FINDING HOLES IN CONDITIONAL ACCESS POLICIES

Cloud Village - DC32

WHOAMI

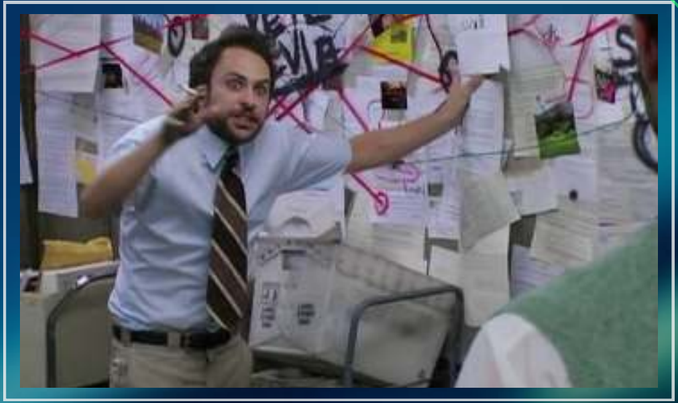
BRANDON COLLEY
@TECHBRANDON

FOUNDER - BNR CONSULTING

SERVICE LEAD & SENIOR SECURITY CONSULTANT - TRIMARC

Common misconfigurations

Why they matter

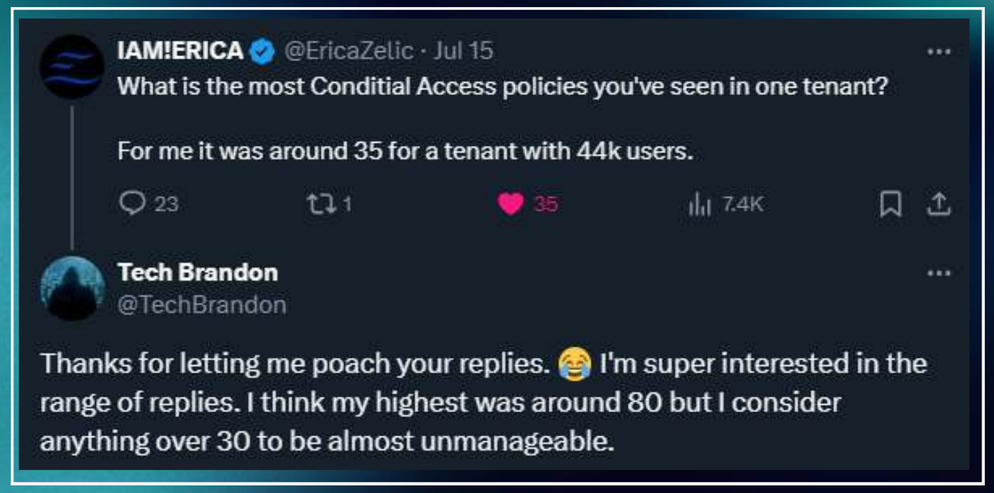


What you can do about it

LARGE NUMBER OF POLICIES

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure.

All policies	Microsoft-managed policies
61	1
Total	out of 61



17 REPLIES

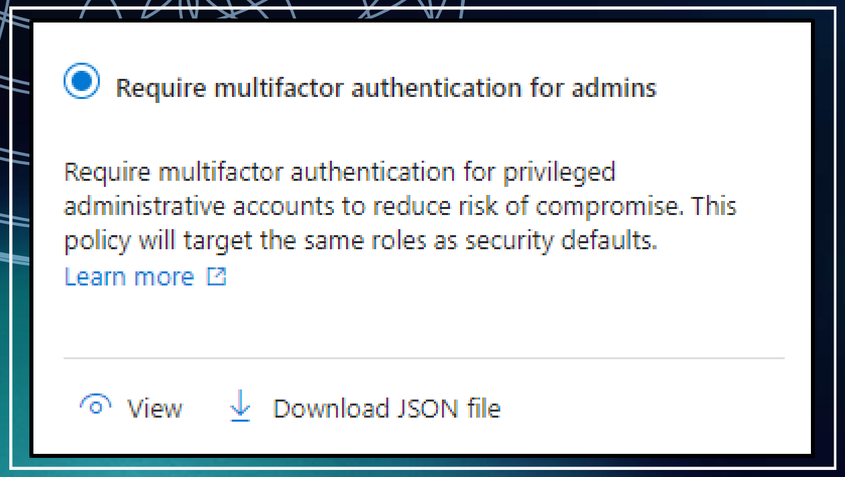
High/Low: 16 - 120

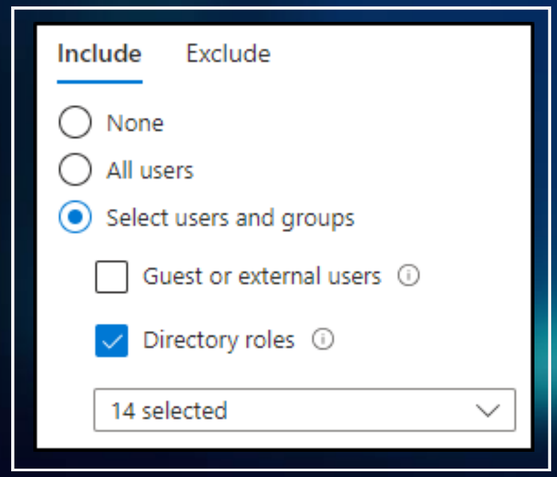
Average: 57.7

LARGE NUMBER OF POLICIES

LARGE NUMBER OF POLICIES

REQUIRE MFA FOR ADMINS





14 ROLES BY DEFAULT

Global Administrator
Security Administrator
SharePoint Administrator
Exchange Administrator
Conditional Access Administrator
Helpdesk Administrator
Billing Administrator
User Administrator
Authentication Administrator
Application Administrator
Cloud Application Administrator
Password Administrator
Privileged Authentication Administrator
Privileged Role Administrator

REQUIRE MFA FOR ADMINS

ADD AT LEAST:

Authentication Policy Administrator
Directory Writers
External Identity Provider Administrator
Hybrid Identity Administrator
Identity Governance Administrator
Intune Administrator
License Administrator
Partner Tier 1 Support
Partner Tier 2 Support

14 ROLES BY DEFAULT

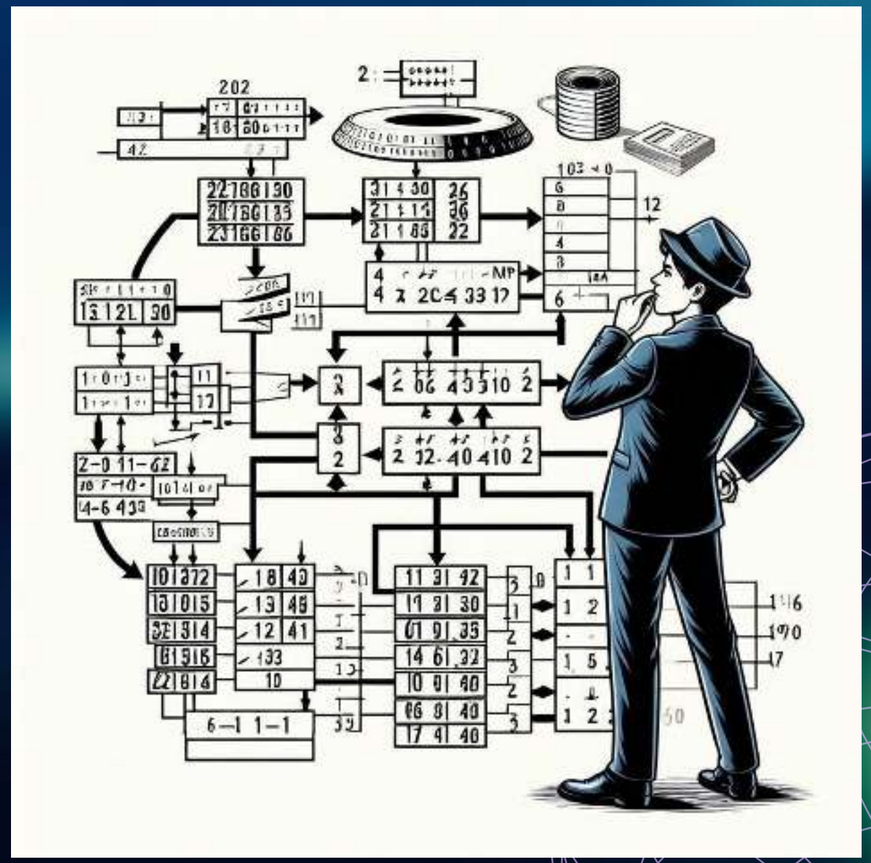
Global Administrator
Security Administrator
SharePoint Administrator
Exchange Administrator
Conditional Access Administrator
Helpdesk Administrator
Billing Administrator
User Administrator
Authentication Administrator
Application Administrator
Cloud Application Administrator
Password Administrator
Privileged Authentication Administrator
Privileged Role Administrator

REQUIRE MFA FOR ADMINS

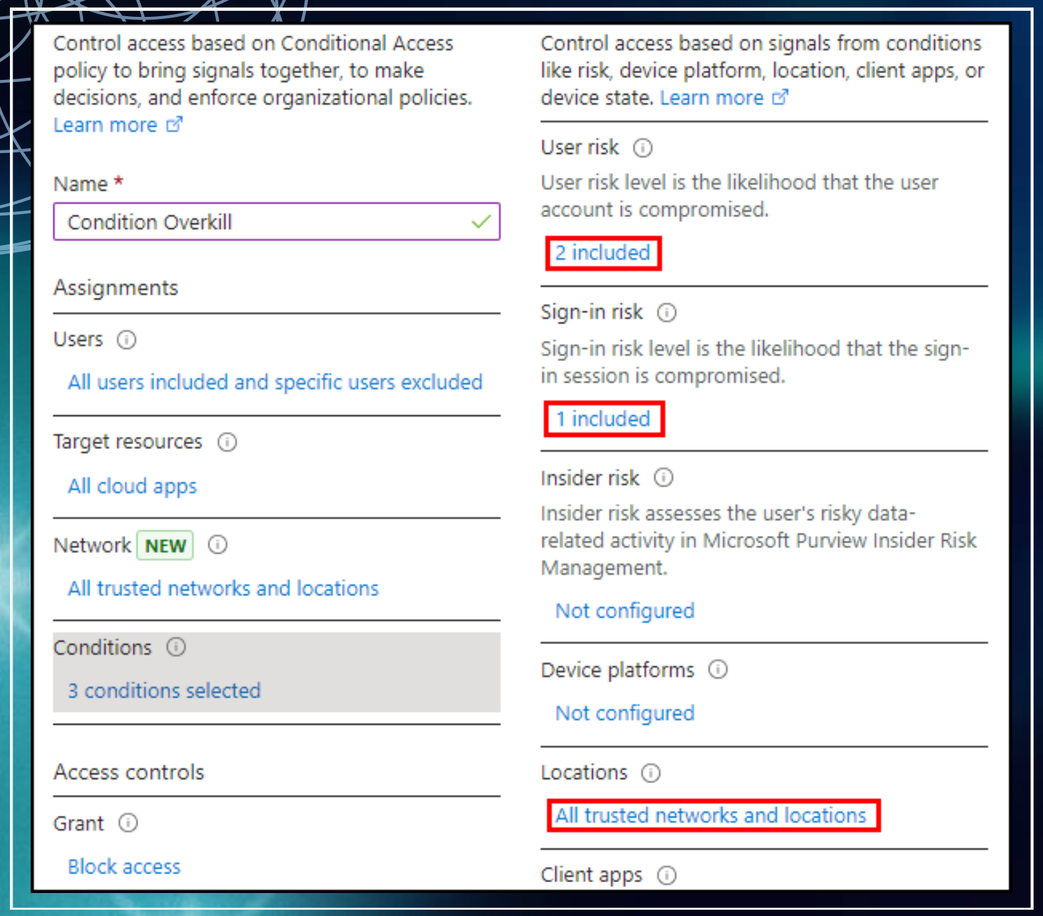
NAMED LOCATIONS

SUBNETS!!!

- Regular maintenance
- Narrow scopes
- Overlapping IP space



MULTIPLE CONDITIONS



MULTIPLE CONDITIONS

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Condition Overkill

Assignments

Users

All users included and specific users excluded

Target resources

All cloud apps

Network NEW

All trusted networks and locations

Conditions

3 conditions selected

Access controls

Grant

Block access

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk

User risk level is the likelihood that the user account is compromised.

2 included

Sign-in risk

Sign-in risk level is the likelihood that the sign-in session is compromised.

1 included

Insider risk

Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.

Not configured

Device platforms

Not configured

Locations

All trusted networks and locations

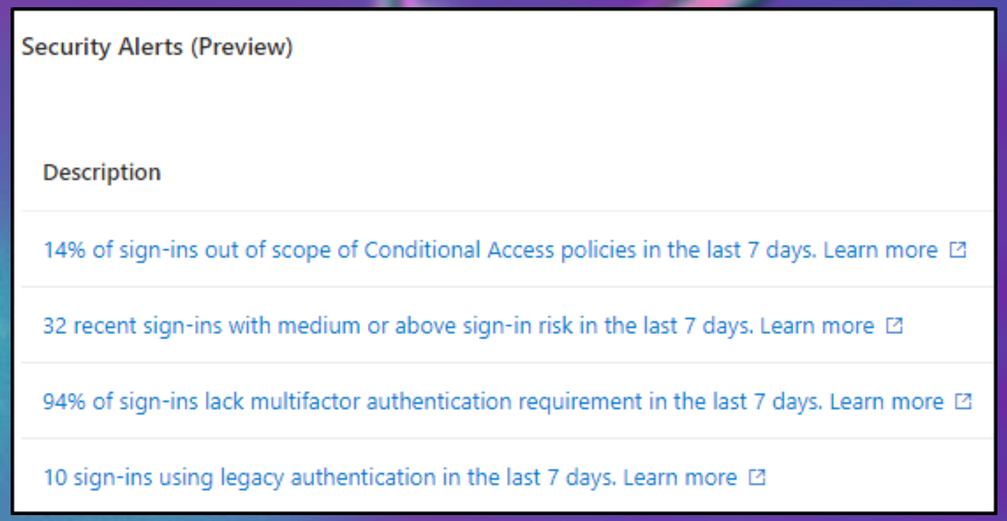
Client apps

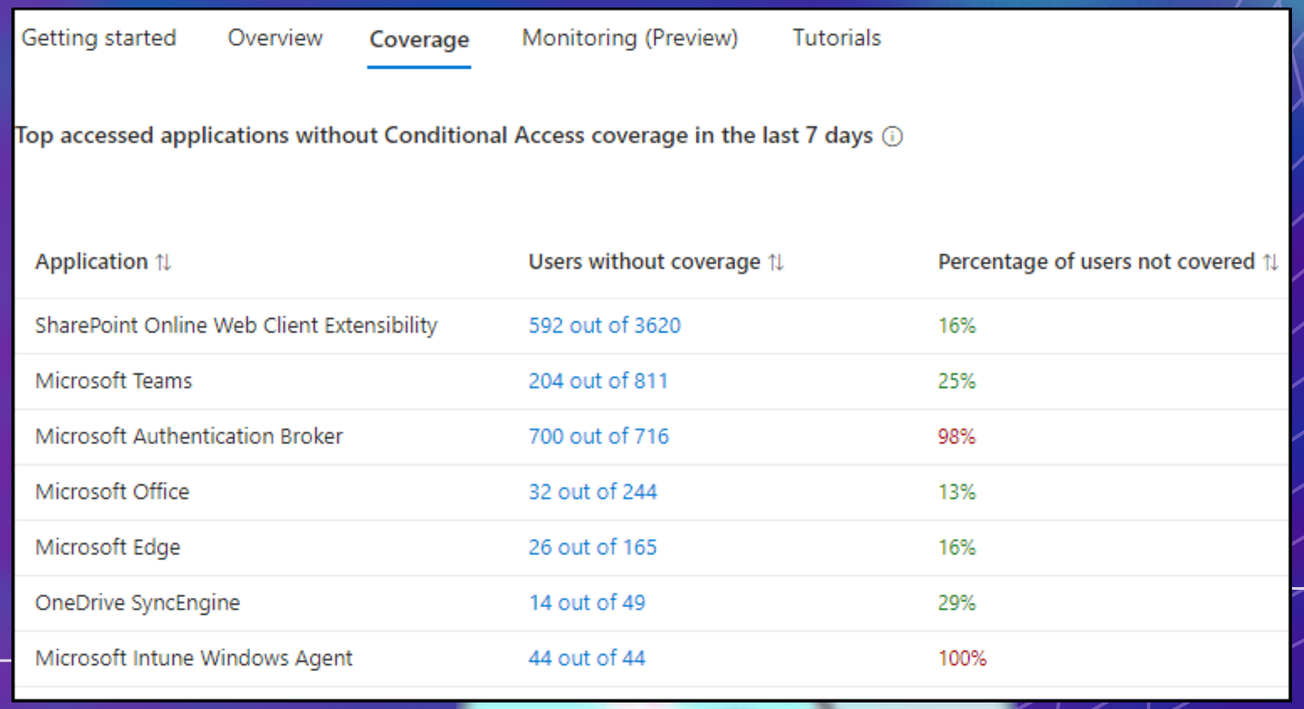
FINDING HOLES

FINDING HOLES

FINDING HOLES

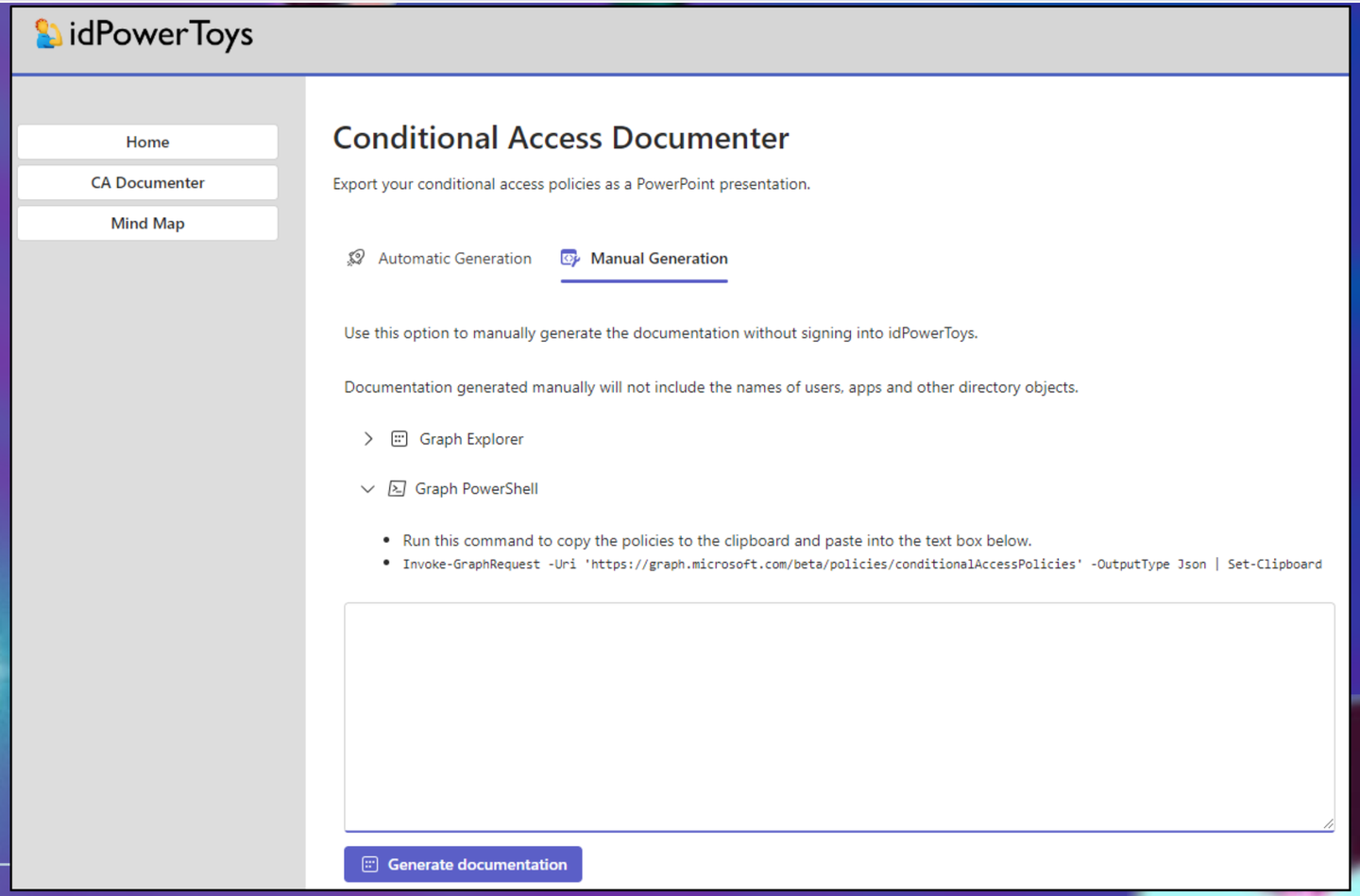
BUILT IN TOOLS



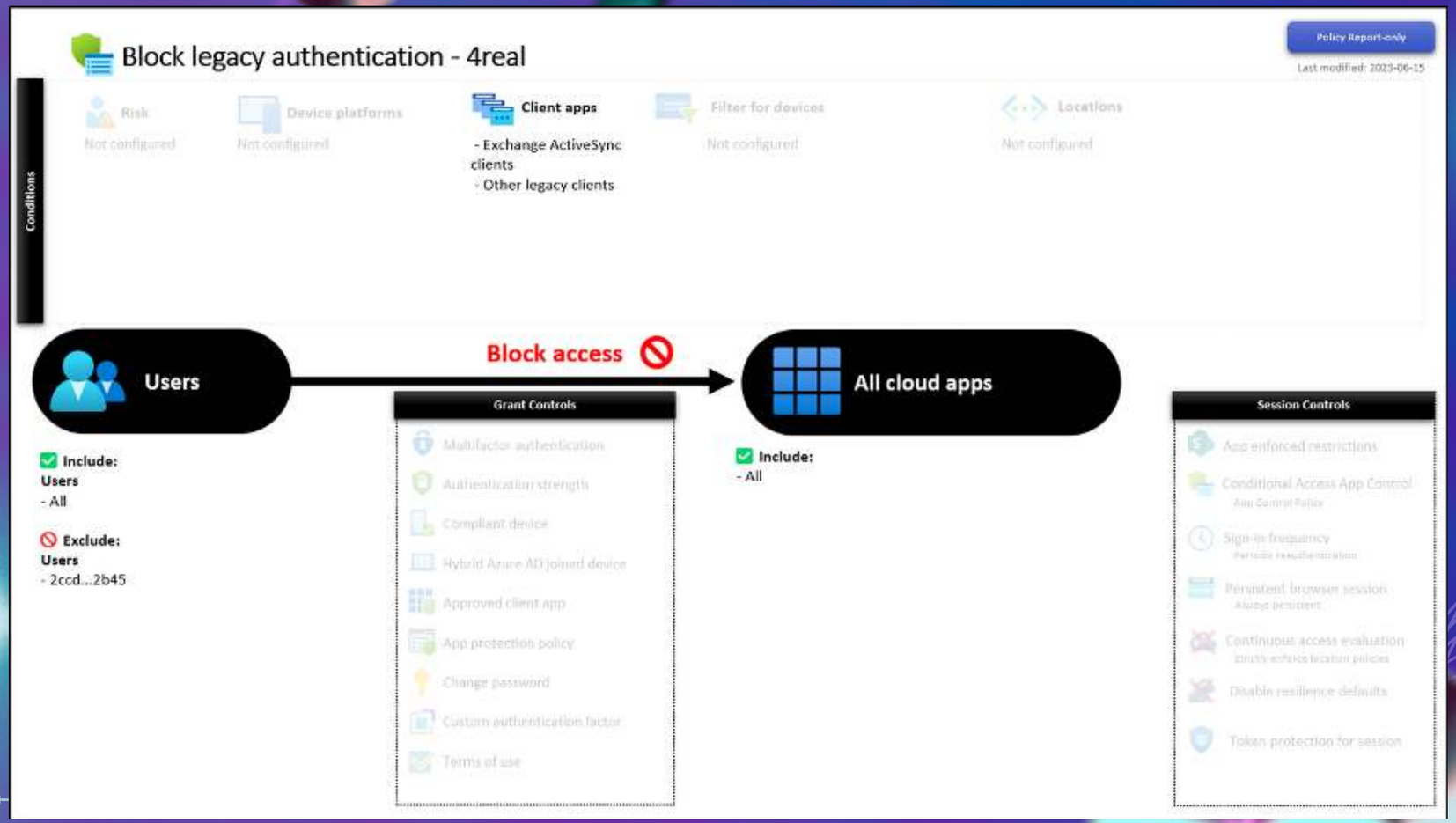


Application	Users without coverage	Percentage of users not covered
SharePoint Online Web Client Extensibility	592 out of 3620	16%
Microsoft Teams	204 out of 811	25%
Microsoft Authentication Broker	700 out of 716	98%
Microsoft Office	32 out of 244	13%
Microsoft Edge	26 out of 165	16%
OneDrive SyncEngine	14 out of 49	29%
Microsoft Intune Windows Agent	44 out of 44	100%

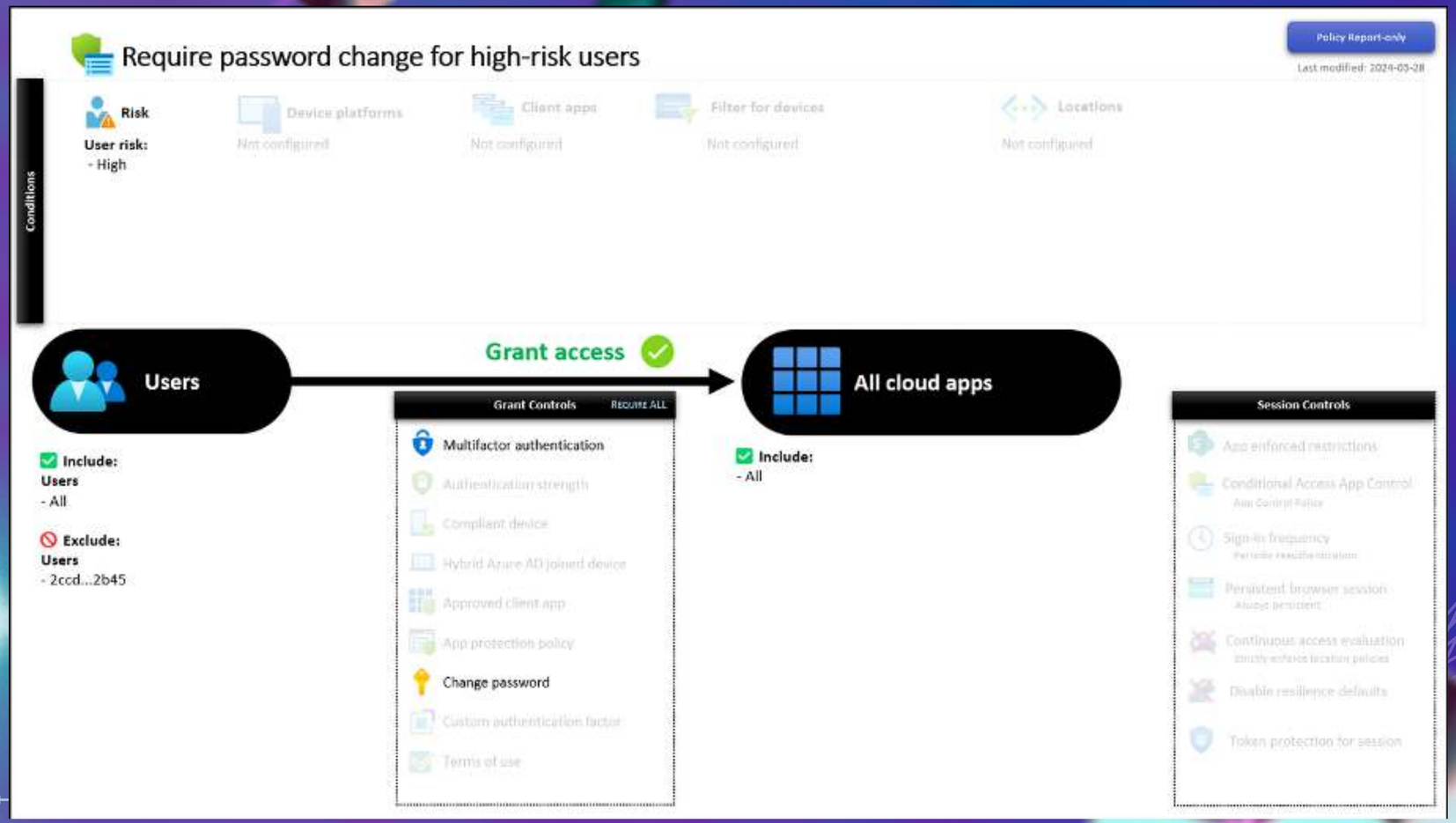
IDPOWERTOYS



IDPOWERTOYS



IDPOWERTOYS



MAESTER.DEV

Maester Test Results

This is a summary of the test results from the Maester test run.

Tenant: MSFT

Date: 08/05/2024 16:01:21

Total Tests	Passed	Failed	Not Run
278	64	130	****

MAESTER.DEV

MT.1003: At least one Conditional Access policy is configured with All Apps.

Passed

Overview

Microsoft recommends creating at least one conditional access policy targetting all cloud apps and ideally all users.

See Plan a Conditional Access deployment - Microsoft Learn

Test Results

These conditional access policies target all cloud apps:

- test enabled
- block Lee from my IP

Learn more: https://maester.dev/docs/tests/MT.1003

Tag: `Maester` `CA` `Security` `All`

Category: `Conditional Access Baseline Policies`

Source: `/home/runner/work/maester-tests/maester-tests/public-tests/tests/Maester/Entra/Test-ConditionalAccessBaseline.Tests.ps1`

MAESTER.DEV

⚠ MT.1001: At least one Conditional Access policy is configured with device compliance.

Overview ⚠ Failed

It is recommended to have at least one conditional access policy that enforces the use of a compliant device.

