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

QUESTION 207
Case Study 3 - Litware Inc
Overview

Fabrikam, Inc. is a financial services company.

The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment

Identity Environment

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

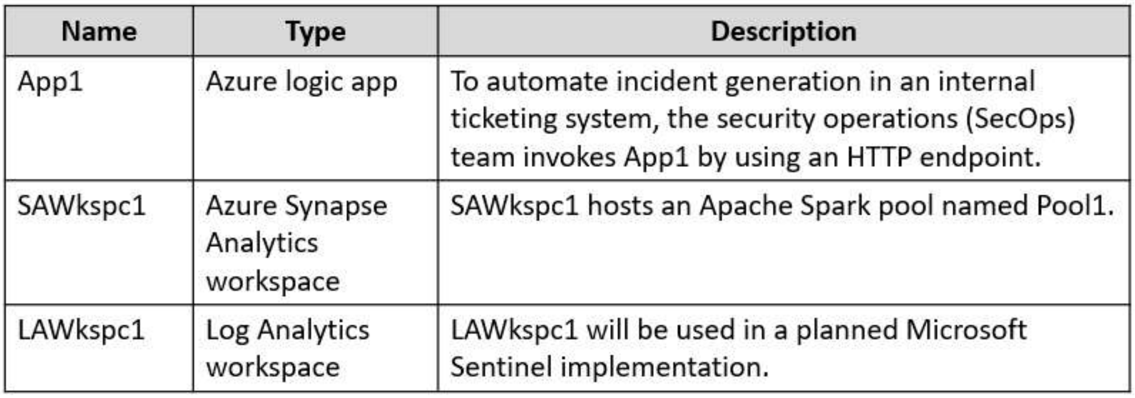
Microsoft 365 Environment

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment

Fabrikam has an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

Planned changes
Fabrikam plans to implement the following services:
- Microsoft Defender for Cloud
- Microsoft Sentinel

Business Requirements
Fabrikam identifies the following business requirements:
- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements
Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:
- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements
Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements
Fabrikam identifies the following Microsoft Defender for Cloud requirements:
- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements
Fabrikam identifies the following Microsoft Sentinel requirements:
- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.

You need to minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts.
What should you review?

A. the status update time
B. the resolution method of the source computer
C. the alert status
D. the certainty of the source computer

Answer: D
Explanation:
https://learn.microsoft.com/en-us/defender-for-identity/understanding-security-alerts#defender-for-identity-and-nnr-network-name-resolution

QUESTION 208
Case Study 3 - Litware Inc
Overview
Fabrikam, Inc. is a financial services company.
The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment

Identity Environment

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

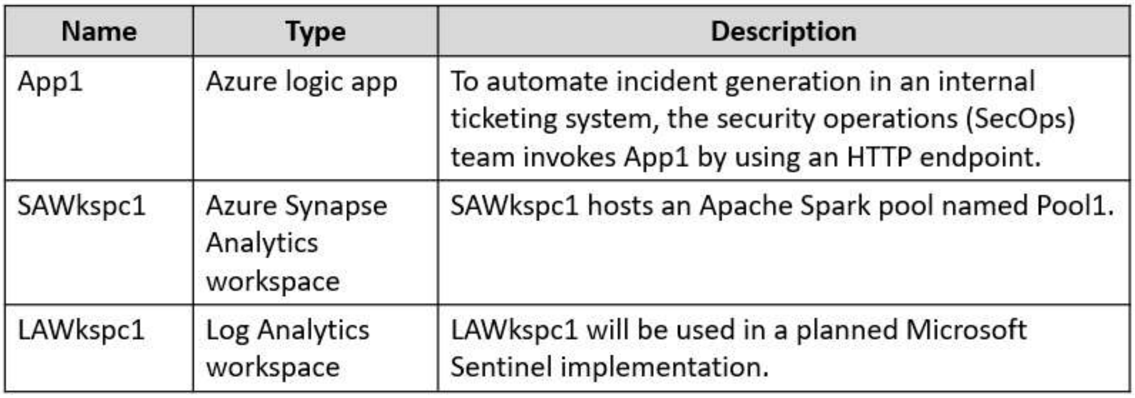
Microsoft 365 Environment

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment

Fabrikam has an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

Planned changes

Fabrikam plans to implement the following services:

- Microsoft Defender for Cloud
- Microsoft Sentinel

Business Requirements

Fabrikam identifies the following business requirements:

- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model

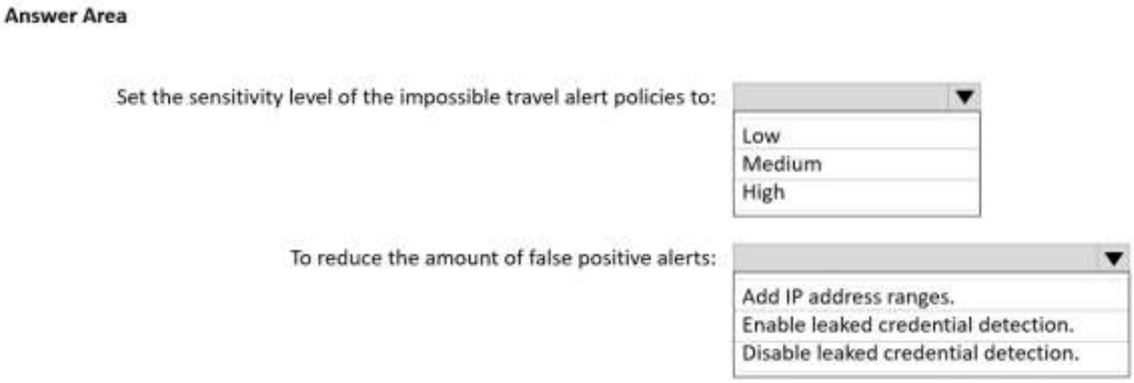
(ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.

