

# Microsoft Security Operations Analyst

## Microsoft SC-200 Dumps Available Here at:

<https://www.certification-questions.com/microsoft-exam/sc-200-dumps.html>

Enrolling now you will get access to 196 questions in a unique set of SC-200 dumps

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

### Question 1

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

**Options:**

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

**Answer: B**

**Explanation:**

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

Explanation:

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

### Question 2

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

**Options:**

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

**Answer: B**

**Explanation:**

<https://www.certification-questions.com>

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

Explanation:

**HOTSPOT for the Azure virtual**

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.

[PIC-2-2115240394]

**Question 3**

**HOTSPOT for the Azure virtual**

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.

**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).

**Options:**

A.

## 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: A**

**Explanation:**

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

Explanation:

You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

### Question 4

You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

**Options:**

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

**Answer: B**

**Explanation:**

Reference:

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

### 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.

[PIC-5-1838839195]

### Question 5

#### 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.

	▼
CloudAppEvents	
DeviceFileEvents	
DeviceProcessEvents	

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

```
| summarize activityCount = 

|         |   |
|---------|---|
|         | ▼ |
| avg()   |   |
| count() |   |
| sum()   |   |

 by FolderPath, FileName, ActionType, AccountDisplayName
```

```
| where activityCount > 5
```

Options:

A.

	▼
CloudAppEvents	
DeviceFileEvents	
DeviceProcessEvents	

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

```
| summarize activityCount = 

|         |   |
|---------|---|
|         | ▼ |
| avg()   |   |
| count() |   |
| sum()   |   |

 by FolderPath, FileName, ActionType, AccountDisplayName
```

```
| where activityCount > 5
```

**Answer: A**

You need to remediate active attacks to meet the technical requirements.  
What should you include in the solution?

**Question 6**

You need to remediate active attacks to meet the technical requirements.  
What should you include in the solution?

**Options:**

- A. Azure Automation runbooks
- B. Azure Logic Apps
- C. Azure Functions
- D. Azure Sentinel livestreams

**Answer: B**

**Explanation:**

<https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks>

Explanation:

**HOTSPOT**

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.

[PIC-6-3440576900]

**Question 7**

**HOTSPOT**

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.

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

	▼
0	
1	
2	
3	

Query element required to correlate data between tenants:

	▼
extend	
project	
workspace	

Options:

A.

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

	▼
0	
1	
2	
3	

Query element required to correlate data between tenants:

	▼
extend	
project	
workspace	

Answer: A

Explanation:

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

Explanation:

## TESTLET-2.

Litware inc.

### 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 8

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?

**Options:**

- A. Security alerts in Azure Security Center
- B. Activity log in Azure
- C. Azure Advisor
- D. the query windows of the Log Analytics workspace

**Answer: D**

TESTLET-2.

Litware inc.

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

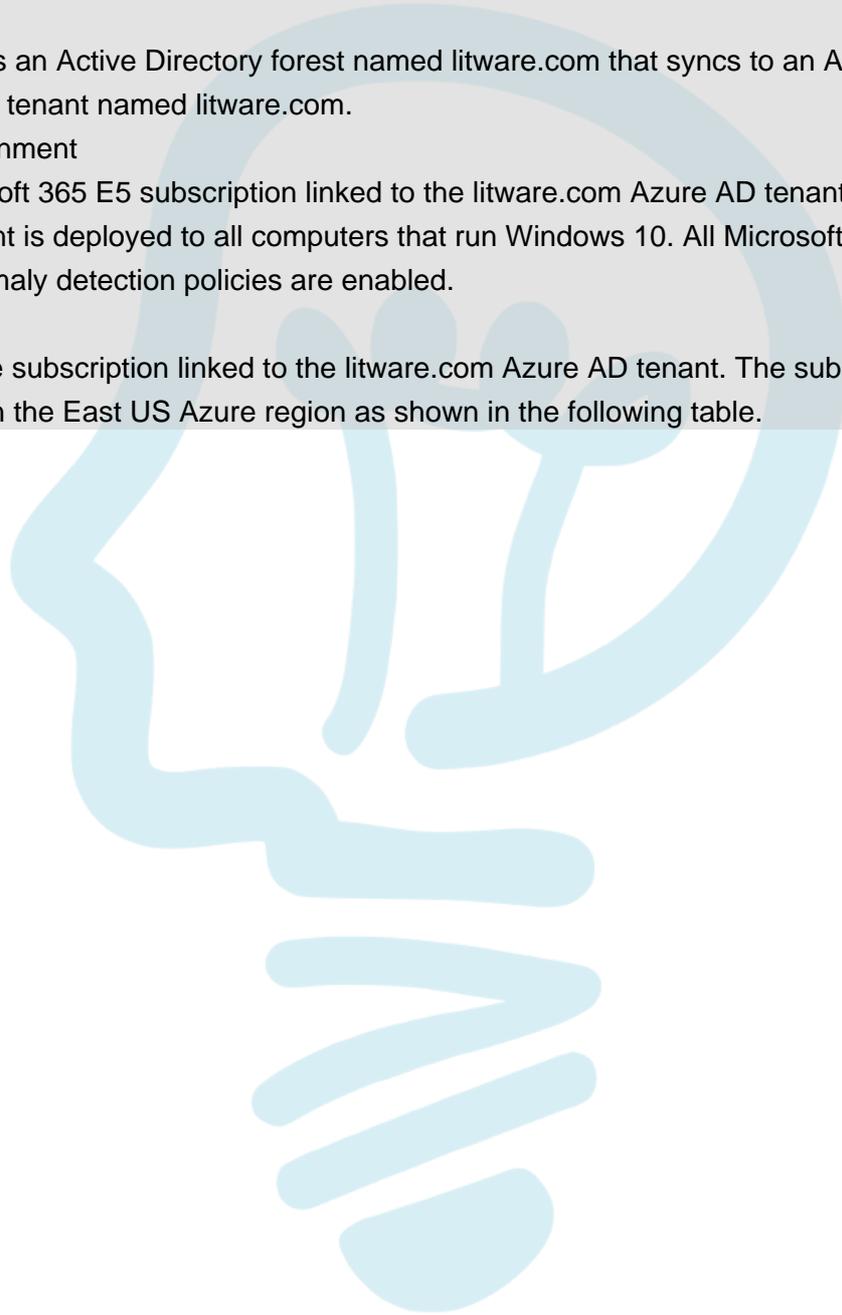
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

##### 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 9

You need to implement the Azure Information Protection requirements. What should you configure first?

### Options:

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

### Answer: D

### Explanation:

[microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview](https://microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview)

Explanation:

## TESTLET-2.

Litware inc.

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 10

You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements. Which policy should you modify?

### Options:

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

### Answer: C

### Explanation:

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

Explanation:

**Would you like to see more? Don't miss our SC-200 PDF file at:**

<https://www.certification-questions.com/microsoft-pdf/sc-200-pdf.html>