See Require a compliant device, Microsoft Entra hybrid joined device, or MFA - Microsoft Learn

Test Results

There was no conditional access policy requiring device compliance.

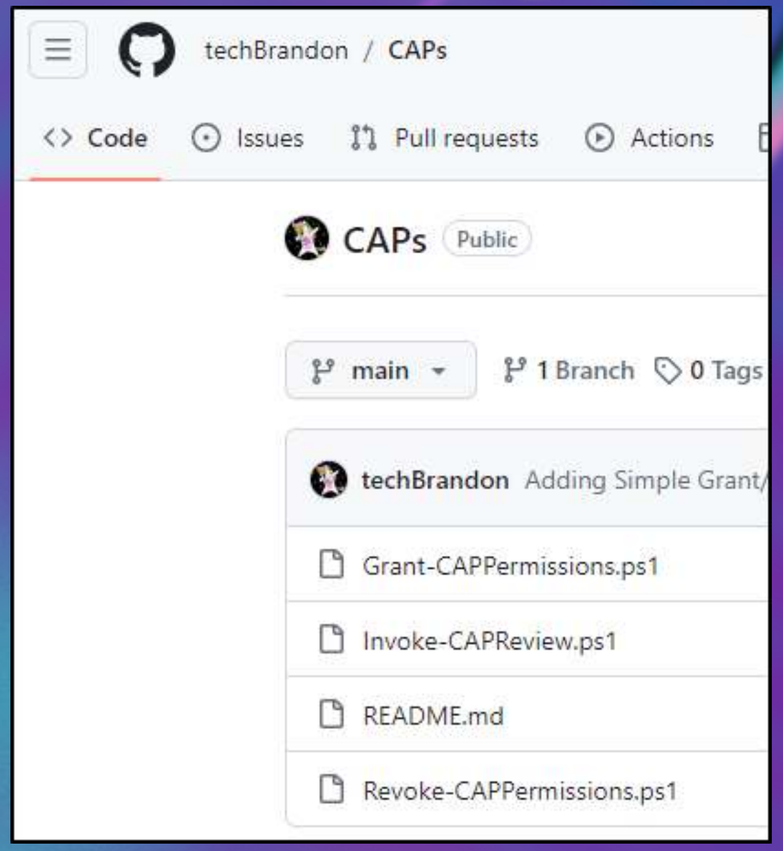
Learn more: https://maester.dev/docs/tests/MT.1001

Tag: `Maester` `CA` `Security` `All`

Category: `Conditional Access Baseline Policies`

Source: `/home/runner/work/maester-tests/maester-tests/private-tests/tests/Maester/Entra/Test-ConditionalAccessBaseline.Tests.ps1`

INVOKE-CAPREVIEW



https://github.com/techbrandon/caps

INVOKE-CAPREVIEW

```
Conditional Access Statistics
23 Conditional Access policies are configured for the tenant
0 are Microsoft Managed and are set to Report-only
2 are On (enabled)
20 are set to Report-only
1 are Off (disabled)

All Conditional Access Policies

DisplayName                                          State                                 CreatedDateTime       ModifiedDateTime
-----------                                          -----                                 ---------------       ----------------
Require multifactor authentication for admins        enabledForReportingButNotEnforced     6/9/2023 9:05:41 PM   3/28/2024 8:31:18 PM
Block legacy authentication                          enabledForReportingButNotEnforced     6/12/2023 9:54:07 PM  12/20/2023 7:32:33 PM
Allow Legacy app for Adele - test                    enabledForReportingButNotEnforced     6/12/2023 10:02:07 PM 4/5/2024 12:12:47 PM
Require multifactor authentication for all users - test disabled                           6/12/2023 10:24:33 PM 8/5/2024 2:48:23 PM
Block legacy authentication SMTP                     enabledForReportingButNotEnforced     6/15/2023 1:53:23 AM  12/20/2023 7:32:42 PM
```

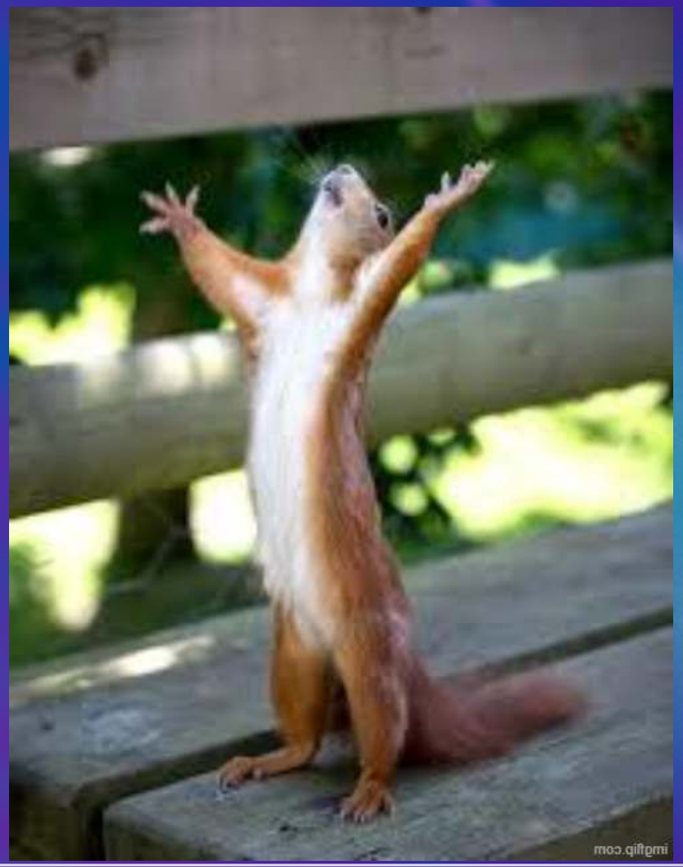
INVOKE-CAPREVIEW

```
Categorize Policies:

Policies that block Legacy Authentication
Block legacy authentication SMTP
Block legacy authentication - 4real

Policies that enforce MFA for Administrators
Require multifactor authentication for admins
Require multifactor authentication for admins - template

Policies that enforce MFA for Users
Allow Legacy app for Adele - test
Require multifactor authentication for all users
Require multifactor authentication for risky sign-ins
Require password change for high&Med-risk users
Require password change for high-risk users
register device
Require MFA for Device Registration
```

```
Policies that affect risky users
Require multifactor authentication for risky sign-ins
Require password change for high&Med-risk users
Require password change for high-risk users

Policies that require approved client or app protection
Require approved client apps
Require approved client apps or app protection policies

Policies that require device compliance
Require compliant device for admins
Require compliant or hybrid Azure AD joined device for admins

Policies that restrict access by location
Require multifactor authentication for admins
trusted IP test
block Lee from my IP

Policies that restrict access to the admin portal
block azure portal

Policies that require MFA for device join or registration
register device
Require MFA for Device Registration
```

THANK YOU!

