Hunting for accumulations of sensitive data with Content Search and Defender for Cloud Apps

CollabDays Bremen 2025

Tatu Seppälä

⭐ Data security

⭐ Insider risk

Power Platform

Governance

IAM / Entra ID

Generative AI

SULAVA

CREATING BETTER WORKLIFE

The Digital **Neighborhood**

Tatu Seppälä

Security & Compliance Architect

MVP Microsoft® Most Valuable Professional

Topics

- Why do we need to discover accumulations?
- Demo! **High-level discovery:** Content Search
- Demo! **Targeted discovery:** Defender for Cloud Apps
- Putting your findings to work
- RBAC, governance and other considerations

More data is being created than ever
Stale data is almost never purged
Ungoverned sensitive data accumulates

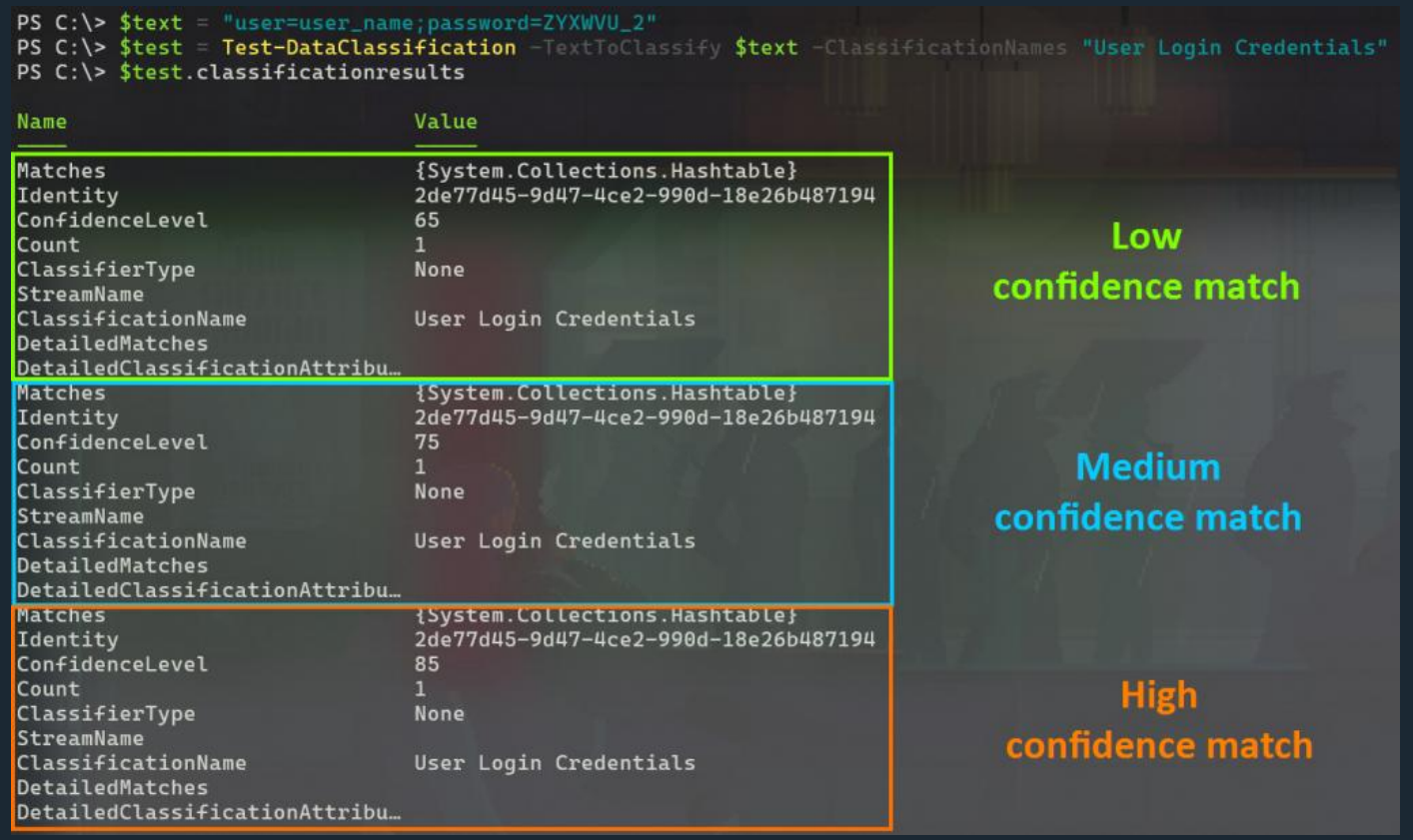
→ **Perpetual & unsustainable risk**

Why?

- Data leak & breach risk
- Data governance and quality
- Compliance (laws & regulations)
- Copilot for Microsoft 365 considerations

Understand SIT confidence levels

- To get the most out of Content Search & MDA File Policies, you need to understand SIT confidence levels & scoring
- Purview under the hood: Classifier confidence scoring, rule packs and the inconsistency of bundled SITs – Seppala365.cloud



Learn / Microsoft Purview /

Sensitive information type entity definitions

Article • 02/08/2024 • 2 contributors

Feedback

This article is a list of all sensitive information type (SIT) entity definitions. Each link takes you to the definition of that specific SIT and shows what a DLP policy looks for to detect each type. To learn more about sensitive information types, see Sensitive information types.

Note

Mapping of confidence level (high/medium/low) with accuracy number (numeric value of 1 to 100)

- Low confidence: 65 or below
- Medium confidence: 75
- High confidence: 85

- ABA routing number
- All credentials
- All full names
- All medical terms and conditions
- All Physical Addresses
- Amazon S3 Client Secret Access Key
- Argentina national identity (DNI) number
- Argentina Unique Tax Identification Key (CUIT/CUIL)
- ASP.NET machine Key
- Australia bank account number
- Australia business number
- Australia company number
- Australia drivers license number
- Australia medical account number
- Australia passport number
- Australia physical addresses
- Australia tax file number
- Austria drivers license number
- Austria identity card
- Austria passport number
- Austria physical addresses
- Austria social security number
- Austria tax identification number

Where to start?

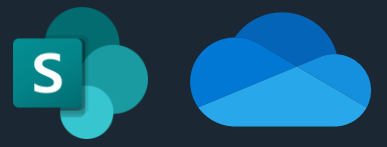
- Look through Microsoft's list of built-in Sensitive Information Types (SITs) and pick out the relevant ones
- You can programmatically get a list of SITs with full metadata with the Security & Compliance PowerShell command:

```
Get-DlpSensitiveInformationType
```

High-level accumulation discovery with..

Content Search

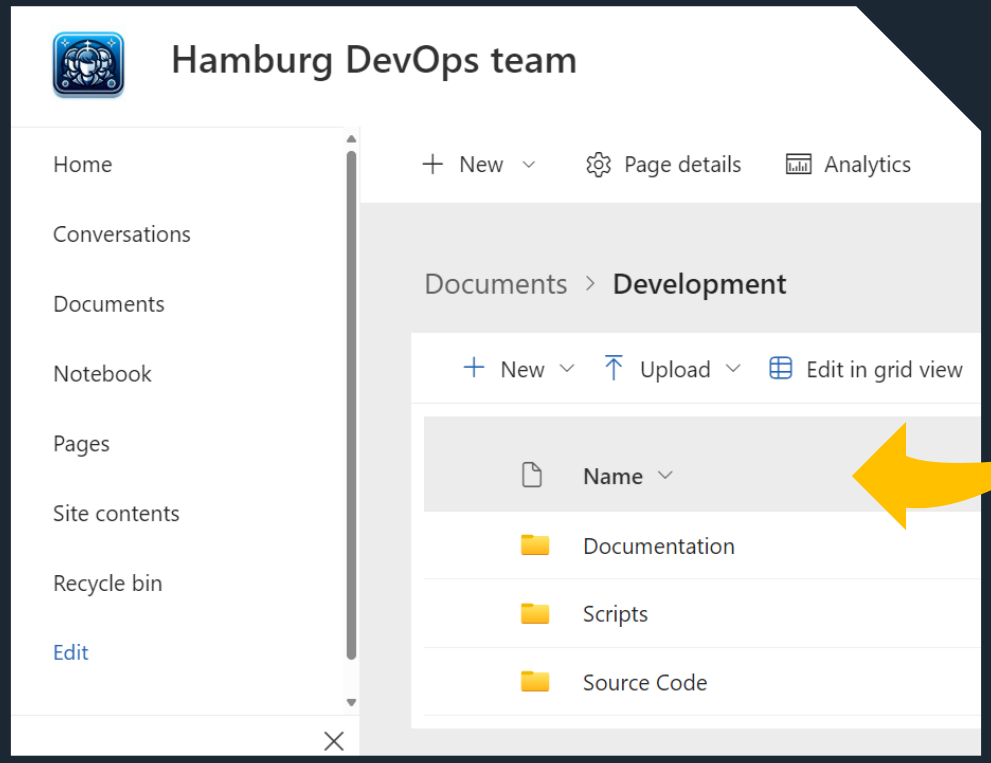
High-level discovery
Content Search

- Rapidly identify top accumulations in 
- Searching by SITs doesn't work with email!
- You need a bit of Keyword Query Language (KeyQL) – *not KQL!*
- Built-in and custom Sensitive Info Types are supported
- You can filter for stale and/or externally shared docs + more..


