Vendor: Microsoft

Exam Code: SC-200

Exam Name: Microsoft Security Operations Analyst

Version: DEMO

QUESTION 1
Case Study 1 - Contoso Ltd

Overview
A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment
End-User Environment
All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure
All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems
The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements
Planned Changes
Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements
Contoso identifies the following technical requirements:

- Receive alerts if an Azure virtual machine is under brute force attack.
- Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
- Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.

- Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure AD applications.
- Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

```
BehaviorAnalytics
 | where ActivityType == "FailedLogOn"
 | where ________ == True
```

The issue for which team can be resolved by using Microsoft Defender for Endpoint?

A. executive
B. sales
C. marketing
D. security

Answer: B
Explanation:
Sales need iOS EndPoint Protection from DfE.
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios

QUESTION 2
Case Study 2 - Litware Inc

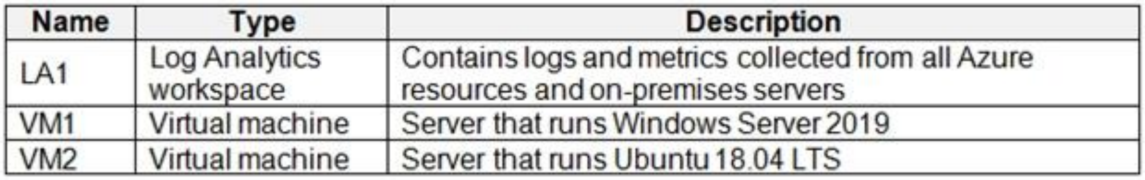
Overview
Litware Inc. is a renewable company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment
Identity Environment
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment
Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment
Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.



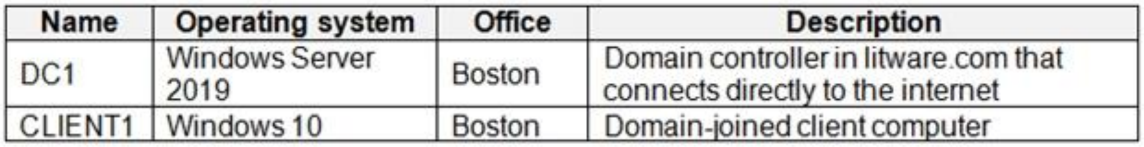
Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment

The on-premises network contains the computers shown in the following table.



Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes

Litware plans to implement the following changes:

- Create and configure Azure Sentinel in the Azure subscription.
- Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements

Litware identifies the following business requirements:

- The principle of least privilege must be used whenever possible.
- Costs must be minimized, as long as all other requirements are met.
- Logs collected by Log Analytics must provide a full audit trail of user activities.
- All domain controllers must be protected by using Microsoft Defender for Identity.

Azure Information Protection Requirements

All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection – Data discovery dashboard.

Microsoft Defender for Endpoint requirements

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Microsoft Cloud App Security requirements

Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements

All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements

Litware must meet the following Azure Sentinel requirements:

- Integrate Azure Sentinel and Cloud App Security.
- Ensure that a user named admin1 can configure Azure Sentinel playbooks.
- Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
- Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.

- Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

You need to implement the Azure Information Protection requirements.

What should you configure first?

A. Device health and compliance reports settings in Microsoft Defender Security Center
B. scanner clusters in Azure Information Protection from the Azure portal
C. content scan jobs in Azure Information Protection from the Azure portal
D. Advanced features from Settings in Microsoft Defender Security Center

Answer: D
Explanation:
Turn on the Azure Information Protection integration so that when a file that contains sensitive information is discovered by Defender for Endpoint though labels or information types, it is automatically forwarded to Azure Information Protection from the device.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/information-protection-in-windows-overview?view=o365-worldwide#data-discovery-and-data-classification

QUESTION 3
You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online.

You delete users from the subscription.

You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted.

What should you use?

