

SC-200.pre.exam.51q - DEMO

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



SC-200

Microsoft Security Operations Analyst



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 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>

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, CEOLaptop, 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.vceup.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.

VCEup

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

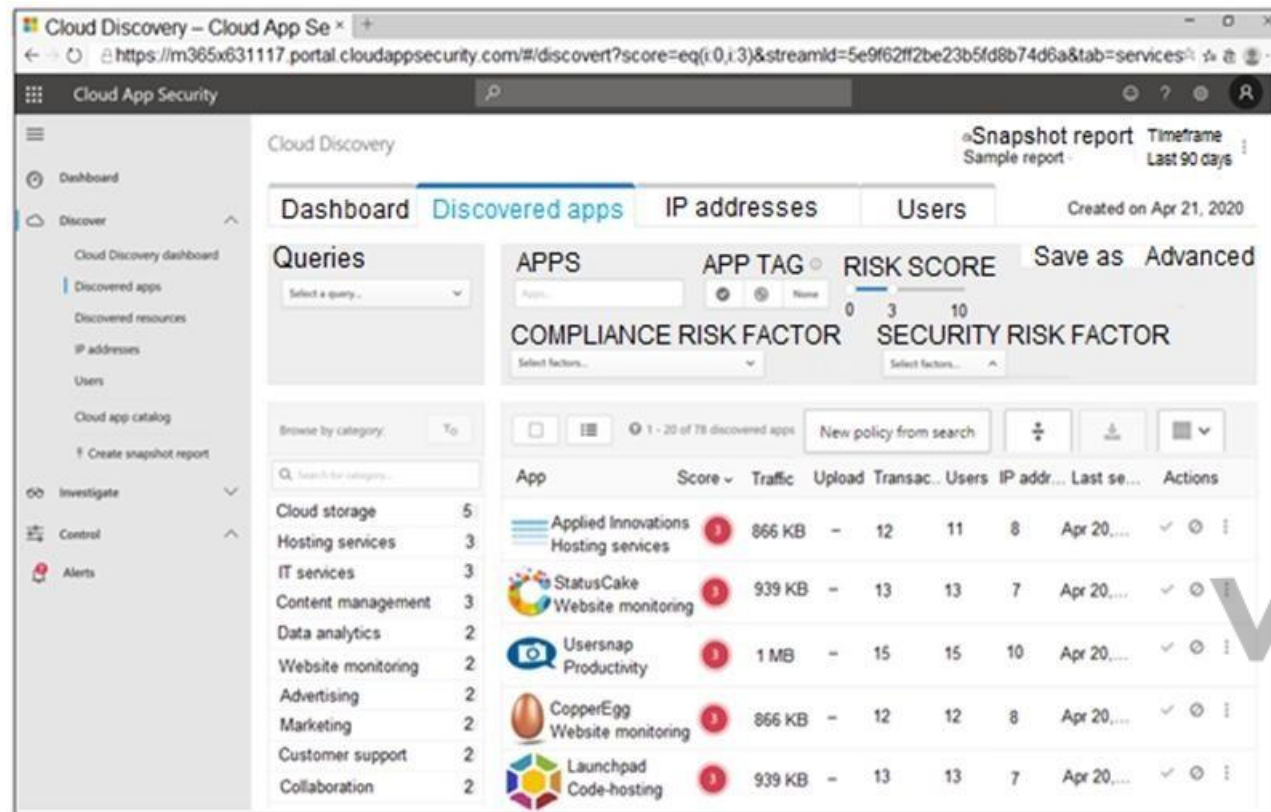
Explanation/Reference:

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.



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:	<div><div></div><div>Add resource locks to the key vault.</div><div>Modify the access policy settings for the key vault.</div><div>Modify the role-based access control (RBAC) settings for the key vault.</div></div>
External threat:	<div><div></div><div>Implement Azure Firewall.</div><div>Modify the Key Vault firewall settings.</div><div>Modify the network security groups (NSGs).</div></div>

Correct Answer:

Answer Area

Internal threat:	<div><div></div><div>Add resource locks to the key vault.</div><div>Modify the access policy settings for the key vault.</div><div>Modify the role-based access control (RBAC) settings for the key vault.</div></div>
External threat:	<div><div></div><div>Implement Azure Firewall.</div><div>Modify the Key Vault firewall settings.</div><div>Modify the network security groups (NSGs).</div></div>

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.)



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: ☒ On

Controls	Potential score increase	Unhealthy resources	Resource Health
> Restrict unauthorized network access	+9% (4 points)	2 of 2 resources	<div></div>
> Secure management ports	+9% (4 points)	1 of 2 resources	<div></div>
> Enable encryption at rest	+9% (4 points)	2 of 2 resources	<div></div>
> Remediate security configurations	+4% (2 points)	1 of 2 resources	<div></div>
> Apply adaptive application control	+3% (2 points)	1 of 2 resources	<div></div>
> Apply system updates Completed	+0% (0 points)	None	<div></div>
> Enable endpoint protection Completed	+0% (0 points)	None	<div></div>
> Remediate vulnerabilities Completed	+0% (0 points)	None	<div></div>
> Implement security best practices Completed	+0% (0 points)	None	<div></div>
> Enable MFA Completed	+0% (0 points)	None	<div></div>
> Manage access and permissions Completed	+0% (0 points)	None	<div></div>

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

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 - 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

Sort: Scope, Compliance, Resource compliance, 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_alertttest_662jfi039n`
- B. `./alertttest testing eicar pipe`
- C. `cp /bin/echo ./alertttest`
- D. `./asc_alertttest_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.	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.

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:

- 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: [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>

VCEup

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://davemcollough.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. 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: [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>