

SC-200.VCEplus.premium.exam.51q

Number: SC-200
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Website: <https://vceplus.com> - <https://vceplus.co>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

SC-200

Microsoft Security Operations Analyst (beta)



Testlet 1

Case study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

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
```

QUESTION 1 The issue for which team can be resolved by using Microsoft Defender for Endpoint?

- A. executive
- B. sales
- C. marketing

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios>

QUESTION 2 The issue for which team can be resolved by using Microsoft Defender for Office 365?

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



Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide> Testlet 2

Case study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question. **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.

QUESTION 1 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

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview>

QUESTION 2 You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements.

Which policy should you modify?

- A. Activity from suspicious IP addresses
- B. Activity from anonymous IP addresses
- C. Impossible travelID. Risky sign-in

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

Question Set 3**QUESTION 1**
DRAG DROP

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFOLaptop, CEO Laptop, and COOLaptop.

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

NOTE: Each correct selection is worth one point.

Select and Place:

Correct Answer:

Section: [none]

Explanation

Explanation/Reference:

QUESTION 2

You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.

Which anomaly detection policy should you use?

- A. Impossible travel
- B. Activity from anonymous IP addresses
- C. Activity from infrequent country
- D. Malware detection

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

QUESTION 3 You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.

You need to create a data loss prevention (DLP) policy to protect the sensitive documents.

What should you use to detect which documents are sensitive?

- A. SharePoint search
- B. a hunting query in Microsoft 365 Defender
- C. Azure Information Protection
- D. RegEx pattern matching

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en->



[us/azure/information-protection/what-is-information-protection](https://www.vceplus.com/us/azure/information-protection/what-is-information-protection)

QUESTION 4 Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.

You need to identify which Office VBA macros might be affected.

Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

```
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled  
Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode  
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode  
Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```

A.

B.

C.

D.



Correct Answer: BC

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction>

QUESTION 5 Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.
- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Correct Answer: BCE

Section: [none]

Explanation

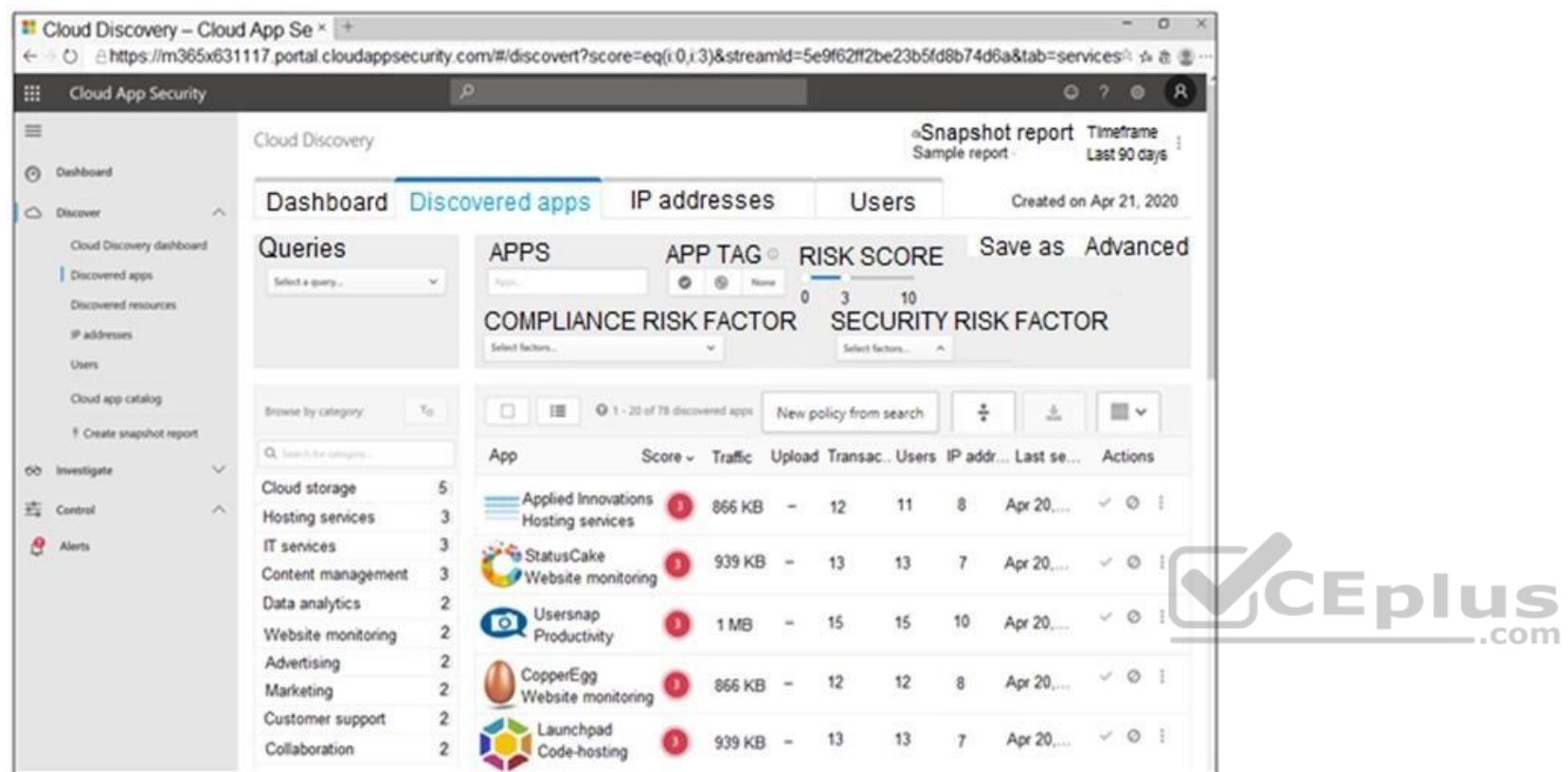
Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts>

QUESTION 6

DRAG DROP

You open the **Cloud App Security** portal as shown in the following exhibit.



App	Score	Traffic	Upload	Transac...	Users	IP addr...	Last se...	Actions
Applied Innovations Hosting services	5	866 KB	-	12	11	8	Apr 20, 2020	
StatusCake Website monitoring	3	939 KB	-	13	13	7	Apr 20, 2020	
Usersnap Productivity	2	1 MB	-	15	15	10	Apr 20, 2020	
CopperEgg Website monitoring	2	866 KB	-	12	12	8	Apr 20, 2020	
Launchpad Code-hosting	2	939 KB	-	13	13	7	Apr 20, 2020	

You need to remediate the risk for the Launchpad app.

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

Select and Place:

Correct Answer:

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery>

QUESTION 7

HOTSPOT

You have a Microsoft 365 E5 subscription.

You plan to perform cross-domain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o365-worldwide>

QUESTION 8

You have the following advanced hunting query in Microsoft 365 Defender.

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.



A. Create a detection rule.

B. Create a suppression rule.

C. Add | order by Timestamp to the query.

D. Replace DeviceProcessEvents with DeviceNetworkEvents.

E. Add DeviceId and ReportId to the output of the query.

Correct Answer: AE

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules>

QUESTION 9 You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Add a tag to the device group.

B. Add the device users to the admin role.

C. Add a tag to the machines.

- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.
- F. Create a new device group that has a rank of 4.

Correct Answer: BDE

Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://www.drware.com/how-to-use-tagging-effectively-in-microsoft-defender-for-endpoint-part-1/>

QUESTION 10

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Entity tags, you add the accounts as Honeytoken accounts.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section: [none]

Explanation



Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 11

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Azure Identity Protection, you configure the sign-in risk policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 12

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>



Testlet 1

Case study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

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
```

QUESTION 1

HOTSPOT

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

What should you recommend for each threat? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

Correct Answer:

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.**

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.**
- Modify the network security groups (NSGs).

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

QUESTION 2

You need to recommend a solution to meet the technical requirements for the Azure virtual machines.

What should you include in the recommendation?

- A. just-in-time (JIT) access
- B. Azure Defender
- C. Azure Firewall
- D. Azure Application Gateway

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/azure-defender>



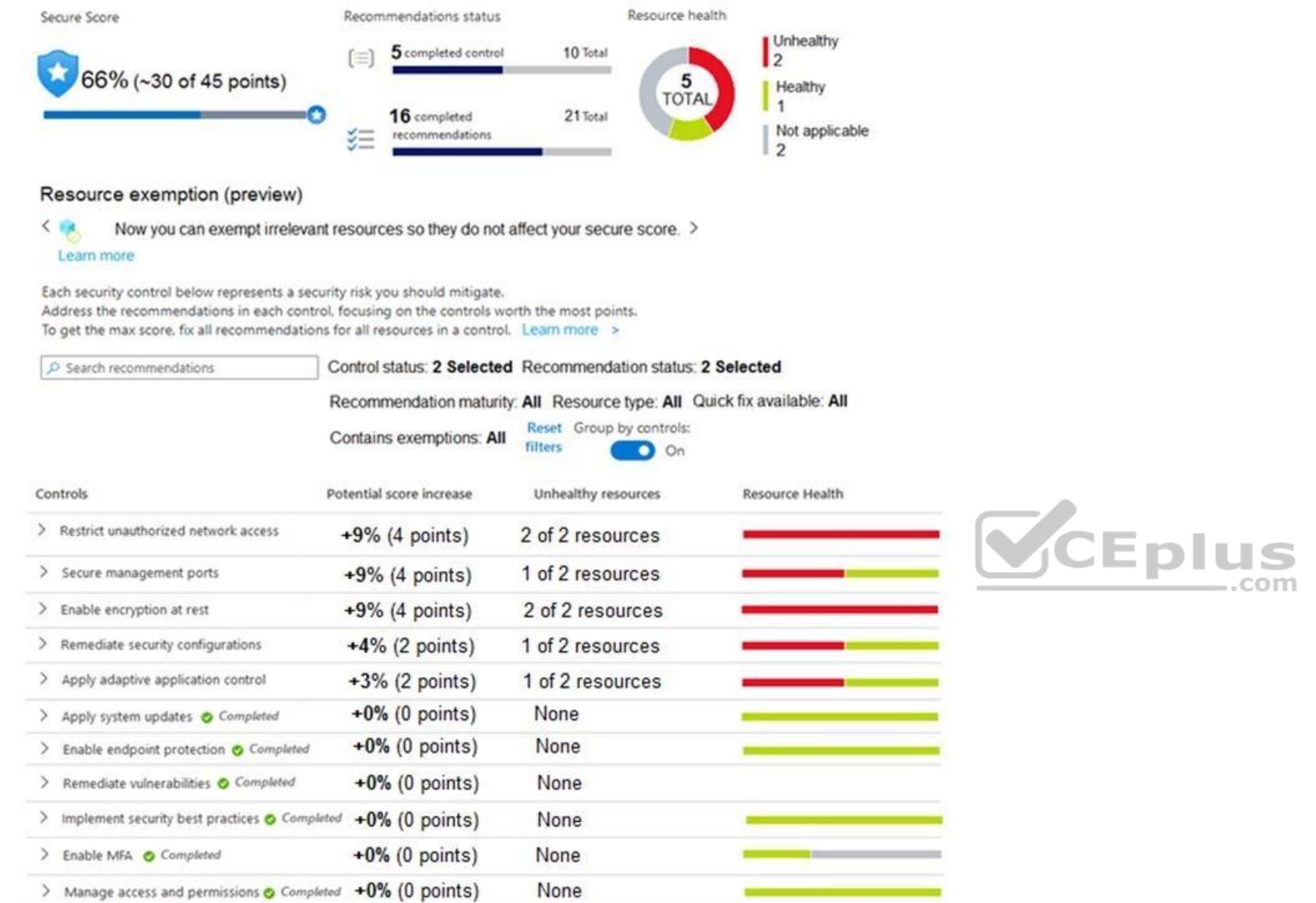
Question Set 2

QUESTION 1

HOTSPOT

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the **Security Center** tab.)



Azure Policy assignments are configured as shown in the Policies exhibit. (Click the **Policies** tab.)

Policy - Compliance

Search (Ctrl+ /) <

[Assign policy](#) [Assign initiative](#) [Refresh](#)

Scope	Microsoft Azure	Type	All definition types	Compliance state	All compliance states	Search
-------	-----------------	------	----------------------	------------------	-----------------------	--------

Overall resource compliance [100%](#)

Resources by compliance state [0](#)

Non-compliant initiatives [0](#)

Non-compliant policies [0](#)

Name [↓ Scope](#) [↓ Compliance](#) [↑ Resource compliance](#)

No assignments to display within the given scope [↑↓ Non-Compliant Resources](#) [↑↓ Non-compliant policies](#)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area


Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input checked="" type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input checked="" type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input checked="" type="radio"/>	<input type="radio"/>

Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833> <https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770>

QUESTION 2

DRAG DROP

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Correct Answer:

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271>

QUESTION 3

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select **Take Action**, and then expand the Prevent future attacks section.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

Explanation:

You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the 'Mitigate the threat' option.

Reference: <https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 4

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

- A. Modify the access control settings for the key vault.
- B. Enable the Key Vault firewall.
- C. Create an application security group.
- D. Modify the access policy for the key vault.

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage>

QUESTION 5

HOTSPOT

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

You need to test LA1 in Security Center.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations
Workflow automation

Correct Answer:

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations
Workflow automation

Section: [none]**Explanation****Explanation/Reference:**Reference: <https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run>**QUESTION 6** You have a Microsoft 365 subscription that uses Azure Defender.

You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

- A. the Security Reader role for the subscription
- B. the Contributor for the subscription
- C. the Contributor role for RG1
- D. the Owner role for RG1

**Correct Answer: C****Section: [none]****Explanation****Explanation/Reference:****QUESTION 7** You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. cp /bin/echo ./asc_alerttest_662jfi039n
- B. ./alerttest testing eicar pipe
- C. cp /bin/echo ./alerttest
- D. ./asc_alerttest_662jfi039n testing eicar pipe

Correct Answer: AD

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux->

QUESTION 8 You create an Azure subscription named sub1.

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

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

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

What should you do?

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

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 9

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.

Select and Place:

Correct Answer:

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation>

QUESTION 10 Your company uses Azure Security Center and

Azure Defender.

The security operations team at the company informs you that it does **NOT** receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Security solutions
- B. Security policy
- C. Pricing & settings
- D. Security alerts
- E. Azure Defender



Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

QUESTION 11

DRAG DROP

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions	Answer Area
Enable Security Health Analytics.	
From Azure Security Center, add cloud connectors.	
Configure the GCP Security Command Center.	 
Create a dedicated service account and a private key.	
Enable the GCP Security Command Center API.	 

Correct Answer:

Actions	Answer Area
Enable Security Health Analytics.	Configure the GCP Security Command Center.
From Azure Security Center, add cloud connectors.	Enable Security Health Analytics.
Configure the GCP Security Command Center.	 
Create a dedicated service account and a private key.	Enable the GCP Security Command Center API.
Enable the GCP Security Command Center API.	 

Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp>

QUESTION 12

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section: [none]

Explanation



Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select **Take Action**, and then expand the Mitigate the threat section.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

Testlet 1

Case study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

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
```

QUESTION 1**HOTSPOT**

You need to create an advanced hunting query to investigate the executive team issue.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]

Explanation

Explanation/Reference:



Testlet 2

Case study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question. **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.

QUESTION 1

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.

Which role should you assign?

- A. Automation Operator
- B. Automation Runbook Operator
- C. Azure Sentinel Contributor
- D. Logic App Contributor

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

QUESTION 2 You need to create the test rule to meet the Azure Sentinel requirements.

What should you do when you create the rule?

- A. From Set rule logic, turn off suppression.
- B. From Analytics rule details, configure the tactics.
- C. From Set rule logic, map the entities.
- D. From Analytics rule details, configure the severity.

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

QUESTION 3

HOTSPOT

You need to create the analytics rule to meet the Azure Sentinel requirements.

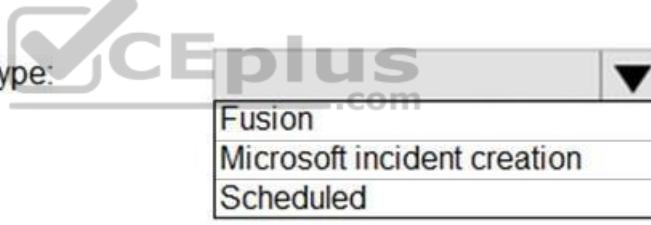
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

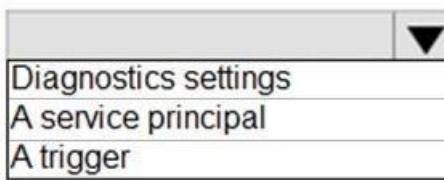
Hot Area:

Answer Area

Create the rule of type:



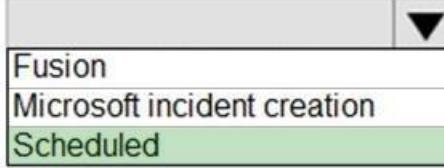
Configure the playbook to include:



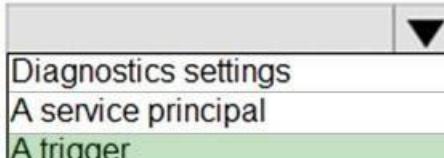
Correct Answer:

Answer Area

Create the rule of type:



Configure the playbook to include:



Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#set-automated-responses-and-create-the-rule>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>



Question Set 3**QUESTION 1**

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart.

What should you include in the query?

- A. extend
- B. bin
- C. makeset
- D. workspace

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries>

QUESTION 2 You are configuring

Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

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

Correct Answer: AB

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

QUESTION 3

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

Section: [none]

Explanation



Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

QUESTION 4

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

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations>

QUESTION 5 You use
Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.



- A. Create a livestream
- B. Add a data connector
- C. Create an analytics rule
- D. Create a hunting query.
- E. Create a bookmark.

Correct Answer: BD

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/livestream>

QUESTION 6
DRAG DROP

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

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

Select and Place:

Correct Answer:

Section: [none]

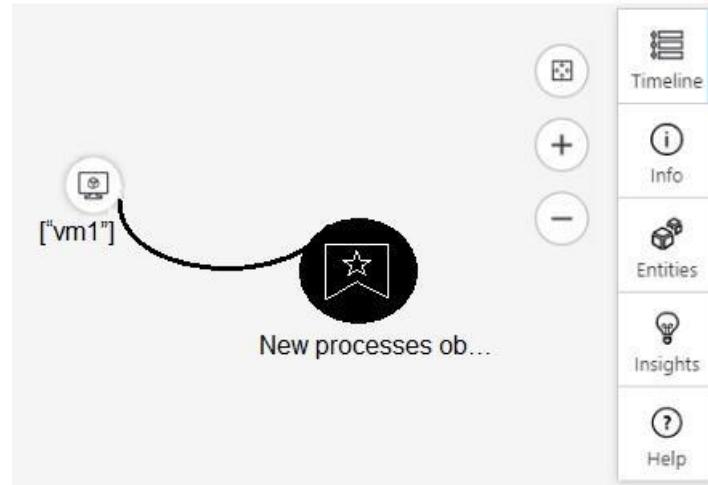
Explanation**Explanation/Reference:**

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog>

QUESTION 7

HOTSPOT

From Azure Sentinel, you open the **Investigation** pane for a high-severity incident as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:**Correct Answer:****Section: [none]****Explanation****Explanation/Reference:**

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive>

QUESTION 8

DRAG DROP

You have an Azure Sentinel deployment.