A. a file policy in Microsoft Defender for Cloud Apps
B. an access review policy
C. an alert policy in Microsoft Defender for Office 365
D. an insider risk policy

Answer: C
Explanation:
When users leave your organization, there are specific risk indicators typically associated with data theft by departing users. This policy template uses exfiltration indicators for risk scoring and focuses on detection and alerts in this risk area.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-policies?view=o365-worldwide#data-theft-by-departing-users

QUESTION 4
You have five on-premises Linux servers.

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to use Defender for Cloud to protect the Linux servers.

What should you install on the servers first?

A. the Dependency agent
B. the Log Analytics agent
C. the Azure Connected Machine agent
D. the Guest Configuration extension

Answer: B
Explanation:
Defender for Cloud depends on the Log Analytics agent.
Use the Log Analytics agent if you need to:
* Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure
* Etc.

Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#log-analytics-agent

QUESTION 5
You have two Azure subscriptions that use Microsoft Defender for Cloud.

You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.

What should you do in the Azure portal?

A. Create an Azure Policy assignment.
B. Modify the Workload protections settings in Defender for Cloud.
C. Create an alert rule in Azure Monitor.
D. Modify the alert settings in Defender for Cloud.

Answer: A
Explanation:
To suppress alerts at the management group level, use Azure Policy.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules#create-a-suppression-rule

QUESTION 6
Drag and Drop Question

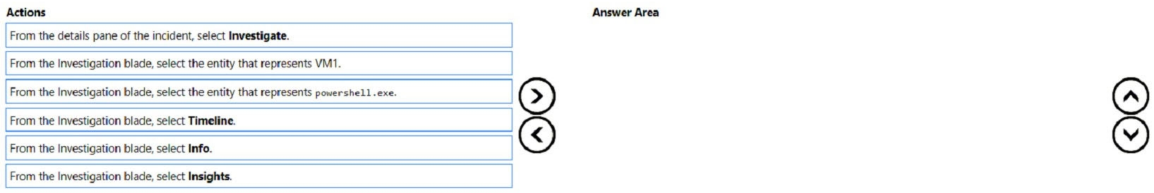
You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.

You receive an alert for suspicious use of PowerShell on VM1.

You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:

- The modification of local group memberships
- The purging of event logs

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

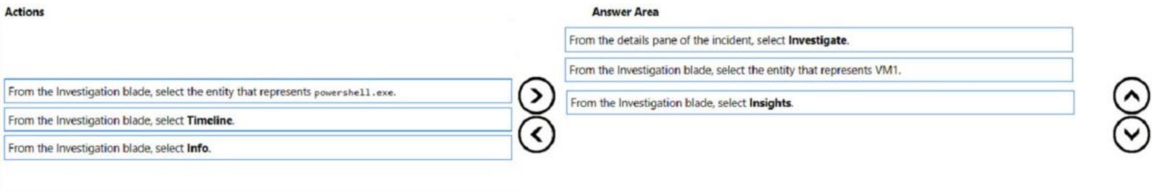


Actions

- From the details pane of the incident, select **Investigate**.
- From the Investigation blade, select the entity that represents VM1.
- From the Investigation blade, select the entity that represents `powershell.exe`.
- From the Investigation blade, select **Timeline**.
- From the Investigation blade, select **Info**.
- From the Investigation blade, select **Insights**.

Answer Area

Answer:



Actions

- From the Investigation blade, select the entity that represents `powershell.exe`.
- From the Investigation blade, select **Timeline**.
- From the Investigation blade, select **Info**.

Answer Area

- From the details pane of the incident, select **Investigate**.
- From the Investigation blade, select the entity that represents VM1.
- From the Investigation blade, select **Insights**.

Explanation:
Step 1: From the details pane of the incident, select Investigate.
Choose a single incident and click View full details or Investigate.

Step 2: From the Investigation blade, select the entity that represents VM1.
The Investigation Insights workbook is broken up into 2 main sections, Incident Insights and Entity Insights.

Incident Insights
The Incident Insights gives the analyst a view of ongoing Sentinel Incidents and allows for quick access to their associated metadata including alerts and entity information.

Entity Insights
The Entity Insights allows the analyst to take entity data either from an incident or through manual entry and explore related information about that entity. This workbook presently provides view of the following entity types:

- IP Address
- Account
- Host
- URL

Step 3: From the Investigation blade, select Insights
The Investigation Insights Workbook is designed to assist in investigations of Azure Sentinel Incidents or individual IP/Account/Host/URL entities.

Reference:
https://github.com/Azure/Azure-Sentinel/wiki/Investigation-Insights---Overview
https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

QUESTION 7
You create an Azure subscription.

You enable Azure Defender for the subscription.

You need to use Azure Defender to protect on-premises computers.

What should you do on the on-premises computers?

A. Install the Log Analytics agent.
B. Install the Dependency agent.
C. Configure the Hybrid Runbook Worker role.
D. Install the Connected Machine agent.

Answer: A
Explanation:
Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.
Data is collected using:

- The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.
- Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.

Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

QUESTION 8
You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.

You need to identify all the changes made to sensitivity labels during the past seven days.

What should you use?

A. the Incidents blade of the Microsoft 365 Defender portal
B. the Alerts settings on the Data Loss Prevention blade of the Microsoft 365 compliance center
C. Activity explorer in the Microsoft 365 compliance center
D. the Explorer settings on the Email & collaboration blade of the Microsoft 365 Defender portal

Answer: C
Explanation:
Labeling activities are available in Activity explorer.

For example:
Sensitivity label applied
This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label.

It is captured at the time of save in Office native applications and web applications. It is captured at the time of occurrence in Azure Information protection add-ins. Upgrade and downgrade labels actions can also be monitored via the Label event type field and filter.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer-available-events?view=o365-worldwide

QUESTION 9
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

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 10
You create a custom analytics rule to detect threats in Azure Sentinel.

You discover that the rule fails intermittently.

What are two possible causes of the failures? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. The rule query takes too long to run and times out.
B. The target workspace was deleted.
C. Permissions to the data sources of the rule query were modified.
D. There are connectivity issues between the data sources and Log Analytics

Answer: AD
Explanation:
Incorrect Answers:
B: This would cause it to fail every time, not just intermittently.
C: This would cause it to fail every time, not just intermittently.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom#troubleshooting

QUESTION 11
You have a Microsoft Sentinel workspace that contains the following incident.

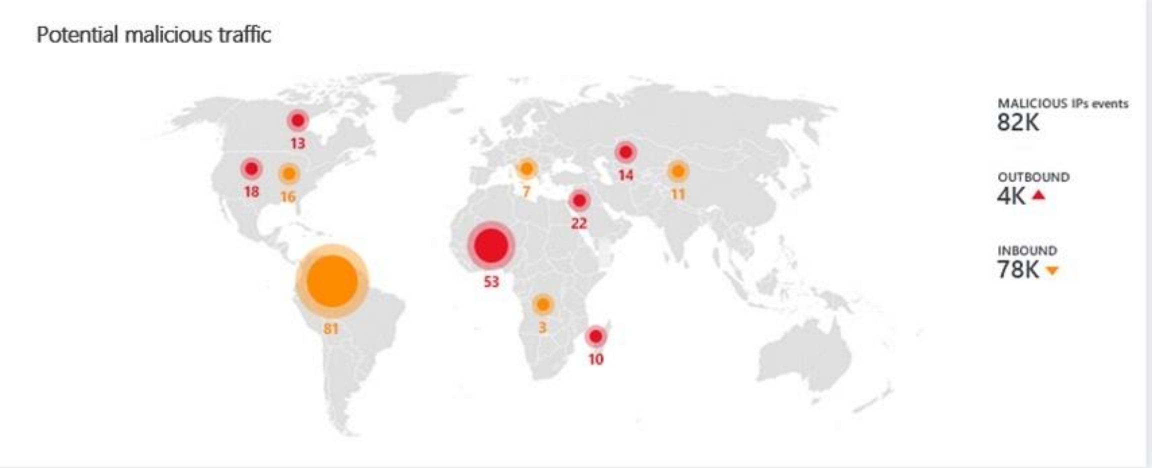
Brute force attack against Azure Portal analytics rule has been triggered.

You need to identify the geolocation information that corresponds to the incident.

What should you do?

A. From Overview, review the Potential malicious events map.
B. From Incidents, review the details of the iPCustomEntity entity associated with the incident.
C. From Incidents, review the details of the AccouncCuscomEntity entity associated with the incident.
D. From Investigation, review insights on the incident entity.

Answer: A
Explanation:
Potential malicious events: When traffic is detected from sources that are known to be malicious, Microsoft Sentinel alerts you on the map. If you see orange, it is inbound traffic: someone is trying to access your organization from a known malicious IP address. If you see Outbound (red) activity, it means that data from your network is being streamed out of your organization to a known malicious IP address.



Reference:
https://docs.microsoft.com/en-us/azure/sentinel/get-visibility#get-visualization

QUESTION 12
You have a Microsoft Sentinel workspace named workspace1 that contains custom Kusto queries.

You need to create a Python-based Jupyter notebook that will create visuals. The visuals will display the results of the queries and be pinned to a dashboard. The solution must minimize development effort.

What should you use to create the visuals?

A. plotly
B. TensorFlow
C. msticpy
D. matplotlib

Answer: C
Explanation:
msticpy is a library for InfoSec investigation and hunting in Jupyter Notebooks. It includes functionality to: query log data from multiple sources. enrich the data with Threat Intelligence, geolocations and Azure resource data. extract Indicators of Activity (IoA) from logs and unpack encoded data.

MSTICPy reduces the amount of code that customers need to write for Microsoft Sentinel, and provides:

- Data query capabilities, against Microsoft Sentinel tables, Microsoft Defender for Endpoint, Splunk, and other data sources.
- Threat intelligence lookups with TI providers, such as VirusTotal and AlienVault OTX. Enrichment functions like geolocation of IP addresses, Indicator of Compromise (IoC) extraction, and WhoIs lookups.
- Visualization tools using event timelines, process trees, and geo mapping. Advanced analyses, such as time series decomposition, anomaly detection, and clustering.

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started
https://msticpy.readthedocs.io/en/latest/

QUESTION 13
You have a Microsoft 365 subscription that uses Microsoft 365 Defender.

You need to identify all the entities affected by an incident.

Which tab should you use in the Microsoft 365 Defender portal?

A. Investigations
B. Devices
C. Evidence and Response
D. Alerts

Answer: C
Explanation:
The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents

QUESTION 14
You have an Azure subscription that uses Microsoft Sentinel and contains 100 Linux virtual machines.
You need to monitor the virtual machines by using Microsoft Sentinel. The solution must meet the following requirements:

- Minimize administrative effort.
- Minimize the parsing required to read fog data.

What should you configure?

A. a Log Analytics Data Collector API
B. REST API integration
C. a Common Evert Format (CEF) connector
D. a Syslog connector

Answer: C

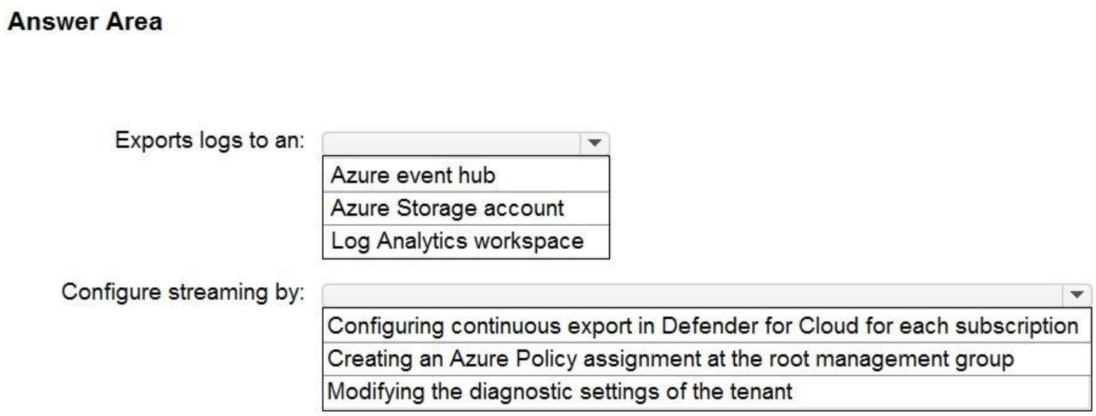
Explanation:
Minimize the parsing required to read fog data. CEF connector sends Common Event Format data which means easy to read. As for administrative effort. You only need to configure the CEF server to listen for syslog from all the linux vms and then send the CEF data to Sentinel.