Demo
time

Content Search: common use cases

Find **sites** with many documents containing any # of SIT matches



For example:

- An e-commerce department's SharePoint site with order forms containing customer credit card numbers
- An IT or dev team’s site with configuration files that include credentials like server passwords and API keys

Content Search: common use cases

Find **sites** with many documents containing any # of SIT matches

KeyQL

```
SensitiveType:”Credit card number|*|85..”
```

Sensitive Information Type

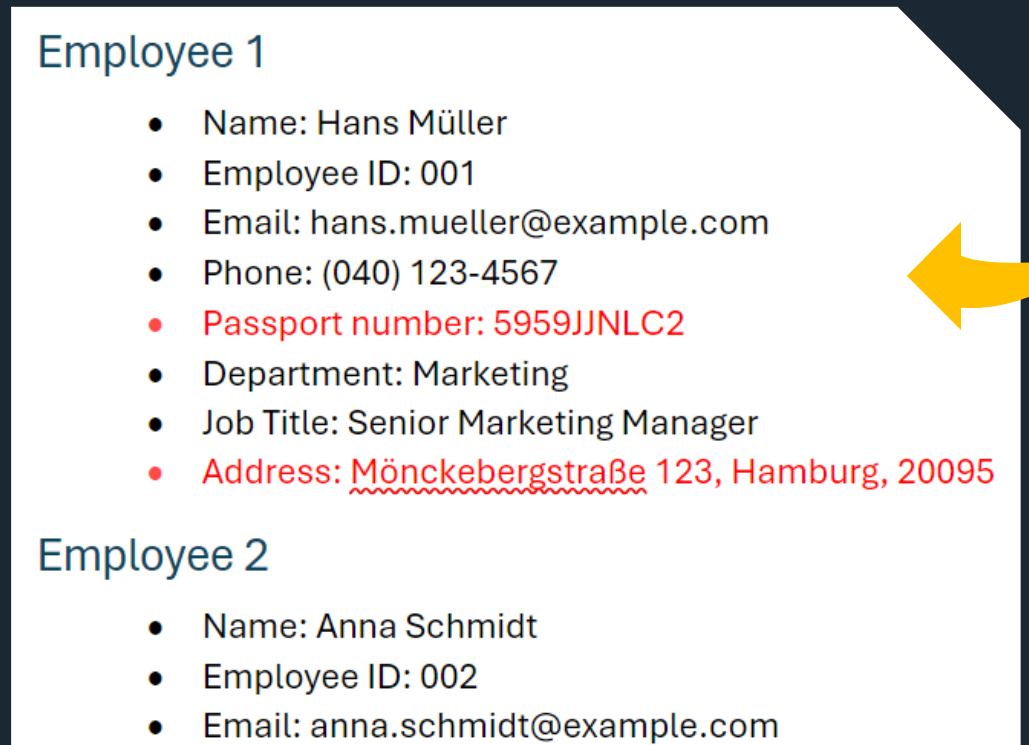
Required number of matches

Required confidence score (0-100)

Content Search: common use cases

Find **individual documents..**

- ..with many sensitive info type matches
- ..with medium confidence



For example:

- An employee database export containing multiple instances of personal data
- A configuration file with numerous occurrences of API keys and access tokens for various services

Content Search: common use cases

Find **individual documents..**

- ..with many sensitive info type matches
- ..with medium confidence

KeyQL

```
SensitiveType:”Credit card number|10..|75..”
```

Content Search: common use cases

Find accumulations of **stale** sensitive information (esp. personal data)

For example:

- Archived HR site with old employee records containing national ID numbers
- HR specialists' OneDrive sites w/ departed employees' PII data
- Legacy internal corporate travel arrangements site with outdated travel documents containing passport numbers.

Content Search: common use cases

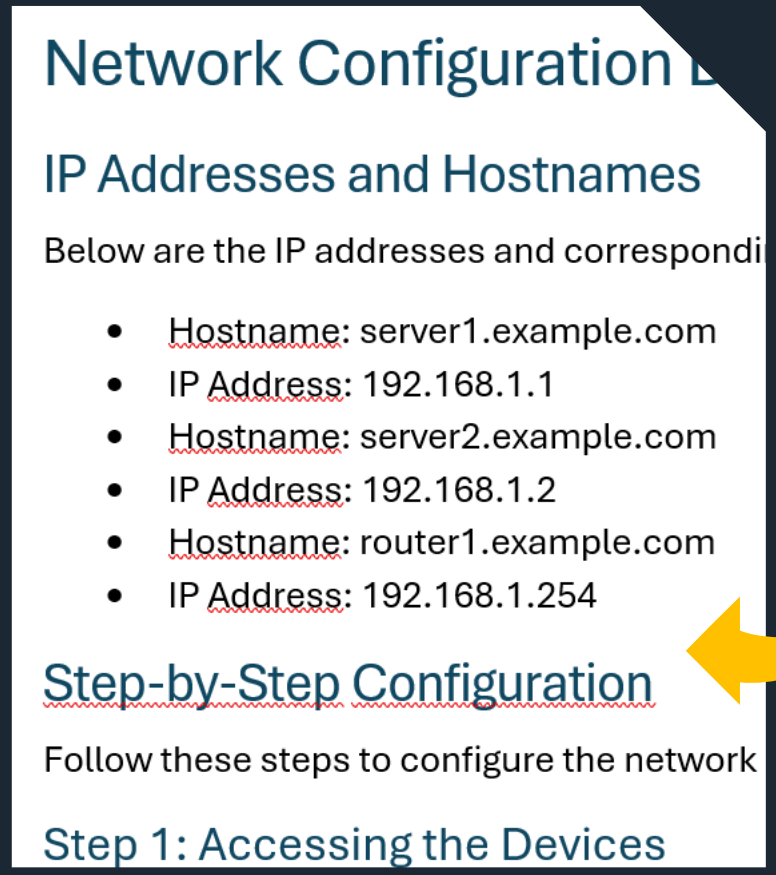
Find accumulations of **stale** sensitive information (esp. personal data)

KeyQL

```
SensitiveType:”Germany Identity Card Number|*|85..”
AND LastModifiedTime>=2023-12-31
```

Content Search: common use cases

Find accumulations of **externally shared** sensitive information



For example:

- A financial report shared with an external auditor containing multiple IBAN numbers for vendor payments
- Solution documentation shared with and worked on by vendors containing internal server hostnames along with IP addresses

Content Search: common use cases

Find accumulations of **externally shared** sensitive information

KeyQL

```
SensitiveType:”User Login Credentials|*|85..”
AND ViewableByExternalUsers:true
```

Content Search: search tips

You can look for many types of sensitive information in a single query.

Max query length = 4000 characters

👉 Good for credentials, passport numbers, national IDs & more..

