To configure the devices:

Add a network assessment job
Create a device group that contains the devices and set Automation level to Full
Create a device group that contains the devices and set Automation level to No automated response

Section:

Explanation:

Box 1: Turn on Live Response Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.

Box: 2 : Add a network assessment job

Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.

Reference:

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

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

QUESTION 20

HOTSPOT

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.

Hot Area:



```
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      |


```

Answer Area:

```
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      |


```

Section:

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
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-huntingquery-emails-devices?view=o365-worldwide
```

QUESTION 21

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

Correct Answer: A, D

Section:



QUESTION 22

You have a Microsoft Sentinel workspace.

You receive multiple alerts for failed sign in attempts to an account.

You identify that the alerts are false positives.

You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements.

- Ensure that failed sign-in alerts are generated for other accounts.
- Minimize administrative effort

What should do?

- A. Create an automation rule.
- B. Create a watchlist.
- C. Modify the analytics rule.
- D. Add an activity template to the entity behavior.

Correct Answer: A

Section:

Explanation:

An automation rule will allow you to specify which alerts should be suppressed, ensuring that failed sign-in alerts are generated for other accounts while minimizing administrative effort. To create an automation rule, navigate to the

Automation Rules page in the Microsoft Sentinel workspace and configure the rule parameters to suppress the false positive alerts.

QUESTION 23

DRAG DROP

A company wants to analyze by using Microsoft 365 Apps.

You need to describe the connected experiences the company can use.

Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the split between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Connected experiences

Editor Tag Similarity checker

Family links

Answer Area

Description

Provides advanced grammar and style refinements such as clarity, conciseness, formality, and vocabulary suggestions.

Allows you to use and repurpose existing content from relevant files most often used by coworkers.

Identifies how much content in a document is original and inserts citations when necessary.

Connected experience

Correct Answer:

Connected experiences

Editor Tag Similarity checker

Family links

Answer Area

Description

Provides advanced grammar and style refinements such as clarity, conciseness, formality, and vocabulary suggestions.

Allows you to use and repurpose existing content from relevant files most often used by coworkers.

Identifies how much content in a document is original and inserts citations when necessary.

Connected experience

Editor Tag Similarity checker

Section:

Explanation:

QUESTION 24

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.

Correct Answer: B

Section:

QUESTION 25

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

Correct Answer: A

Section:

QUESTION 26

You have a Microsoft Sentinel workspace named Workspace1.

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

What should you create in Workspace1?

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

Correct Answer: A

Section:

QUESTION 27

You have an Azure subscription that uses Microsoft Defender for Endpoint.

You need to ensure that you can allow or block a user-specified range of IP addresses and URLs.

What should you enable first in the advanced features from the Endpoints Settings in the Microsoft 365 Defender portal?

- A. endpoint detection and response (EDR) in block mode
- B. custom network indicators
- C. web content filtering
- D. Live response for servers

Correct Answer: A

Section:

QUESTION 28

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 Azure Storage Analytics logs



- B. the activity logs of storage1
- C. the alert details
- D. the related entities of the alert

Correct Answer: B

Section:

QUESTION 29

You have an Azure subscription that has Microsoft Defender for Cloud enabled.
 You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed.
 You need to simulate an attack on the virtual machine that will generate an alert.
 What should you do first?

- A. Run the Log Analytics Troubleshooting Tool.
- B. Copy a executable and rename the file as ASC_AlerTest_662jf10N.exe
- C. Modify the settings of the Microsoft Monitoring Agent.
- D. Run the MMASetup executable and specify the -foo argument

Correct Answer: B

Section:

QUESTION 30

HOTSPOT

You have the following KQL query.

```
let IPList = _GetWatchlist('Bad_IPs');
Event
| where Source == "Microsoft-Windows-Sysmon"
| where EventID == 3
| extend EvData = parse_xml(EventData)
| extend EventDetail = EvData.DataItem.EventData.Data
| extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
| where SourceIP in (IPList) or DestinationIP in (IPList)
| extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
| extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer, '
```



Hot Area:

Statements	Yes	No
The UserName field is set as the account entity.	<input type="checkbox"/>	<input type="checkbox"/>
The watchlist cannot be updated after it is created.	<input type="checkbox"/>	<input type="checkbox"/>
The IPList variable is set as the IP address entity.	<input type="checkbox"/>	<input type="checkbox"/>

Answer Area:

Statements	Yes	No
The Username field is set as the account entity.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
The watchlist cannot be updated after it is created.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
The IPList variable is set as the IP address entity.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Section:

Explanation:

QUESTION 31

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

You need to add threat indicators for all the IP addresses in a range of 171.23.3432-171.2334.63. The solution must minimize administrative effort.

What should you do in the Microsoft 365 Defender portal?

- A. Create an import file that contains the IP address of 171.23.34.32/27. Select Import and import the file.
- B. Select Add indicator and set the IP address to 171.2334.32-171.23.34.63.
- C. Select Add indicator and set the IP address to 171.23.34.32/27
- D. Create an import file that contains the individual IP addresses in the range. Select Import and import the file.

Correct Answer: D

Section:

Explanation:

This will add all the IP addresses in the range of 171.23.34.32/27 as threat indicators. This is the simplest and most efficient way to add all the IP addresses in the range. Reference: [1] <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/threat-intelligence-manage-indicators>

QUESTION 32

You have a Microsoft Sentinel workspace.

You have a query named Query1 as shown in the following exhibit.

```
1 OfficeActivity
2 where TimeGenerated > ago(7h)
3 where Operation contains "delete"
4 project TimeGenerated, UserId, Operation, OfficeWorkload, RecordType, _ResourceId
5 sort by TimeGenerated desc nulls last
6
```

You plan to create a custom parser named Parser 1. You need to use Query1 in Parser1. What should you do first?

- A. Remove line 2.
- B. In line 4, remove the TimeGenerated predicate.
- C. Remove line 5.
- D. In line 3, replace the 'contains operator with the !has operator.

Correct Answer: A

Section:

QUESTION 33

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)

Correct Answer: D

Section:

QUESTION 34

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

You need to review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription. The solution must minimize administrative effort. Which blade should you use in the Microsoft 365 Defender portal?

- A. Advanced hunting
- B. Threat analytics
- C. Incidents & alerts
- D. Learning hub

Correct Answer: B

Section:

Explanation:

To review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription, you should use the Threat Analytics blade in the Microsoft 365 Defender portal. The Threat Analytics blade provides insights into attack techniques, configuration vulnerabilities, and suspicious activities, and it can help you identify risks and prioritize threats in your environment.

Reference: A, <https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-365-defenderthreat-analytics>

QUESTION 35

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.

Correct Answer: B



Section:

QUESTION 36

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

Correct Answer: D

Section:

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>

QUESTION 37

Your company uses Microsoft Sentinel

A new security analyst reports that she cannot assign and resolve incidents in Microsoft Sentinel.

You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

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

Correct Answer: A

Section:

Explanation:

The Microsoft Sentinel Responder role allows users to investigate, triage, and resolve security incidents, which includes the ability to assign incidents to other users. This role is designed to provide the necessary permissions for incident management and response while still adhering to the principle of least privilege. Other roles such as Logic App Contributor and Microsoft Sentinel Contributor would have more permissions than necessary and may not be suitable for the analyst's needs. Microsoft Sentinel Reader role is not sufficient as it doesn't have permission to assign and resolve incidents.

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/role-based-access-control-rbac>

QUESTION 38

You provision Azure Sentinel for a new Azure subscription.

You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query.



```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. a workbook
- B. a hunting query
- C. a notebook
- D. a playbook

Correct Answer: A

Section:

Explanation:

A workbook is a data-driven interactive report in Microsoft Sentinel. You can use workbooks to create custom reports based on data from your Azure subscription. Reference: <https://docs.microsoft.com/en-us/azure/sentinel/workbooks-overview>

QUESTION 39

You create an Azure subscription.

You enable Microsoft Defender for Cloud for the subscription.

You need to use Defender for Cloud to protect on-premises computers.

What should you do on the on-premises computers?

- A. Configure the Hybrid Runbook Worker role.
- B. Install the Connected Machine agent.
- C. Install the Log Analytics agent
- D. Install the Dependency agent.

Correct Answer: C

Section:

Explanation:

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

QUESTION 40

HOTSPOT

You have a Microsoft Sentinel workspace.

You need to create a KQL query that will identify successful sign-ins from multiple countries during the last three hours.

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

NOTE Each correct selection is worth one point

Hot Area:




```
let timeframe = ago(3h);
let threshold = 5;
imAuthentication
imAuthentication
imNetworkSession
imProcessCreate
imWebSession

| where TimeGenerated > timeframe
| where EventType=='Logon' and EventResult=='Success'
| where isnotempty(SrcGeoCountry)
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct),
NumOfCountries = dcount( DstGeoCountry ) by TargetUserId, TargetUserPrincipalName, TargetUserType
SrcGeoCountry
SrcGeoRegion

| where NumOfCountries >= threshold
```

Answer Area:



```
let timeframe = ago(3h);
let threshold = 5;
imAuthentication
imAuthentication
imNetworkSession
imProcessCreate
imWebSession

| where TimeGenerated > timeframe
| where EventType=='Logon' and EventResult=='Success'
| where isnotempty(SrcGeoCountry)
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct),
NumOfCountries = dcount( DstGeoCountry ) by TargetUserId, TargetUserPrincipalName, TargetUserType
SrcGeoCountry
SrcGeoRegion

| where NumOfCountries >= threshold
```

Section:

Explanation:

QUESTION 41

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

Correct Answer: D

Section:

QUESTION 42

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

- A. the risk detections report
- B. the risky users report
- C. Identity Secure Score recommendations
- D. the risky sign-ins report

Correct Answer: B

Section:

QUESTION 43

You have an Azure subscription that uses Microsoft Defender for Cloud. You have an Amazon Web Services (AWS) account that contains an Amazon Elastic Compute Cloud (EC2) instance named EC2-1. You need to onboard EC2-1 to Defender for Cloud. What should you install on EC2-1?

- A. the Log Analytics agent
- B. the Azure Connected Machine agent
- C. the unified Microsoft Defender for Endpoint solution package
- D. Microsoft Monitoring Agent

Correct Answer: A

Section:

QUESTION 44

You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schema. You need to make the 200 parsers available in Workspace1. The solution must minimize administrative effort. What should you do first?

- A. Copy the parsers to the Azure Monitor Logs page.
- B. Create a JSON file based on the DNS template.
- C. Create an XML file based on the DNS template.
- D. Create a YAML file based on the DNS template.



Correct Answer: A

Section:

Explanation:

QUESTION 45

You use Microsoft Sentinel.

You need to receive an alert in near real-time whenever Azure Storage account keys are enumerated.

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

Each correct selection is worth one point

- A. Create a bookmark.
- B. Create an analytics rule.
- C. Create a livestream.
- D. Create a hunting query.
- E. Add a data connector.

Correct Answer: D, E

Section:

QUESTION 46

You need to minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts. What should you review?

- A. the status update time
- B. the alert status
- C. the certainty of the source computer
- D. the resolution method of the source computer



Correct Answer: B

Section:

QUESTION 47

HOTSPOT

You need to meet the Microsoft Defender for Cloud Apps requirements

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Set the sensitivity level of the impossible travel alert policies to:

Low
Low
Medium
High

To reduce the amount of false positive alerts:

Enable leaked credential detection.
Add IP address ranges.
Enable leaked credential detection.
Disable leaked credential detection.

Answer Area:

Answer Area

Set the sensitivity level of the impossible travel alert policies to:

Low
Low
Medium
High

To reduce the amount of false positive alerts:

Enable leaked credential detection.
Add IP address ranges.
Enable leaked credential detection.
Disable leaked credential detection.

Section:

Explanation:

QUESTION 48

You need to deploy the native cloud connector to Account! to meet the Microsoft Defender for Cloud requirements. What should you do in Account! first?

- A. Create an AWS user for Defender for Cloud.
- B. Create an Access control (IAM) role for Defender for Cloud.
- C. Configure AWS Security Hub.
- D. Deploy the AWS Systems Manager (SSM) agent

Correct Answer: D

Section:

QUESTION 49

HOTSPOT

You need to create a query to investigate DNS-related activity. 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.

Hot Area:

Answer Area

Answer Area:

Answer Area



Section:

Explanation:

Answer Area

QUESTION 50

HOTSPOT

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.

Hot Area:

Answer Area

Group1: Security Admin
Contributor
Owner
Security Admin
Security Assessment Contributor

Group2: Contributor
Contributor
Owner
Security Admin
Security Assessment Contributor

Answer Area:

Answer Area

Group1: Security Admin
Contributor
Owner
Security Admin
Security Assessment Contributor

Group2: Contributor
Contributor
Owner
Security Admin
Security Assessment Contributor

Section:

Explanation:

QUESTION 51

You need to ensure that you can run hunting queries to meet the Microsoft Sentinel requirements. Which type of workspace should you create?

- A. Azure Synapse AnarytKS
- B. AzureDalabricks
- C. Azure Machine Learning
- D. LogAnalytics

Correct Answer: D

Section:

QUESTION 52

You need to correlate data from the SecurityEvent Log Anarytks table to meet the Microsoft Sentinel requirements for using UEBA. Which Log Analytics table should you use?

- A. SentWIAuoNt
- B. AADRiskyUsers
- C. IdentityOirectoryEvents
- D. Identityinfo

Correct Answer: C

Section:

QUESTION 53

You need to identify which mean time metrics to use to meet the Microsoft Sentinel requirements. Which workbook should you use?

- A. Analytics Efficiency
- B. Security Operations Efficiency
- C. Event Analyzer
- D. Investigation insights

Correct Answer: C


Section:

QUESTION 54

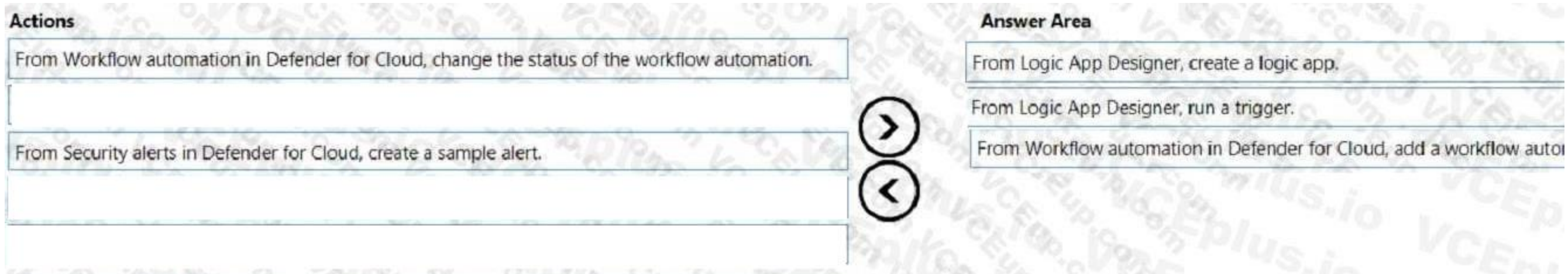
DRAG DROP

You have an Azure subscription. The subscription contains 10 virtual machines that are onboarded to Microsoft Defender for Cloud. You need to ensure that when Defender for Cloud detects digital currency mining behavior on a virtual machine, you receive an email notification. The solution must generate a test email. 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.

Select and Place:

Actions	Answer Area
From Workflow automation in Defender for Cloud, change the status of the workflow automation.	
From Logic App Designer, run a trigger.	
From Security alerts in Defender for Cloud, create a sample alert.	
From Logic App Designer, create a logic app.	
From Workflow automation in Defender for Cloud, add a workflow automation.	

Correct Answer:



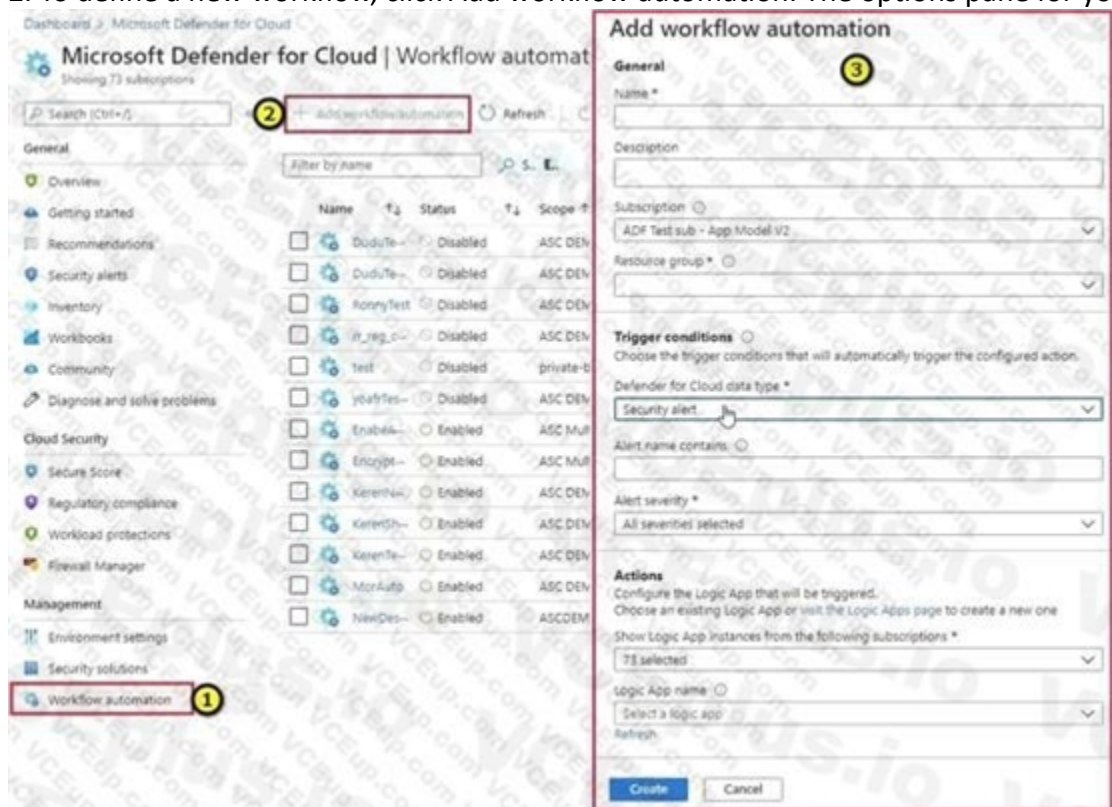
Section:

Explanation:

Step 1: From Logic App Designer, create a logic app.

Create a logic app and define when it should automatically run

1. From Defender for Cloud's sidebar, select Workflow automation.
2. To define a new workflow, click Add workflow automation. The options pane for your new automation opens.



Here you can enter:

A name and description for the automation.

The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.

The Logic App that will run when your trigger conditions are met.

3. From the Actions section, select visit the Logic Apps page to begin the Logic App creation process.

4. Etc.

Step 2: From Logic App Designer, run a trigger.

Manually trigger a Logic App

You can also run Logic Apps manually when viewing any security alert or recommendation.

Step 3: From Workflow automation in Defender for cloud, add a workflow automation.

Configure workflow automation at scale using the supplied policies

Automating your organization's monitoring and incident response processes can greatly improve the time it takes to investigate and mitigate security incidents.





Reference: <https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation>

QUESTION 55

HOTSPOT

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.

Hot Area:



```

| 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()
    bin()
    count()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
  by OperationNameValue, Caller, CallerIpAddress

```



Answer Area:

```

| 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

```



Section:

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
 Reference: https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/AzureActivity/Anomalous_Listing_Of_Storage_Keys.yaml

QUESTION 56

DRAG DROP

You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.

You receive an alert for suspicious use of PowerShell on VM1.

You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:

The modification of local group memberships

The purging of event logs

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

Select and Place:

Actions	Answer Area
From the details pane of the incident, select Investigate .	
From the Investigation blade, select the entity that represents VM1.	
From the Investigation blade, select the entity that represents powershell.exe.	
From the Investigation blade, select Timeline .	
From the Investigation blade, select Info .	
From the Investigation blade, select Insights .	

Correct Answer:

Actions	Answer Area
	From the details pane of the incident, select Investigate .
	From the Investigation blade, select the entity that represents VM1.
From the Investigation blade, select the entity that represents powershell.exe.	
From the Investigation blade, select Timeline .	
From the Investigation blade, select Info .	From the Investigation blade, select Insights .

Section:

Explanation:

Step 1: From the Investigation blade, select Insights

The Investigation Insights Workbook is designed to assist in investigations of Azure Sentinel Incidents or individual IP/Account/Host/URL entities.

Step 2: From the Investigation blade, select the entity that represents VM1.

The Investigation Insights workbook is broken up into 2 main sections, Incident Insights and Entity Insights.

Incident Insights The Incident Insights gives the analyst a view of ongoing Sentinel Incidents and allows for quick access to their associated metadata including alerts and entity information.

Entity Insights The Entity Insights allows the analyst to take entity data either from an incident or through manual entry and explore related information about that entity. This workbook presently provides view of the following entity types:

IP Address
Account
Host
URL

Step 3: From the details pane of the incident, select Investigate.
Choose a single incident and click View full details or Investigate.

Reference:

<https://github.com/Azure/Azure-Sentinel/wiki/Investigation-Insights---Overview>
<https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases>

QUESTION 57

HOTSPOT

You have the following SQL query.

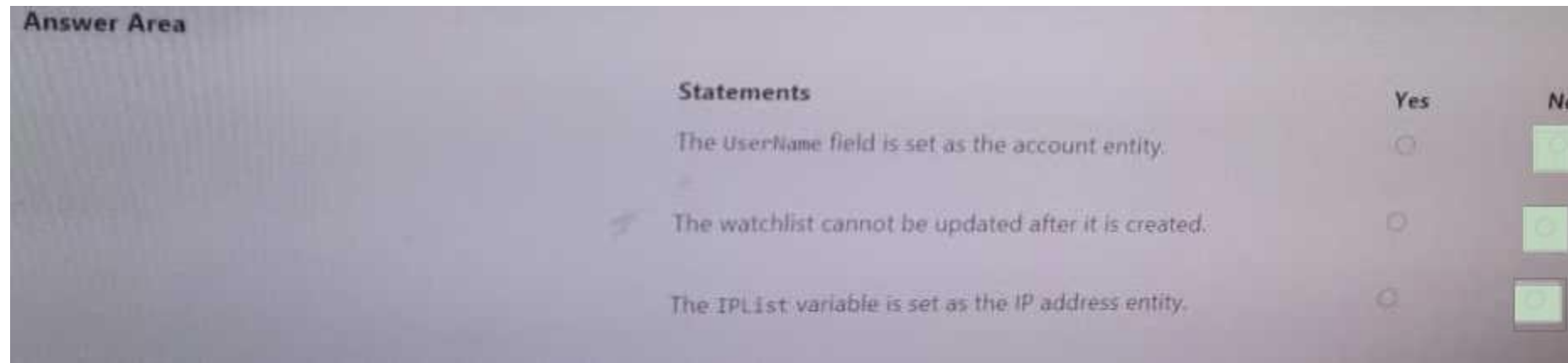
```
let IPList = _GetWatchlist('Bad_IPs');
Event
| where Source == "Microsoft-Windows-Sysmon"
| where EventID == 3
| extend EvData = parse_xml(EventData)
| extend EventDetail = EvData.DataItem.EventData.Data
| extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
| where SourceIP in (IPList) or DestinationIP in (IPList)
| extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
| extend timestamp = TimeGenerated, AccountCustomEntity = Username, HostCustomEntity = Computer
```

Hot Area:

Answer Area

Statements	Yes	No
The UserName field is set as the account entity.	<input type="radio"/>	<input checked="" type="radio"/>
The watchlist cannot be updated after it is created.	<input type="radio"/>	<input checked="" type="radio"/>
The IPList variable is set as the IP address entity.	<input type="radio"/>	<input checked="" type="radio"/>

Answer Area:



Section:

Explanation:

QUESTION 58

You have a Microsoft 365 E5 subscription that is linked to a hybrid Azure AD tenant. You need to identify all the changes made to Domain Admins group during the past 30 days. What should you use?

- A. the Azure Active Directory Provisioning Analysis workbook
- B. the Overview settings of Insider risk management
- C. the Modifications of sensitive groups report in Microsoft Defender for Identity
- D. the identity security posture assessment in Microsoft Defender for Cloud Apps

Correct Answer: C

Section:



QUESTION 59

You need to meet the Microsoft Sentinel requirements for App1. What should you configure for App1?

- A. an API connection
- B. a trigger
- C. an connector
- D. authorization

Correct Answer: B

Section:

QUESTION 60

HOTSPOT

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.

Hot Area:

Answer Area

Deploy the: Log Analytics agent
 Azure Monitor agent
 Windows Azure VM Agent
 Log Analytics agent

Query by using: KQL
 KQL
 WQL
 XPath

Answer Area:

Answer Area

Deploy the: Log Analytics agent
 Azure Monitor agent
 Windows Azure VM Agent
 Log Analytics agent

Query by using: KQL
 WQL
 XPath

Section:

Explanation:

QUESTION 61

HOTSPOT

You have 100 Azure subscriptions that have enhanced security features in Microsoft Defender for Cloud enabled. All the subscriptions are linked to a single Azure AD tenant. You need to stream the Defender for Cloud logs to a syslog server. The solution must minimize administrative effort. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Export logs to an:

- Log Analytics workspace
- Azure event hub
- Azure Storage account
- Log Analytics workspace

Configure streaming by:

- Configuring continuous export in Defender for Cloud for each subscription
- Configuring continuous export in Defender for Cloud for each subscription
- Creating an Azure Policy assignment at the root management group
- Modifying the diagnostic settings of the tenant

Answer Area:

Answer Area

Export logs to an:

- Log Analytics workspace
- Azure event hub
- Azure Storage account
- Log Analytics workspace

Configure streaming by:

- Configuring continuous export in Defender for Cloud for each subscription
- Configuring continuous export in Defender for Cloud for each subscription
- Creating an Azure Policy assignment at the root management group
- Modifying the diagnostic settings of the tenant

Section:

Explanation:

QUESTION 62

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. You have the hunting query shown in the following exhibit.

The users perform the following actions:

```
1 AuditLogs
2 where TimeGenerated >ago(7d)
3 where OperationName == "Add user"
4 project AddedTime = TimeGenerated, user = tostring(TargetResources[0].userPrincipalName)
5 join (AzureActivity
6 where OperationName == "Create role assignment"
7 project OperationName, RoleAssignmentTime = TimeGenerated, user = Caller) on user
8 project-away user1
9
```

- User1 assigns User2 the Global administrator role.

- User1 creates a new user named User3 and assigns the user a Microsoft Teams license.
- User2 creates a new user named User4 and assigns the user the Security reader role.
- User2 creates a new user named User5 and assigns the user the Security operator role.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	<input type="radio"/>	<input type="radio"/>
The query will identify the creation of User3.	<input type="radio"/>	<input type="radio"/>
The query will identify the creation of User5.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	<input checked="" type="radio"/>	<input type="radio"/>
The query will identify the creation of User3.	<input checked="" type="radio"/>	<input type="radio"/>
The query will identify the creation of User5.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

QUESTION 63

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

Correct Answer: C

Section:

Explanation:

QUESTION 64

HOTSPOT

You need to implement Microsoft Sentinel queries for Contoso and Fabrikam to meet the technical 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.

Hot Area:

Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

Query element required to correlate data between tenants:

Answer Area:

Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

Query element required to correlate data between tenants:

Section:

Explanation:

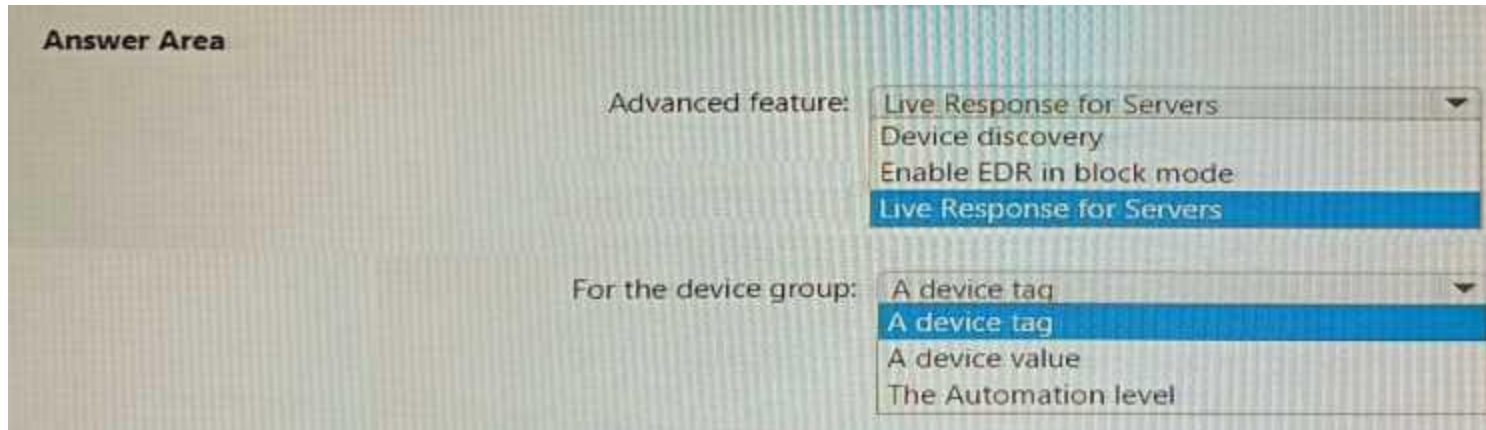
QUESTION 65

HOTSPOT

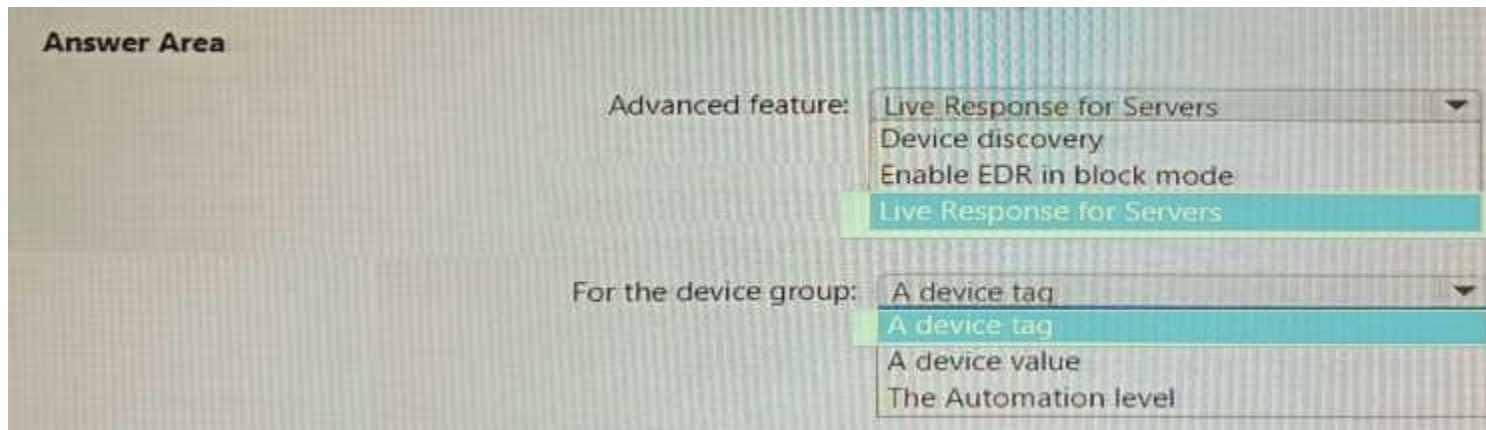
You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender for Endpoint. You need to ensure that you can initiate remote shell connections to Windows servers by using the Microsoft 365 Defender portal. What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

Vdumps

QUESTION 66

HOTSPOT

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.

Hot Area:

Answer Area

Configure the connector to use: ▼
A managed identity
A service principal
An Azure AD user account

Role to assign to the credentials: ▼
Microsoft Sentinel Automation Contributor
Microsoft Sentinel Reader
Microsoft Sentinel Responder

Answer Area:
Answer Area

Configure the connector to use: ▼
A managed identity
A service principal
An Azure AD user account

Role to assign to the credentials: ▼
Microsoft Sentinel Automation Contributor
Microsoft Sentinel Reader
Microsoft Sentinel Responder

Section:
Explanation:

QUESTION 67

HOTSPOT

You have a Microsoft Sentinel workspace named sws1.

You need to create a query that will detect when a user creates an unusually large numbers of Azure AD user accounts.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
AzureActivity
AuditLogs
AzureActivity
BehaviorAnalytics
SecurityEvent

| where ActionType == "Add user"

| where ActivityInsights has "True"

| join(

BehaviorAnalytics
AuditLogs
AzureActivity
BehaviorAnalytics
SecurityEvent

= $right._ItemId

| select _id, TimeGenerated, UserPrincipalName, UsersInsights.AccountDisplayName),

| sort by TimeGenerated desc

| project TimeGenerated, UserName, UserPrincipalName, UsersInsights,
ActivityType, ActionType
```

Answer Area:



Answer Area

The screenshot shows a query editor interface. At the top, a dropdown menu is open with 'AzureActivity' selected. Below it, a list of activity types is shown: 'AuditLogs', 'AzureActivity', 'BehaviorAnalytics', and 'SecurityEvent'. The 'AzureActivity' option is highlighted in green. To the right of this dropdown, the text 'user"' is visible. Below the first dropdown, the query snippet includes the following lines: '| where ActionType == "Add user"', '| where ActivityInsights has "True"', and '| join('.

Below the first dropdown, there is a second dropdown menu with 'BehaviorAnalytics' selected. Below it, a list of activity types is shown: 'AuditLogs', 'AzureActivity', 'BehaviorAnalytics', and 'SecurityEvent'. The 'BehaviorAnalytics' option is highlighted in green. To the right of this dropdown, the text '= \$right._ItemId' is visible. Below the second dropdown, the query snippet includes the following lines: '| where AccountDisplayName == \$right.AccountDisplayName)', '| sort by TimeGenerated desc', '| project TimeGenerated, UserName, UserPrincipalName, UsersInsights,', and 'ActivityType, ActionType.'



Section:

Explanation:

QUESTION 68

HOTSPOT

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.

Hot Area:

Answer Area

Azure role:
Microsoft Sentinel Automation Contributor
Microsoft Sentinel Contributor
Microsoft Sentinel Responder

Azure AD role:
Attribute assignment reader
Directory readers
Global reader

Answer Area:

Answer Area

Azure role:
Microsoft Sentinel Automation Contributor
Microsoft Sentinel Contributor
Microsoft Sentinel Responder

Azure AD role:
Attribute assignment reader
Directory readers
Global reader

Section:

Explanation:

QUESTION 69

HOTSPOT

You have a custom detection rule that includes the following KQL query.

```
AlertInfo
| where Severity == "High"
| distinct AlertId
| join AlertEvidence on AlertId
| where EntityType in ("User", "Mailbox")
| where EvidenceRole == "Impacted"
| summarize by Timestamp, AlertId, AccountName, AccountObjectId, EntityType, DeviceId, SHA256
| join EmailEvents on $left.AccountObjectId == $right.RecipientObjectId
| where DeliveryAction == "Delivered"
| summarize by Timestamp, AlertId, ReportId, RecipientObjectId, RecipientEmailAddress, EntityType, DeviceId, SHA256
```

For each of the following statements, select Yes if True. Otherwise select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the RecipientEmailAddress column.	<input type="radio"/>	<input type="radio"/>
The custom detection rule can be used to restrict app execution automatically based on the DeviceId column.	<input type="radio"/>	<input type="radio"/>
The custom detection rule can be used to automate the deletion of a file based on the SHA256 column.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the RecipientEmailAddress column.	<input type="radio"/>	<input checked="" type="checkbox"/>
The custom detection rule can be used to restrict app execution automatically based on the DeviceId column.	<input type="radio"/>	<input checked="" type="checkbox"/>
The custom detection rule can be used to automate the deletion of a file based on the SHA256 column.	<input type="radio"/>	<input checked="" type="checkbox"/>

Section:

Explanation:

QUESTION 70

HOTSPOT

You have a Microsoft Sentinel workspace.

You need to configure a report visual for a custom workbook. The solution must meet the following requirements:

* The count and usage trend of AppDisplayName must be included

* The TrendList column must be useable in a sparkline visual,

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.

Hot Area:

Answer Area

SigninLogs

```
| where ResultType == 0 and AppDisplayName != ""
```

```
| summarize count() by AppDisplayName
```

```
| join (
```

```
let  
| lookup  
mv-expand  
) on AppDisplayName
```

```
TrendList = count() on TimeGenerated in range({TimeRange:start}, {TimeRange:end}, 4h) by AppDisplayName
```

```
| top 10 by count_desc
```

SigninLogs

```
make-series  
make_bag()  
make-series  
mv-expand  
render
```

```
TrendList = count() on TimeGenerated in range({TimeRange:start}, {TimeRange:end}, 4h) by AppDisplayName
```

```
) on AppDisplayName
```

```
| top 10 by count_desc
```



Answer Area:

Answer Area

SigninLogs

| where ResultType == 0 and AppDisplayName != ""

| summarize count() by AppDisplayName

| join (

SigninLogs

| let

| lookup

| mv-expand

) on AppDisplayName

| top 10 by count_desc

SigninLogs

| make-series

| make_bag()

| mv-expand

| render

) on AppDisplayName

| top 10 by count_desc

TrendList = count() on TimeGenerated in range({TimeRange:start}, {TimeRange:end}, 4h) by AppDisplayName

TrendList = count() on TimeGenerated in range({TimeRange:start}, {TimeRange:end}, 4h) by AppDisplayName



Section:

Explanation:

QUESTION 71

HOTSPOT

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.

Hot Area:

Answer Area

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

Answer Area:

Answer Area

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



Section:

Explanation:

QUESTION 72

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

Correct Answer: B

Section:

QUESTION 73

You have a Microsoft 365 subscription that uses Microsoft Purview.

Your company has a project named Project1.

You need to identify all the email messages that have the word Project1 in the subject line. The solution must search only the mailboxes of users that worked on Project1.

What should you do?

- A. Create a records management disposition.
- B. Perform a user data search.
- C. Perform an audit search.
- D. Perform a content search.

Correct Answer: D

Section:

QUESTION 74

DRAG DROP

You have an Azure subscription that contains the users shown in the following table.

Name	Role
User1	Security administrator
User2	Security reader
User3	Contributor



You need to delegate the following tasks:

* Enable Microsoft Defender for Servers on virtual machines.

* Review security recommendations and enable server vulnerability scans.

The solution must use the principle of least privilege.

Which user should perform each task? To answer, drag the appropriate users to the correct tasks. Each user 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.

Users

User1

User2

User3

Answer Area

Enable Microsoft Defender for Servers on virtual machines:

Review security recommendations and enable server vulnerability scans:

Answer:

Users

User1
User2
User3

Answer Area

Enable Microsoft Defender for Servers on virtual machines: User1

Review security recommendations and enable server vulnerability scans: User2

Select and Place:

Users

User1
User2
User3

Answer Area

Enable Microsoft Defender for Servers on virtual machines:

Review security recommendations and enable server vulnerability scans:

Correct Answer:

Users

User3

Answer Area

Enable Microsoft Defender for Servers on virtual machines: User1

Review security recommendations and enable server vulnerability scans: User2

Section:

Explanation:

QUESTION 75

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

Correct Answer: D

Section:

QUESTION 76

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

Correct Answer: A

Section:

QUESTION 77

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

You need to create a query that will link the AlertInfo, AlertEvidence, and DeviceLogonEvents tables. The solution must return all the rows in the tables.

Which operator should you use?

- A. join kind = inner
- B. evaluate hint. Remote =
- C. search *
- D. union kind = inner

Correct Answer: A

Section:

QUESTION 78

DRAG DROP

You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online.

You need to identify phishing email messages.

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

Select and Place:

Cmdlets	Answer Area
Connect-IPPSSession	
Start-ComplianceSearch	
New-ComplianceSearch	
Connect-ExchangeOnline	
Search-UnifiedAuditLog	

Navigation icons: Right arrow, Left arrow, Up arrow, Down arrow.

Correct Answer:



Cmdlets

Connect-IPPSSession
Start-ComplianceSearch

Answer Area

New-ComplianceSearch
Connect-ExchangeOnline
Search-UnifiedAuditLog

**Section:****Explanation:**

New-ComplianceSearch
 Connect-ExchangeOnline
 Search-UnifiedAuditLog

QUESTION 79

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 for 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

Correct Answer: B

Section:**QUESTION 80****HOTSPOT**

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

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD. You need to identify the 100 most recent sign-in attempts recorded on devices and AD DS domain controllers. 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.

Hot Area:

Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| (
  union
  join kind=full outer
  join kind=inner
  union
  IdentityLogonEvents
  IdentityInfo
  IdentityLogonEvents
  IdentityQueryEvents
  | extend Table = 'table2'
  | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

Answer Area:



Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| (
  union
  join kind=full outer
  join kind=inner
  union
  IdentityLogonEvents
  IdentityInfo
  IdentityLogonEvents
  IdentityQueryEvents
)
| extend Table = 'table2'
| take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

Section:

Explanation:

QUESTION 81

HOTSPOT

You have a Microsoft Sentinel workspace.

A Microsoft Sentinel incident is generated as shown in the following exhibit.

Home > Microsoft Sentinel >

Incident

Incident ID: 203443

Refresh

Authentication Methods Changed for Privileged Acc...
Incident ID: 203443

Unassigned Owner | New Status | High Severity

Description
Identifies authentication methods being changed for a privileged account. This could be an indicated of an attacker adding an auth method to the account so they can have continued access. Ref : <https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1>

Alert product names
• Microsoft Sentinel

Evidence
1 Events | 1 Alerts | 0 Bookmarks

Last update time: 05/11/22, 12:50 PM | Creation time: 05/11/22, 12:49 PM

Entities (2)
gbarnes@contoso... | 192.168.65.82
[View full details >](#)

Tactics and techniques
Persistence (1)

Investigate | Actions

Timeline | Similar incidents (Preview) | Alerts

Search

Timeline content : All | Severity : All | Tactics : All

May 11 11:13 AM | **Authentication Methods Changed for Privileged Account**
High | Detected by Microsoft Sentinel | Tactics: Persistence

Authentication Methods Changed for Privileged Accou...

Description
Identifies authentication methods being changed for a privileged account. This could be an indicated of an attacker adding an auth method to the account so they can have continued access. Ref : <https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1>

Severity: High | Status: New

Events: [Link to LA](#) | Product name: Microsoft Sentinel

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.

Hot Area:

Answer Area

A map of the entities connected to the alert can be viewed by selecting [answer choice].

Investigate	▼
Alerts	
Entities	
Investigate	

A list of the activities performed during the investigation can be viewed by selecting [answer choice].

Comments	▼
Alerts	
Bookmarks	
Comments	
Status	

Answer Area:

Answer Area

A map of the entities connected to the alert can be viewed by selecting [answer choice].

Investigate	▼
Alerts	
Entities	
Investigate	

A list of the activities performed during the investigation can be viewed by selecting [answer choice].

Comments	▼
Alerts	
Bookmarks	
Comments	
Status	

Section:

Explanation:

QUESTION 82

HOTSPOT

You have an Azure subscription that uses Microsoft Defender for Cloud.

You create a Google Cloud Platform (GCP) organization named GCP1.

You need to onboard GCP1 to Defender for Cloud by using the native cloud connector. The solution must ensure that all future GCP projects are onboarded automatically.

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.

Hot Area:

Answer Area

Create:

By:

Answer Area:

Answer Area

Create:

By:



Section:

Explanation:

QUESTION 83

HOTSPOT

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.

Hot Area:

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

Answer Area:

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

Section:

Explanation:

QUESTION 84

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

Correct Answer: D

Section:

QUESTION 85

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

Correct Answer: C
Section:

QUESTION 86

HOTSPOT

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

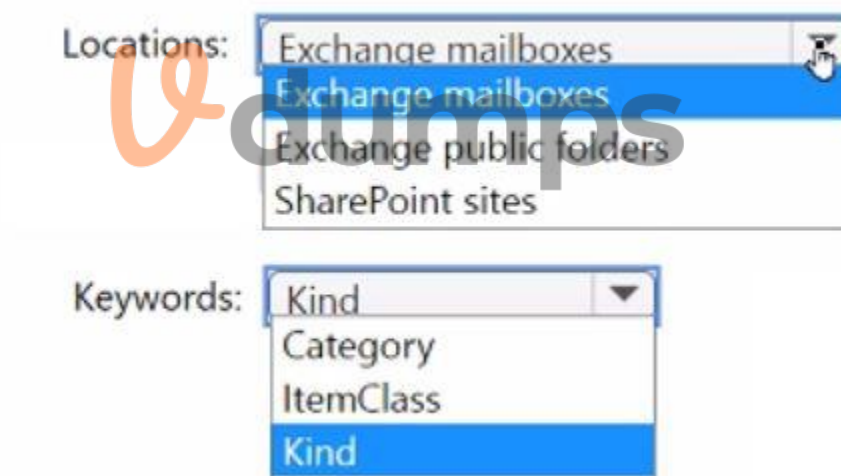
You need to perform a content search of Teams chats for a user by using the Microsoft Purview compliance portal. The solution must minimize the scope of the search.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Answer Area:

Answer Area

Locations:
Exchange mailboxes
Exchange public folders
SharePoint sites

Keywords:
Kind
Category
ItemClass
Kind

Section:

Explanation:

QUESTION 87

HOTSPOT

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.

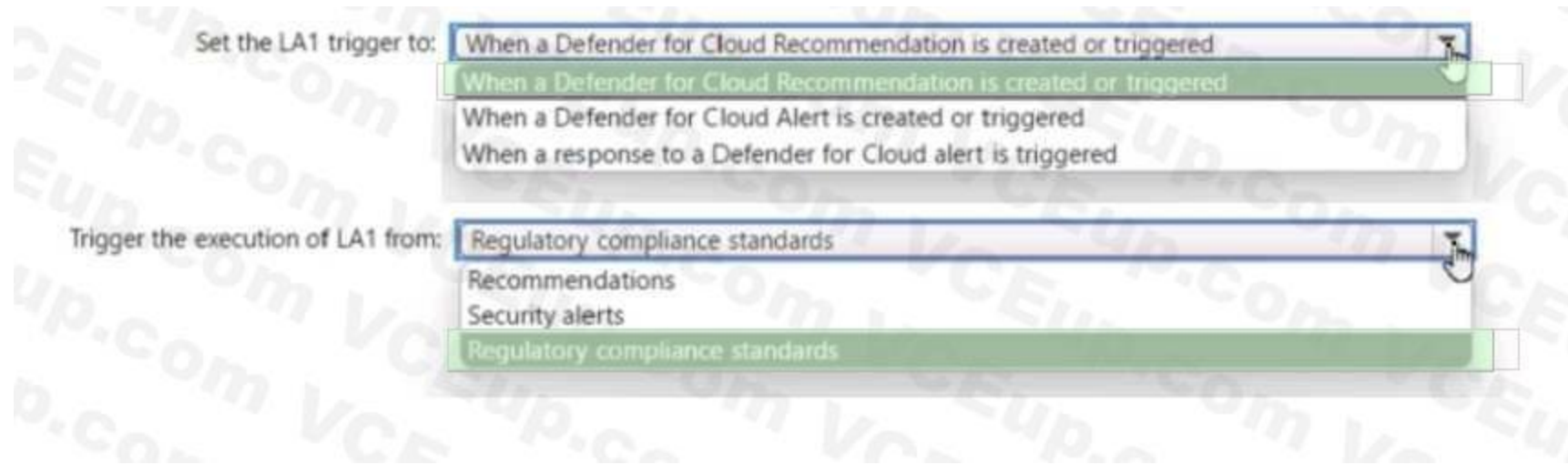
Vdumps

Hot Area:

Set the LA1 trigger to:
When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Alert is created or triggered
When a response to a Defender for Cloud alert is triggered

Trigger the execution of LA1 from:
Regulatory compliance standards
Recommendations
Security alerts
Regulatory compliance standards

Answer Area:



Section:

Explanation:

QUESTION 88

DRAG DROP

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.

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

NOTE Each correct selection is worth one point

Select and Place:

Values

Answer Area



- | project LogonFailures=count()
- | summarize LogonFailures=count()
by DeviceName, LogonType
- | where ActionType == FailureReason
- | where DeviceName in ("CFOLaptop",
"CEOLaptop", "COOLaptop")
- ActionType == "LogonFailed"
- ActionType == FailureReason
- DeviceEvents
- DeviceLogonEvents

-
-
-
-
-
-

and

Correct Answer:

Values	Answer Area
project LogonFailures=count()	
where ActionType == FailureReason	DeviceLogonEvents
	where DeviceName in ("CFOLaptop", and "CEOLaptop", "COOLaptop")
ActionType == "LogonFailed"	ActionType == FailureReason
	summarize LogonFailures=count() by DeviceName, LogonType
DeviceEvents	

Section:

Explanation:



QUESTION 89

HOTSPOT

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.

Hot Area:

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.

Answer Area:



Section:

Explanation:

QUESTION 90

HOTSPOT

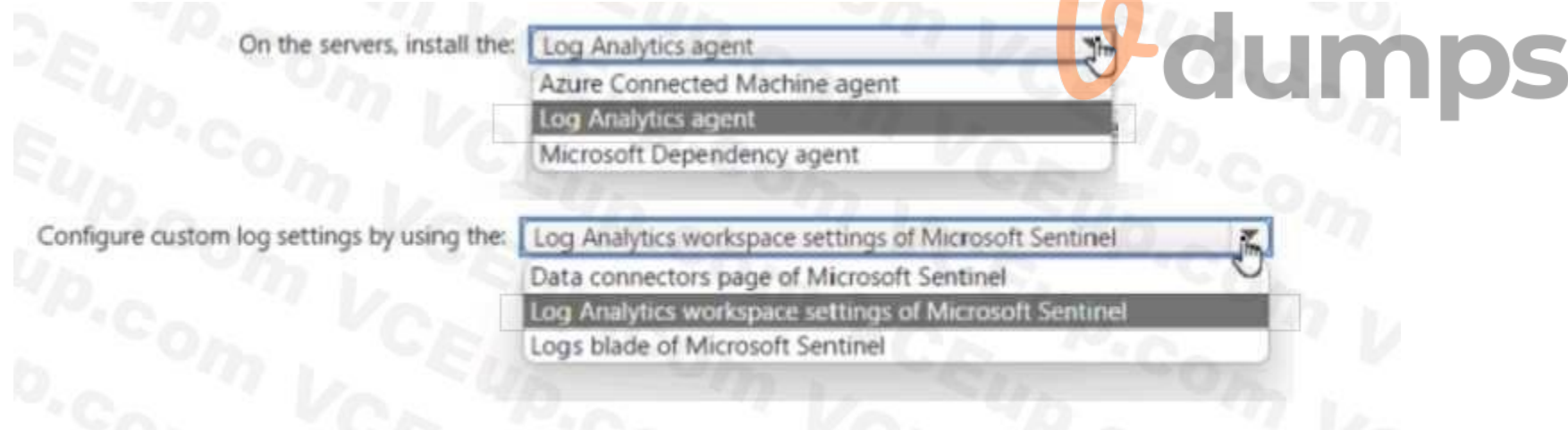
Your on-premises network contains 100 servers that run Windows Server.

You have an Azure subscription that uses Microsoft Sentinel.

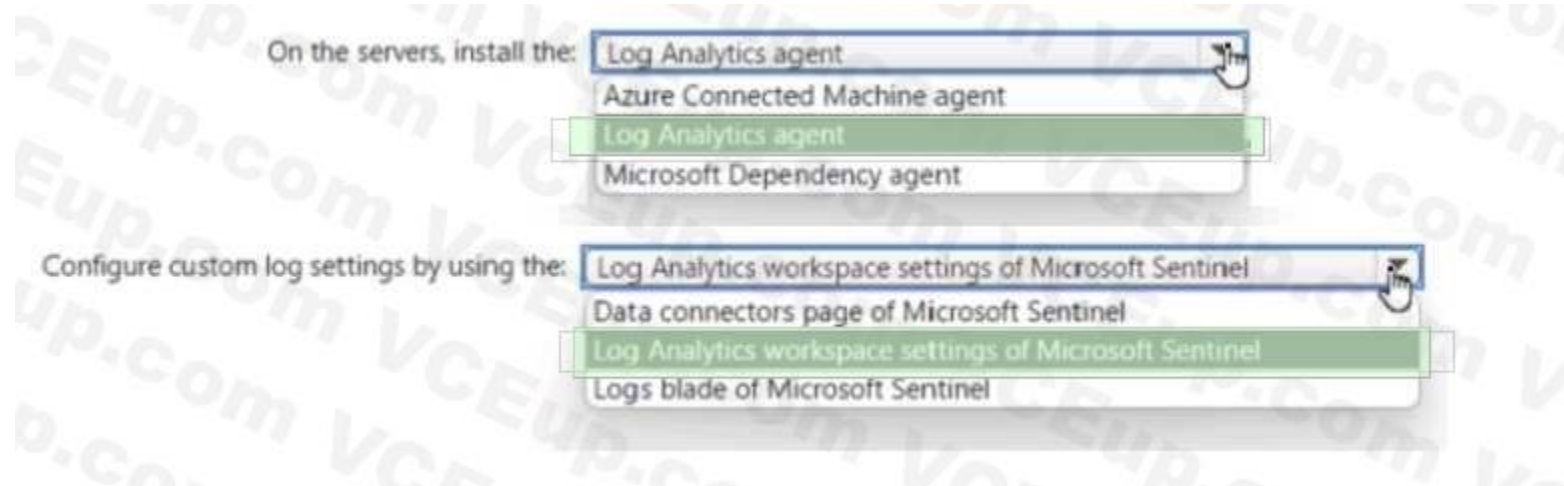
You need to upload custom logs from the on-premises servers to Microsoft Sentinel.

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

Hot Area:



Answer Area:



Section:

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.

QUESTION 91

HOTSPOT

You have a Microsoft Sentinel workspace

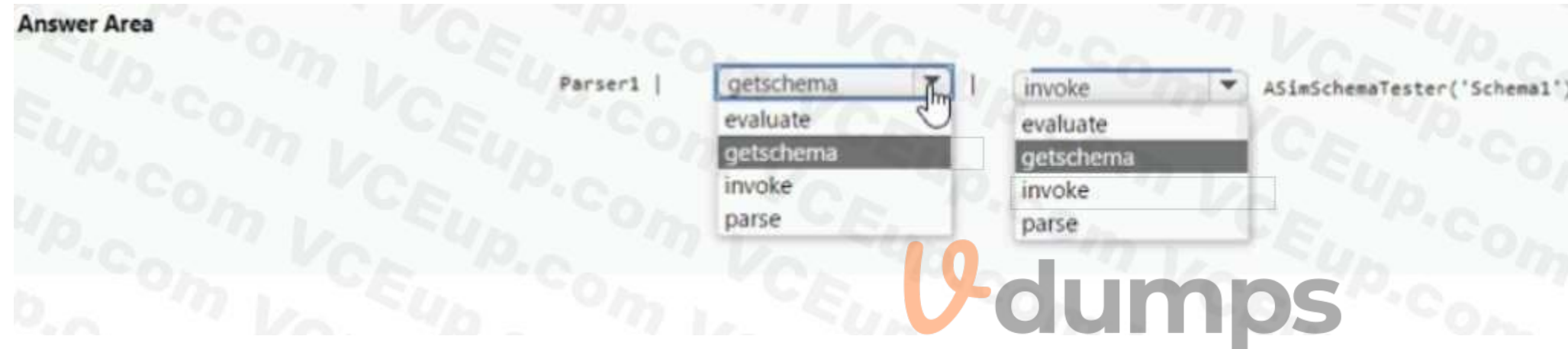
You develop a custom Advanced Security information Model (ASIM) parser named Parser1 that produces a schema named Schema1.

You need to validate Schema1.

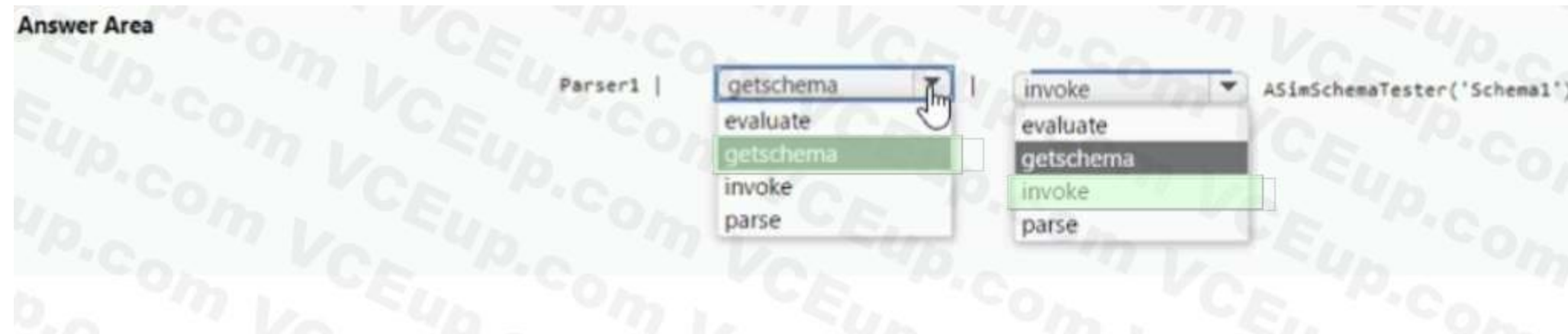
How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:



QUESTION 92

HOTSPOT

You have a Microsoft Sentinel workspace that has User and Entity Behavior Analytics (UEBA) enabled.

You need to identify all the log entries that relate to security-sensitive user actions performed on a server named Server1. The solution must meet the following requirements:

- Only include security-sensitive actions by users that are NOT members of the IT department.
- Minimize the number of false positives.

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

Hot Area:

Answer Area

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
| join kind=inner (
| join kind=fullouter (
| join kind=inner (
| join kind=innerunique (
IdentityInfo
BehaviorAnalytics
IdentityInfo
| wh SecurityEvent
```

These are the selections for the first missing value.

dumps

Answer Area:

Answer Area

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
| join kind=inner (
| join kind=fullouter (
| join kind=inner (
| join kind=innerunique (
IdentityInfo
BehaviorAnalytics
IdentityInfo
| wh SecurityEvent
```

These are the selections for the first missing value.

Section:

Explanation:

Answer Area

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
| join kind=inner (
  IdentityInfo
  | summarize arg_max(TimeGenerated, *) by AccountObjectId) on $left.SubjectUserSid == $right.AccountSID
| where Department != "IT"
```

QUESTION 93

You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server. You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. From the workspace created by Defender for Cloud, set the data collection level to Common
- B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment.
- C. From the Azure portal, create an Azure Event Grid subscription.
- D. From the workspace created by Defender for Cloud, set the data collection level to All Events
- E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines.

Correct Answer: D, E
Section:

QUESTION 94

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

Correct Answer: B
Section:

QUESTION 95

DRAG DROP

You have an Azure subscription that contains 100 Linux virtual machines. You need to configure Microsoft Sentinel to collect event logs from the virtual machines. 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.

Select and Place:

Actions

- Add a Syslog connector to the workspace.
- Add an Microsoft Sentinel workbook.
- Add Microsoft Sentinel to a workspace.
- Install the Log Analytics agent for Linux on the virtual machines.
- Add a Security Events connector to the workspace.

Answer Area

Correct Answer:

Actions

- Add a Syslog connector to the workspace.
- Add Microsoft Sentinel to a workspace.

Answer Area

- Add an Microsoft Sentinel workbook.
- Install the Log Analytics agent for Linux on the virtual machines.
- Add a Security Events connector to the workspace.

Section:

Explanation:

QUESTION 96

HOTSPOT

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.

Hot Area:

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)
```

Answer Area:

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)
```



Section:

Explanation:

QUESTION 97

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Purview and contains a user named User1.

User1 shares a Microsoft Power BI report file from the Microsoft OneDrive folder of your company to an external user by using Microsoft Teams.

You need to identify which Power BI report file was shared.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Activities: Shared Power BI report
Copied file
Downloaded files to computer
Share file, folder, or site
Shared Power BI report

Record type: Shared Power BI report
MicrosoftTeams
OneDrive
PowerBiAudit
Shared Power BI report

Workload: MicrosoftTeams
MicrosoftTeams
OneDrive
PowerBI
SharePoint

Answer Area:
Answer Area



Activities: Shared Power BI report
Copied file
Downloaded files to computer
Share file, folder, or site
Shared Power BI report

Record type: Shared Power BI report
MicrosoftTeams
OneDrive
PowerBiAudit
Shared Power BI report

Workload: MicrosoftTeams
MicrosoftTeams
OneDrive
PowerBI
SharePoint

Section:
Explanation:

QUESTION 98

DRAG DROP

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.

Select and Place:

Actions

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



Answer Area



Correct Answer:

Actions

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

Rename the executable file as AlertTest.exe.

Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.

Answer Area

Run the executable file and specify the appropriate arguments.

Change the alert severity threshold for emails to **Medium**.

Change the alert severity threshold for emails to **Low**.



Section:

Explanation:

QUESTION 99

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) subscription. The subscription contains multiple virtual machines that run Windows Server.

You need to enable Microsoft Defender for Servers on the virtual machines.

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

NOTE: Each correct answer is worth one point.

- A. From Defender for Cloud, enable agentless scanning.
- B. Install the Azure Virtual Machine Agent (VM Agent) on each virtual machine.
- C. Onboard the virtual machines to Microsoft Defender for Endpoint.
- D. From Defender for Cloud, configure auto-provisioning.
- E. From Defender for Cloud, configure the AWS connector.

Correct Answer: B, C

Section:

QUESTION 100

You have a Microsoft 365 E5 subscription that contains 100 Linux devices. The devices are onboarded to Microsoft Defender 365. You need to initiate the collection of investigation packages from the devices by using the Microsoft 365 Defender portal. Which response action should you use?

- A. Run antivirus scan
- B. Initiate Automated Investigation
- C. Collect investigation package
- D. Initiate Live Response Session



Correct Answer: D

Section:

QUESTION 101

You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector. From Microsoft Sentinel, you investigate a Microsoft 365 incident. You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps. What should you use?

- A. the entity side panel of the Timeline card in Microsoft Sentinel
- B. the investigation graph on the Incidents page of Microsoft Sentinel
- C. the Timeline tab on the Incidents page of Microsoft Sentinel
- D. the Alerts page in the Microsoft 365 Defender portal

Correct Answer: A

Section:

QUESTION 102

OTSPOT

You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace. You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions. Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Connector type:

- API-based
- Diagnostic settings**
- Log Analytics agent-based

Use:

- A remediation task**
- A workbook
- An analytics rule

Answer Area:

Answer Area

Connector type:

- Diagnostic settings
- API-based
- Diagnostic settings
- Log Analytics agent-based

Use:

- A remediation task
- A remediation task
- A workbook
- An analytics rule

Section:

Explanation:

QUESTION 103

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

Correct Answer: B

Section:

QUESTION 104

HOTSPOT

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.

Hot Area:



Answer Area

Azure AD role:

- Global administrator
- Identity Governance Administrator
- Security administrator**
- Security operator

Azure role:

- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Contributor**
- Security Admin
- Security Assessment Contributor

Answer Area:

Answer Area

Azure AD role:

- Global administrator
- Identity Governance Administrator
- Security administrator**
- Security operator

Azure role:

- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Contributor**
- Security Admin
- Security Assessment Contributor

Section:

Explanation:

QUESTION 105

HOTSPOT

You have a Microsoft Sentinel workspace that contains a custom workbook.

You need to query the number of daily security alerts. The solution must meet the following requirements:

- * Identify alerts that occurred during the last 30 days.
- * Display the results in a timechart.

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

Hot Area:

Answer Area

```
SecurityAlert
| where TimeGenerated >= ago(30d)
|  count() by ProviderName, 
| 
| 
| 
| render timechart
```

Answer Area:

Answer Area

```
SecurityAlert
| where TimeGenerated >= ago(30d)
| 
| 
| 
| render timechart
```

Section:

Explanation:

QUESTION 106

You have an Azure subscription that uses Microsoft Sentinel and contains 100 Linux virtual machines.

You need to monitor the virtual machines by using Microsoft Sentinel. The solution must meet the following requirements:

- * Minimize administrative effort
- * Minimize the parsing required to read log data

What should you configure?

- A. REST API integration
- B. a SysLog connector
- C. a Log Analytics Data Collector API
- D. a Common Event Format (CEF) connector

Correct Answer: B

Section:

QUESTION 107

HOTSPOT

You have an Microsoft Sentinel workspace named SW1.

You plan to create a custom workbook that will include a time chart.

You need to create a query that will identify the number of security alerts per day for each provider.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

SecurityAlert

| where TimeGenerated >= ago(30d)

| summarize count() by ProviderName,

| timechart

- render
- materialize
- project
- render

(TimeGenerated, 1d)

- bin
- series_add
- series_fill_linear
- take

Answer Area:

Answer Area

SecurityAlert

| where TimeGenerated >= ago(30d)

| summarize count() by ProviderName,

| timechart

- render
- materialize
- project
- render

(TimeGenerated, 1d)

- bin
- series_add
- series_fill_linear
- take

Section:

Explanation:

QUESTION 108

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

You are investigating an attacker that is known to use the Microsoft Graph API as an attack vector. The attacker performs the tactics shown the following table.

Name	Tactic
Tactic1	Conditional Access policy reconnaissance
Tactic2	Mailbox reconnaissance
Tactic3	Invites guest users to the tenant

You need to search for malicious activities in your organization.
Which tactics can you analyze by using the MicrosoftGraphActivityLogs table?

- A. Tactic? only
- B. Tactic1 and Tactic2 only
- C. Tac1ic2 and Tactic3 only
- D. Taclic1. Tac1ic2. andTactic3

Correct Answer: B

Section:

QUESTION 109

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains 500 Windows devices. As part of an incident investigation, you identify the following suspected malware files:

- * sys
- * pdf
- * docx
- * xlsx

You need to create indicator hashes to block users from downloading the files to the devices. Which files can you block by using the indicator hashes?

- A. File1.sysonly
- B. File1.sysand File3.docxonly
- C. File1.sys. File3.docx, and File4jclsx only
- D. File2.pdf. File3.docxr and File4.xlsx only
- E. File1.sys, File2.pdf, File3.dooc, and File4.xlsx

Correct Answer: A

Section:

QUESTION 110

DRAG DROP

You have a Microsoft Sentinel workspace named SW1.

In SW1. you enable User and Entity Behavior Analytics (UEBA).

You need to use KQL to perform the following tasks:

- * View the entity data that has fields for each type of entity.
- * Assess the quality of rules by analyzing how well a rule performs.

Which table should you use in KQL for each task? To answer, drag the appropriate tables to the correct tasks. Each table 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.

Select and Place:



Tables

- Anomalies
- AuditLogs
- AzureDiagnostics
- BehaviorAnalytics
- CommonSecurityLog

Answer Area

View entity data:

Assess rule quality:

Correct Answer:

Tables

-
- AuditLogs
- AzureDiagnostics
-
- CommonSecurityLog

Answer Area

View entity data:

Assess rule quality:

Section:

Explanation:

QUESTION 111

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint and contains a user named user1 and a Microsoft 365 group named Group1. All users are assigned a Defender for Endpoint Plan 1 license. You enable Microsoft Defender XDR Unified role-based access control (RBAC) for Endpoints & Vulnerability Management.

You need to ensure that User1 can configure alerts that will send email notifications to Group1. The solution must follow the principle of least privilege.

Which permissions should you assign to User1?

- A. Alerts investigation
- B. Manage security settings
- C. Defender Vulnerability Management - Remediation handling
- D. Live response capabilities: Basic

Correct Answer: A

Section:

QUESTION 112

You have a Microsoft Sentinel workspace named SW1.

You need to identify which anomaly rules are enabled in SW1.

What should you review in Microsoft Sentine1?

- A. Settings
- B. Entity behavior
- C. Analytics



D. Content hub

Correct Answer: C

Section:

