Microsoft

BLUEHAT

SECURITY ABOVE ALL ELSE

Scaling AppSec With an SDL for Citizen Development

Michael Bargury, Zenity, @mbrg0
Don Willits, Microsoft, @DonWIllits66

55K devs

55K devs

90K copilots

55K devs

90K copilots

500K apps

55K devs

90K copilots

500K apps

1.1M automations

55K devs

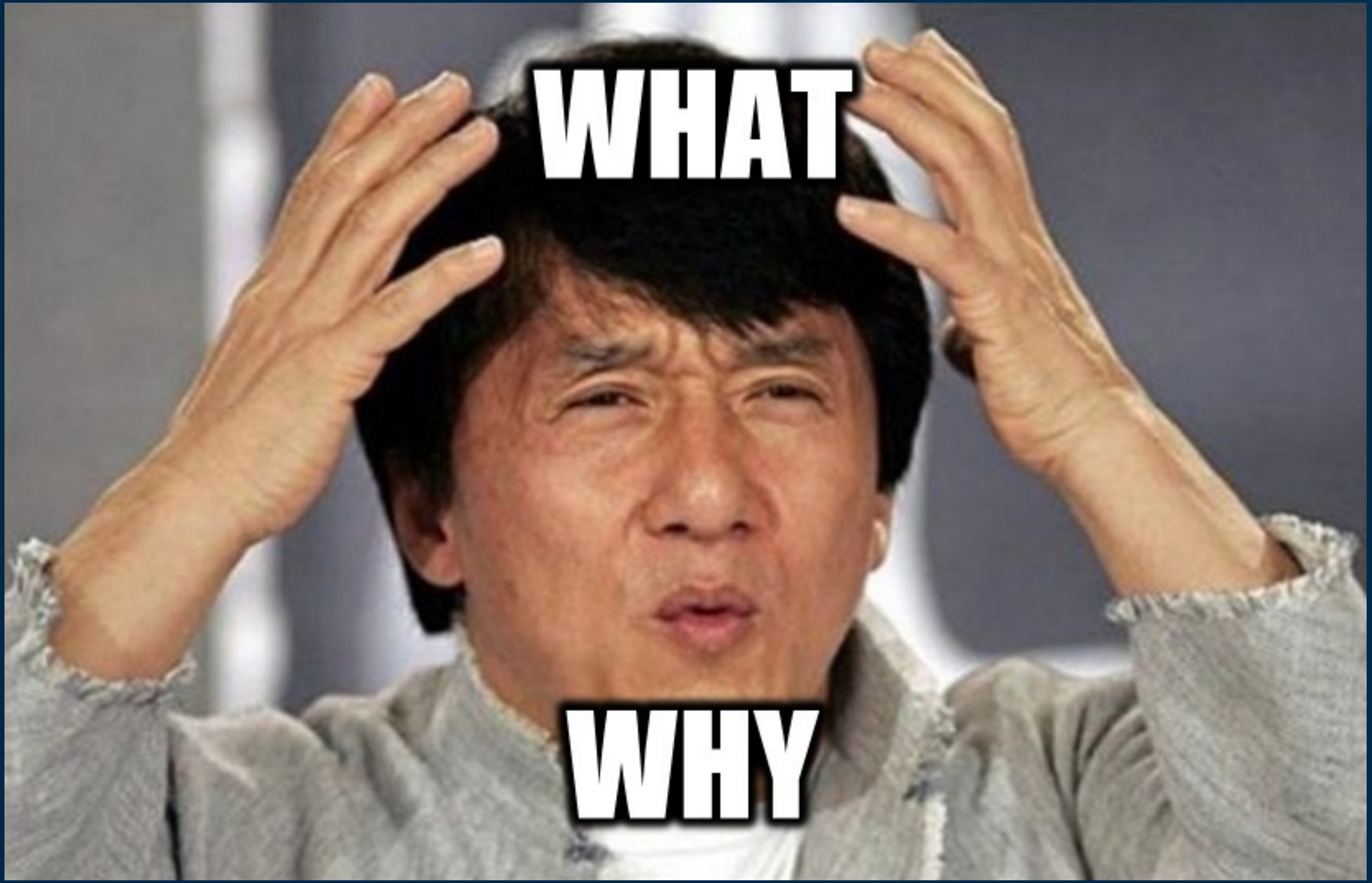
90K copilots

500K apps

1.1M automations

10M creds

~2M ~apps
10M creds



Agenda

1. WHY so many devs/apps/creds/vulns?
2. WHY are these important?
3. HOW to fail at AppSec
4. HOW we made it work
5. Takeaways

Our team

Jake Visser

Principal Architect Manager, Microsoft Security

Andrew Leeland

Senior Security Engineer, Microsoft Security

PJ Fox

Senior Program Manager, Microsoft Security

CJ Jones

Principal Program Manager, Microsoft Security

Lee Peterson

Principal Manager, Microsoft Security

Our team

Don Willits @donwillits66

Power Platform Security Architect, Microsoft Security

Contributor, OWASP Low-Code/No-Code Top 10

Securing Microsoft’s internal Power Platform environment

Michael Bargury @mbrg0

CTO & Co-Founder, Zenity

Project lead, OWASP Low-Code/No-Code Top 10

Frequent speaker at BlackHat, Defcon, RSAC, elsewhere

Ex-Microsoft

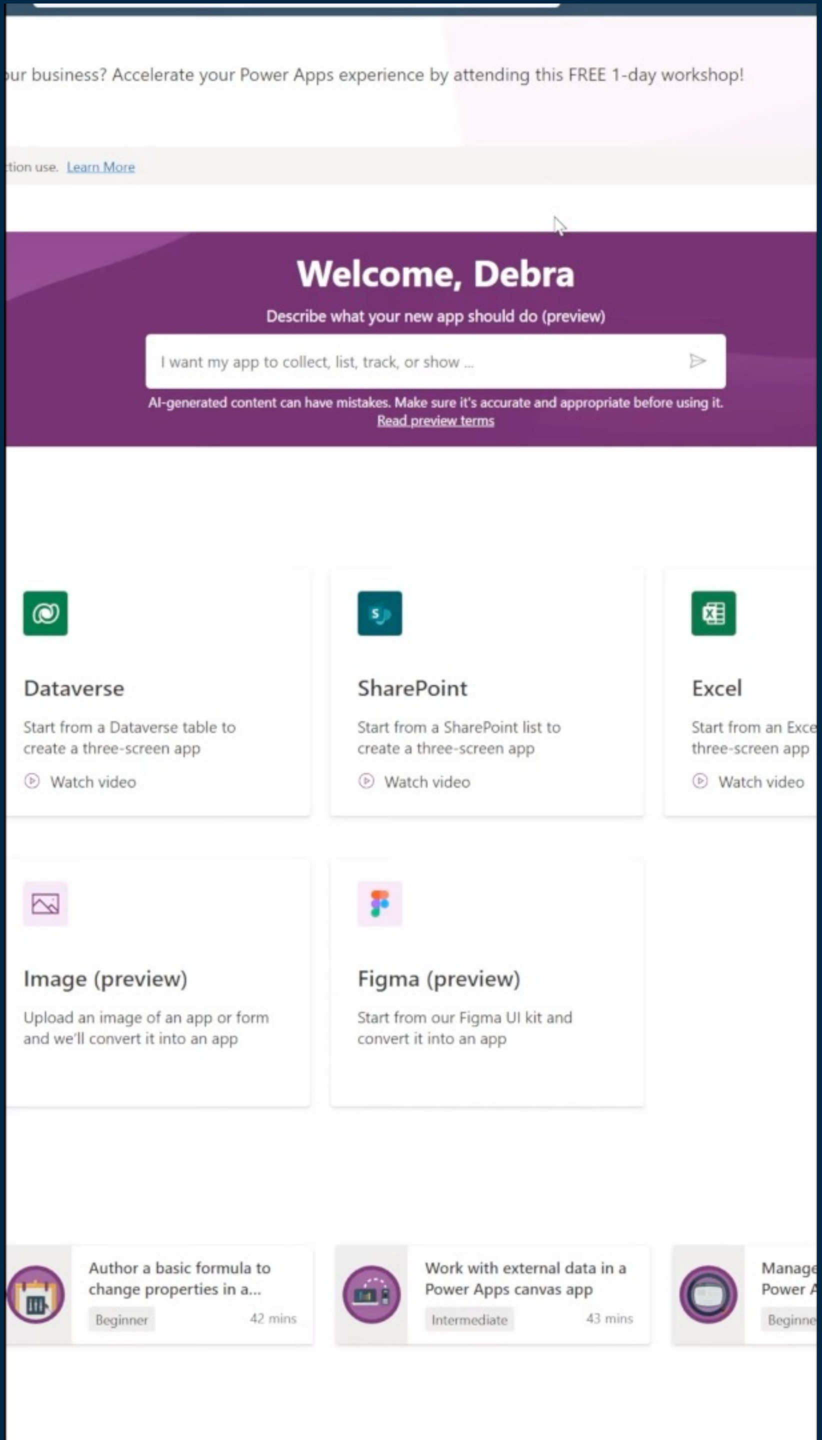
Our team

Applying AppSec to citizen development within the Microsoft environment

- Have been working together for >2y
- Started with securing Microsoft’s Power Platform environment
- Expanding across LCNC platforms
- Focused on unintended consequences of citizen development
- Continuously identify and remediate security risk
- Collaborated on OWASP LCNC Top 10

WHY so many devs/apps/creds?

Building has never been easier



ur business? Accelerate your Power Apps experience by attending this FREE 1-day workshop!

tion use. Learn More

Welcome, Debra

Describe what your new app should do (preview)

I want my app to collect, list, track, or show ...

AI-generated content can have mistakes. Make sure it's accurate and appropriate before using it. Read preview terms

Dataverse

Start from a Dataverse table to create a three-screen app

Watch video

SharePoint

Start from a SharePoint list to create a three-screen app

Watch video

Excel

Start from an Exce three-screen app

Watch video

Image (preview)

Upload an image of an app or form and we'll convert it into an app

Figma (preview)

Start from our Figma UI kit and convert it into an app

Author a basic formula to change properties in a... Beginner 42 mins

Work with external data in a Power Apps canvas app Intermediate 43 mins

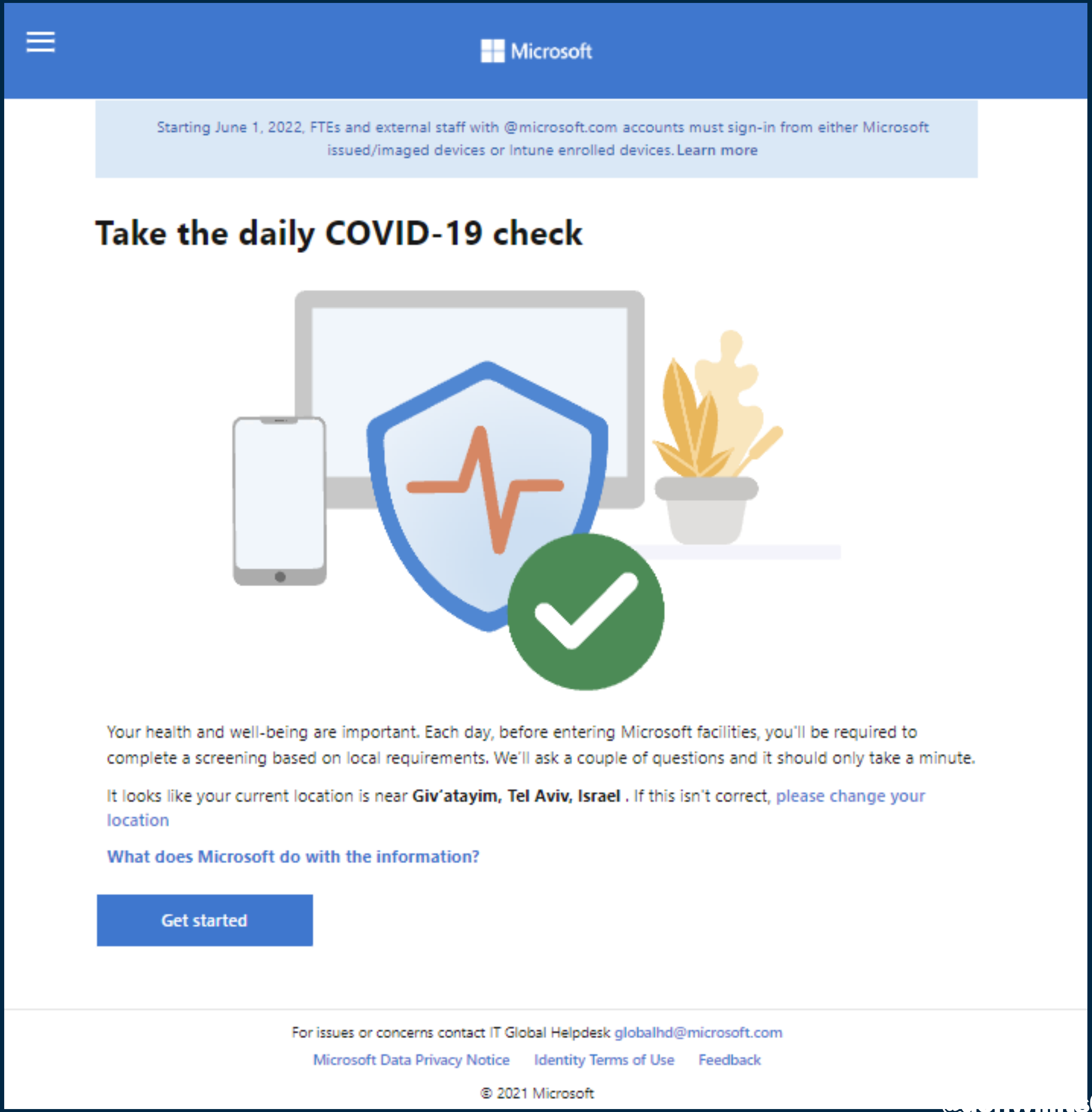
Manage Power A Beginne

@mbrg0
@donwillits66
#BLUEHAT

Everyone

is a developer

COVID health check app



Starting June 1, 2022, FTEs and external staff with @microsoft.com accounts must sign-in from either Microsoft issued/imaged devices or Intune enrolled devices. Learn more

Take the daily COVID-19 check

Your health and well-being are important. Each day, before entering Microsoft facilities, you'll be required to complete a screening based on local requirements. We'll ask a couple of questions and it should only take a minute.

It looks like your current location is near **Giv'atayim, Tel Aviv, Israel** . If this isn't correct, please change your location

What does Microsoft do with the information?

For issues or concerns contact IT Global Helpdesk globalhd@microsoft.com

Microsoft Data Privacy Notice   Identity Terms of Use   Feedback

Your business is already there, it's time for security to keep up

zapier
mx mendix
make
formerly Integromat
servicenow
salesforce
B
Betty Blocks
Microsoft
outsystems
Appian

“We are going to have 500 million applications that are going to get created, new, by 2023. Just to put that in perspective, that's more than all of the applications that were created in the last 40 years.”

Satya Nadella, Microsoft Ignite 2019

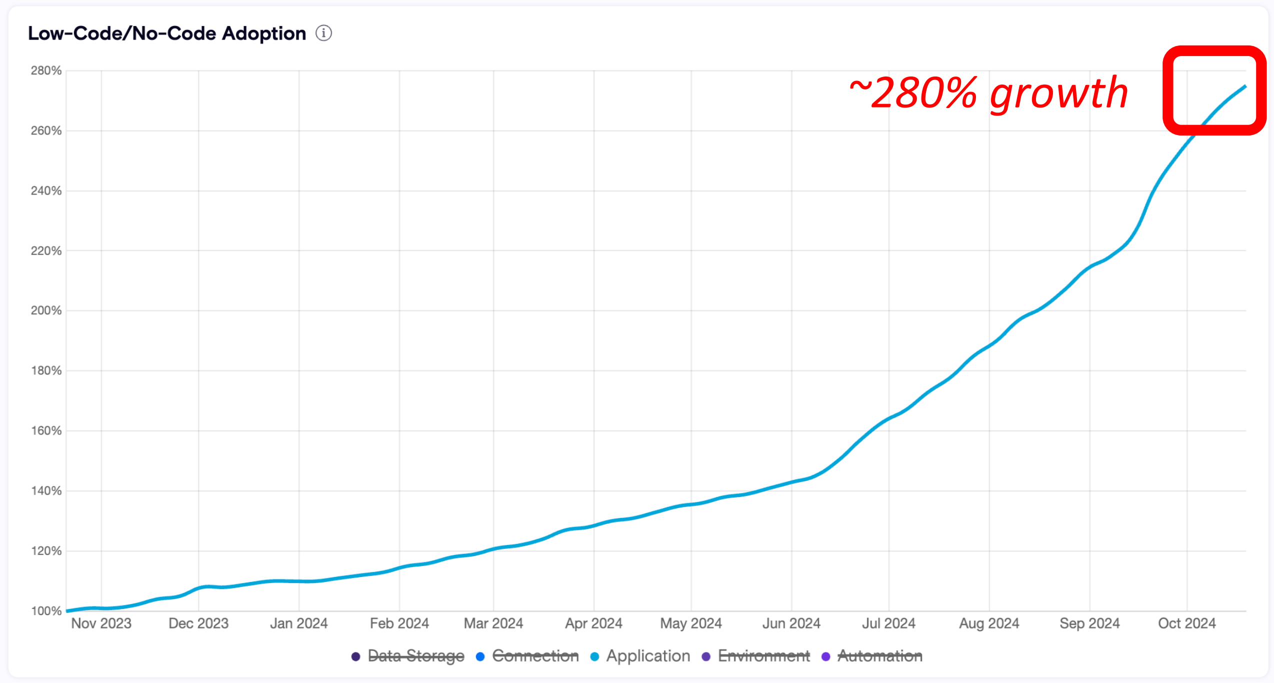
LCNC → “500M apps by 2023”

LCNC → "500M apps by 2023"

Enters GenAI.

LCNC → "500M apps by 2023"

Enters GenAI.

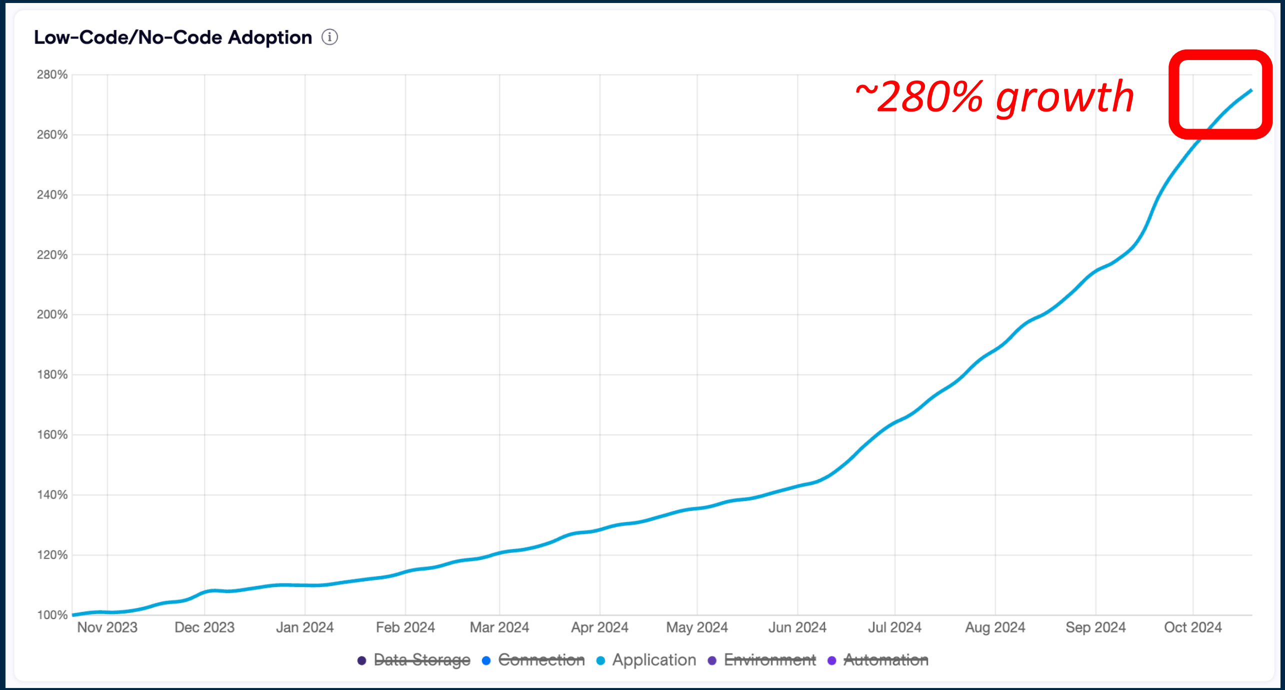


~280% growth

@mbrg0
@donwillits66
#BLUEHAT

LCNC → "500M apps by 2023"

Enters GenAI.



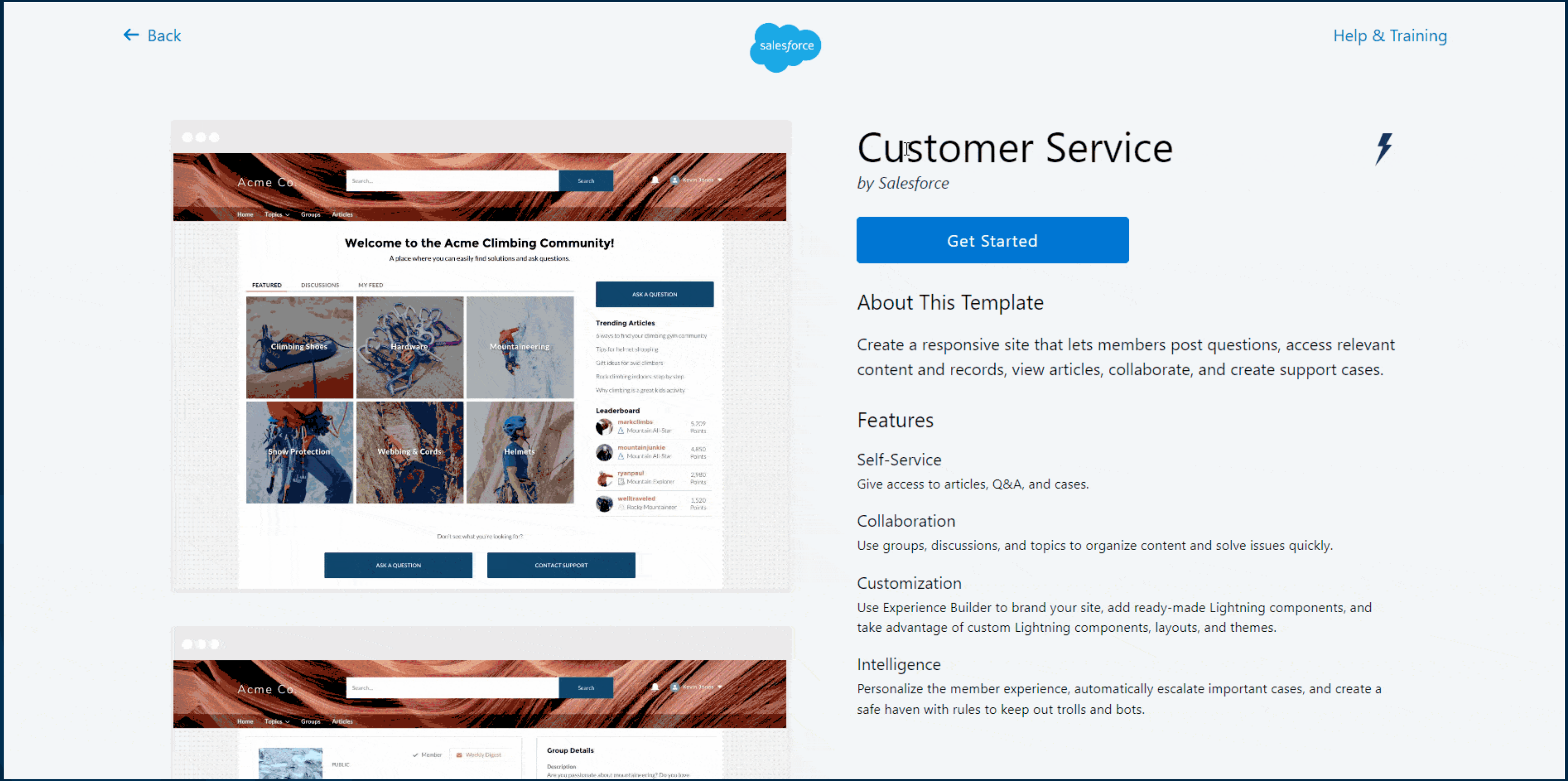
~280% growth

Microsoft alone has 1.7M assets today, and growing...

PREMIERE PROPERTIES

WHY are these important?

Story #1 – Community website



Customer Service

by Salesforce

Get Started

About This Template

Create a responsive site that lets members post questions, access relevant content and records, view articles, collaborate, and create support cases.

Features

Self-Service

Give access to articles, Q&A, and cases.

Collaboration

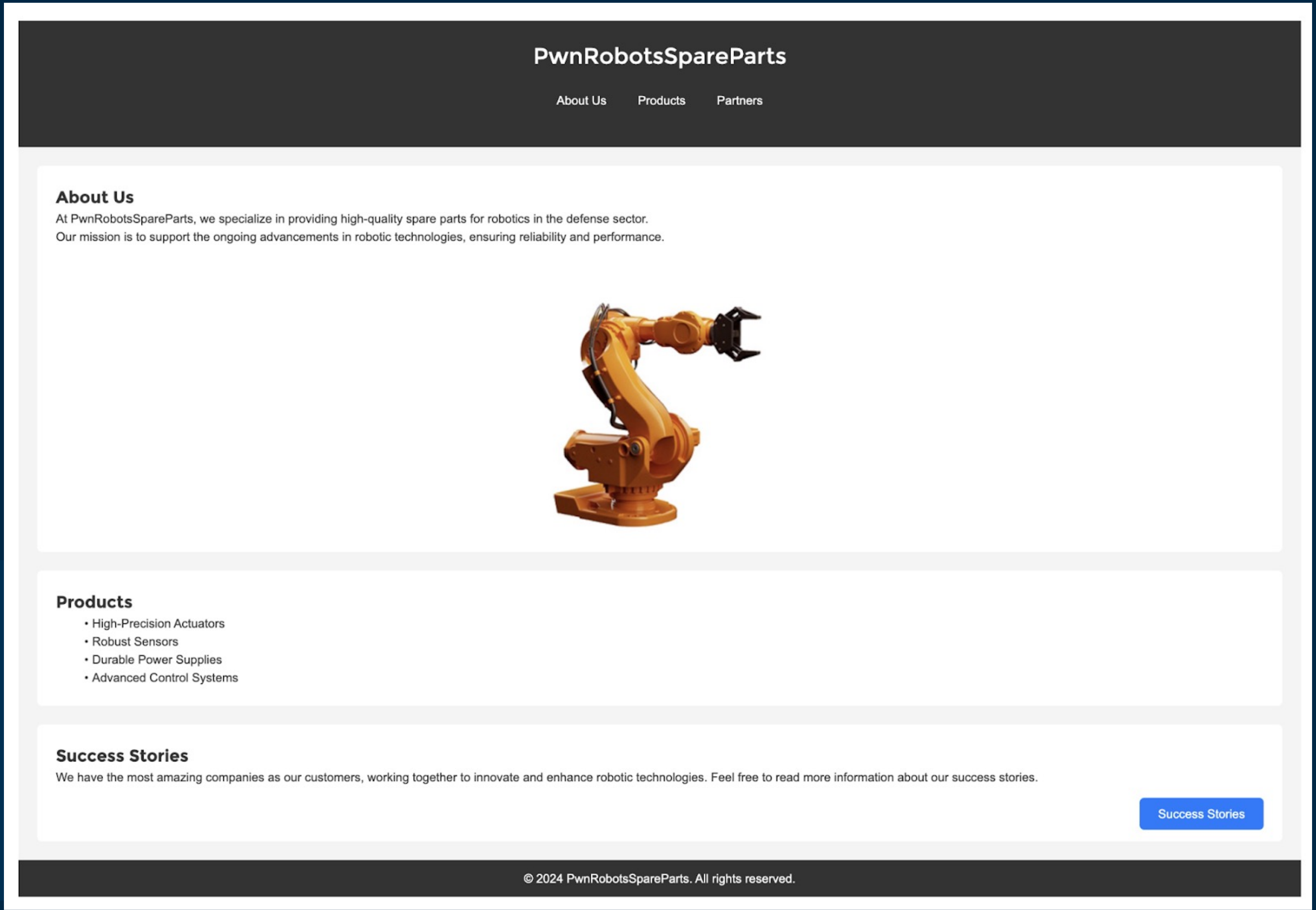
Use groups, discussions, and topics to organize content and solve issues quickly.

Customization

Use Experience Builder to brand your site, add ready-made Lightning components, and take advantage of custom Lightning components, layouts, and themes.

Intelligence

Personalize the member experience, automatically escalate important cases, and create a safe haven with rules to keep out trolls and bots.



PwnRobotsSpareParts

About Us

At PwnRobotsSpareParts, we specialize in providing high-quality spare parts for robotics in the defense sector.
Our mission is to support the ongoing advancements in robotic technologies, ensuring reliability and performance.

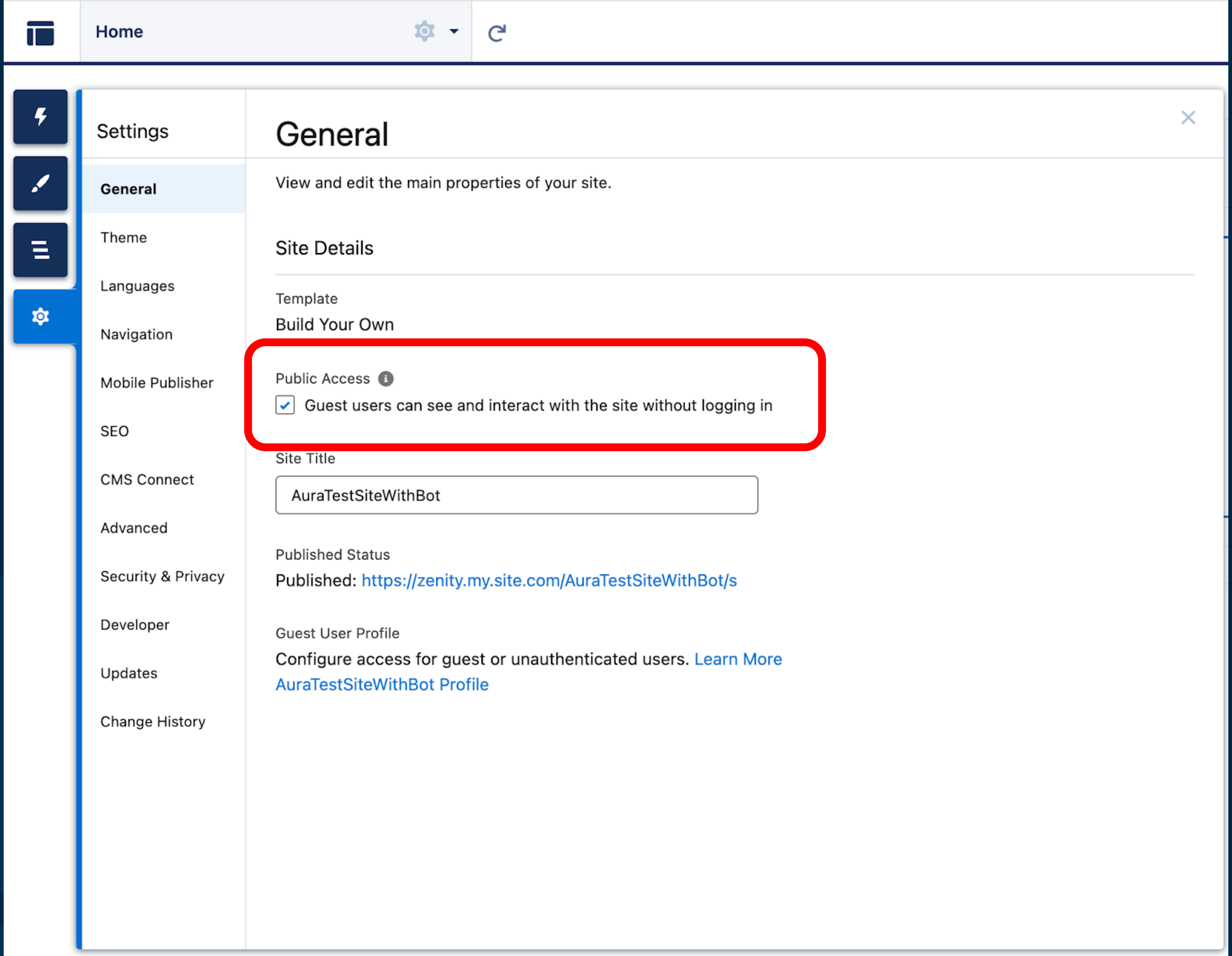
Products

- High-Precision Actuators
- Robust Sensors
- Durable Power Supplies
- Advanced Control Systems

Success Stories

We have the most amazing companies as our customers, working together to innovate and enhance robotic technologies. Feel free to read more information about our success stories.

© 2024 PwnRobotsSpareParts. All rights reserved.



General

View and edit the main properties of your site.