Hotspot Question

You need to meet the Microsoft Defender for Cloud Apps requirements.

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

NOTE: Each correct selection is worth one point.

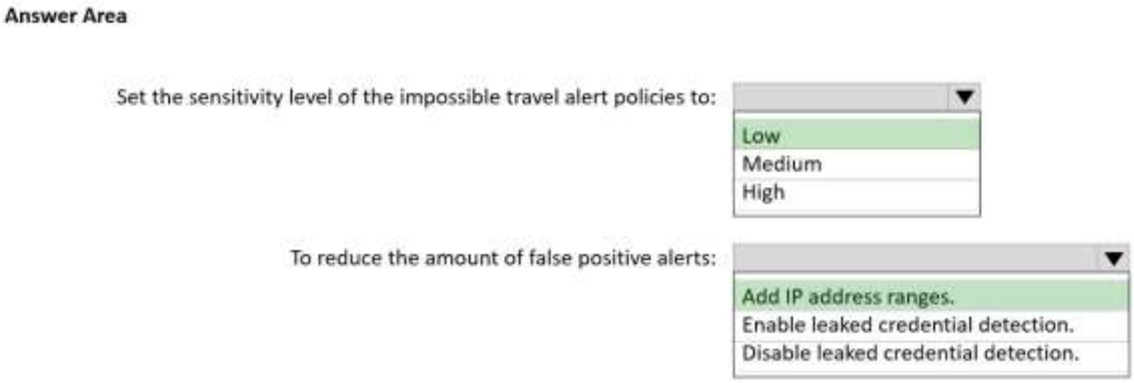


Answer Area

Set the sensitivity level of the impossible travel alert policies to: ▼
Low
Medium
High

To reduce the amount of false positive alerts: ▼
Add IP address ranges.
Enable leaked credential detection.
Disable leaked credential detection.

Answer:



Answer Area

Set the sensitivity level of the impossible travel alert policies to: ▼
[✓ Low]
Medium
High

To reduce the amount of false positive alerts: ▼
[✓ Add IP address ranges.]
Enable leaked credential detection.
Disable leaked credential detection.

QUESTION 209

Case Study 3 - Litware Inc

Overview

Fabrikam, Inc. is a financial services company.

The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment

Identity Environment

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

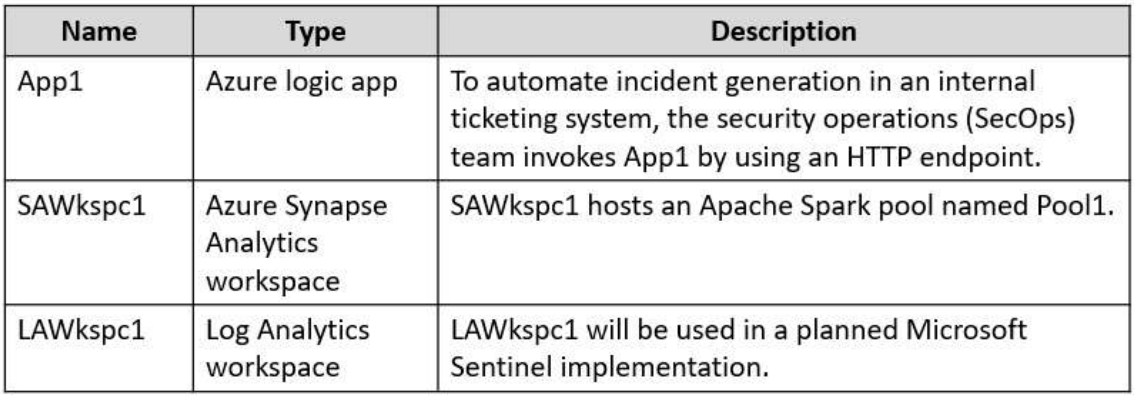
Microsoft 365 Environment

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment

Fabrikam has an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

Planned changes

Fabrikam plans to implement the following services:

- Microsoft Defender for Cloud
- Microsoft Sentinel

Business Requirements

Fabrikam identifies the following business requirements:

- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

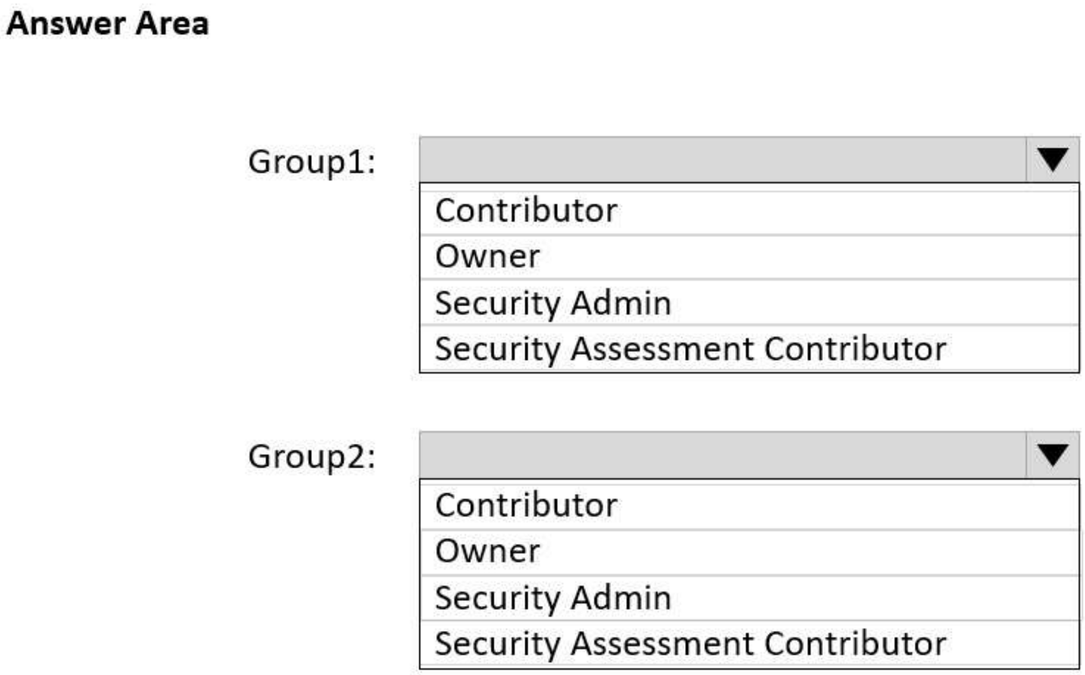
Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.

- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.

Hotspot Question
You need to assign role-based access control (RBAC) roles to Group1 and Group2 to meet the Microsoft Defender for Cloud requirements and the business requirements.
Which role should you assign to each group? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

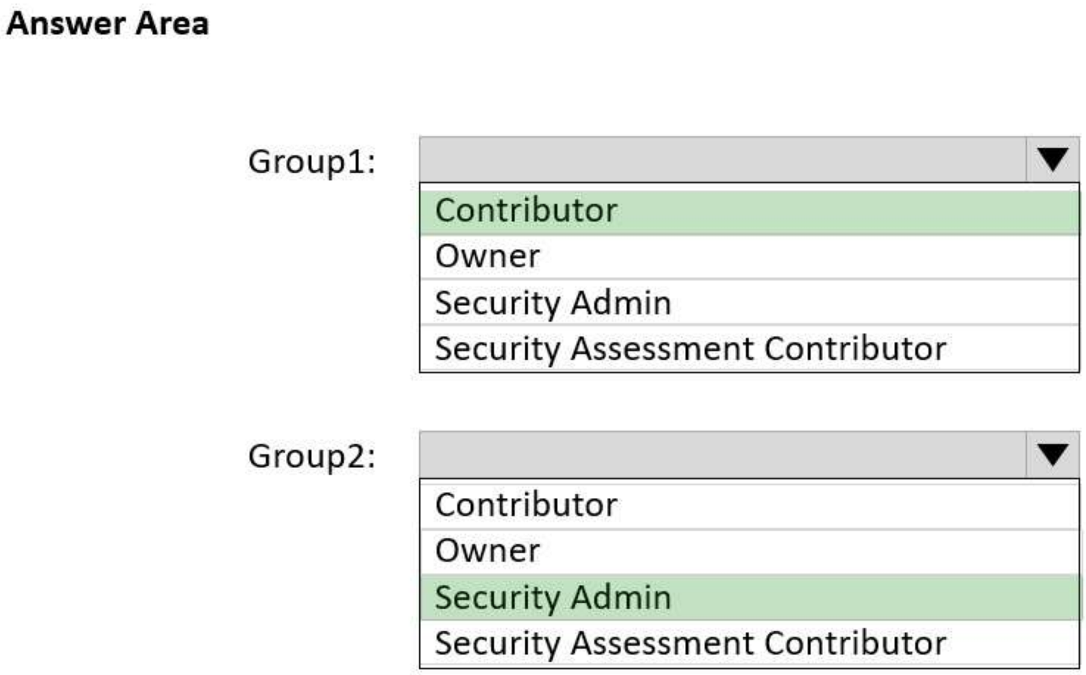


Answer Area

Group1:
- Contributor
- Owner
- Security Admin
- Security Assessment Contributor

Group2:
- Contributor
- Owner
- Security Admin
- Security Assessment Contributor

Answer:



Answer Area

Group1:

- [✓ Contributor]
- Owner
- Security Admin
- Security Assessment Contributor

Group2:

- Contributor
- Owner
- [✓ Security Admin]
- Security Assessment Contributor

QUESTION 210
Case Study 3 - Litware Inc
Overview

Fabrikam, Inc. is a financial services company.

The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment

Identity Environment

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

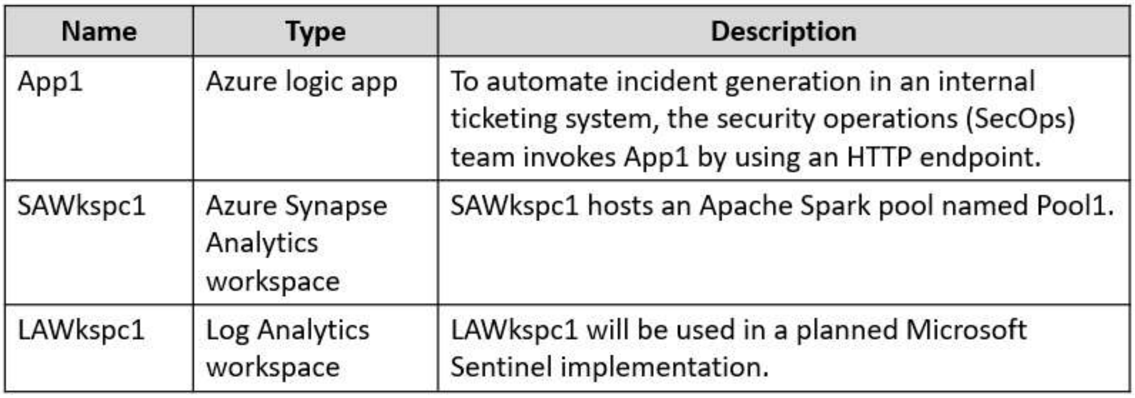
Microsoft 365 Environment

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment

Fabrikam has an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

Planned changes

Fabrikam plans to implement the following services:

- Microsoft Defender for Cloud
- Microsoft Sentinel

Business Requirements

Fabrikam identifies the following business requirements:

- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.