KeyQL

```
SensitiveType:"Azure SQL Connection String|*|85.."
OR SensitiveType:"Client Secret / Api Key|*|85.."
OR SensitiveType:"User Login Credentials|*|85.."
```

Content Search: search tips

Standardize your search naming convention & orchestrate with the Security & Compliance PowerShell!

```
New-ComplianceSearch
-Name "Discovery / Credit card numbers / High confidence"
-SharePointLocation "All"
-Description "Discovery search: Credit card numbers / High confidence"
-ContentMatchQuery 'SensitiveType:"Credit Card Number|*|85.."'
```

Content Search: search tips

Standardize your search naming convention & orchestrate with the Security & Compliance PowerShell!

```powershell
# Run or rerun all created credential content searches
Get-ComplianceSearch
| Where-Object {$_.name -like "Discovery / Credentials*"}
| Start-ComplianceSearch
```

Credential searches split by individual SIT

PowerShell

```powershell
# SIT: Amazon S3 Client Secret Access Key
New-ComplianceSearch -Name "Discovery / Credentials: Amazon S3 Client Secret Access Key / High confide
-SharePointLocation "All" -Description "Discovery search: Amazon S3 Client Secret Access Key / High
confidence." -ContentMatchQuery 'SensitiveType:"Amazon S3 Client Secret Access Key|*|85.."'

# SIT: ASP.NET Machine Key
New-ComplianceSearch -Name "Discovery / Credentials: ASP.NET Machine Key / High confidence" -
SharePointLocation "All" -Description "Discovery search: ASP.NET Machine Key / High confidence." -
ContentMatchQuery 'SensitiveType:"ASP.NET Machine Key|*|85.."'

# SIT: Azure AD Client Access Token
New-ComplianceSearch -Name "Discovery / Credentials: Azure AD Client Access Token / High confidence" -
SharePointLocation "All" -Description "Discovery search: Azure AD Client Access Token / High confidenc
ContentMatchQuery 'SensitiveType:"Azure AD Client Access Token|*|85.."'

# SIT: Azure AD Client Secret
New-ComplianceSearch -Name "Discovery / Credentials: Azure AD Client Secret / High confidence" -
SharePointLocation "All" -Description "Discovery search: Azure AD Client Secret / High confidence." -
ContentMatchQuery 'SensitiveType:"Azure AD Client Secret|*|85.."'

# SIT: Azure AD User Credentials
New-ComplianceSearch -Name "Discovery / Credentials: Azure AD User Credentials / High confidence" -
SharePointLocation "All" -Description "Discovery search: Azure AD User Credentials / High confidence."
ContentMatchQuery 'SensitiveType:"Azure AD User Credentials|*|85.."'

# SIT: Azure App Service Deployment Password
New-ComplianceSearch -Name "Discovery / Credentials: Azure App Service Deployment Password / High
confidence" -SharePointLocation "All" -Description "Discovery search: Azure App Service Deployment Pas
/ High confidence." -ContentMatchQuery 'SensitiveType:"Azure App Service Deployment Password|*|85.."'

# SIT: Azure Batch Shared Access Key
New-ComplianceSearch -Name "Discovery / Credentials: Azure Batch Shared Access Key / High confidence"
SharePointLocation "All" -Description "Discovery search: Azure Batch Shared Access Key / High confider
-ContentMatchQuery 'SensitiveType:"Azure Batch Shared Access Key|*|85.."'

# SIT: Azure Bot Framework Secret Key
New-ComplianceSearch -Name "Discovery / Credentials: Azure Bot Framework Secret Key /
SharePointLocation "All" -Description "Discovery search: Azure Bot Framework Secret Key /
-ContentMatchQuery 'SensitiveType:"Azure Bot Framework Secret Key|*|85.."'

# SIT: Azure Bot Service App Secret
New-ComplianceSearch -Name "Discovery / Credentials: Azure Bot Service App Secret / High confidence" -
SharePointLocation "All" -Description "Discovery search: Azure Bot Service App Secret / High confidenc
ContentMatchQuery 'SensitiveType:"Azure Bot Service App Secret|*|85.."'
```

Content search

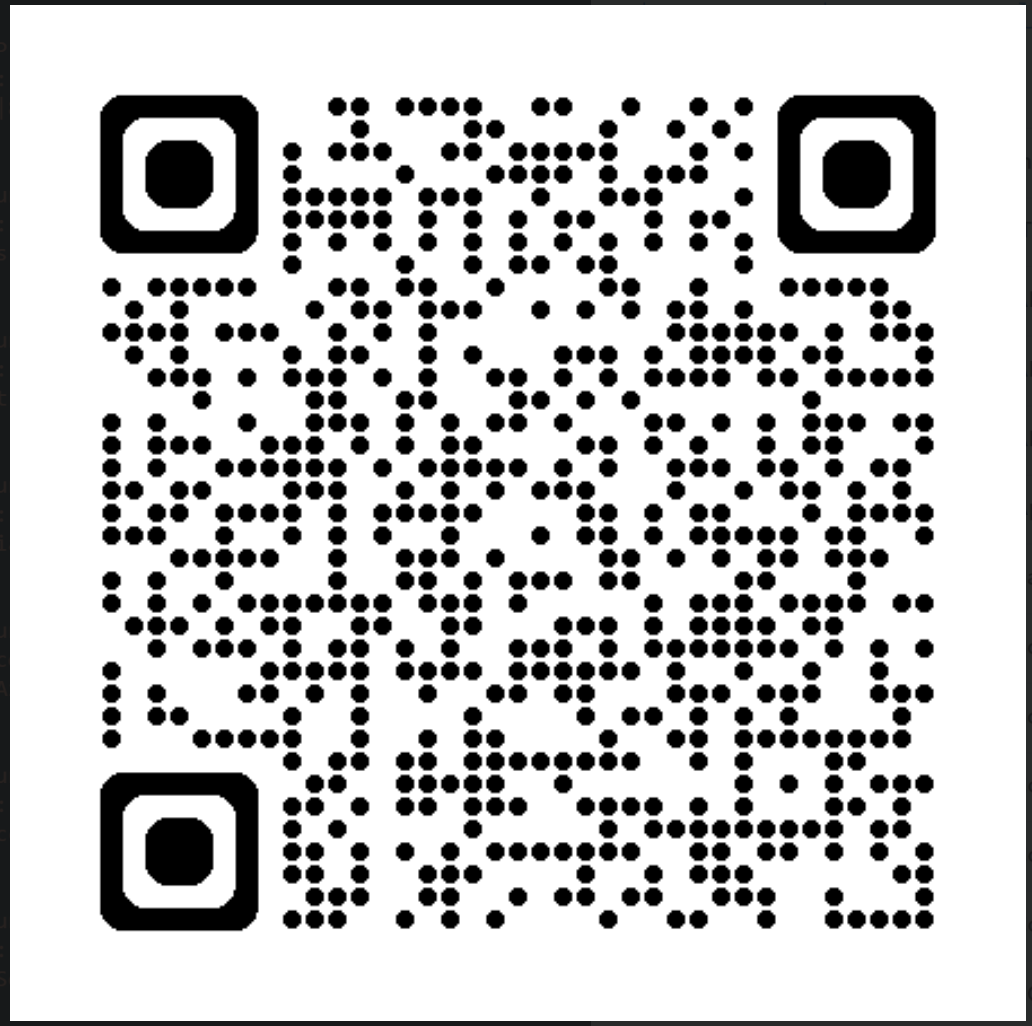
Search your organization for content in emails, documents, Skype for Business conversations, and more. You can

Search | Export

+ New search | Download list | Refresh

Name	Status
Discovery / Credentials: Amazon S3 Client Secret Access Key / High confidence	Completed
Discovery / Credentials: ASP.NET Machine Key / High confidence	Completed
Discovery / Credentials: Azure AD Client Access Token / High confidence	Completed
Discovery / Credentials: Azure AD Client Secret / High confidence	Completed
Discovery / Credentials: Azure AD User Credentials / High confidence	Completed
Discovery / Credentials: Azure App Service Deployment Password / High confidence	Completed
Discovery / Credentials: Azure Batch Shared Access Key / High confidence	Completed
Discovery / Credentials: Azure Bot Framework Secret Key / High confidence	Completed
Discov y / Credentials: Azure Bot Service App Secret / High confidence	Completed
Discov dentials: Azure Cognitive Search API Key / High confidence	Completed
s: Azure Cognitive Service Key / High confidence	Completed
Azure Container Registry Access Key / High confidence	Completed
ntials: Azure COSMOS DB Account Access Key / High confidence	Completed
Discov Credentials: Azure Databricks Personal Access Token / High confidence	Completed
Discovery / Credentials: Azure DevOps App Secret / High confidence	Completed

Rapid setup script from my GitHub



Discovery / Credit card numbers / High confidence

Search content

Condition report

Top locations

Download your top locations report.