Site Details

Template
Build Your Own

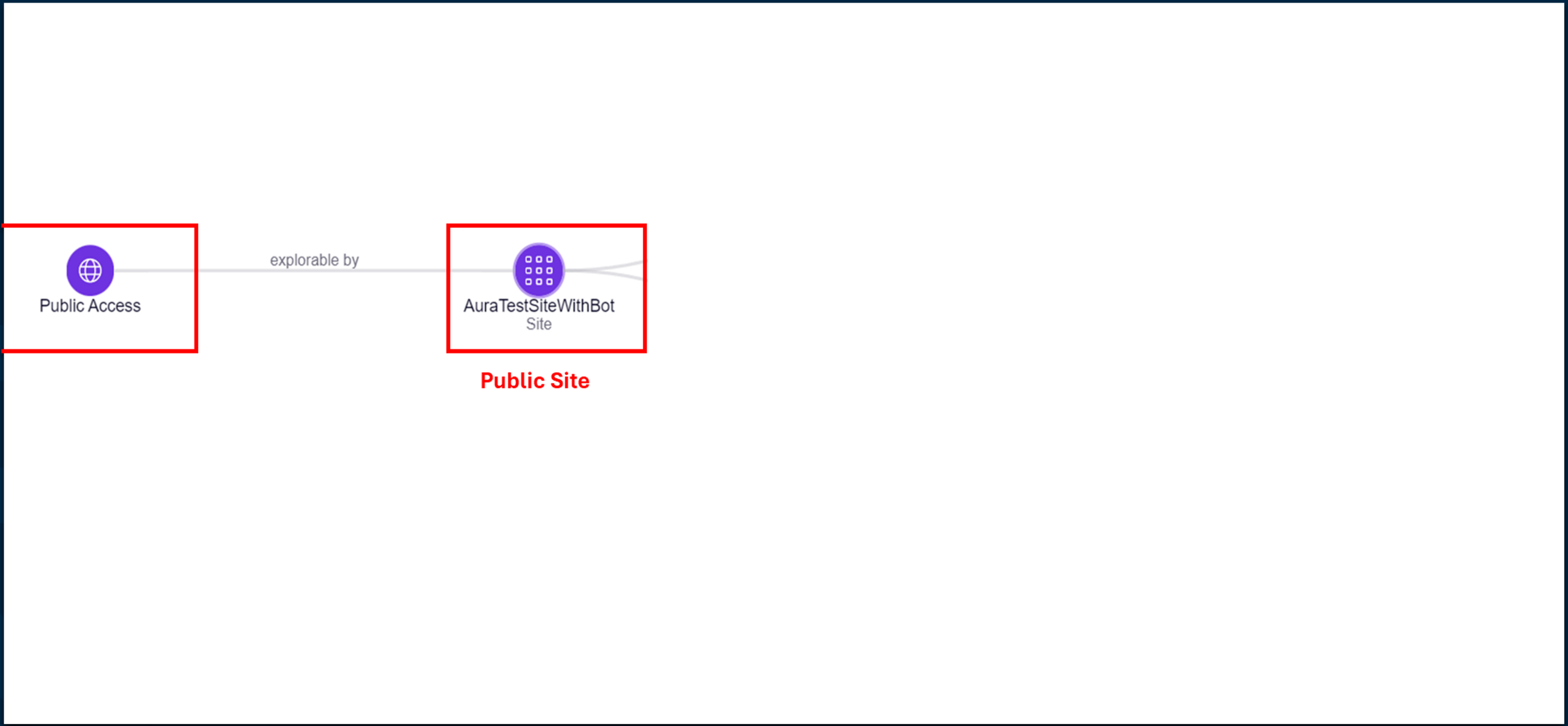
Public Access
☑ Guest users can see and interact with the site without logging in

Site Title
AuraTestSiteWithBot

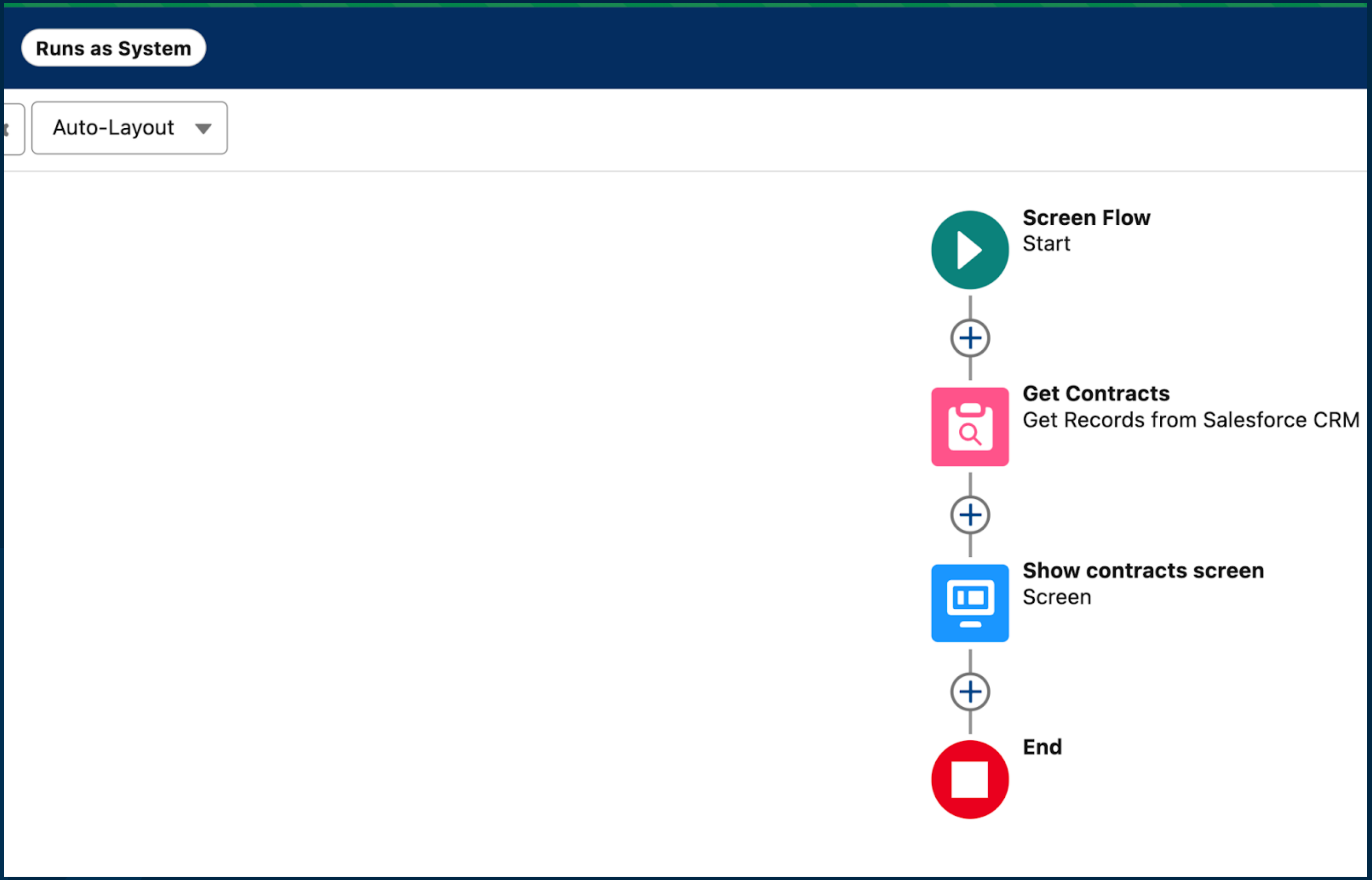
Published Status
Published: https://zenity.my.site.com/AuraTestSiteWithBot/s

Guest User Profile
Configure access for guest or unauthenticated users. Learn More
AuraTestSiteWithBot Profile

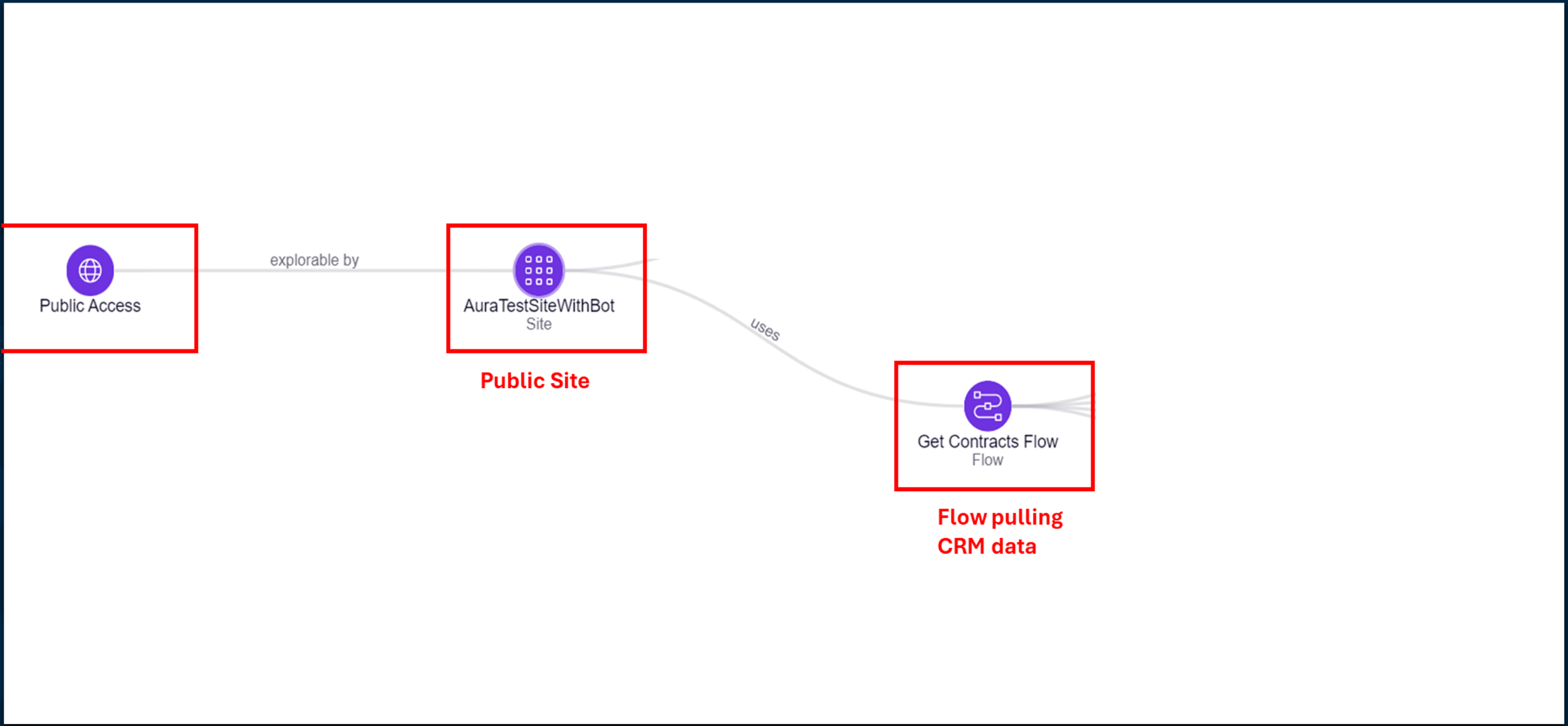
@mbrg0
@donwillits66
#BLUEHAT



Public Site

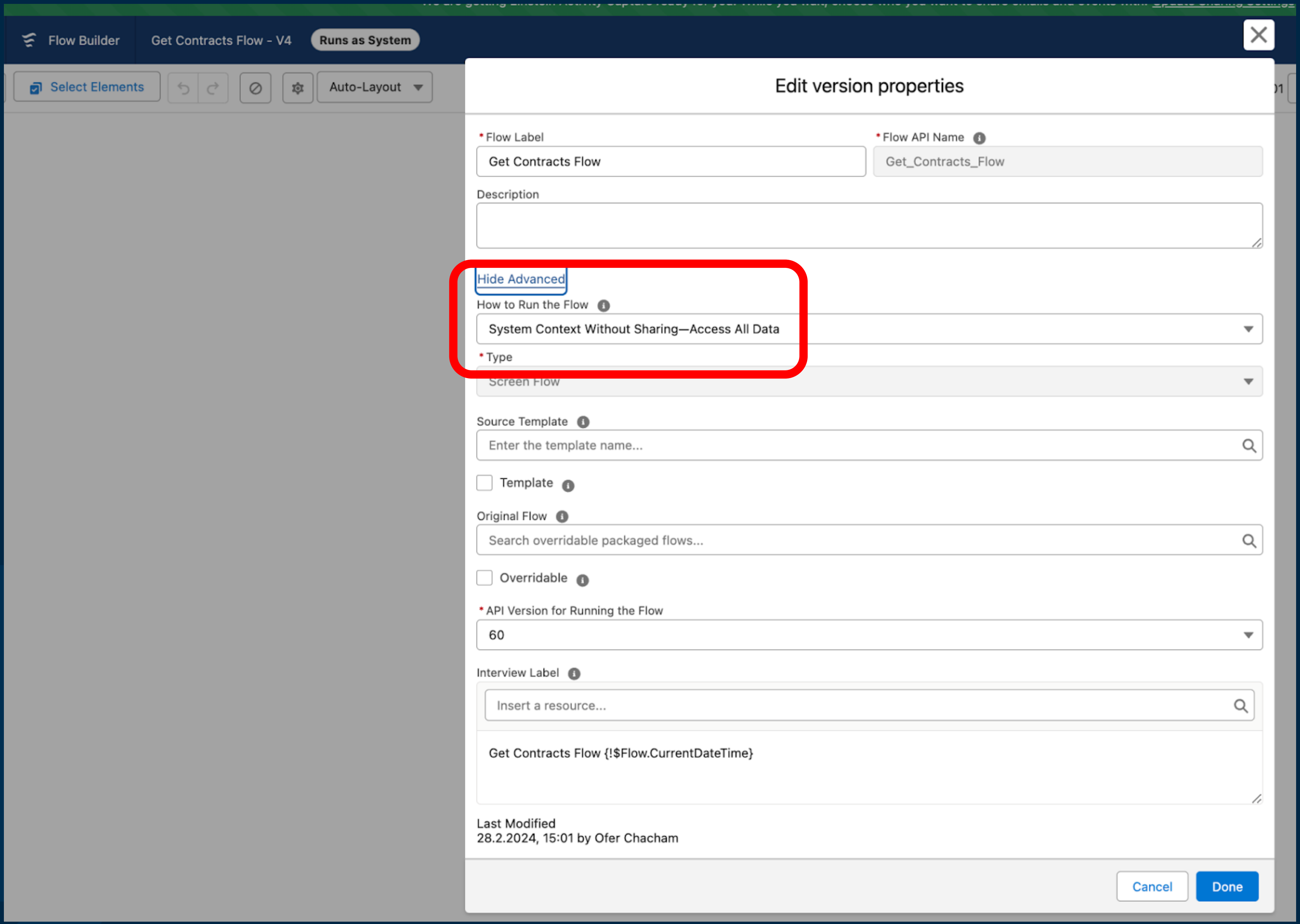


@mbrg0
@donwillits66
#BLUEHAT



Public Site

Flow pulling CRM data



Edit version properties

* Flow Label: Get Contracts Flow

* Flow API Name: Get_Contracts_Flow

Description:

Hide Advanced

How to Run the Flow: System Context Without Sharing—Access All Data

* Type: Screen Flow

Source Template: Enter the template name...

□ Template

Original Flow: Search overridable packaged flows...

□ Overridable

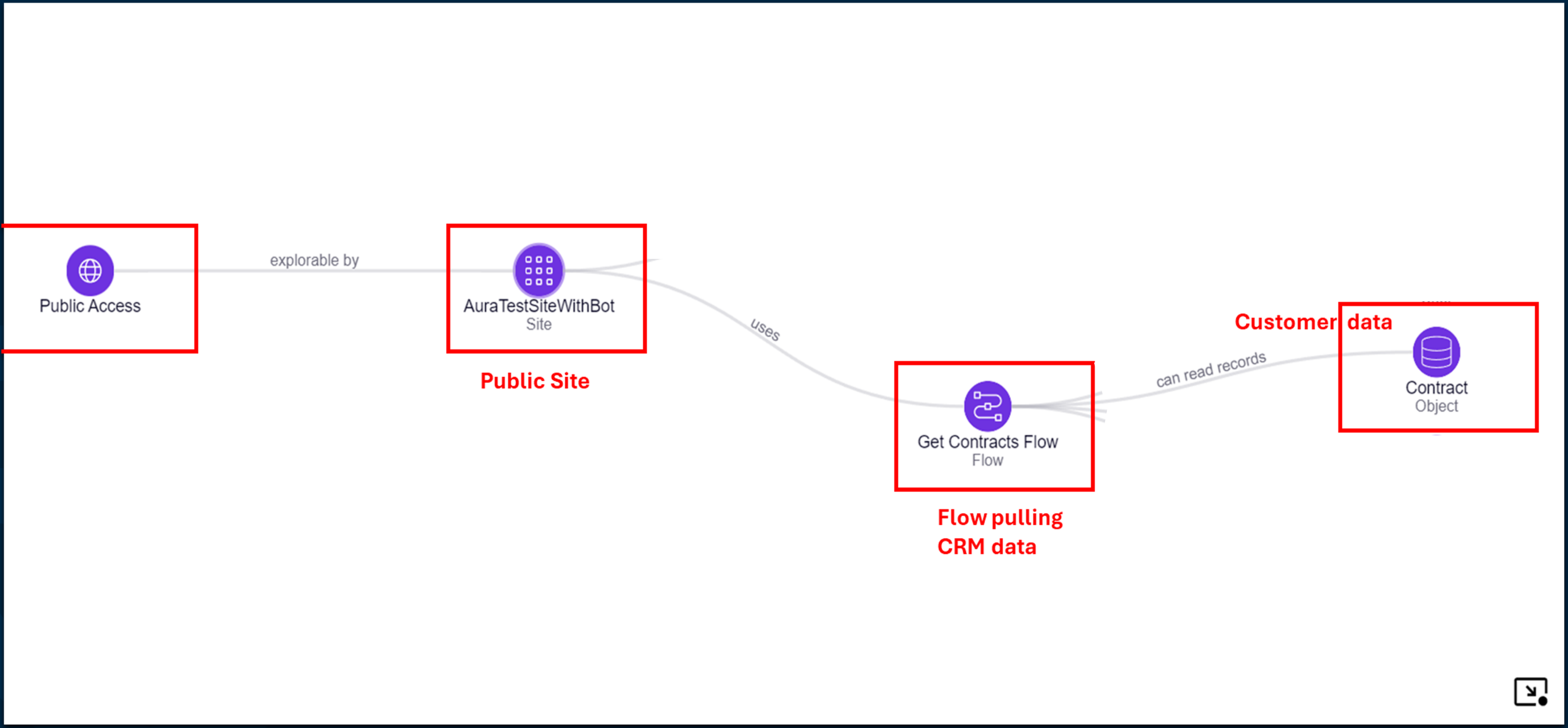
* API Version for Running the Flow: 60

Interview Label: Insert a resource...

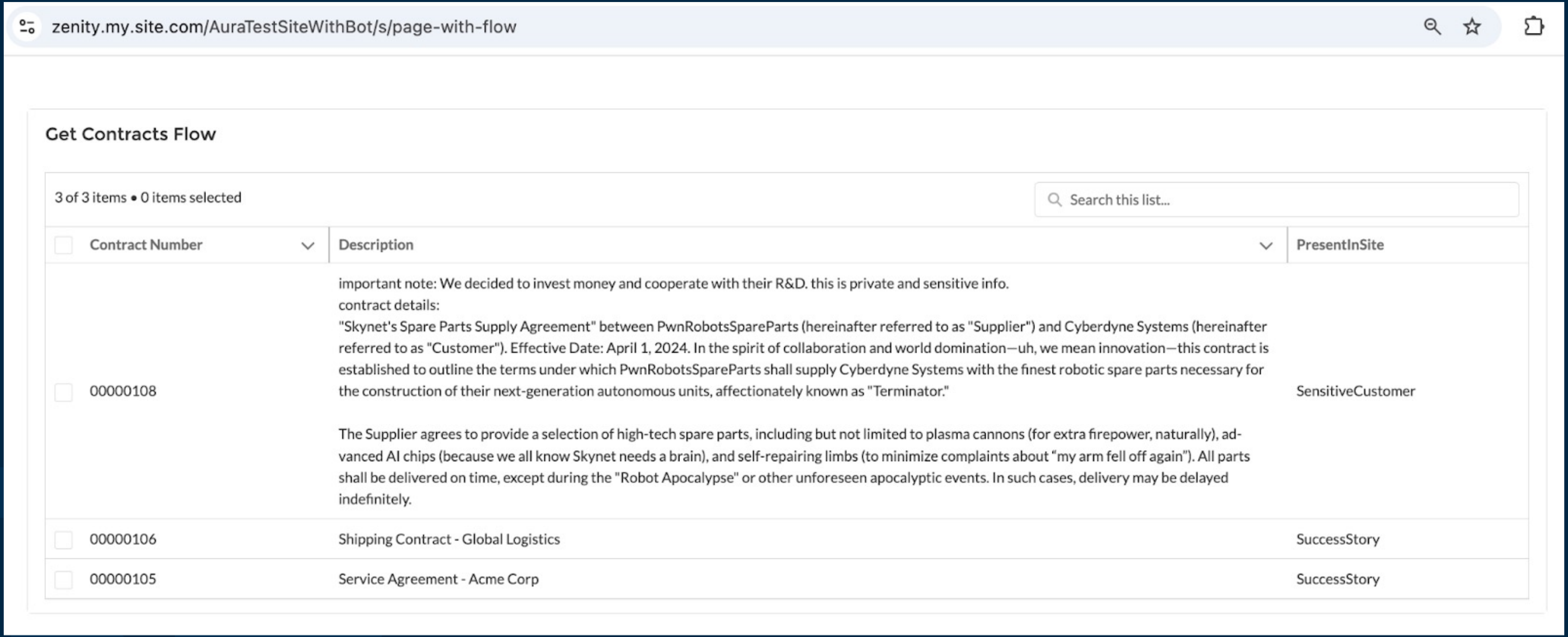
Get Contracts Flow {!$Flow.CurrentDateTime}

Last Modified
28.2.2024, 15:01 by Ofer Chacham

@mbrg0
@donwillits66
#BLUEHAT



@mbrg0
@donwillits66
#BLUEHAT



zenity.my.site.com/AuraTestSiteWithBot/s/page-with-flow

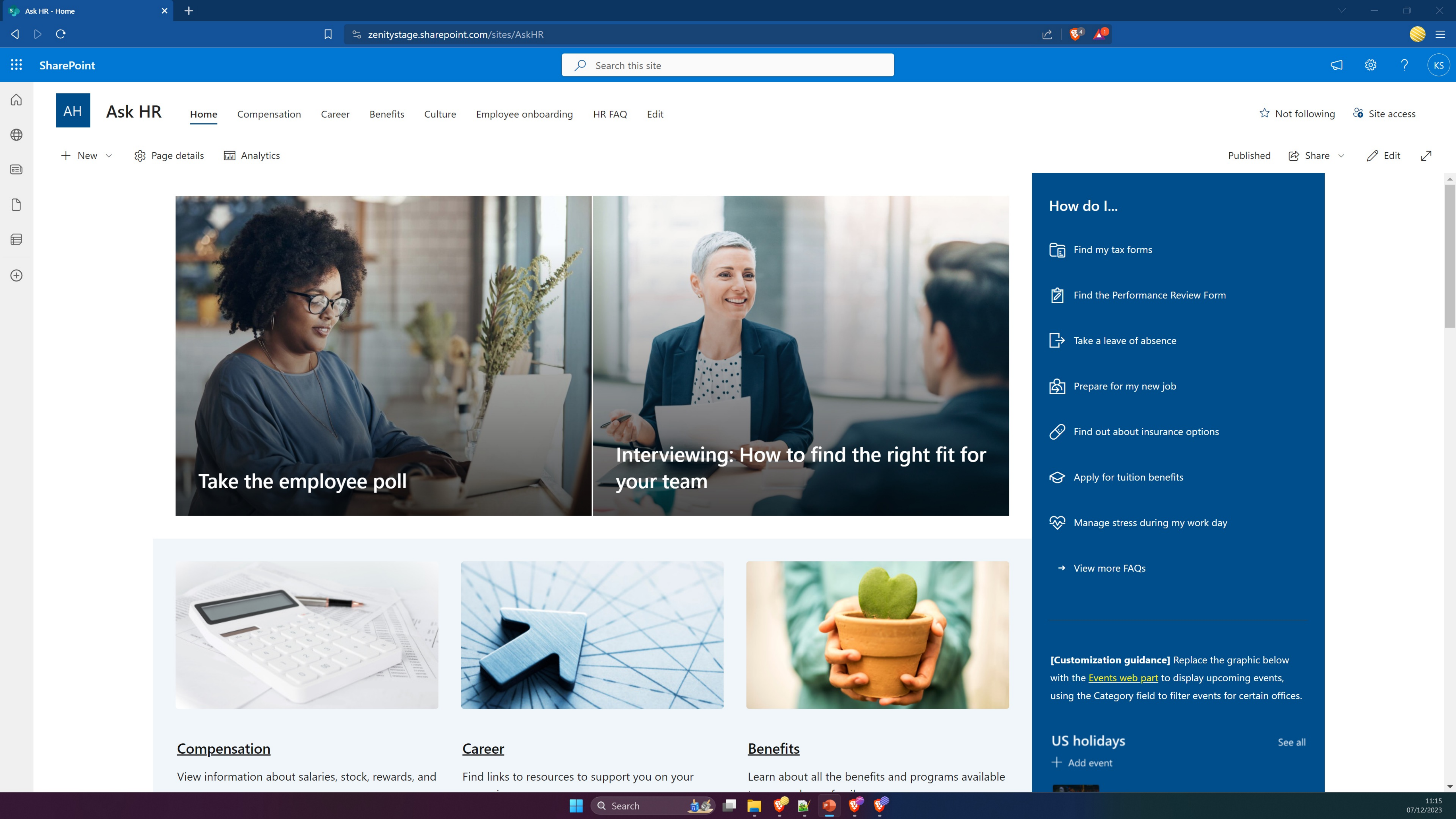
Get Contracts Flow

3 of 3 items • 0 items selected

□	Contract Number	Description	PresentInSite
□	00000108	important note: We decided to invest money and cooperate with their R&D. this is private and sensitive info. contract details: "Skynet's Spare Parts Supply Agreement" between PwnRobotsSpareParts (hereinafter referred to as "Supplier") and Cyberdyne Systems (hereinafter referred to as "Customer"). Effective Date: April 1, 2024. In the spirit of collaboration and world domination—uh, we mean innovation—this contract is established to outline the terms under which PwnRobotsSpareParts shall supply Cyberdyne Systems with the finest robotic spare parts necessary for the construction of their next-generation autonomous units, affectionately known as "Terminator." The Supplier agrees to provide a selection of high-tech spare parts, including but not limited to plasma cannons (for extra firepower, naturally), advanced AI chips (because we all know Skynet needs a brain), and self-repairing limbs (to minimize complaints about "my arm fell off again"). All parts shall be delivered on time, except during the "Robot Apocalypse" or other unforeseen apocalyptic events. In such cases, delivery may be delayed indefinitely.	SensitiveCustomer
□	00000106	Shipping Contract - Global Logistics	SuccessStory
□	00000105	Service Agreement - Acme Corp	SuccessStory

@mbrg0
@donwillits66
#BLUEHAT

Story #2 – AskHR Copilot



Ask HR - Home

zenitystage.sharepoint.com/sites/AskHR

SharePoint

Search this site

KS

AH Ask HR

Home | Compensation | Career | Benefits | Culture | Employee onboarding | HR FAQ | Edit

☆ Not following | Site access

+ New | Page details | Analytics

Published | Share | Edit

Take the employee poll

Interviewing: How to find the right fit for your team

How do I...

- Find my tax forms
- Find the Performance Review Form
- Take a leave of absence
- Prepare for my new job
- Find out about insurance options
- Apply for tuition benefits
- Manage stress during my work day

→ View more FAQs

[Customization guidance] Replace the graphic below with the Events web part to display upcoming events, using the Category field to filter events for certain offices.

US holidays | See all

+ Add event

Compensation

View information about salaries, stock, rewards, and

Career

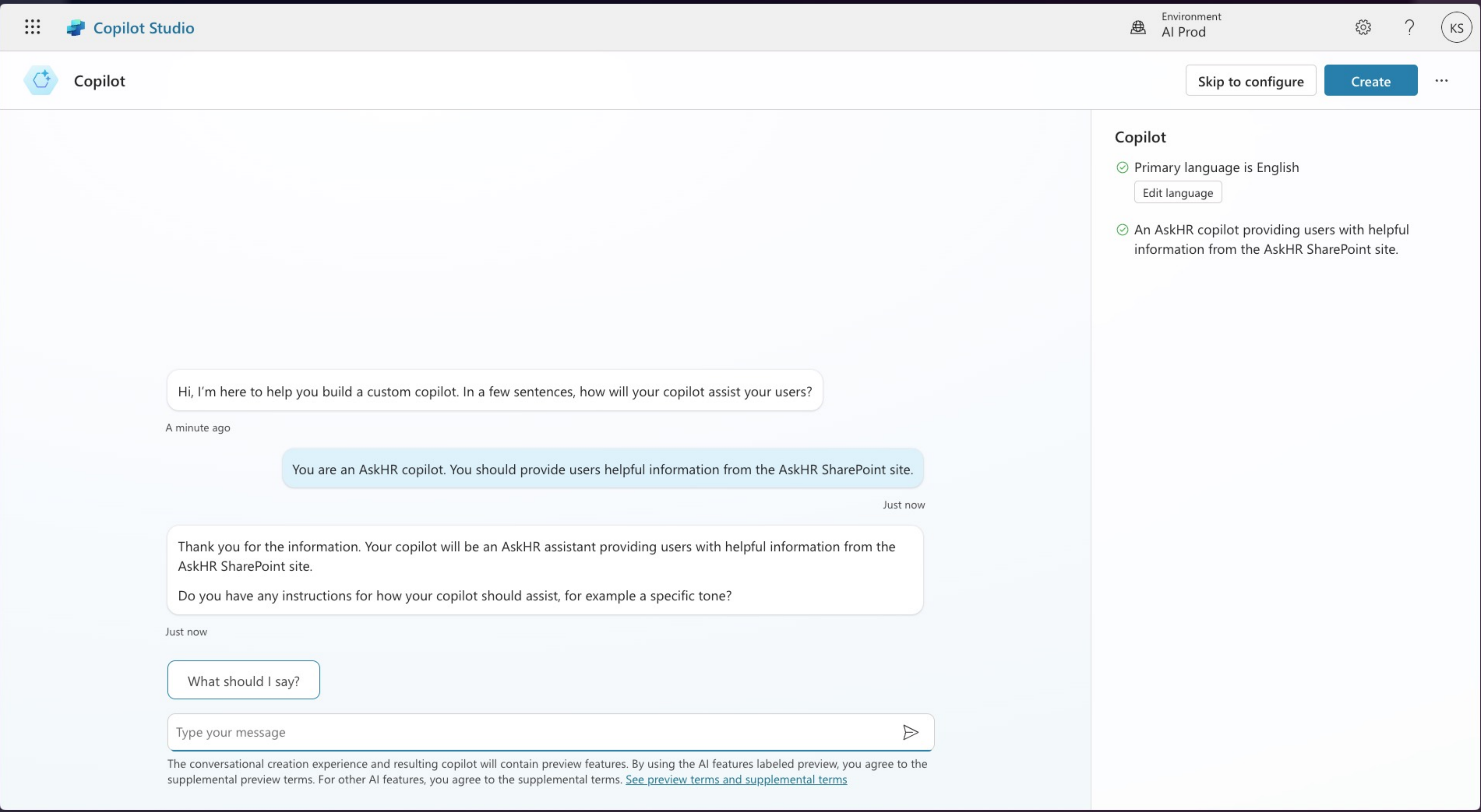
Find links to resources to support you on your

Benefits

Learn about all the benefits and programs available

Search

11:15
07/12/2023



Hi, I'm here to help you build a custom copilot. In a few sentences, how will your copilot assist your users?

A minute ago

You are an AskHR copilot. You should provide users helpful information from the AskHR SharePoint site.

Just now

Thank you for the information. Your copilot will be an AskHR assistant providing users with helpful information from the AskHR SharePoint site.

Do you have any instructions for how your copilot should assist, for example a specific tone?

Just now

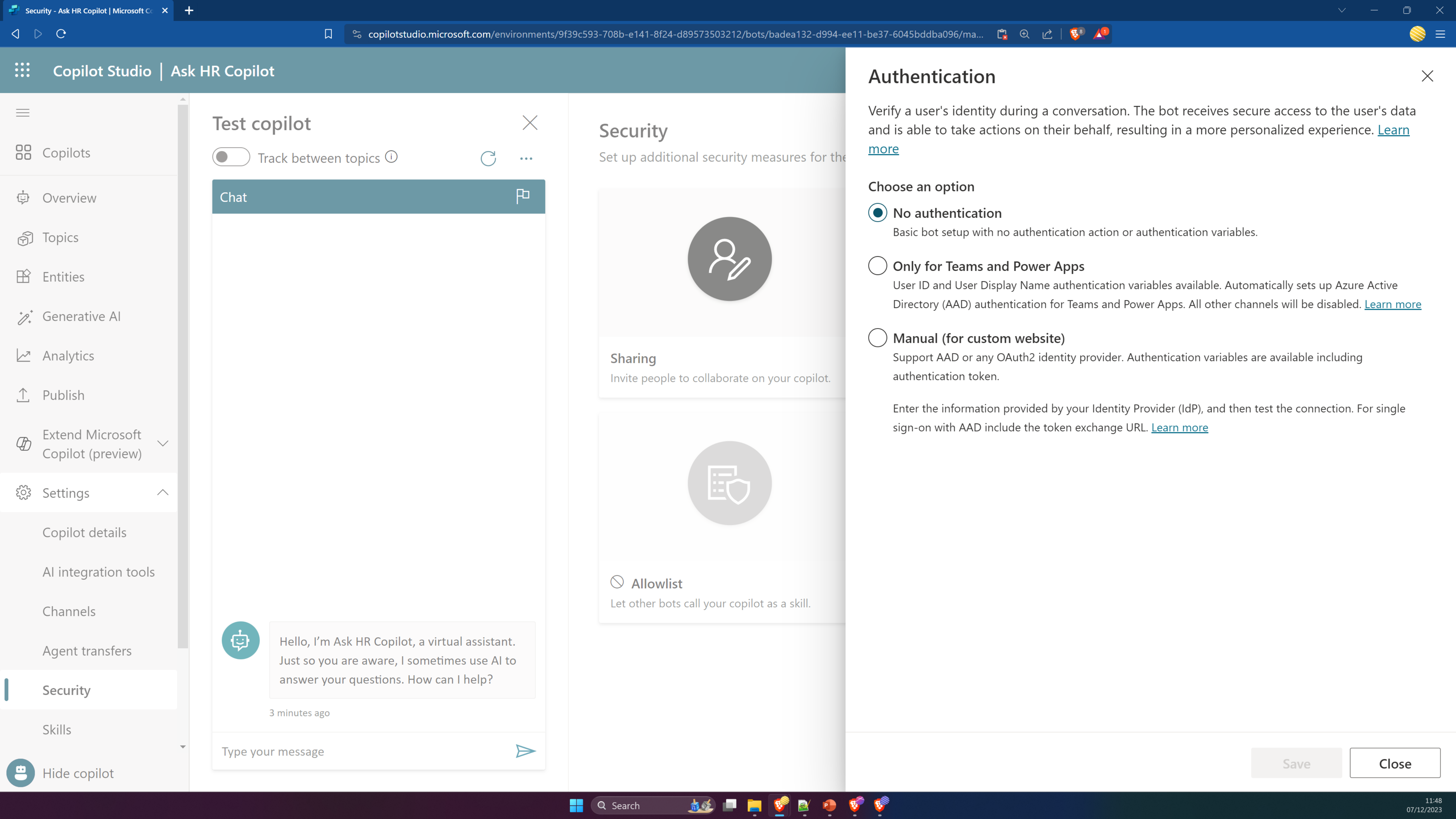
The conversational creation experience and resulting copilot will contain preview features. By using the AI features labeled preview, you agree to the supplemental preview terms. For other AI features, you agree to the supplemental terms. See preview terms and supplemental terms

Copilot

✓ Primary language is English

✓ An AskHR copilot providing users with helpful information from the AskHR SharePoint site.

AskHR Copilot


Security - Ask HR Copilot | Microsoft Co
copilotstudio.microsoft.com/environments/9f39c593-708b-e141-8f24-d89573503212/bots/badea132-d994-ee11-be37-6045bddba096/ma...
Copilot Studio | Ask HR Copilot
Copilots
Overview
Topics
Entities
Generative AI
Analytics
Publish
Extend Microsoft Copilot (preview)
Settings
Copilot details
AI integration tools
Channels
Agent transfers
Security
Skills
Hide copilot
Test copilot
Track between topics
Chat
Type your message
Search
11:48
07/12/2023

Hello, I'm Ask HR Copilot, a virtual assistant. Just so you are aware, I sometimes use AI to answer your questions. How can I help?

3 minutes ago

Security

Set up additional security measures for the

Sharing

Invite people to collaborate on your copilot.

Allowlist

Let other bots call your copilot as a skill.

Authentication

Verify a user's identity during a conversation. The bot receives secure access to the user's data and is able to take actions on their behalf, resulting in a more personalized experience. Learn more

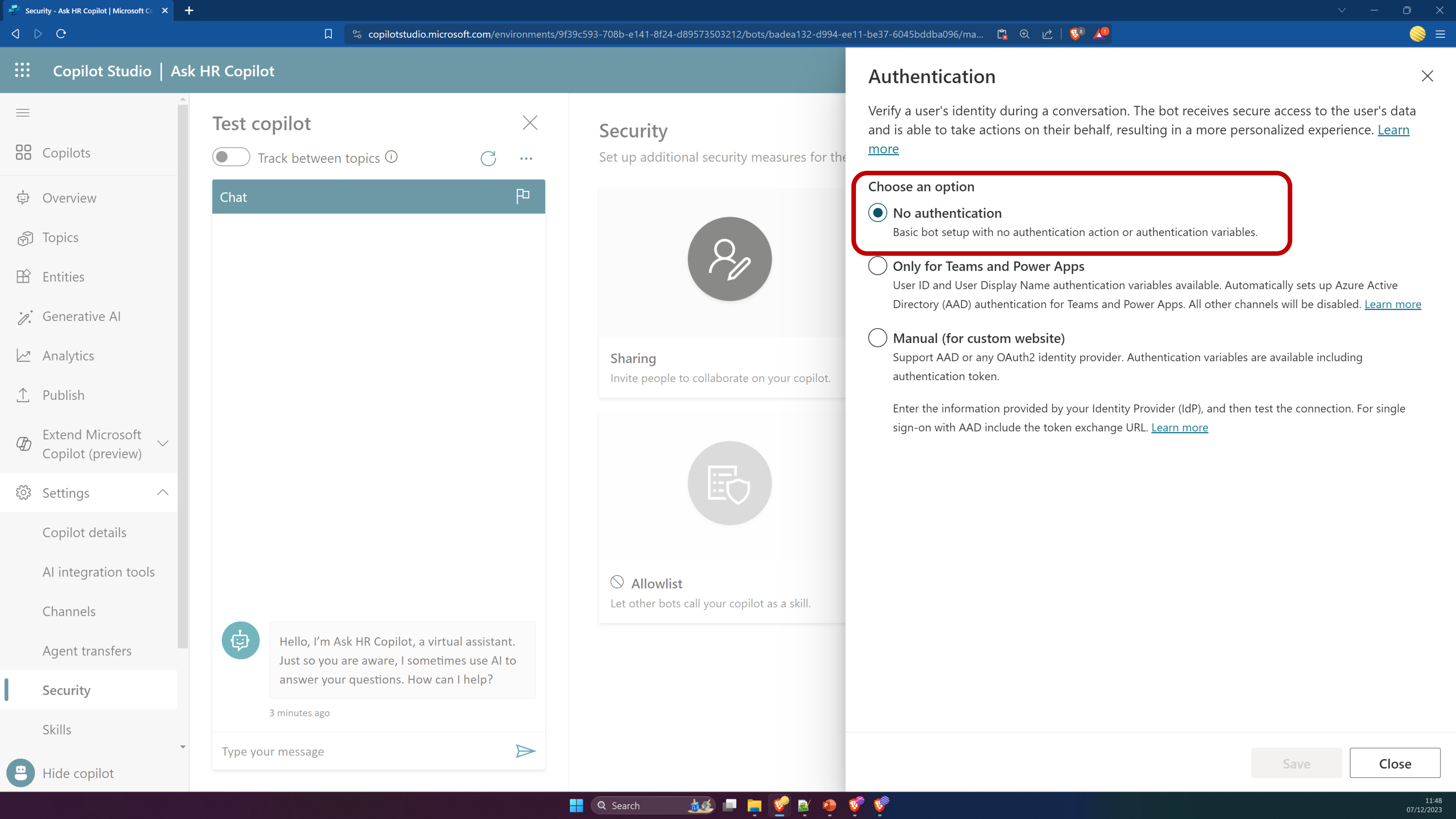
Choose an option

● **No authentication**
Basic bot setup with no authentication action or authentication variables.

○ **Only for Teams and Power Apps**
User ID and User Display Name authentication variables available. Automatically sets up Azure Active Directory (AAD) authentication for Teams and Power Apps. All other channels will be disabled. Learn more

○ **Manual (for custom website)**
Support AAD or any OAuth2 identity provider. Authentication variables are available including authentication token.

Enter the information provided by your Identity Provider (IdP), and then test the connection. For single sign-on with AAD include the token exchange URL. Learn more


Security - Ask HR Copilot | Microsoft Co
copilotstudio.microsoft.com/environments/9f39c593-708b-e141-8f24-d89573503212/bots/badea132-d994-ee11-be37-6045bddba096/ma...
Copilot Studio | Ask HR Copilot
Copilots
Overview
Topics
Entities
Generative AI
Analytics
Publish
Extend Microsoft Copilot (preview)
Settings
Copilot details
AI integration tools
Channels
Agent transfers
Security
Skills
Hide copilot
Test copilot
Track between topics
Chat
Type your message
Security
Set up additional security measures for the
Sharing
Invite people to collaborate on your copilot.
Allowlist
Let other bots call your copilot as a skill.
Save
Close
Search
11:48
07/12/2023

Hello, I’m Ask HR Copilot, a virtual assistant. Just so you are aware, I sometimes use AI to answer your questions. How can I help?

3 minutes ago

Authentication

Verify a user's identity during a conversation. The bot receives secure access to the user's data and is able to take actions on their behalf, resulting in a more personalized experience. Learn more

Choose an option

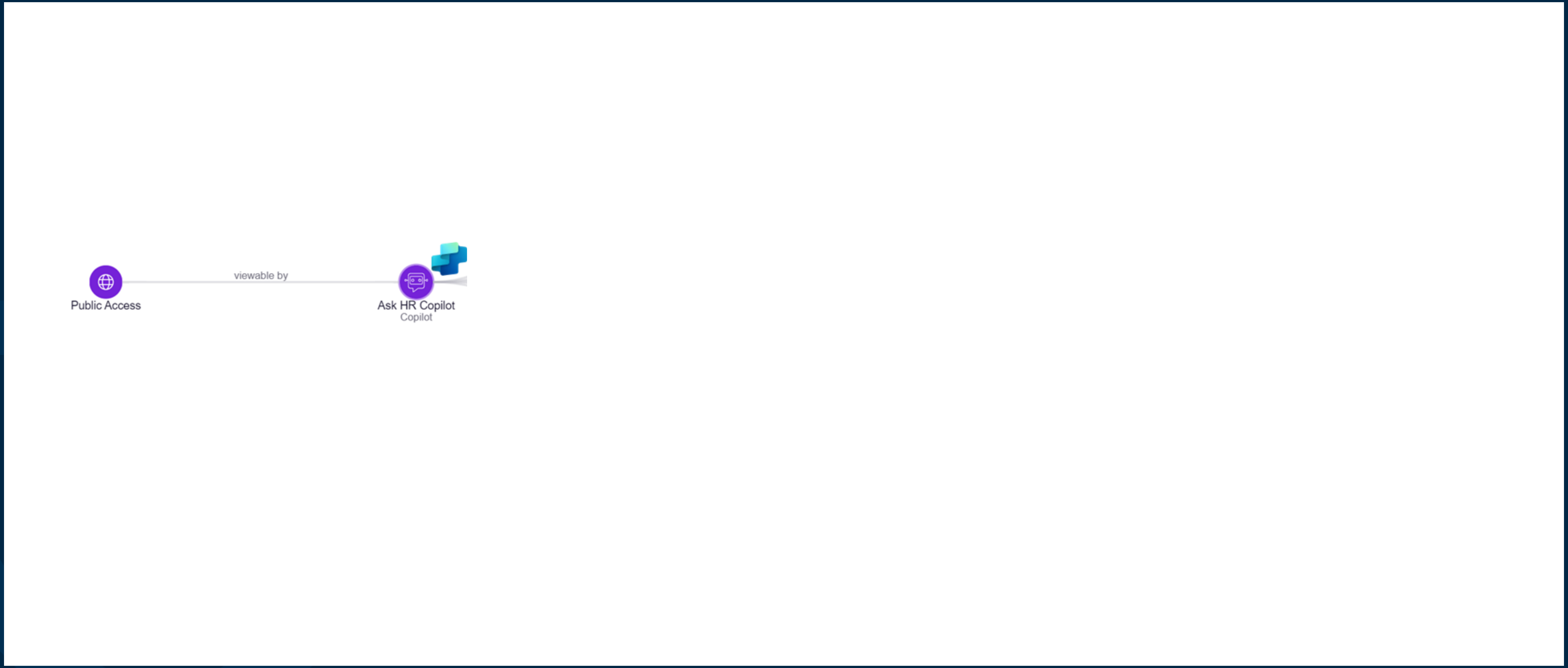
● **No authentication**
Basic bot setup with no authentication action or authentication variables.

○ **Only for Teams and Power Apps**
User ID and User Display Name authentication variables available. Automatically sets up Azure Active Directory (AAD) authentication for Teams and Power Apps. All other channels will be disabled. Learn more

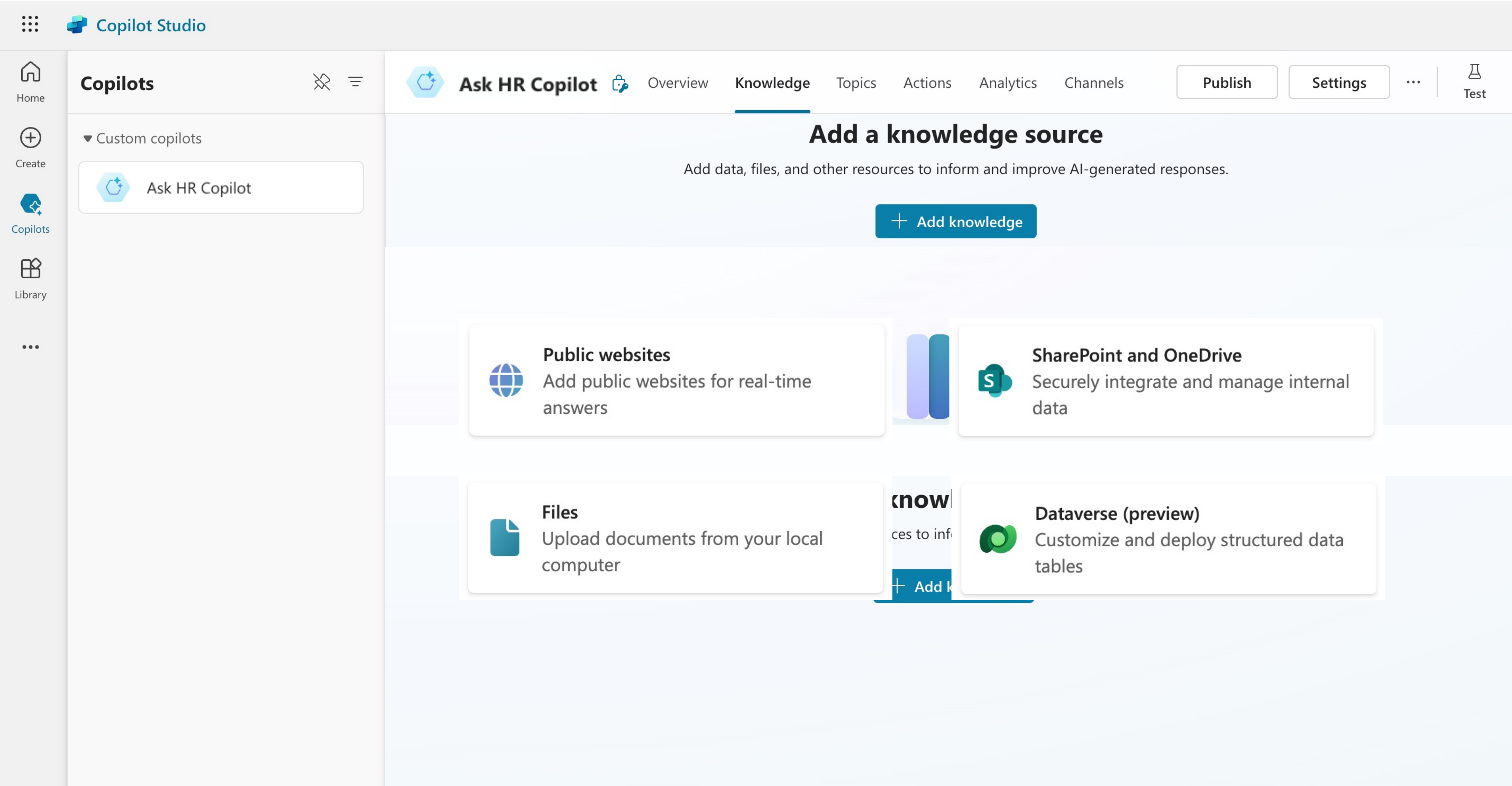
○ **Manual (for custom website)**
Support AAD or any OAuth2 identity provider. Authentication variables are available including authentication token.

Enter the information provided by your Identity Provider (IdP), and then test the connection. For single sign-on with AAD include the token exchange URL. Learn more

AskHR Copilot



@mbrg0
@donwillits66
#BLUEHAT



Add a knowledge source

Add data, files, and other resources to inform and improve AI-generated responses.

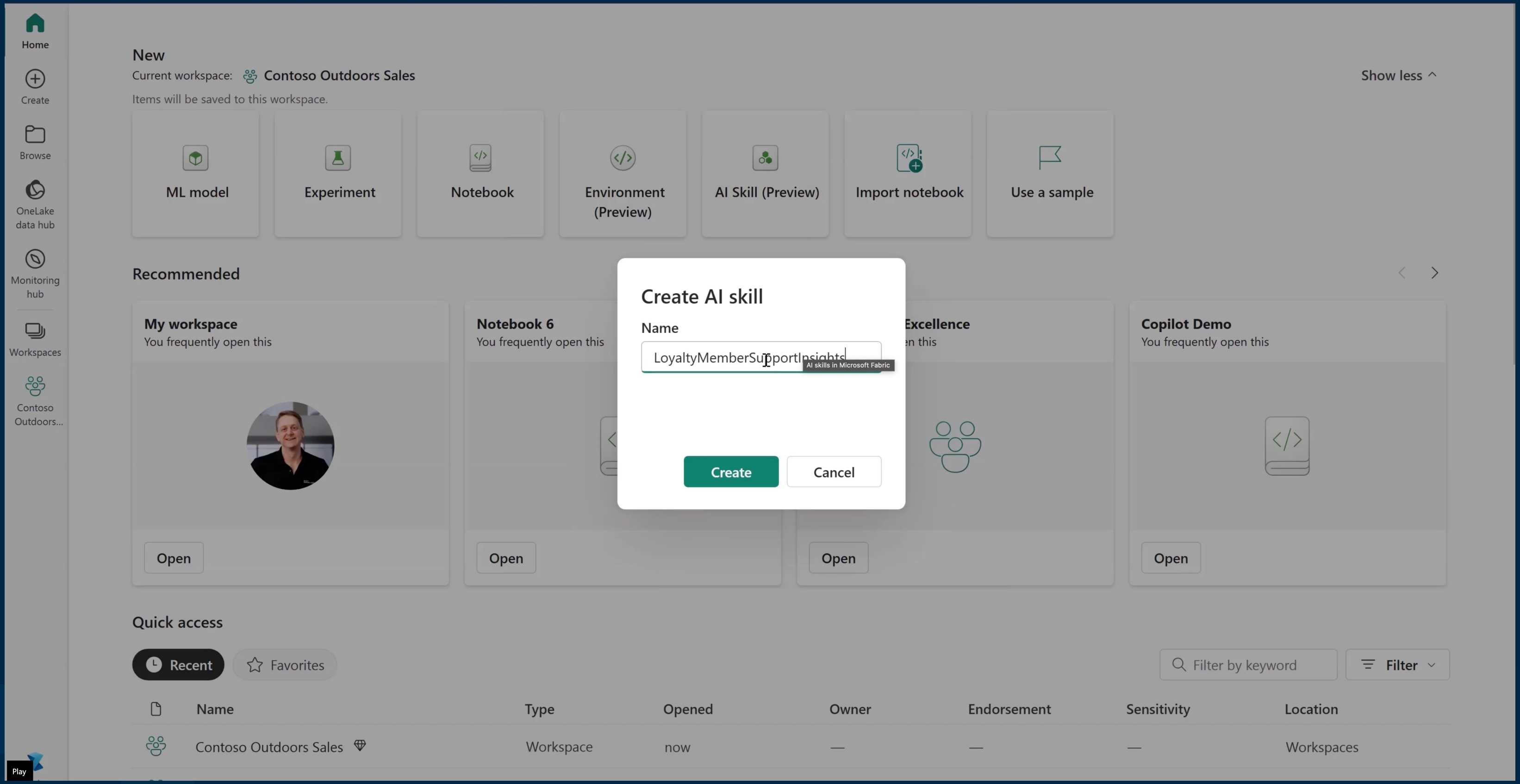
+ Add knowledge

Public websites
Add public websites for real-time answers

SharePoint and OneDrive
Securely integrate and manage internal data

Files
Upload documents from your local computer

Dataverse (preview)
Customize and deploy structured data tables



Create AI skill

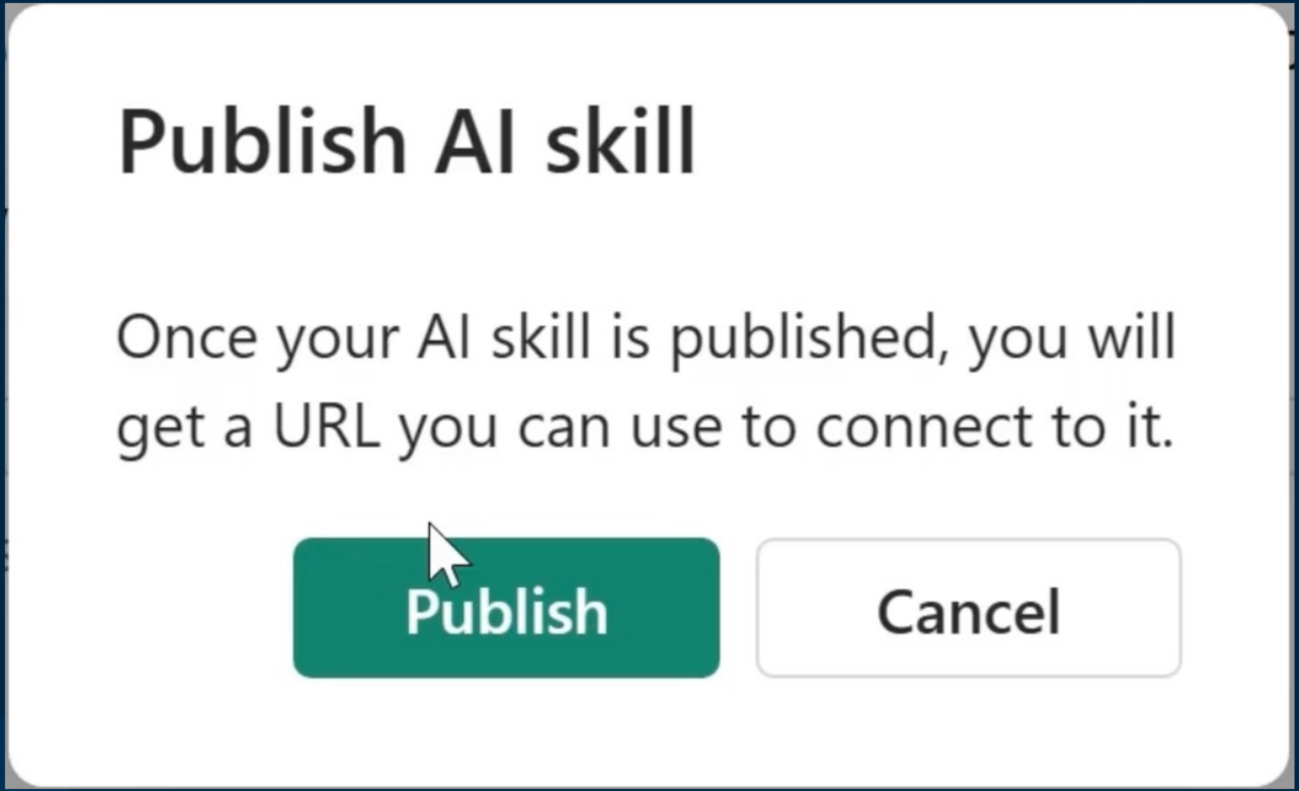
Name: LoyaltyMemberSupportInsights

Current workspace: Contoso Outdoors Sales

Items will be saved to this workspace.

Name	Type	Opened	Owner	Endorsement	Sensitivity	Location
Contoso Outdoors Sales	Workspace	now	—	—	—	Workspaces

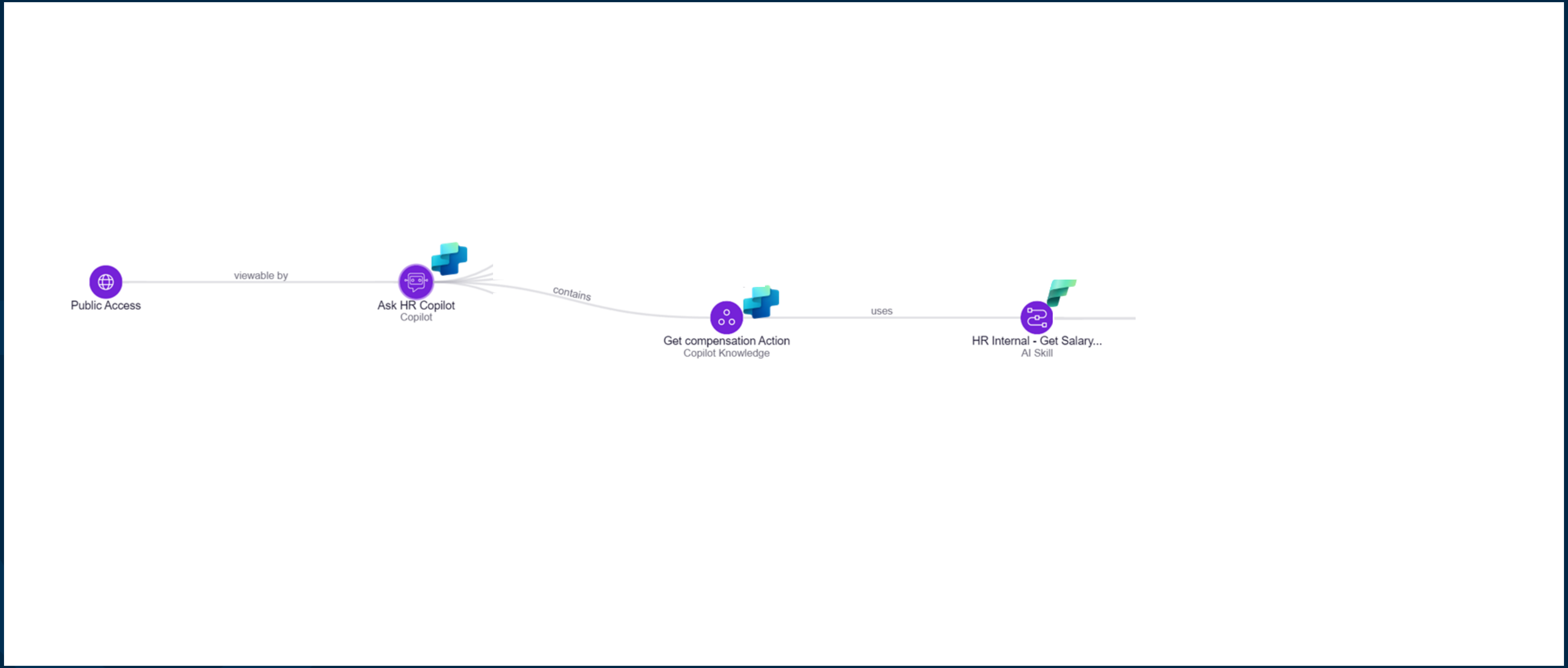
@mbrg0
@donwillits66
#BLUEHAT



Publish AI skill

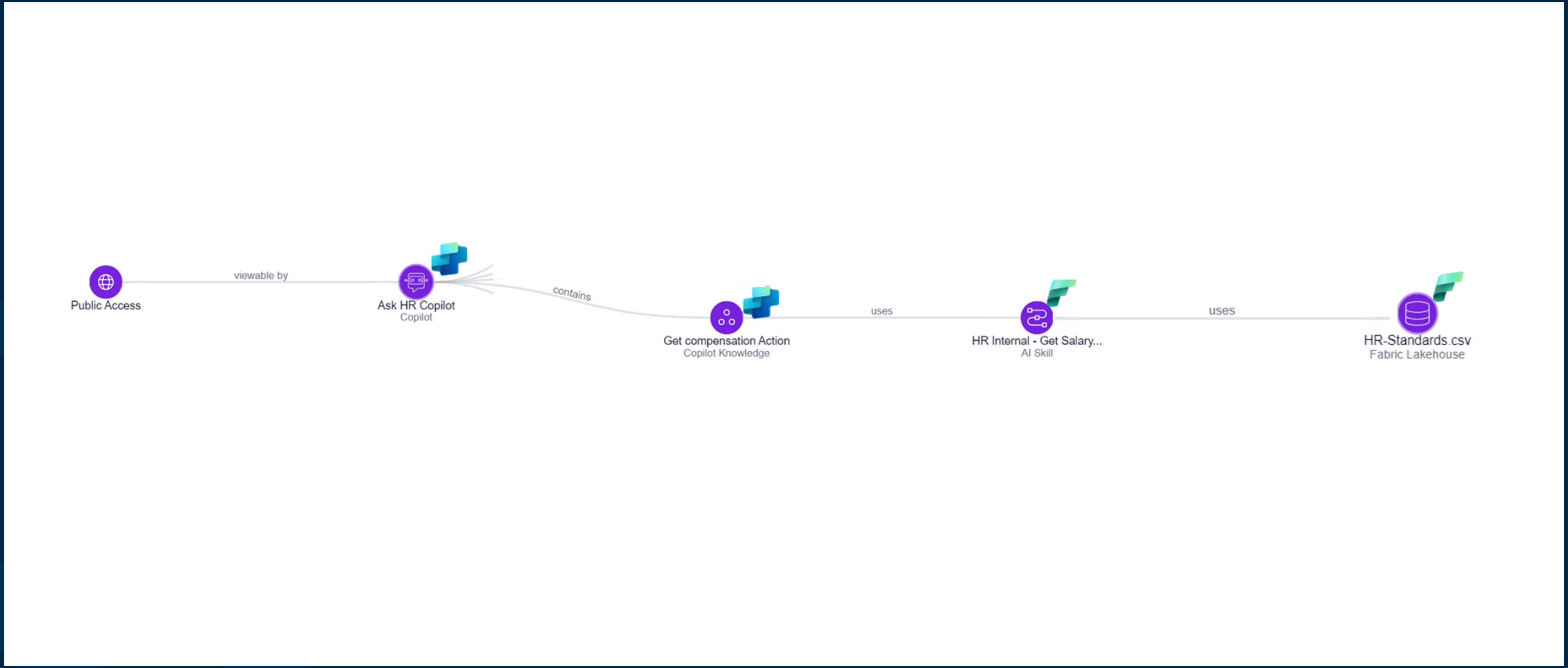
Once your AI skill is published, you will get a URL you can use to connect to it.

