Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

SC-401 MCQs
SC-401 TestPrep
SC-401 Study Guide
SC-401 Practice Test
SC-401 Exam Questions

killexams.com

**Microsoft**

# SC-401

*Administering Information Security in Microsoft 365*

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/SC-401

**Question: 665**

A Defender for Cloud Apps file policy alert indicates a sensitive file was accessed from an unrecognized IP address. You need to investigate and respond to this alert. Which two steps should you take? (Select two.)

A. Apply a session policy to restrict access
B. Review the activity log in Defender for Cloud Apps
C. Suspend the user account
D. Update the file policy to include IP restrictions

Answer: A, B

Explanation: To investigate and respond to a Defender for Cloud Apps file policy alert, review the activity log in the Defender for Cloud Apps portal to understand the context of the access. Additionally, apply a session policy to restrict access from unrecognized IP addresses, preventing further unauthorized access. Suspending the user is too drastic without investigation, and updating the file policy is a long-term action, not immediate response.

**Question: 666**

Contoso, Ltd. must protect standard lease agreement forms containing lease IDs (format: LSE-123456). What is the best approach in Microsoft Purview?

A. Create a custom sensitive info type for lease IDs
B. Enable document fingerprinting for lease agreements
C. Train a classifier to detect lease agreements
D. Use the built-in sensitive info type for lease IDs

Answer: B

Explanation: Document fingerprinting is ideal for standard lease agreement forms with consistent structure, even with variable data like lease IDs. A digital fingerprint of the form template ensures accurate detection. Custom sensitive info types are less effective for form-based detection, and no built-in type exists for lease IDs. Classifiers are unnecessary for structured forms.

**Question: 667**

You are enabling just-in-time protection for a DLP policy to block sensitive data access on macOS devices. Which prerequisite must be met?

A. Enable advanced classification scanning in Endpoint DLP settings
B. Install KB5016688 on macOS devices

C. Configure a retention label with encryption
D. Set up a sensitive service domain group

Answer: A

Explanation: Just-in-time protection on macOS devices requires advanced classification scanning to be enabled in Endpoint DLP settings for real-time monitoring and blocking. KB5016688 is specific to Windows, retention labels protect content, and sensitive service domain groups restrict website access, not device-level protection.

**Question: 668**

You are managing roles and permissions for DSPM for AI in Microsoft Purview. A security analyst needs to monitor AI-related data risks but should not modify policies. Which role should you assign to the analyst?

A. Compliance Administrator
B. Compliance Data Administrator
C. Security Reader
D. Information Protection Analyst

Answer: D

Explanation: The Information Protection Analyst role in Microsoft Purview grants permissions to monitor data risks, view reports, and access DSPM for AI dashboards without the ability to modify policies. Compliance Administrator and Compliance Data Administrator roles include policy modification permissions, while Security Reader is too restrictive and not specific to DSPM for AI.

**Question: 669**

You are configuring a sensitivity label named "Board Meeting" for a Microsoft 365 E5 tenant. The label must prevent external sharing in Microsoft Teams and apply a footer with the text "BOARD MEETING - CONFIDENTIAL". Which settings should you configure in the Microsoft Purview Compliance Portal?

A. Enable external sharing, set footer text to "BOARD MEETING - CONFIDENTIAL", and apply to Exchange
B. Enable guest access, set watermark text to "BOARD MEETING - CONFIDENTIAL", and apply to SharePoint sites
C. Disable external sharing, set header text to "BOARD MEETING - CONFIDENTIAL", and apply to OneDrive
D. Disable external sharing, set footer text to "BOARD MEETING - CONFIDENTIAL", and apply to Teams containers

Answer: D

Explanation: To configure the "Board Meeting" label, disable external sharing in the Microsoft Purview Compliance Portal to prevent external access to Teams channels. Set the footer text to "BOARD MEETING - CONFIDENTIAL" and apply the label to Teams containers.

**Question: 670**

You are implementing information protection for Windows file shares. The Purview scanner must classify files containing tax IDs and apply the "Tax" label. Which PowerShell command configures this?

A. Set-ContentScanJob -Name "TaxScan" -SensitiveInfoType "Tax ID" -LabelId "Tax"
B. Set-AIPScannerConfiguration -ContentScanJob "TaxScan" -SensitiveInfoType "Tax ID" -Label "Tax"
C. New-ContentScanJob -Name "TaxScan" -SensitiveInfoTypeIds "Tax ID" -ApplyLabel "Tax"
D. New-AIPScannerContentScan -JobName "TaxScan" -SensitiveInfoType "Tax ID" -SensitivityLabel "Tax"

Answer: C

Explanation: The New-ContentScanJob cmdlet configures the Purview scanner for on-premises files. The -SensitiveInfoTypeIds parameter specifies the sensitive info type ("Tax ID"), and -ApplyLabel applies the "Tax" label.