Location	Location type	Items	Size
https://seppala365.sharepoint.com/sites/Landingpad	SharePoint	5	0.09
https://seppala365.sharepoint.com/sites/Marketsteam	SharePoint	4	0.07
https://seppala365-my.sharepoint.com/personal/adm-tatu_...	SharePoint	4	0.04
https://seppala365.sharepoint.com/sites/OfficeTeam	SharePoint	1	0.02
https://seppala365.sharepoint.com/sites/Onboarding-Welco...	SharePoint	1	0.02

Actions

Review sample

Close

Discovery / Credit card numbers / High confidence samples

Download list | Refresh | 1 selected | Customize columns

Subject/Title	Date ↓	Sender/Author
Examples-CreditCardNumbers (3)	Aug 26, 2024 11:43 AM	ADM Tatu Seppälä
Examples-CreditCardNumbers (2)	Aug 26, 2024 11:43 AM	ADM Tatu Seppälä
Examples-CreditCardNumbers (1)	Aug 26, 2024 11:43 AM	ADM Tatu Seppälä
Examples-CreditCardNumbers	Aug 26, 2024 11:43 AM	ADM Tatu Seppälä
Examples-CreditCardNumbers1_2C62287B-C157-4135-AFB...	Aug 21, 2024 9:43 PM	ADM Tatu Seppälä
Examples-CreditCardNumbers1_E60069A5-411E-4FF3-9535...	Aug 21, 2024 9:40 PM	ADM Tatu Seppälä
Dynamic token demonstration - SharePoint - Credit card n...	Aug 8, 2024 9:36 PM	ADM Tatu Seppälä
Dynamic token demonstration - SharePoint - Credit card n...	Aug 8, 2024 9:35 PM	ADM Tatu Seppälä
Dynamic token demonstration - SharePoint - Credit card n...	Aug 8, 2024 9:27 PM	ADM Tatu Seppälä
Dynamic token demonstration - SharePoint - Credit card n...	Aug 8, 2024 9:25 PM	ADM Tatu Seppälä
Dynamic token demonstration - SharePoint - Credit card n...	Aug 8, 2024 8:57 PM	ADM Tatu Seppälä
token demonstration - SharePoint - Credit card numbers t...	Aug 8, 2024 6:54 PM	ADM Tatu Seppälä
Dynamic token demonstration - OneDrive - Credit card nu...	Aug 7, 2024 9:39 PM	ADM Tatu Seppälä
Examples-CreditCardNumbers	May 7, 2024 11:16 AM	ADM Tatu Seppälä
Examples-CreditCardNumbers_39D95054-E4EA-48D6-B5C...	May 7, 2024 10:20 AM	ADM Tatu Seppälä
Examples-CreditCardNumbers	May 7, 2024 10:20 AM	ADM Tatu Seppälä

Examples-CreditCardNumbers

Source

This document type is not supported by preview. Please click here to download a copy.

Home
Solutions
eDiscovery
Unified Catalog
Data Map
Data Loss Prevention
Communi... Compliance

Discovery / PII / National IDs / Low to High confidence

Top locations

Download your top locations report.

Location	Location type	Items	Size
https://seppala365dev.sharepoint.com/sites/HRteam	SharePoint	12	0.25
https://seppala365dev.sharepoint.com/sites/C-levelteam	SharePoint	9	0.22
https://seppala365dev-my.sharepoint.com/personal/adm-ta...	SharePoint	6	0.1
https://seppala365dev-my.sharepoint.com/personal/tatu_se...	SharePoint	5	3.23
https://seppala365dev.sharepoint.com/sites/Valhalla	SharePoint	2	0.04
https://seppala365dev.sharepoint.com/sites/Seppala365	SharePoint	2	0.04

Actions
Review sample
Close

Row Labels	Sum of Items
SharePoint	
https://contoso.sharepoint.com/sites/Smar	
Financial IBAN High confidence	
PII Finland National IDs Medium to High co	
PII Passport numbers Medium to High confi	
Credentials User Login Credentials High co	
Credentials Client Secret Api Key High con	
https://contoso.sharepoint.com/sites/Quan	
PII Finland National IDs Medium to High co	
Financial IBAN High confidence	
PII Passport numbers Medium to High confi	
Credentials User Login Credentials High co	
Any credentials Medium to High confidence	
Financial Credit card numbers High confide	
https://contoso.sharepoint.com/sites/Tech	
Financial IBAN High confidence	
PII Finland National IDs Medium to High co	
PII Passport numbers Medium to High confi	
Credentials General Password High confide	
Credentials User Login Credentials High co	
https://contoso.sharepoint.com/sites/InnovateHub	1258
Financial IBAN High confidence	1137

Row Labels	Sum of Items
SharePoint	12320
Financial IBAN High confidence	9644
PII Finland National IDs Medium to High confidence	2574
PII Passport numbers Medium to High confidence	31
Financial Credit card numbers High confidence	23
https://contoso.sharepoint.com/sites/InnovateHub	11
https://contoso.sharepoint.com/sites/TechPioneers	4
https://contoso.sharepoint.com/sites/DigitalDynamics	2
https://contoso.sharepoint.com/sites/QuantumLeap	1
https://contoso.sharepoint.com/sites/NextGenTech	1
https://contoso.sharepoint.com/sites/CyberSolutions	1
https://contoso.sharepoint.com/teams/ITSupportTeam	1
https://contoso.sharepoint.com/sites/CodeMasters	1
https://contoso.sharepoint.com/sites/ByteBuilders	1
Any credentials Medium to High confidence	19
Credentials User Login Credentials High confidence	18
Credentials General Password High confidence	10
Credentials Client Secret Api Key High confidence	1
Grand Total	12320

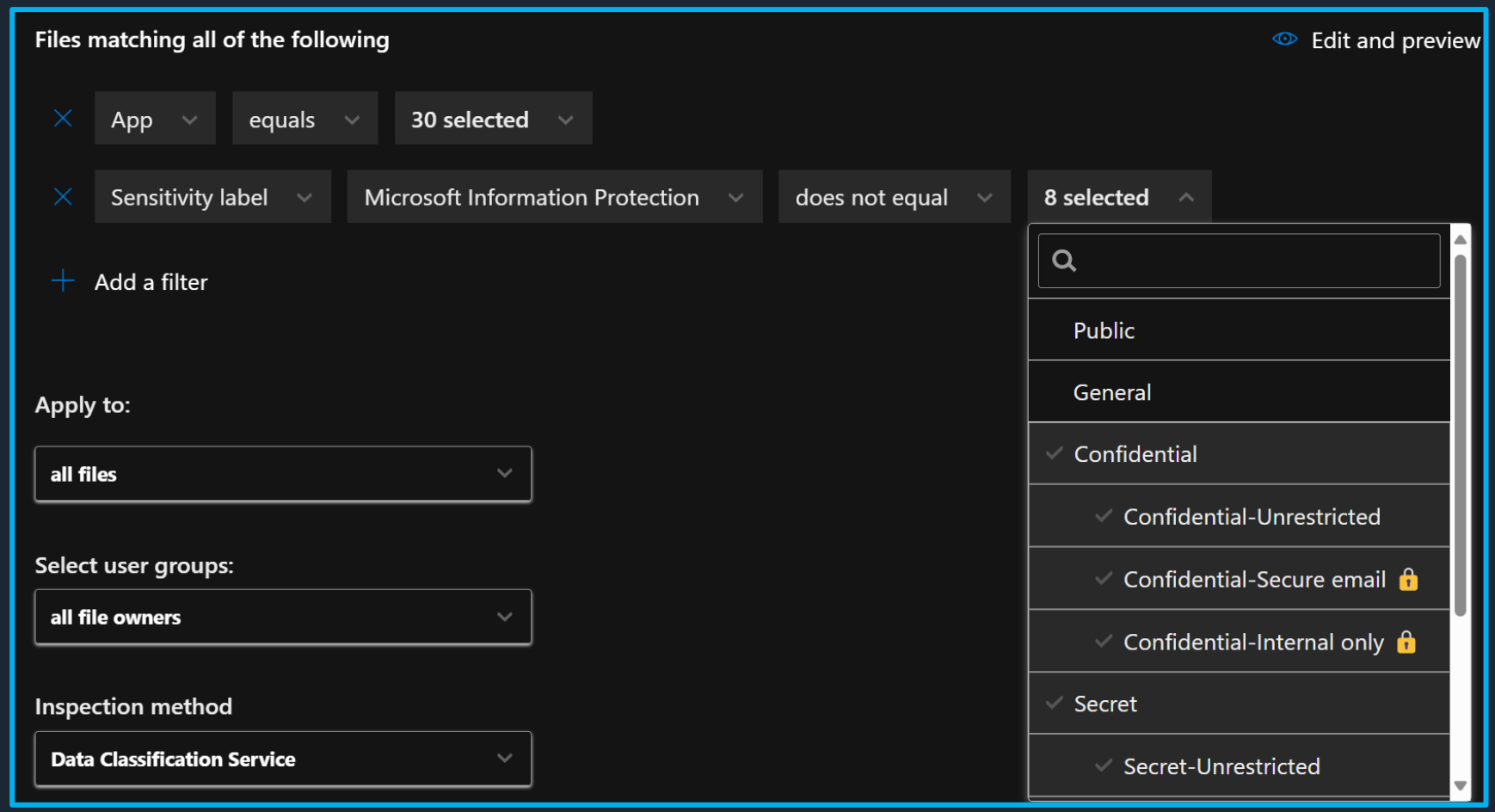
More granular insights from..