@TECHBRANDON
LINKEDIN.COM/IN/TECHBRANDON



RESOURCES

https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Overview
https://learn.microsoft.com/en-us/entra/identity/conditional-access/what-if-tool
https://idpowertoys.merill.net/ca
https://maester.dev/
https://github.com/techBrandon/CAPs
https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-admin-mfa
https://techcommunity.microsoft.com/t5/microsoft-entra-blog/introducing-the-microsoft-entra-powershell-module/ba-p/4173546

THANK YOU!

@TECHBRANDON
LINKEDIN.COM/IN/TECHBRANDON

WRITE YOUR TOPIC OR IDEA

Back to Agenda Page

ADD A MAIN POINT

Briefly elaborate on what you want to discuss.

ADD A MAIN POINT

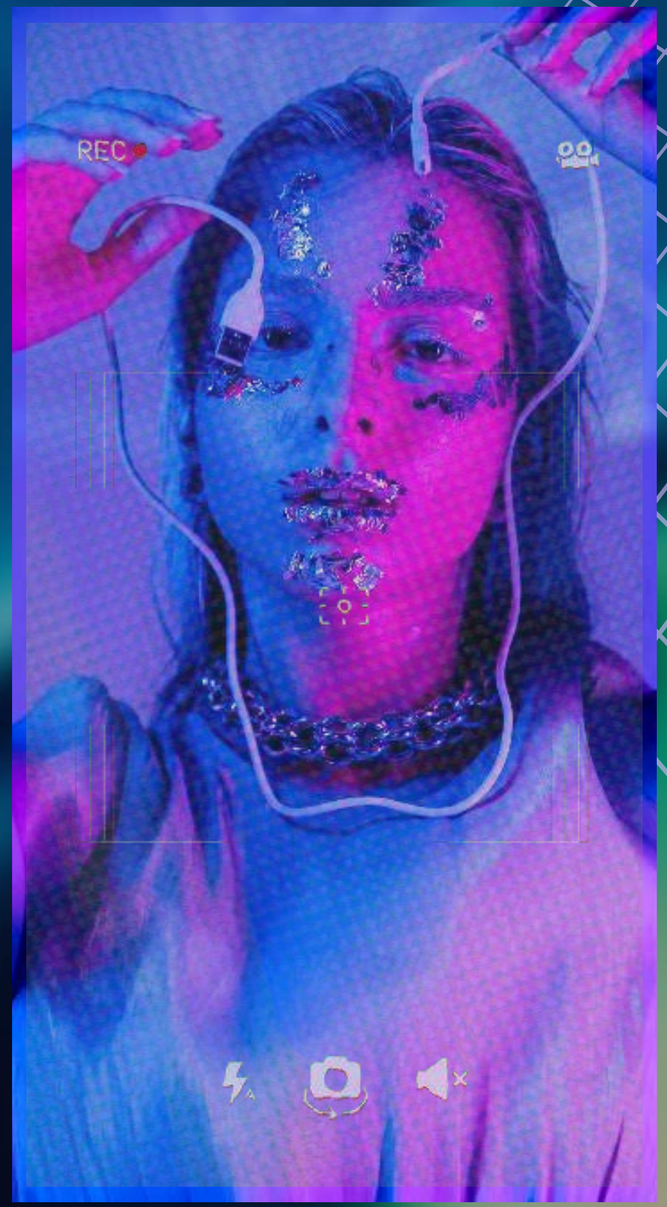
Briefly elaborate on what you want to discuss.

ADD A MAIN POINT

Briefly elaborate on what you want to discuss.

WRITE YOUR TOPIC OR IDEA

Briefly elaborate on what you want to discuss.

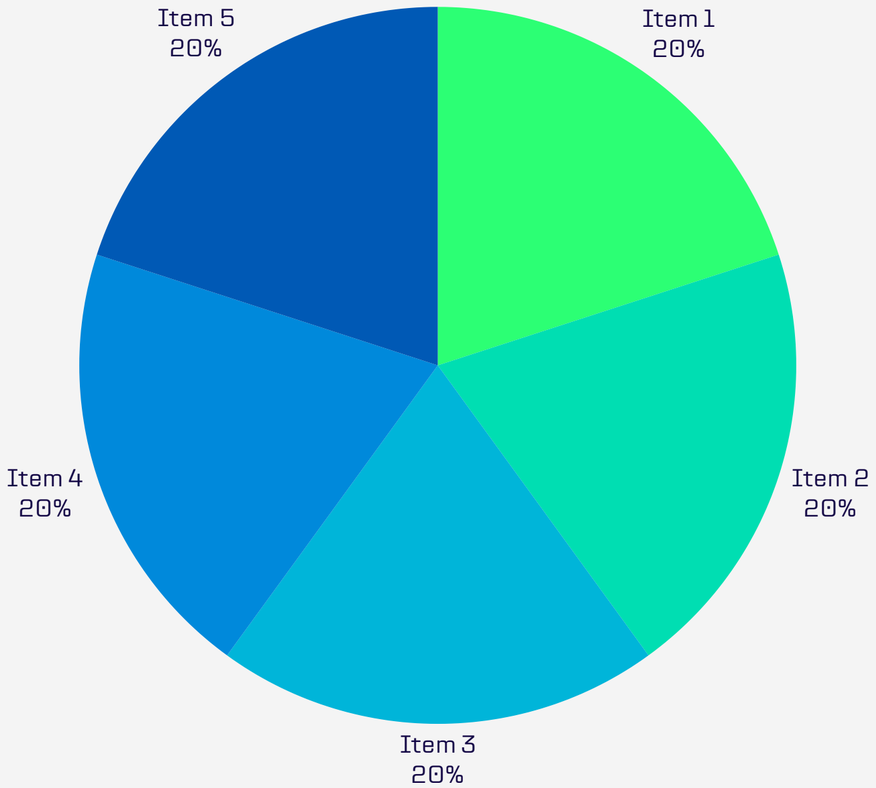


Back to Agenda Page

WRITE YOUR TOPIC OR IDEA

Write a column name	Write a column name	Write a column name	Write a column name	Write a column name

Back to Agenda Page

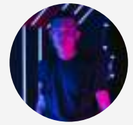


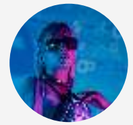
WRITE YOUR TOPIC OR IDEA

Briefly elaborate on what you want to discuss.