You need to query for all suspicious credential access activities.

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

Select and Place:**Correct Answer:****Section: [none]****Explanation****Explanation/Reference:**

Reference:

<https://davemccollough.com/2020/11/28/threat-hunting-with-azure-sentinel/>

QUESTION 9 You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.

You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel.

What should you do first?

- A. And a new scheduled query rule.
- B. Add a data connector to Azure Sentinel.
- C. Configure a custom Threat Intelligence connector in Azure Sentinel.
- D. Modify the trigger in the logic app.

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

QUESTION 10 Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.

A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.

You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.

What should you include in the recommendation?

- A. built-in queries
- B. livestream
- C. notebooks
- D. bookmarks

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

QUESTION 11 You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a parameter and modify the trigger.
- B. Add a custom data connector and modify the trigger.
- C. Add a condition and modify the action.
- D. Add a parameter and modify the action.

Correct Answer: D

Section: [none]

Explanation



Explanation/Reference:

Reference:

<https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/>

QUESTION 12 You provision Azure Sentinel for a new Azure subscription.

You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query.

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. user
- B. resource group
- C. IP address
- D. computer

Correct Answer: CD

Section: [none]

Explanation

Explanation/Reference:**QUESTION 13**

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add the Security Events connector to the Azure Sentinel workspace.
- B. Create a query that uses the `workspace` expression and the `union` operator.
- C. Use the `alias` statement.
- D. Create a query that uses the `resource` expression and the `alias` operator.
- E. Add the Azure Sentinel solution to each workspace.

Correct Answer: BE



Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 14 You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal.

From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand>

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

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

- A. There are connectivity issues between the data sources and Log Analytics.
- B. The number of alerts exceeded 10,000 within two minutes.
- C. The rule query takes too long to run and times out.
- D. Permissions to one of the data sources of the rule query were modified.

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

QUESTION 16 Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel.

You need to resolve the issue for the analyst. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

- A. Azure Sentinel Responder
- B. Logic App Contributor
- C. Azure Sentinel Contributor

D. Azure Sentinel Reader

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>



Microsoft Security Operations Analyst

Exam Code: SC-200

Version: July 2021

Join us: <https://www.facebook.com/groups/itknowledge247>

Prepared by MA

Question #1

Topic 1 DRAG DROP -

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFO Laptop, CEO Laptop, and COOL Laptop.

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

Select and Place:

Answers:

Values	Answer Area
project LogonFailures=count()	where DeviceName in ("CFO Laptop", "CEO Laptop", "COOL Laptop")
summarize LogonFailures=count() by DeviceName, LogonType	ActionType == "LogonFailed"
where ActionType == FailureReason	summarize LogonFailures=count() by DeviceName, LogonType and
where DeviceName in ("CFO Laptop", "CEO Laptop", "COOL Laptop")	where ActionType == FailureReason
ActionType == "LogonFailed"	project LogonFailures=count()

OR

| where DeviceName in ("CFO Laptop", "CEO Laptop", "COOL Laptop")

| where ActionType == FailureReason and LogonType == "LogonFailed"

| summarize LogonFailures=count() by DeviceName,

| LogonType | project LogonFailures

Question #2

You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.

Which anomaly detection policy should you use?

- A. Impossible travel
- B. Activity from anonymous IP addresses
- C. Activity from infrequent country
- D. Malware detection

Question #3

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.

You need to create a data loss prevention (DLP) policy to protect the sensitive documents.

What should you use to detect which documents are sensitive?

- A. SharePoint search
- B. a hunting query in Microsoft 365 Defender
- C. Azure Information Protection
- D. RegEx pattern matching

Question #4

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.

You need to identify which Office VBA macros might be affected.

Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A.
`Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

B.
`Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`

C.
`Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`

D.
`Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

Question #5

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.
- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Question #6

DRAG DROP -

You open the Cloud App Security portal as shown in the following exhibit.

The screenshot shows the Cloud Discovery – Cloud App Security portal interface. The left sidebar includes sections for Dashboard, Discover (Cloud Discovery dashboard, Discovered apps, Discovered resources, IP addresses, Users), Cloud app catalog, and Investigate (Cloud storage, Hosting services, IT services, Content management, Data analytics, Website monitoring, Advertising, Marketing, Customer support, Collaboration). The main area is titled 'Cloud Discovery' and has tabs for Dashboard, Discovered apps (selected), IP addresses, and Users. It features a 'Queries' section and a 'RISK SCORE' slider (0 to 10) with two tabs: 'COMPLIANCE RISK FACTOR' and 'SECURITY RISK FACTOR'. Below these are dropdown menus for 'Select factors...' under both tabs. A table lists 78 discovered apps, with the first few rows visible:

App	Score	Traffic	Upload	Transac.	Users	IP addr...	Last se...	Actions
Applied Innovations	5	866 KB	-	12	11	8	Apr 20,...	✓ ○ ⚡
Hosting services	3							
StatusCake	3	939 KB	-	13	13	7	Apr 20,...	✓ ○ ⚡
Website monitoring								
Usersnap	3	1 MB	-	15	15	10	Apr 20,...	✓ ○ ⚡
Productivity								
CopperEgg	3	866 KB	-	12	12	8	Apr 20,...	✓ ○ ⚡
Website monitoring								
Launchpad	3	939 KB	-	13	13	7	Apr 20,...	✓ ○ ⚡
Code-hosting								

You need to remediate the risk for the Launchpad app.

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

Select and Place:

Actions

Tag the app as **Unsanctioned**.

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Select the app.

Tag the app as **Sanctioned**.

Generate a block script.

Answer Area



Answers:

Actions

Tag the app as **Unsanctioned**.

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Select the app.

Tag the app as **Sanctioned**.

Generate a block script.

Answer Area

Select the app.

Tag the app as **Unsanctioned**.

Generate a block script.

Run the script on the source appliance.



Question #7

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You plan to perform cross-domain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

|  (

extend
join
project
union

DeviceFileEvents

|  FileName, SHA256

extend
join
project
union

) on SHA256

|  Timestamp, FileName, SHA256, DeviceName, DeviceId,

extend
join
project
union

NetworkMessageId, SenderFromAddress, RecipientEmailAddress

Answer:

Answer Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

|

|         |
|---------|
| extend  |
| join    |
| project |
| union   |


( 

DeviceFileEvents

|

|         |
|---------|
| extend  |
| join    |
| project |
| union   |


FileName, SHA256

) on SHA256

|

|         |
|---------|
| extend  |
| join    |
| project |
| union   |


Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Question #8

You have the following advanced hunting query in Microsoft 365 Defender.

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a detection rule.
- B. Create a suppression rule.
- C. Add | order by Timestamp to the query.
- D. Replace DeviceProcessEvents with DeviceNetworkEvents.
- E. Add DeviceId and ReportId to the output of the query.

Question #9

You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group.
- B. Add the device users to the admin role.
- C. Add a tag to the machines.
- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.
- F. Create a new device group that has a rank of 4.

Question #10

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Entity tags, you add the accounts as Honeytoken accounts.

Does this meet the goal?

- A. Yes
- B. No

Question #11

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Azure Identity Protection, you configure the sign-in risk policy.

Does this meet the goal?

- A. Yes
- B. No

Question #12

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group.

Does this meet the goal?

- A. Yes
- B. No

Question #13

HOTSPOT -

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Resource exemption (preview)

< Now you can exempt irrelevant resources so they do not affect your secure score. >
[Learn more](#)

Each security control below represents a security risk you should mitigate.
Address the recommendations in each control, focusing on the controls worth the most points.
To get the max score, fix all recommendations for all resources in a control. [Learn more](#) >

Search recommendations		Control status: 2 Selected	Recommendation status: 2 Selected
Recommendation maturity: All Resource type: All Quick fix available: All Contains exemptions: All Reset filters Group by controls: <input checked="" type="checkbox"/> On			
Controls	Potential score increase	Unhealthy resources	Resource Health
> Restrict unauthorized network access	+9% (4 points)	2 of 2 resources	
> Secure management ports	+9% (4 points)	1 of 2 resources	
> Enable encryption at rest	+9% (4 points)	2 of 2 resources	
> Remediate security configurations	+4% (2 points)	1 of 2 resources	
> Apply adaptive application control	+3% (2 points)	1 of 2 resources	
> Apply system updates Completed	+0% (0 points)	None	
> Enable endpoint protection Completed	+0% (0 points)	None	
> Remediate vulnerabilities Completed	+0% (0 points)	None	
> Implement security best practices Completed	+0% (0 points)	None	
> Enable MFA Completed	+0% (0 points)	None	
> Manage access and permissions Completed	+0% (0 points)	None	

Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)

Home > Policy

Policy - Compliance

Overall resource compliance: 100%

Resources by compliance state:

- 0 - Compliant
- 0 - Exempt
- 1 - Non-compliant
- 0 - Conflicting

Non-compliant initiatives: 0 out of 0

Non-compliant policies: 0 out of 0

Name

No assignments to display within the given scope

Scope: Microsoft Azure | Type: All definition types | Compliance state: All compliance states

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input checked="" type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input checked="" type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input checked="" type="radio"/>	<input type="radio"/>

Question #14

DRAG DROP -

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

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

Select and Place:

Actions

Answer Area

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

From Advanced hunting, search for CveId in the DeviceTvmSoftwareInventoryVulnerabilitites table.

Create the remediation request.

Select **Security recommendations**.



Actions

Answer Area

From Device Inventory, search for the CVE.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

Open the Threat Protection report.

Select **Security recommendations**.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

Create the remediation request.



From Advanced hunting, search for CveId in the DeviceTvmSoftwareInventoryVulnerabilitites table.

Create the remediation request.

Select **Security recommendations**.

Question #15

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.

Does this meet the goal?

- A. Yes
- B. No
- You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the "Mitigate the threat™" option.

Question #16

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

- A. Modify the access control settings for the key vault.
- B. Enable the Key Vault firewall.
- C. Create an application security group.
- D. Modify the access policy for the key vault.

Question #17

HOTSPOT -

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

You need to test LA1 in Security Center.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations
Workflow automation

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations
Workflow automation

Question #18

You have a Microsoft 365 subscription that uses Azure Defender.

You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

- A. the Security Reader role for the subscription
- B. the Contributor for the subscription
- C. the Contributor role for RG1
- D. the Owner role for RG1

Question #19

You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. cp /bin/echo ./asc_alerttest_662jfi039n
- B. ./alerttest testing eicar pipe
- C. cp /bin/echo ./alerttest
- D. ./asc_alerttest_662jfi039n testing eicar pipe

Question #20

You create an Azure subscription named sub1.

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

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

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

What should you do?

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

Question #21

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.

Select and Place:

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.	

Actions	Answer Area
Change the alert severity threshold for emails to Medium .	Enable Azure Defender for the subscription.
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.	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.	Run the executable file and specify the appropriate arguments.
Rename the executable file as AlertTest.exe.	

Question #22

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Security solutions
- B. Security policy
- C. Pricing & settings
- D. Security alerts
- E. Azure Defender

Question #23

DRAG DROP -

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

Answer Area

Enable Security Health Analytics.

From Azure Security Center, add cloud connectors.

Configure the GCP Security Command Center.

Create a dedicated service account and a private key.

Enable the GCP Security Command Center API.



Correct

Answer:

Actions	Answer Area
Enable Security Health Analytics.	Configure the GCP Security Command Center.
From Azure Security Center, add cloud connectors.	Enable Security Health Analytics.
Configure the GCP Security Command Center.	 Enable the GCP Security Command Center API. 
Create a dedicated service account and a private key.	Create a dedicated service account and a private key.
Enable the GCP Security Command Center API.	 From Azure Security Center, add cloud connectors. 

Question #24

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

- A. Yes
- B. No

Question #25

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.

Does this meet the goal?

- A. Yes
- B. No

Question #26

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart.

What should you include in the query?

- A. extend.
- B. bin
- C. makeset
- D. workspace

Question #27

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

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

Question #28

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

Question #29

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

Question #30

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a livestream
- B. Add a data connector
- C. Create an analytics rule
- D. Create a hunting query.
- E. Create a bookmark.

Question #31

DRAG DROP -

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

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

Select and Place:

Actions	Answer Area
Deploy an OMS Gateway on the network.	
Set the syslog daemon to forward the events directly to Azure Sentinel.	
Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.	 
Download and install the Log Analytics agent.	
Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.	

Actions	Answer Area
Deploy an OMS Gateway on the network.	Download and install the Log Analytics agent.
Set the syslog daemon to forward the events directly to Azure Sentinel.	Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.
Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.	 
Download and install the Log Analytics agent.	
Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.	

Question #32

HOTSPOT -

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If you hover over the virtual machine named vm1, you can view [answer choice].

the inbound network security group (NSG) rules
the last five Windows security log events
the open ports on the host
the running processes

If you select [answer choice], you can navigate to the bookmarks related to the incident.

Entities
Info
Insights
Timeline

Question #33

DRAG DROP

You have an Azure Sentinel deployment.

You need to query for all suspicious credential access activities.

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

Select and Place:

Actions

From Azure Sentinel, select **Hunting**.

Select **Run All Queries**.

Select **New Query**.

Filter by tactics.

From Azure Sentinel, select **Notebooks**.

Answer Area



[Reveal Solution](#)

Actions

From Azure Sentinel, select **Hunting**.

Select **Run All Queries**.

Select **New Query**.

Filter by tactics.

From Azure Sentinel, select **Notebooks**.

Answer Area

From Azure Sentinel, select **Hunting**.

Filter by tactics.

Select **Run All Queries**.



Question #34

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.

You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel.

What should you do first?

- A. And a new scheduled query rule.
- B. Add a data connector to Azure Sentinel.
- C. Configure a custom Threat Intelligence connector in Azure Sentinel.
- D. Modify the trigger in the logic app.

Question #35

Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.

A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.

You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.

What should you include in the recommendation?

- A. built-in queries
- B. livestream
- C. notebooks
- D. bookmarks

Question #36

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a parameter and modify the trigger.
- B. Add a custom data connector and modify the trigger.
- C. Add a condition and modify the action.
- D. Add a parameter and modify the action.

Question #37

You provision Azure Sentinel for a new Azure subscription.

You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query.

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. user
- B. resource group
- C. IP address
- D. computer

Question #38

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add the Security Events connector to the Azure Sentinel workspace.
- B. Create a query that uses the workspace expression and the union operator.

- C. Use the alias statement.
- D. Create a query that uses the resource expression and the alias operator.
- E. Add the Azure Sentinel solution to each workspace.

Question #39

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal.

From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Question #40

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

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

- A. There are connectivity issues between the data sources and Log Analytics.
- B. The number of alerts exceeded 10,000 within two minutes.
- C. The rule query takes too long to run and times out.
- D. Permissions to one of the data sources of the rule query were modified.

Question #41

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel.

You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?

- A. Azure Sentinel Responder
- B. Logic App Contributor
- C. Azure Sentinel Contributor
- D. Azure Sentinel Reader

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All-information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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
```

Question #42

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

- A. executive
- B. sales
- C. marketing

Question #43

The issue for which team can be resolved by using Microsoft Defender for Office 365?

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

Question #44

HOTSPOT -

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam. What should you recommend for each threat? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Internal threat:

Add resource locks to the key vault.
Modify the access policy settings for the key vault.
Modify the role-based access control (RBAC) settings for the key vault.

External threat:

Implement Azure Firewall.
Modify the Key Vault firewall settings.
Modify the network security groups (NSGs).

- **The answer should be:**

- Internal Threat: Modify the access policy settings for the key vault External Threat.
- Implement Azure Firewall.

Question #45

You need to recommend a solution to meet the technical requirements for the Azure virtual machines.

What should you include in the recommendation?

- A. just-in-time (JIT) access
- B. Azure Defender
- C. Azure Firewall
- D. Azure Application Gateway

Question #46

HOTSPOT -

You need to create an advanced hunting query to investigate the executive team issue.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)
```

```
| summarize activityCount =
```

```
    ActionType, AccountDisplayName
```

```
| where activityCount > 5
```

avg()
count()
sum()

```
by FolderPath, FileName,
```

- **The answer should be:**

- DeviceFileEvents
- Count()

Case study 2

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

Question #47

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

Question #48

You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements.

Which policy should you modify?

- A. Activity from suspicious IP addresses
- B. Activity from anonymous IP addresses
- C. Impossible travel
- D. Risky sign-in

Question #49

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.
Which role should you assign?

- A. Automation Operator
- B. Automation Runbook Operator
- C. Azure Sentinel Contributor
- D. Logic App Contributor

Question #50

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

- A. From Set rule logic, turn off suppression.
- B. From Analytics rule details, configure the tactics.
- C. From Set rule logic, map the entities.
- D. From Analytics rule details, configure the severity.

Question #51

HOTSPOT -

You need to create the analytics rule to meet the Azure Sentinel requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:

Diagnostics settings
A service principal
A trigger

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:

Diagnostics settings
A service principal
A trigger

Question #52

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Azure Defender
- B. Security policy
- C. Pricing & settings (correct)**
- D. Security alerts
- E. Security solutions

Question #53

You create an Azure subscription named sub1.

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

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

You need to collect security event logs from the Azure virtual machines that report to workspace1

What should you do?

- A. In workspace 1, create a workbook.
- B. From Security Center, enable data collection (correct)
- C. From Security Center, create a workflow automation.
- D. In sub1, register a provider.

Question #54

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 resource level
- B- at the subscription level (correct)
- C- at the workspace level

Question #55

You are responsible for responding to Azure Defender for Key vault alerts.

During an investigation of an alert, you discover unauthorized attempts to access a key vault from a for exit node.

What should you configure to mitigate the threat?

- A. the access policy settings of the key vault
- B. role - based access control (RBAC) for the key vault
- C. Azure Active Directory (Azure AD) permissions
- D. Key Vault firewalls and virtual networks. (might be)

Question #56

You receive a security bulletin about a potential attack that uses an image file.

You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.

Which indicator type should you use?

- A. a URL / domain indicator that has Action set to **Alert and block**
- B. a certificate indicator that has Action set to **Alert and block**
- C. a URL / domain indicator that has Action set to **Alert only**
- D. a file hash indicator that has Action set to **Alert and block** (correct)

Question #57

our company deploys the following services:

- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365

You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Defender for Endpoint.

The solution must use the principle of least privilege.

Which two roles should you assign to the analyst? Each correct answer presents part of the solution

NOTE: Each correct selection is worth one point.

- A. the Security Reader role in Azure Active Directory (Azure AD) (correct)
- B. the Security Administrator role in Azure Active Directory (Azure AD)
- C. the Active remediation actions role in Microsoft Defender for Endpoint (correct)
- D. the Compliance Data Administrator in Azure Active Directory (Azure AD)

Question #58

You implement Safe Attachments policies in Microsoft Defender for Office 365.

Users report that email messages containing attachments take longer than expected to be received. You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for messages that contain malware must be blocked.

What should you configure in the Safe Attachments policies?

- A. Replace
- B. Monitor and Enable redirect
- C. Dynamic Delivery (correct)
- D. Block and Enable redirect

Question #59

You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled. You need to ensure that the Fusion rule can generate alerts.