Defender for Cloud Apps File Policies

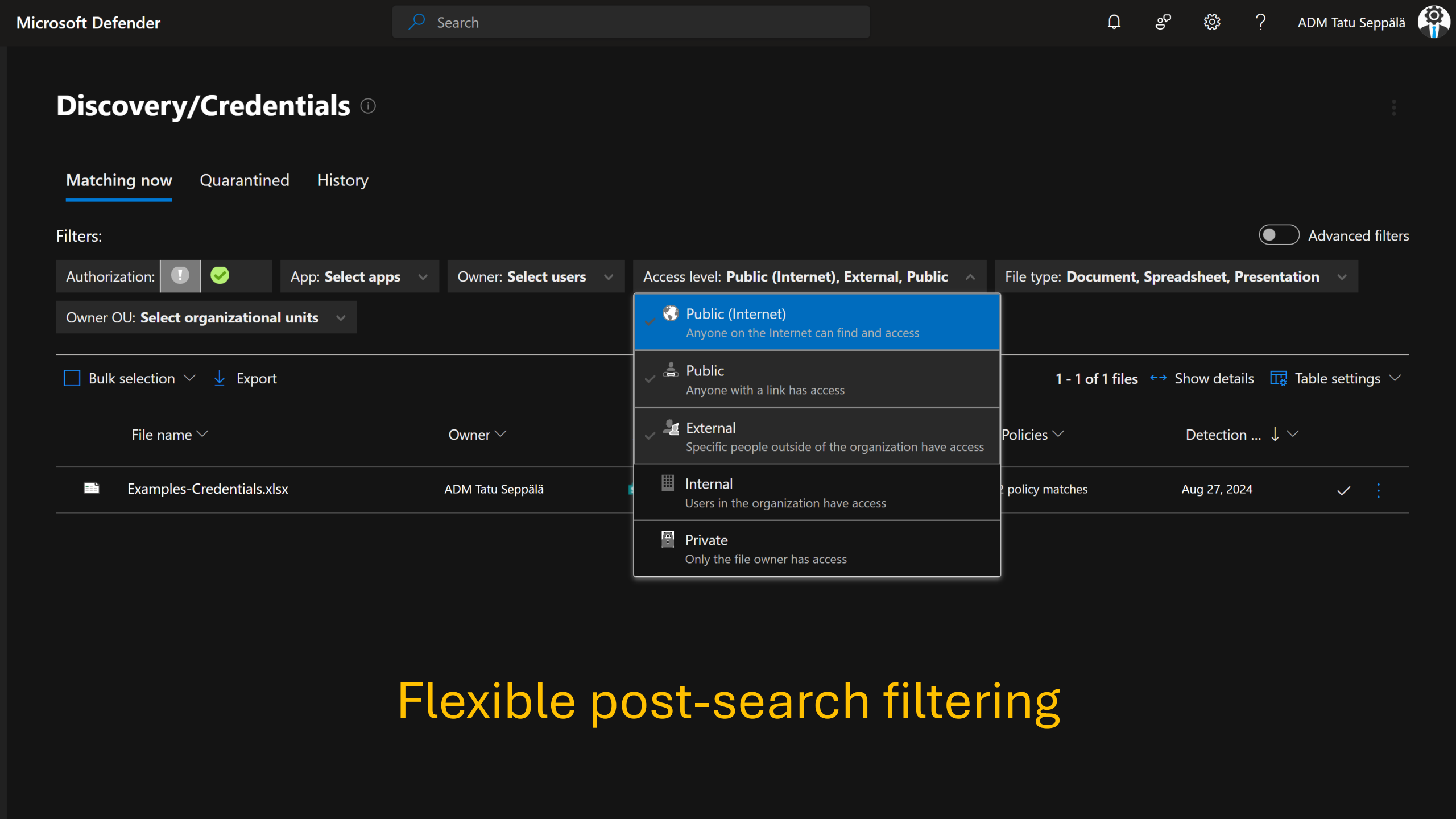

Demo
time

Targeted discovery
Defender for Cloud Apps

File Policies help reinforce specific weaknesses of Content Search



Policy granularity


Microsoft Defender
Search
ADM Tatu Seppälä
Discovery/Credentials
Matching now
Quarantined
History
Filters:
Advanced filters
Authorization:
App: Select apps
Owner: Select users
Access level: Public (Internet), External, Public
File type: Document, Spreadsheet, Presentation
Owner OU: Select organizational units
Public (Internet)
Anyone on the Internet can find and access
Public
Anyone with a link has access
External
Specific people outside of the organization have access
Internal
Users in the organization have access
Private
Only the file owner has access
Bulk selection
Export
1 - 1 of 1 files
Show details
Table settings
File name
Owner
Policies
Detection ...
Examples-Credentials.xlsx
ADM Tatu Seppälä
policy matches
Aug 27, 2024
Flexible post-search filtering

Microsoft Defender | Search | ADM Tatu Seppälä

Discovery/Credentials

Matching now | Quarantined | History

Filters:

Advanced filters

Authorization: | App: **Select apps** | Owner: **Select users** | Access level: **Public (Internet), External, Public** | File type: **Document, Spreadsheet, Presentation**