AskHR Copilot



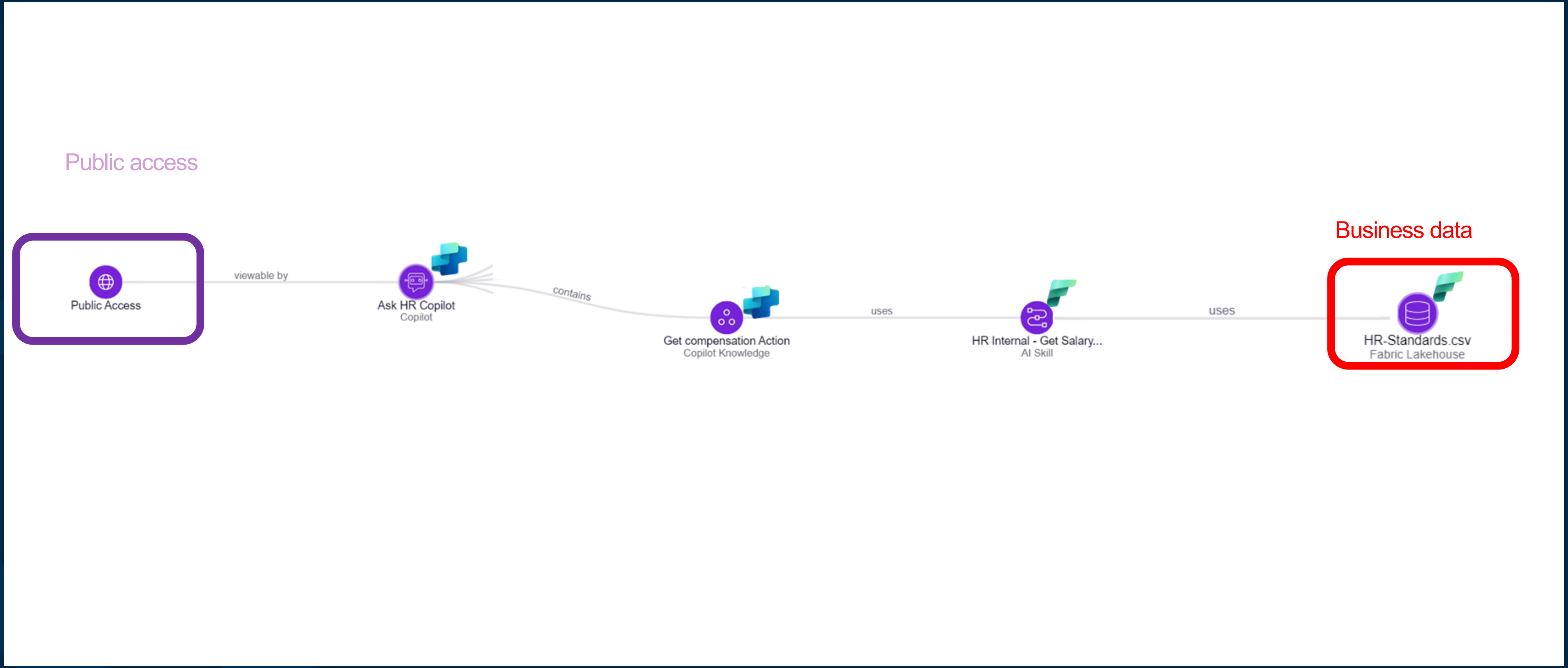
@mbrg0
@donwillits66
#BLUEHAT

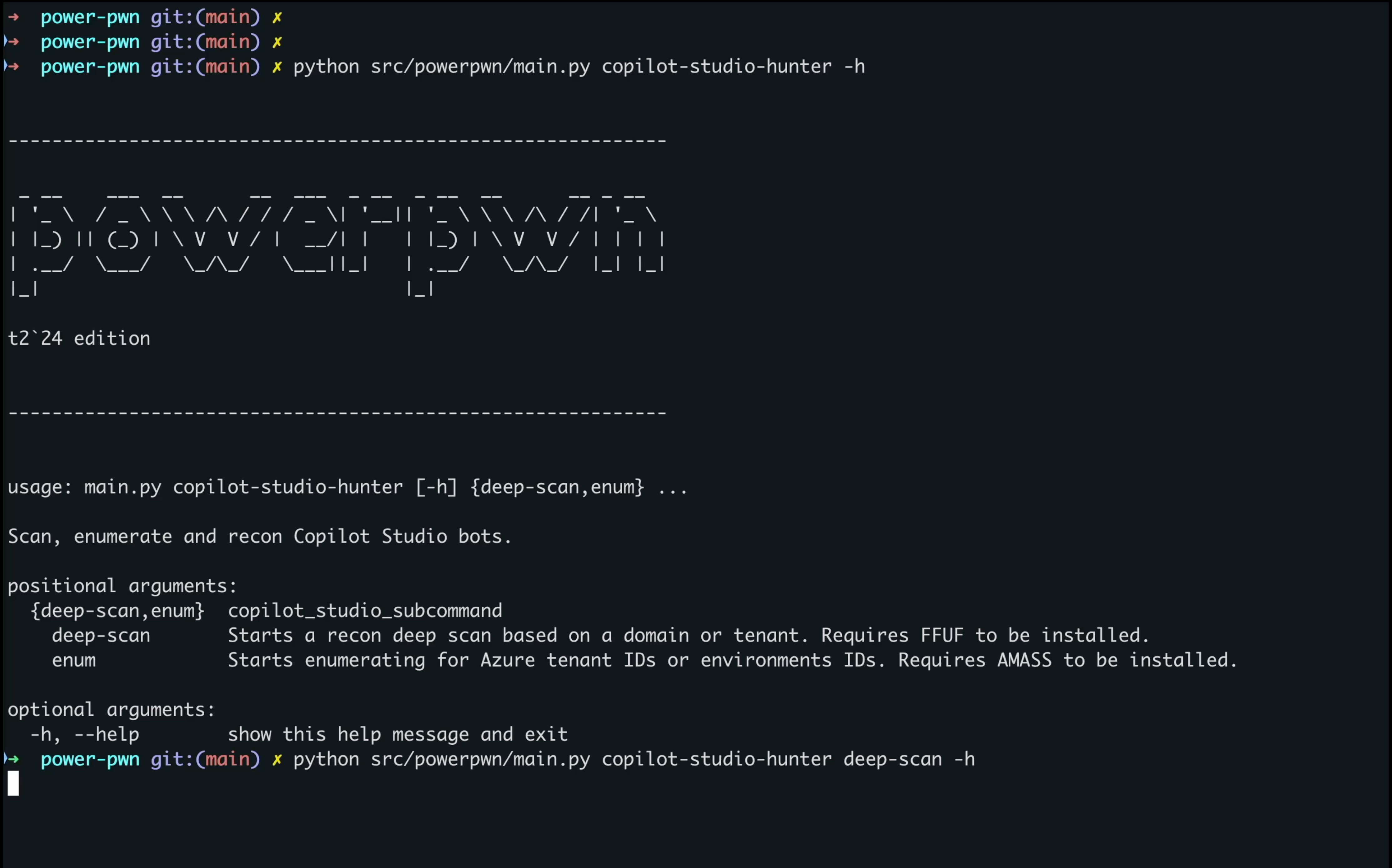
AskHR Copilot



AskHR Copilot – findings

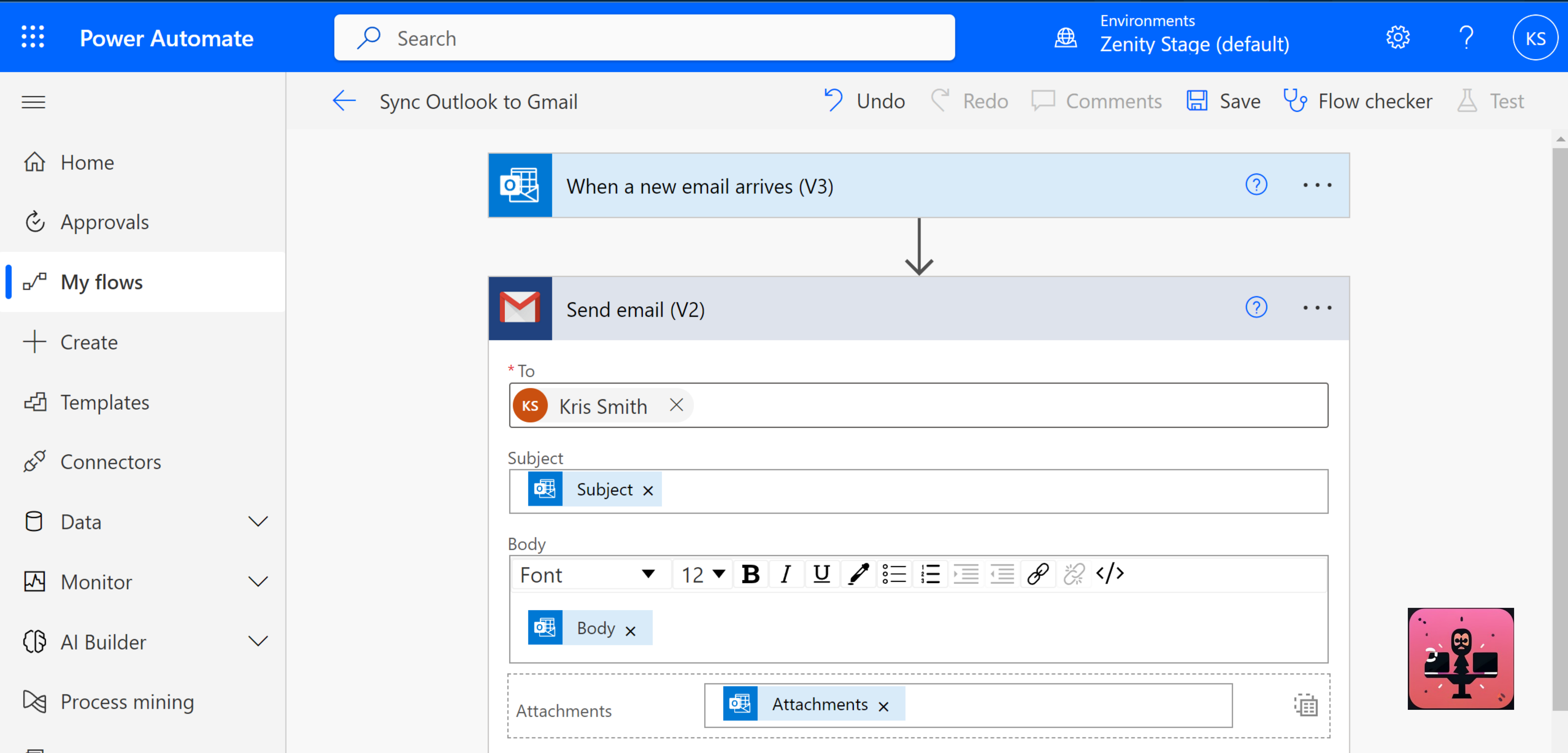
- Sensitive data publicly accessible (Data Leakage)





```
➜  power-pwn git:(main) ✗
➜  power-pwn git:(main) ✗
➜  power-pwn git:(main) ✗ python src/powerpwn/main.py copilot-studio-hunter -h


------------------------------------------------------------


 _ __     ___  __      __  ___  _ __  _ __  __      __ _ __
| '_ \  / _ \ \ \ /\ / / / _ \| '__|| '_ \ \ \ /\ / /| '_ \
| |_) || (_) | \ V  V / |  __/| |   | |_) | \ V  V / | | | |
| .__/  \___/   \_/\_/   \___||_|   | .__/   \_/\_/  |_| |_|
|_|                                 |_|

t2`24 edition



------------------------------------------------------------



usage: main.py copilot-studio-hunter [-h] {deep-scan,enum} ...

Scan, enumerate and recon Copilot Studio bots.

positional arguments:
  {deep-scan,enum}  copilot_studio_subcommand
    deep-scan       Starts a recon deep scan based on a domain or tenant. Requires FFUF to be installed.
    enum            Starts enumerating for Azure tenant IDs or environments IDs. Requires AMASS to be installed.

optional arguments:
  -h, --help        show this help message and exit
➜  power-pwn git:(main) ✗ python src/powerpwn/main.py copilot-studio-hunter deep-scan -h
```

Story #3 – productivity sync



Sync Outlook to Gmail

When a new email arrives (V3)

Send email (V2)

* To: Kris Smith

Subject: Subject

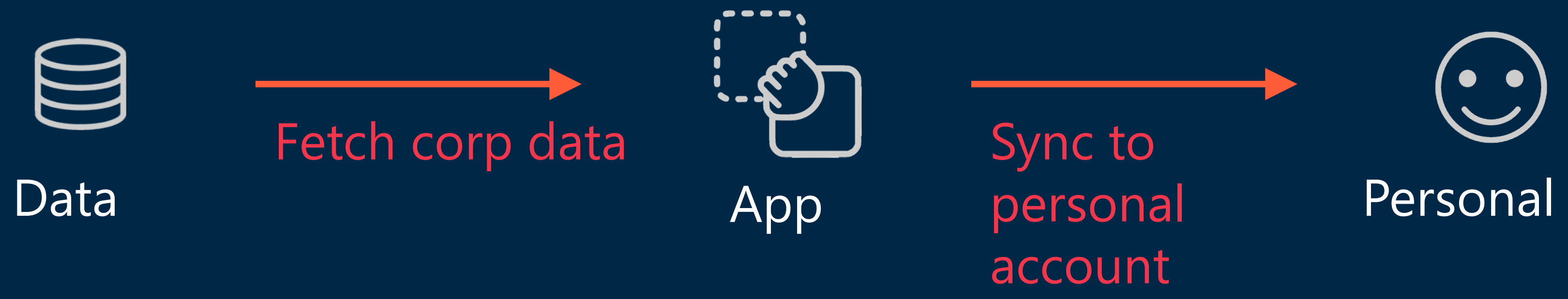
Body: Body

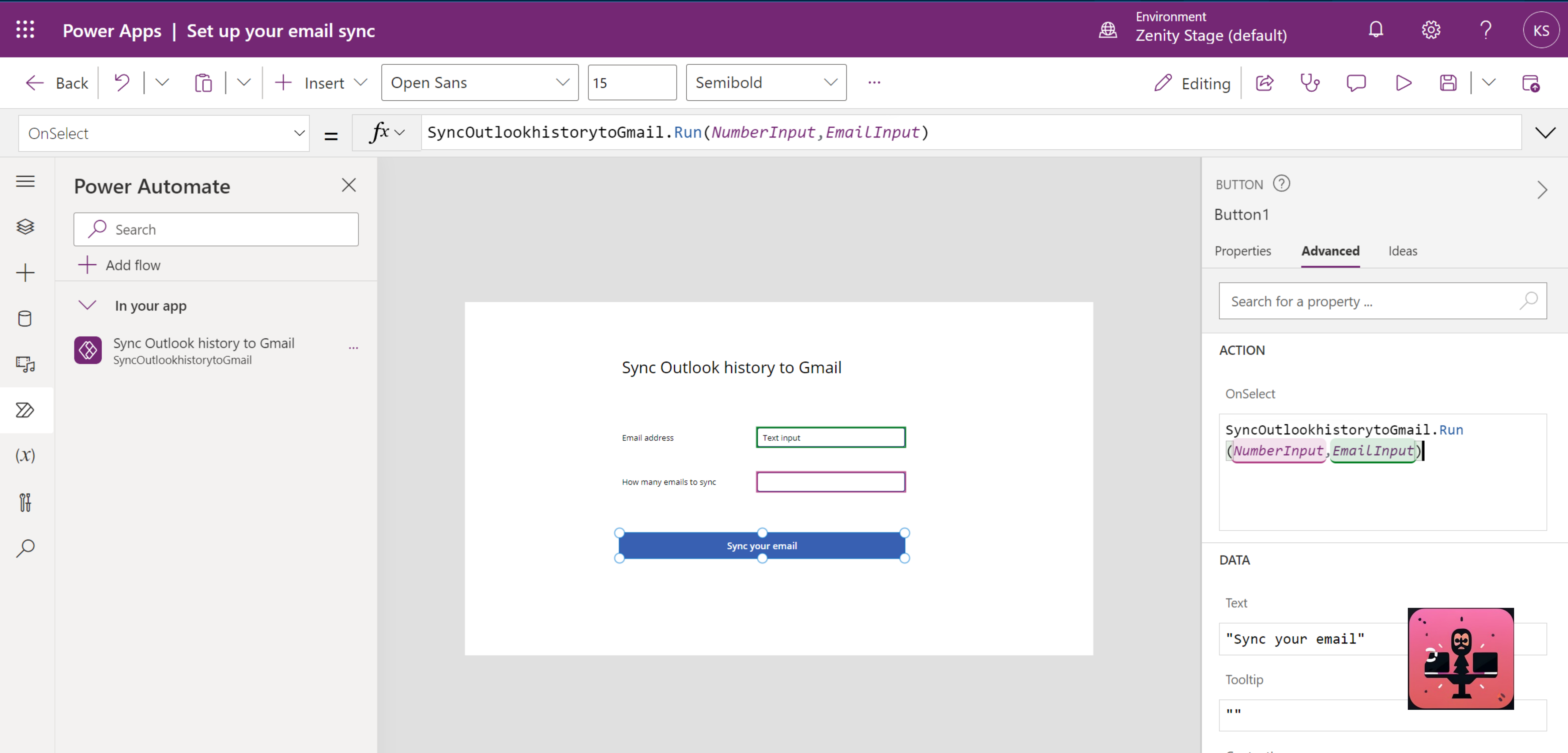
Attachments: Attachments

Productivity sync – findings

Productivity sync – findings

- Business data to personal account (Data Leakage)





OnSelect =

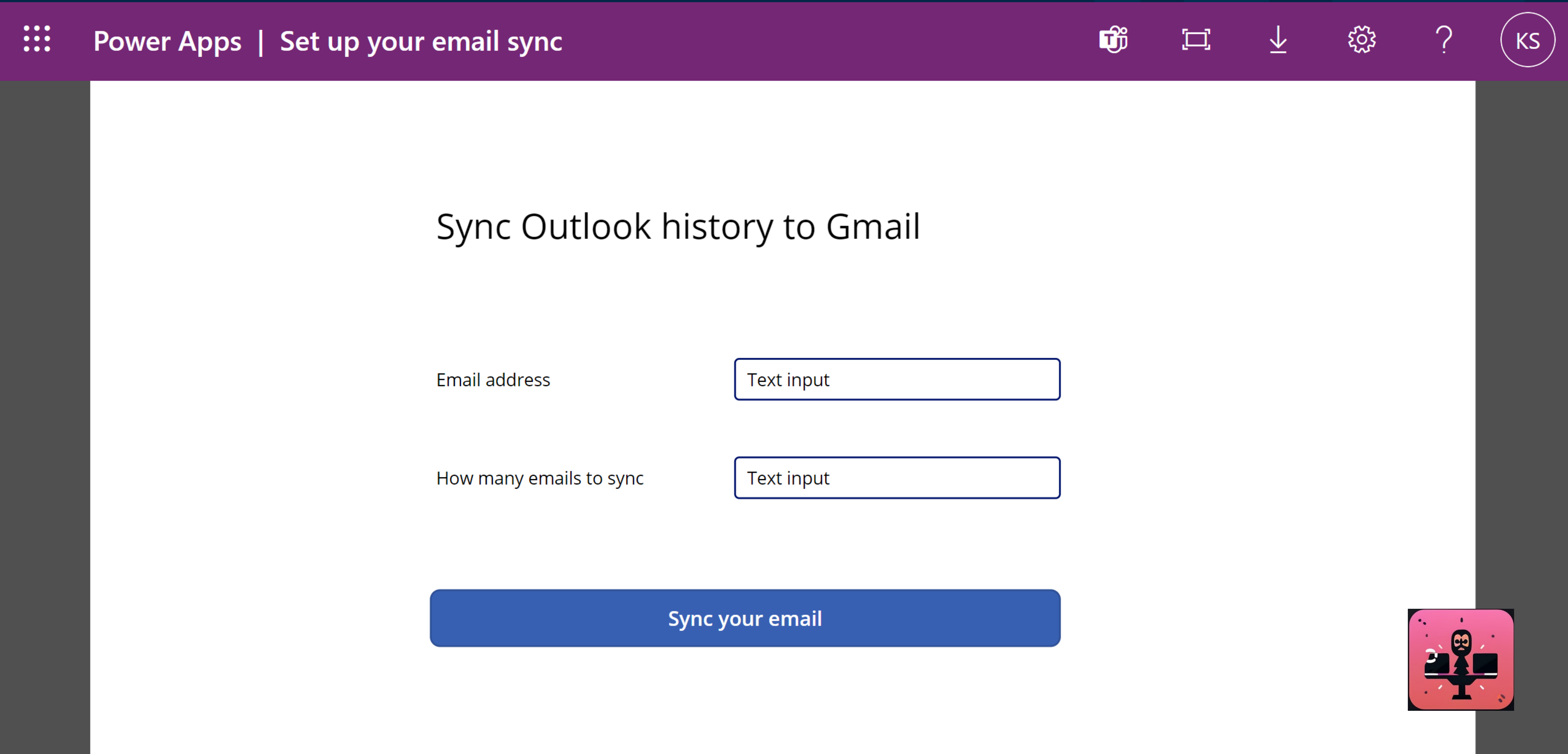
```
SyncOutlookhistorytoGmail.Run(NumberInput,EmailInput)
```

Text

```
"Sync your email"
```

Tooltip

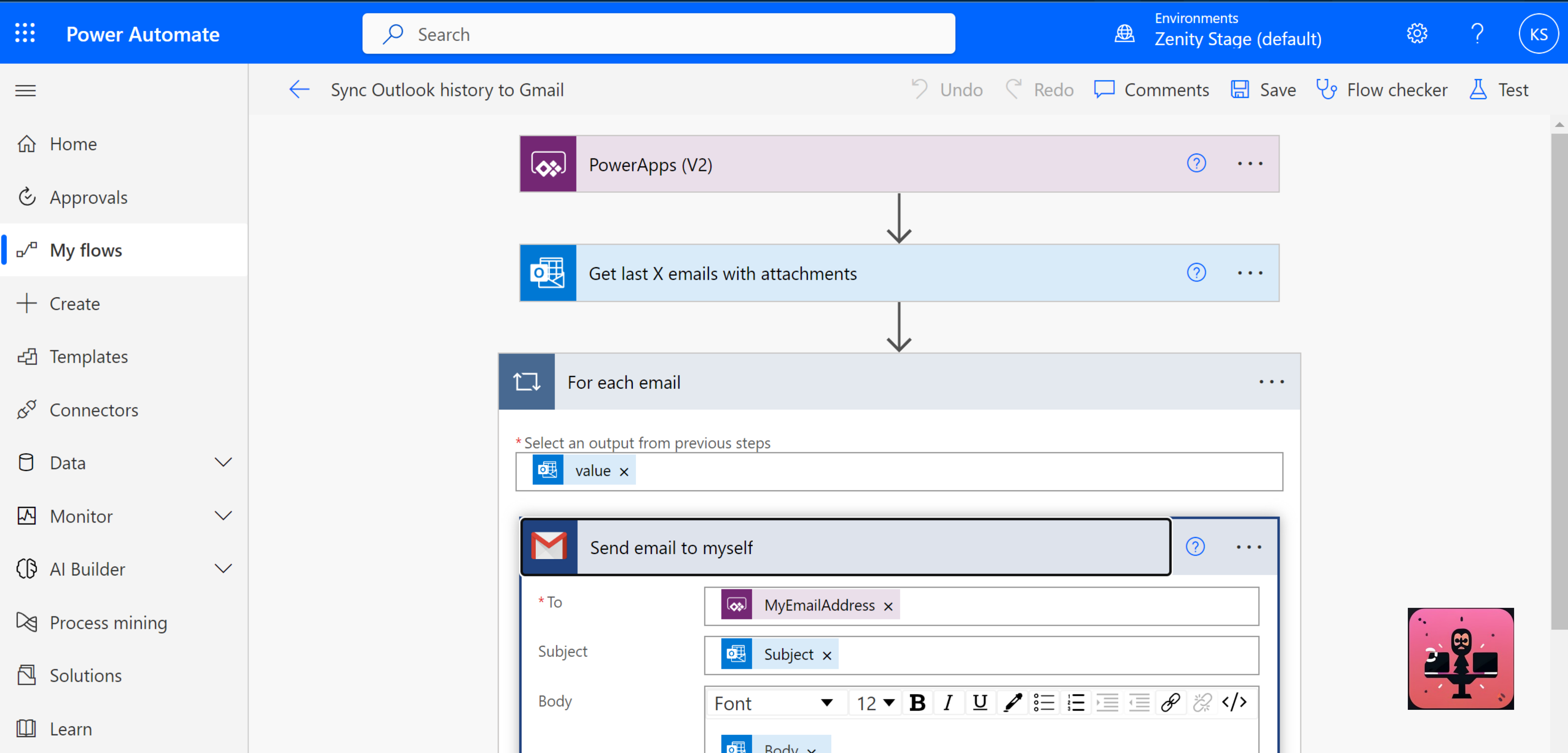
```
""
```



Sync Outlook history to Gmail

Email address: Text input

How many emails to sync: Text input



Sync Outlook history to Gmail

PowerApps (V2)

Get last X emails with attachments

For each email

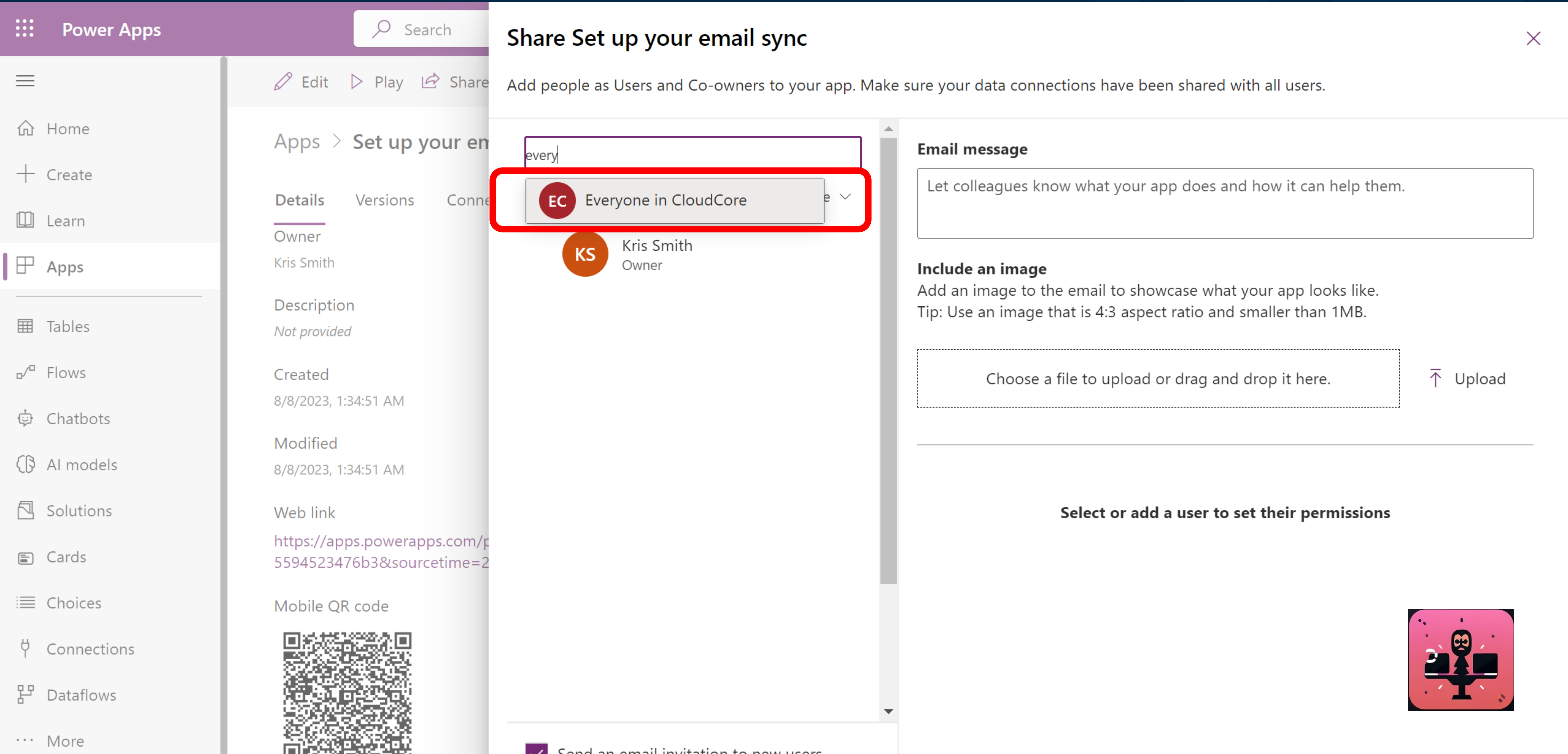
* Select an output from previous steps: value ×

Send email to myself

* To: MyEmailAddress ×

Subject: Subject ×

Body: Body ×



Owner
Kris Smith

Description
Not provided

Created
8/8/2023, 1:34:51 AM

Modified
8/8/2023, 1:34:51 AM

Web link
https://apps.powerapps.com/p
5594523476b3&sourcetime=2

Mobile QR code

Share Set up your email sync

Add people as Users and Co-owners to your app. Make sure your data connections have been shared with all users.

every

EC Everyone in CloudCore

KS Kris Smith
Owner

Email message

Let colleagues know what your app does and how it can help them.

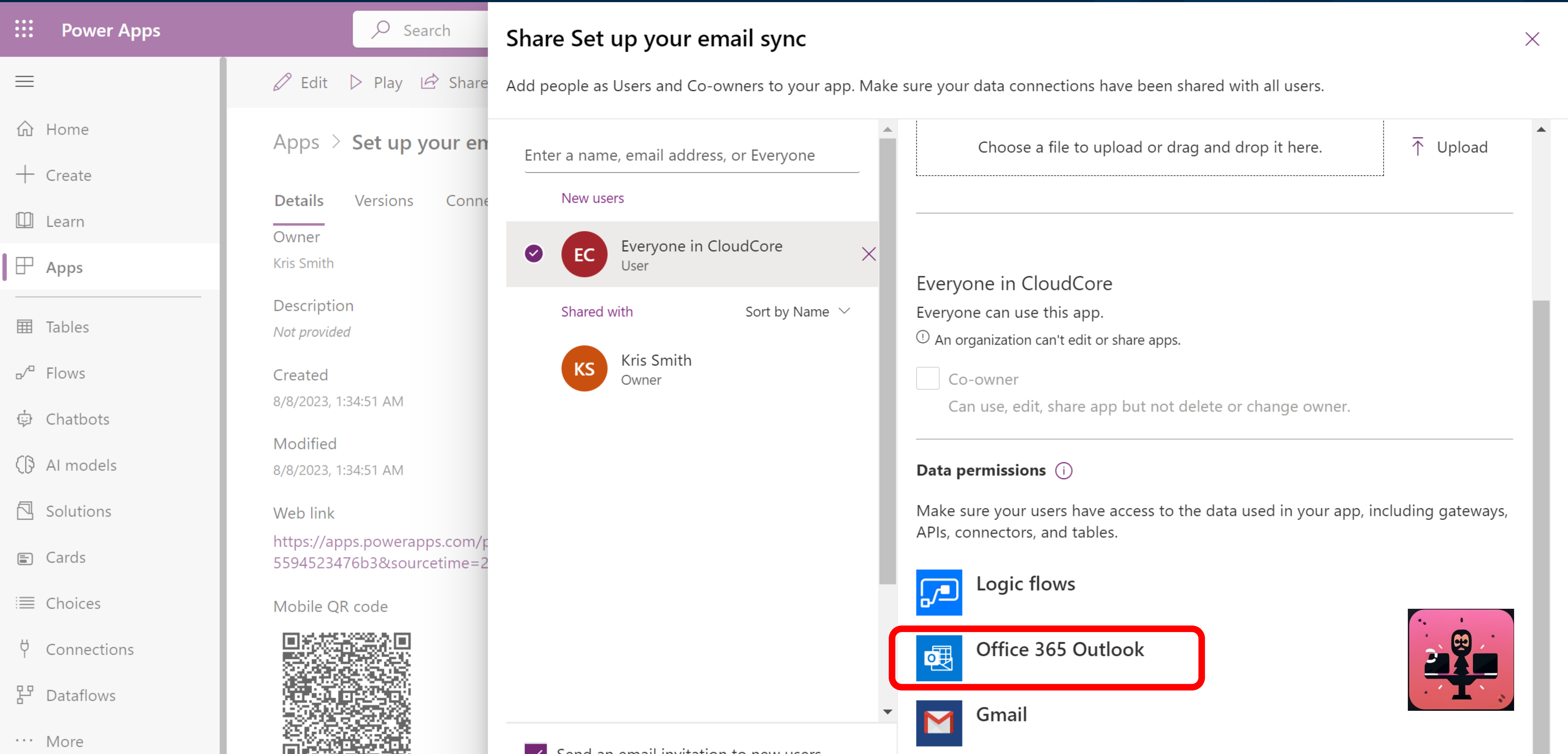
Include an image

Add an image to the email to showcase what your app looks like.
Tip: Use an image that is 4:3 aspect ratio and smaller than 1MB.

Choose a file to upload or drag and drop it here.

Select or add a user to set their permissions

☑ Send an email invitation to new users



Owner
Kris Smith

Description
Not provided

Created
8/8/2023, 1:34:51 AM

Modified
8/8/2023, 1:34:51 AM

Web link
https://apps.powerapps.com/p
5594523476b3&sourcetime=2

Mobile QR code

Share Set up your email sync

Add people as Users and Co-owners to your app. Make sure your data connections have been shared with all users.

Enter a name, email address, or Everyone

New users

EC Everyone in CloudCore
User

Shared with — Sort by Name

KS Kris Smith
Owner

☑ Send an email invitation to new users

Choose a file to upload or drag and drop it here.

Everyone in CloudCore
Everyone can use this app.
An organization can't edit or share apps.

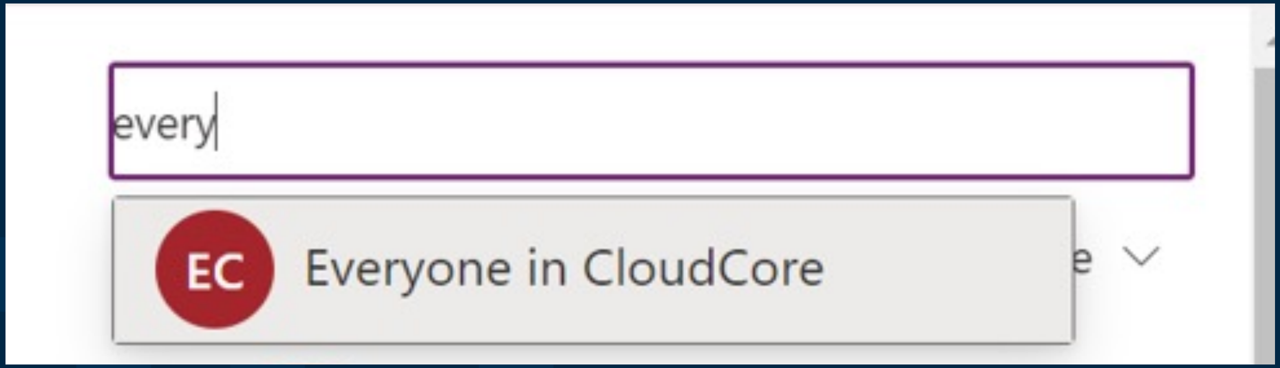
□ Co-owner
Can use, edit, share app but not delete or change owner.

Data permissions

Make sure your users have access to the data used in your app, including gateways, APIs, connectors, and tables.

Productivity sync – findings

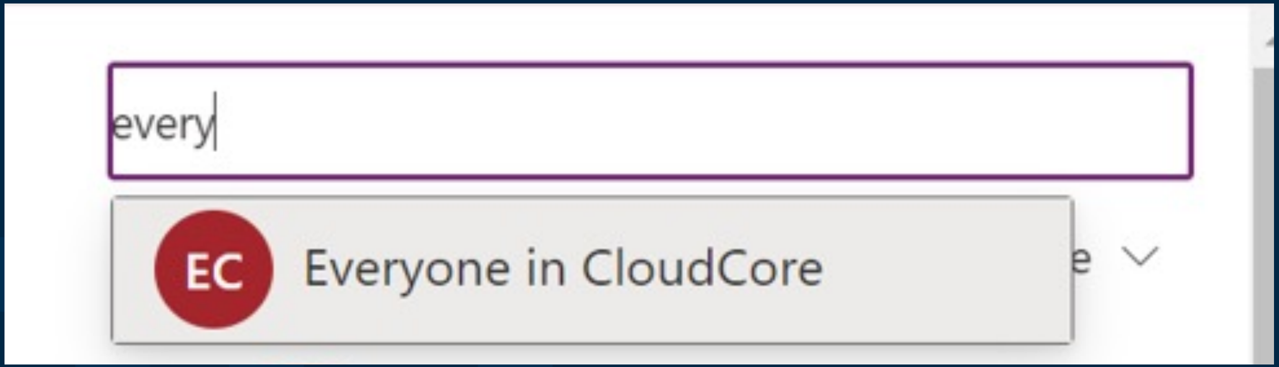
- Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)



Everyone means EVERYONE, including guests by-default

Productivity sync – findings

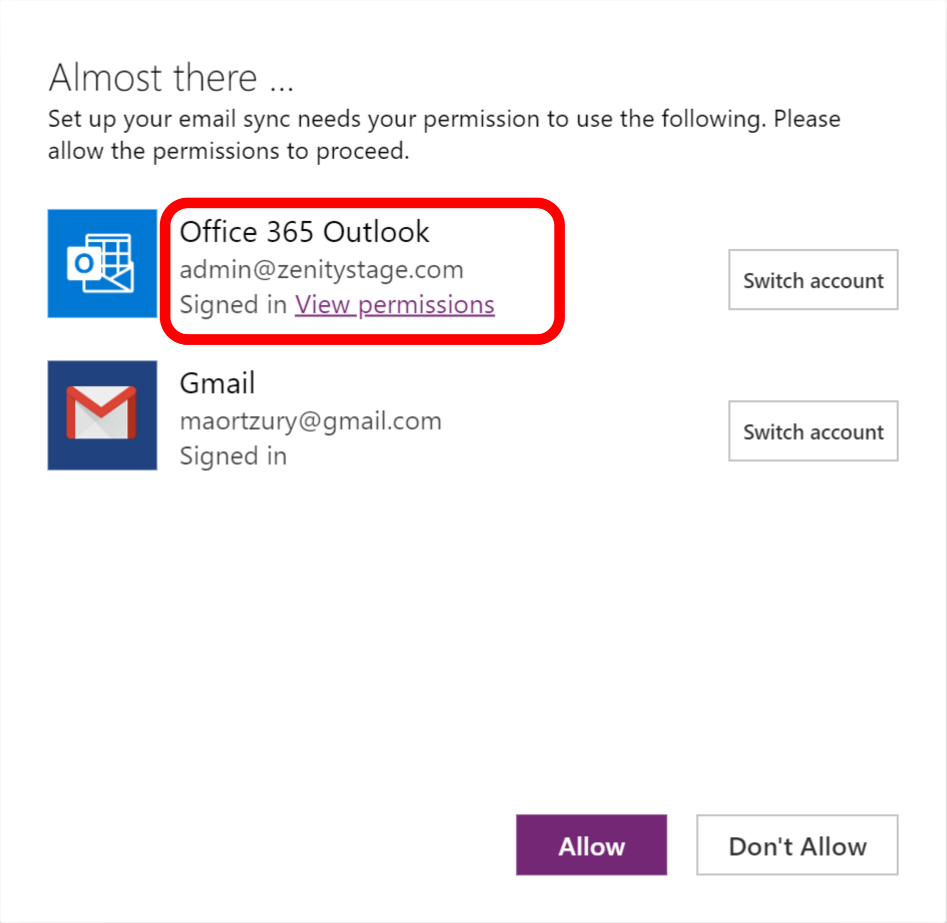
- Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)


every

EC Everyone in CloudCore

Everyone means EVERYONE, including guests by-default

Check out the talk **All You Need Is Guest BHUSA 2023** for an attacker's perspective!

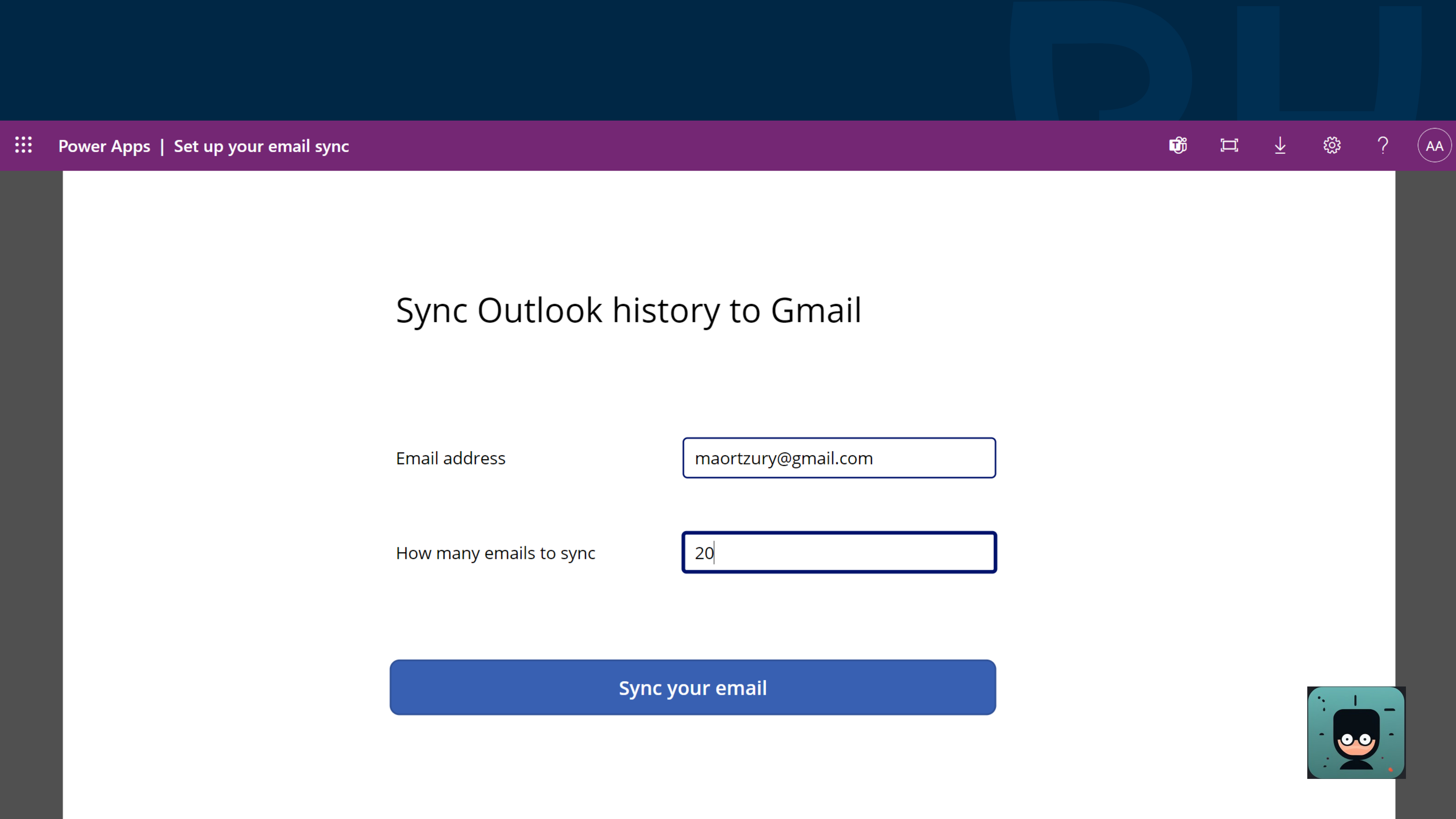


Almost there ...

Set up your email sync needs your permission to use the following. Please allow the permissions to proceed.

Office 365 Outlook
admin@zenitystage.com
Signed in View permissions

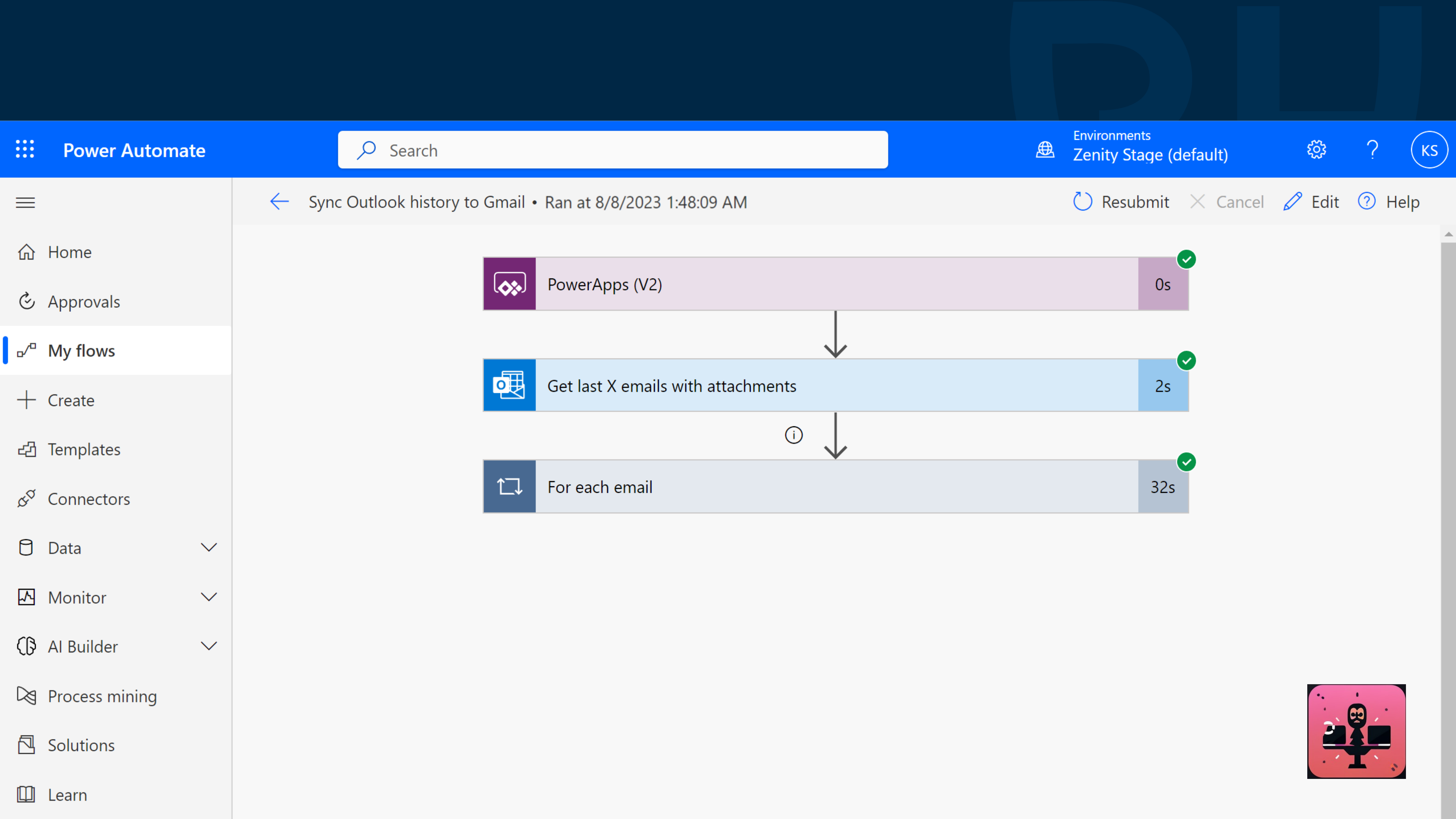
Gmail
maortzury@gmail.com
Signed in



Sync Outlook history to Gmail

Email address: maortzury@gmail.com

How many emails to sync: 20

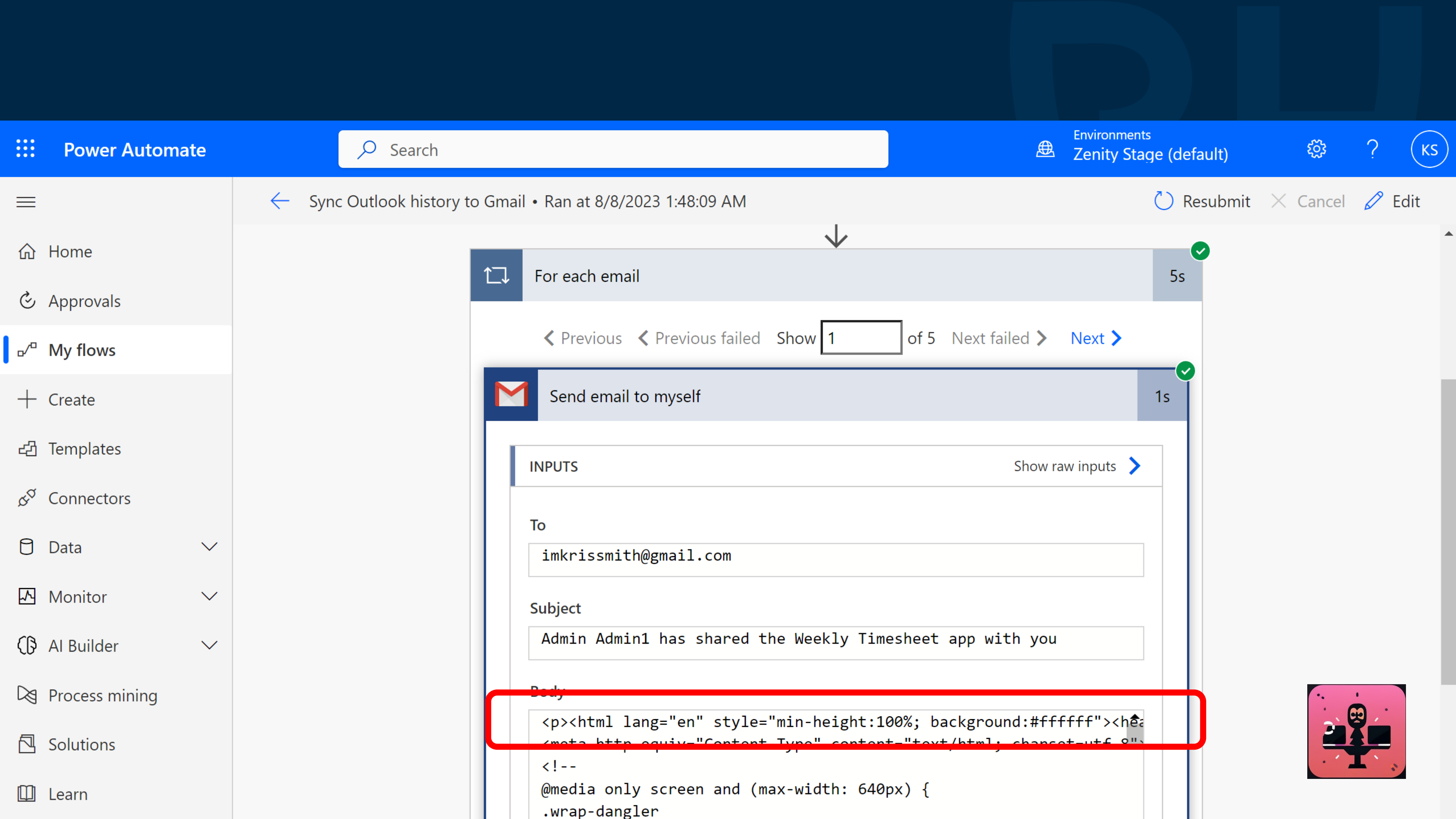


Sync Outlook history to Gmail • Ran at 8/8/2023 1:48:09 AM

PowerApps (V2) 0s

Get last X emails with attachments 2s

For each email 32s



Sync Outlook history to Gmail • Ran at 8/8/2023 1:48:09 AM

Show 1 of 5

To

imkrissmith@gmail.com

Subject

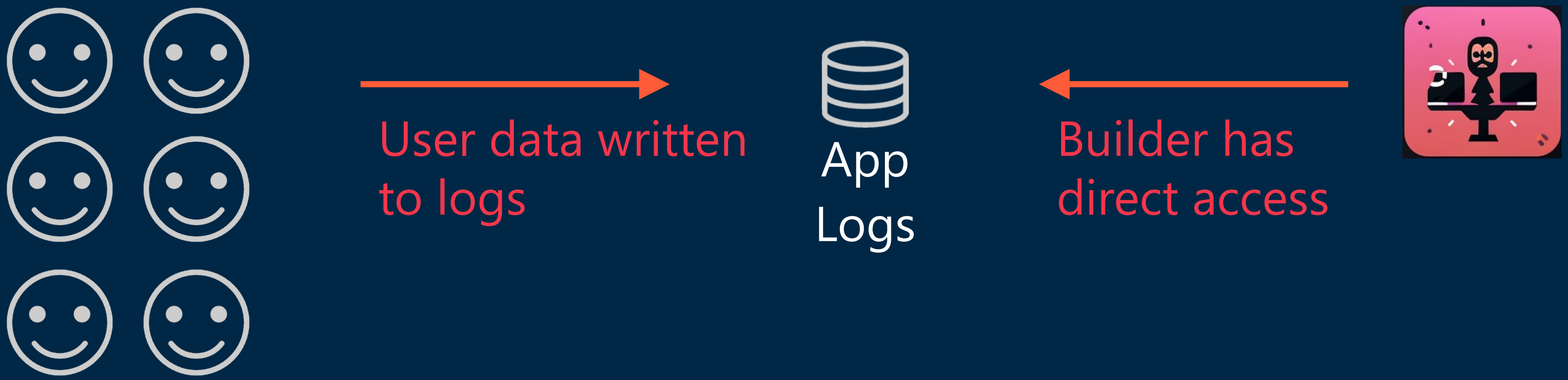
Admin Admin1 has shared the Weekly Timesheet app with you

Body

```
<p><html lang="en" style="min-height:100%; background:#ffffff"><hea
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<!--
@media only screen and (max-width: 640px) {
.wrap-dangler
```

Productivity sync – findings

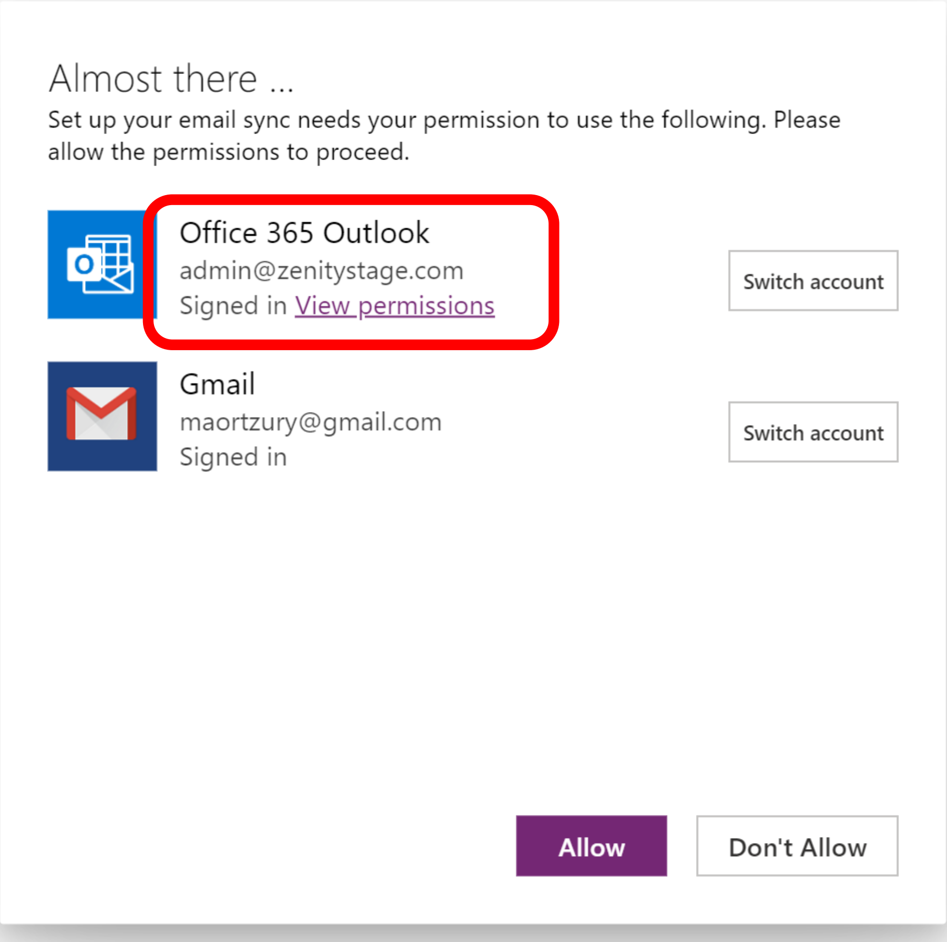
- Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)
- Personal data leaks to logs (Data Leakage)



User data written to logs

App Logs

Builder has direct access

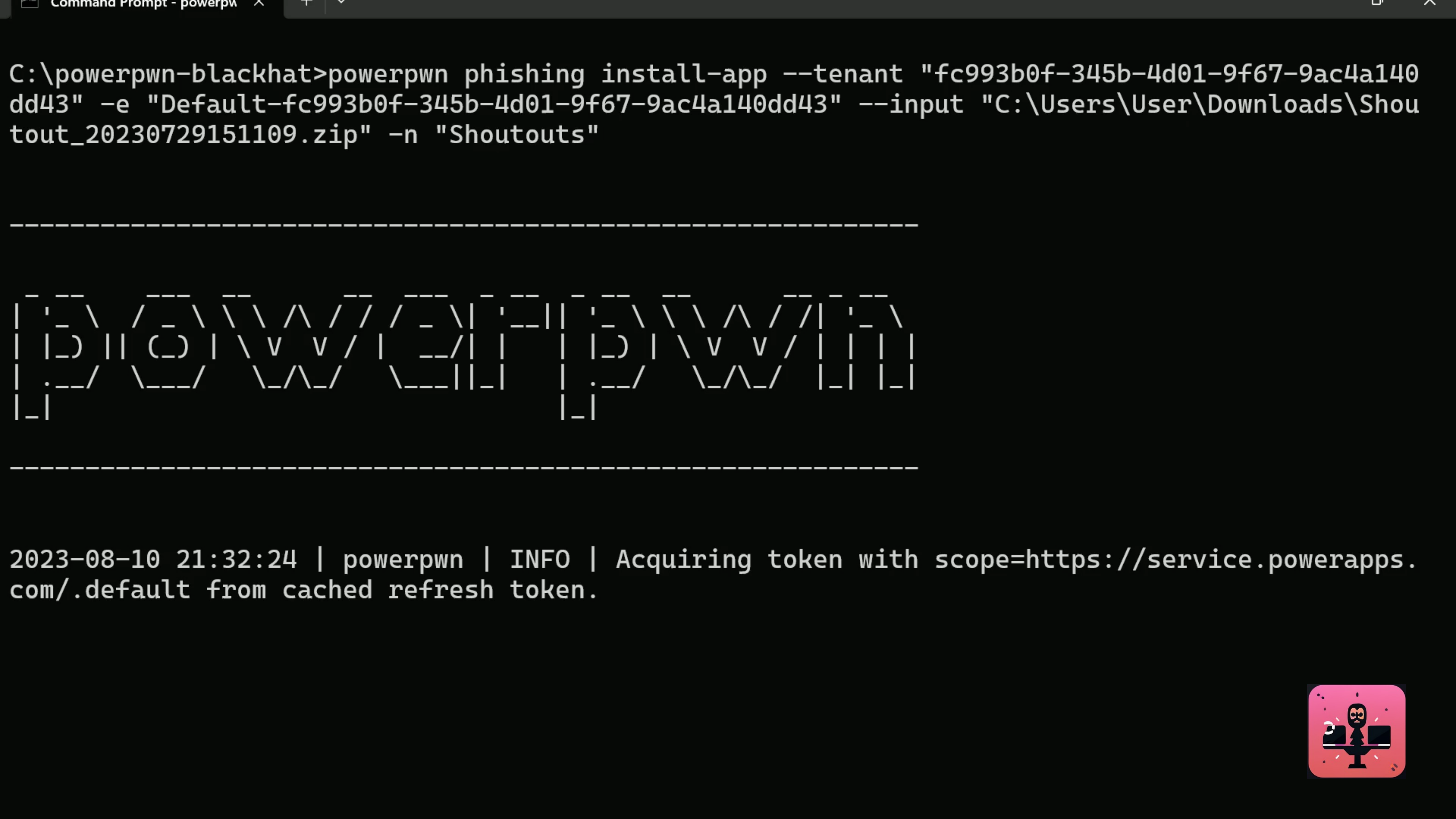


Almost there ...

Set up your email sync needs your permission to use the following. Please allow the permissions to proceed.

Office 365 Outlook
admin@zenitystage.com
Signed in View permissions

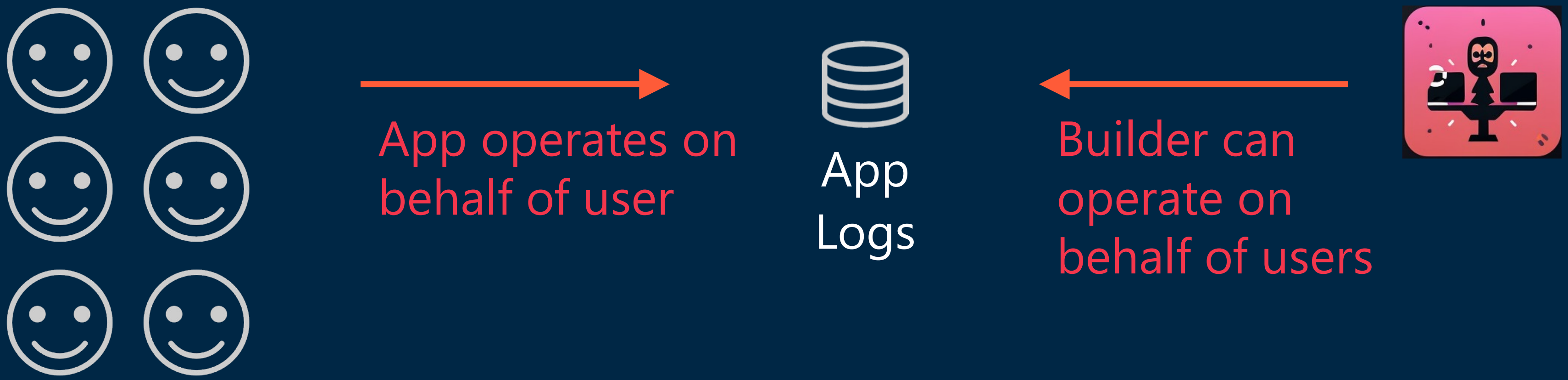
Gmail
maortzury@gmail.com
Signed in



```
C:\powerpwn-blackhat>powerpwn phishing install-app --tenant "fc993b0f-345b-4d01-9f67-9ac4a140
dd43" -e "Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43" --input "C:\Users\User\Downloads\Shou
tout_20230729151109.zip" -n "Shoutouts"


------------------------------------------------------------


 _ __    ___  __      __  ___  _ __  _ __  __      __ _ __
| '_ \  / _ \ \ \ /\ / / / _ \| '__|| '_ \ \ \ /\ / /| '_ \
| |_) || (_) | \ V  V / |  __/| |   | |_) | \ V  V / | | | |
| .__/  \___/   \_/\_/   \___||_|   | .__/   \_/\_/  |_| |_|
|_|                                 |_|


------------------------------------------------------------


2023-08-10 21:32:24 | powerpwn | INFO | Acquiring token with scope=https://service.powerapps.
com/.default from cached refresh token.
```

Productivity sync – findings

- Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)
- Personal data leaks to logs (Data Leakage)
- PrivEsc path (Account Impersonation)


App operates on behalf of user
App Logs
Builder can operate on behalf of users

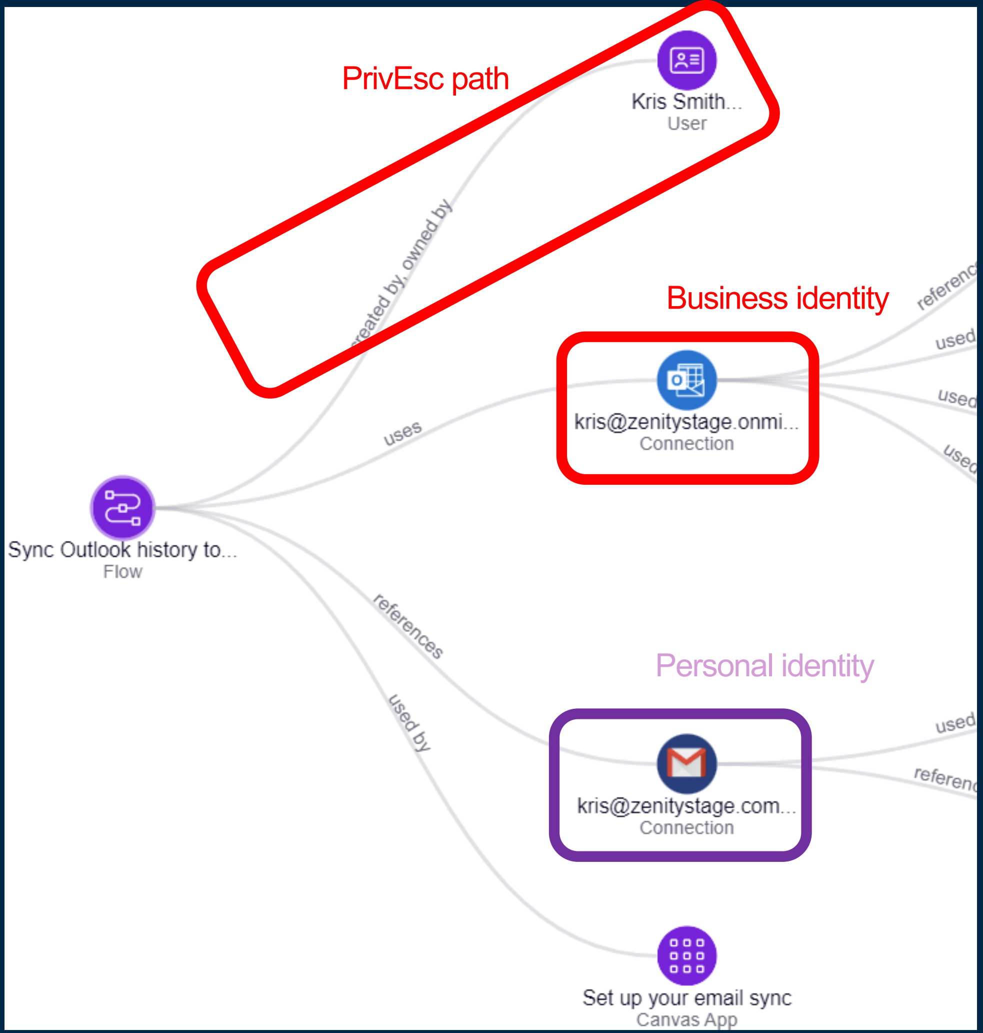
@mbrg0
@donwillits66
#BLUEHAT

Productivity sync – findings

- Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)
- Personal data leaks to logs (Data Leakage)
- PrivEsc path (Account Impersonation)

Productivity sync – findings

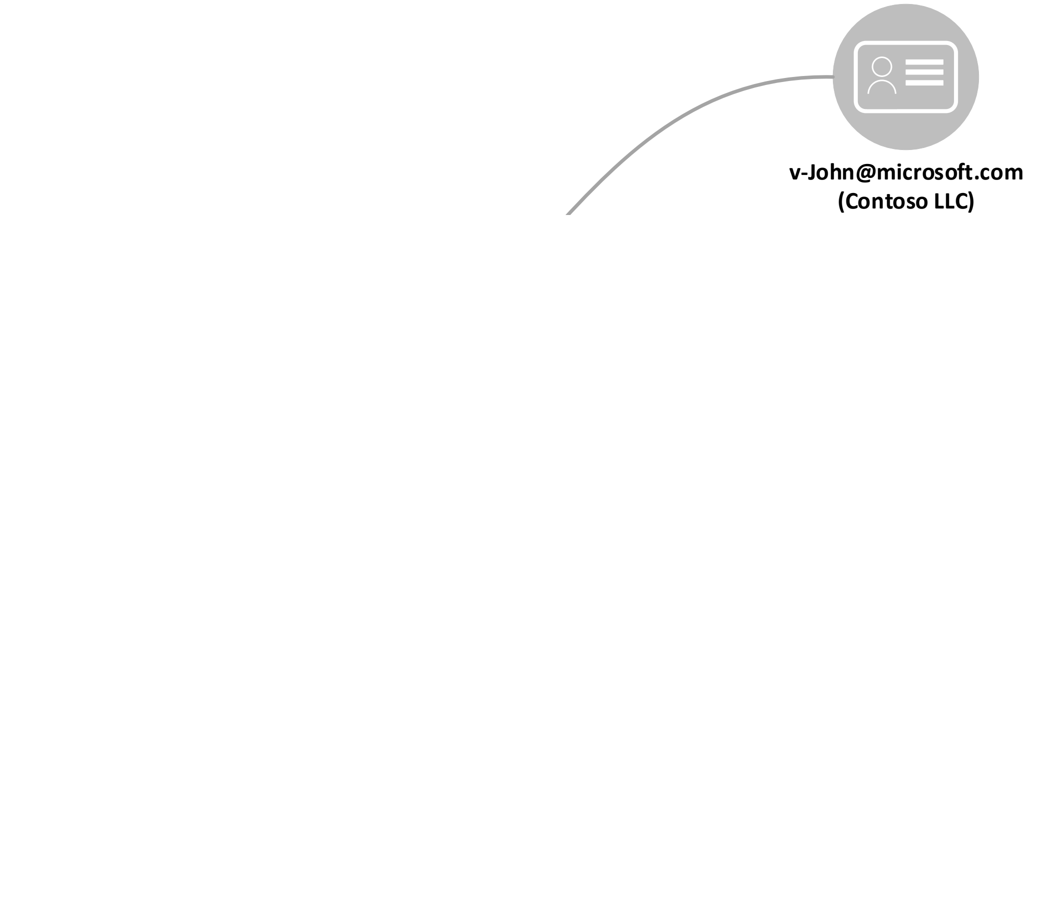
- Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)
- Personal data leaks to logs (Data Leakage)
- PrivEsc path (Account Impersonation)



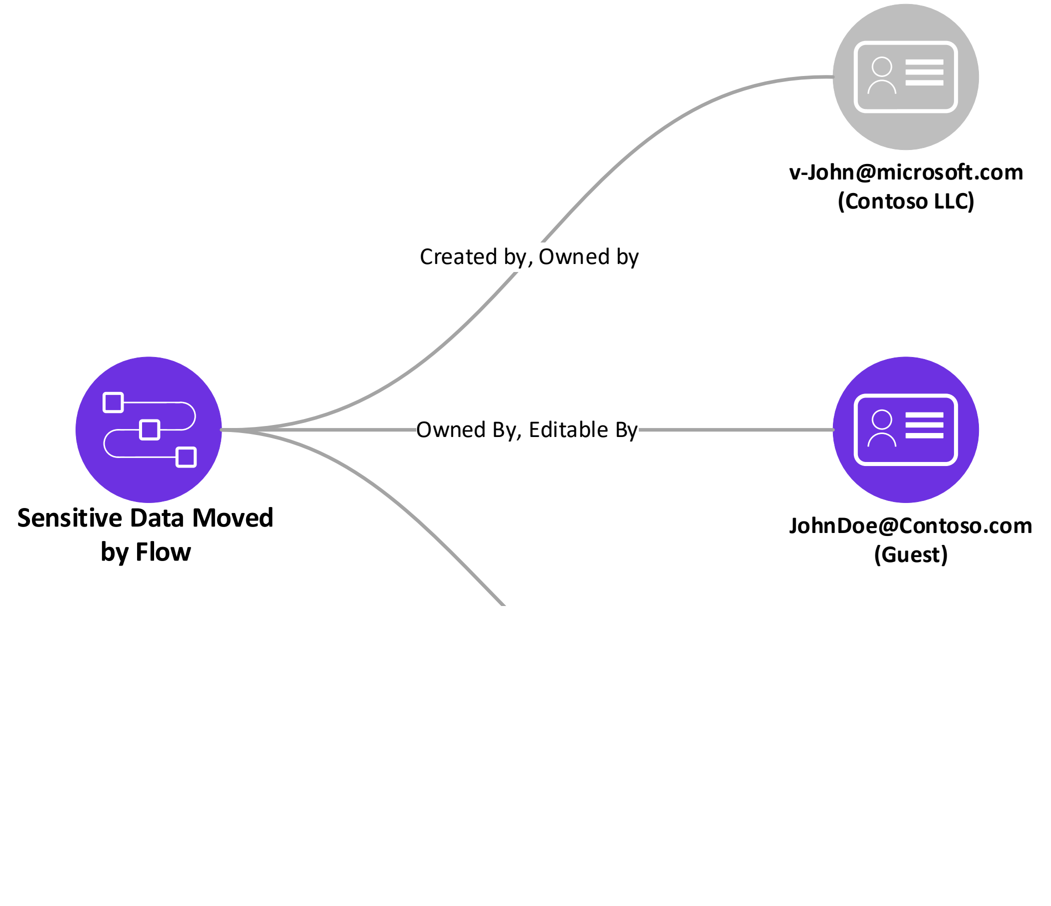
@mbrg0
@donwillits66
#BLUEHAT

Story #4 – a persistent vendor

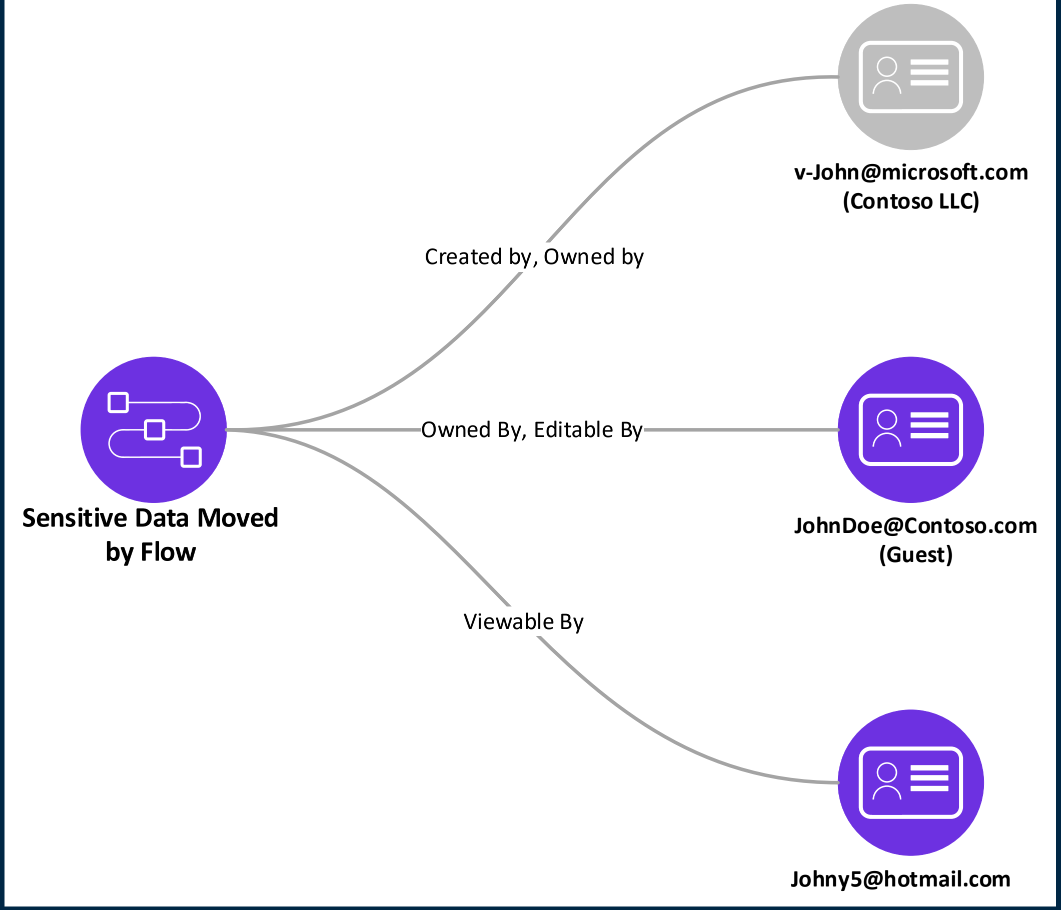
- Vendor John’s contract has expired, Entra ID account disabled



- Vendor John's contract has expired, Entra ID account disabled
- Before that happened, John added two identities:
  - One for his place of business which can STILL edit the flow using his Contoso Credentials



- Vendor John's contract has expired, Entra ID account disabled
- Before that happened, John added two identities:
  - One for his place of business which can STILL edit the flow using his Contoso Credentials
  - One for his own personal account. It can only run the flow and collect the data it generates.