What should you do?

- A. Add a hunting bookmark.
- B. Create a new machine learning analytics rule.
- C. Disable, and then enable the rule
- D. Add data connectors. (correct)

Question #60

You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region.

You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.

What should you do first?

- A. Create a data connector in Azure Sentinel.
- B. Add Azure Sentinel to a workspace (correct)
- C. Deploy Azure Data Catalog to the West US Azure region.
- D. Modify the workspace settings of the existing Azure Sentinel deployment.

Question #61

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. (correct)
- B. Permissions to the data sources of the rule query were modified.
- C. The target workspace was deleted
- D. There are connectivity issues between the data sources and Log Analytics (correct)

Question #62

You have a third - party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-in events in near real time.

What should you do to route events to the SIEM solution?

- A. Configure the Diagnostics settings in Azure AD to archive to a storage account.
- B. Create an Azure Sentinel workspace that has a Security Events connector.
- C. Configure the Diagnostics settings in Azure AD to stream to an event hub. (correct)
- D. Create an Azure Sentinel workspace that has an Azure Active Directory connector.

Question #63

After you answer a question in this section, you will NOT be able to return to it. As a result, ti

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for Identity portal, you need to configure several accounts for attacker Solution: You add each account as a Sensitive account.

Does this meet the goal?

- A. Yes
- B. No (correct)

Question#64

You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.

You need to hide the alerts automatically in Security Center.

Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Pricing & settings.
- B. Security policy.
- C. Azure Resource as the entity type and specify the ID.
- D. Suppression rules, and then select Create new suppression rule. (here)
- E. IP as the entity type and specify the IP address.

Question#65

You are informed of an increase in malicious email being received by users.

You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.

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:

```
let Malicious Emails=
|where MalwareFilterVerdict == Malware "
| project TimeEmail = Timestamp , Subject , Sender FromAddress , AccountName =
| tostring ( split ( RecipientEmailAddress , " @ " ) [ 0 ] );
Malicious Emails
```

the answers:

- **Email Events**
- **IdentityLogonEvents**
- **take 20**

Question#66

Your company has a single office in Istanbul and a Microsoft 365 subscription.

The company plans to use conditional access policies to enforce multi - factor authentication (MFA).

You need to enforce MFA for all users who work remotely.

What should you include in the solution?

- A- a sign - in user policy
- B- a user risk policy
- C- a named location (correct)
- D- a fraud alert.

Question#67

You are configuring Microsoft Cloud App Security.

You have a custom threat detection policy based on the IP address ranges of your company's United States - based offices. You receive many alerts related to impossible travel and sign - ins from risky IP addresses.

You determine that 99 % of the alerts are legitimate sign - ins from your corporate offices.

You need to prevent alerts for legitimate sign - ins from known locations.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add the IP addresses to the other address range category and add a tag (might)
- B. Create an activity policy that has an exclusion for the IP addresses.
- C. Increase the sensitivity level of the impossible travel anomaly detection policy
- D. Override automatic data enrichment (might)

Question#68

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a custom data connector and modify the trigger
- B. Add an alert and modify the action.
- C. Add a condition and modify the action
- D. Add a parameter and modify the trigger. (might be)

Question#69

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Sentinel workspace named workspace 1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.

You need to use the Fusion rule to detect multi - staged attacks that include suspicious sign - ins to contoso.com followed by anomalous Microsoft Office 365 activity.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a Microsoft Cloud App Security connector. (correct)
- B. Create a Microsoft incident creation rule based on Azure Security Center.
- C. Create an Azure AD Identity Protection Connector (correct)
- D. Create a custom rule based on the office connector templates.

Question#70

deploy Azure Sentinel.

You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.

Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area:

- Microsoft Teams: Office 365
- Linux virtual machines in Azure: syslog

Question#71

You need to complete the query for failed sign - ins to meet the technical requirements.

Where can you find the column name to complete the where clause?

- A- Security alerts in Azure Security Center
- B- the query window of the Log Analytics workspace (correct)
- C- Activity log in Azure
- D- Azure Advisor

Question#72

You need to remediate active attacks to meet the technical requirements.

What should you include in the solution?

- A- Azure Functions
- B- Azure Automation runbooks
- C- Azure Logic Apps (might)
- D- Azure Sentinel livestreams

Question#73

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 Dependency agent
- B- Install the Connected Machine agent
- C- Configure the Hybrid Runbook Worker role
- D- Install the Log Analytics agent (correct)

Question#74

A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks. The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center. You need to ensure that the security administrator receives email alerts for all the activities.

What should you configure in the Security Center settings?

- A- The integration settings for Threat detection
- B- the Azure Defender plans
- C- a cloud connector
- D- the severity level of email notifications (correct)

Question#75

You plan to create a data loss prevention (DLP) policy that will be used with insider risk management. The severity level is set to Low. You need to ensure that insider risk management alerts are generated from rules in the DLP policies.

What should you do?

- A- Set the severity level to Medium
- B- Scope the policy to only specified users
- C- Set the scope of the policy to the Data leaks template
- D- Set the severity level to High (might)

Question#76

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 alert, select the alert, select Take Action, and then expand the Prevent future attacks section.
- B- From Security alerts, select the alert, select Take Action, and then expand the Mitigate the threat section. (correct)
- C- From Regulatory compliance, download the report
- D- From Recommendations, download the CSV report

Question#77

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(correct)

Question#78

You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.

Which two configurations should you modify?

Each correct answer presents part of the solution.

NOTE Each correct selection is worth one point.

- A- the Onboarding settings from Device management in Microsoft Defender Security Center
- B- the Cloud Discovery settings in Cloud App Security (correct)
- C- Advanced features from Settings in Microsoft Defender Security Center (correct)
- D- Cloud App Security anomaly detection policies

Question#79

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

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

Answer Area:

- F. Log Analytics workspace to use:
- G. Windows security events to collect:

Question#80

You have an Azure Storage account that will be accessed by multiple Azure Functions apps during the development of an application. You need to hide Azure Defender alerts for the storage account.

Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area:

- Entity type: (IP address, Azure Resource, Host, User account) Azure resource
- Field: (name, resource ID, Address, Command line) Resource ID

Question#81

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 Dependency agent
- B- Install the Connected Machine agent
- C- Configure the Hybrid Runbook Worker role
- D- Install the Log Analytics agent (correct)

Question#82

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:

- J. Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:(0,1,2,3) (1)
- K. Query element required to correlate data between tenants:(extend, project, workspace) (workspace

Question#83

You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Center.

How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area:

```
“resources”: [  
    {  
        “type”: “..... /automations”,  
        “apiVersion”: 2019-01-01-preview”,  
        “name”: [parameters(‘name’)],  
        “location”: “[parameters(‘location’)]”,  
        “properties”: {  
  
            “Actions”: [  
                {  
                    “actionType”: “LogicApp”,  
                    “logicAppResourceId”: “[resourceId(‘ITEM2/workflows’,  
                        parameters(‘appName’))]”,  
                    “uri”: “[listCallbackURL(resourceId(parameters(‘subscriptionId’),  
                        Parameters(‘resourceGroupName’), ‘..... /workflows/triggers’,  
                        Parameters(‘appName’), ‘manual’, ‘2019-05-01’).value]”  
                }  
            ]  
        }  
    }  
]
```

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You need to configure the continuous export of high-severity alerts to enable their retrieval from a third-party security information and event management (SIEM) solution.

To which service should you export the alerts?

A. Azure Data Lake

B. Azure Event Hubs

C. Azure Cosmos DB

D. Azure Event Grid

SC-200_51q_June_2021_By_DrunkMonk

Number: 000-000

Passing Score: 800

Time Limit: 120 min

File Version: 1.0



Exam SC-200 Compiled by DrunkMonk June 2021

Sections

1. Multiple Choice
2. Hotspot
3. Drag & Drop
4. Case Study - Contoso Ltd
5. Case Study - Litware Inc.

Exam A

QUESTION 1 DRAG DROP

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFO Laptop, CEO Laptop, and COOL Laptop.

How should you complete the query?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Select and Place:

Values

Answer Area

```
| project LogonFailures=count()
```

```
| summarize LogonFailures=count()  
by DeviceName, LogonType
```

```
| where ActionType ==  
FailureReason
```

```
| where DeviceName in ("CFO Laptop,  
"CEO Laptop", "COOL Laptop")
```

```
ActionType == "LogonFailed"
```

Answer:

Values

Answer Area

```
| summarize LogonFailures=count()  
by DeviceName, LogonType
```

```
| where DeviceName in ("CFOlaptop,  
"CEOlaptop", "COOLaptop")
```

```
| where ActionType ==  
FailureReason
```

```
ActionType == "LogonFailed"
```

```
| project LogonFailures=count()
```

Section: Drag & Drop

Explanation/Reference:

Explanation:

Reference:

QUESTION 2

You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.

Which anomaly detection policy should you use?

- A. Impossible travel
- B. Activity from anonymous IP addresses
- C. Activity from infrequent country
- D. Malware detection

Answer: C

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

QUESTION 3

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.

You need to create a data loss prevention (DLP) policy to protect the sensitive documents.

What should you use to detect which documents are sensitive?

- A. SharePoint search
- B. a hunting query in Microsoft 365 Defender
- C. Azure Information Protection
- D. RegEx pattern matching

Answer: C

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection>

QUESTION 4

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.

You need to identify which Office VBA macros might be affected.

Which two commands can you run to achieve the goal?

Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
- B. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
- C. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
- D. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled

Answer: BC

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction>

QUESTION 5

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.
- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Answer: BCE

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts>

QUESTION 6**DRAG DROP**

You open the Cloud App Security portal as shown in the following exhibit:

The screenshot shows the Cloud Discovery - Cloud App Security interface. The left sidebar includes sections for Dashboard, Discover (Cloud Discovery dashboard, Discovered apps, Discovered resources, IP addresses, Users), Investigate (Cloud storage, Hosting services, IT services, Content management, Data analytics, Website monitoring, Advertising, Marketing, Customer support, Collaboration), Control, and Alerts. The main area has tabs for Dashboard, Discovered apps (selected), IP addresses, and Users. It features a 'Queries' section with a dropdown for 'Select a query...' and a 'Browse by category' section with a search bar for 'Search for category...'. Below these are two filter sections: 'APPS' (with dropdowns for 'Apps', 'APP TAG' set to 'None', and a risk score slider from 0 to 10) and 'COMPLIANCE RISK FACTOR' and 'SECURITY RISK FACTOR' (both with dropdowns for 'Select factors...'). A table lists 78 discovered apps, including columns for App, Score (dropdown), Traffic, Upload, Transactions, Users, IP address, Last seen, and Action. The table shows several entries, with the first five being: Applied Innovations (Hosting services), StatusCake (Website monitoring), Usersnap (Productivity), CopperEgg (Website monitoring), and Launchpad (Code-hosting). Each entry includes a red circular icon with a number (e.g., 1, 2, 3, 4, 5) and a small icon representing the app type.

You need to remediate the risk for the Launchpad app.

Which four actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place

Actions

Answer Area

Tag the app as **Unsanctioned**.

Run the script on the source appliance.

Run the script in Azure Cloud Shell.



Select the app.



Tag the app as **Sanctioned**.

Generate a block script.

Answer:

Actions

Answer Area

Select the app.

Run the script in Azure Cloud Shell.



Tag the app as **Unsanctioned**.

Tag the app as **Sanctioned**.



Generate a block script.

Run the script on the source appliance.

Section: Drag & Drop

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery>

QUESTION 7

HOTSPOT

You have a Microsoft 365 E5 subscription.

You plan to perform cross-domain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment.

How should you complete the query?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

|  (

extend
join
project
union

DeviceFileEvents

|  FileName, SHA256

extend
join
project
union

) on SHA256

|  Timestamp, FileName, SHA256, DeviceName, DeviceId,

extend
join
project
union

NetworkMessageId, SenderFromAddress, RecipientEmailAddress

Answer:

Answer Area

```
EmailAttachmentInfo
```

```
| where SenderFromAddress =~ "MaliciousSender@example.com"
```

```
| where isnotempty (SHA256)
```

```
| ▾ (
```

extend
join
project
union

```
DeviceFileEvents
```

```
| ▾ File Name, SHA256
```

extend
join
project
union

```
) on SHA256
```

```
| ▾ ▾ Timestamp, File Name, SHA256, DeviceName, DeviceId,
```

extend
join
project
union

```
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Section: Hotspot

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o365-worldwide>

QUESTION 8

You have the following advanced hunting query in Microsoft 365 Defender:

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

Which two actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a detection rule.
- B. Create a suppression rule.
- C. Add | order by Timestamp to the query.
- D. Replace DeviceProcessEvents with DeviceNetworkEvents.
- E. Add DeviceId and ReportId to the output of the query.

Answer: AE

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules>

QUESTION 9

You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices.

Which three actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group.
- B. Add the device users to the admin role.
- C. Add a tag to the machines.
- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.

F. Create a new device group that has a rank of 4.

Answer: ADE

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://www.drware.com/how-to-use-tagging-effectively-in-microsoft-defender-for-endpoint-part-1/>

QUESTION 10

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Entity tags, you add the accounts as Honeytoken accounts.

Does this meet the goal?

A. Yes

B. No

Answer: A

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 11

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Azure Identity Protection, you configure the sign-in risk policy.

Does this meet the goal?

A. Yes

B. No

Answer: B

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 12

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 13

HOTSPOT

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Exhibit\Security Center tab.)

Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Exhibit\Policies tab.)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input checked="" type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input checked="" type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input checked="" type="radio"/>	<input type="radio"/>

Section: Hotspot

Explanation/Reference:

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833>

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770>

QUESTION 14

DRAG DROP

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your

environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

Which three actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

Answer Area

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

From Advanced hunting, search for CveId in the DeviceTvmSoftwareInventoryVulnerabilitites table.

Create the remediation request.

Select **Security recommendations**.



Answer:

Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Advanced hunting, search for CveId in the
DeviceTvmSoftwareInventoryVulnerabilitites
table.

Answer Area

From Threat & Vulnerability Manager
Weaknesses, and search for the C

Select **Security recommendations**

Create the remediation request.

Section: Drag & Drop

Explanation/Reference:

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271>

QUESTION 15

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 16

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue.

The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

- A. Modify the access control settings for the key vault.
- B. Enable the Key Vault firewall.
- C. Create an application security group.
- D. Modify the access policy for the key vault.

Answer: B

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage>

QUESTION 17

HOTSPOT

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

You need to test LA1 in Security Center.

What should you do?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Set the LA1 trigger to:

- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

- ▼
- Recommendations
- Workflow automation

Answer:

Answer Area

Set the LA1 trigger to:

- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

- ▼
- Recommendations
- Workflow automation

Section: Hotspot

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run>

QUESTION 18

You have a Microsoft 365 subscription that uses Azure Defender.

You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender.

The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

- A. the Security Reader role for the subscription
- B. the Contributor for the subscription
- C. the Contributor role for RG1
- D. the Owner role for RG1

Answer: C

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

QUESTION 19

You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. cp /bin/echo ./asc_alerttest_662jfi039n
- B. ./alerttest testing eicar pipe
- C. cp /bin/echo ./alerttest
- D. ./asc_alerttest_662jfi039n testing eicar pipe

Answer: AD

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux>

QUESTION 20

You create an Azure subscription named sub1.

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

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

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

What should you do?

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

Answer: A

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

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

QUESTION 21

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.

Select and Place:

Actions

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.

Answer Area



Answer:

Actions

Change the alert severity threshold for emails to **Medium**.

Answer Area

Enable Azure Defender for the subscription.

Change the alert severity threshold for emails to **Low**.



Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N

Rename the executable file as AlertTest.exe.

Run the executable file and specify the appropriate arguments.

Section: Drag & Drop

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation>

QUESTION 22

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does **NOT** receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Security solutions
- B. Security policy
- C. Pricing & settings
- D. Security alerts
- E. Azure Defender

Answer: C

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

QUESTION 23

DRAG DROP

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions?

To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

Enable Security Health Analytics.

From Azure Security Center, add cloud connectors.

Configure the GCP Security Command Center.

Create a dedicated service account and a private key.

Enable the GCP Security Command Center API.

Answer Area



Answer:

Actions

Answer Area

Configure the GCP Security Command Center.

Enable Security Health Analytics.



Enable the GCP Security Command Center API.

Create a dedicated service account and a private key.

From Azure Security Center, add cloud connectors.

Section: Drag & Drop

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp>

QUESTION 24

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Section: Multiple Choice

Explanation/Reference:**Explanation:****Reference:**

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 25

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Section: Multiple Choice

Explanation/Reference:**Explanation:****Reference:**

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 26

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart.

What should you include in the query?

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

Answer: B

Section: Multiple Choice

Explanation/Reference:**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries>

QUESTION 27

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

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

Answer: AB

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

QUESTION 28

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

Answer: A

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

QUESTION 29

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

Answer: C

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations>

QUESTION 30

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated.

Which two actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a livestream
- B. Add a data connector
- C. Create an analytics rule
- D. Create a hunting query.
- E. Create a bookmark.

Answer: BD

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/livestream>

QUESTION 31

DRAG DROP

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

Which three actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Answer Area



Answer:

Actions

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Answer Area

Download and install the Log Analytics agent.



Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Section: Drag & Drop

Explanation/Reference:**Explanation:****Reference:**

<https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog>

QUESTION 32**HOTSPOT**

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit:



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If you hover over the virtual machine named vm1, you can view [answer choice].

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select [answer choice], you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

Answer:

Answer Area

If you hover over the virtual machine named vm1, you can view [answer choice].

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select [answer choice], you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

Section: Hotspot

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive>

QUESTION 33

DRAG DROP

You have an Azure Sentinel deployment.

You need to query for all suspicious credential access activities.

Which three actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions	Answer Area
From Azure Sentinel, select Hunting .	
Select Run All Queries .	
Select New Query .	
Filter by tactics.	
From Azure Sentinel, select Notebooks .	

Answer:

Actions	Answer Area
	From Azure Sentinel, select Hunting .
Select New Query .	 Filter by tactics.
	Select Run All Queries .
From Azure Sentinel, select Notebooks .	

Section: Drag & Drop

Explanation/Reference:

Explanation:

Reference:

<https://davemccollough.com/2020/11/28/threat-hunting-with-azure-sentinel/>

QUESTION 34

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.

You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel.

What should you do first?

- A. Add a new scheduled query rule.
- B. Add a data connector to Azure Sentinel.
- C. Configure a custom Threat Intelligence connector in Azure Sentinel.
- D. Modify the trigger in the logic app.

Answer: B

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

QUESTION 35

Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.

A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.

You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.

What should you include in the recommendation?

- A. built-in queries
- B. livestream
- C. notebooks
- D. bookmarks

Answer: C

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

QUESTION 36

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a parameter and modify the trigger.
- B. Add a custom data connector and modify the trigger.
- C. Add a condition and modify the action.
- D. Add a parameter and modify the action.

Answer: D

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/>

QUESTION 37

You provision Azure Sentinel for a new Azure subscription.

You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query:

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated)
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents?

Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. user
- B. resource group
- C. IP address
- D. computer

Answer: CD

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

QUESTION 38

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add the Security Events connector to the Azure Sentinel workspace.
- B. Create a query that uses the workspace expression and the union operator.
- C. Use the alias statement.
- D. Create a query that uses the resource expression and the alias operator.
- E. Add the Azure Sentinel solution to each workspace.

Answer: BE

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

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

QUESTION 39

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal.

From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Answer: D

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand>

QUESTION 40

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

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

- A. There are connectivity issues between the data sources and Log Analytics.
- B. The number of alerts exceeded 10,000 within two minutes.
- C. The rule query takes too long to run and times out.
- D. Permissions to one of the data sources of the rule query were modified.

Answer: D

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

QUESTION 41

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel.

You need to resolve the issue for the analyst. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

- A. Azure Sentinel Responder
- B. Logic App Contributor
- C. Azure Sentinel Contributor
- D. Azure Sentinel Reader

Answer: A

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

QUESTION 42

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

Case Study Title (Case Study):

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the

case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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
```

- A. executive
- B. sales
- C. marketing

Answer: B

Section: Case Study - Contoso Ltd

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios>

QUESTION 43

The issue for which team can be resolved by using Microsoft Defender for Office 365?

