SC-200 Q&As

Microsoft Security Operations Analyst

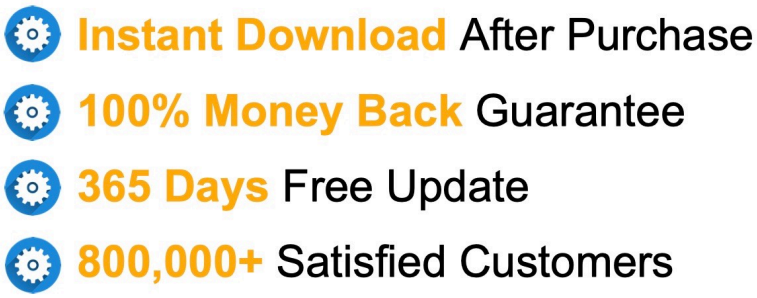
Pass Microsoft SC-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/sc-200.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center



QUESTION 1

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 2

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

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

QUESTION 3

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

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

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

A. Create an Azure Sentinel workspace that has a Security Events connector.

B. Configure the Diagnostics settings in Azure AD to stream to an event hub.

C. Create an Azure Sentinel workspace that has an Azure Active Directory connector.

D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

Correct Answer: B

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

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 are configuring Microsoft Defender for Identity integration with Active Directory.

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

Solution: You add each account as a Sensitive account.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

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

QUESTION 5

HOTSPOT

You have a Microsoft 365 E5 subscription.

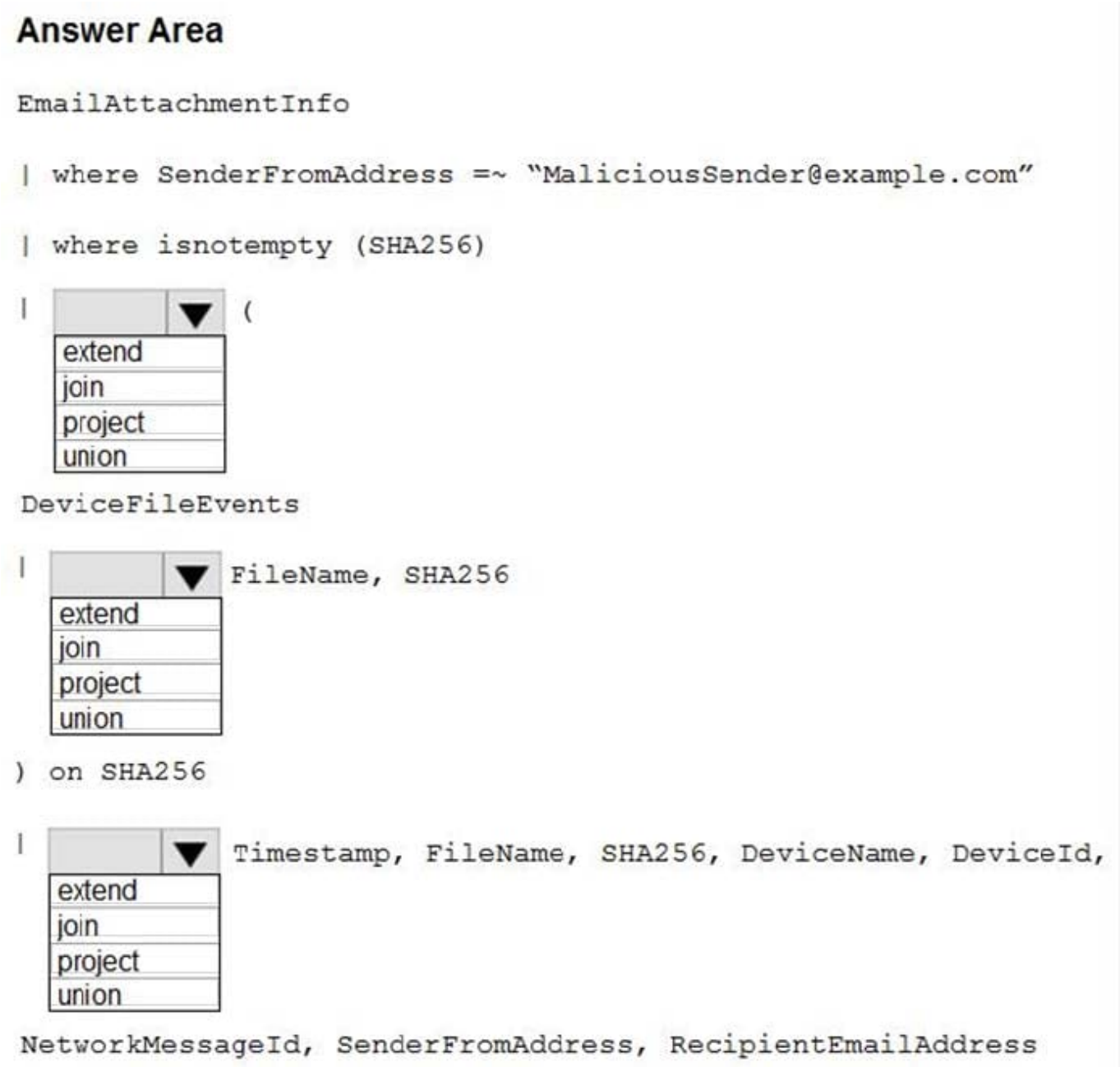
You plan to perform cross-domain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment.