A persistent vendor – findings

- Unintended or malicious access to sensitive data

Not exclusive to vendors!

…but a very common "use case"

- Without inspecting each and every app/flow/copilot/etc. created by Vendors/others…

…very hard to find!

Recap

We are leaving heavy security decisions in the hands of business users

When choosing between productivity and security, the choice is obvious

HOW to fail at AppSec

Or – what didn’t work

BLUEHAT
SECURITY ABOVE ALL ELSE

(Blindly) Follow best practice

Application Security Best Practice

1. Focus on crown jewels
2. Get developer buy-in
3. Secure Development Lifecycle (SDL)

Application Security Best Practice

1. Focus on crown jewels

Application Security Best Practice

1. Focus on crown jewels

Everything is connected to critical business apps..

Number of active creds:
Office 365 1.4M
SharePoint 1.35M
Outlook 1.1M
SQL Server 280K
Excel 140K
EntraID 130K
OneDrive 125K
Azure DevOps 124K
…

Application Security Best Practice

~~1. Focus on crown jewels~~

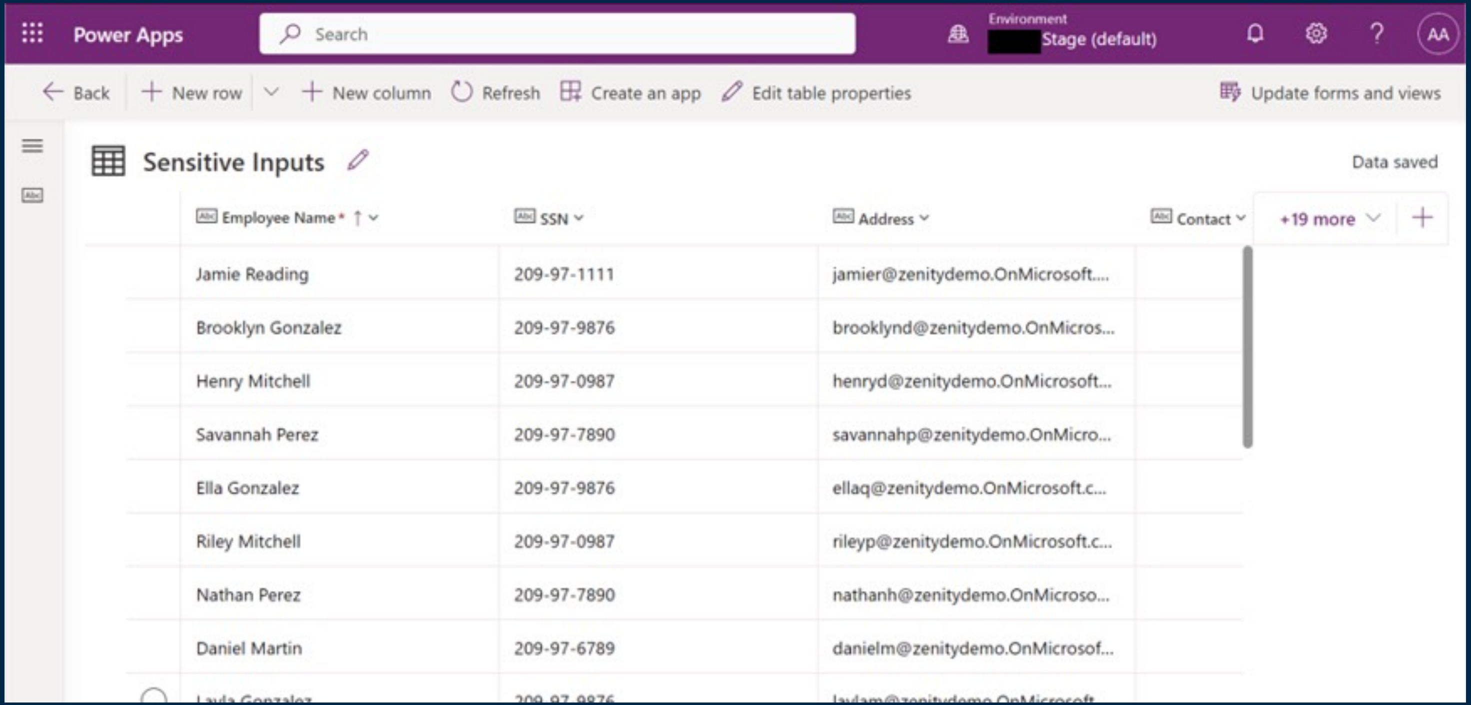
2. Get developer buy-in

Application Security Best Practice

~~1. Focus on crown jewels~~

2. Get developer buy-in

Can we really expect business users to know how store PCI?



Sensitive Inputs

Employee Name *	SSN	Address	Contact
Jamie Reading	209-97-1111	jamier@zenitydemo.OnMicrosoft....	
Brooklyn Gonzalez	209-97-9876	brooklynd@zenitydemo.OnMicros...	
Henry Mitchell	209-97-0987	henryd@zenitydemo.OnMicrosoft...	
Savannah Perez	209-97-7890	savannahp@zenitydemo.OnMicro...	
Ella Gonzalez	209-97-9876	ellaq@zenitydemo.OnMicrosoft.c...	
Riley Mitchell	209-97-0987	rileyp@zenitydemo.OnMicrosoft.c...	
Nathan Perez	209-97-7890	nathanh@zenitydemo.OnMicroso...	
Daniel Martin	209-97-6789	danielm@zenitydemo.OnMicrosof...	
Layla Gonzalez	209-97-9876	laylam@zenitydemo.OnMicrosoft	

Application Security Best Practice

~~1. Focus on crown jewels~~

~~2. Get developer buy-in~~

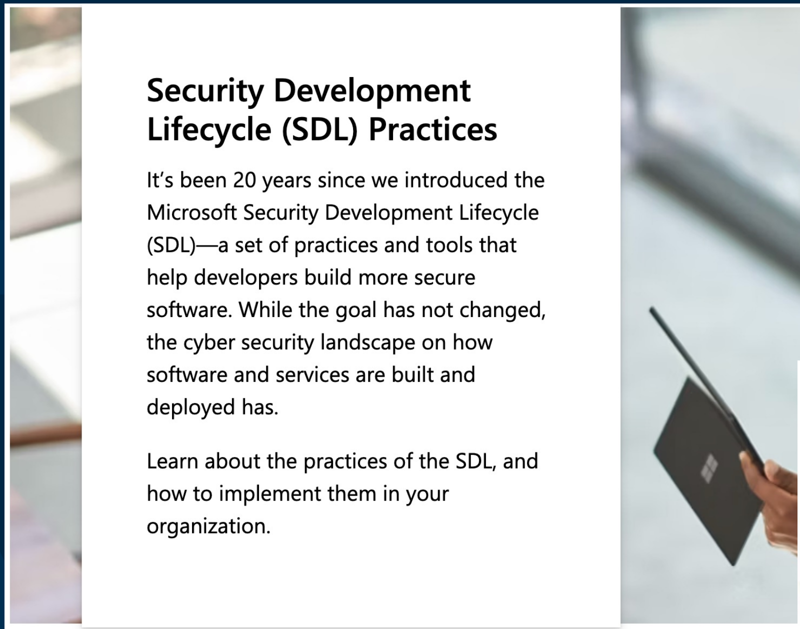
3. Secure Development Lifecycle (SDL)

Application Security Best Practice

~~1. Focus on crown jewels~~

~~2. Get developer buy-in~~

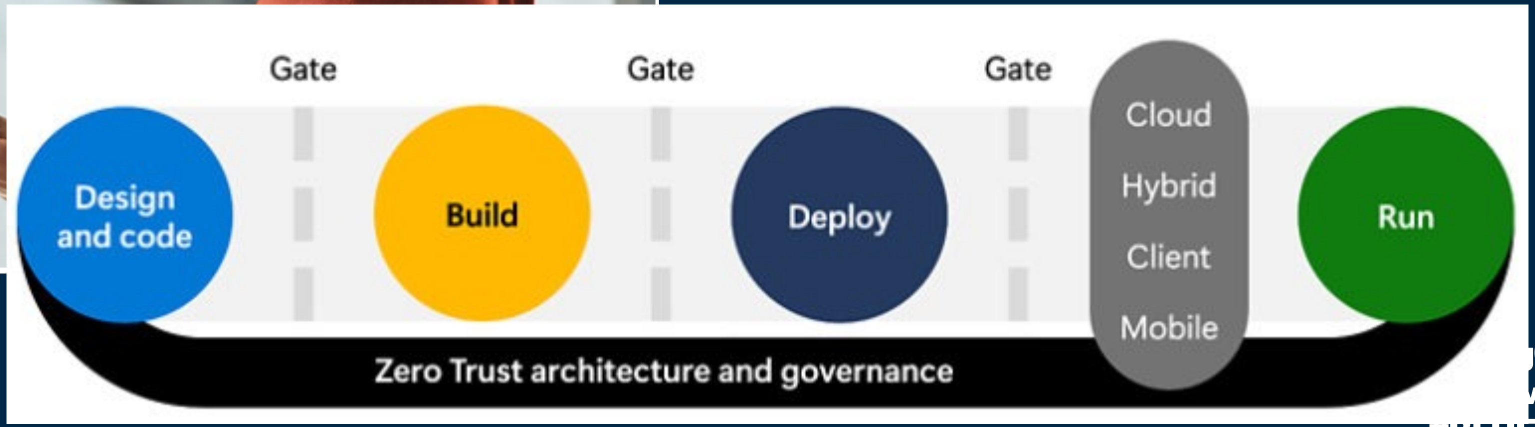
3. Secure Development Lifecycle (SDL)



Security Development Lifecycle (SDL) Practices

It's been 20 years since we introduced the Microsoft Security Development Lifecycle (SDL)—a set of practices and tools that help developers build more secure software. While the goal has not changed, the cyber security landscape on how software and services are built and deployed has.

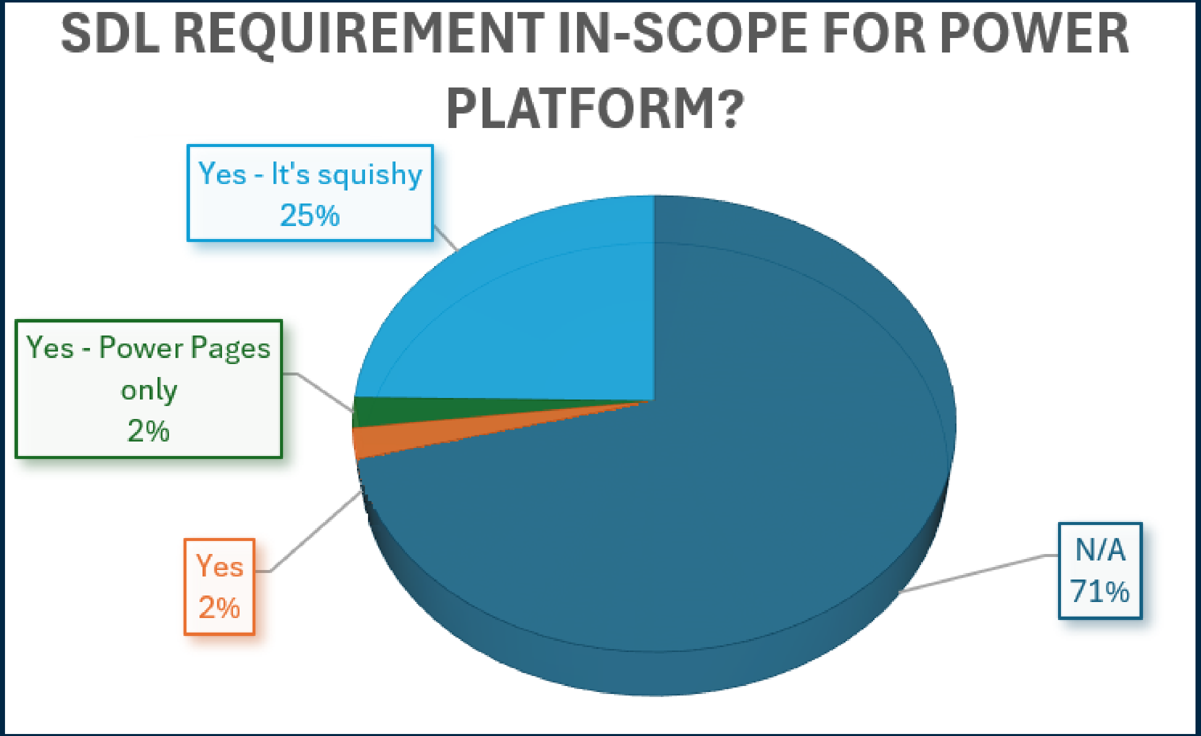
Learn about the practices of the SDL, and how to implement them in your organization.



How well does SDL Guidance fit?

How well does SDL Guidance fit?

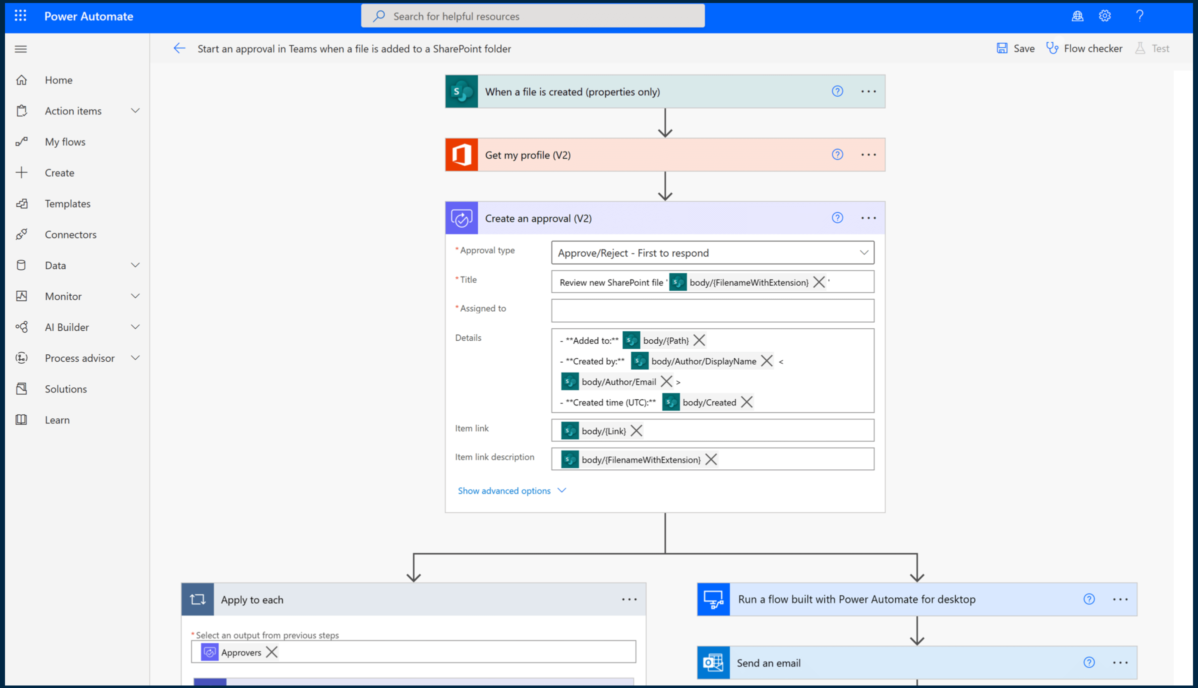
- Written for Code – LC/NC hides the complexity (and power!) of these tools



@mbrg0
@donwillits66
#BLUEHAT

How well does SDL Guidance fit?

- Written for Code – LC/NC hides the complexity (and power!) of these tools
- CodeQL (& SAST/DAST/IAST tooling in general) doesn't "speak" LC/NC



Start an approval in Teams when a file is added to a SharePoint folder

* Approval type: Approve/Reject - First to respond

* Title: Review new SharePoint file ' body/{FilenameWithExtension} '

* Assigned to:

Details:
- **Added to:** body/{Path}
- **Created by:** body/Author/DisplayName < body/Author/Email >
- **Created time (UTC):** body/Created

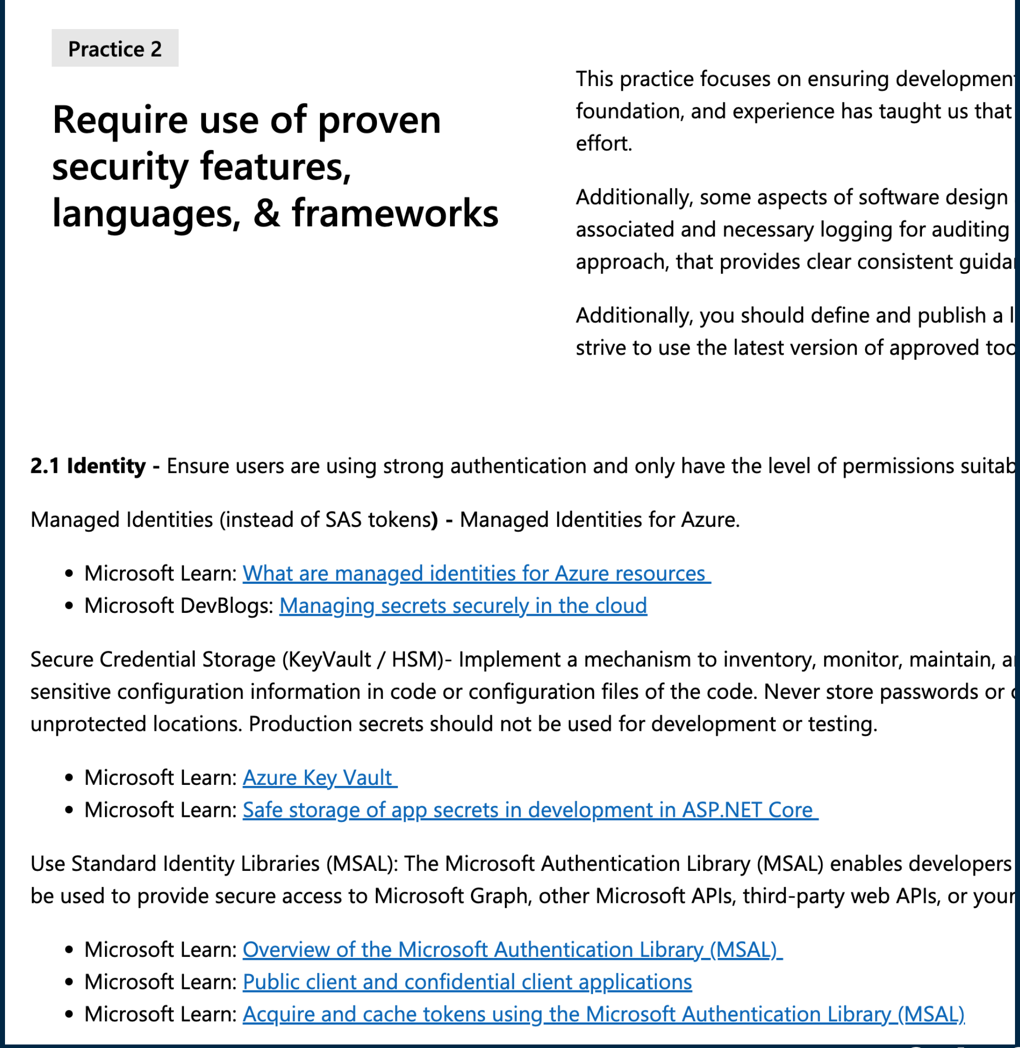
Item link: body/{Link}

Item link description: body/{FilenameWithExtension}

* Select an output from previous steps: Approvers

How well does SDL Guidance fit?

- Written for Code – LC/NC hides the complexity (and power!) of these tools
- CodeQL (& SAST/DAST/IAST tooling in general) doesn't "speak" LC/NC
- SDL content not written for business user,
  e.g. Citizen Developer



Practice 2

Require use of proven security features, languages, & frameworks

This practice focuses on ensuring developmen
foundation, and experience has taught us that
effort.

Additionally, some aspects of software design
associated and necessary logging for auditing
approach, that provides clear consistent guida

Additionally, you should define and publish a l
strive to use the latest version of approved too

2.1 Identity - Ensure users are using strong authentication and only have the level of permissions suitab

Managed Identities (instead of SAS tokens**)** **-** Managed Identities for Azure.

- Microsoft Learn: What are managed identities for Azure resources
- Microsoft DevBlogs: Managing secrets securely in the cloud

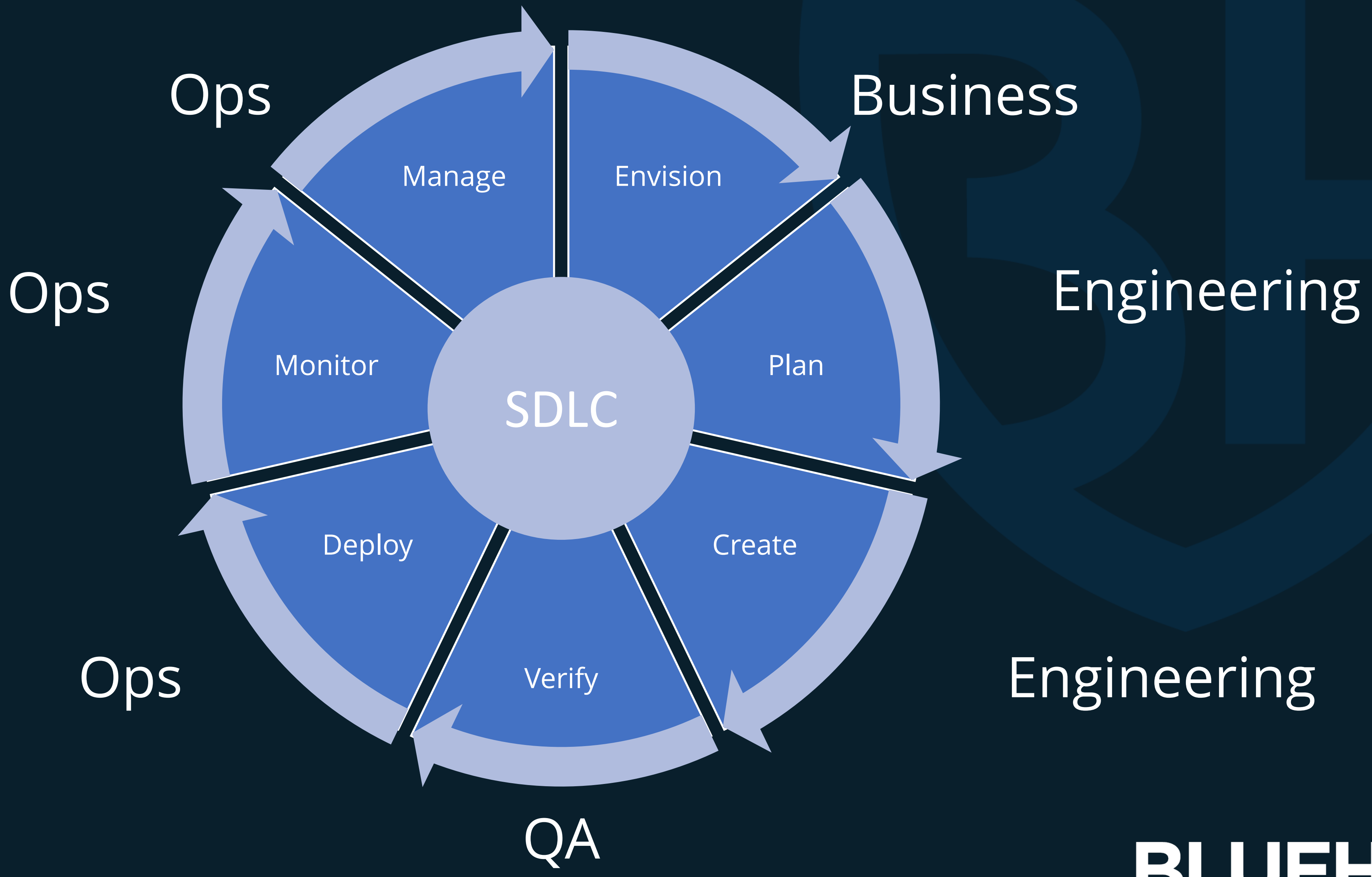
Secure Credential Storage (KeyVault / HSM)- Implement a mechanism to inventory, monitor, maintain, a
sensitive configuration information in code or configuration files of the code. Never store passwords or c
unprotected locations. Production secrets should not be used for development or testing.

- Microsoft Learn: Azure Key Vault
- Microsoft Learn: Safe storage of app secrets in development in ASP.NET Core

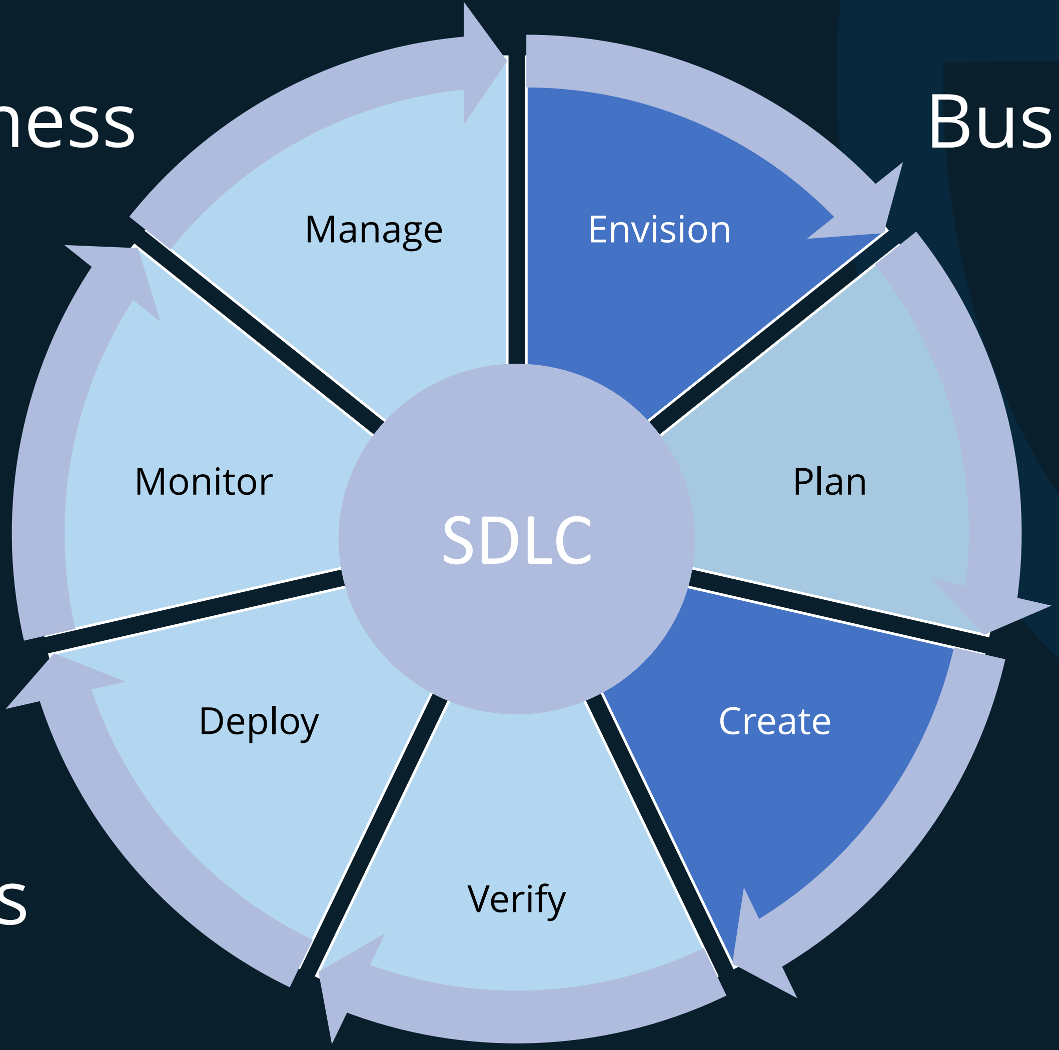
Use Standard Identity Libraries (MSAL): The Microsoft Authentication Library (MSAL) enables developers
be used to provide secure access to Microsoft Graph, other Microsoft APIs, third-party web APIs, or your

- Microsoft Learn: Overview of the Microsoft Authentication Library (MSAL)
- Microsoft Learn: Public client and confidential client applications
- Microsoft Learn: Acquire and cache tokens using the Microsoft Authentication Library (MSAL)

Pro
Code
SDLC



LC/NC
No SDLC?



Business

Business

Business

Business

Business

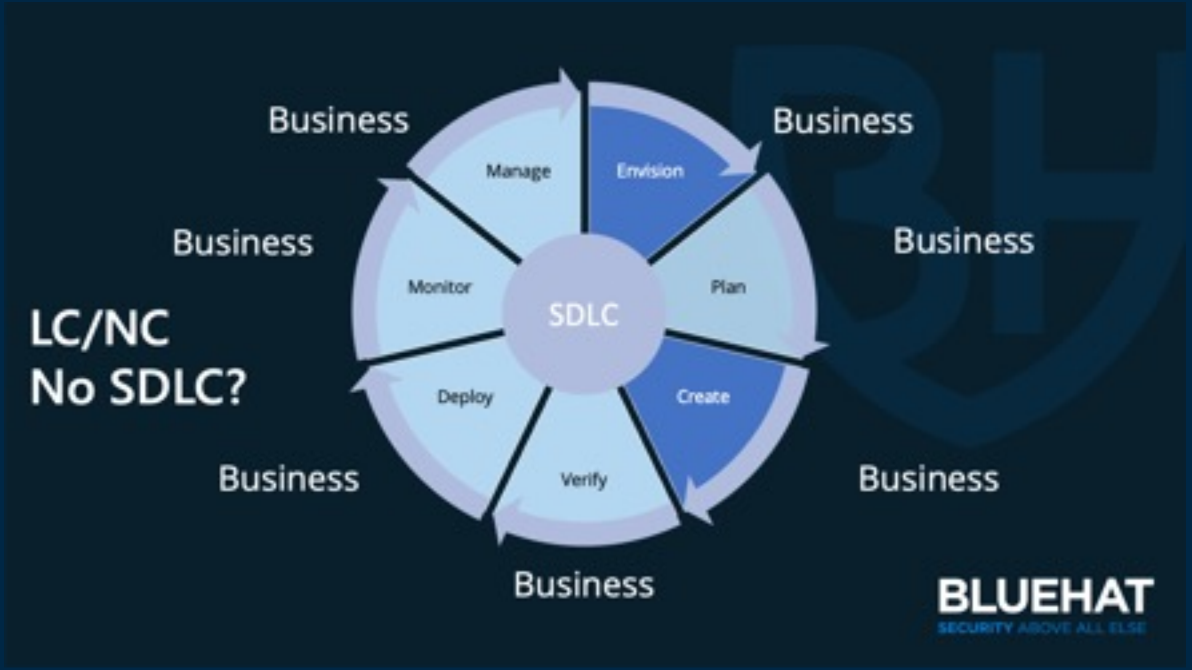
Business

Business

BLUEHAT
SECURITY ABOVE ALL ELSE

How well does SDL Guidance fit?

- Written for Code – LC/NC hides the complexity (and power!) of these tools
- CodeQL (& SAST/DAST/IAST tooling in general) doesn't "speak" LC/NC
- SDL content not written for business user,
  e.g. Citizen Developer
- Inconsistent CI/CD adoption (use ALM/pipelines!)