You need to deploy the native cloud connector to Account 1 to meet the Microsoft Defender for Cloud requirements.

What should you do in Account1 first?

A. Create an AWS user for Defender for Cloud.
B. Configure AWS Security Hub.
C. Deploy the AWS Systems Manager (SSM) agent.
D. Create an Access control (IAM) role for Defender for Cloud.

Answer: A

QUESTION 211

Case Study 3 - Litware Inc

Overview

Fabrikam, Inc. is a financial services company.

The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment

Identity Environment

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

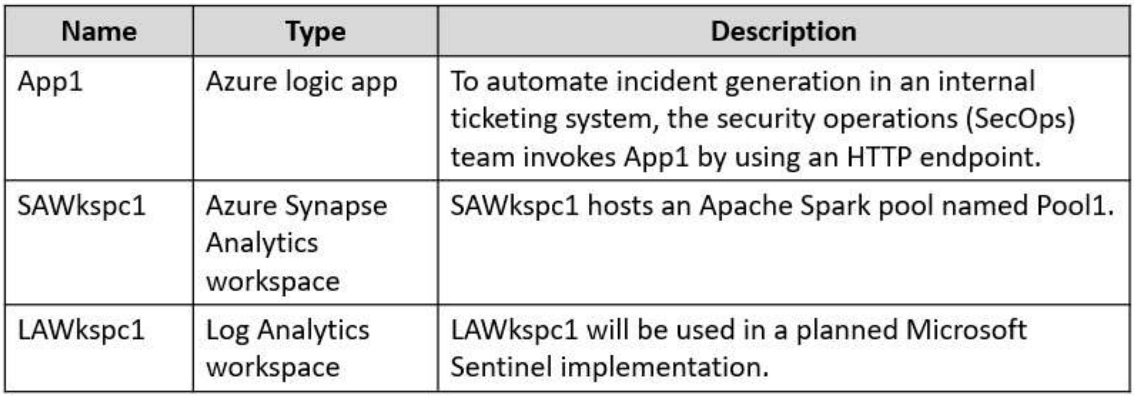
Microsoft 365 Environment

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment

Fabrikam has an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

Planned changes

Fabrikam plans to implement the following services:

- Microsoft Defender for Cloud
- Microsoft Sentinel

Business Requirements

Fabrikam identifies the following business requirements:

- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.

- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

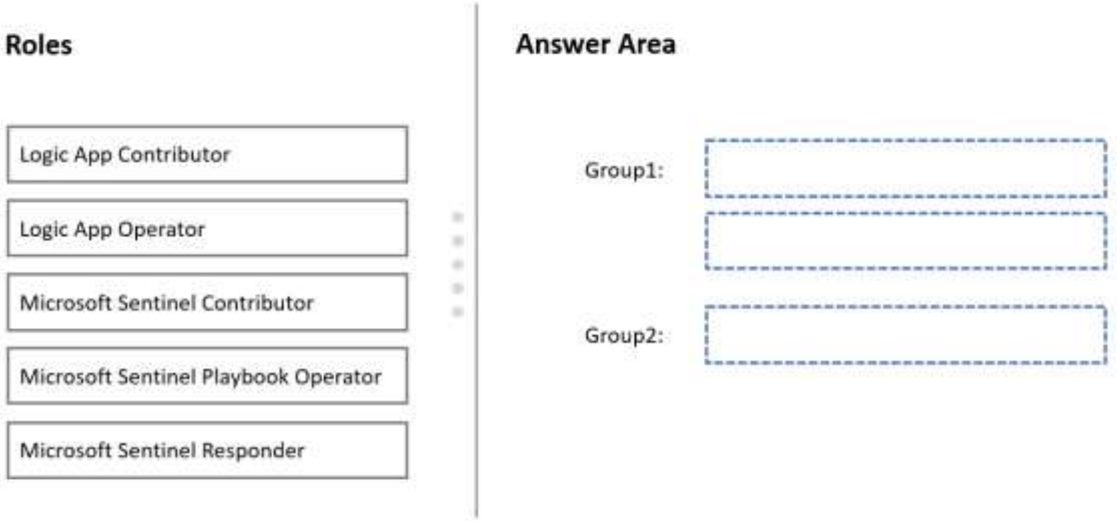
- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.

Drag and Drop Question

You need to assign role-based access control (RBAC) roles to Group1 and Group2 to meet the Microsoft Sentinel requirements and the business requirements.

Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role 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.



Roles

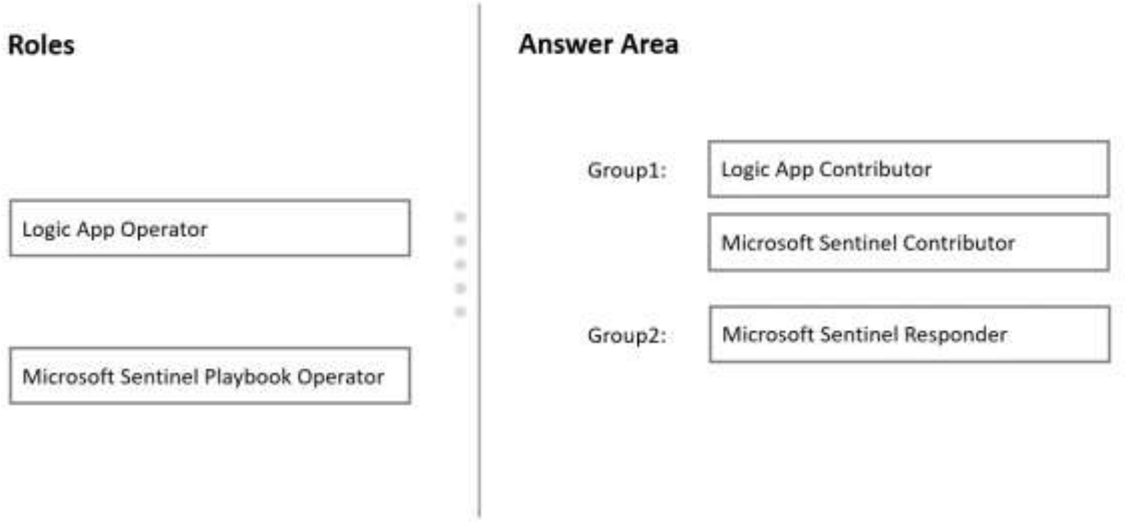
- Logic App Contributor
- Logic App Operator
- Microsoft Sentinel Contributor
- Microsoft Sentinel Playbook Operator
- Microsoft Sentinel Responder

