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

Correct Answer:

```
SecurityIncident
| summarize arg_max (LasModifiedTime,*) by IncidentNumber
```

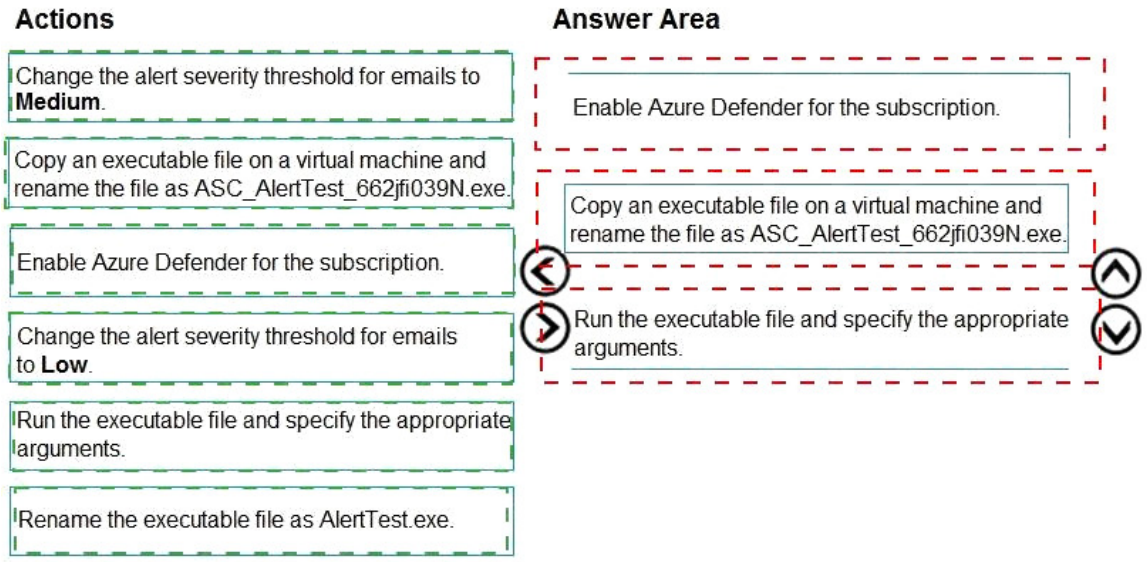
QUESTION 6
DRAG DROP
You create a new Azure subscription and start collecting logs for Azure Monitor.

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.

Actions	Answer Area
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.	

Correct Answer:



QUESTION 7
You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC). What should you use?

A. notebooks in Azure Sentinel
B. Microsoft Cloud App Security
C. Azure Monitor
D. hunting queries in Azure Sentinel

Correct Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

QUESTION 8
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
D. none of the above

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

QUESTION 9

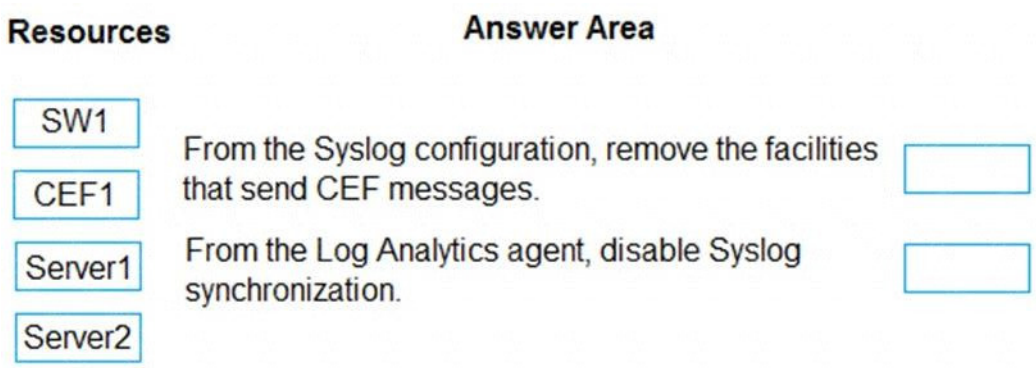
DRAG DROP
You have the resources shown in the following table.

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

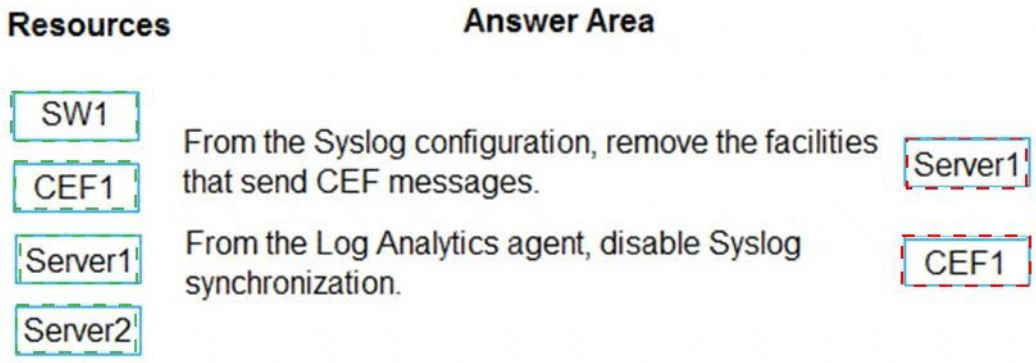
You need to prevent duplicate events from occurring in SW1.

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.



Correct Answer:



QUESTION 10

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 appthat has a manual trigger
C. Create an Azure logic app that has an Azure Security Center alert trigger.
D. Create an Azure logic appthat has an HTTP trigger.
E. From Azure Active Directory (Azure AD), add an app registration.

Correct Answer: AC
Explanation:
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

QUESTION 11
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
Explanation:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

QUESTION 12
A company uses Azure Sentinel.

You need to create an automated threat response.

What should you use?

A. a data connector
B. a playbook
C. a workbook
D. a Microsoft incident creation rule

Correct Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION 13
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 are configuring Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a Microsoft incident creation rule for a data connector.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

QUESTION 14
You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center. You need to create a query that will be used to display a bar graph. What should you include in the query?

A. extend
B. bin
C. count
D. workspace

Correct Answer: C
Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations

QUESTION 15
You create a custom analytics rule to detect threats in Azure Sentinel.

You discover that the rule fails intermittently.