**Question: 671**

You are using Content Explorer to monitor a sensitivity label "Private" applied to 600 files. You need to identify files with credit card numbers. Which filter and PowerShell cmdlet should you use?

A. Filter by "Private Label"; Get-LabelUsage
B. Filter by "Sensitive Info Type"; Get-ContentExplorerData
C. Filter by "Credit Card"; Get-ComplianceTag
D. Filter by "Content Type"; Get-SensitivityLabel

Answer: B

Explanation: In Content Explorer, the "Sensitive Info Type" filter identifies files with credit card numbers under the "Private" label. The Get-ContentExplorerData PowerShell cmdlet retrieves file metadata, including sensitive info types.

**Question: 672**

A legal firm needs a DLP policy to detect attorney-client privileged documents in SharePoint and block external sharing. The policy must use a custom SIT with a keyword list (e.g., "privileged," "confidential"). Which configuration is correct?

A. Custom SIT: Keywords > Create policy > Scope: SharePoint > Detect: Keyword SIT > Action: Prevent external sharing
B. Define keyword-based SIT > DLP policy > SharePoint location > Rule: Detect keywords > Restrict external access
C. New SIT with keyword list > Policy wizard > Select SharePoint > Condition: Keyword SIT > Block sharing externally
D. Create custom SIT with keywords > New DLP policy > Location: SharePoint > Condition: Custom SIT detected > Action: Block external sharing

Answer: D

Explanation: To detect privileged documents, a custom sensitive information type with a keyword list is created. The DLP policy is configured in Microsoft Purview by selecting SharePoint, setting the condition to detect the custom SIT, and blocking external sharing.

**Question: 673**

You are implementing JIT protection for a Microsoft 365 tenant to block access to OneDrive when excessive file downloads are detected. The policy must integrate with Insider Risk Management. What should you configure?

A. JIT protection in Microsoft Defender for Cloud Apps linked to Insider Risk Management
B. A DLP policy with a user override for OneDrive
C. A retention policy to limit OneDrive access
D. An adaptive scope to restrict OneDrive users

Answer: A

Explanation: JIT protection in Microsoft Defender for Cloud Apps, integrated with Insider Risk Management, dynamically blocks access to OneDrive based on risky behaviors like excessive downloads. DLP policies focus on data protection, retention policies manage retention, and adaptive scopes are for dynamic policy application, not real-time access control.

**Question: 674**

Your organization requires a retention policy to retain OneDrive files for 5 years after creation. Which PowerShell command creates this policy?

A. Set-RetentionComplianceRule -Policy "OneDriveRetention" -RetentionDuration 1825
B. New-RetentionCompliancePolicy -Name "OneDriveRetention" -SharePointLocation All -RetentionDuration 1825 -Enabled $true
C. Set-RetentionCompliancePolicy -Identity "OneDriveRetention" -RetentionDuration 1825
D. New-RetentionCompliancePolicy -Name "OneDriveRetention" -OneDriveLocation All -

RetentionDuration 1825 -Enabled $true

Answer: D

Explanation: To create a retention policy for OneDrive files for 5 years (1825 days), use the New-RetentionCompliancePolicy cmdlet with -OneDriveLocation All to target all OneDrive accounts, -RetentionDuration 1825 to set the retention period, and -Enabled $true to activate the policy. The other options target incorrect locations or modify existing policies.

**Question: 675**

Northwind Traders has a Microsoft 365 E5 tenant and needs to protect HR onboarding forms containing employee SSNs and internal IDs (format: EID-12345). What is the most efficient way to classify these forms in Microsoft Purview?

A. Use built-in sensitive info types for both SSNs and internal IDs
B. Enable document fingerprinting for onboarding forms
C. Train a classifier to detect onboarding forms
D. Combine built-in SSN type with a custom internal ID type

Answer: D

Explanation: The built-in sensitive info type for SSNs can be used directly. The internal ID (EID-\d{5}) requires a custom sensitive info type with a regular expression. Combining these in a policy ensures accurate classification. Document fingerprinting is less precise for dynamic IDs, and classifiers are less efficient for structured patterns.

**Question: 676**

You are monitoring Endpoint, including extensions, and the Microsoft Purview portal shows alerts for Endpoint DLP policy violations on Windows 11 devices. An alert indicates a user attempted to copy a file with a Social Security Number to a USB drive. Which dashboard should you check for detailed metadata, and what action can you take to investigate further?