Answer Area

Group1:

Group2:

Answer:



Roles

Logic App Operator

Microsoft Sentinel Playbook Operator

Answer Area

Group1: Logic App Contributor

Microsoft Sentinel Contributor

Group2: Microsoft Sentinel Responder

QUESTION 212
Case Study 3 - Litware Inc
Overview

Fabrikam, Inc. is a financial services company.

The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment

Identity Environment

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

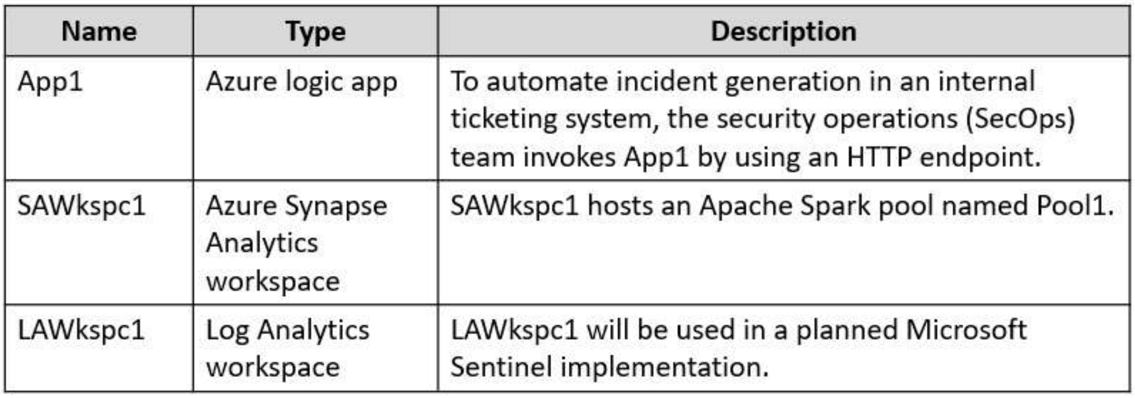
Microsoft 365 Environment

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment

Fabrikam has an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

Planned changes

Fabrikam plans to implement the following services:

- Microsoft Defender for Cloud
- Microsoft Sentinel

Business Requirements

Fabrikam identifies the following business requirements:

- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.

You need to correlate data from the SecurityEvent Log Analytics table to meet the Microsoft Sentinel requirements for using UEBA.

Which Log Analytics table should you use?

A. IdentityInfo
B. AADRiskyUsers
C. SentinelAudit
D. IdentityDirectoryEvents

Answer: A

QUESTION 213

Case Study 3 - Litware Inc

Overview

Fabrikam, Inc. is a financial services company.

The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment

Identity Environment

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

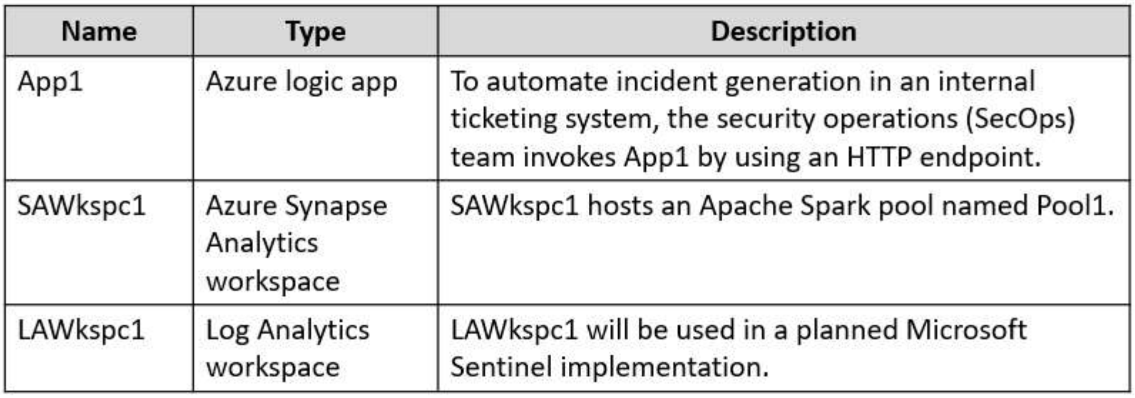
Microsoft 365 Environment

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment

Fabrikam has an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

Planned changes

Fabrikam plans to implement the following services:

- Microsoft Defender for Cloud
- Microsoft Sentinel

Business Requirements

Fabrikam identifies the following business requirements:

- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

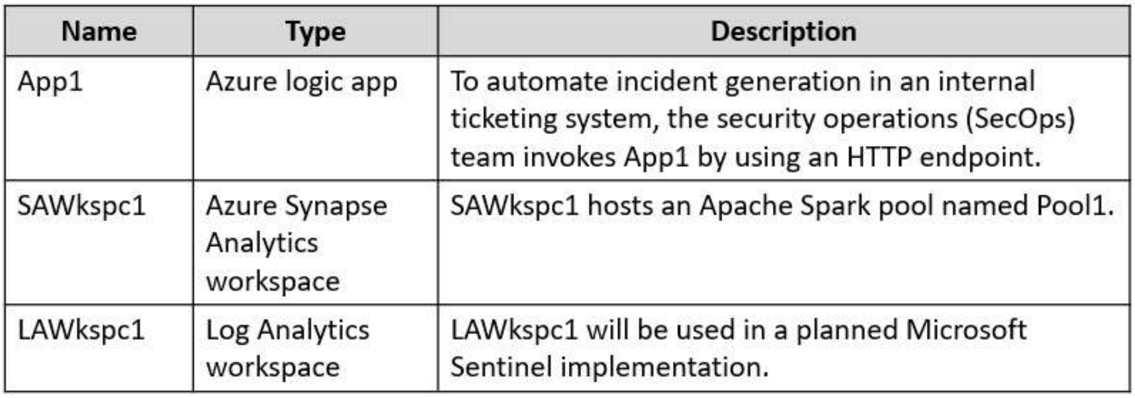
- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.

You need to meet the Microsoft Sentinel requirements for App1.
What should you configure for App1?

A. a trigger
B. a connector
C. authorization
D. an API connection

Answer: A

QUESTION 214
Case Study 3 - Litware Inc
Overview
Fabrikam, Inc. is a financial services company.
The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.
Existing Environment
Identity Environment
The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.
The fabrikam.com forest contains two global groups named Group1 and Group2.
Microsoft 365 Environment
All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.
Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.
Azure Environment
Fabrikam has an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

Planned changes

Fabrikam plans to implement the following services:

- Microsoft Defender for Cloud
- Microsoft Sentinel

Business Requirements

Fabrikam identifies the following business requirements:

- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.

You need to ensure that you can run hunting queries to meet the Microsoft Sentinel requirements.
Which type of workspace should you create?

A. Azure Synapse Analytics
B. Azure Machine Learning
C. Log Analytics
D. Azure Databricks

Answer: B

QUESTION 215
Case Study 3 - Litware Inc

Overview

Fabrikam, Inc. is a financial services company.

The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment

Identity Environment

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

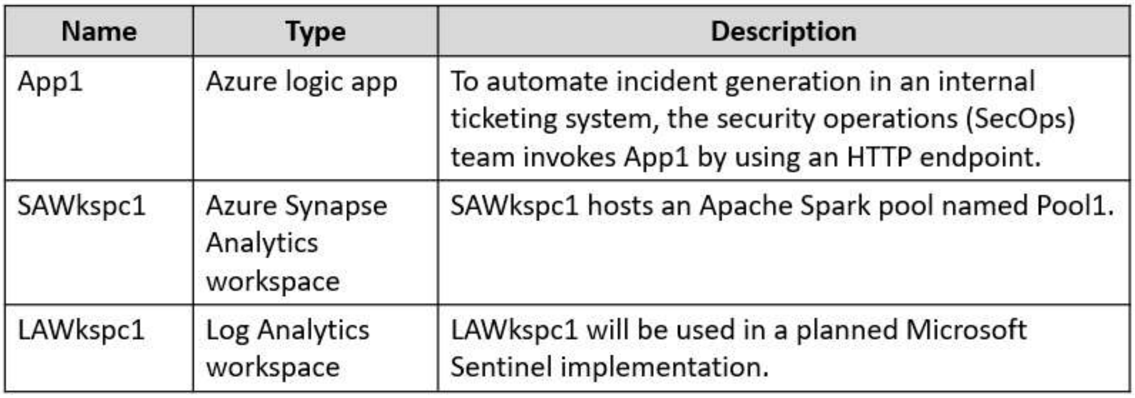
Microsoft 365 Environment

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment

Fabrikam has an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

Planned changes

Fabrikam plans to implement the following services:

- Microsoft Defender for Cloud
- Microsoft Sentinel

Business Requirements

Fabrikam identifies the following business requirements:

- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.

- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.
- Minimize the amount of collected data.

You need to identify which mean time metrics to use to meet the Microsoft Sentinel requirements.
Which workbook should you use?

A. Event Analyzer
B. Investigation Insights
C. Security Operations Efficiency
D. Analytics Efficiency

Answer: C
Explanation:
https://learn.microsoft.com/en-us/azure/sentinel/manage-soc-with-incident-metrics

QUESTION 216
Case Study 3 - Litware Inc
Overview

Fabrikam, Inc. is a financial services company.
The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment
Identity Environment

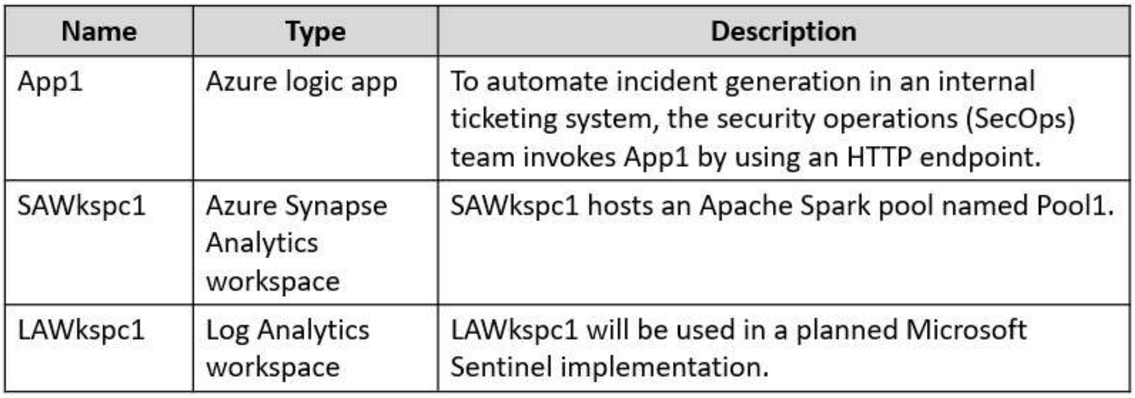
The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.
The fabrikam.com forest contains two global groups named Group1 and Group2.