QUESTION 15
Hotspot Question

You have 100 Azure subscriptions that have enhanced security features in Microsoft Defender for Cloud enabled.
All the subscriptions are inked to a single Azure Active Directory (Azure AD) tenant.

You need to stream the Defender for Cloud logs to a syslog server. The solution must minimize administrative effort.

What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

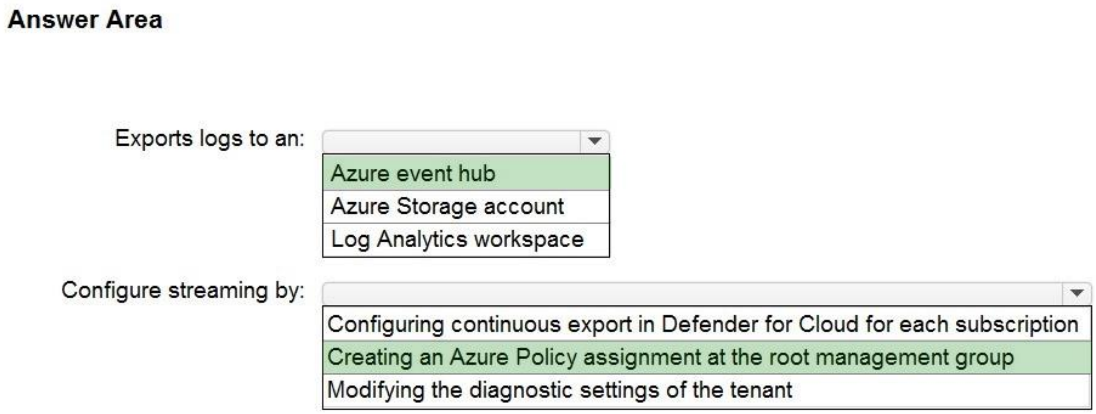


Answer Area

Exports logs to an:
- Azure event hub
- Azure Storage account
- Log Analytics workspace

Configure streaming by:
- Configuring continuous export in Defender for Cloud for each subscription
- Creating an Azure Policy assignment at the root management group
- Modifying the diagnostic settings of the tenant

Answer:



Answer Area

Exports logs to an:
- [✓ Azure event hub]
- Azure Storage account
- Log Analytics workspace

Configure streaming by:
- Configuring continuous export in Defender for Cloud for each subscription
- [✓ Creating an Azure Policy assignment at the root management group]
- Modifying the diagnostic settings of the tenant

Explanation:
Box 1: Azure Event hub
To stream alerts into //Syslog servers// ,and other monitoring solutions, connect Defender for Cloud using continuous export and Azure Event Hubs.

Box 2: Azure Policy
Note:
To stream alerts at the tenant level, use this //Azure policy// and set the scope at the root management group.

Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/export-to-siem#stream-alerts-with-continuous-export
https://docs.microsoft.com/en-us/azure/defender-for-cloud/continuous-export?tabs=azure-policy#configure-continuous-export-at-scale-using-the-supplied-policies

QUESTION 16
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 have Linux virtual machines on Amazon Web Services (AWS).

You deploy Azure Defender and enable auto-provisioning.

You need to monitor the virtual machines by using Azure Defender.

Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc.

Does this meet the goal?

A. Yes
B. No

Answer: A
Explanation:
A machine with Azure Arc-enabled servers becomes an Azure resource and - when you've installed the Log Analytics agent on it - appears in Defender for Cloud with recommendations like your other Azure resources.
Install Log Analytics manually or when you enable auto provisioning of Log Analytics in "Autoprovisioning" tag, auto provisioning is already turned on.

Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc
https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-feature