Owner OU: **Select organizational units**

Bulk selection | Export | 1 - 1 of 1 files | Show details | Table settings

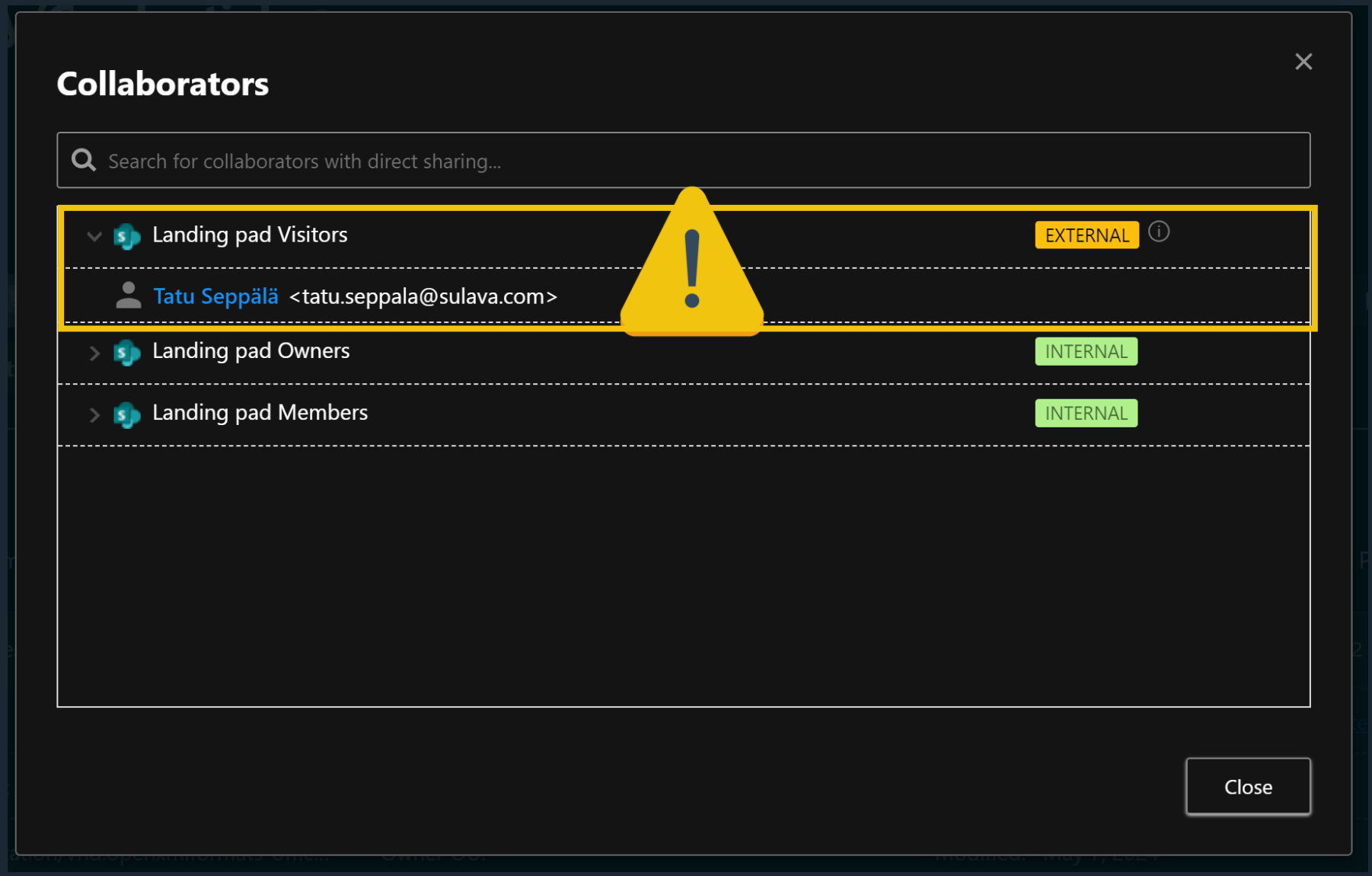
File name	Owner	App	Collaborators	Policies	Detection ...
Examples-Credentials.xlsx	ADM Tatu Seppälä	Microsoft SharePoint O...	3 collaborators	2 policy matches	Aug 27, 2024

Path: Landing pad / Shared Documents / General / Purview demo documents - View hierarchy

URL: https://seppala365.sharepoint.com/sites/Landingpad/Shared Documents/General/Purview dem...

Type: spreadsheet	Owner: ADM Tatu Seppälä	Created: May 7, 2024	Policies: 2 Externally shared document with credenti
MIME type: application/vnd.openxmlformats-offic...	Owner OU: —	Modified: May 7, 2024	Sensitivity labels: 2 AZURE RMS ENCRYPTED FILE ...
File identifiers: View file identifiers	Collaborators: 3 collaborators	File size: ~23 KB	Scan status: 1 completed, 1 failed

Enriched metadata for each match

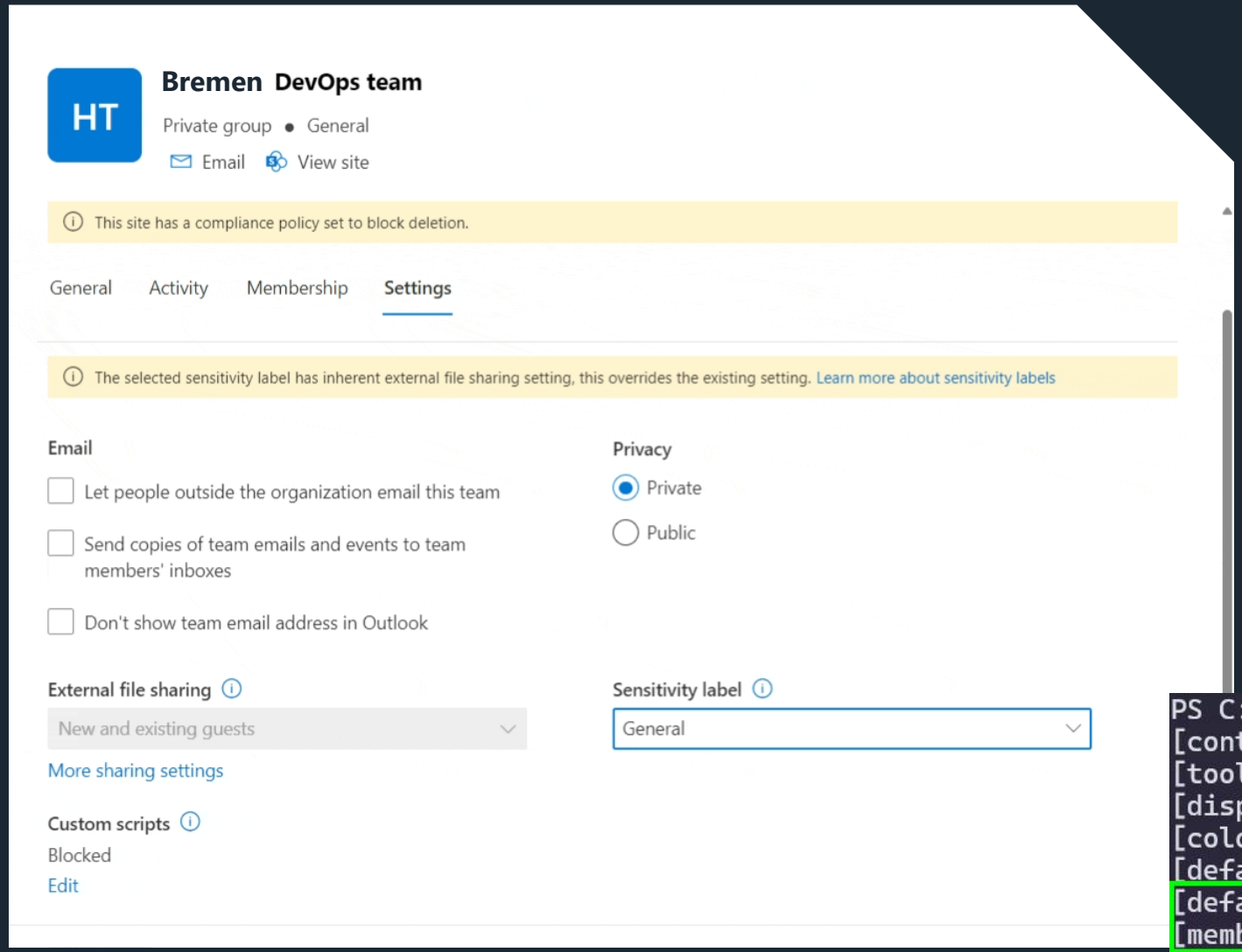


Deep visibility into sharing scenarios

Ok, so now you've got the visibility..

Putting your findings to work

Putting your findings into practice

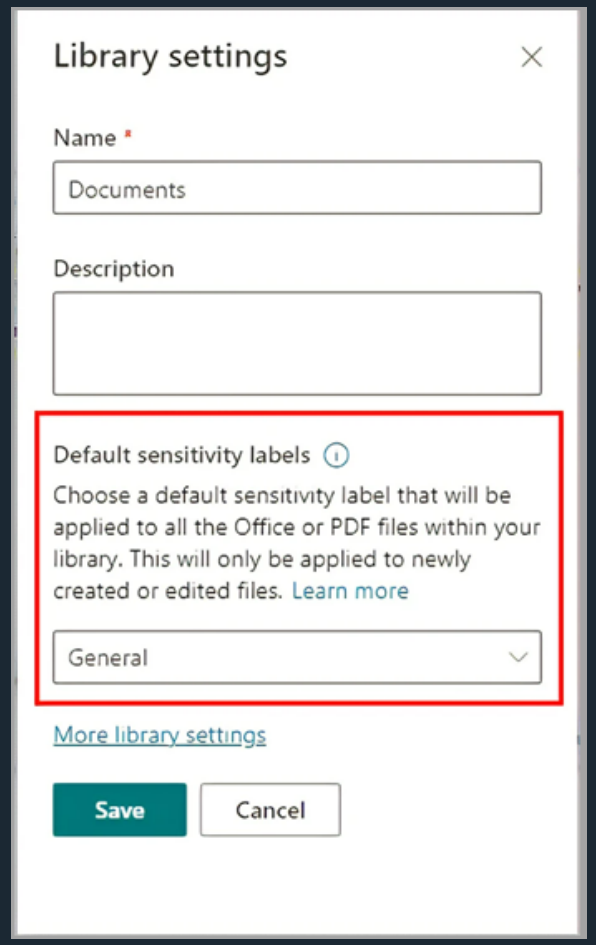


Apply elevated container sensitivity labels to most risky sites

- Sharing guardrails
- Access controls

```
PS C:\> (get-label Secret).settings
[contenttype, File, Email, Site, UnifiedGroup]
[tooltip, Highest confidentiality. Cannot be shared externally.]
[displayname, Secret]
[color, #A4262C]
[defaultsublabelid, 8bf9f609-91f9-4eda-998b-6fcf20a16870]
[defaultsharelinktoexistingaccess, True]
[memberscanshare, MemberShareNone]
```