Case Study Title (Case Study):

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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
```

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

Answer: B

Section: Case Study - Contoso Ltd

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide>

QUESTION 44

You need to implement the Azure Information Protection requirements.

What should you configure first?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

- 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

Section: Case Study - Litware Inc.

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview>

QUESTION 45

You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements.

Which policy should you modify?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

- A. Activity from suspicious IP addresses
- B. Activity from anonymous IP addresses
- C. Impossible travel
- D. Risky sign-in

Answer: C

Section: Case Study - Litware Inc.

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

QUESTION 46

HOTSPOT

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

Answer:

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.**

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.**
- Modify the network security groups (NSGs).

Section: Case Study - Contoso Ltd

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

QUESTION 47

You need to recommend a solution to meet the technical requirements for the Azure virtual machines.

What should you include in the recommendation?

Case Study Title (Case Study):

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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
```

- A. just-in-time (JIT) access
- B. Azure Defender
- C. Azure Firewall
- D. Azure Application Gateway

Answer: B

Section: Case Study - Contoso Ltd

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/azure-defender>

QUESTION 48**HOTSPOT**

You need to create an advanced hunting query to investigate the executive team issue. How should you complete the query? To answer, select the appropriate options in the answer area.

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)  
  
| summarize activityCount =  
  by FolderPath, FileName,  
  ActionType, AccountDisplayName  
  
| where activityCount > 5
```

avg()
count()
sum()

Answer:

Answer Area

CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)  
  
| summarize activityCount =  
  by FolderPath, FileName,  
  ActionType, AccountDisplayName  
  
| where activityCount > 5
```

avg()
count()
sum()

Section: Case Study - Contoso Ltd

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

QUESTION 49

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.

Which role should you assign?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

- A. Automation Operator
- B. Automation Runbook Operator
- C. Azure Sentinel Contributor
- D. Logic App Contributor

Answer: C

Section: Case Study - Litware Inc.

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

QUESTION 50

You need to create the test rule to meet the Azure Sentinel requirements.

What should you do when you create the rule?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

- A. From Set rule logic, turn off suppression.
- B. From Analytics rule details, configure the tactics.
- C. From Set rule logic, map the entities.
- D. From Analytics rule details, configure the severity.

Answer: C

Section: Case Study - Litware Inc.

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

QUESTION 51

HOTSPOT

You need to create the analytics rule to meet the Azure Sentinel requirements.

What should you do?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:

Diagnostics settings
A service principal
A trigger

Answer:

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:

Diagnostics settings
A service principal
A trigger

Section: Case Study - Litware Inc.

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#set-automated-responses-and-create-the-rule>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Exam SC-200: Microsoft Security Operations Analyst

Skills measured

- The content of this exam will be updated on July 23, 2021.
- Mitigate threats using Microsoft 365 Defender (25-30%)
- Mitigate threats using Azure Defender (25-30%)
- Mitigate threats using Azure Sentinel (40-45%)

Exam SC-200 Compiled by DrunkMonk July 2021



Sections

1. Multiple Choice
2. Hotspot
3. Drag & Drop
4. Case Study - Contoso Ltd
5. Case Study - Litware Inc.

Exam A

QUESTION 1 DRAG DROP

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFO Laptop, CEO Laptop, and COOL Laptop.

How should you complete the query?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Select and Place:

Select and Place:

Values

Answer Area

```
| project LogonFailures=count()
```

```
| summarize LogonFailures=count()  
by DeviceName, LogonType
```

```
| where ActionType ==  
FailureReason
```

```
| where DeviceName in ("CFO Laptop,  
"CEO Laptop", "COOL Laptop")
```

```
ActionType == "LogonFailed"
```

and

Correct Answer:

Values

Answer Area

```
| where DeviceName in ("CFO Laptop",
"CEO Laptop", "COO Laptop")

| where ActionType == "LogonFailed"

| summarize LogonFailures=count() and
by DeviceName, LogonType

| where ActionType ==
FailureReason

| project LogonFailures=count()
```

Section: Drag & Drop Explanation

Explanation/Reference: Explanation:

Reference:

<https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/General%20queries/Failed%20Logon%20Attempt.txt>

QUESTION 2

You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.

Which anomaly detection policy should you use?

- A. Impossible travel
- B. Activity from anonymous IP addresses
- C. Activity from infrequent country

D. Malware detection

Correct Answer: C

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

QUESTION 3

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.

You need to create a data loss prevention (DLP) policy to protect the sensitive documents.

What should you use to detect which documents are sensitive?

- A. SharePoint search
- B. a hunting query in Microsoft 365 Defender
- C. Azure Information Protection
- D. RegEx pattern matching

Correct Answer: C

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection>

QUESTION 4

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.

You need to identify which Office VBA macros might be affected.

Which two commands can you run to achieve the goal?

Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`
- B. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`
- C. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`
- D. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

Correct Answer: BC

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction>

QUESTION 5

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.

- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Correct Answer: BCE

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts>

QUESTION 6

DRAG DROP

You open the Cloud App Security portal as shown in the following exhibit:

The screenshot shows the Cloud Discovery - Cloud App Security interface. The left sidebar has sections for Dashboard, Discover (Cloud Discovery dashboard, Discovered apps, Discovered resources, IP addresses, Users), Investigate (Cloud app catalog, Create snapshot report), Control (Investigate, Control, Alerts), and Alerts. The main area has tabs for Dashboard, Discovered apps (selected), IP addresses, and Users. It includes a 'Snapshot report' section with a timeframe of 'Last 90 days'. Below is a search bar and a table titled 'APPS' with columns: APP TAG, RISK SCORE, COMPLIANCE RISK FACTOR, SECURITY RISK FACTOR, App, Score, Traffic, Upload Transac., Users, IP addr..., Last se..., Actions. The table lists several apps with their respective details.

	APP TAG	RISK SCORE	COMPLIANCE RISK FACTOR	SECURITY RISK FACTOR	App	Score	Traffic	Upload Transac.	Users	IP addr...	Last se...	Actions
Applied Innovations	1	866 KB	-	12	11	8	Apr 20, 2020	✓	○	⋮		
Hosting services	1	939 KB	-	13	13	7	Apr 20, 2020	✓	○	⋮		
StatusCake	1	939 KB	-	13	13	7	Apr 20, 2020	✓	○	⋮		
Website monitoring	1	1 MB	-	15	15	10	Apr 20, 2020	✓	○	⋮		
Usersnap	1	866 KB	-	12	12	8	Apr 20, 2020	✓	○	⋮		
Productivity	1	939 KB	-	13	13	7	Apr 20, 2020	✓	○	⋮		
CopperEgg	1	866 KB	-	12	12	8	Apr 20, 2020	✓	○	⋮		
Website monitoring	1	939 KB	-	13	13	7	Apr 20, 2020	✓	○	⋮		
Launchpad	1	939 KB	-	13	13	7	Apr 20, 2020	✓	○	⋮		
Code-hosting	1	939 KB	-	13	13	7	Apr 20, 2020	✓	○	⋮		

You need to remediate the risk for the Launchpad app.

Which four actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place

Select and Place:

Actions

Tag the app as **Unsanctioned**.

Run the script on the source appliance.

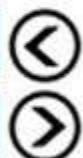
Run the script in Azure Cloud Shell.

Select the app.

Tag the app as **Sanctioned**.

Generate a block script.

Answer Area



Correct Answer:

Actions

Answer Area

Select the app.

Tag the app as **Unsanctioned**.

Generate a block script.

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Tag the app as **Sanctioned**.

Section: Drag & Drop
Explanation

Explanation/Reference:
Explanation:

Reference:
<https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery>

QUESTION 7
HOTSPOT

You have a Microsoft 365 E5 subscription.

You plan to perform cross-domain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment.

How should you complete the query?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Hot Area:

Answer Area

```
EmailAttachmentInfo
```

```
| where SenderFromAddress =~ "MaliciousSender@example.com"
```

```
| where isnotempty (SHA256)
```

```
|  
|  
| extend  
| join  
| project  
| union  
(
```

```
DeviceFileEvents
```

```
|  
|  
| File Name, SHA256  
| extend  
| join  
| project  
| union
```

```
) on SHA256
```

```
|  
|  
| Timestamp, FileName, SHA256, DeviceName, DeviceId,  
| extend  
| join  
| project  
| union
```

```
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Correct Answer:

Answer Area

```
EmailAttachmentInfo
```

```
| where SenderFromAddress =~ "MaliciousSender@example.com"
```

```
| where isnotempty (SHA256)
```

```
|  
|  
| extend  
| join  
| project  
| union  
|  
(
```

```
DeviceFileEvents
```

```
|  
|  
| File Name, SHA256  
| extend  
| join  
| project  
| union  
|  
)
```

```
on SHA256
```

```
|  
|  
| Timestamp, FileName, SHA256, DeviceName, DeviceId,  
| extend  
| join  
| project  
| union  
|  
)
```

```
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Section: Hotspot

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o365-worldwide>

QUESTION 8

You have the following advanced hunting query in Microsoft 365 Defender:

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

Which two actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a detection rule.
- B. Create a suppression rule.
- C. Add | order by Timestamp to the query.
- D. Replace DeviceProcessEvents with DeviceNetworkEvents.
- E. Add DeviceId and ReportId to the output of the query.

Correct Answer: AE

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules>

QUESTION 9

You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices.

Which three actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group.
- B. Add the device users to the admin role.
- C. Add a tag to the machines.
- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.
- F. Create a new device group that has a rank of 4.

Correct Answer: ACD

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access>

QUESTION 10

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Entity tags, you add the accounts as Honeytoken accounts.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 11

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Azure Identity Protection, you configure the sign-in risk policy.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 12

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 Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: Multiple Choice

Explanation:

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 13

HOTSPOT

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Exhibit\Security Center tab.)
Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Exhibit\Policies tab.)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Security Center (exhibit):

Secure Score



66% (~30 of 45 points)

Recommendations status



5 completed control

10 Total



16 completed recommendations

21 Total

Resource health



Unhealthy

2

Healthy

1

Not applicable

2

Resource exemption (preview)



Now you can exempt irrelevant resources so they do not affect your secure score.

[Learn more](#)

Each security control below represents a security risk you should mitigate.

Address the recommendations in each control, focusing on the controls worth the most points.

To get the max score, fix all recommendations for all resources in a control. [Learn more](#)

Control status: **2 Selected** Recommendation status: **2 Selected**

Recommendation maturity: All Resource type: All Quick fix available: All

Contains exemptions: All

[Reset](#)Group by controls:
 filters

On

Controls	Potential score increase	Unhealthy resources	Resource Health
> Restrict unauthorized network access	+9% (4 points)	2 of 2 resources	<div style="width: 100%; background-color: red;"></div>
> Secure management ports	+9% (4 points)	1 of 2 resources	<div style="width: 50%; background-color: red;"></div> <div style="width: 50%; background-color: limegreen;"></div>
> Enable encryption at rest	+9% (4 points)	2 of 2 resources	<div style="width: 100%; background-color: red;"></div>
> Remediate security configurations	+4% (2 points)	1 of 2 resources	<div style="width: 50%; background-color: red;"></div> <div style="width: 50%; background-color: limegreen;"></div>
> Apply adaptive application control	+3% (2 points)	1 of 2 resources	<div style="width: 30%; background-color: red;"></div> <div style="width: 70%; background-color: limegreen;"></div>
> Apply system updates Completed	+0% (0 points)	None	<div style="width: 100%; background-color: limegreen;"></div>
> Enable endpoint protection Completed	+0% (0 points)	None	<div style="width: 100%; background-color: limegreen;"></div>
> Remediate vulnerabilities Completed	+0% (0 points)	None	<div style="width: 100%; background-color: limegreen;"></div>
> Implement security best practices Completed	+0% (0 points)	None	<div style="width: 100%; background-color: limegreen;"></div>
> Enable MFA Completed	+0% (0 points)	None	<div style="width: 100%; background-color: lightgrey;"></div>
> Manage access and permissions Completed	+0% (0 points)	None	<div style="width: 100%; background-color: limegreen;"></div>

Policies (exhibit):

Home > Policy

Policy - Compliance

Search (Ctrl+ /) «

Assign policy Assign initiative Refresh

Scope Microsoft Azure Type All definition types Compliance state All compliance states Search Filter by name or id...

Overall resource compliance 100%

Resources by compliance state 0

Non-compliant initiatives 0 out of 0

Non-compliant policies 0 out of 0

0 - Compliant
0 - Exempt
1 - Non-compliant
0 - Conflicting

Name ↑↓ Scope ↑↓ Compliance ↑↓ Resource compliance

No assignments to display within the given scope ↑↓ Non-Compliant Resources ↑↓ Non-compliant policies

Assignments Definitions Exemptions

Blueprints (preview) Resource Graph User privacy

Hot Area:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input checked="" type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input checked="" type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input checked="" type="radio"/>	<input type="radio"/>

Section: Hotspot
Explanation:

Explanation/Reference:
Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833>

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770>

QUESTION 14
DRAG DROP

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

Which three actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Select and Place:

Actions

Answer Area

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

From Advanced hunting, search for CveId in the DeviceTvmSoftwareInventoryVulnerabilitites table.

Create the remediation request.

Select **Security recommendations**.



Correct Answer:

Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Advanced hunting, search for CveId in the
DeviceTvmSoftwareInventoryVulnerabilitites
table.

Answer Area

From Threat & Vulnerability Management, select
Weaknesses, and search for the CVE.

Select **Security recommendations**.

Create the remediation request.

Section: Drag & Drop
Explanation:

Explanation/Reference:
Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271>

QUESTION 15

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 16

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue.

The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

- A. Modify the access control settings for the key vault.
- B. Enable the Key Vault firewall.

- C. Create an application security group.
- D. Modify the access policy for the key vault.

Correct Answer: B

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage>

QUESTION 17

HOTSPOT

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

You need to test LA1 in Security Center.

What should you do?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Hot Area:

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

▼
Recommendations
Workflow automation

Correct Answer:

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

▼
Recommendations
Workflow automation

Section: Hotspot
Explanation

Explanation/Reference:
Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run>

QUESTION 18

You have a Microsoft 365 subscription that uses Azure Defender.

You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender.

The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

- A. the Security Reader role for the subscription
- B. the Contributor for the subscription
- C. the Contributor role for RG1
- D. the Owner role for RG1

Correct Answer: C

Section: Multiple Choice

Explanation:

Explanation/Reference:

Explanation:

Reference:

QUESTION 19

You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. cp /bin/echo ./asc_alerttest_662jfi039n
- B. ./alerttest testing eicar pipe

- C. cp /bin/echo ./alerttest
- D. ./asc_alerttest_662jfi039n testing eicar pipe

Correct Answer: AD

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

[https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux-](https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux)

QUESTION 20

You create an Azure subscription named sub1.

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

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

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

What should you do?

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

Correct Answer: A

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

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

QUESTION 21

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.

Select and Place:

Select and Place:

Actions

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.

Answer Area



Correct Answer:

Actions

Change the alert severity threshold for emails to **Medium**.

Answer Area

Enable Azure Defender for the subscription.

Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.



Run the executable file and specify the appropriate arguments.



Change the alert severity threshold for emails to **Low**.

Rename the executable file as AlertTest.exe.

Section: Drag & Drop
Explanation:

Explanation/Reference:
Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation>

QUESTION 22

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does **NOT** receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Security solutions
- B. Security policy
- C. Pricing & settings
- D. Security alerts
- E. Azure Defender

Correct Answer: C

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

QUESTION 23

DRAG DROP

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions?

To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Select and Place:

Actions

Answer Area

Enable Security Health Analytics.

From Azure Security Center, add cloud connectors.

Configure the GCP Security Command Center.

Create a dedicated service account and a private key.

Enable the GCP Security Command Center API.



Correct Answer:

Actions

Answer Area

Configure the GCP Security Command Center.

Enable Security Health Analytics.



Enable the GCP Security Command Center API.



Create a dedicated service account and a private key.

From Azure Security Center, add cloud connectors.

Section: Drag & Drop
Explanation:

Explanation/Reference:
Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp>

QUESTION 24

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 25

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 26

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart.

What should you include in the query?

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

Correct Answer: B

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries>

QUESTION 27

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

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. Add a playbook.
- B. Associate a playbook to an incident.
- C. Enable Entity behavior analytics.

- D. Create a workbook.
- E. Enable the Fusion rule.

Correct Answer: AB

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

QUESTION 28

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

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

QUESTION 29

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

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations>

QUESTION 30

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated.

Which two actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a livestream
- B. Add a data connector
- C. Create an analytics rule
- D. Create a hunting query.
- E. Create a bookmark.

Correct Answer: BD

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/livestream>

QUESTION 31

DRAG DROP

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

Which three actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Select and Place:

Actions

Answer Area

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.



Correct Answer:

Actions

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Answer Area

Download and install the Log Analytics agent.



Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.



Section: Drag & Drop

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog>

QUESTION 32

HOTSPOT

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit:



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Hot Area:

Answer Area

If you hover over the virtual machine named vm1, you can view [answer choice].

the inbound network security group (NSG) rules
the last five Windows security log events
the open ports on the host
the running processes

If you select [answer choice], you can navigate to the bookmarks related to the incident.

Entities
Info
Insights
Timeline

Correct Answer:

Answer Area

If you hover over the virtual machine named vm1, you can view [answer choice].

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select [answer choice], you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

Section: Hotspot

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive>

QUESTION 33

DRAG DROP

You have an Azure Sentinel deployment.

You need to query for all suspicious credential access activities.

Which three actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Select and Place:

Actions

Answer Area

From Azure Sentinel, select **Hunting**.

Select **Run All Queries**.

Select **New Query**.

Filter by tactics.

From Azure Sentinel, select **Notebooks**.



Correct Answer:

Actions

Answer Area

From Azure Sentinel, select **Hunting**.

Select **New Query**.

Filter by tactics.

Select **Run All Queries**.

From Azure Sentinel, select **Notebooks**.



Section: Drag & Drop
Explanation

Explanation/Reference:

Explanation:

Reference:

<https://davemccollough.com/2020/11/28/threat-hunting-with-azure-sentinel/>

QUESTION 34

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually. You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel.

