SC-200 Visual Cert Test | Exam SC-200 Bootcamp

P.S. Free 2026 Microsoft SC-200 dumps are available on Google Drive shared by Exam-Killer: https://drive.google.com/open?id=1rkLp9sCQBceICxyXpq_qBh-MV1xNAq7M

For candidates who will buy SC-200 training materials online, they may pay more attention to privacy protection. We respect your private information, and your personal identification information will be protected well if you choose us. Once the order finishes, your personal information will be concealed. In addition, SC-200 Exam Dumps contain not only quality but also certain quantity. It will be enough for you to pass the exam. In order to build up your confidence for SC-200 exam dumps, we are pass guarantee and money back guarantee, if you fail to pass the exam, we will give you full refund.

Microsoft SC-200 Exam measures a candidate's ability to implement various security solutions, including threat protection, data governance, and identity and access management. SC-200 exam also assesses a candidate's knowledge of security operations center (SOC) operations, incident response, and compliance. Passing the SC-200 Exam demonstrates that a candidate has the necessary skills and knowledge to identify and respond to security incidents, manage security operations, and protect against security threats.

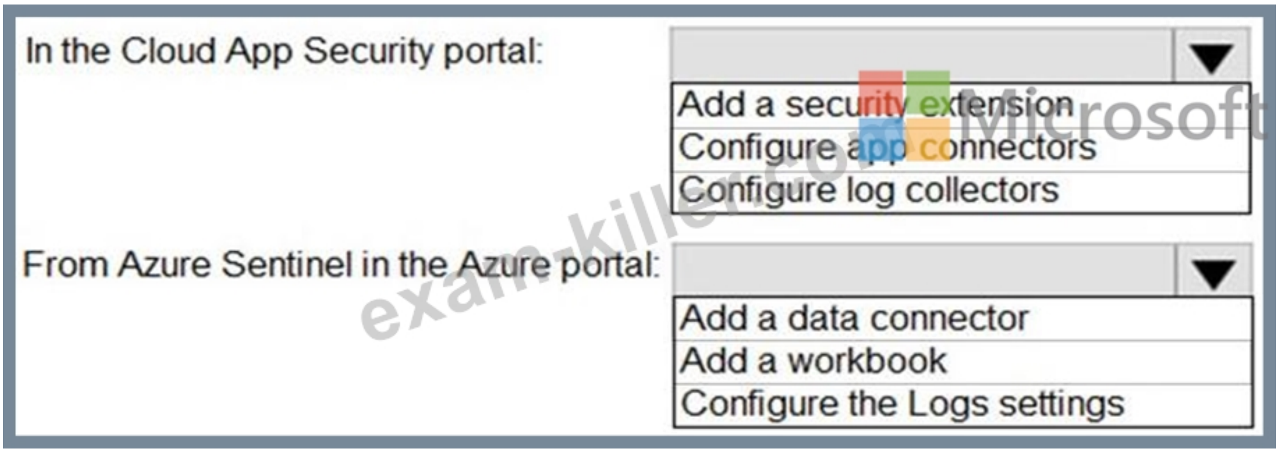
>> SC-200 Visual Cert Test <<

Exam SC-200 Bootcamp - SC-200 Dumps Torrent

They work together and put all their efforts to ensure the top standard of Microsoft SC-200 exam practice test questions. The SC-200 exam practice test questions are being offered in three different formats. These Microsoft SC-200 Exam Questions formats are PDF dumps files, desktop practice test software, and web-based practice test software.

Microsoft Security Operations Analyst Sample Questions (Q368-Q373):

NEW QUESTION # 368
You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



In the Cloud App Security portal:

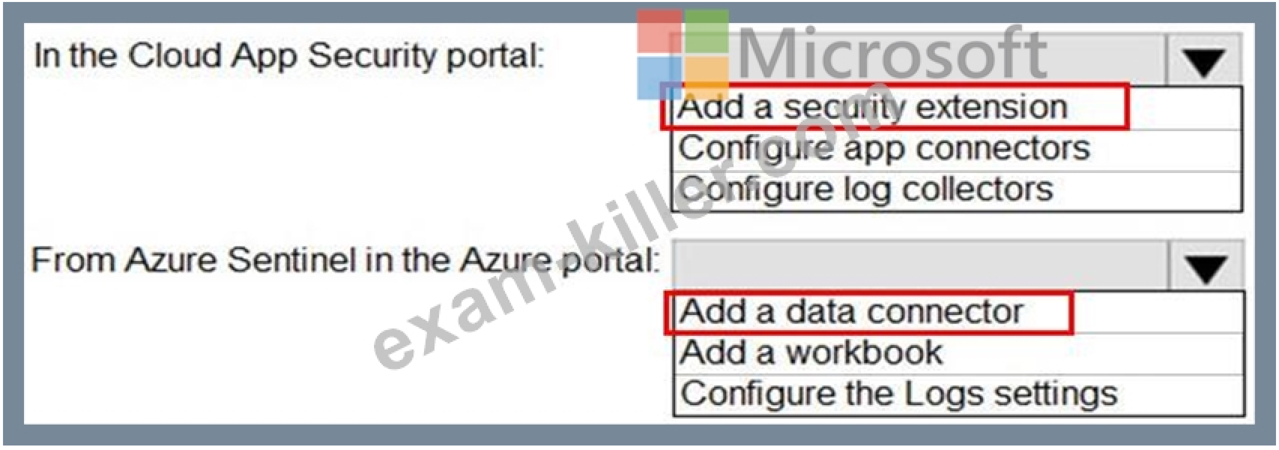
- Add a security extension
- Configure app connectors
- Configure log collectors

From Azure Sentinel in the Azure portal:

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

Answer:

Explanation:



In the Cloud App Security portal:

- [✓ Add a security extension]
- Configure app connectors
- Configure log collectors

From Azure Sentinel in the Azure portal:

- [✓ Add a data connector]
- Add a workbook
- Configure the Logs settings

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

NEW QUESTION # 369

You have a Microsoft Sentinel workspace named sws1.

You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.

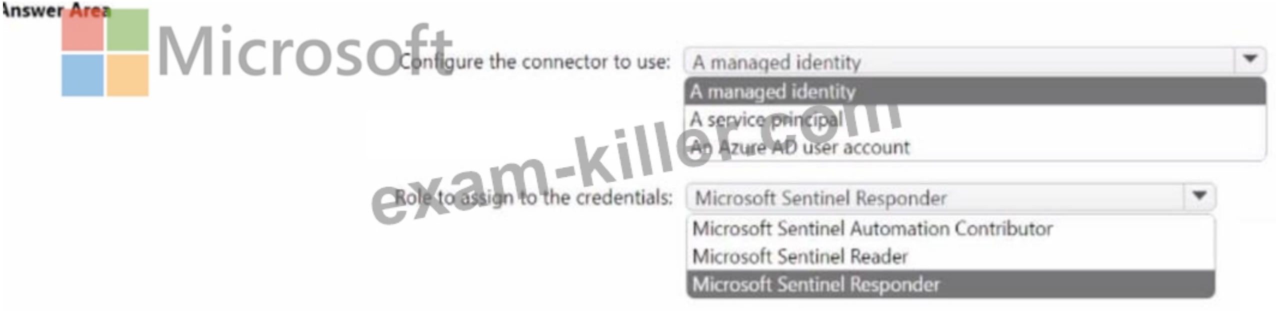
You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the following requirements:

* Minimize administrative effort.

* Use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.



Answer Area

Configure the connector to use: A managed identity

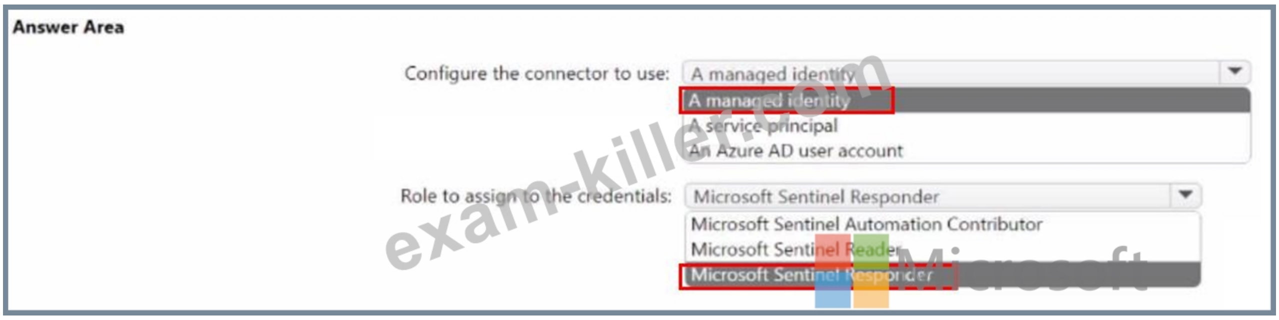
- A managed identity
- A service principal
- An Azure AD user account