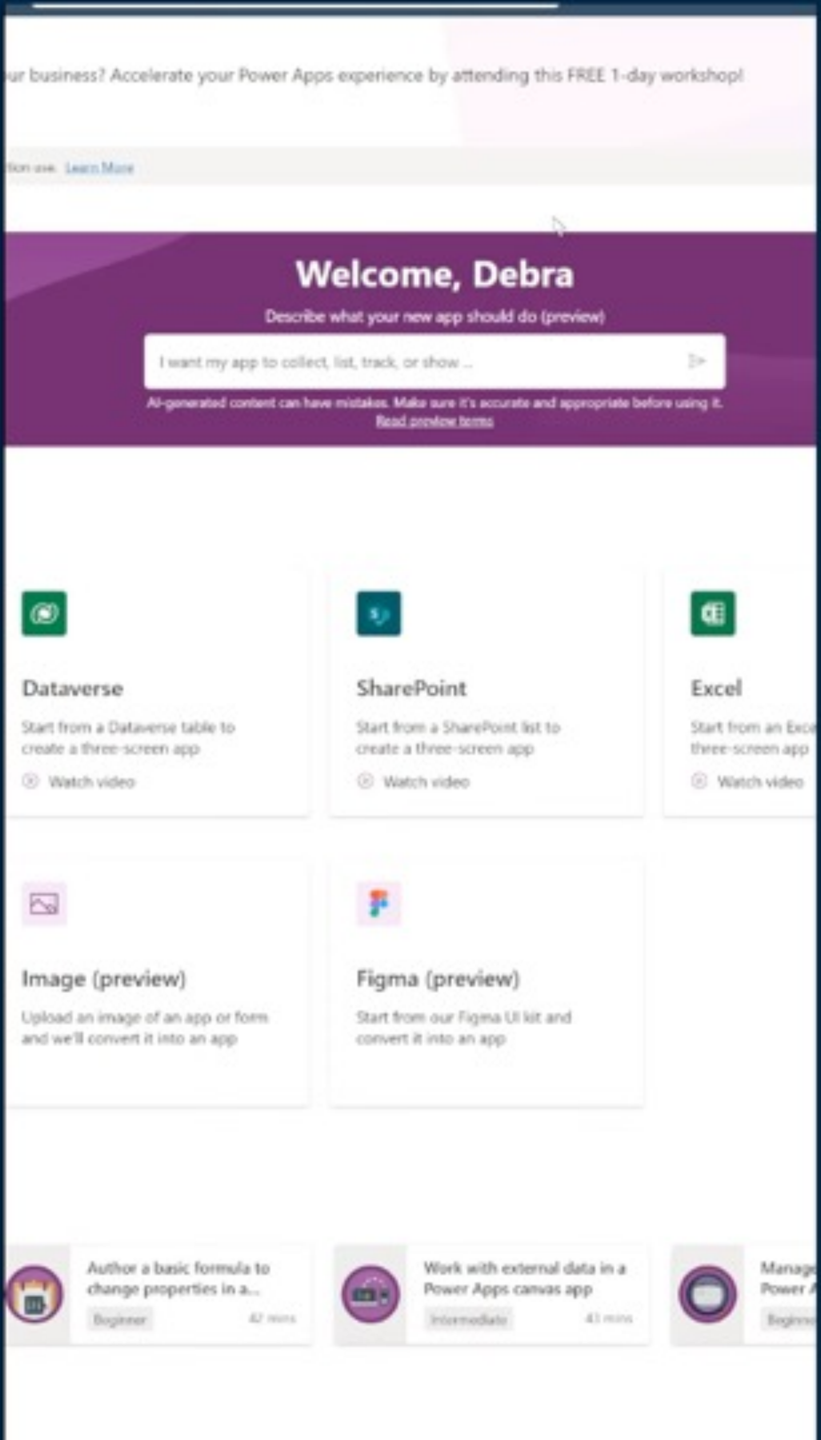
Sure, Let Business Users Build Their Own. What Could Go Wrong?
Michael Bargury, BlackHat USA 2023

Stuck at get-go

1. ~~Focus on crown jewels~~
2. ~~Get developer buy-in~~
3. ~~Secure Development Lifecycle (SDL)~~

1.1M apps

Building has never been easier



ur business? Accelerate your Power Apps experience by attending this FREE 1-day workshop!

tion use. Learn More

Welcome, Debra

Describe what your new app should do (preview)

I want my app to collect, list, track, or show ...

AI-generated content can have mistakes. Make sure it's accurate and appropriate before using it.
Read preview terms

Dataverse
Start from a Dataverse table to create a three-screen app
Watch video

SharePoint
Start from a SharePoint list to create a three-screen app
Watch video

Excel
Start from an Exce
three-screen app
Watch video

Image (preview)
Upload an image of an app or form and we'll convert it into an app

Figma (preview)
Start from our Figma UI kit and convert it into an app

Author a basic formula to change properties in a...
Beginner 42 mins

Work with external data in a Power Apps canvas app
Intermediate 41 mins

Manag
Power A
Beginn

@mbrg0
@donwillits66
#BLUEHAT

If building is easy, shouldn’t fixing vulns be easy too…?

AUTO-FIX

Remove unused credentials

Sanitize logs

Sanitize inputs

Change configs

Turn on logs

Use secure properties

Auto-fix ➔ Early success

Auto-fix → Early success

Early success → Buy-in

Auto-fix ➔ Early success

Early success ➔ Buy-in

Buy-in ➔ World domination ;)

Auto-fix → Early success

Early success → Buy-in

Buy-in → ~~World domination~~

Scale it

@mbrg0
@donwillits66
#BLUEHAT

PREMIERE PROPERTIES

HOW we made it work

Our goals

- Remediate all vulnerabilities (Get-to-Green/Stay-Green)

Our goals

- Remediate all vulnerabilities
- With 2-3 dedicated headcounts

Our goals

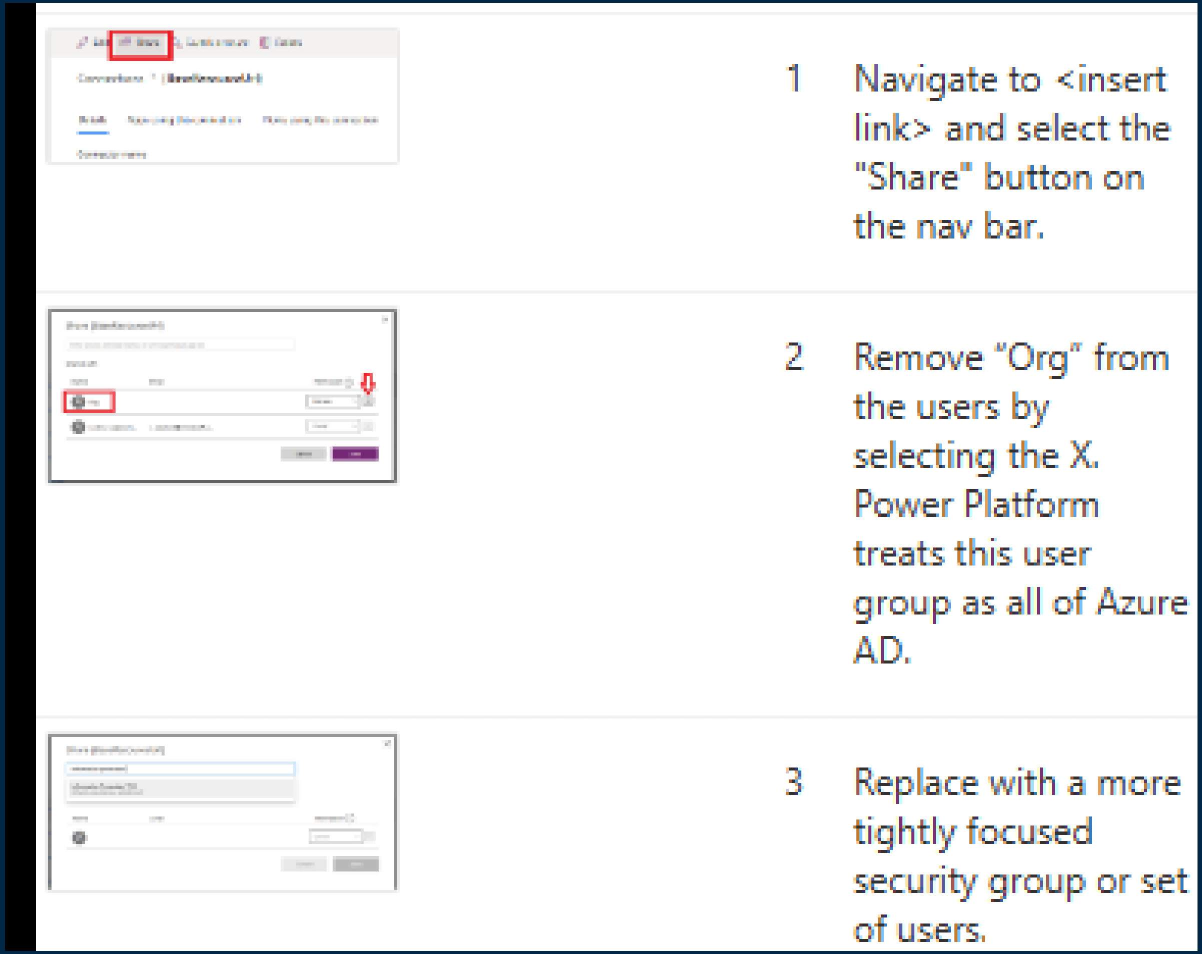
- Remediate all vulnerabilities
- With 2-3 dedicated headcounts
- Were given 6 months; we finished in a little over 4 months

Our goals

- Remediate all vulnerabilities
- With 2-3 dedicated headcounts
- Were given 6 months; we finished in a little over 4 months
- Minimum viable product / Self-serve

Minimum Viable Product

- Remediation Guidance: Write it for the business user, not a technical developer



1 Navigate to <insert link> and select the "Share" button on the nav bar.

2 Remove "Org" from the users by selecting the X. Power Platform treats this user group as all of Azure AD.

3 Replace with a more tightly focused security group or set of users.

Our goals

- Remediate all vulnerabilities
- With 2-3 dedicated headcounts
- Were given 6 months; we finished in a little over 4 months
- Minimum viable product / Self-serve
- Auto-fix (where possible)

Minimum Viable Product

- Automatic Remediation: Is the security violation auto-fixable?

Minimum Viable Product

- Automatic Remediation: Is the security violation auto-fixable?
  - Do we have enough context?
  - Can Zenity put the asset in a secure state?

Minimum Viable Product

- Automatic Remediation: Is the security violation auto-fixable?
  - Do we have enough context?
  - Can Zenity put the asset in a secure state?
  - If YES… we trigger correcting the misconfiguration silently while the developer sleeps

Minimum Viable Product

- Balance a reasonable time to fix before we “shift + delete” in secure assets (Apps, Flows, etc.)
  - We settled on “30 days-to-fix” as a reasonable compromise providing “just enough time” vs. “not too much time”

Minimum Viable Product

- Brownfield: Pre-existing risk/security violations created on or before Jan 1st, 2024 (when our campaigns started)

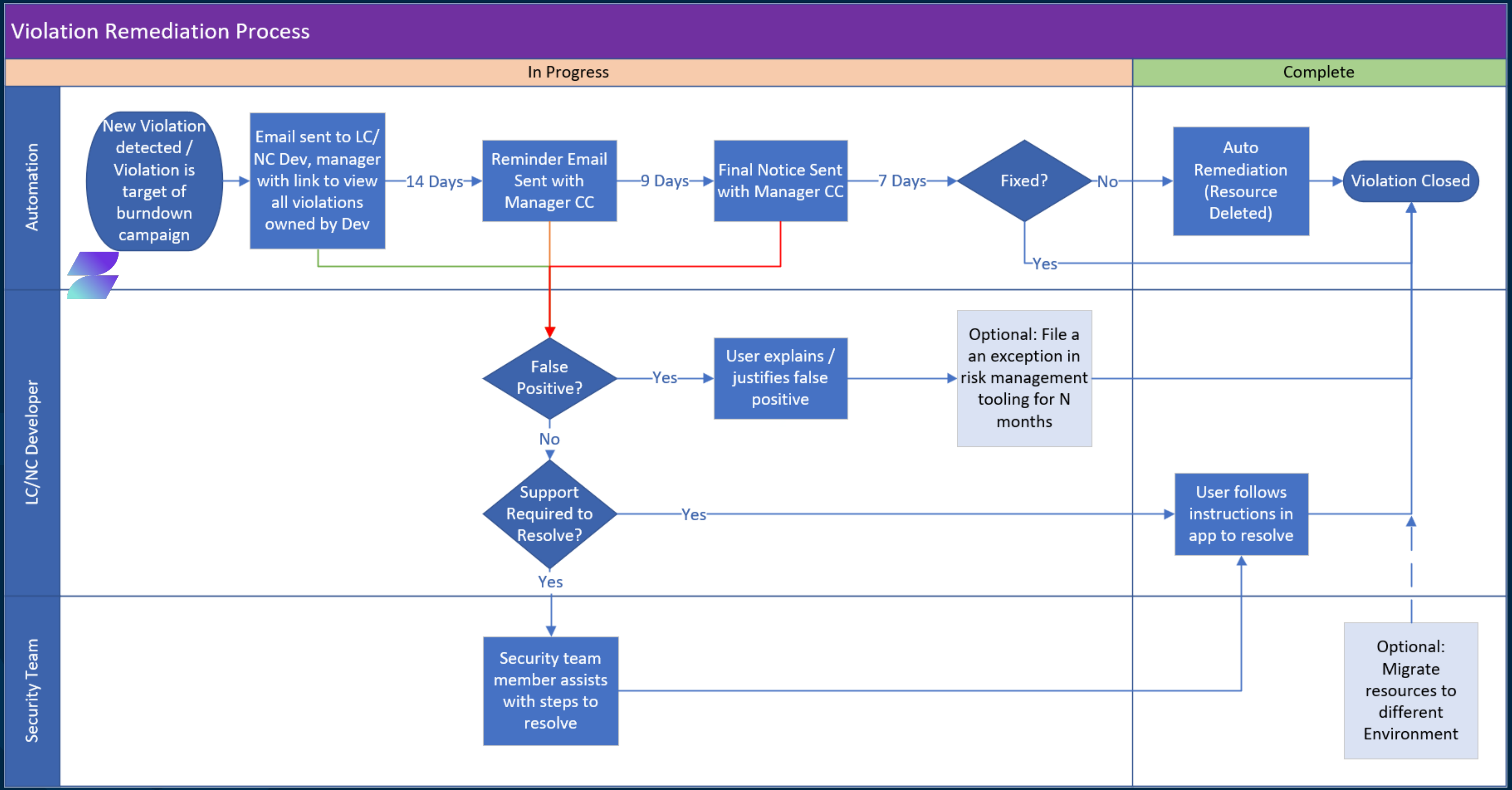
  a.k.a. “Get to Green”

Minimum Viable Product

- Brownfield: Pre-existing risk/security violations created on or before Jan 1st, 2024 (when our campaigns started)
- Greenfield: Net new risk created continuously/daily in our tenant after Jan 1st, 2024

a.k.a. “Stay Green”

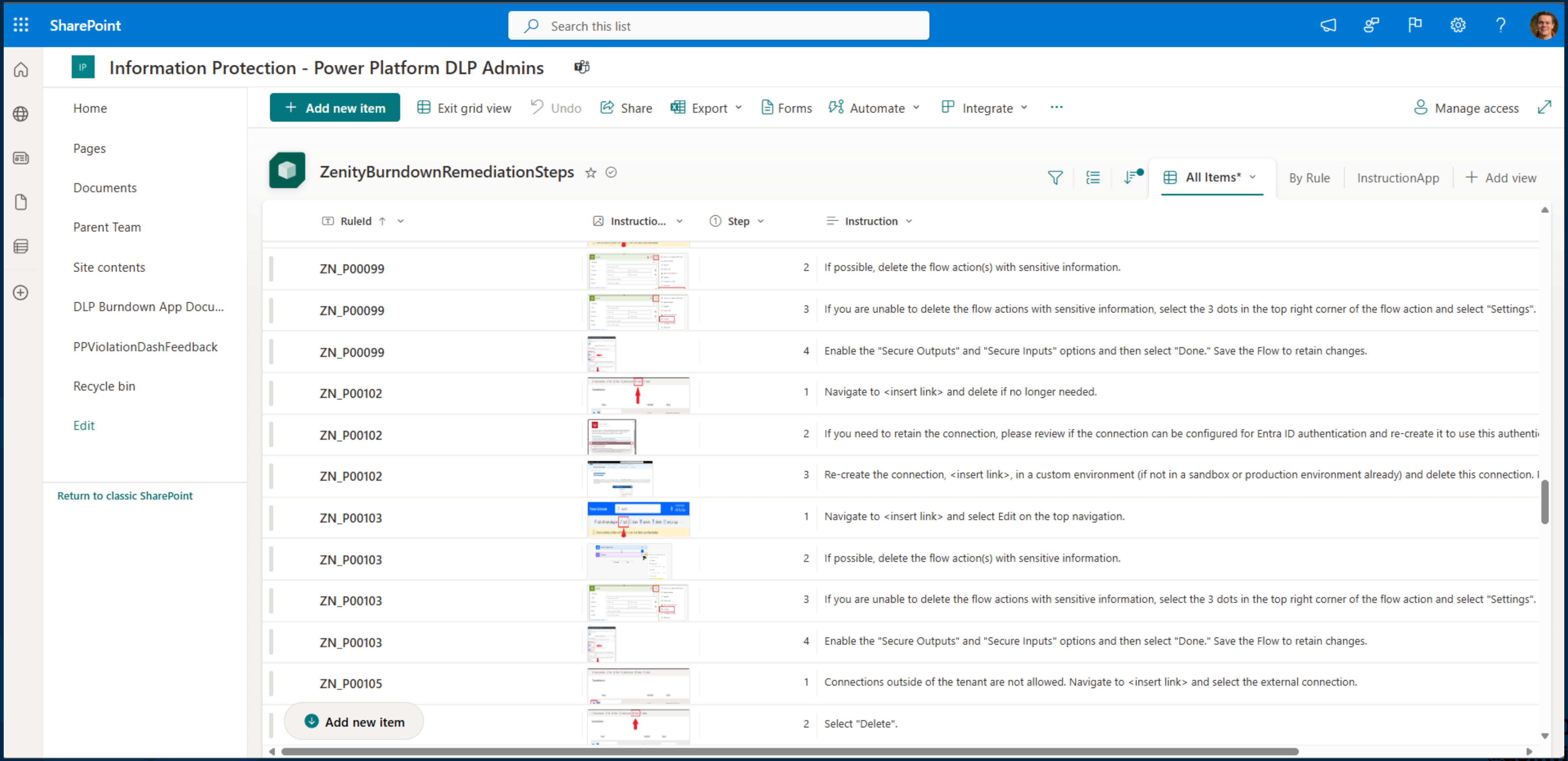
Early Success led to longer campaigns



Violation Remediation Process
In Progress
Complete
Automation
LC/NC Developer
Security Team
New Violation detected / Violation is target of burndown campaign
Email sent to LC/ NC Dev, manager with link to view all violations owned by Dev
14 Days
Reminder Email Sent with Manager CC
9 Days
Final Notice Sent with Manager CC
7 Days
Fixed?
No
Yes
Auto Remediation (Resource Deleted)
Violation Closed
False Positive?
Yes
User explains / justifies false positive
Optional: File a an exception in risk management tooling for N months
No
Support Required to Resolve?
Yes
User follows instructions in app to resolve
Yes
Security team member assists with steps to resolve
Optional: Migrate resources to different Environment

@mbrg0
@donwillits66
#BLUEHAT

Self Service – SharePoint List of Instructions

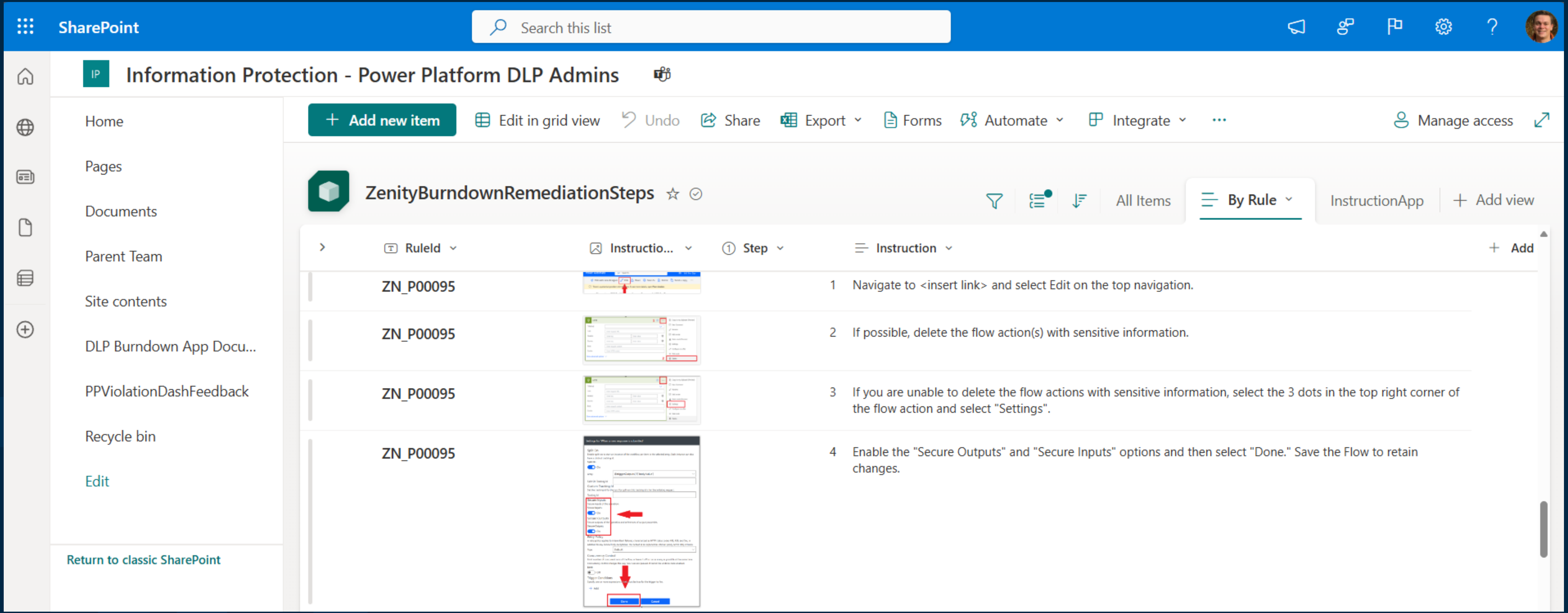


Information Protection - Power Platform DLP Admins

ZenityBurndownRemediationSteps

RuleId	Instructio...	Step	Instruction
ZN_P00099		2	If possible, delete the flow action(s) with sensitive information.
ZN_P00099		3	If you are unable to delete the flow actions with sensitive information, select the 3 dots in the top right corner of the flow action and select "Settings".
ZN_P00099		4	Enable the "Secure Outputs" and "Secure Inputs" options and then select "Done." Save the Flow to retain changes.
ZN_P00102		1	Navigate to <insert link> and delete if no longer needed.
ZN_P00102		2	If you need to retain the connection, please review if the connection can be configured for Entra ID authentication and re-create it to use this authenti
ZN_P00102		3	Re-create the connection, <insert link>, in a custom environment (if not in a sandbox or production environment already) and delete this connection. I
ZN_P00103		1	Navigate to <insert link> and select Edit on the top navigation.
ZN_P00103		2	If possible, delete the flow action(s) with sensitive information.
ZN_P00103		3	If you are unable to delete the flow actions with sensitive information, select the 3 dots in the top right corner of the flow action and select "Settings".
ZN_P00103		4	Enable the "Secure Outputs" and "Secure Inputs" options and then select "Done." Save the Flow to retain changes.
ZN_P00105		1	Connections outside of the tenant are not allowed. Navigate to <insert link> and select the external connection.
		2	Select "Delete".

Self Service – Step-by-Step Instructions

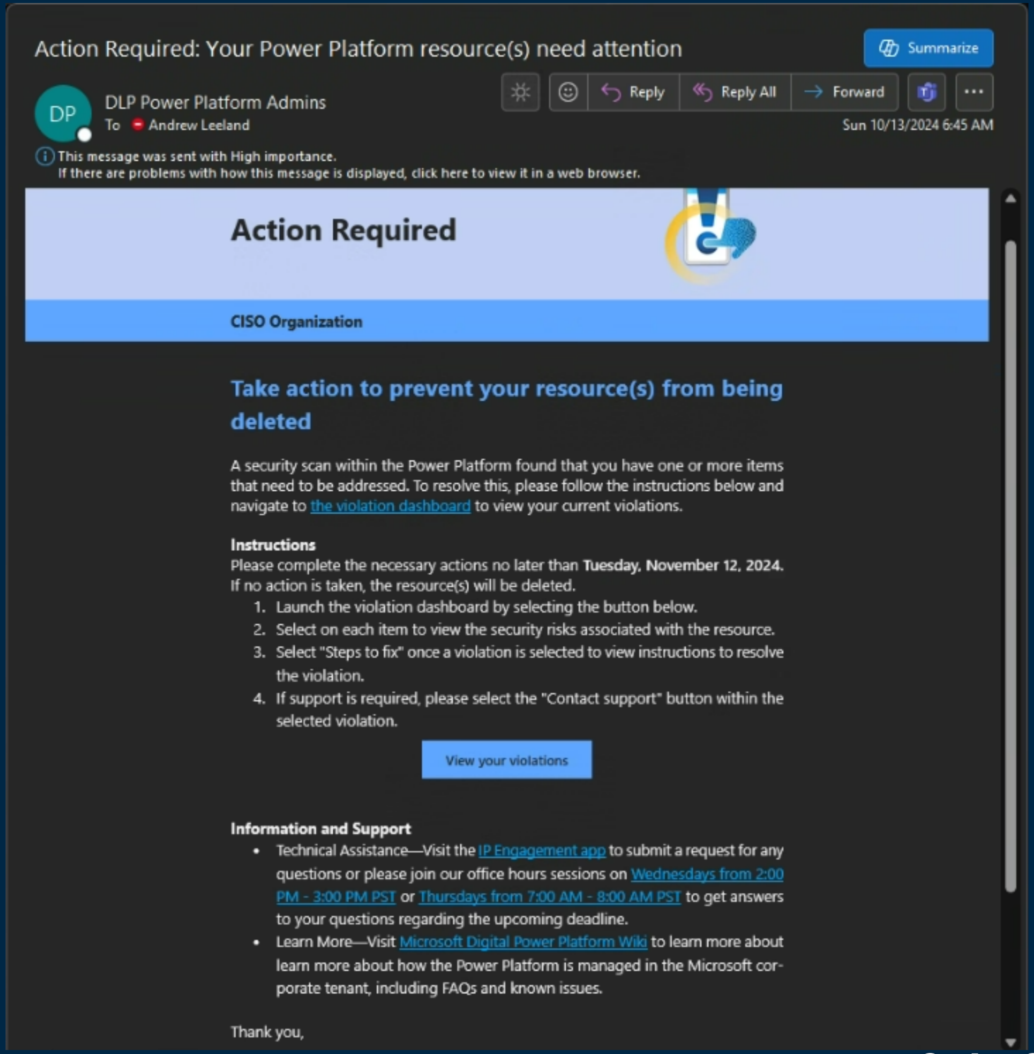


RuleId	Instructio...	Step	Instruction
ZN_P00095		1	Navigate to <insert link> and select Edit on the top navigation.
ZN_P00095		2	If possible, delete the flow action(s) with sensitive information.
ZN_P00095		3	If you are unable to delete the flow actions with sensitive information, select the 3 dots in the top right corner of the flow action and select "Settings".
ZN_P00095		4	Enable the "Secure Outputs" and "Secure Inputs" options and then select "Done." Save the Flow to retain changes.

@mbrg0
@donwillits66
#BLUEHAT

Self Service – Email

- 1st mail goes out
- Redirects user to Violations Dashboard (PowerApp)
  - Manage all their violations
- 30 days-to-fix
- Goes to both Creator and Current Owners of the asset



Action Required: Your Power Platform resource(s) need attention

DLP Power Platform Admins
To Andrew Leeland

Sun 10/13/2024 6:45 AM

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

Action Required

CISO Organization

Take action to prevent your resource(s) from being deleted

A security scan within the Power Platform found that you have one or more items that need to be addressed. To resolve this, please follow the instructions below and navigate to the violation dashboard to view your current violations.

Instructions
Please complete the necessary actions no later than **Tuesday, November 12, 2024.** If no action is taken, the resource(s) will be deleted.

1. Launch the violation dashboard by selecting the button below.
2. Select on each item to view the security risks associated with the resource.
3. Select "Steps to fix" once a violation is selected to view instructions to resolve the violation.
4. If support is required, please select the "Contact support" button within the selected violation.

View your violations

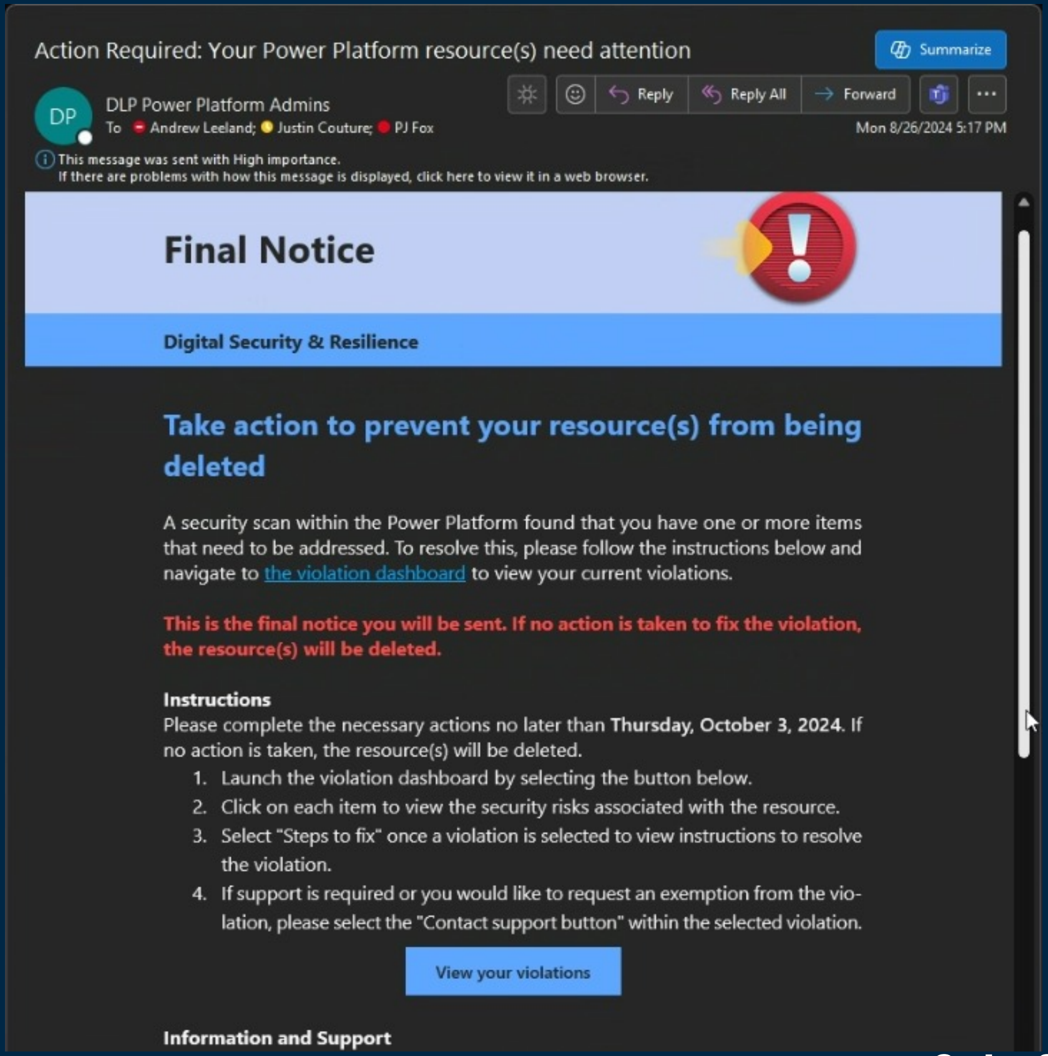
Information and Support

- Technical Assistance—Visit the IP Engagement app to submit a request for any questions or please join our office hours sessions on Wednesdays from 2:00 PM - 3:00 PM PST or Thursdays from 7:00 AM - 8:00 AM PST to get answers to your questions regarding the upcoming deadline.
- Learn More—Visit Microsoft Digital Power Platform Wiki to learn more about learn more about how the Power Platform is managed in the Microsoft corporate tenant, including FAQs and known issues.

Thank you,

Self Service – Final Email

- Final Warning mail



Action Required: Your Power Platform resource(s) need attention

DLP Power Platform Admins
To Andrew Leeland; Justin Couture; PJ Fox
Mon 8/26/2024 5:17 PM

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

Final Notice

Digital Security & Resilience

Take action to prevent your resource(s) from being deleted

A security scan within the Power Platform found that you have one or more items that need to be addressed. To resolve this, please follow the instructions below and navigate to the violation dashboard to view your current violations.

This is the final notice you will be sent. If no action is taken to fix the violation, the resource(s) will be deleted.

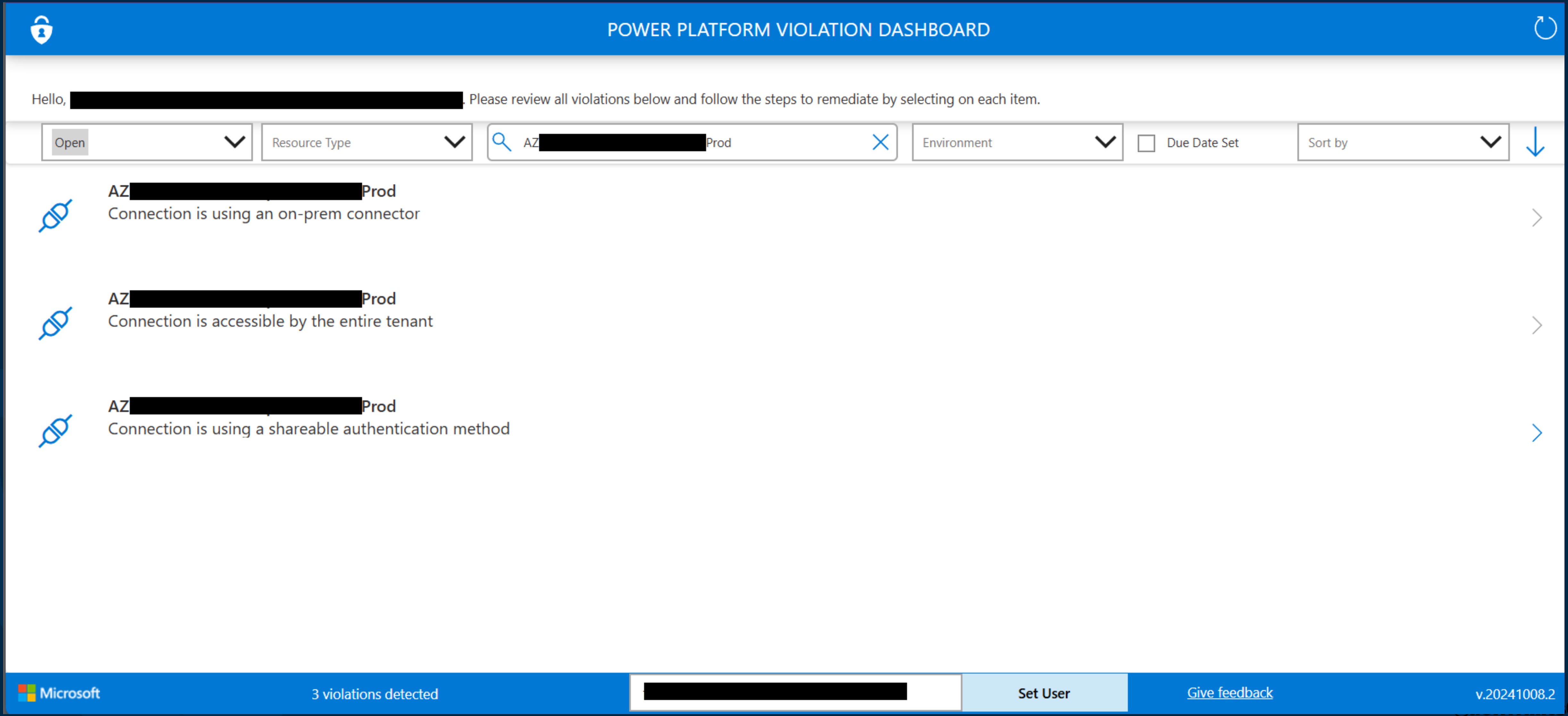
Instructions
Please complete the necessary actions no later than **Thursday, October 3, 2024**. If no action is taken, the resource(s) will be deleted.