Microsoft 365 Environment

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.
Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment

Fabrikam has an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

Planned changes

Fabrikam plans to implement the following services:

- Microsoft Defender for Cloud
- Microsoft Sentinel

Business Requirements

Fabrikam identifies the following business requirements:

- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.

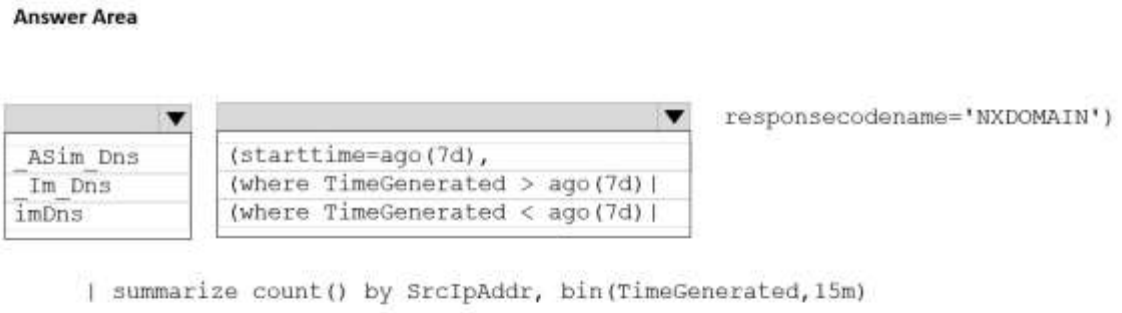
- Minimize the amount of collected data.

Hotspot Question

You need to create a query to investigate DNS-related activity. The solution must meet the Microsoft Sentinel requirements.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

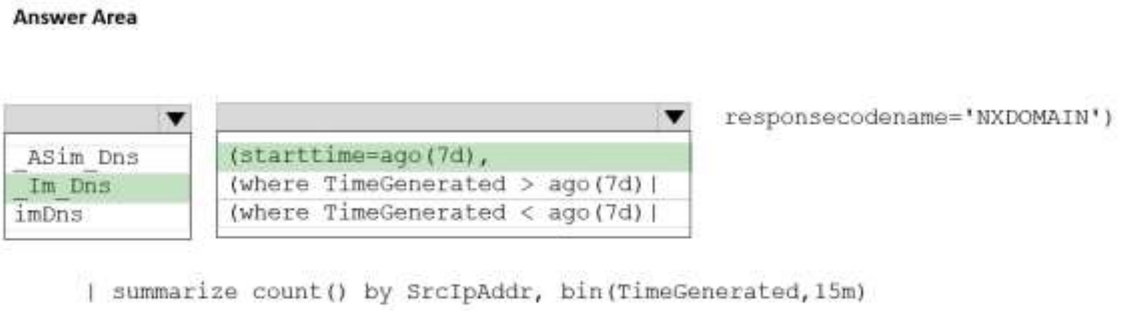
_ASim_Dns
_Im_Dns
imDns

(starttime=ago(7d),
(where TimeGenerated > ago(7d)|
(where TimeGenerated < ago(7d)|

responsecodename='NXDOMAIN')

| summarize count() by SrcIpAddr, bin(TimeGenerated,15m)

Answer:



Answer Area

_ASim_Dns
[✓ _Im_Dns]
imDns

[✓ (starttime=ago(7d),]
(where TimeGenerated > ago(7d)|
(where TimeGenerated < ago(7d)|

responsecodename='NXDOMAIN')

| summarize count() by SrcIpAddr, bin(TimeGenerated,15m)

QUESTION 217

Case Study 3 - Litware Inc

Overview

Fabrikam, Inc. is a financial services company.

The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment

Identity Environment

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

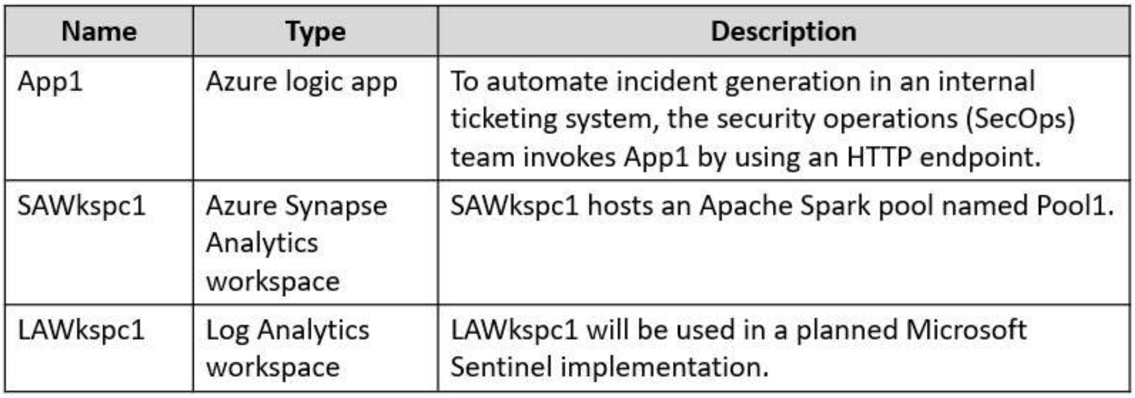
Microsoft 365 Environment

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment

Fabrikam has an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

Planned changes

Fabrikam plans to implement the following services:

- Microsoft Defender for Cloud
- Microsoft Sentinel

Business Requirements

Fabrikam identifies the following business requirements:

- Use the principle of least privilege, whenever possible.
- Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

- Ensure that impossible travel alert policies are based on the previous activities of each user.
- Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

- Ensure that the members of Group2 can modify security policies.
- Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
- Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
- Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

- Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
- From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
- Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
- Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
- Ensure that App1 is available for use in Microsoft Sentinel automation rules.
- Identify the mean time to triage for incidents generated during the last 30 days.
- Identify the mean time to close incidents generated during the last 30 days.
- Ensure that the members of Group1 can create and run playbooks.
- Ensure that the members of Group1 can manage analytics rules.
- Run hunting queries on Pool1 by using Jupyter notebooks.
- Ensure that the members of Group2 can manage incidents.
- Maximize the performance of data queries.