What should you do first?

- A. Add a new scheduled query rule.
- B. Add a data connector to Azure Sentinel.
- C. Configure a custom Threat Intelligence connector in Azure Sentinel.
- D. Modify the trigger in the logic app.

Correct Answer: B

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

QUESTION 35

Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.

A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.

You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.

What should you include in the recommendation?

- A. built-in queries
- B. livestream

- C. notebooks
- D. bookmarks

Correct Answer: C

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

QUESTION 36

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a parameter and modify the trigger.
- B. Add a custom data connector and modify the trigger.
- C. Add a condition and modify the action.
- D. Add a parameter and modify the action.

Correct Answer: D

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/>

QUESTION 37

You provision Azure Sentinel for a new Azure subscription.

You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query:

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents?

Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. user
- B. resource group
- C. IP address
- D. computer

Correct Answer: CD

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://azsec.azurewebsites.net/2020/02/24/alert-grouping-feature-in-azure-sentinel/>

QUESTION 38

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add the Security Events connector to the Azure Sentinel workspace.
- B. Create a query that uses the workspace expression and the union operator.
- C. Use the alias statement.
- D. Create a query that uses the resource expression and the alias operator.
- E. Add the Azure Sentinel solution to each workspace.

Correct Answer: BE

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

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

QUESTION 39

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal.

From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Correct Answer: D

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand>

QUESTION 40

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

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED. What is a possible cause of the issue?

- A. There are connectivity issues between the data sources and Log Analytics.
- B. The number of alerts exceeded 10,000 within two minutes.
- C. The rule query takes too long to run and times out.
- D. Permissions to one of the data sources of the rule query were modified.

Correct Answer: D

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#issue-a-scheduled-rule-failed-to-execute-or-appears-with-auto-disabled-added-to-the-name>

QUESTION 41

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel.

You need to resolve the issue for the analyst. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

- A. Azure Sentinel Responder
- B. Logic App Contributor
- C. Azure Sentinel Contributor
- D. Azure Sentinel Reader

Correct Answer: A

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles#roles-for-working-in-azure-sentinel>

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

QUESTION 42

You create an Azure subscription named sub1.

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

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

You need to collect security event logs from the Azure virtual machines that report to workspace1

What should you do?

- A. In workspace 1, create a workbook.
- B. From Security Center, enable data collection
- C. From Security Center, create a workflow automation.
- D. In sub1, register a provider.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 43

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 resource level
- B. at the subscription level

C. at the workspace level

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 44

You are responsible for responding to Azure Defender for Key vault alerts.

During an investigation of an alert, you discover unauthorized attempts to access a key vault from a for exit node.

What should you configure to mitigate the threat?

- A. the access policy settings of the key vault
- B. role - based access control (RBAC) for the key vault
- C. Azure Active Directory (Azure AD) permissions
- D. Key Vault firewalls and virtual networks.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 45

You receive a security bulletin about a potential attack that uses an image file.

You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.

Which indicator type should you use?

- A. a URL / domain indicator that has Action set to Alert and block
- B. a certificate indicator that has Action set to Alert and block

- C. a URL / domain indicator that has Action set to Alert only
- D. a file hash indicator that has Action set to Alert and block

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 46

Your company deploys the following services:

- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365

You need to provide a security analyst with the ability to use the Microsoft 365 security center.

The analyst must be able to approve and reject pending actions generated by Defender for Endpoint.

The solution must use the principle of least privilege.

Which two roles should you assign to the analyst?

Each correct answer presents part of the solution

NOTE: Each correct selection is worth one point.

- A. the Security Reader role in Azure Active Directory (Azure AD)
- B. the Security Administrator role in Azure Active Directory (Azure AD)
- C. the Active remediation actions role in Microsoft Defender for Endpoint
- D. the Compliance Data Administrator in Azure Active Directory (Azure AD)

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 47

You implement Safe Attachments policies in Microsoft Defender for Office 365.

Users report that email messages containing attachments take longer than expected to be received.

You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security.

The attachments must be scanned for messages that contain malware must be blocked.

What should you configure in the Safe Attachments policies?

- A. Replace
- B. Monitor and Enable redirect
- C. Dynamic Delivery
- D. Block and Enable redirect

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 48

You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled. You need to ensure that the Fusion rule can generate alerts.

What should you do?

- A. Add a hunting bookmark.
- B. Create a new machine learning analytics rule.
- C. Disable, and then enable the rule
- D. Add data connectors.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 49

You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region.

You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.

What should you do first?

- A. Create a data connector in Azure Sentinel.
- B. Add Azure Sentinel to a workspace
- C. Deploy Azure Data Catalog to the West US Azure region.
- D. Modify the workspace settings of the existing Azure Sentinel deployment.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 50

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. Permissions to the data sources of the rule query were modified.
- C. The target workspace was deleted
- D. There are connectivity issues between the data sources and Log Analytics

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 51

You have a third - party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign - in events in near real time.

What should you do to route events to the SIEM solution?

- A. Configure the Diagnostics settings in Azure AD to archive to a storage account.
- B. Create an Azure Sentinel workspace that has a Security Events connector.
- C. Configure the Diagnostics settings in Azure AD to stream to an event hub.
- D. Create an Azure Sentinel workspace that has an Azure Active Directory connector.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 52

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for Identity portal, you need to configure several accounts for attacker Solution: You add each account as a Sensitive account.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 53

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

Case Study Title (Case Study):

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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

- A. executive
- B. sales
- C. marketing

Correct Answer: B

Section: Case Study - Contoso Ltd

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios>

QUESTION 54

The issue for which team can be resolved by using Microsoft Defender for Office 365?

Case Study Title (Case Study):

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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

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

Correct Answer: B

Section: Case Study - Contoso Ltd

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide>

QUESTION 55

You need to implement the Azure Information Protection requirements.

What should you configure first?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

- 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

Correct Answer: D

Section: Case Study - Litware Inc.

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview>

QUESTION 56

You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements.

Which policy should you modify?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the

other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

A. Activity from suspicious IP addresses

- B. Activity from anonymous IP addresses
- C. Impossible travel
- D. Risky sign-in

Correct Answer: C

Section: Case Study - Litware Inc.

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

QUESTION 57

Case Study - Click the exhibit tab

HOTSPOT

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

What should you recommend for each threat?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Exhibit:

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. You can also use the back and forward buttons in the browser to move between the different problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Next button.

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, Boston, Chicago, Atlanta, and San Jose. 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 of its resources.

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.

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 has experienced several file corruption issues.

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 sensitive files were shared with unauthorized parties.

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 information:

Hot Area:

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

Correct Answer:

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

Section: Case Study - Contoso Ltd

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

QUESTION 58

You need to recommend a solution to meet the technical requirements for the Azure virtual machines.

What should you include in the recommendation?

Case Study Title (Case Study):

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain

exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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
```

- A. just-in-time (JIT) access
- B. Azure Defender
- C. Azure Firewall
- D. Azure Application Gateway

Correct Answer: B

Section: Case Study - Contoso Ltd

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/azure-defender>

QUESTION 59

Case Study - Click the exhibit tab

HOTSPOT

You need to create an advanced hunting query to investigate the executive team issue.

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

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Exhibit:

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. You can also use the back and forward buttons in the browser to move between the different problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Next button.

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, Boston, Chicago, Atlanta, and San Jose. 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 of its resources.

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 and which are false positives.

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 has experienced several incidents where sensitive files were lost or corrupted.

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 sensitive files were shared with unauthorized parties.

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 list of countries:

Hot Area:

Answer Area

CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)  
  
| summarize activityCount =  
    by FolderPath, FileName,  
    ActionType, AccountDisplayName  
  
| where activityCount > 5
```

avg()
count()
sum()

Correct Answer:

Answer Area

CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)

| summarize activityCount =
    by FolderPath, FileName,
    ActionType, AccountDisplayName
| where activityCount > 5
```

avg()
count()
sum()

Section: Case Study - Contoso Ltd

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

QUESTION 60

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.

Which role should you assign?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the

other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

A. Automation Operator

- B. Automation Runbook Operator
- C. Azure Sentinel Contributor
- D. Logic App Contributor

Correct Answer: C

Section: Case Study - Litware Inc.

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

QUESTION 61

You need to create the test rule to meet the Azure Sentinel requirements.

What should you do when you create the rule?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

- A. From Set rule logic, turn off suppression.
- B. From Analytics rule details, configure the tactics.
- C. From Set rule logic, map the entities.
- D. From Analytics rule details, configure the severity.

Correct Answer: C

Section: Case Study - Litware Inc.

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

QUESTION 62

Case Study - Click the exhibit tab

HOTSPOT

You need to create the analytics rule to meet the Azure Sentinel requirements.
What should you do?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Capture (exhibit):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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
------	------	-------------

Capture (exhibit):

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~~

Hot Area:

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:

Diagnostics settings
A service principal
A trigger

Correct Answer:

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:

Diagnostics settings
A service principal
A trigger

Section: Case Study - Litware Inc.

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#set-automated-responses-and-create-the-rule>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

SC-200

Number: SC-200

Passing Score: 800

Time Limit: 120 min

File Version: 1

SC-200



Mitigate threats using Microsoft 365 Defender

Testlet 1

Case study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

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
```

QUESTION 1

The issue for which team can be resolved by using Microsoft Defender for Office 365?



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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide>

Mitigate threats using Microsoft 365 Defender

Testlet 2

Case study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

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.

QUESTION 1

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview>

QUESTION 2

You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements.

Which policy should you modify?

- A. Activity from suspicious IP addresses
- B. Activity from anonymous IP addresses
- C. Impossible travel
- D. Risky sign-in

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

Mitigate threats using Microsoft 365 Defender

Question Set 3

QUESTION 1

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.
- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts>

QUESTION 2

You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group.
- B. Add the device users to the admin role.
- C. Add a tag to the machines.
- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.
- F. Create a new device group that has a rank of 4.

Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://www.drware.com/how-to-use-tagging-effectively-in-microsoft-defender-for-endpoint-part-1/>

QUESTION 3

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Entity tags, you add the accounts as Honeytoken accounts.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

Mitigate threats using Azure Defender

Question Set 1

QUESTION 1

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select **Take Action**, and then expand the Prevent future attacks section.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the 'Mitigate the threat' option.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 2

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

- A. Modify the access control settings for the key vault.
- B. Enable the Key Vault firewall.
- C. Create an application security group.
- D. Modify the access policy for the key vault.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage>

QUESTION 3

You create an Azure subscription named sub1.

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

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

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

What should you do?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 4

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select **Take Action**, and then expand the Mitigate the threat section.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

Mitigate threats using Azure Sentinel

Testlet 1

Case study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

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.

QUESTION 1

You need to create the test rule to meet the Azure Sentinel requirements.

What should you do when you create the rule?

- A. From Set rule logic, turn off suppression.
- B. From Analytics rule details, configure the tactics.
- C. From Set rule logic, map the entities.
- D. From Analytics rule details, configure the severity.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

Mitigate threats using Azure Sentinel

Question Set 2

QUESTION 1

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart.

What should you include in the query?

- A. extend
- B. bin
- C. makeset
- D. workspace

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries>

QUESTION 2

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

QUESTION 3

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

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

QUESTION 4

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a livestream
- B. Add a data connector
- C. Create an analytics rule
- D. Create a hunting query.
- E. Create a bookmark.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/livestream>

QUESTION 5

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.

You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel.

What should you do first?

- A. And a new scheduled query rule.
- B. Add a data connector to Azure Sentinel.
- C. Configure a custom Threat Intelligence connector in Azure Sentinel.
- D. Modify the trigger in the logic app.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add the Security Events connector to the Azure Sentinel workspace.
- B. Create a query that uses the `workspace` expression and the `union` operator.
- C. Use the `alias` statement.
- D. Create a query that uses the `resource` expression and the `alias` operator.
- E. Add the Azure Sentinel solution to each workspace.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 7

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal.

From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand>

QUESTION 8

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

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

- A. There are connectivity issues between the data sources and Log Analytics.
- B. The number of alerts exceeded 10,000 within two minutes.
- C. The rule query takes too long to run and times out.
- D. Permissions to one of the data sources of the rule query were modified.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

QUESTION 9

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel.

You need to resolve the issue for the analyst. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

- A. Azure Sentinel Responder
- B. Logic App Contributor
- C. Azure Sentinel Contributor
- D. Azure Sentinel Reader

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

Microsoft Security Operations Analyst

Exam Code: SC-200

Version: July 2021

Join us: <https://www.facebook.com/groups/itknowledge247>

Prepared by MA

Question #1

Topic 1 DRAG DROP -

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFO Laptop, CEO Laptop, and COOL Laptop.

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

Select and Place:

Answers:

Values	Answer Area
project LogonFailures=count()	where DeviceName in ("CFO Laptop", "CEO Laptop", "COOL Laptop")
summarize LogonFailures=count() by DeviceName, LogonType	ActionType == "LogonFailed"
where ActionType == FailureReason	summarize LogonFailures=count() by DeviceName, LogonType and
where DeviceName in ("CFO Laptop", "CEO Laptop", "COOL Laptop")	where ActionType == FailureReason
ActionType == "LogonFailed"	project LogonFailures=count()

OR

| where DeviceName in ("CFO Laptop", "CEO Laptop", "COOL Laptop")

| where ActionType == FailureReason and LogonType == "LogonFailed"

| summarize LogonFailures=count() by DeviceName,

| LogonType | project LogonFailures

Question #2

You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.

Which anomaly detection policy should you use?

- A. Impossible travel
- B. Activity from anonymous IP addresses
- C. Activity from infrequent country
- D. Malware detection

Question #3

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.

You need to create a data loss prevention (DLP) policy to protect the sensitive documents.

What should you use to detect which documents are sensitive?

- A. SharePoint search
- B. a hunting query in Microsoft 365 Defender
- C. Azure Information Protection
- D. RegEx pattern matching

Question #4

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.

You need to identify which Office VBA macros might be affected.

Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A.
`Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

B.
`Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`

C.
`Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`

D.
`Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

Question #5

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.
- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Question #6

DRAG DROP -

You open the Cloud App Security portal as shown in the following exhibit.

The screenshot shows the Cloud Discovery – Cloud App Security portal interface. The left sidebar includes sections for Dashboard, Discover (Cloud Discovery dashboard, Discovered apps, Discovered resources, IP addresses, Users), Cloud app catalog, and Investigate (Cloud storage, Hosting services, IT services, Content management, Data analytics, Website monitoring, Advertising, Marketing, Customer support, Collaboration). The main area is titled 'Cloud Discovery' and has tabs for Dashboard, Discovered apps (selected), IP addresses, and Users. It features a 'Queries' section and a 'RISK SCORE' slider from 0 to 10. Below these are two risk factor sliders: 'COMPLIANCE RISK FACTOR' and 'SECURITY RISK FACTOR'. A table lists 78 discovered apps, including their names, scores, traffic, upload, transaction, user counts, IP addresses, and last seen dates. The 'Launchpad' app, which has a score of 2, is highlighted in the table.

App	Score	Traffic	Upload	Transac.	Users	IP addr...	Last se...	Actions
Applied Innovations	5	866 KB	-	12	11	8	Apr 20, 2020	<input checked="" type="checkbox"/> <input type="radio"/> <input type="radio"/>
Hosting services	3							<input type="checkbox"/> <input checked="" type="radio"/> <input type="radio"/>
StatusCake	3	939 KB	-	13	13	7	Apr 20, 2020	<input checked="" type="checkbox"/> <input type="radio"/> <input type="radio"/>
Website monitoring								<input type="checkbox"/> <input checked="" type="radio"/> <input type="radio"/>
Usersnap	3	1 MB	-	15	15	10	Apr 20, 2020	<input checked="" type="checkbox"/> <input type="radio"/> <input type="radio"/>
Productivity								<input type="checkbox"/> <input checked="" type="radio"/> <input type="radio"/>
CopperEgg	2	866 KB	-	12	12	8	Apr 20, 2020	<input checked="" type="checkbox"/> <input type="radio"/> <input type="radio"/>
Website monitoring								<input type="checkbox"/> <input checked="" type="radio"/> <input type="radio"/>
Launchpad	2	939 KB	-	13	13	7	Apr 20, 2020	<input checked="" type="checkbox"/> <input type="radio"/> <input type="radio"/>
Code-hosting								<input type="checkbox"/> <input checked="" type="radio"/> <input type="radio"/>

You need to remediate the risk for the Launchpad app.

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

Select and Place:

Actions

Tag the app as **Unsanctioned**.

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Select the app.

Tag the app as **Sanctioned**.

Generate a block script.

Answer Area



Answers:

Actions

Tag the app as **Unsanctioned**.

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Select the app.

Tag the app as **Sanctioned**.

Generate a block script.

Answer Area

Select the app.

Tag the app as **Unsanctioned**.

Generate a block script.

Run the script on the source appliance.



Question #7

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You plan to perform cross-domain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

|  (

extend
join
project
union

DeviceFileEvents

|  FileName, SHA256

extend
join
project
union

) on SHA256

|  Timestamp, FileName, SHA256, DeviceName, DeviceId,

extend
join
project
union

NetworkMessageId, SenderFromAddress, RecipientEmailAddress

Answer:

Answer Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

|

|         |
|---------|
| extend  |
| join    |
| project |
| union   |


( 

DeviceFileEvents

|

|         |
|---------|
| extend  |
| join    |
| project |
| union   |


FileName, SHA256

) on SHA256

|

|         |
|---------|
| extend  |
| join    |
| project |
| union   |


Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Question #8

You have the following advanced hunting query in Microsoft 365 Defender.

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a detection rule.
- B. Create a suppression rule.
- C. Add | order by Timestamp to the query.
- D. Replace DeviceProcessEvents with DeviceNetworkEvents.
- E. Add DeviceId and ReportId to the output of the query.

Question #9

You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group.
- B. Add the device users to the admin role.
- C. Add a tag to the machines.
- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.
- F. Create a new device group that has a rank of 4.

Question #10

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Entity tags, you add the accounts as Honeytoken accounts.

Does this meet the goal?

- A. Yes
- B. No

Question #11

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Azure Identity Protection, you configure the sign-in risk policy.

Does this meet the goal?

- A. Yes
- B. No

Question #12

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group.

Does this meet the goal?

- A. Yes
- B. No

Question #13

HOTSPOT -

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Resource exemption (preview)

< Now you can exempt irrelevant resources so they do not affect your secure score. >
[Learn more](#)

Each security control below represents a security risk you should mitigate.
Address the recommendations in each control, focusing on the controls worth the most points.
To get the max score, fix all recommendations for all resources in a control. [Learn more](#) >

Search recommendations		Control status: 2 Selected	Recommendation status: 2 Selected
Recommendation maturity: All Resource type: All Quick fix available: All Contains exemptions: All Reset filters Group by controls: <input checked="" type="checkbox"/> On			
Controls	Potential score increase	Unhealthy resources	Resource Health
> Restrict unauthorized network access	+9% (4 points)	2 of 2 resources	
> Secure management ports	+9% (4 points)	1 of 2 resources	
> Enable encryption at rest	+9% (4 points)	2 of 2 resources	
> Remediate security configurations	+4% (2 points)	1 of 2 resources	
> Apply adaptive application control	+3% (2 points)	1 of 2 resources	
> Apply system updates Completed	+0% (0 points)	None	
> Enable endpoint protection Completed	+0% (0 points)	None	
> Remediate vulnerabilities Completed	+0% (0 points)	None	
> Implement security best practices Completed	+0% (0 points)	None	
> Enable MFA Completed	+0% (0 points)	None	
> Manage access and permissions Completed	+0% (0 points)	None	

Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)

Home > Policy

Policy - Compliance

Overall resource compliance: 100%

Resources by compliance state:

- 0 - Compliant
- 0 - Exempt
- 1 - Non-compliant
- 0 - Conflicting

Non-compliant initiatives: 0 out of 0

Non-compliant policies: 0 out of 0

Name

No assignments to display within the given scope

Scope: Microsoft Azure | Type: All definition types | Compliance state: All compliance states

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input checked="" type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input checked="" type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input checked="" type="radio"/>	<input type="radio"/>

Question #14

DRAG DROP -

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

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

Select and Place:

Actions

Answer Area

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

From Advanced hunting, search for CveId in the DeviceTvmSoftwareInventoryVulnerabilitites table.

Create the remediation request.

Select **Security recommendations**.



Actions

Answer Area

From Device Inventory, search for the CVE.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

Open the Threat Protection report.

Select **Security recommendations**.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

Create the remediation request.



From Advanced hunting, search for CveId in the DeviceTvmSoftwareInventoryVulnerabilitites table.

Create the remediation request.

Select **Security recommendations**.

Question #15

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.

Does this meet the goal?

- A. Yes
- B. No
- You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the "Mitigate the threat™" option.

Question #16

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

- A. Modify the access control settings for the key vault.
- B. Enable the Key Vault firewall.
- C. Create an application security group.
- D. Modify the access policy for the key vault.

Question #17

HOTSPOT -

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

You need to test LA1 in Security Center.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations
Workflow automation

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations
Workflow automation

Question #18

You have a Microsoft 365 subscription that uses Azure Defender.

You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

- A. the Security Reader role for the subscription
- B. the Contributor for the subscription
- C. the Contributor role for RG1
- D. the Owner role for RG1

Question #19

You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. cp /bin/echo ./asc_alerttest_662jfi039n
- B. ./alerttest testing eicar pipe
- C. cp /bin/echo ./alerttest
- D. ./asc_alerttest_662jfi039n testing eicar pipe

Question #20

You create an Azure subscription named sub1.

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

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

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

What should you do?

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

Question #21

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.

Select and Place:

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.	

Actions	Answer Area
Change the alert severity threshold for emails to Medium .	Enable Azure Defender for the subscription.
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.	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.	Run the executable file and specify the appropriate arguments.
Rename the executable file as AlertTest.exe.	

Question #22

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Security solutions
- B. Security policy
- C. Pricing & settings
- D. Security alerts
- E. Azure Defender

Question #23

DRAG DROP -

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

Answer Area

Enable Security Health Analytics.

From Azure Security Center, add cloud connectors.

Configure the GCP Security Command Center.

Create a dedicated service account and a private key.

Enable the GCP Security Command Center API.



Correct

Answer:

Actions	Answer Area
Enable Security Health Analytics.	Configure the GCP Security Command Center.
From Azure Security Center, add cloud connectors.	Enable Security Health Analytics.
Configure the GCP Security Command Center.	 Enable the GCP Security Command Center API. 
Create a dedicated service account and a private key.	Create a dedicated service account and a private key.
Enable the GCP Security Command Center API.	 From Azure Security Center, add cloud connectors. 

Question #24

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

- A. Yes
- B. No

Question #25

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.

Does this meet the goal?

- A. Yes
- B. No

Question #26

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart.

What should you include in the query?

- A. extend.
- B. bin
- C. makeset
- D. workspace

Question #27

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

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

Question #28

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

Question #29

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

Question #30

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a livestream
- B. Add a data connector
- C. Create an analytics rule
- D. Create a hunting query.
- E. Create a bookmark.

Question #31

DRAG DROP -

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

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

Select and Place:

Actions	Answer Area
Deploy an OMS Gateway on the network.	
Set the syslog daemon to forward the events directly to Azure Sentinel.	
Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.	 
Download and install the Log Analytics agent.	
Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.	

Actions	Answer Area
Deploy an OMS Gateway on the network.	Download and install the Log Analytics agent.
Set the syslog daemon to forward the events directly to Azure Sentinel.	Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.
Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.	 
Download and install the Log Analytics agent.	
Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.	

Question #32

HOTSPOT -

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If you hover over the virtual machine named vm1, you can view [answer choice].

the inbound network security group (NSG) rules
the last five Windows security log events
the open ports on the host
the running processes

If you select [answer choice], you can navigate to the bookmarks related to the incident.

Entities
Info
Insights
Timeline

Question #33

DRAG DROP

You have an Azure Sentinel deployment.

You need to query for all suspicious credential access activities.

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

Select and Place:

Actions

From Azure Sentinel, select **Hunting**.

Select **Run All Queries**.

Select **New Query**.

Filter by tactics.

From Azure Sentinel, select **Notebooks**.

Answer Area



[Reveal Solution](#)

Actions

From Azure Sentinel, select **Hunting**.

Select **Run All Queries**.

Select **New Query**.

Filter by tactics.

From Azure Sentinel, select **Notebooks**.

Answer Area

From Azure Sentinel, select **Hunting**.

Filter by tactics.

Select **Run All Queries**.



Question #34

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.

You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel.

What should you do first?

- A. And a new scheduled query rule.
- B. Add a data connector to Azure Sentinel.
- C. Configure a custom Threat Intelligence connector in Azure Sentinel.
- D. Modify the trigger in the logic app.

Question #35

Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.

A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.

You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.

What should you include in the recommendation?

- A. built-in queries
- B. livestream
- C. notebooks
- D. bookmarks

Question #36

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a parameter and modify the trigger.
- B. Add a custom data connector and modify the trigger.
- C. Add a condition and modify the action.
- D. Add a parameter and modify the action.

Question #37

You provision Azure Sentinel for a new Azure subscription.

You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query.

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. user
- B. resource group
- C. IP address
- D. computer

Question #38

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add the Security Events connector to the Azure Sentinel workspace.
- B. Create a query that uses the workspace expression and the union operator.

- C. Use the alias statement.
- D. Create a query that uses the resource expression and the alias operator.
- E. Add the Azure Sentinel solution to each workspace.

Question #39

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal.

From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Question #40

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

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

- A. There are connectivity issues between the data sources and Log Analytics.
- B. The number of alerts exceeded 10,000 within two minutes.
- C. The rule query takes too long to run and times out.
- D. Permissions to one of the data sources of the rule query were modified.

Question #41

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel.

You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?

- A. Azure Sentinel Responder
- B. Logic App Contributor
- C. Azure Sentinel Contributor
- D. Azure Sentinel Reader

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All-information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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
```

Question #42

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

- A. executive
- B. sales
- C. marketing

Question #43

The issue for which team can be resolved by using Microsoft Defender for Office 365?

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

Question #44

HOTSPOT -

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam. What should you recommend for each threat? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Internal threat:

Add resource locks to the key vault.
Modify the access policy settings for the key vault.
Modify the role-based access control (RBAC) settings for the key vault.

External threat:

Implement Azure Firewall.
Modify the Key Vault firewall settings.
Modify the network security groups (NSGs).

- **The answer should be:**

- Internal Threat: Modify the access policy settings for the key vault External Threat.
- Implement Azure Firewall.

Question #45

You need to recommend a solution to meet the technical requirements for the Azure virtual machines.

What should you include in the recommendation?

- A. just-in-time (JIT) access
- B. Azure Defender
- C. Azure Firewall
- D. Azure Application Gateway

Question #46

HOTSPOT -

You need to create an advanced hunting query to investigate the executive team issue.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)
```

```
| summarize activityCount =
```

```
ActionType, AccountDisplayName
```

```
| where activityCount > 5
```

avg()
count()
sum()

```
by FolderPath, FileName,
```

- **The answer should be:**

- DeviceFileEvents
- Count()

Case study 2

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

Question #47

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

Question #48

You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements.

Which policy should you modify?

- A. Activity from suspicious IP addresses
- B. Activity from anonymous IP addresses
- C. Impossible travel
- D. Risky sign-in

Question #49

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.
Which role should you assign?

- A. Automation Operator
- B. Automation Runbook Operator
- C. Azure Sentinel Contributor
- D. Logic App Contributor

Question #50

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

- A. From Set rule logic, turn off suppression.
- B. From Analytics rule details, configure the tactics.
- C. From Set rule logic, map the entities.
- D. From Analytics rule details, configure the severity.

Question #51

HOTSPOT -

You need to create the analytics rule to meet the Azure Sentinel requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:

Diagnostics settings
A service principal
A trigger

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:

Diagnostics settings
A service principal
A trigger

Question #52

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Azure Defender
- B. Security policy
- C. Pricing & settings (correct)**
- D. Security alerts
- E. Security solutions

Question #53

You create an Azure subscription named sub1.

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

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

You need to collect security event logs from the Azure virtual machines that report to workspace1

What should you do?

- A. In workspace 1, create a workbook.
- B. From Security Center, enable data collection (correct)
- C. From Security Center, create a workflow automation.
- D. In sub1, register a provider.

Question #54

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 resource level
- B- at the subscription level (correct)
- C- at the workspace level

Question #55

You are responsible for responding to Azure Defender for Key vault alerts.

During an investigation of an alert, you discover unauthorized attempts to access a key vault from a for exit node.

What should you configure to mitigate the threat?

- A. the access policy settings of the key vault
- B. role - based access control (RBAC) for the key vault
- C. Azure Active Directory (Azure AD) permissions
- D. Key Vault firewalls and virtual networks. (might be)

Question #56

You receive a security bulletin about a potential attack that uses an image file.

You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.

Which indicator type should you use?

- A. a URL / domain indicator that has Action set to **Alert and block**
- B. a certificate indicator that has Action set to **Alert and block**
- C. a URL / domain indicator that has Action set to **Alert only**
- D. a file hash indicator that has Action set to **Alert and block** (correct)

Question #57

our company deploys the following services:

- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365

You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Defender for Endpoint.

The solution must use the principle of least privilege.

Which two roles should you assign to the analyst? Each correct answer presents part of the solution

NOTE: Each correct selection is worth one point.

- A. the Security Reader role in Azure Active Directory (Azure AD) (correct)
- B. the Security Administrator role in Azure Active Directory (Azure AD)
- C. the Active remediation actions role in Microsoft Defender for Endpoint (correct)
- D. the Compliance Data Administrator in Azure Active Directory (Azure AD)

Question #58

You implement Safe Attachments policies in Microsoft Defender for Office 365.

Users report that email messages containing attachments take longer than expected to be received. You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for messages that contain malware must be blocked.

What should you configure in the Safe Attachments policies?

- A. Replace
- B. Monitor and Enable redirect
- C. Dynamic Delivery (correct)
- D. Block and Enable redirect

Question #59

You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled. You need to ensure that the Fusion rule can generate alerts.

What should you do?

- A. Add a hunting bookmark.
- B. Create a new machine learning analytics rule.
- C. Disable, and then enable the rule
- D. Add data connectors. (correct)

Question #60

You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region.

You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.

What should you do first?

- A. Create a data connector in Azure Sentinel.
- B. Add Azure Sentinel to a workspace (correct)
- C. Deploy Azure Data Catalog to the West US Azure region.
- D. Modify the workspace settings of the existing Azure Sentinel deployment.

Question #61

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. (correct)
- B. Permissions to the data sources of the rule query were modified.
- C. The target workspace was deleted
- D. There are connectivity issues between the data sources and Log Analytics (correct)

Question #62

You have a third - party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-in events in near real time.

What should you do to route events to the SIEM solution?

- A. Configure the Diagnostics settings in Azure AD to archive to a storage account.
- B. Create an Azure Sentinel workspace that has a Security Events connector.
- C. Configure the Diagnostics settings in Azure AD to stream to an event hub. (correct)
- D. Create an Azure Sentinel workspace that has an Azure Active Directory connector.

Question #63

After you answer a question in this section, you will NOT be able to return to it. As a result, ti

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for Identity portal, you need to configure several accounts for attacker Solution: You add each account as a Sensitive account.

Does this meet the goal?

- A. Yes
- B. No (correct)

Question#64

You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.

You need to hide the alerts automatically in Security Center.

Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Pricing & settings.
- B. Security policy.
- C. Azure Resource as the entity type and specify the ID.
- D. Suppression rules, and then select Create new suppression rule. (here)
- E. IP as the entity type and specify the IP address.

Question#65

You are informed of an increase in malicious email being received by users.

You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.

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:

```
let Malicious Emails=
|where MalwareFilterVerdict == Malware "
| project TimeEmail = Timestamp , Subject , Sender FromAddress , AccountName =
| tostring ( split ( RecipientEmailAddress , " @ " ) [ 0 ] );
Malicious Emails
```

the answers:

- **Email Events**
- **IdentityLogonEvents**
- **take 20**

Question#66

Your company has a single office in Istanbul and a Microsoft 365 subscription.

The company plans to use conditional access policies to enforce multi - factor authentication (MFA).

You need to enforce MFA for all users who work remotely.

What should you include in the solution?

- A- a sign - in user policy
- B- a user risk policy
- C- a named location (correct)
- D- a fraud alert.

Question#67

You are configuring Microsoft Cloud App Security.

You have a custom threat detection policy based on the IP address ranges of your company's United States - based offices. You receive many alerts related to impossible travel and sign - ins from risky IP addresses.

You determine that 99 % of the alerts are legitimate sign - ins from your corporate offices.

You need to prevent alerts for legitimate sign - ins from known locations.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add the IP addresses to the other address range category and add a tag (might)
- B. Create an activity policy that has an exclusion for the IP addresses.
- C. Increase the sensitivity level of the impossible travel anomaly detection policy
- D. Override automatic data enrichment (might)

Question#68

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a custom data connector and modify the trigger
- B. Add an alert and modify the action.
- C. Add a condition and modify the action
- D. Add a parameter and modify the trigger. (might be)

Question#69

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Sentinel workspace named workspace 1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.

You need to use the Fusion rule to detect multi - staged attacks that include suspicious sign - ins to contoso.com followed by anomalous Microsoft Office 365 activity.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a Microsoft Cloud App Security connector. (correct)
- B. Create a Microsoft incident creation rule based on Azure Security Center.
- C. Create an Azure AD Identity Protection Connector (correct)
- D. Create a custom rule based on the office connector templates.

Question#70

deploy Azure Sentinel.

You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.

Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area:

- Microsoft Teams: Office 365
- Linux virtual machines in Azure: syslog

Question#71

You need to complete the query for failed sign - ins to meet the technical requirements.

Where can you find the column name to complete the where clause?

- A- Security alerts in Azure Security Center
- B- the query window of the Log Analytics workspace (correct)
- C- Activity log in Azure
- D- Azure Advisor

Question#72

You need to remediate active attacks to meet the technical requirements.

What should you include in the solution?

- A- Azure Functions
- B- Azure Automation runbooks
- C- Azure Logic Apps (might)
- D- Azure Sentinel livestreams

Question#73

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 Dependency agent
- B- Install the Connected Machine agent
- C- Configure the Hybrid Runbook Worker role
- D- Install the Log Analytics agent (correct)

Question#74

A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks. The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center. You need to ensure that the security administrator receives email alerts for all the activities.

What should you configure in the Security Center settings?

- A- The integration settings for Threat detection
- B- the Azure Defender plans
- C- a cloud connector
- D- the severity level of email notifications (correct)

Question#75

You plan to create a data loss prevention (DLP) policy that will be used with insider risk management. The severity level is set to Low. You need to ensure that insider risk management alerts are generated from rules in the DLP policies.

What should you do?

- A- Set the severity level to Medium
- B- Scope the policy to only specified users
- C- Set the scope of the policy to the Data leaks template
- D- Set the severity level to High (might)

Question#76

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 alert, select the alert, select Take Action, and then expand the Prevent future attacks section.
- B- From Security alerts, select the alert, select Take Action, and then expand the Mitigate the threat section. (correct)
- C- From Regulatory compliance, download the report
- D- From Recommendations, download the CSV report

Question#77

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(correct)

Question#78

You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.

Which two configurations should you modify?

Each correct answer presents part of the solution.

NOTE Each correct selection is worth one point.

- A- the Onboarding settings from Device management in Microsoft Defender Security Center
- B- the Cloud Discovery settings in Cloud App Security (correct)
- C- Advanced features from Settings in Microsoft Defender Security Center (correct)
- D- Cloud App Security anomaly detection policies

Question#79

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

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

Answer Area:

- F. Log Analytics workspace to use:
- G. Windows security events to collect:

Question#80

You have an Azure Storage account that will be accessed by multiple Azure Functions apps during the development of an application. You need to hide Azure Defender alerts for the storage account.

Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area:

- Entity type: (IP address, Azure Resource, Host, User account) Azure resource
- Field: (name, resource ID, Address, Command line) Resource ID

Question#81

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 Dependency agent
- B- Install the Connected Machine agent
- C- Configure the Hybrid Runbook Worker role
- D- Install the Log Analytics agent (correct)

Question#82

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:

- J. Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:(0,1,2,3) (1)
- K. Query element required to correlate data between tenants:(extend, project, workspace) (workspace

Question#83

You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Center.

How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area:

```
“resources”: [  
    {  
        “type”: “..... /automations”,  
        “apiVersion”: 2019-01-01-preview”,  
        “name”: [parameters(‘name’)],  
        “location”: “[parameters(‘location’)]”,  
        “properties”: {  
  
            “Actions”: [  
                {  
                    “actionType”: “LogicApp”,  
                    “logicAppResourceId”: “[resourceId(‘ITEM2/workflows’,  
                        parameters(‘appName’))]”,  
                    “uri”: “[listCallbackURL(resourceId(parameters(‘subscriptionId’),  
                        Parameters(‘resourceGroupName’), ‘..... /workflows/triggers’,  
                        Parameters(‘appName’), ‘manual’, ‘2019-05-01’).value]”  
                }  
            ]  
        }  
    }  
]
```

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You need to configure the continuous export of high-severity alerts to enable their retrieval from a third-party security information and event management (SIEM) solution.

To which service should you export the alerts?

A. Azure Data Lake

B. Azure Event Hubs

C. Azure Cosmos DB

D. Azure Event Grid

SC-200_51q_June_2021_By_DrunkMonk

Number: 000-000

Passing Score: 800

Time Limit: 120 min

File Version: 1.0



Exam SC-200 Compiled by DrunkMonk June 2021

Sections

1. Multiple Choice
2. Hotspot
3. Drag & Drop
4. Case Study - Contoso Ltd
5. Case Study - Litware Inc.

Exam A

QUESTION 1 DRAG DROP

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFO Laptop, CEO Laptop, and COOL Laptop.

How should you complete the query?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Select and Place:

Values

Answer Area

```
| project LogonFailures=count()
```

```
| summarize LogonFailures=count()  
by DeviceName, LogonType
```

```
| where ActionType ==  
FailureReason
```

```
| where DeviceName in ("CFO Laptop,  
"CEO Laptop", "COOL Laptop")
```

```
ActionType == "LogonFailed"
```

Answer:

Values

Answer Area

```
| summarize LogonFailures=count()  
by DeviceName, LogonType
```

```
| where DeviceName in ("CFOlaptop,  
"CEOlaptop", "COOLaptop")
```

```
| where ActionType ==  
FailureReason
```

```
ActionType == "LogonFailed"
```

```
| project LogonFailures=count()
```

Section: Drag & Drop

Explanation/Reference:

Explanation:

Reference:

QUESTION 2

You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.

Which anomaly detection policy should you use?

- A. Impossible travel
- B. Activity from anonymous IP addresses
- C. Activity from infrequent country
- D. Malware detection

Answer: C

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

QUESTION 3

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.

You need to create a data loss prevention (DLP) policy to protect the sensitive documents.

What should you use to detect which documents are sensitive?

- A. SharePoint search
- B. a hunting query in Microsoft 365 Defender
- C. Azure Information Protection
- D. RegEx pattern matching

Answer: C

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection>

QUESTION 4

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.

You need to identify which Office VBA macros might be affected.

Which two commands can you run to achieve the goal?

Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
- B. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
- C. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
- D. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled

Answer: BC

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction>

QUESTION 5

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.
- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Answer: BCE

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts>

QUESTION 6**DRAG DROP**

You open the Cloud App Security portal as shown in the following exhibit:

The screenshot shows the Cloud Discovery - Cloud App Security interface. The left sidebar includes sections for Dashboard, Discover (Cloud Discovery dashboard, Discovered apps, Discovered resources, IP addresses, Users), Investigate (Cloud storage, Hosting services, IT services, Content management, Data analytics, Website monitoring, Advertising, Marketing, Customer support, Collaboration), Control, and Alerts. The main area is titled 'Cloud Discovery' and has tabs for Dashboard, Discovered apps (selected), IP addresses, and Users. It features a 'Queries' section with a dropdown menu 'Select a query...'. Below it is a table with columns: APPS, APP TAG, RISK SCORE, COMPLIANCE RISK FACTOR, SECURITY RISK FACTOR, and several other columns for each app entry. The table lists several apps with their respective details.

App	Score	Traffic	Upload	Transac..	Users	IP addr...	Last se...	Action
Applied Innovations Hosting services	3	866 KB	-	12	11	8	Apr 20, 2021	✓
StatusCake Website monitoring	3	939 KB	-	13	13	7	Apr 20, 2021	✓
Usersnap Productivity	3	1 MB	-	15	15	10	Apr 20, 2021	✓
CopperEgg Website monitoring	3	866 KB	-	12	12	8	Apr 20, 2021	✓
Launchpad Code-hosting	3	939 KB	-	13	13	7	Apr 20, 2021	✓

You need to remediate the risk for the Launchpad app.

Which four actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place

Actions

Answer Area

Tag the app as **Unsanctioned**.

Run the script on the source appliance.

Run the script in Azure Cloud Shell.



Select the app.



Tag the app as **Sanctioned**.

Generate a block script.

Answer:

Actions

Answer Area

Select the app.

Run the script in Azure Cloud Shell.



Tag the app as **Unsanctioned**.

Tag the app as **Sanctioned**.



Generate a block script.

Run the script on the source appliance.

Section: Drag & Drop

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery>

QUESTION 7

HOTSPOT

You have a Microsoft 365 E5 subscription.

You plan to perform cross-domain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment.

How should you complete the query?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

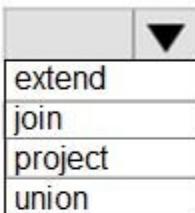
Hot Area:

Answer Area

EmailAttachmentInfo

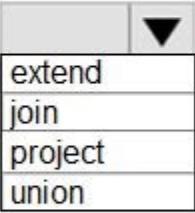
| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

|  (

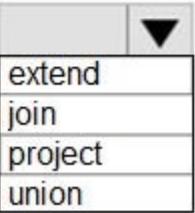
extend
join
project
union

DeviceFileEvents

|  FileName, SHA256

extend
join
project
union

) on SHA256

|  Timestamp, FileName, SHA256, DeviceName, DeviceId,

extend
join
project
union

NetworkMessageId, SenderFromAddress, RecipientEmailAddress

Answer:

Answer Area

```
EmailAttachmentInfo
```

```
| where SenderFromAddress =~ "MaliciousSender@example.com"
```

```
| where isnotempty (SHA256)
```

```
| ▼ (
```

extend
join
project
union

```
DeviceFileEvents
```

```
| ▼ FileName, SHA256
```

extend
join
project
union

```
) on SHA256
```

```
| ▼ ▼ Timestamp, FileName, SHA256, DeviceName, DeviceId,
```

extend
join
project
union

```
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Section: Hotspot

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o365-worldwide>

QUESTION 8

You have the following advanced hunting query in Microsoft 365 Defender:

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

Which two actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a detection rule.
- B. Create a suppression rule.
- C. Add | order by Timestamp to the query.
- D. Replace DeviceProcessEvents with DeviceNetworkEvents.
- E. Add DeviceId and ReportId to the output of the query.

Answer: AE

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules>

QUESTION 9

You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices.

Which three actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group.
- B. Add the device users to the admin role.
- C. Add a tag to the machines.
- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.

F. Create a new device group that has a rank of 4.

Answer: ADE

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://www.drware.com/how-to-use-tagging-effectively-in-microsoft-defender-for-endpoint-part-1/>

QUESTION 10

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Entity tags, you add the accounts as Honeytoken accounts.

Does this meet the goal?

A. Yes

B. No

Answer: A

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 11

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Azure Identity Protection, you configure the sign-in risk policy.

Does this meet the goal?

A. Yes

B. No

Answer: B

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 12

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 13

HOTSPOT

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Exhibit\Security Center tab.)

Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Exhibit\Policies tab.)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input checked="" type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input checked="" type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input checked="" type="radio"/>	<input type="radio"/>

Section: Hotspot

Explanation/Reference:

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833>

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770>

QUESTION 14

DRAG DROP

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your

environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

Which three actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

Answer Area

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

From Advanced hunting, search for CveId in the DeviceTvmSoftwareInventoryVulnerabilitites table.

Create the remediation request.

Select **Security recommendations**.



Answer:

Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Advanced hunting, search for CveId in the
DeviceTvmSoftwareInventoryVulnerabilitites
table.

Answer Area

From Threat & Vulnerability Manager
Weaknesses, and search for the C

Select **Security recommendations**

Create the remediation request.

Section: Drag & Drop

Explanation/Reference:

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271>

QUESTION 15

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 16

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue.

The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

- A. Modify the access control settings for the key vault.
- B. Enable the Key Vault firewall.
- C. Create an application security group.
- D. Modify the access policy for the key vault.

Answer: B

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage>

QUESTION 17

HOTSPOT

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

You need to test LA1 in Security Center.

What should you do?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Set the LA1 trigger to:

- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

- ▼
- Recommendations
- Workflow automation

Answer:

Answer Area

Set the LA1 trigger to:

- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

- ▼
- Recommendations
- Workflow automation

Section: Hotspot

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run>

QUESTION 18

You have a Microsoft 365 subscription that uses Azure Defender.

You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender.

The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

- A. the Security Reader role for the subscription
- B. the Contributor for the subscription
- C. the Contributor role for RG1
- D. the Owner role for RG1

Answer: C

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

QUESTION 19

You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. cp /bin/echo ./asc_alerttest_662jfi039n
- B. ./alerttest testing eicar pipe
- C. cp /bin/echo ./alerttest
- D. ./asc_alerttest_662jfi039n testing eicar pipe

Answer: AD

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux>

QUESTION 20

You create an Azure subscription named sub1.

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

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

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

What should you do?

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

Answer: A

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

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

QUESTION 21

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.

Select and Place:

Actions

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.

Answer Area



Answer:

Actions

Change the alert severity threshold for emails to **Medium**.

Answer Area

Enable Azure Defender for the subscription.

Change the alert severity threshold for emails to **Low**.



Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N

Rename the executable file as AlertTest.exe.

Run the executable file and specify the appropriate arguments.

Section: Drag & Drop

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation>

QUESTION 22

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does **NOT** receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Security solutions
- B. Security policy
- C. Pricing & settings
- D. Security alerts
- E. Azure Defender

Answer: C

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

QUESTION 23

DRAG DROP

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions?

To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

Enable Security Health Analytics.

From Azure Security Center, add cloud connectors.

Configure the GCP Security Command Center.

Create a dedicated service account and a private key.

Enable the GCP Security Command Center API.

Answer Area



Answer:

Actions

Answer Area

Configure the GCP Security Command Center.

Enable Security Health Analytics.



Enable the GCP Security Command Center API.

Create a dedicated service account and a private key.

From Azure Security Center, add cloud connectors.

Section: Drag & Drop

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp>

QUESTION 24

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Section: Multiple Choice

Explanation/Reference:**Explanation:****Reference:**

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 25

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Section: Multiple Choice

Explanation/Reference:**Explanation:****Reference:**

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 26

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart.

What should you include in the query?

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

Answer: B

Section: Multiple Choice

Explanation/Reference:**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries>

QUESTION 27

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

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

Answer: AB

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

QUESTION 28

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

Answer: A

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

QUESTION 29

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

Answer: C

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations>

QUESTION 30

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated.

Which two actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a livestream
- B. Add a data connector
- C. Create an analytics rule
- D. Create a hunting query.
- E. Create a bookmark.

Answer: BD

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/livestream>

QUESTION 31

DRAG DROP

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

Which three actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Answer Area



Answer:

Actions

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Answer Area

Download and install the Log Analytics agent.



Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Section: Drag & Drop

Explanation/Reference:**Explanation:****Reference:**

<https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog>

QUESTION 32**HOTSPOT**

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit:



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If you hover over the virtual machine named vm1, you can view [answer choice].

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select [answer choice], you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

Answer:

Answer Area

If you hover over the virtual machine named vm1, you can view [answer choice].

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select [answer choice], you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

Section: Hotspot

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive>

QUESTION 33

DRAG DROP

You have an Azure Sentinel deployment.

You need to query for all suspicious credential access activities.

Which three actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions	Answer Area
From Azure Sentinel, select Hunting .	
Select Run All Queries .	
Select New Query .	
Filter by tactics.	
From Azure Sentinel, select Notebooks .	

Answer:

Actions	Answer Area
	From Azure Sentinel, select Hunting .
Select New Query .	
From Azure Sentinel, select Notebooks .	Filter by tactics.
	Select Run All Queries .

Section: Drag & Drop

Explanation/Reference:

Explanation:

Reference:

<https://davemccollough.com/2020/11/28/threat-hunting-with-azure-sentinel/>

QUESTION 34

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.

You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel.

What should you do first?

- A. Add a new scheduled query rule.
- B. Add a data connector to Azure Sentinel.
- C. Configure a custom Threat Intelligence connector in Azure Sentinel.
- D. Modify the trigger in the logic app.

Answer: B

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

QUESTION 35

Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.

A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.

You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.

What should you include in the recommendation?

- A. built-in queries
- B. livestream
- C. notebooks
- D. bookmarks

Answer: C

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

QUESTION 36

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a parameter and modify the trigger.
- B. Add a custom data connector and modify the trigger.
- C. Add a condition and modify the action.
- D. Add a parameter and modify the action.

Answer: D

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/>

QUESTION 37

You provision Azure Sentinel for a new Azure subscription.

You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query:

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated)
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents?

Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. user
- B. resource group
- C. IP address
- D. computer

Answer: CD

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

QUESTION 38

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add the Security Events connector to the Azure Sentinel workspace.
- B. Create a query that uses the workspace expression and the union operator.
- C. Use the alias statement.
- D. Create a query that uses the resource expression and the alias operator.
- E. Add the Azure Sentinel solution to each workspace.

Answer: BE

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

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

QUESTION 39

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal.

From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Answer: D

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand>

QUESTION 40

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

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

- A. There are connectivity issues between the data sources and Log Analytics.
- B. The number of alerts exceeded 10,000 within two minutes.
- C. The rule query takes too long to run and times out.
- D. Permissions to one of the data sources of the rule query were modified.

Answer: D

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

QUESTION 41

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel.

You need to resolve the issue for the analyst. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

- A. Azure Sentinel Responder
- B. Logic App Contributor
- C. Azure Sentinel Contributor
- D. Azure Sentinel Reader

Answer: A

Section: Multiple Choice

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

QUESTION 42

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

Case Study Title (Case Study):

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the

case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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
```

- A. executive
- B. sales
- C. marketing

Answer: B

Section: Case Study - Contoso Ltd

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios>

QUESTION 43

The issue for which team can be resolved by using Microsoft Defender for Office 365?

Case Study Title (Case Study):

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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
```

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

Answer: B

Section: Case Study - Contoso Ltd

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide>

QUESTION 44

You need to implement the Azure Information Protection requirements.

What should you configure first?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

- 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

Section: Case Study - Litware Inc.

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview>

QUESTION 45

You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements.

Which policy should you modify?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

- A. Activity from suspicious IP addresses
- B. Activity from anonymous IP addresses
- C. Impossible travel
- D. Risky sign-in

Answer: C

Section: Case Study - Litware Inc.

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

QUESTION 46

HOTSPOT

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

Answer:

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.**

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.**
- Modify the network security groups (NSGs).

Section: Case Study - Contoso Ltd

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

QUESTION 47

You need to recommend a solution to meet the technical requirements for the Azure virtual machines.

What should you include in the recommendation?

Case Study Title (Case Study):

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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
```

- A. just-in-time (JIT) access
- B. Azure Defender
- C. Azure Firewall
- D. Azure Application Gateway

Answer: B

Section: Case Study - Contoso Ltd

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/azure-defender>

QUESTION 48**HOTSPOT**

You need to create an advanced hunting query to investigate the executive team issue. How should you complete the query? To answer, select the appropriate options in the answer area.

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)  
  
| summarize activityCount =  
  by FolderPath, FileName,  
  ActionType, AccountDisplayName  
  
| where activityCount > 5
```

avg()
count()
sum()

Answer:

Answer Area

CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)  
  
| summarize activityCount =  
  by FolderPath, FileName,  
  ActionType, AccountDisplayName  
  
| where activityCount > 5
```

avg()
count()
sum()

Section: Case Study - Contoso Ltd

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

QUESTION 49

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.

Which role should you assign?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

- A. Automation Operator
- B. Automation Runbook Operator
- C. Azure Sentinel Contributor
- D. Logic App Contributor

Answer: C

Section: Case Study - Litware Inc.

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

QUESTION 50

You need to create the test rule to meet the Azure Sentinel requirements.

What should you do when you create the rule?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

- A. From Set rule logic, turn off suppression.
- B. From Analytics rule details, configure the tactics.
- C. From Set rule logic, map the entities.
- D. From Analytics rule details, configure the severity.

Answer: C

Section: Case Study - Litware Inc.

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

QUESTION 51

HOTSPOT

You need to create the analytics rule to meet the Azure Sentinel requirements.

What should you do?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:

Diagnostics settings
A service principal
A trigger

Answer:

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:

Diagnostics settings
A service principal
A trigger

Section: Case Study - Litware Inc.

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#set-automated-responses-and-create-the-rule>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Exam SC-200: Microsoft Security Operations Analyst

Skills measured

- The content of this exam will be updated on July 23, 2021.
- Mitigate threats using Microsoft 365 Defender (25-30%)
- Mitigate threats using Azure Defender (25-30%)
- Mitigate threats using Azure Sentinel (40-45%)

Exam SC-200 Compiled by DrunkMonk July 2021



Sections

1. Multiple Choice
2. Hotspot
3. Drag & Drop
4. Case Study - Contoso Ltd
5. Case Study - Litware Inc.

Exam A

QUESTION 1 DRAG DROP

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFO Laptop, CEO Laptop, and COOL Laptop.

How should you complete the query?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Select and Place:

Select and Place:

Values

Answer Area

```
| project LogonFailures=count()
```

```
| summarize LogonFailures=count()  
by DeviceName, LogonType
```

```
| where ActionType ==  
FailureReason
```

```
| where DeviceName in ("CFO Laptop,  
"CEO Laptop", "COOL Laptop")
```

```
ActionType == "LogonFailed"
```

and

Correct Answer:

Values

Answer Area

```
| where DeviceName in ("CFO Laptop",
"CEO Laptop", "COO Laptop")

| where ActionType == "LogonFailed"

| summarize LogonFailures=count() and
by DeviceName, LogonType

| where ActionType ==
FailureReason

| project LogonFailures=count()
```

Section: Drag & Drop Explanation

Explanation/Reference: Explanation:

Reference:

<https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/General%20queries/Failed%20Logon%20Attempt.txt>

QUESTION 2

You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.

Which anomaly detection policy should you use?

- A. Impossible travel
- B. Activity from anonymous IP addresses
- C. Activity from infrequent country

D. Malware detection

Correct Answer: C

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

QUESTION 3

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.

You need to create a data loss prevention (DLP) policy to protect the sensitive documents.

What should you use to detect which documents are sensitive?

- A. SharePoint search
- B. a hunting query in Microsoft 365 Defender
- C. Azure Information Protection
- D. RegEx pattern matching

Correct Answer: C

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection>

QUESTION 4

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.

You need to identify which Office VBA macros might be affected.

Which two commands can you run to achieve the goal?

Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`
- B. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`
- C. `Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode`
- D. `Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled`

Correct Answer: BC

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction>

QUESTION 5

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.

- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Correct Answer: BCE

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts>

QUESTION 6

DRAG DROP

You open the Cloud App Security portal as shown in the following exhibit:

The screenshot shows the Cloud Discovery - Cloud App Security interface. The left sidebar has sections for Dashboard, Discover (Cloud Discovery dashboard, Discovered apps, Discovered resources, IP addresses, Users), Investigate (Cloud app catalog, Create snapshot report), Control (Investigate, Control, Alerts), and Alerts. The main area has tabs for Dashboard, Discovered apps (selected), IP addresses, and Users. It includes a 'Snapshot report' section with a timeframe of 'Last 90 days'. Below is a search bar and a table titled 'APPS' with columns: APP TAG, RISK SCORE, COMPLIANCE RISK FACTOR, SECURITY RISK FACTOR, App, Score, Traffic, Upload Transac., Users, IP addr..., Last se..., Actions. The table lists several apps:

App	Score	Traffic	Upload Transac.	Users	IP addr...	Last se...	Actions
Applied Innovations Hosting services	1	866 KB	-	12	11	8	Apr 20, ...
StatusCake Website monitoring	1	939 KB	-	13	13	7	Apr 20, ...
Usersnap Productivity	1	1 MB	-	15	15	10	Apr 20, ...
CopperEgg Website monitoring	1	866 KB	-	12	12	8	Apr 20, ...
Launchpad Code-hosting	1	939 KB	-	13	13	7	Apr 20, ...

You need to remediate the risk for the Launchpad app.

Which four actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place

Select and Place:

Actions

Tag the app as **Unsanctioned**.

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Select the app.

Tag the app as **Sanctioned**.

Generate a block script.

Answer Area



Correct Answer:

Actions

Answer Area

Select the app.

Tag the app as **Unsanctioned**.

Generate a block script.

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Tag the app as **Sanctioned**.

Section: Drag & Drop
Explanation

Explanation/Reference:
Explanation:

Reference:
<https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery>

QUESTION 7
HOTSPOT

You have a Microsoft 365 E5 subscription.

You plan to perform cross-domain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment.

How should you complete the query?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Hot Area:

Answer Area

```
EmailAttachmentInfo
```

```
| where SenderFromAddress =~ "MaliciousSender@example.com"
```

```
| where isnotempty (SHA256)
```

```
|  
|  
| extend  
| join  
| project  
| union  
(
```

```
DeviceFileEvents
```

```
|  
|  
| File Name, SHA256  
| extend  
| join  
| project  
| union
```

```
) on SHA256
```

```
|  
|  
| Timestamp, FileName, SHA256, DeviceName, DeviceId,  
| extend  
| join  
| project  
| union
```

```
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Correct Answer:

Answer Area

```
EmailAttachmentInfo
```

```
| where SenderFromAddress =~ "MaliciousSender@example.com"
```

```
| where isnotempty (SHA256)
```

```
|  
|  
| extend  
| join  
| project  
| union  
|  
(
```

```
DeviceFileEvents
```

```
|  
|  
| File Name, SHA256  
| extend  
| join  
| project  
| union  
|  
)
```

```
on SHA256
```

```
|  
|  
| Timestamp, FileName, SHA256, DeviceName, DeviceId,  
| extend  
| join  
| project  
| union  
|  
)
```

```
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Section: Hotspot

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o365-worldwide>

QUESTION 8

You have the following advanced hunting query in Microsoft 365 Defender:

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

Which two actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a detection rule.
- B. Create a suppression rule.
- C. Add | order by Timestamp to the query.
- D. Replace DeviceProcessEvents with DeviceNetworkEvents.
- E. Add DeviceId and ReportId to the output of the query.

Correct Answer: AE

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules>

QUESTION 9

You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices.

Which three actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group.
- B. Add the device users to the admin role.
- C. Add a tag to the machines.
- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.
- F. Create a new device group that has a rank of 4.

Correct Answer: ACD

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access>

QUESTION 10

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Entity tags, you add the accounts as Honeytoken accounts.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 11

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Azure Identity Protection, you configure the sign-in risk policy.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 12

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 Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: Multiple Choice

Explanation:

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

QUESTION 13

HOTSPOT

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Exhibit\Security Center tab.)
Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Exhibit\Policies tab.)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Security Center (exhibit):

Secure Score



66% (~30 of 45 points)

Recommendations status



5 completed control

10 Total



16 completed recommendations

21 Total

Resource health



Unhealthy

2

Healthy

1

Not applicable

2

Resource exemption (preview)

< Now you can exempt irrelevant resources so they do not affect your secure score. >

[Learn more](#)

Each security control below represents a security risk you should mitigate.

Address the recommendations in each control, focusing on the controls worth the most points.

To get the max score, fix all recommendations for all resources in a control. [Learn more](#) >
Control status: **2 Selected** Recommendation status: **2 Selected**

Recommendation maturity: All Resource type: All Quick fix available: All

Contains exemptions: All

[Reset](#)Group by controls:
 filters

On

Controls	Potential score increase	Unhealthy resources	Resource Health
> Restrict unauthorized network access	+9% (4 points)	2 of 2 resources	
> Secure management ports	+9% (4 points)	1 of 2 resources	
> Enable encryption at rest	+9% (4 points)	2 of 2 resources	
> Remediate security configurations	+4% (2 points)	1 of 2 resources	
> Apply adaptive application control	+3% (2 points)	1 of 2 resources	
> Apply system updates	+0% (0 points)	None	
> Enable endpoint protection	+0% (0 points)	None	
> Remediate vulnerabilities	+0% (0 points)	None	
> Implement security best practices	+0% (0 points)	None	
> Enable MFA	+0% (0 points)	None	
> Manage access and permissions	+0% (0 points)	None	

Policies (exhibit):

Home > Policy

Policy - Compliance

Search (Ctrl+ /) «

Assign policy Assign initiative Refresh

Scope Microsoft Azure Type All definition types Compliance state All compliance states Search Filter by name or id...

Overall resource compliance 100%

Resources by compliance state 0

Non-compliant initiatives 0 out of 0

0 - Compliant
0 - Exempt
1 - Non-compliant
0 - Conflicting

Non-compliant policies 0 out of 0

Name ↑↓ Scope ↑↓ Compliance ↑↓ Resource compliance
No assignments to display within the given scope ↑↓ Non-Compliant Resources ↑↓ Non-compliant policies

Assignments Definitions Exemptions

Blueprints (preview) Resource Graph User privacy

Hot Area:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input checked="" type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input checked="" type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input checked="" type="radio"/>	<input type="radio"/>

Section: Hotspot
Explanation:

Explanation/Reference:
Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833>

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770>

QUESTION 14
DRAG DROP

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

Which three actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Select and Place:

Actions

Answer Area

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

From Advanced hunting, search for CveId in the DeviceTvmSoftwareInventoryVulnerabilitites table.

Create the remediation request.

Select **Security recommendations**.



Correct Answer:

Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Advanced hunting, search for CveId in the
DeviceTvmSoftwareInventoryVulnerabilitites
table.

Answer Area

From Threat & Vulnerability Management, select
Weaknesses, and search for the CVE.

Select **Security recommendations**.

Create the remediation request.

Section: Drag & Drop
Explanation:

Explanation/Reference:
Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271>

QUESTION 15

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 16

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue.

The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

- A. Modify the access control settings for the key vault.
- B. Enable the Key Vault firewall.

- C. Create an application security group.
- D. Modify the access policy for the key vault.

Correct Answer: B

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage>

QUESTION 17

HOTSPOT

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

You need to test LA1 in Security Center.

What should you do?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Hot Area:

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations
Workflow automation

Correct Answer:

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered
When an Azure Security Center Alert is created or triggered
When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations
Workflow automation

Section: Hotspot
Explanation

Explanation/Reference:
Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run>

QUESTION 18

You have a Microsoft 365 subscription that uses Azure Defender.

You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender.

The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

- A. the Security Reader role for the subscription
- B. the Contributor for the subscription
- C. the Contributor role for RG1
- D. the Owner role for RG1

Correct Answer: C

Section: Multiple Choice

Explanation:

Explanation/Reference:

Explanation:

Reference:

QUESTION 19

You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. cp /bin/echo ./asc_alerttest_662jfi039n
- B. ./alerttest testing eicar pipe

- C. cp /bin/echo ./alerttest
- D. ./asc_alerttest_662jfi039n testing eicar pipe

Correct Answer: AD

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

[https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux-](https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux)

QUESTION 20

You create an Azure subscription named sub1.

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

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

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

What should you do?

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

Correct Answer: A

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

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

QUESTION 21

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.

Select and Place:

Select and Place:

Actions

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.

Answer Area



Correct Answer:

Actions

Change the alert severity threshold for emails to **Medium**.

Answer Area

Enable Azure Defender for the subscription.

Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.



Run the executable file and specify the appropriate arguments.



Change the alert severity threshold for emails to **Low**.

Rename the executable file as AlertTest.exe.

Section: Drag & Drop
Explanation:

Explanation/Reference:
Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation>

QUESTION 22

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does **NOT** receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Security solutions
- B. Security policy
- C. Pricing & settings
- D. Security alerts
- E. Azure Defender

Correct Answer: C

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

QUESTION 23

DRAG DROP

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions?

To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Select and Place:

Actions

Answer Area

Enable Security Health Analytics.

From Azure Security Center, add cloud connectors.

Configure the GCP Security Command Center.

Create a dedicated service account and a private key.

Enable the GCP Security Command Center API.



Correct Answer:

Actions

Answer Area

Configure the GCP Security Command Center.

Enable Security Health Analytics.



Enable the GCP Security Command Center API.

Create a dedicated service account and a private key.

From Azure Security Center, add cloud connectors.



Section: Drag & Drop
Explanation

Explanation/Reference:
Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp>

QUESTION 24

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 25

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts>

QUESTION 26

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart.

What should you include in the query?

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

Correct Answer: B

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries>

QUESTION 27

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

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. Add a playbook.
- B. Associate a playbook to an incident.
- C. Enable Entity behavior analytics.

- D. Create a workbook.
- E. Enable the Fusion rule.

Correct Answer: AB

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

QUESTION 28

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

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

QUESTION 29

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

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations>

QUESTION 30

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated.

Which two actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a livestream
- B. Add a data connector
- C. Create an analytics rule
- D. Create a hunting query.
- E. Create a bookmark.

Correct Answer: BD

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/livestream>

QUESTION 31

DRAG DROP

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

Which three actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Select and Place:

Actions

Answer Area

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.



Correct Answer:

Actions

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Answer Area

Download and install the Log Analytics agent.



Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.



Section: Drag & Drop

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog>

QUESTION 32

HOTSPOT

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit:



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Hot Area:

Answer Area

If you hover over the virtual machine named vm1, you can view [answer choice].

the inbound network security group (NSG) rules
the last five Windows security log events
the open ports on the host
the running processes

If you select [answer choice], you can navigate to the bookmarks related to the incident.

Entities
Info
Insights
Timeline

Correct Answer:

Answer Area

If you hover over the virtual machine named vm1, you can view [answer choice].

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select [answer choice], you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

Section: Hotspot

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive>

QUESTION 33

DRAG DROP

You have an Azure Sentinel deployment.

You need to query for all suspicious credential access activities.

Which three actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Select and Place:

Actions

Answer Area

From Azure Sentinel, select **Hunting**.

Select **Run All Queries**.

Select **New Query**.

Filter by tactics.

From Azure Sentinel, select **Notebooks**.



Correct Answer:

Actions

Answer Area

From Azure Sentinel, select **Hunting**.

Select **New Query**.

Filter by tactics.

Select **Run All Queries**.

From Azure Sentinel, select **Notebooks**.

Section: Drag & Drop
Explanation

Explanation/Reference:

Explanation:

Reference:

<https://davemccollough.com/2020/11/28/threat-hunting-with-azure-sentinel/>

QUESTION 34

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually. You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel.

What should you do first?

- A. Add a new scheduled query rule.
- B. Add a data connector to Azure Sentinel.
- C. Configure a custom Threat Intelligence connector in Azure Sentinel.
- D. Modify the trigger in the logic app.

Correct Answer: B

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

QUESTION 35

Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.

A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.

You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.

What should you include in the recommendation?

- A. built-in queries
- B. livestream

- C. notebooks
- D. bookmarks

Correct Answer: C

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

QUESTION 36

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a parameter and modify the trigger.
- B. Add a custom data connector and modify the trigger.
- C. Add a condition and modify the action.
- D. Add a parameter and modify the action.

Correct Answer: D

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/>

QUESTION 37

You provision Azure Sentinel for a new Azure subscription.

You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query:

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents?

Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. user
- B. resource group
- C. IP address
- D. computer

Correct Answer: CD

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://azsec.azurewebsites.net/2020/02/24/alert-grouping-feature-in-azure-sentinel/>

QUESTION 38

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform?

Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add the Security Events connector to the Azure Sentinel workspace.
- B. Create a query that uses the workspace expression and the union operator.
- C. Use the alias statement.
- D. Create a query that uses the resource expression and the alias operator.
- E. Add the Azure Sentinel solution to each workspace.

Correct Answer: BE

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

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

QUESTION 39

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal.

From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Correct Answer: D

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand>

QUESTION 40

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

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED. What is a possible cause of the issue?

- A. There are connectivity issues between the data sources and Log Analytics.
- B. The number of alerts exceeded 10,000 within two minutes.
- C. The rule query takes too long to run and times out.
- D. Permissions to one of the data sources of the rule query were modified.

Correct Answer: D

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#issue-a-scheduled-rule-failed-to-execute-or-appears-with-auto-disabled-added-to-the-name>

QUESTION 41

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel.

You need to resolve the issue for the analyst. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

- A. Azure Sentinel Responder
- B. Logic App Contributor
- C. Azure Sentinel Contributor
- D. Azure Sentinel Reader

Correct Answer: A

Section: Multiple Choice

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles#roles-for-working-in-azure-sentinel>

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

QUESTION 42

You create an Azure subscription named sub1.

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

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

You need to collect security event logs from the Azure virtual machines that report to workspace1

What should you do?

- A. In workspace 1, create a workbook.
- B. From Security Center, enable data collection
- C. From Security Center, create a workflow automation.
- D. In sub1, register a provider.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 43

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 resource level
- B. at the subscription level

C. at the workspace level

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 44

You are responsible for responding to Azure Defender for Key vault alerts.

During an investigation of an alert, you discover unauthorized attempts to access a key vault from a for exit node.

What should you configure to mitigate the threat?

- A. the access policy settings of the key vault
- B. role - based access control (RBAC) for the key vault
- C. Azure Active Directory (Azure AD) permissions
- D. Key Vault firewalls and virtual networks.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 45

You receive a security bulletin about a potential attack that uses an image file.

You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.

Which indicator type should you use?

- A. a URL / domain indicator that has Action set to Alert and block
- B. a certificate indicator that has Action set to Alert and block

- C. a URL / domain indicator that has Action set to Alert only
- D. a file hash indicator that has Action set to Alert and block

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 46

Your company deploys the following services:

- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365

You need to provide a security analyst with the ability to use the Microsoft 365 security center.

The analyst must be able to approve and reject pending actions generated by Defender for Endpoint.

The solution must use the principle of least privilege.

Which two roles should you assign to the analyst?

Each correct answer presents part of the solution

NOTE: Each correct selection is worth one point.

- A. the Security Reader role in Azure Active Directory (Azure AD)
- B. the Security Administrator role in Azure Active Directory (Azure AD)
- C. the Active remediation actions role in Microsoft Defender for Endpoint
- D. the Compliance Data Administrator in Azure Active Directory (Azure AD)

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 47

You implement Safe Attachments policies in Microsoft Defender for Office 365.

Users report that email messages containing attachments take longer than expected to be received.

You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security.

The attachments must be scanned for messages that contain malware must be blocked.

What should you configure in the Safe Attachments policies?

- A. Replace
- B. Monitor and Enable redirect
- C. Dynamic Delivery
- D. Block and Enable redirect

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 48

You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled. You need to ensure that the Fusion rule can generate alerts.

What should you do?

- A. Add a hunting bookmark.
- B. Create a new machine learning analytics rule.
- C. Disable, and then enable the rule
- D. Add data connectors.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 49

You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region.

You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.

What should you do first?

- A. Create a data connector in Azure Sentinel.
- B. Add Azure Sentinel to a workspace
- C. Deploy Azure Data Catalog to the West US Azure region.
- D. Modify the workspace settings of the existing Azure Sentinel deployment.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 50

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. Permissions to the data sources of the rule query were modified.
- C. The target workspace was deleted
- D. There are connectivity issues between the data sources and Log Analytics

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 51

You have a third - party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign - in events in near real time.

What should you do to route events to the SIEM solution?

- A. Configure the Diagnostics settings in Azure AD to archive to a storage account.
- B. Create an Azure Sentinel workspace that has a Security Events connector.
- C. Configure the Diagnostics settings in Azure AD to stream to an event hub.
- D. Create an Azure Sentinel workspace that has an Azure Active Directory connector.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 52

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for Identity portal, you need to configure several accounts for attacker Solution: You add each account as a Sensitive account.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference:

QUESTION 53

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

Case Study Title (Case Study):

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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

- A. executive
- B. sales
- C. marketing

Correct Answer: B

Section: Case Study - Contoso Ltd

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios>

QUESTION 54

The issue for which team can be resolved by using Microsoft Defender for Office 365?

Case Study Title (Case Study):

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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

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

Correct Answer: B

Section: Case Study - Contoso Ltd

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide>

QUESTION 55

You need to implement the Azure Information Protection requirements.

What should you configure first?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

- 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

Correct Answer: D

Section: Case Study - Litware Inc.

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview>

QUESTION 56

You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements.

Which policy should you modify?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the

other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

A. Activity from suspicious IP addresses

- B. Activity from anonymous IP addresses
- C. Impossible travel
- D. Risky sign-in

Correct Answer: C

Section: Case Study - Litware Inc.

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

QUESTION 57

Case Study - Click the exhibit tab

HOTSPOT

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

What should you recommend for each threat?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Exhibit:

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. You can also use the back and forward buttons in the browser to move between the different problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Next button.

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, Boston, Chicago, Atlanta, and San Jose. 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 of its resources.

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 and which are false positives.

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 has experienced several incidents where sensitive files were lost or corrupted.

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 sensitive files were shared with unauthorized parties.

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 list of countries:

Hot Area:

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

Correct Answer:

Answer Area

Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

Section: Case Study - Contoso Ltd

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

QUESTION 58

You need to recommend a solution to meet the technical requirements for the Azure virtual machines.

What should you include in the recommendation?

Case Study Title (Case Study):

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain

exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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
```

- A. just-in-time (JIT) access
- B. Azure Defender
- C. Azure Firewall
- D. Azure Application Gateway

Correct Answer: B

Section: Case Study - Contoso Ltd

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/azure-defender>

QUESTION 59

Case Study - Click the exhibit tab

HOTSPOT

You need to create an advanced hunting query to investigate the executive team issue.

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

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Exhibit:

Introductory Info

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. You can also use the back and forward buttons in the browser to move between the different problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Next button.

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, Boston, Chicago, Atlanta, and San Jose. 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 of its resources.

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 and which are false positives.

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 has experienced several incidents where sensitive files were lost or corrupted.

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 sensitive files were shared with unauthorized parties.

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 list of countries:

Hot Area:

Answer Area

CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)  
  
| summarize activityCount =  
    by FolderPath, FileName,  
    ActionType, AccountDisplayName  
  
| where activityCount > 5
```

avg()
count()
sum()

Correct Answer:

Answer Area

CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)  
  
| summarize activityCount =  
    by FolderPath, FileName,  
    ActionType, AccountDisplayName  
  
| where activityCount > 5
```

avg()
count()
sum()

Section: Case Study - Contoso Ltd

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

QUESTION 60

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.

Which role should you assign?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the

other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

A. Automation Operator

- B. Automation Runbook Operator
- C. Azure Sentinel Contributor
- D. Logic App Contributor

Correct Answer: C

Section: Case Study - Litware Inc.

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

QUESTION 61

You need to create the test rule to meet the Azure Sentinel requirements.

What should you do when you create the rule?

Case Study Title (Case Study):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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.

- A. From Set rule logic, turn off suppression.
- B. From Analytics rule details, configure the tactics.
- C. From Set rule logic, map the entities.
- D. From Analytics rule details, configure the severity.

Correct Answer: C

Section: Case Study - Litware Inc.

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

QUESTION 62

Case Study - Click the exhibit tab

HOTSPOT

You need to create the analytics rule to meet the Azure Sentinel requirements.
What should you do?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Capture (exhibit):

Introductory Info

Case study:

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study:

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

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
------	------	-------------

Capture (exhibit):

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~~

Hot Area:

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:

Diagnostics settings
A service principal
A trigger

Correct Answer:

Answer Area

Create the rule of type:

Fusion
Microsoft incident creation
Scheduled

Configure the playbook to include:

Diagnostics settings
A service principal
A trigger

Section: Case Study - Litware Inc.

Explanation

Explanation/Reference:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#set-automated-responses-and-create-the-rule>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>