Role to assign to the credentials: Microsoft Sentinel Responder

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

Answer:

Explanation:



Answer Area

Configure the connector to use: A managed identity

- A managed identity
- A service principal
- An Azure AD user account

Role to assign to the credentials: Microsoft Sentinel Responder

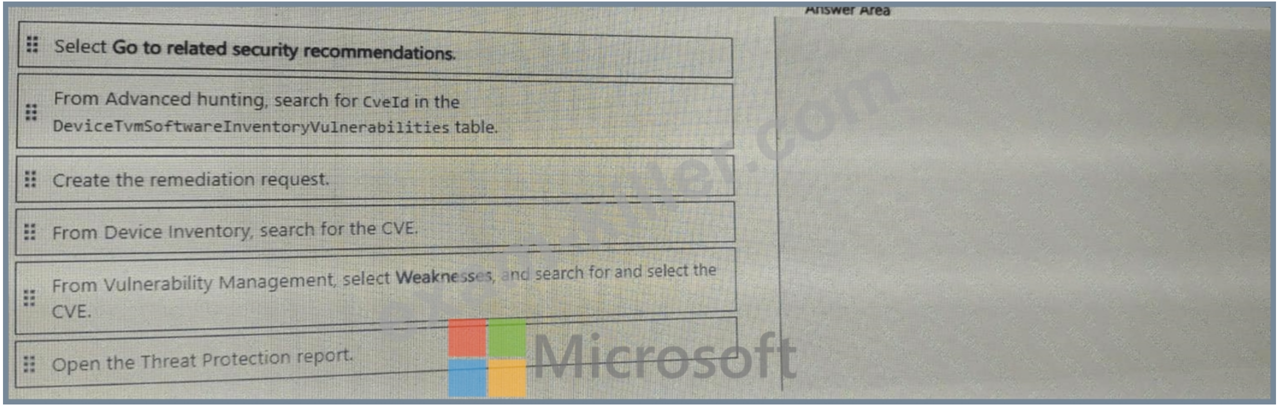
- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Reader
- Microsoft Sentinel Responder

NEW QUESTION # 370

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

You need to use the Microsoft Defender portal 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.

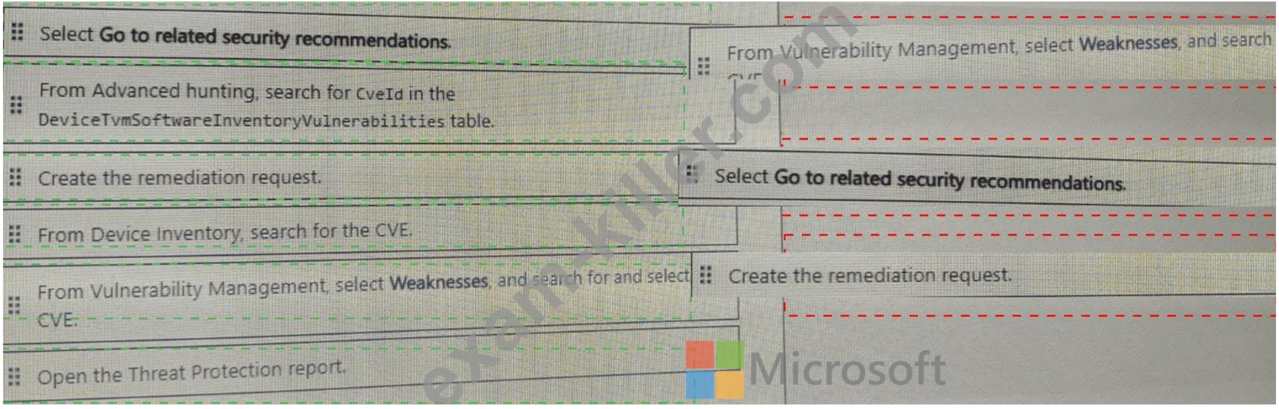


Answer Area

- Select **Go to related security recommendations**.
- From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilities` table.
- Create the remediation request.
- From Device Inventory, search for the CVE.
- From Vulnerability Management, select **Weaknesses**, and search for and select the CVE.
- Open the Threat Protection report.

Answer:

Explanation:



- Select **Go to related security recommendations**.
- From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilities` table.
- Create the remediation request.
- From Device Inventory, search for the CVE.
- From Vulnerability Management, select **Weaknesses**, and search for and select the CVE.
- Open the Threat Protection report.

1. From Vulnerability Management, select **Weaknesses**, and search
2. Select **Go to related security recommendations**.
3. Create the remediation request.

Explanation:

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

* Select Go to related security recommendations.

* Create the remediation request.

According to Microsoft Defender Vulnerability Management documentation, the correct workflow for responding to a new CVE in your organization-especially when there is an active exploit-is to begin your investigation within the Vulnerability Management section of the Microsoft Defender portal.

* From Vulnerability Management, select Weaknesses -Microsoft explains that all known CVEs are listed under Weaknesses in the Defender portal. You search by CVE ID (for example, CVE-2024-xxxx) to view its details, exploitability data, and the devices affected.

* Select Go to related security recommendations -After opening the CVE details, the portal shows associated security recommendations that describe how to remediate the issue (such as updating software, removing an at-risk version, or applying a patch). Selecting Go to related security recommendations links the CVE directly to actionable remediation guidance.

* Create the remediation request -Finally, Microsoft Defender for Endpoint allows security teams to formally request remediation

from IT administrators or system owners. You can create a remediation request directly from the recommendation page, assigning it to the responsible group and specifying a due date.

This sequence aligns with Microsoft's recommended remediation workflow for CVEs as described in Defender Vulnerability Management documentation and ensures that remediation actions are tracked and executed efficiently through the portal.

# Therefore, the correct order is:

(1) From Vulnerability Management # Weaknesses # search CVE # (2) Go to related security recommendations # (3) Create remediation request.

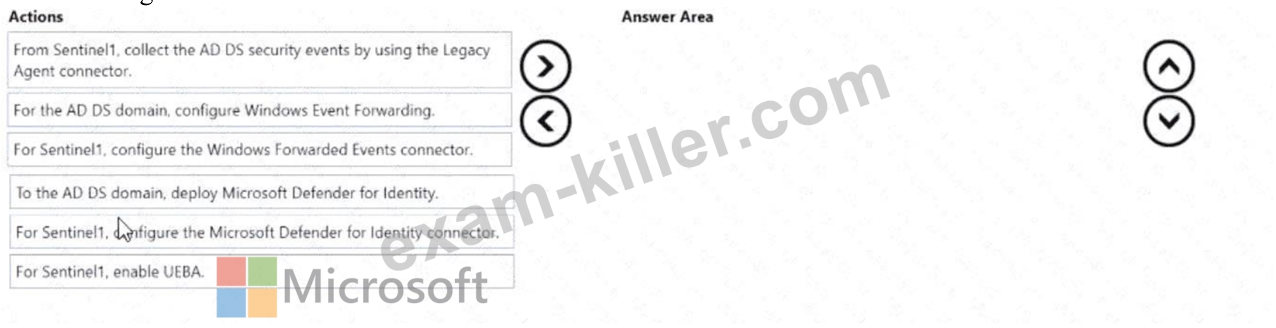
NEW QUESTION # 371

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

You have a Microsoft Sentinel workspace named Sentinel1.

You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel1 and collect security events from the AD DS domain.

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



Actions

From Sentinel1, collect the AD DS security events by using the Legacy Agent connector.

For the AD DS domain, configure Windows Event Forwarding.

For Sentinel1, configure the Windows Forwarded Events connector.

To the AD DS domain, deploy Microsoft Defender for Identity.

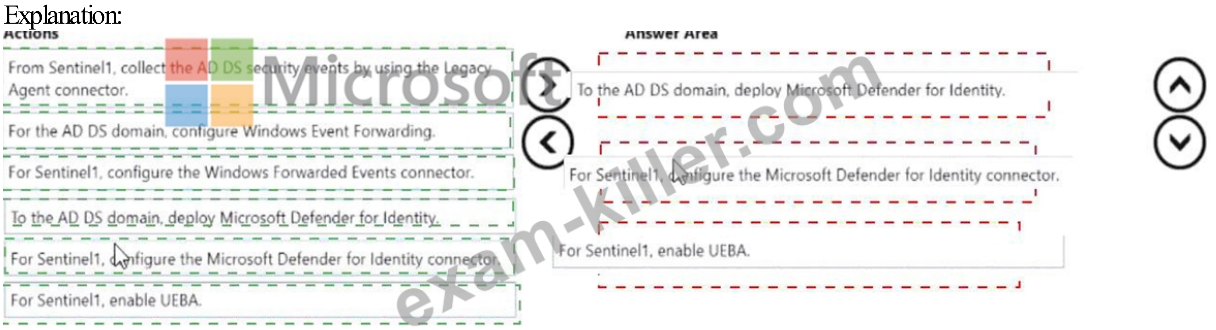
For Sentinel1, configure the Microsoft Defender for Identity connector.

For Sentinel1, enable UEBA.

Answer Area

Answer:

Explanation:



Actions

From Sentinel1, collect the AD DS security events by using the Legacy Agent connector.

For the AD DS domain, configure Windows Event Forwarding.

For Sentinel1, configure the Windows Forwarded Events connector.

To the AD DS domain, deploy Microsoft Defender for Identity.

For Sentinel1, configure the Microsoft Defender for Identity connector.

For Sentinel1, enable UEBA.

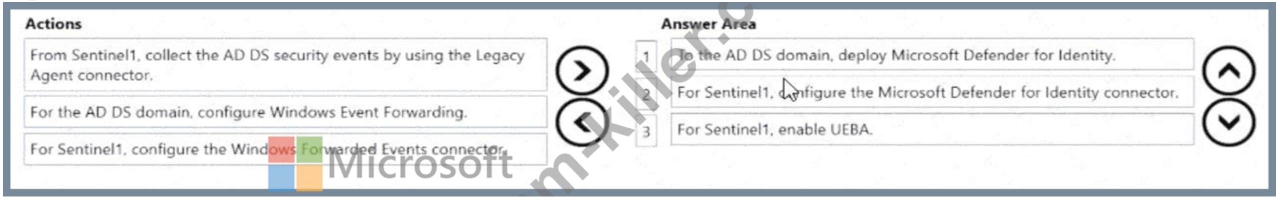
Answer Area

To the AD DS domain, deploy Microsoft Defender for Identity.

For Sentinel1, configure the Microsoft Defender for Identity connector.

For Sentinel1, enable UEBA.

Explanation:



Actions

From Sentinel1, collect the AD DS security events by using the Legacy Agent connector.

For the AD DS domain, configure Windows Event Forwarding.

For Sentinel1, configure the Windows Forwarded Events connector.

Answer Area

1 To the AD DS domain, deploy Microsoft Defender for Identity.

2 For Sentinel1, configure the Microsoft Defender for Identity connector.

3 For Sentinel1, enable UEBA.

To enable User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel and collect Active Directory Domain Services (AD DS) security events, the integration relies on Microsoft Defender for Identity (MDI).

Defender for Identity monitors on-premises domain controllers and provides deep identity-based telemetry that Sentinel consumes for behavioral analytics and threat detection.

Here's the correct sequence explained step-by-step:

* Deploy Microsoft Defender for Identity on the AD DS domain

* Defender for Identity sensors must be installed on each domain controller (or dedicated server) in your on-premises AD DS environment.

* This step enables continuous monitoring of AD activities like logons, Kerberos authentications, and LDAP queries.

* Microsoft documentation states:

"To collect and analyze AD DS activities for UEBA, deploy Microsoft Defender for Identity sensors in your domain controllers."

* Configure the Microsoft Defender for Identity connector in Microsoft Sentinel

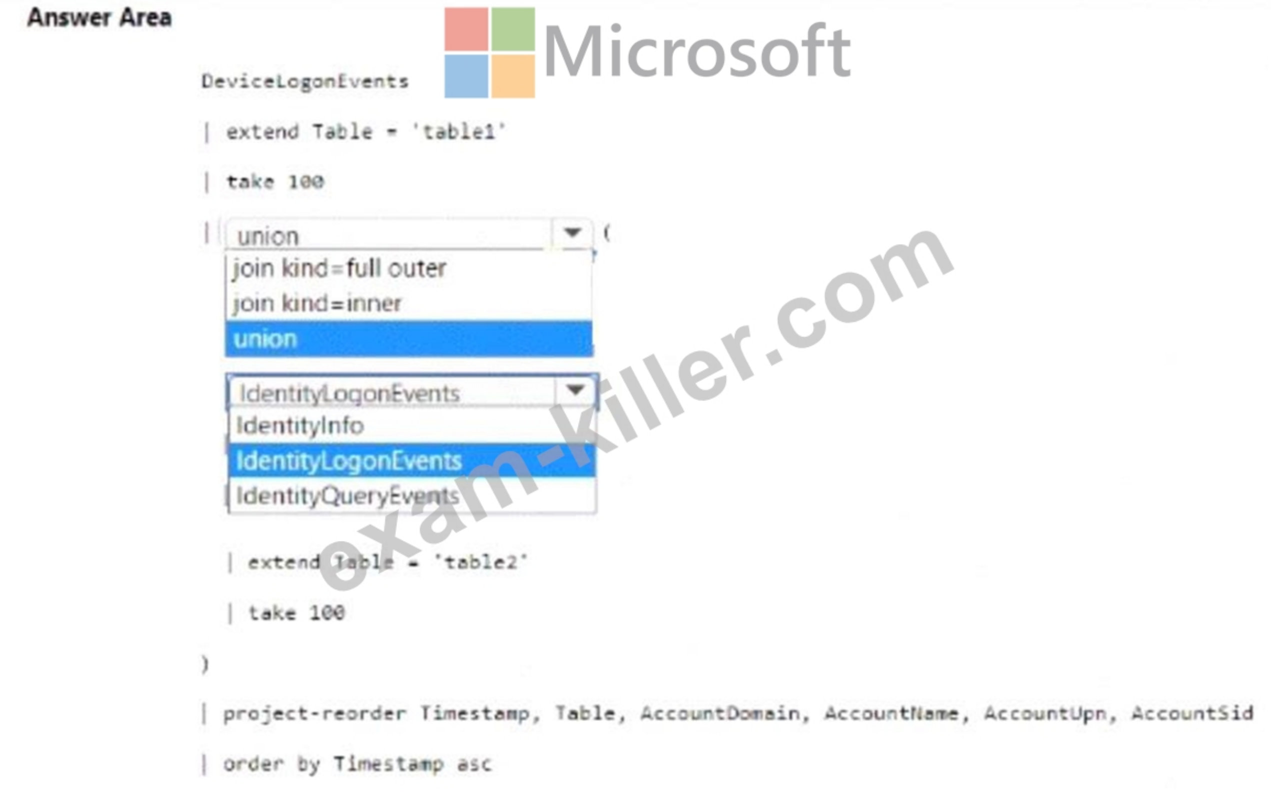
* In the Sentinel workspace (Sentinel1), go to Data connectors # Microsoft Defender for Identity # Connect.

* This connector ingests identity-related alerts and telemetry from Defender for Identity into Sentinel's Log Analytics workspace.

* It allows Sentinel to correlate identity-based security data with other sources for threat detection and investigation.

* Enable UEBA in Microsoft Sentinel
* After integrating MDI, enable UEBA in Sentinel's configuration settings.
* UEBA uses identity data (from MDI and Azure AD) and other logs to build behavioral baselines and detect anomalies such as lateral movement or privilege escalation.
* Microsoft documentation notes:
"To start analyzing user and entity behaviors, enable UEBA after connecting identity data sources such as Defender for Identity."
Other actions listed (such as using legacy connectors or Windows Event Forwarding) are outdated or unnecessary when using MDI and Sentinel's built-in connectors.

NEW QUESTION # 372
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 36S.
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.

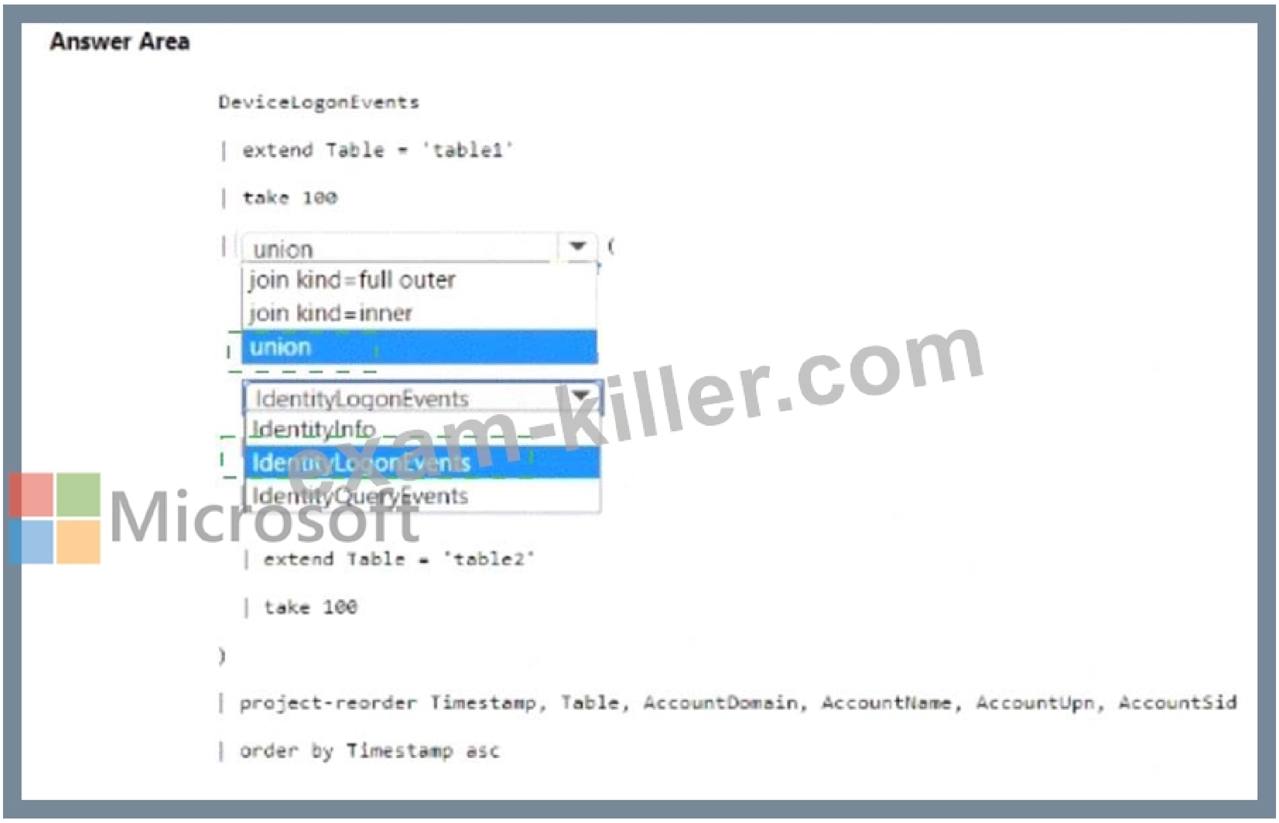


Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| union (
IdentityLogonEvents
  | extend Table = 'table2'
  | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

Answer:

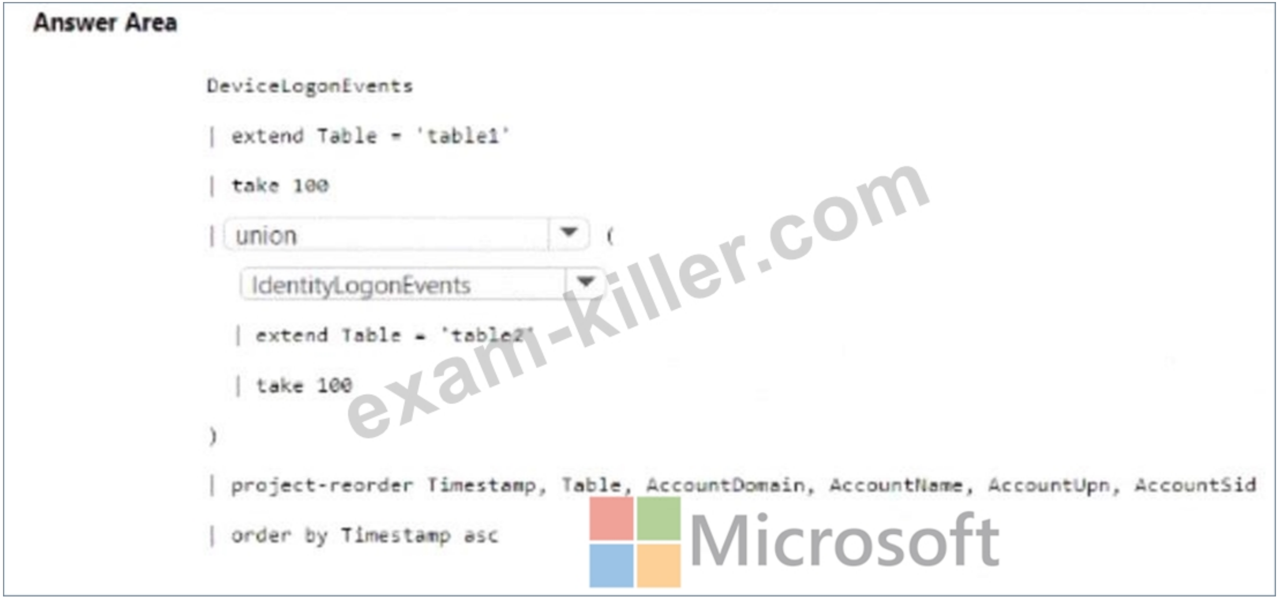
Explanation:



Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| union (
    IdentityLogonEvents
    | extend Table = 'table2'
    | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

Explanation:



Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| union (
    IdentityLogonEvents
    | extend Table = 'table2'
    | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

NEW QUESTION # 373

......

As we all know that, first-class quality always comes with the first-class service. There are also good-natured considerate after sales services offering help on our SC-200 study materials. All your questions about our SC-200 practice braindumps are deemed as prior tasks to handle. So if you have any question about our SC-200 Exam Quiz, just contact with us and we will help you immediately. That is why our SC-200 learning questions gain a majority of praise around the world.

Exam SC-200 Bootcamp: https://www.exam-killer.com/SC-200-valid-questions.html

- 100% Pass Quiz Authoritative Microsoft - SC-200 - Microsoft Security Operations Analyst Visual Cert Test □ Open website ➽ www.torrentvce.com □ and search for □ SC-200 □ for free download □SC-200 Valid Vce Dumps
- Braindumps SC-200 Downloads ⛄ Reliable SC-200 Exam Vce □ SC-200 Test Sample Online □ Search for □ SC-200 □ and download it for free on ➡ www.pdfvce.com □ website □SC-200 New Dumps Questions

- SC-200 Valid Real Exam □ SC-200 Exam Dumps Pdf □ Reliable SC-200 Exam Vce □ Go to website ➽ www.dumpsquestion.com □ open and search for ➡ SC-200 □□□ to download for free □Braindumps SC-200 Downloads
- SC-200 Valid Vce Dumps □ SC-200 New Dumps Questions ♣ SC-200 Reliable Braindumps Ppt □ Search for ▷ SC-200 ◁ and easily obtain a free download on 《 www.pdfvce.com 》 □SC-200 Valid Exam Pass4sure
- Examcollection SC-200 Vce □ Exam SC-200 Objectives Pdf □ SC-200 Sample Questions Answers □ Open □ www.practicevce.com □ and search for " SC-200 " to download exam materials for free □Exam SC-200 Topics
- Latest SC-200 Test Voucher □ SC-200 New Dumps Questions □ SC-200 Reliable Braindumps Ppt □ Enter ➡ www.pdfvce.com □□□ and search for ➠ SC-200 □ to download for free □SC-200 Test Sample Online
- SC-200 Valid Exam Pass4sure □ SC-200 Valid Exam Pass4sure □ SC-200 Valid Vce Dumps □ Easily obtain free download of 《 SC-200 》 by searching on ➽ www.pass4test.com □ □Examcollection SC-200 Vce
- New SC-200 Mock Test □ SC-200 Test Sample Online □ Braindumps SC-200 Downloads □ Simply search for （ SC-200 ） for free download on [www.pdfvce.com] □SC-200 Sample Questions Answers
- 2026 100% Free SC-200 –Professional 100% Free Visual Cert Test | Exam SC-200 Bootcamp □ Download ➠ SC-200 □ for free by simply searching on □ www.testkingpass.com □ □Relevant SC-200 Questions
- Exam SC-200 Topics □ SC-200 Test Sample Online □ New SC-200 Mock Test □ Open website ⇛ www.pdfvce.com ⇚ and search for ➤ SC-200 □ for free download □SC-200 Test Sample Online
- SC-200 Valid Vce Dumps □ SC-200 New Dumps Questions □ Reliable SC-200 Exam Vce □ Simply search for [SC-200] for free download on 【 www.examcollectionpass.com 】 □Reliable SC-200 Exam Vce
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, bigbrainsacademy.co.za, www.stes.tyc.edu.tw, www.huajiaoshu.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.slideshare.net, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, iachm.com, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New SC-200 dumps are available on Google Drive shared by Exam-Killer: https://drive.google.com/open?id=1rkLp9sCQBceICxyXpq_qBh-MV1xNAq7M