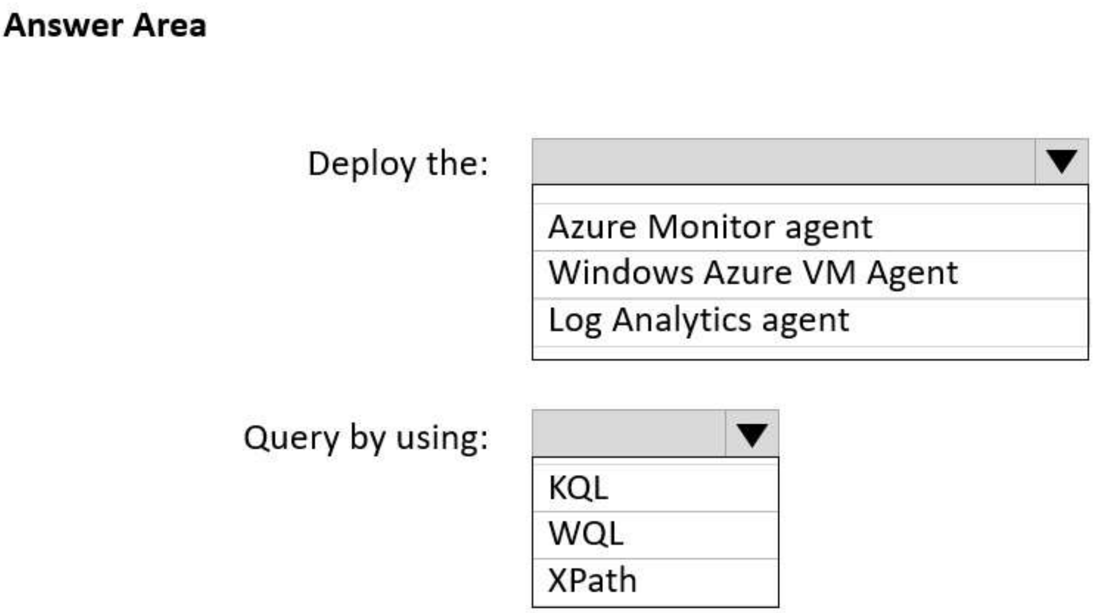
- Minimize the amount of collected data.

Hotspot Question

You need to meet the Microsoft Sentinel requirements for collecting Windows Security event logs.

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

NOTE: Each correct selection is worth one point.



Answer Area

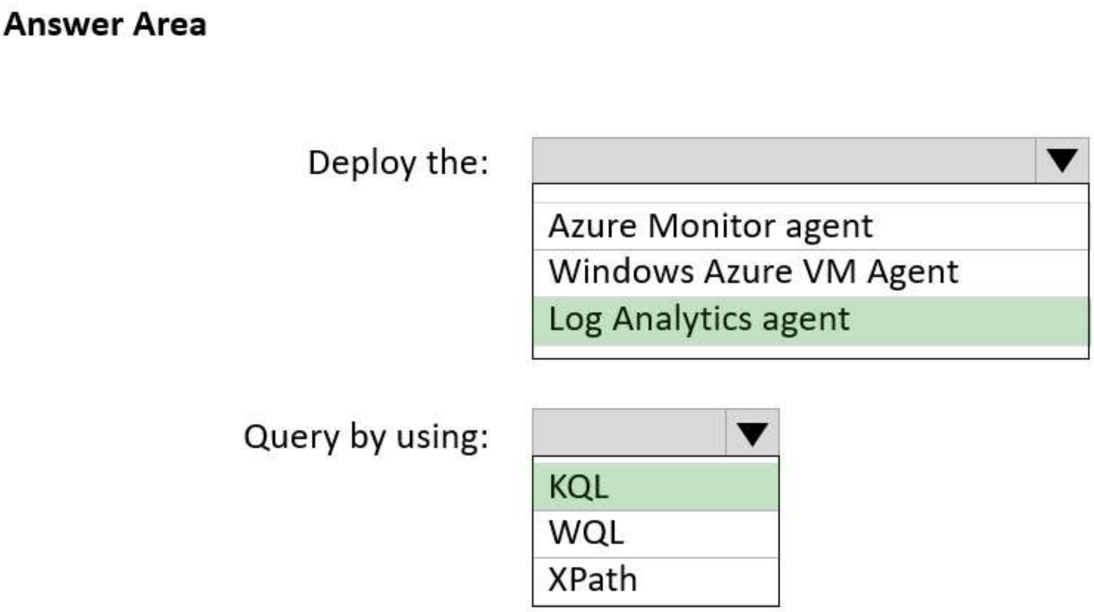
Deploy the:

- Azure Monitor agent
- Windows Azure VM Agent
- Log Analytics agent

Query by using:

- KQL
- WQL
- XPath

Answer:



Answer Area

Deploy the:

- Azure Monitor agent
- Windows Azure VM Agent
- [✓ Log Analytics agent]

Query by using:

- [✓ KQL]
- WQL
- XPath

Explanation:

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent