Vendor: Microsoft

Exam Code:SC-200

Exam Name: Microsoft Security Operations Analyst

Version: Demo

QUESTION 1

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.

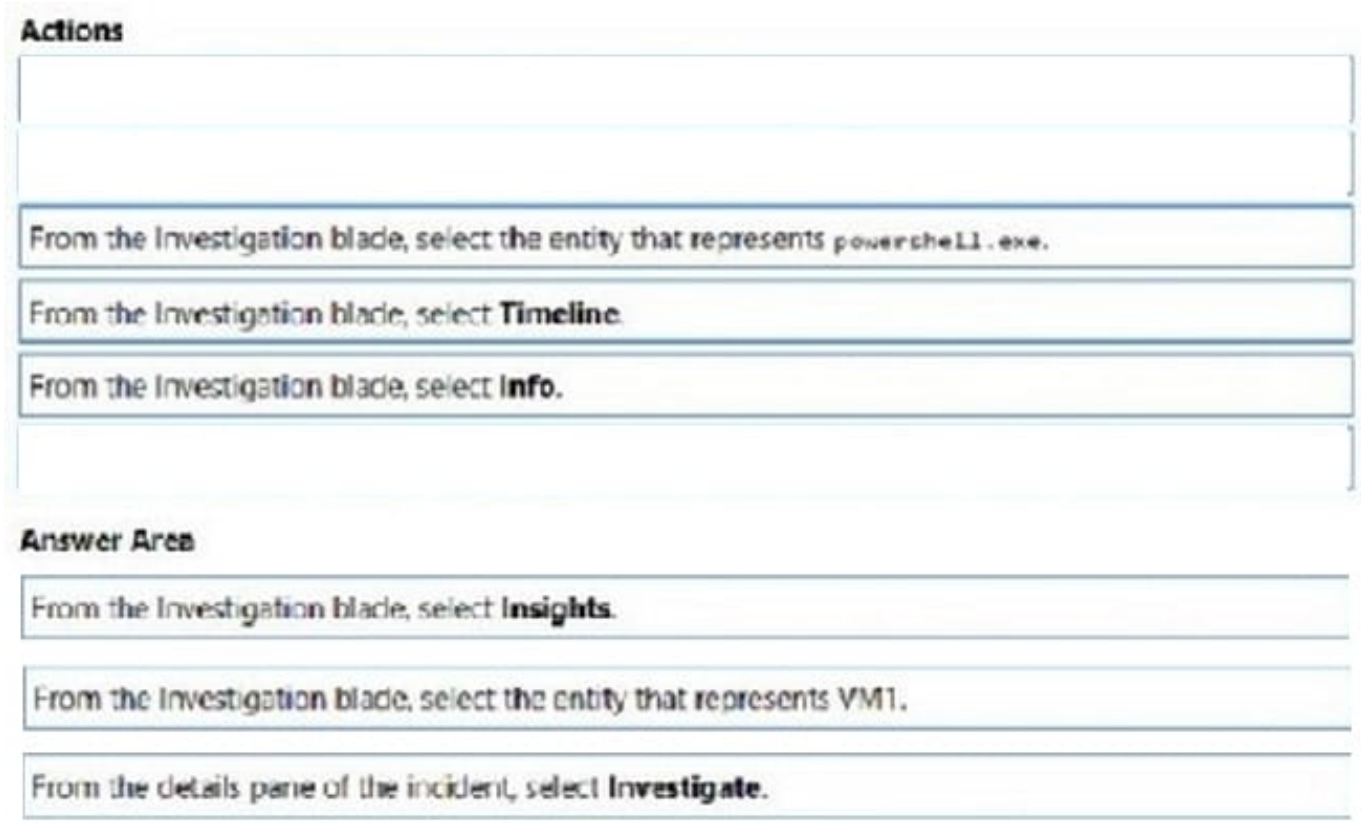
Select and Place:

Actions

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**.

Answer Area

Correct Answer:



QUESTION 2

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

A. executive

B. sales

C. marketing

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios

QUESTION 3

HOTSPOT

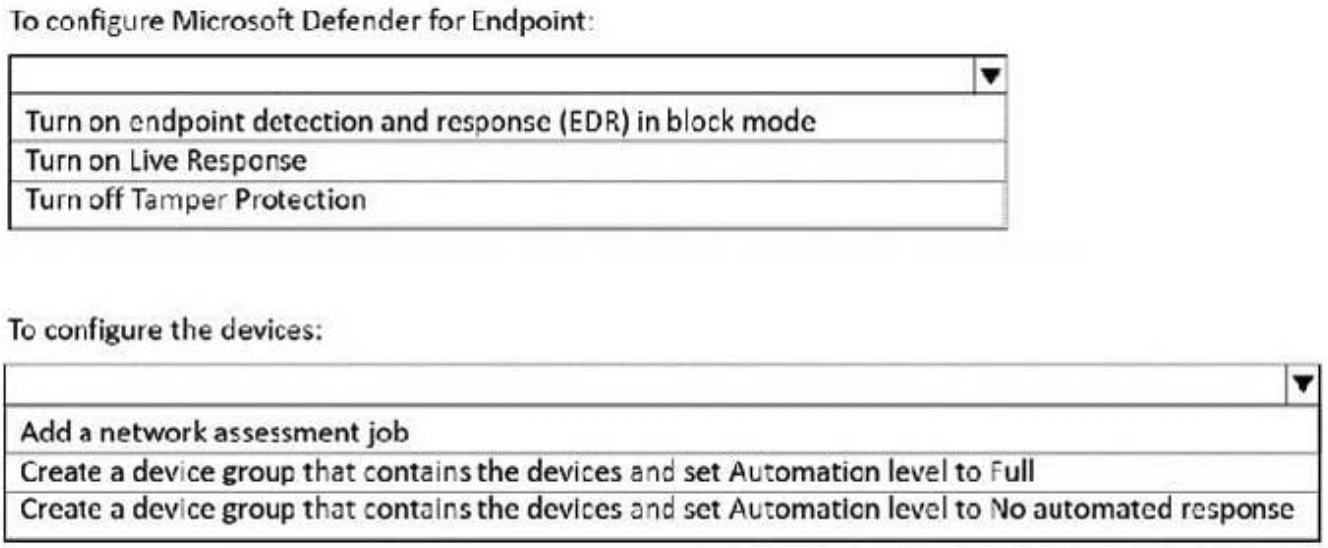
You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.

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:



Correct Answer:

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

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.

QUESTION 4

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

You have Linux virtual machines on Amazon Web Services (AWS).

You deploy Azure Defender and enable auto-provisioning.

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

Solution: You manually install the Log Analytics agent on the virtual machines.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

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

---

QUESTION 5

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

You create a Log Analytics workspace named LogsWest in the West US Azure region.

You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.

What should you do first?

A. Deploy Azure Data Catalog to the West US Azure region.

B. Modify the workspace settings of the existing Azure Sentinel deployment.

C. Add Azure Sentinel to a workspace.

D. Create a data connector in Azure Sentinel.

Correct Answer: C

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

---

QUESTION 6

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

A. IdentityInfo

B. AADRiskyUsers

C. SentinelAudit

D. IdentityDirectoryEvents

Correct Answer: A

UEBA also synchronizes the user information from Azure Active Directory and on-premises Active Directory (currently in preview when using Microsoft Defender for Identity) into the IdentityInfo table, for you to use later on.

Note:

Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).

Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.

Reference:

https://cloudbrothers.info/en/microsoft-sentinel-ueba/

QUESTION 7

You plan to review Microsoft Defender for Cloud alerts by using a third-party security information and event management (SIEM) solution.

You need to locate alerts that indicate the use of the Privilege Escalation MITRE ATTandCK tactic.

Which JSON key should you search?

A. Description

B. Intent

C. ExtendedProperies

D. Entities

Correct Answer: A

Example, misp-galaxy/clusters/mitre-enterprise-attack-attack-pattern.json

{ "authors": [

"MITRE"

],

"category": "attack-pattern",

"description": "ATTandCK tactic",

"name": "Enterprise Attack - Attack Pattern",

"source": "https://github.com/mitre/cti",

"type": "mitre-enterprise-attack-attack-pattern",

"uuid": "fb2242d8-1707-11e8-ab20-6fa7448c3640"

Reference: https://github.com/MISP/misp-galaxy/blob/main/clusters/mitre-enterprise-attack-attack-pattern.json

---

QUESTION 8

You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.

You need to ensure that the Fusion rule can generate alerts.

What should you do?

A. Disable, and then enable the rule.

B. Add data connectors

C. Create a new machine learning analytics rule.

D. Add a hunting bookmark.

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

---

QUESTION 9

You have a Microsoft Sentinel workspace that contains the following incident.

Brute force attack against Azure Portal analytics rule has been triggered.

You need to identify the geolocation information that corresponds to the incident.

What should you do?

A. From Overview, review the Potential malicious events map.

B. From Incidents, review the details of the iPCustomEntity entity associated with the incident.

C. From Incidents, review the details of the AccouncCuscomEntity entity associated with the incident.

D. From Investigation, review insights on the incident entity.

Correct Answer: A

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 10

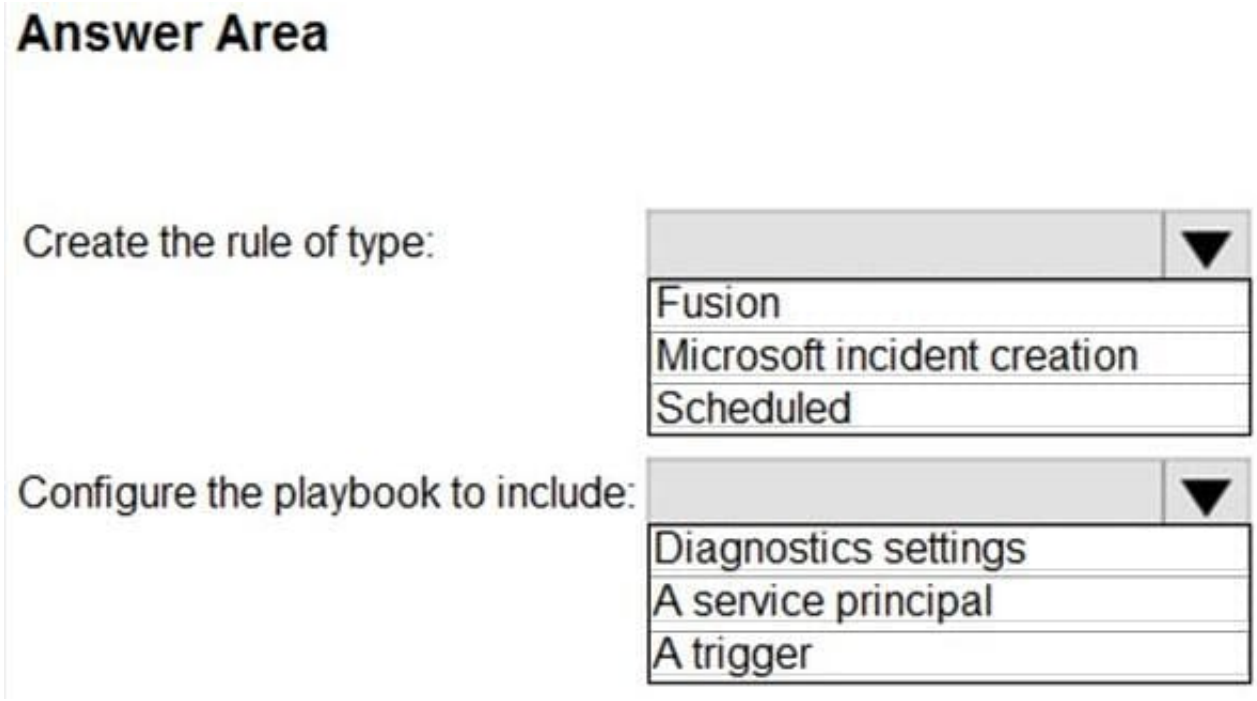
HOTSPOT

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

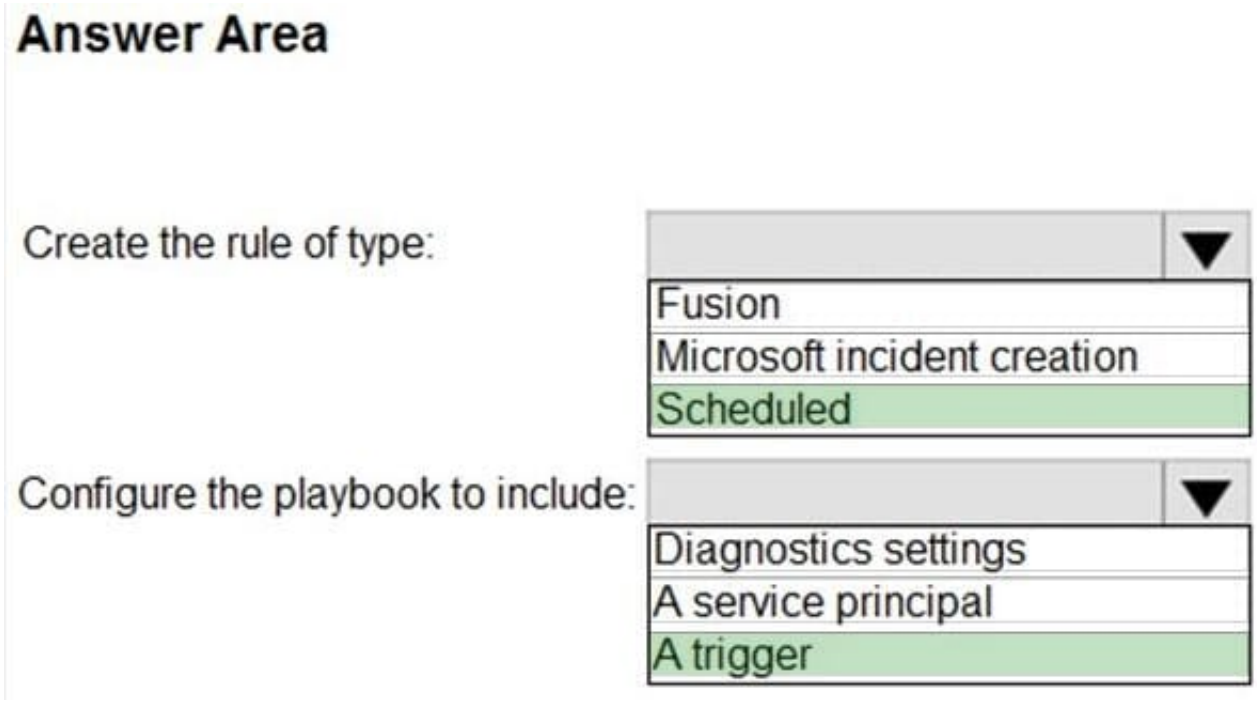
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



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 11

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 and settings

D. Security alerts

E. Azure Defender

Correct Answer: C

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

---

QUESTION 12

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: C

https://learn.microsoft.com/en-us/azure/sentinel/customize-alert-details