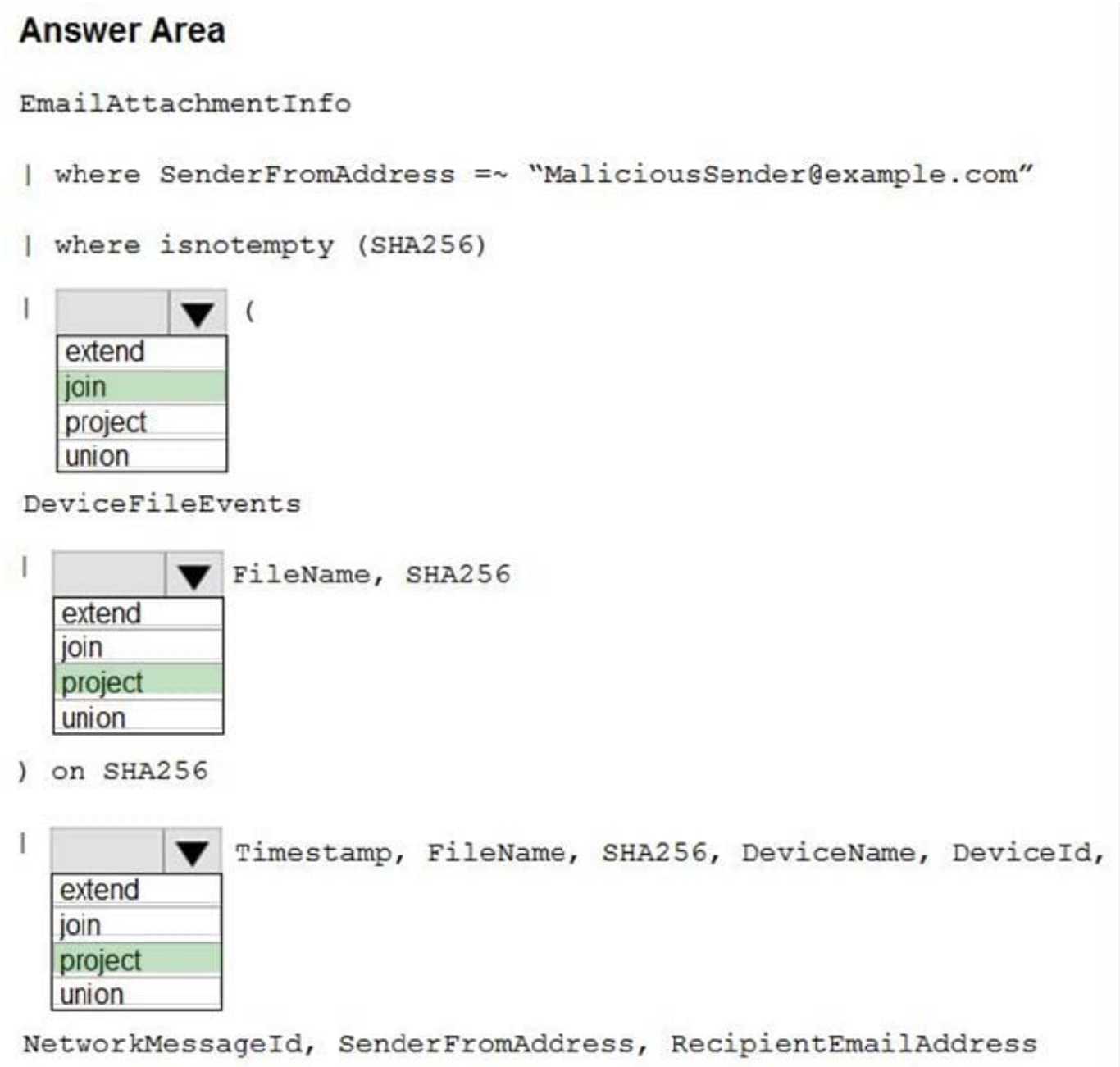
How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



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

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: CD

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

A company uses Azure Security Center and Azure Defender. However, the security operator of the company doesn\\'t receive any email notifications for security alerts. What should be configured in Security Center to enable the email notifications?

A. Pricing and settings

B. Security solutions

C. Security policy

D. Azure Defender

Correct Answer: A

QUESTION 8

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a resource group named RG1. RG1 contains 20 virtual machines that run Windows Server 2019. You need to configure just-in-time (JIT) access for the virtual machines in RG1. The solution must meet the following requirements:

1.

Limit the maximum request time to two hours.

2.

Limit protocols access to Remote Desktop Protocol (RDP) only.

3.

Minimize administrative effort. What should you use?

A. Azure AD Privileged Identity Management (PIM)

B. Azure Policy

C. Azure Bastion

D. Azure Front Door

Correct Answer: C

You can combine Azure Bastion with the JIT VM access feature of Microsoft Defender for Cloud. JIT provides just-in-time network-based access to VMs by locking down your VMs at the network level and blocking all unnecessary inbound traffic to specific management ports, like RDP or SSH. To be able to do this, it adds a deny rule to the Azure network security group (NSG), which protects the VM network interface or the subnet it belongs to.

When a user then requests access to the VM, the service adds a temporary allow rule to the NSG. Because the allow rule has a higher priority than the deny rule, the user can connect to the VM. The user can also only connect for a limited amount of time, with a maximum of 24 hours. This time limit is specified when JIT is configured for a specific VM or VMs.

Reference: https://wmatthyssen.com/2022/11/28/azure-bastion-combine-jit-with-azure-bastion

QUESTION 9

HOTSPOT

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

1.

List all incidents by incident number.

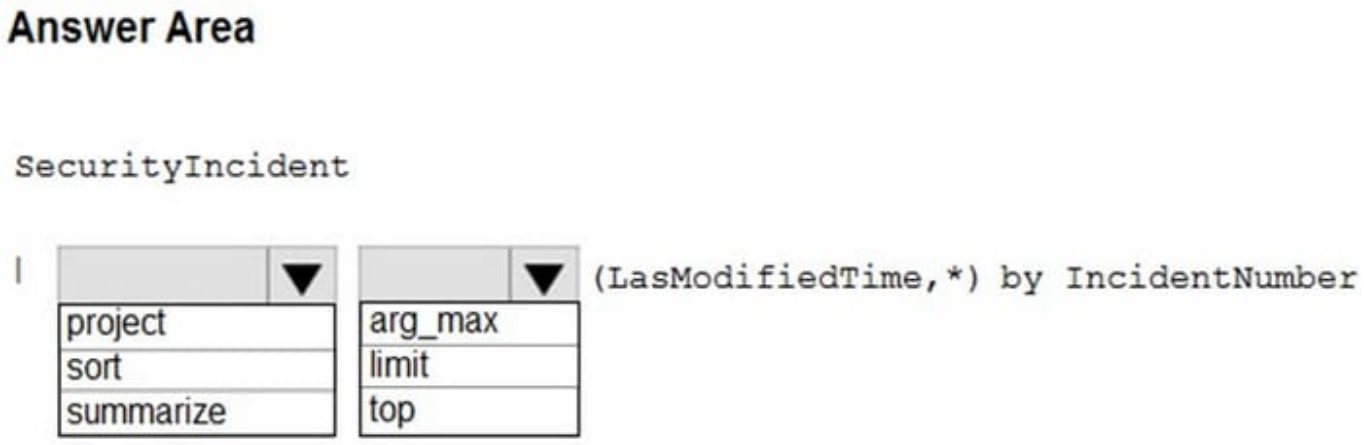
2.

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.

Hot Area:



Correct Answer:

Answer Area

```
SecurityIncident
| [project / sort / summarize] [arg_max / limit / top] (LasModifiedTime,*) by IncidentNumber
```

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

QUESTION 10

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 11

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

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

Which indicator type should you use?

A. a URL/domain indicator that has Action set to Alert only

B. a URL/domain indicator that has Action set to Alert and block

C. a file hash indicator that has Action set to Alert and block

D. a certificate indicator that has Action set to Alert and block

Correct Answer: C

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

QUESTION 12

DRAG DROP

You have a Microsoft subscription that has Microsoft Defender for Cloud enabled You configure the Azure logic apps shown in the following table.

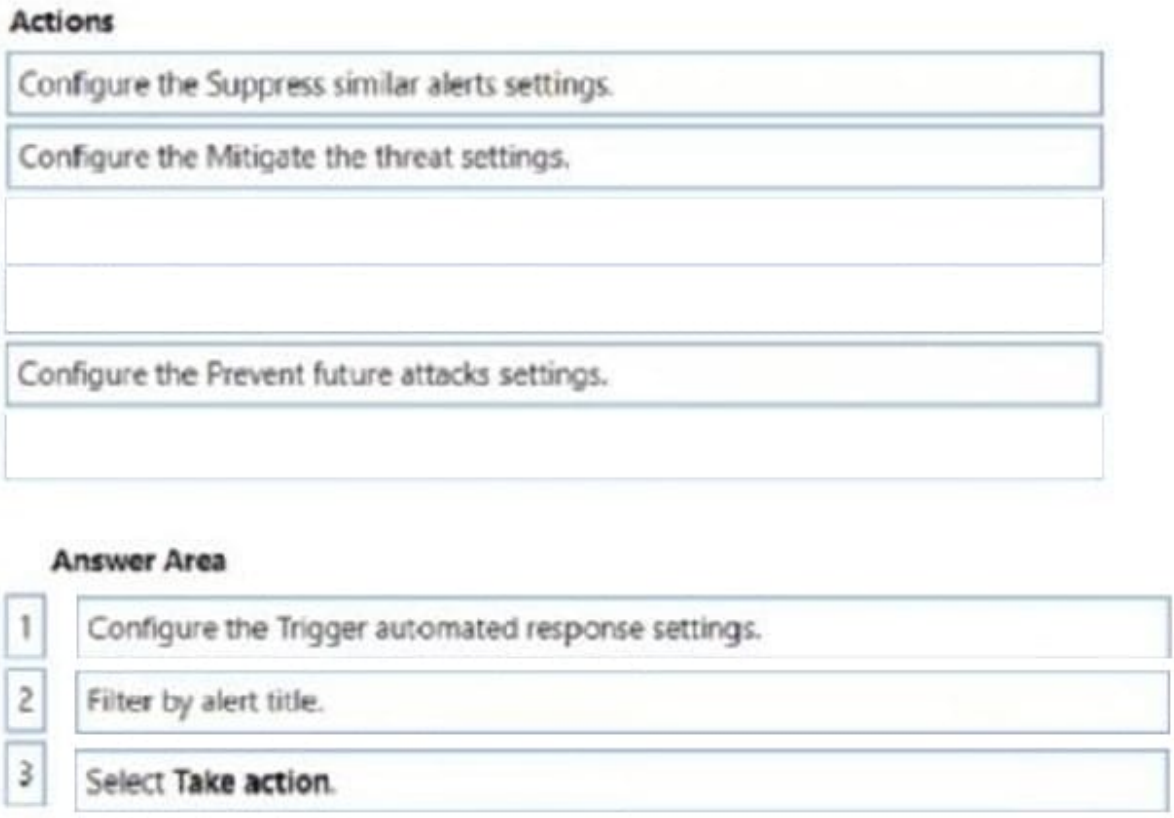
Name	Trigger	Action
LogicApp1	When a Defender for Cloud recommendation is created or triggered	Send an email
LogicApp2	When a Defender for Cloud alert is created or triggered	Send an email

You need to configure an automatic action that will run if a Suspicious process executed alert is triggered. The solution must minimize administrative effort.

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:

Correct Answer:



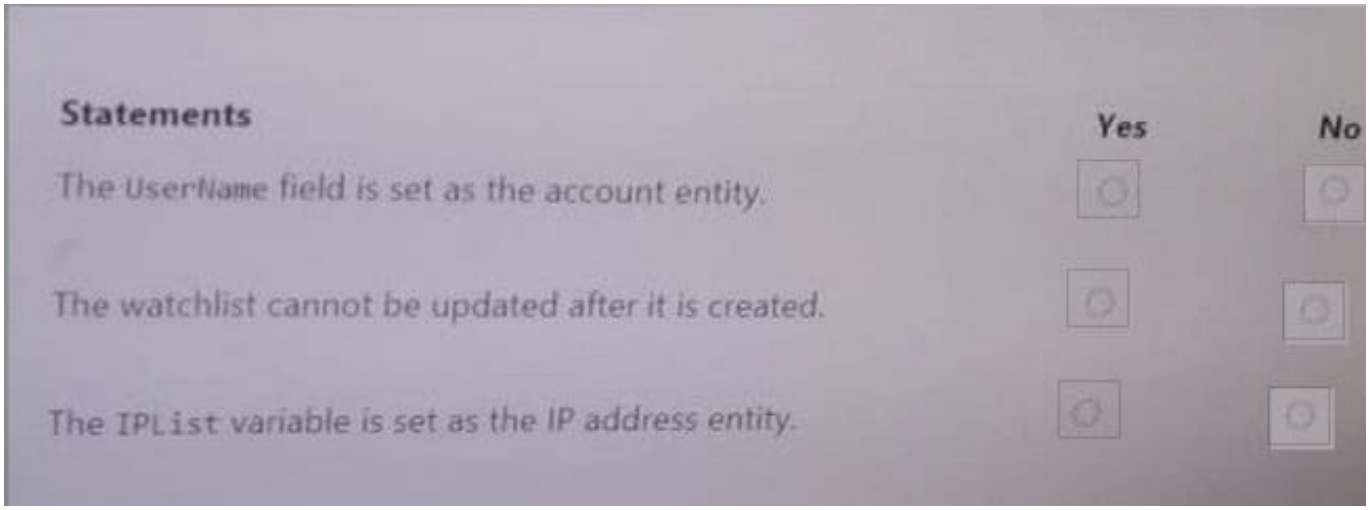
QUESTION 13

HOTSPOT

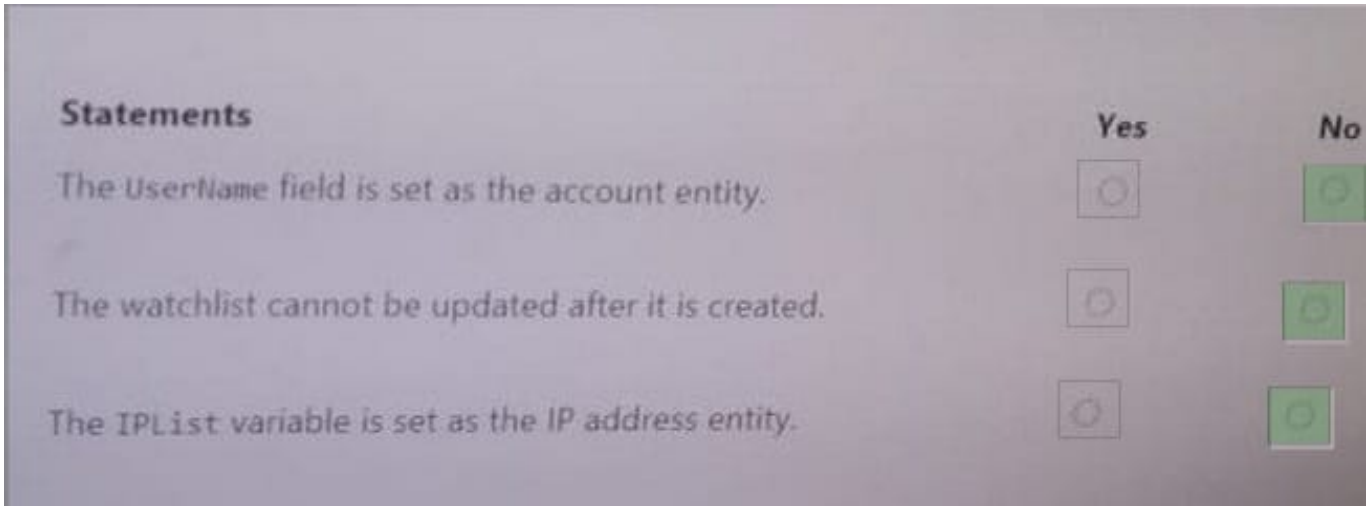
You have the following SQL query.

```
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:



Correct Answer:



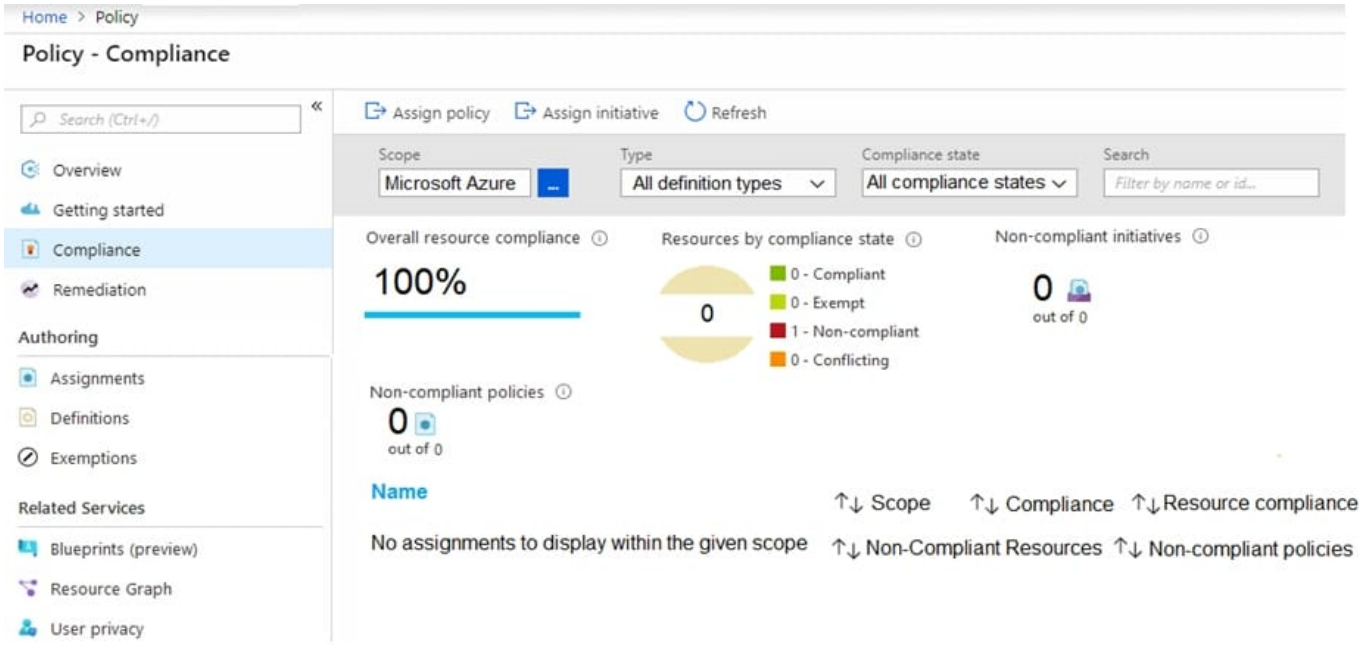
QUESTION 14

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.)

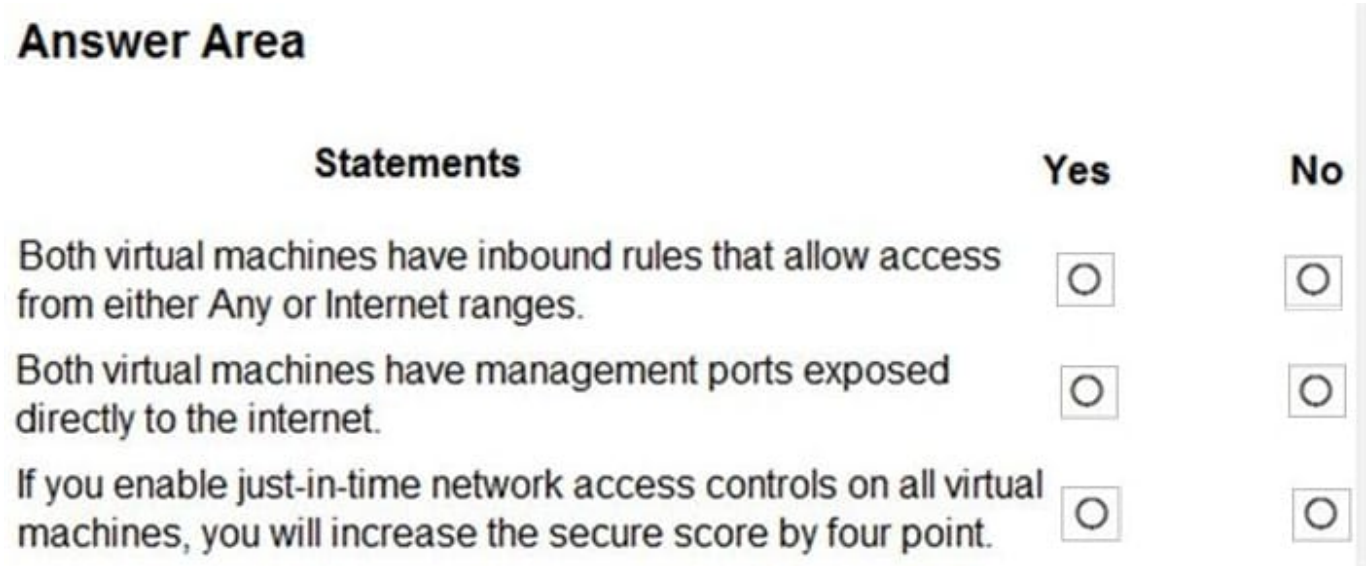
Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)



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:



Correct Answer:

Answer Area

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

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 15

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: AC

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/security-center/workflow-automation