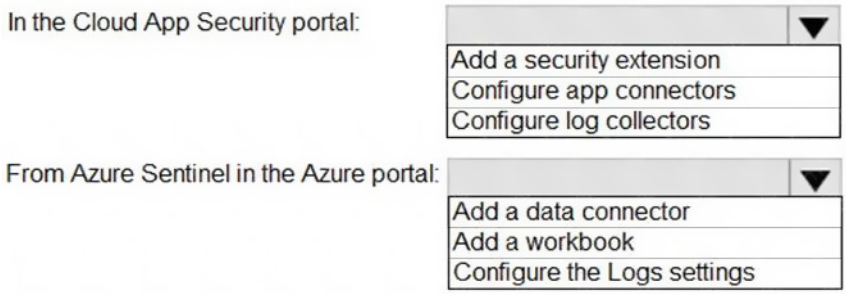
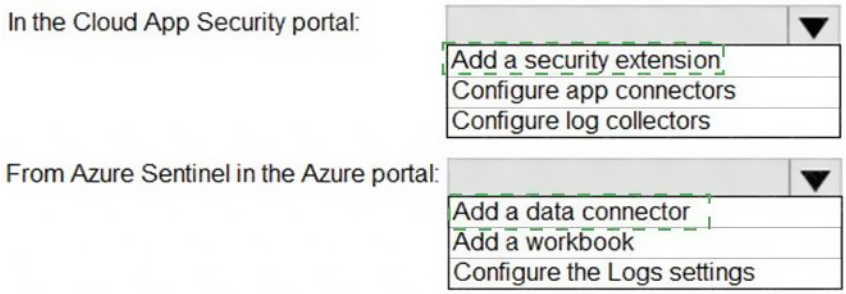
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Correct Answer:



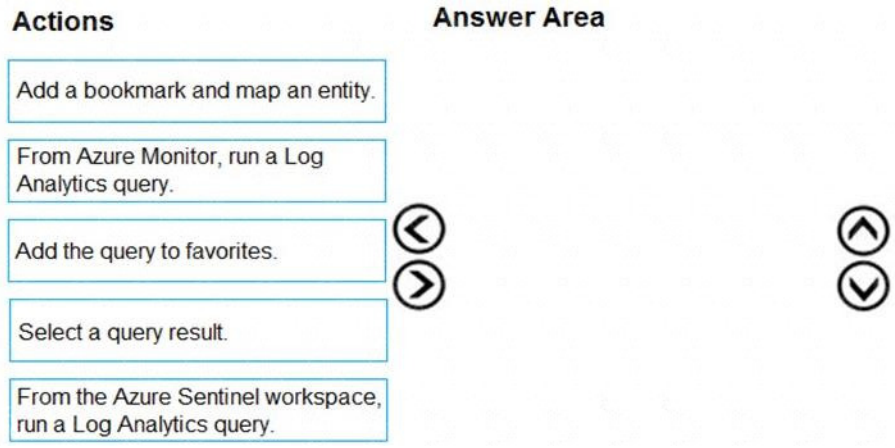
QUESTION 6
You need to create the test rule to meet the Azure Sentinel requirements. What should you do when you create the rule?

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.

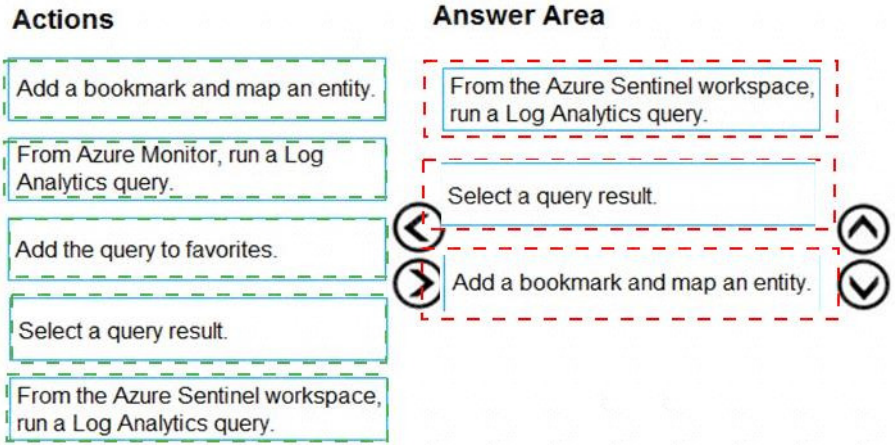
Correct Answer: C
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

QUESTION 7
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.



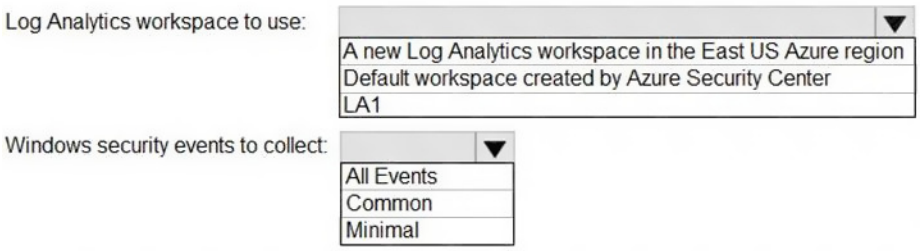
Correct Answer:



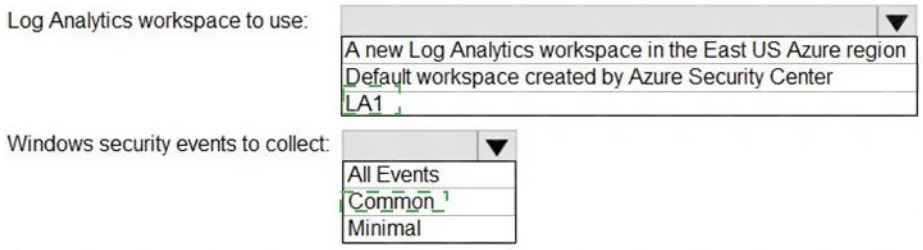
QUESTION 8
HOTSPOT
You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.

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.

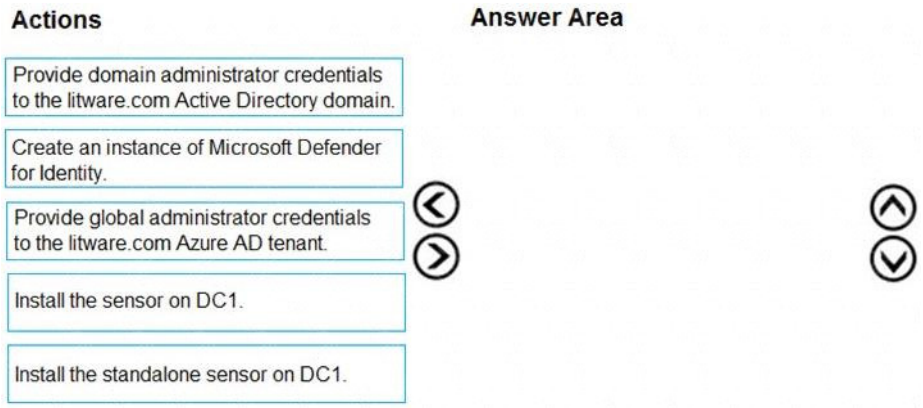


Correct Answer:

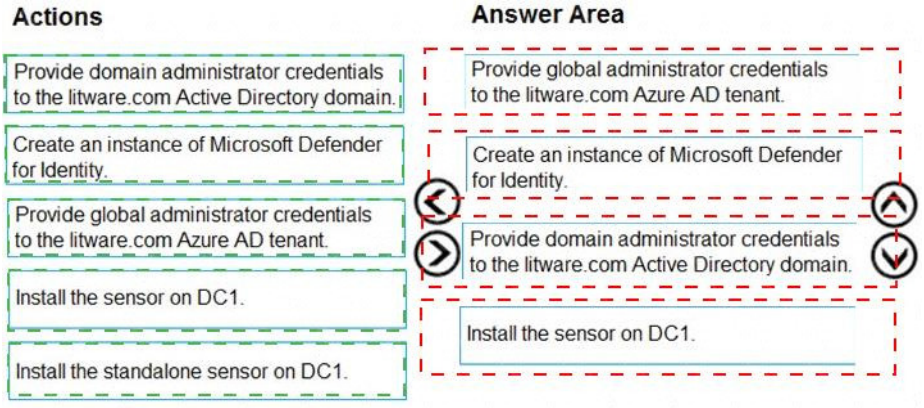


QUESTION 9
DRAG DROP
You need to configure DC1 to meet the business requirements.

Which four 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.



Correct Answer:



QUESTION 10
You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements. Which policy should you modify?

A. Activity from suspicious IP addresses
B. Activity from anonymous IP addresses
C. Impossible travel

D. Risky sign-in

Correct Answer: C
Explanation:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

Topic 3, Mix Questions

QUESTION 1
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
Explanation:
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

QUESTION 2
You are investigating an incident in Azure Sentinel that contains more than 127 alerts.

You discover eight alerts in the incident that require further investigation.

You need to escalate the alerts to another Azure Sentinel administrator.

What should you do to provide the alerts to the administrator?

A. Create a Microsoft incident creation rule
B. Share the incident URL
C. Create a scheduled query rule
D. Assign the incident

Correct Answer: D
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

QUESTION 3

You create an Azure subscription named sub1.

In sub1, you create a Log Analytics workspace named workspace1.

You enable Azure Security Center and configure Security Center to use workspace1.

You need to ensure that Security Center processes events from the Azure virtual machines that report to workspace1.

What should you do?

A. In workspace1, install a solution.
B. In sub1, register a provider.
C. From Security Center, create a Workflow automation.
D. In workspace1, create a workbook.

Correct Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

QUESTION 4
You have a Microsoft 365 tenant that uses Microsoft Exchange Online and Microsoft Defender for Office 365. What should you use to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user?

A. the Threat Protection Status report in Microsoft Defender for Office 365
B. the mailbox audit log in Exchange
C. the Safe Attachments file types report in Microsoft Defender for Office 365
D. the mail flow report in Exchange

Correct Answer: A
Explanation:
To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections).

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

QUESTION 5
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.