- **Vendor:** Microsoft
- **Exam Code:** SC-200
- **Exam Name:** Microsoft Security Operations Analyst
- **New Updated Questions from Braindump2go**
- **(Updated in September/2021)**

QUESTION 82
Hotspot Question
You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical 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.

Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

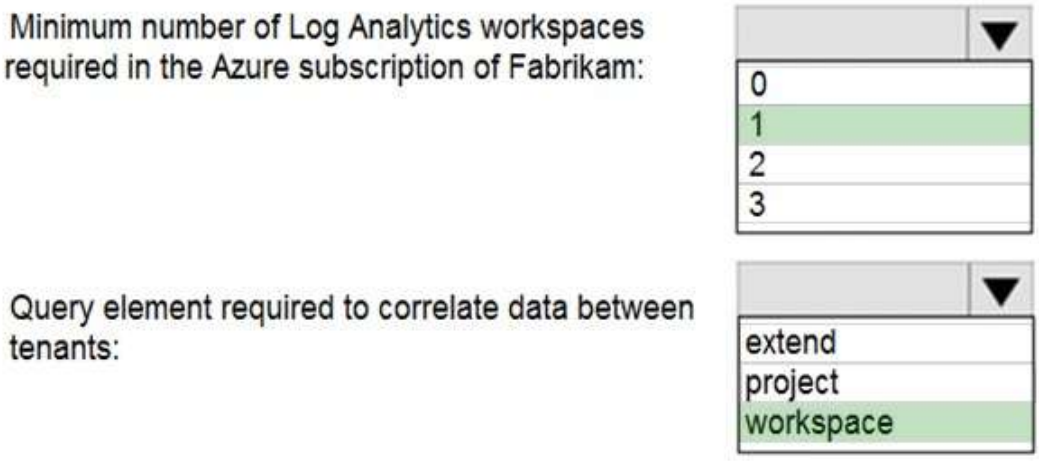
- 0
- 1
- 2
- 3

Query element required to correlate data between tenants:

- extend
- project
- workspace

Answer:

Answer Area



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

QUESTION 83
You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.
Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant.
B. Select Investigate files, and then filter App to Office 365.
C. Select Investigate files, and then select New policy from search.
D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings.
E. From Settings, select Information Protection, select Files, and then enable file monitoring.
F. Select Investigate files, and then filter File Type to Document.

Answer: DE
Explanation:
https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp
https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

QUESTION 84
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.

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

QUESTION 85
You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.
You are troubleshooting an issue on the virtual machines.
In Security Center, you need to view the alerts generated by the virtual machines during the last five days.
What should you do?

A. Change the rule expiration date of the suppression rule.
B. Change the state of the suppression rule to Disabled.
C. Modify the filter for the Security alerts page.
D. View the Windows event logs on the virtual machines.

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules

QUESTION 86
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

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

QUESTION 87
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Enable Entity behavior analytics.
B. Associate a playbook to the analytics rule that triggered the incident.
C. Enable the Fusion rule.
D. Add a playbook.
E. Create a workbook.

Answer: AB
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/enable-entity-behavior-analytics
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

QUESTION 88
You have the following environment:
- Azure Sentinel
- A Microsoft 365 subscription
- Microsoft Defender for Identity
- An Azure Active Directory (Azure AD) tenant

You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.
You deploy Microsoft Defender for Identity by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified in Active Directory.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Configure the Advanced Audit Policy Configuration settings for the domain controllers.
B. Modify the permissions of the Domain Controllers organizational unit (OU).
C. Configure auditing in the Microsoft 365 compliance center.
D. Configure Windows Event Forwarding on the domain controllers.

Answer: AD
Explanation:
https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection
https://docs.microsoft.com/en-us/defender-for-identity/configure-event-collection