A. Microsoft 365 Defender Portal; Run an Advanced Hunting query
B. DLP Alerts Management Dashboard; Perform a Content Search
C. Activity Explorer; Export audit logs
D. Endpoint DLP Settings; Configure file path exclusions

Answer: B

Explanation: The DLP Alerts Management Dashboard in the Microsoft Purview portal provides detailed metadata for Endpoint DLP policy violations, such as the sensitive info type (Social Security Number) and the action (copy to USB). To investigate further, you can perform a Content Search to locate the file

or related activities.

**Question: 677**

To protect AI service data, you need to ensure Copilot respects sensitivity labels with encryption. Which configuration should you implement?

A. Sensitivity labels with encryption denying EXTRACT rights
B. DLP policy for Copilot with sensitive info types
C. DSPM for AI to block Copilot access
D. Defender for Cloud Apps policy for Copilot

Answer: A

Explanation: Sensitivity labels with encryption denying EXTRACT rights ensure Copilot respects permissions.

**Question: 678**

At Trey Research, you are configuring an insider risk management policy in Microsoft Purview to detect data exfiltration. The policy must trigger alerts only when a user downloads more than 100 files from SharePoint within 24 hours and uploads them to an unapproved cloud service. Which configuration should you use?

A. Use adaptive protection to dynamically adjust the download threshold
B. Create a custom indicator with a PowerShell script to monitor file downloads and uploads
C. Configure a DLP policy to block uploads and link it to the insider risk policy
D. Set the policy threshold to 100 files and enable the “Upload to unapproved cloud” indicator

Answer: D

Explanation: In Microsoft Purview Insider Risk Management, configuring a policy with a threshold of 100 file downloads from SharePoint and enabling the “Upload to unapproved cloud” indicator ensures alerts are triggered only when both conditions are met within 24 hours. Custom indicators via PowerShell are not supported, DLP policies are separate, and adaptive protection adjusts risk levels, not thresholds.

**Question: 679**

A financial institution uses Microsoft 365 E5 and has a sensitivity label named "Financial Records" applied to documents in SharePoint. You need to configure the label to apply a footer with the text "CONFIDENTIAL - PROPERTY OF FINANCE DEPT" and enforce co-authoring restrictions to only the Finance department. Which PowerShell command should you use to achieve this?

A. Set-Label -Identity "Financial Records" -ContentMarking Footer -FooterText "CONFIDENTIAL - PROPERTY OF FINANCE DEPT" -EncryptionEnabled $false -EncryptionRightsUrl "FinanceDept"
B. New-Label -Name "Financial Records" -ContentMarking Header -HeaderText "CONFIDENTIAL - PROPERTY OF FINANCE DEPT" -EncryptionEnabled $true -EncryptionAipTemplateId "FinanceDept"
C. Set-Label -Identity "Financial Records" -ContentMarking Footer -FooterText "CONFIDENTIAL - PROPERTY OF FINANCE DEPT" -EncryptionEnabled $true -EncryptionRightsDefinitions "FinanceDept:CoAuthor"
D. New-Label -Name "Financial Records" -ContentMarking Watermark -WatermarkText "CONFIDENTIAL - PROPERTY OF FINANCE DEPT" -EncryptionEnabled $true -EncryptionProtectionType UserDefined

Answer: C

Explanation: To configure the "Financial Records" label, use the Set-Label cmdlet to modify the existing label. The -ContentMarking Footer parameter with -FooterText "CONFIDENTIAL - PROPERTY OF FINANCE DEPT" applies the footer. The -EncryptionEnabled $true and -EncryptionRightsDefinitions "FinanceDept:CoAuthor" parameters enforce encryption and restrict co-authoring to the Finance department.

**Question: 680**

You are the compliance administrator for a multinational corporation using Microsoft 365 E5. You need to configure an advanced DLP rule to restrict employees from uploading files containing sensitive customer data to unapproved cloud services via unmanaged devices. The rule must detect U.S. Social Security Numbers (SSNs) with high confidence and block uploads only when the device is not enrolled in Microsoft Intune. Which two components should you include in the DLP rule configuration?

A. Add a condition to check for device enrollment status using Microsoft Intune
B. Configure the rule to detect SSNs with a confidence level of 85% or higher
C. Set the action to audit only for managed devices
D. Use a sensitive information type (SIT) for U.S. SSNs with a low confidence threshold

Answer: A, B

Explanation: To restrict uploads from unmanaged devices, the DLP rule must check device enrollment status using Microsoft Intune, which can be configured as a condition in advanced DLP rules. Additionally, detecting U.S. SSNs with a high confidence level (85% or higher) ensures accurate identification of sensitive data. Setting a low confidence threshold would increase false positives, and auditing only for managed devices would not address the requirement to block uploads from unmanaged devices.

# KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.


## Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

## Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

## Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

## Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

## Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.