Putting your findings into practice



Apply default sensitivity label to document libraries in sites w/ accumulations

- Newly-created and modified files on the site get protection by default unless already manually labeled
- Its easier to train users to apply **exceptions**
- **Auto-labeling** can also elevate the sensitivity applied by this mechanism

Putting your findings into practice

- Fetch a report of SharePoint sites & relevant sharing & access controls
  - Get-SPOSite (Microsoft.Online.SharePoint.PowerShell
- Pull in additional data from Content Search & MDA File Policies
- Contact owners of identified sites with stale data and facilitate cleanups
- Harden sharing settings and implement additional access controls

	A	B	C	D	E	F	G
1	Url	Title	Files w/ credentials	Owner	ConditionalAccessPolicy	SharingCapability	SiteDefinedSharingCapability
79	https://seppala365.sharepoint.com/sites/Landingpad	Landing pad	5		AllowFullAccess	ExternalUserSharingOnly	ExternalUserSharingOnly
80	https://seppala365.sharepoint.com/sites/TeamBremen	Team Bremen	1		AllowFullAccess	ExternalUserSharingOnly	ExternalUserSharingOnly
81	https://seppala365.sharepoint.com/sites/Informationprotectiontr	Information protection training hub	1	tatu@seppala365.cloud	AllowFullAccess	Disabled	Disabled
82	https://seppala365.sharepoint.com/sites/Arkaluontoistentietojen	Arkaluontoisten tietojen säilö	1		AllowFullAccess	ExternalUserSharingOnly	ExternalUserSharingOnly

SAM is your friend

Initiate site access review | View all reviews | Restrict site access

100 of 10,000 items

Filters: Site Template: **Classic sites, +3** | Privacy (Team sites only): **Private** | Sensitivity: **Confidential, +24** | External sharing: **On**

Site name	URL	Items shared ↓	Primary admin	Teams	Template	Sensitivity	External sharing	Privacy
Contoso HR	.../teams/contosohr	435	John Doe		Team site	Top secret	On	Private
Contoso Sales	../teams/contososales	354	Group owners		Classic site	Top secret	On	Private
Contoso Finance	../sites/contosofin	234	Sesha Mani		Team site	Highly confidential	On	Private
Contoso Giving	../sites/contosogiv	205	Karthik Gangidi		Team site	Top secret	On	Private
Contoso team	../sites/contosoteam	178	Group owners		Team site	Top secret	On	Private
Contoso Vac	../sites/contosovac	146	Shikha Verma		Classic site	Highly confidential	On	Private
Contoso HRA	../teams/contosohra	123	Group owners		Team site	Top secret	On	Private
Contoso Media	../sites/contosomedia	100	Brenda Thomas		Team site	Top secret	On	Private
Contoso in house	../sites/contosoinh	89	Chris Smith		Classic site	Highly confidential	On	Private
Contoso infra	../sites/contosoinfra	75	Group owners		Team site	Top secret	On	Private
Contoso design	../sites/contosodesign	64	Jack Becker		Classic site	Highly confidential	On	Private
Contoso leaders	../teams/contosolead	56	Zhao Zhang		Classic site	Highly confidential	On	Private
Contoso data	../teams/contosodata	40	Emily Baker		Team site	Top secret	On	Private
Contoso BI	../teams/contosobi	30	Emily Baker		Team site	Top secret	On	Private

SAM is your friend

Discover sites with specific sensitivity labelled files

Know your site admins

Govern these sites for right policy settings

Site ID	Site URL	Primary Admin	Primary Admin Email	Labelled documents	Site Sensitivi	Site Sensitivity	Site Unmanaged Device Policy	Site External Sharing
f7dab2e5-e0	.../sites/InvestmentBanking	Michelle Harris	michelle.harris@contoso.onmicrosoft.com	971	162fbb5e-1f	General	None	TRUE
00bb177f-22	.../sites/ContosoLife	Caleb Foster	caleb.foster@contoso.oncalrosoft.com	933	162fbb5e-1f	General	Limited, web-only access	FALSE
bde6e6c9-9e	.../sites/LeadershipTeam	Avery Howard	avery.howard@contoso.onaverosoft.com	911	162fbb5e-1f	Confidential	Block access	FALSE
3aefb921-e9	.../sites/USSales	Riley Ramirez	riley.ramirez@contoso.onrilrosoft.com	908	222a35d4-8a	Confidential	Block access	FALSE
6d75c83f-3e	.../sites/Operations	Amber Rodriguez	amber.rodriguez@contoso.onambrosoft.com	908	162fbb5e-1f	General	Limited, web-only access	TRUE
3c6e4459-8a	.../sites/DroneWorkshop	Maria Sullivan	maria.sullivan@contoso.onmarrosoft.com	868	162fbb5e-1f	General	None	TRUE
160f9cc7-8e	.../sites/FlySafeConference	Grace Taylor	grace.taylor@contoso.ongrarosoft.com	839	162fbb5e-1f	General	Limited, web-only access	FALSE
eb95ec98-9f	.../sites/LeadershipConnection	Sam Centrell	sam.centrell@contoso.onsamrosoft.com	634	222a35d4-8a	Confidential	Block access	FALSE
aee6640b-30	.../sites/MarkProjectTeam	Vance DeLeon	vance.deleon@contoso.onvanrosoft.com	588	162fbb5e-1f	Confidential	Block access	FALSE
d2bdc732-9e	.../sites/Give	Cameron Baker	cameron.baker@contoso.oncamrosoft.com	558	162fbb5e-1f	General	Limited, web-only access	TRUE
46d12cf3-76	.../sites/NewEmployeeOnboardin	Oscar Ward	oscar.ward@contoso.onoscrosoft.com	501	162fbb5e-1f	General	None	TRUE
50f07137-47	.../sites/ParentsofContoso	Eugenia Lopez	eugenia.lopez@contoso.oneugrosoft.com	479	222a35d4-8a	General	Limited, web-only access	FALSE
7ba4e7e9-3a	.../sites/ContosoBrand	Casey Jensen	casey.jensen@contoso.oncasrosoft.com	446	162fbb5e-1f	Confidential	Block access	FALSE
d84d7015-71	.../sites/ProductSupport	Brandon Stuart	brandon.stuart@contoso.onbrarosoft.com	360	162fbb5e-1f	Confidential	Block access	FALSE
8836bd59-35	.../sites/RetailOperations	Devon Torres	devon.torres@contoso.ondevrosoft.com	341	162fbb5e-1f	General	Limited, web-only access	TRUE
08f03943-20	.../sites/SalesandMarketing	Michael Peltier	michael.peltier@contoso.onmicrosoft.com	218	222a35d4-8a	General	None	TRUE
50f748af-4b	.../sites/SalesBestPractices	Kayla Lewis	kayla.lewis@contoso.onkayrosoft.com	174	162fbb5e-1f	General	Limited, web-only access	FALSE
51763230-74	.../sites/USSales	Isabel Gracia	isabel.gracia@contoso.onisarosoft.com	171	162fbb5e-1f	Confidential	Block access	FALSE
3a0abc9c-61	.../sites/AllCompany	Kerry Allen	kerry.allen@contoso.onkerrosoft.com	150	162fbb5e-1f	Confidential	Block access	FALSE
32b81ef7-26	.../sites/Benefits	Parker McLean	parker.mclean@contoso.onparrosoft.com	130	222a35d4-8a	General	Limited, web-only access	TRUE

Sharing link reports

These reports are useful in identifying sites which are active in collaboration and hence n
mitigate any potential oversharing risk. These 'RecentActivity' based reports identify sites
number of sharing links in the last 28 days.

Anyone sharing links created in last 28 days

PowerShell

```
Start-SPODataAccessGovernanceInsight -ReportEntity SharingLinks_Anyone -Workloa
```

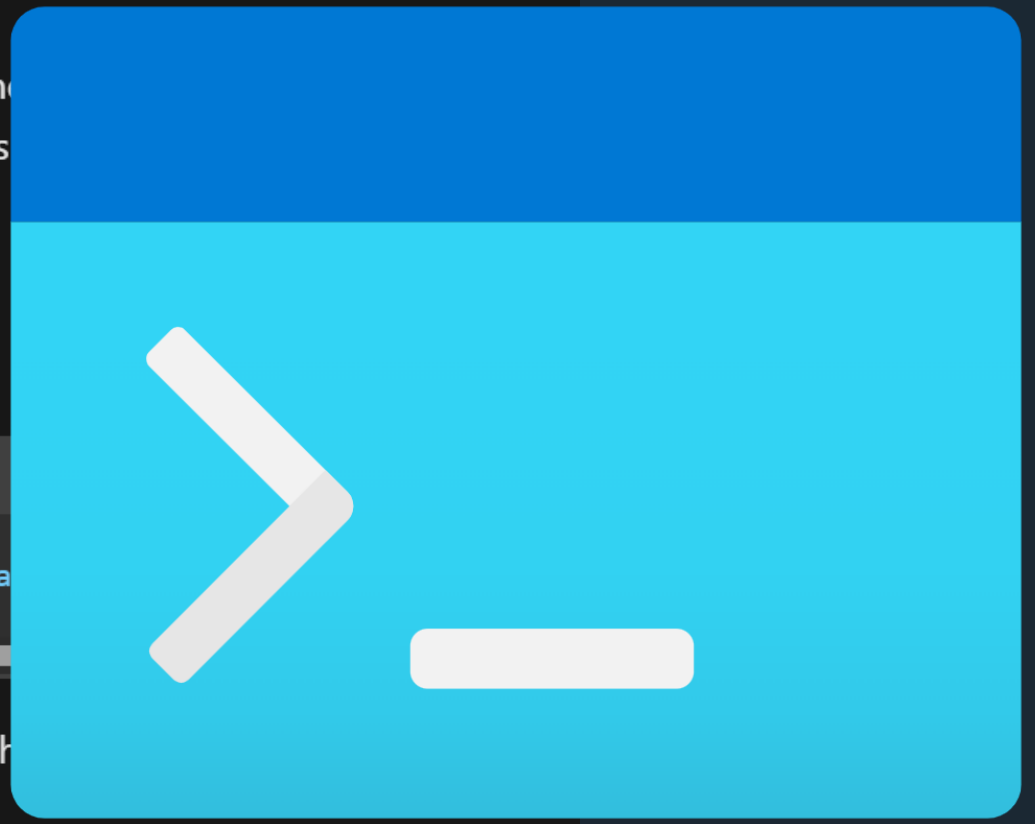
Provide the workload value as 'OneDriveForBusiness' to get all OneDrive accounts with th

PeopleInYourOrg sharing links created in last 28 days

PowerShell Copy

```
Start-
```

Provide the workload value as 'OneDriveForBusiness' to get all OneDrive accounts with the same criteria.



[Manage Data access governance reports using SharePoint Online PowerShell - SharePoint in Microsoft 365 | Microsoft Learn]

RBAC, governance & more

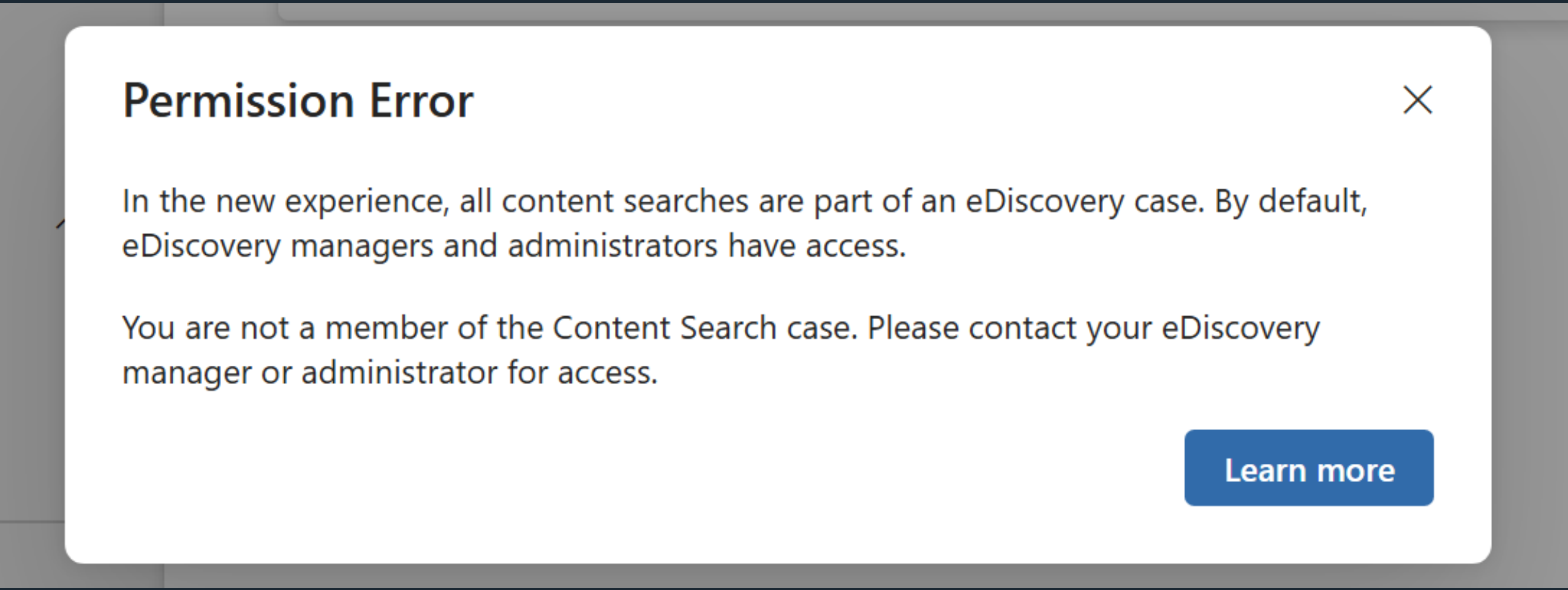
RBAC & governance considerations

Content Search (classic)

- Everyone with sufficient admin privileges can see everyone else's Content Searches and can review + export the results
- Purge unnecessary search jobs once data has been collected and analyzed

Name	Modified by
Legal team / Insider investigation 29082024	Tatu Seppälä
Discovery / Credentials / Medium to High confidence	ADM Tatu Seppälä

New Content Search fixes the issue

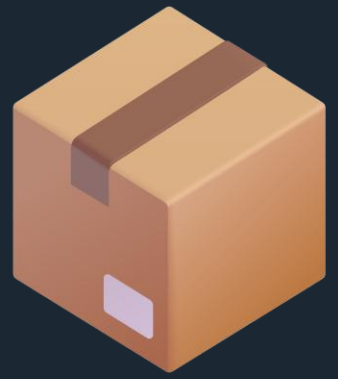


RBAC & governance considerations

Defender for Cloud Apps File Policies

- Be mindful that MDA File Policies give access to previews of snippets of file content even without special additional roles
- In some countries this might pose a compliance challenge due to various privacy and other laws and regulations
- MDA File Policies take time to crawl your entire data estate. Create them as early as possible and give them a week or two before reviewing results.
  - They keep running persistently so you don’t need to rerun them periodically

What’s next?



Starting **June 2025**, admins can **inherit** document library default label from the container label of a group/site/team.

By **September 30, 2025**, Microsoft will detect and remove the **Everyone Except External User** permission from the root site of each user’s OneDrive and the default document library in OneDrive.

Comments or questions?

Connect with me!