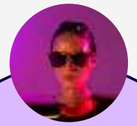
Back to Agenda Page

WHITEBOARD PAGE





Write a note here



Write a note here

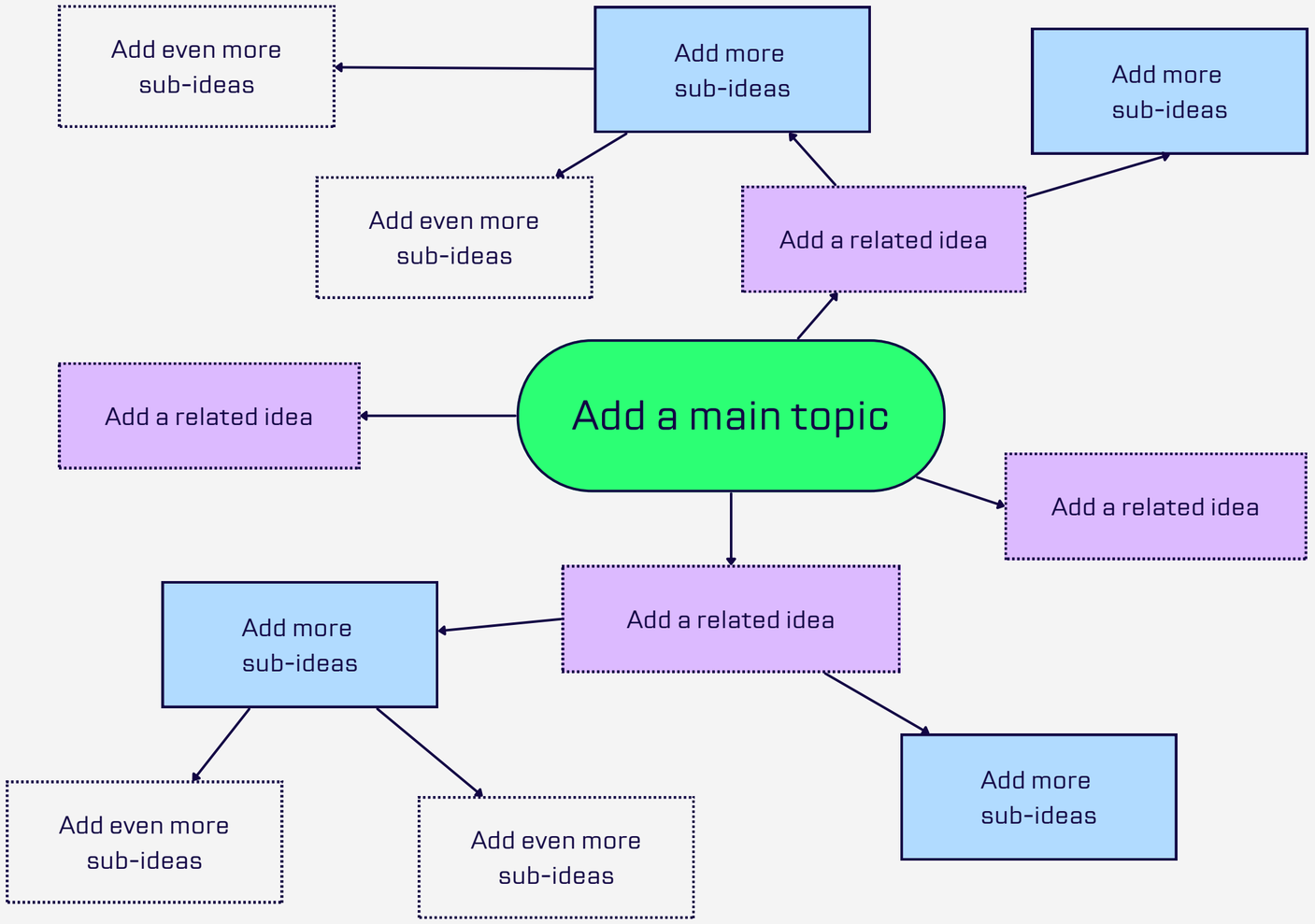
Tip: Collaboration makes teamwork easier! Click "Share" and invite your teammates to fill this up. Use this page for bulletins, brainstorms, and other fun team ideas.

Right-click on the **background** of the slide, or on the **thumbnail** below, for the option to **expand** this page into a **whiteboard** for more space.

Copy a note, drag to the board, and write your ideas.

Copy a note, drag to the board, and write your ideas.

Brainstorm better! Set a time limit for yourself for a more focused brainstorming session.



Tip: Collaboration makes teamwork easier! Click "Share" and invite your teammates to fill this up. Use this page for bulletins, brainstorms, and other fun team ideas.

Right-click on the **background** of the slide, or on the **thumbnail** below, for the option to **expand** this page into a **whiteboard** for more space.

RESOURCE PAGE

Use these design resources in your Canva Presentation. Happy designing!

Don't forget to delete or hide this page before presenting.

RESOURCE PAGE

Use these design resources in your Canva Presentation. Happy designing!

Don't forget to delete or hide this page before presenting.

RESOURCE PAGE

Find the magic and fun in presenting with Canva Presentations. Press the following keys while on Present mode!

Delete or hide this page before presenting.

B for blur	C for confetti
D for a drumroll	M for mic drop
O for bubbles	Q for quiet
U for unveil	Any number from 0-9 for a timer