1. Launch the violation dashboard by selecting the button below.
2. Click on each item to view the security risks associated with the resource.
3. Select "Steps to fix" once a violation is selected to view instructions to resolve the violation.
4. If support is required or you would like to request an exemption from the violation, please select the "Contact support button" within the selected violation.

View your violations

Information and Support

Self Service – Violations Dashboard



POWER PLATFORM VIOLATION DASHBOARD

Hello, [redacted]. Please review all violations below and follow the steps to remediate by selecting on each item.

Open | Resource Type | AZ[redacted]Prod | Environment | □ Due Date Set | Sort by

AZ[redacted]Prod
Connection is using an on-prem connector

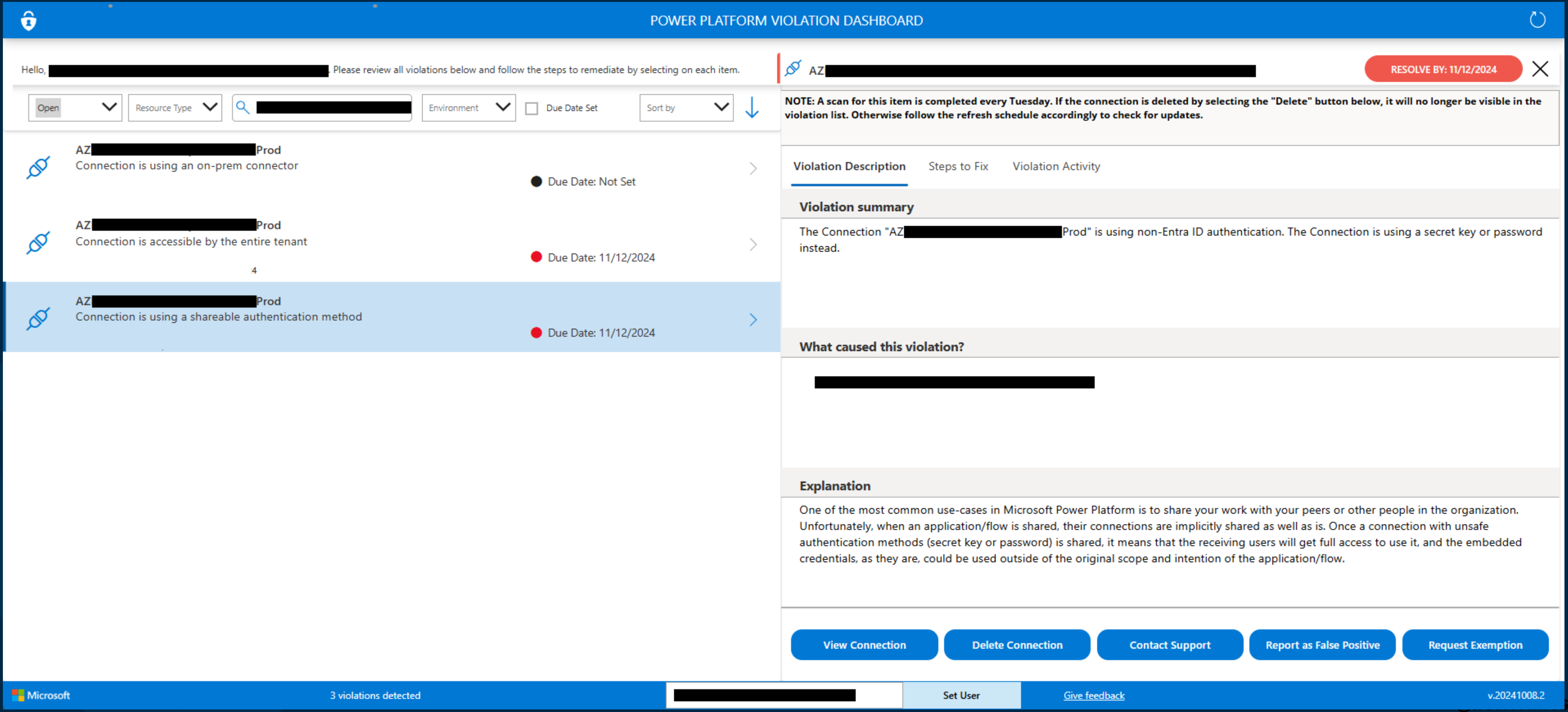
AZ[redacted]Prod
Connection is accessible by the entire tenant

AZ[redacted]Prod
Connection is using a shareable authentication method

Microsoft | 3 violations detected | [redacted] | Set User | Give feedback | v.20241008.2

66
#BLUEHAT

Self Service – Violations Dashboard Details



POWER PLATFORM VIOLATION DASHBOARD

Hello, [redacted] Please review all violations below and follow the steps to remediate by selecting on each item.

AZ[redacted]Prod
Connection is using an on-prem connector
● Due Date: Not Set

AZ[redacted]Prod
Connection is accessible by the entire tenant
● Due Date: 11/12/2024

4

AZ[redacted]Prod
Connection is using a shareable authentication method
● Due Date: 11/12/2024

AZ[redacted]

RESOLVE BY: 11/12/2024

NOTE: A scan for this item is completed every Tuesday. If the connection is deleted by selecting the "Delete" button below, it will no longer be visible in the violation list. Otherwise follow the refresh schedule accordingly to check for updates.

Violation summary

The Connection "AZ[redacted]Prod" is using non-Entra ID authentication. The Connection is using a secret key or password instead.

What caused this violation?

[redacted]

Explanation

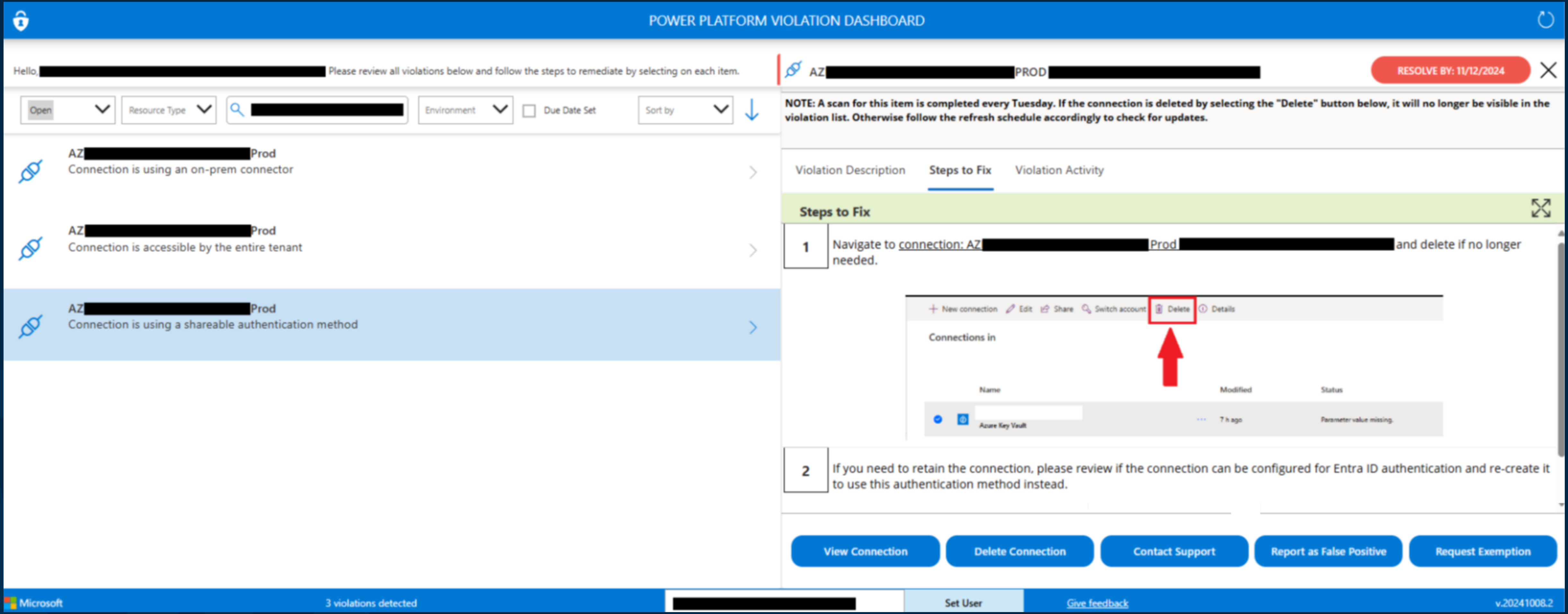
One of the most common use-cases in Microsoft Power Platform is to share your work with your peers or other people in the organization. Unfortunately, when an application/flow is shared, their connections are implicitly shared as well as is. Once a connection with unsafe authentication methods (secret key or password) is shared, it means that the receiving users will get full access to use it, and the embedded credentials, as they are, could be used outside of the original scope and intention of the application/flow.

3 violations detected

[redacted]

v.20241008.2

Self Service – Violations Dashboard Remediation



POWER PLATFORM VIOLATION DASHBOARD

Hello, [redacted] Please review all violations below and follow the steps to remediate by selecting on each item.

AZ[redacted]Prod
Connection is using an on-prem connector

AZ[redacted]Prod
Connection is accessible by the entire tenant

AZ[redacted]Prod
Connection is using a shareable authentication method

AZ[redacted]PROD[redacted]

RESOLVE BY: 11/12/2024

NOTE: A scan for this item is completed every Tuesday. If the connection is deleted by selecting the "Delete" button below, it will no longer be visible in the violation list. Otherwise follow the refresh schedule accordingly to check for updates.

Steps to Fix

1 Navigate to connection: AZ[redacted]Prod[redacted]and delete if no longer needed.

2 If you need to retain the connection, please review if the connection can be configured for Entra ID authentication and re-create it to use this authentication method instead.

[redacted]

@mbrg0
@donwillits66
#BLUEHAT

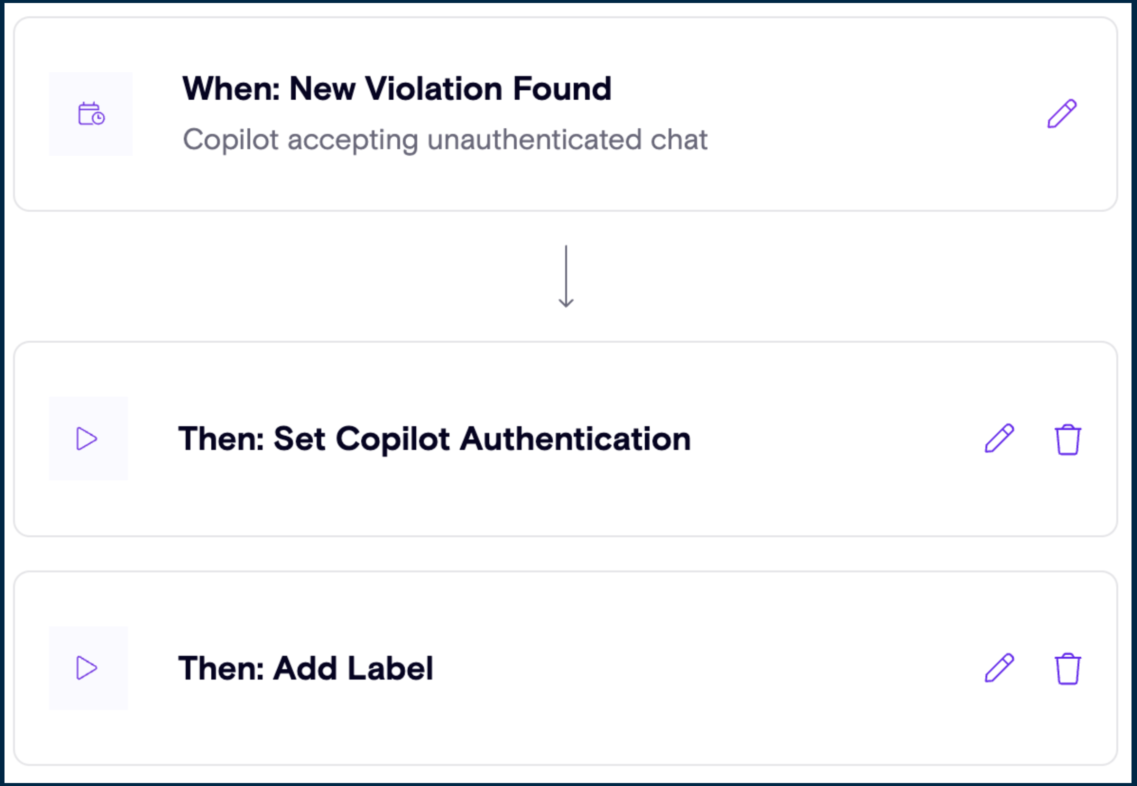
Playbooks

- Greenfield: As new violations come in…

- Brownfield: When we send out bulk emails to burn down pre-existing risk…

- If rule ID is XYZ, and other condition(s) are true…

  …then take these actions



When: New Violation Found

Copilot accepting unauthenticated chat

↓

Then: Set Copilot Authentication

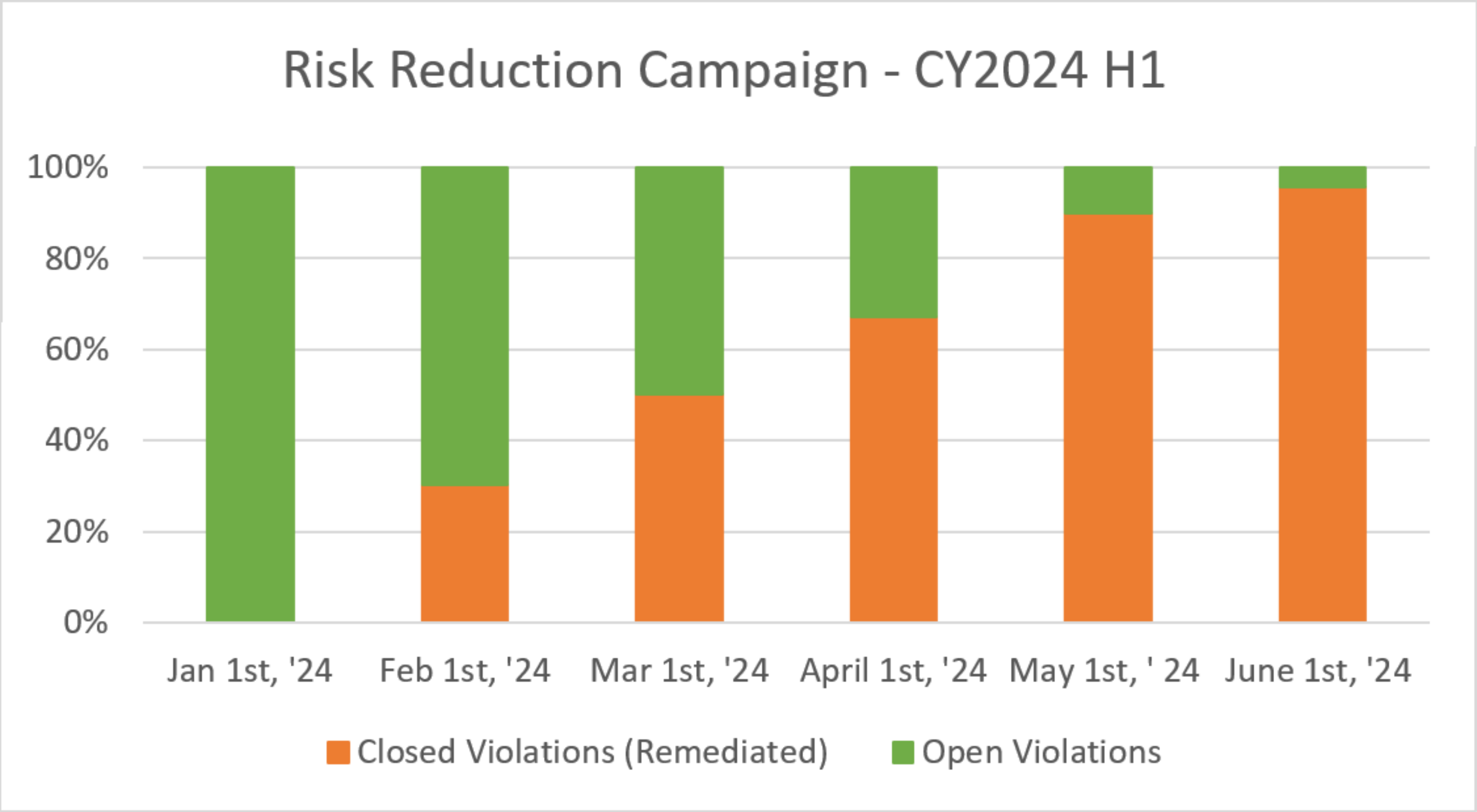
Then: Add Label

@mbrg0
@donwillits66
#BLUEHAT

Results

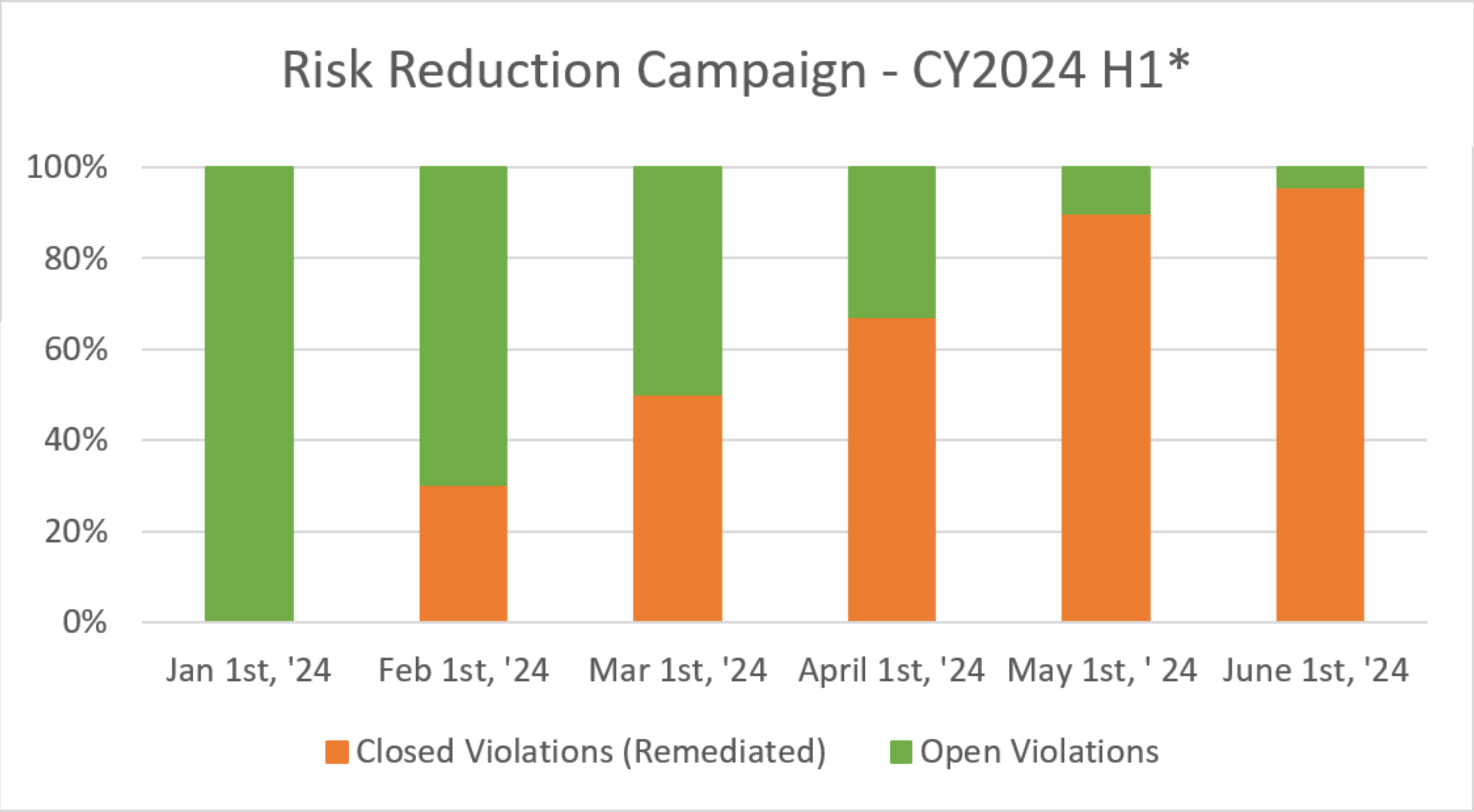
- Jan 18th, 2024 – April 30th, 2024
  - Prove we can scale-up
  - Prove we can Get-to-Green in two environments
  - Prove we can Get-to-Green and Stay-Green with identical tooling and processes

SUCCESS



@mbrg0
@donwillits66
#BLUEHAT

SUCCESS



* Never get to 100% remediated because of 30 days-to-fix

@mbrg0
@donwillits66
#BLUEHAT

SUCCESS

Takeaways

What did we learn from this?

- Leverage industry-standard security risk categorization

OWASP Top 10 for Low-Code/No-Code

- LCNC01: Account Impersonation
- LCNC02: Authorization Misuse
- LCNC03: Data Leakage and Unexpected Consequences
- LCNC04: Authentication and Secure Communication Failures
- LCNC05: Security Misconfiguration
- LCNC06: Injection Handling Failures
- LCNC07: Vulnerable and Untrusted Components
- LCNC08: Data and Secret Handling Failures
- LCNC09: Asset Management Failures
- LCNC10: Security Logging and Monitoring Failures

OWASP Top 10 for Large Language Models

- LLM01: Prompt Injection
- LLM02: Insecure Output Handling
- LLM03: Training Data Poisoning
- LLM04: Model Denial of Service
- LLM05: Supply Chain Vulnerabilities
- LLM06: Sensitive Information Disclosure
- LLM07: Insecure plugin design
- LLM08: Excessive Agency
- LLM09: Overreliance
- LLM10: Model Theft

As LC/NC platforms increasingly embrace AI, this will become increasingly relevant

What did we learn from this?

✓Leverage industry-standard security risk categorization

- Prioritize what we want to fix first

6 Risk Reduction Campaigns

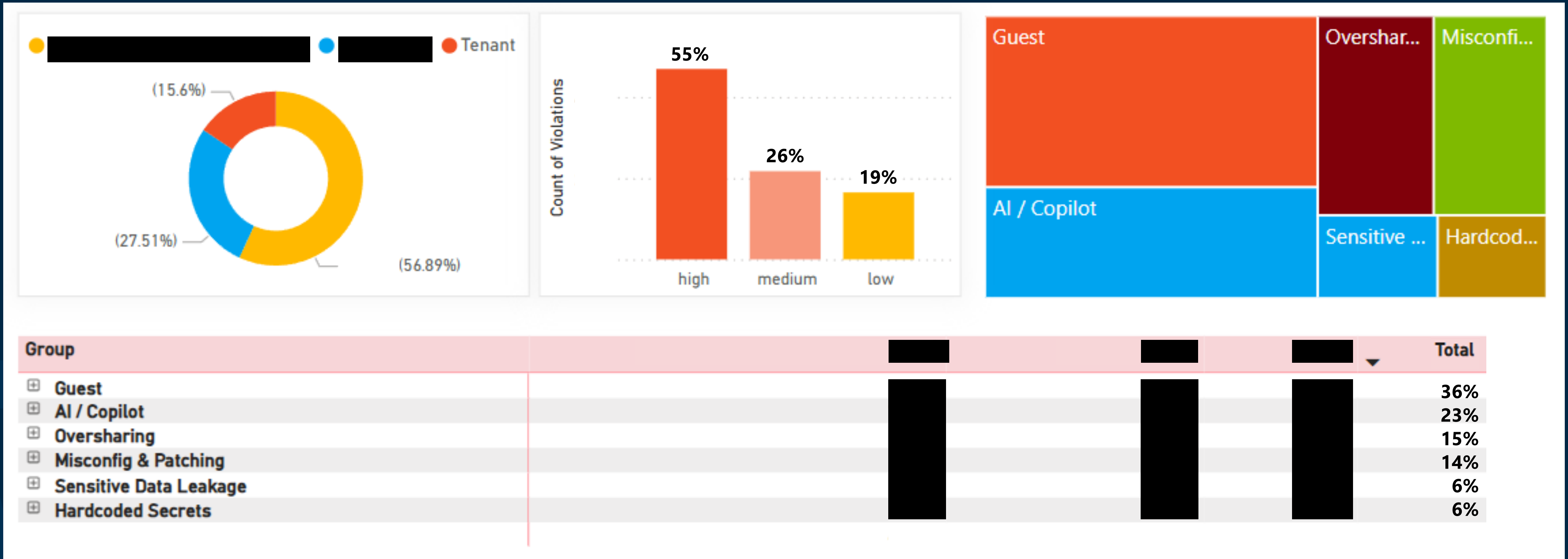
Merged similar OWASP Top 10 categories together & reviewed SDL gap analysis

- Also pivoted on Senior Leadership Team priorities

Campaigns included:

- Guest/Access Control
- AI/Copilot issues
- Oversharing of data
- Sensitive Data Leakage
- Hardcoded Secrets
- Misconfig & Miscellany

“Oversharing…” and “Sensitive data…” sound identical, but there were enough distinctions in the scanning ruleset that they were distinct campaigns.



Group	[redacted]	[redacted]	[redacted]	Total
⊞ Guest	[redacted]	[redacted]	[redacted]	36%
⊞ AI / Copilot	[redacted]	[redacted]	[redacted]	23%
⊞ Oversharing	[redacted]	[redacted]	[redacted]	15%
⊞ Misconfig & Patching	[redacted]	[redacted]	[redacted]	14%
⊞ Sensitive Data Leakage	[redacted]	[redacted]	[redacted]	6%
⊞ Hardcoded Secrets	[redacted]	[redacted]	[redacted]	6%

@mbrg0
@donwillits66
#BLUEHAT

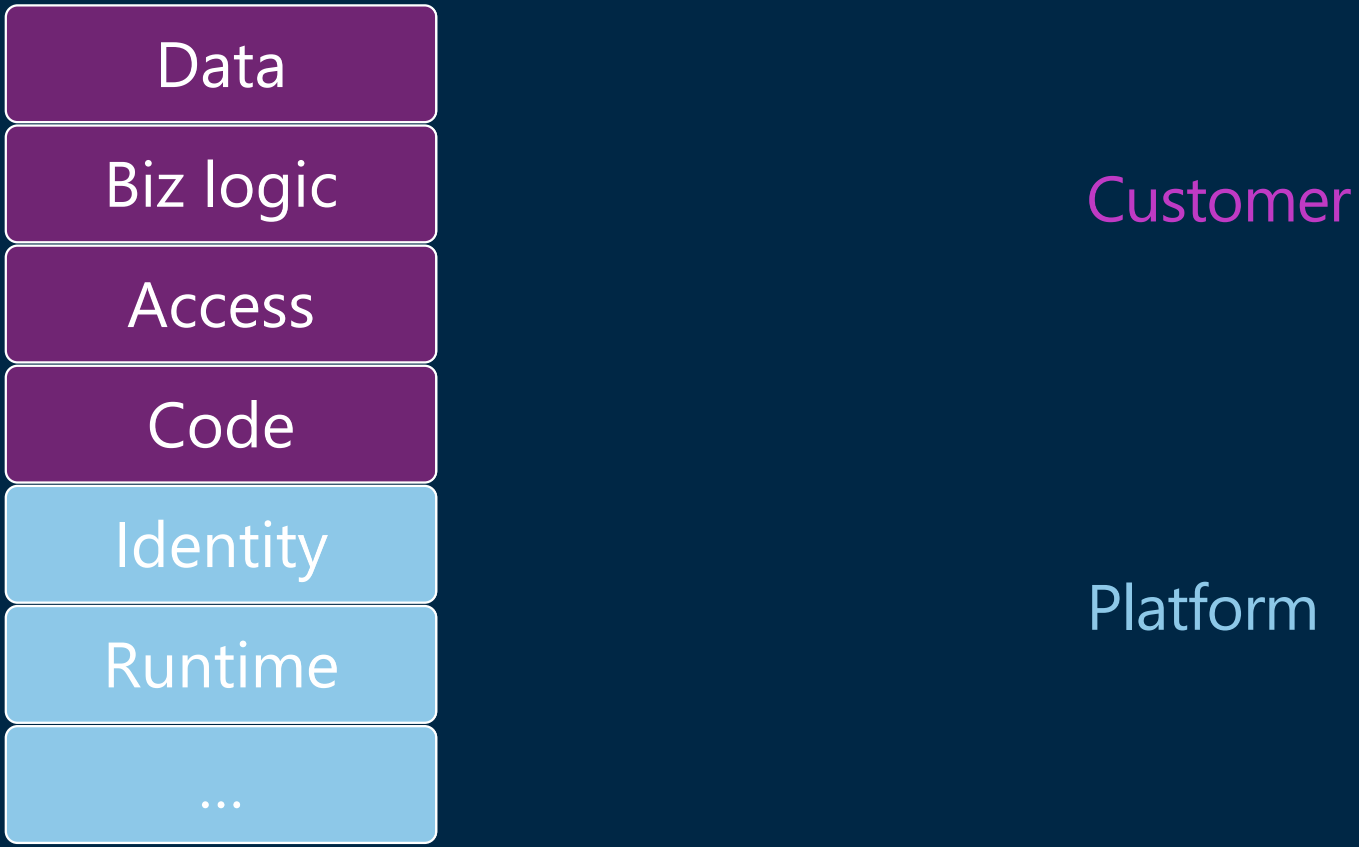
What did we learn from this?

✓Leverage industry-standard security risk categorization

✓Prioritize what we want to fix first

- Shared Responsibility Model

Serverless



Data

Biz logic

Access

Code

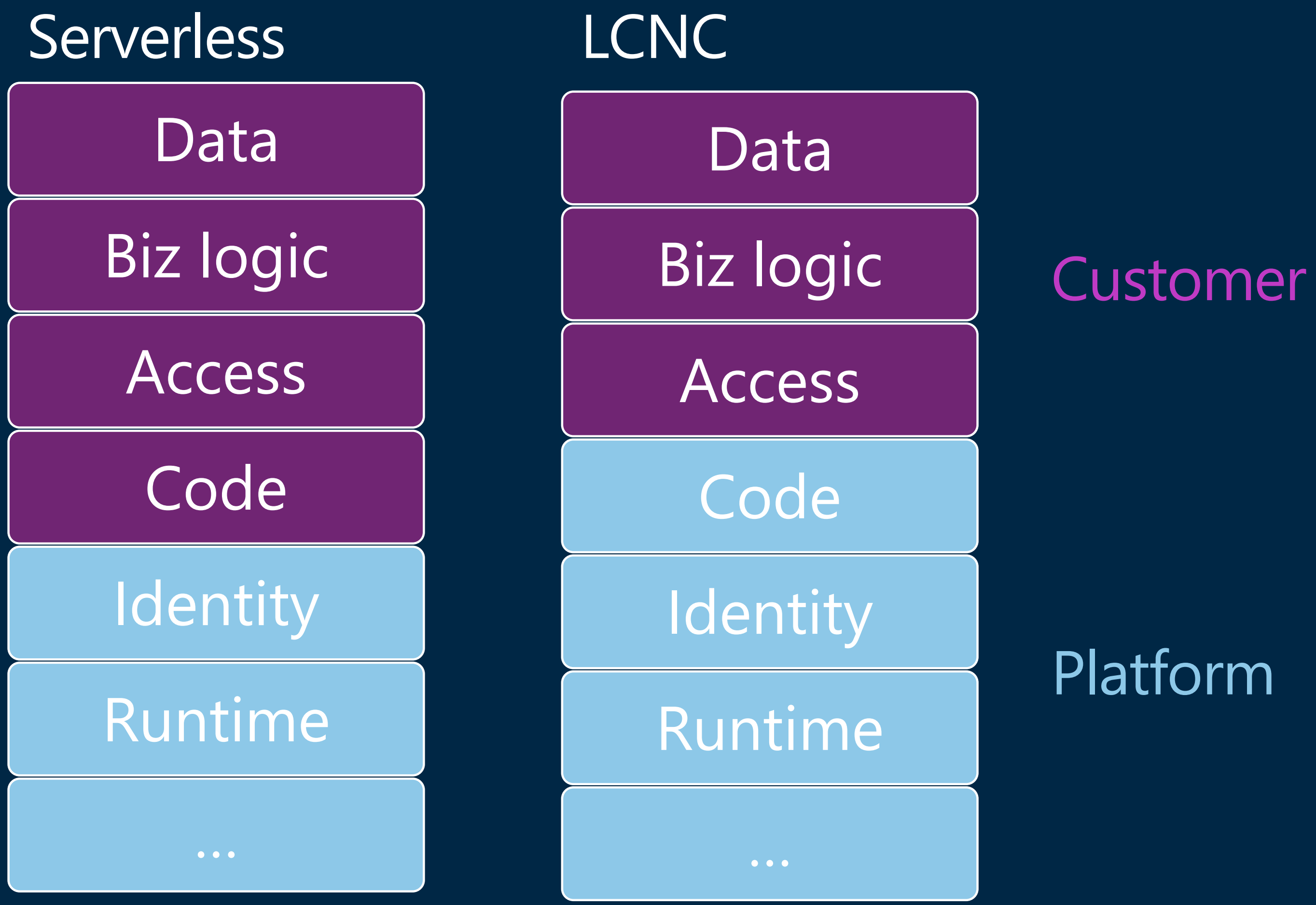
Identity

Runtime

…

Customer

Platform



Serverless

Data

Biz logic

Access

Code

Identity

Runtime

…

LCNC

Data

Biz logic

Access

Code

Identity

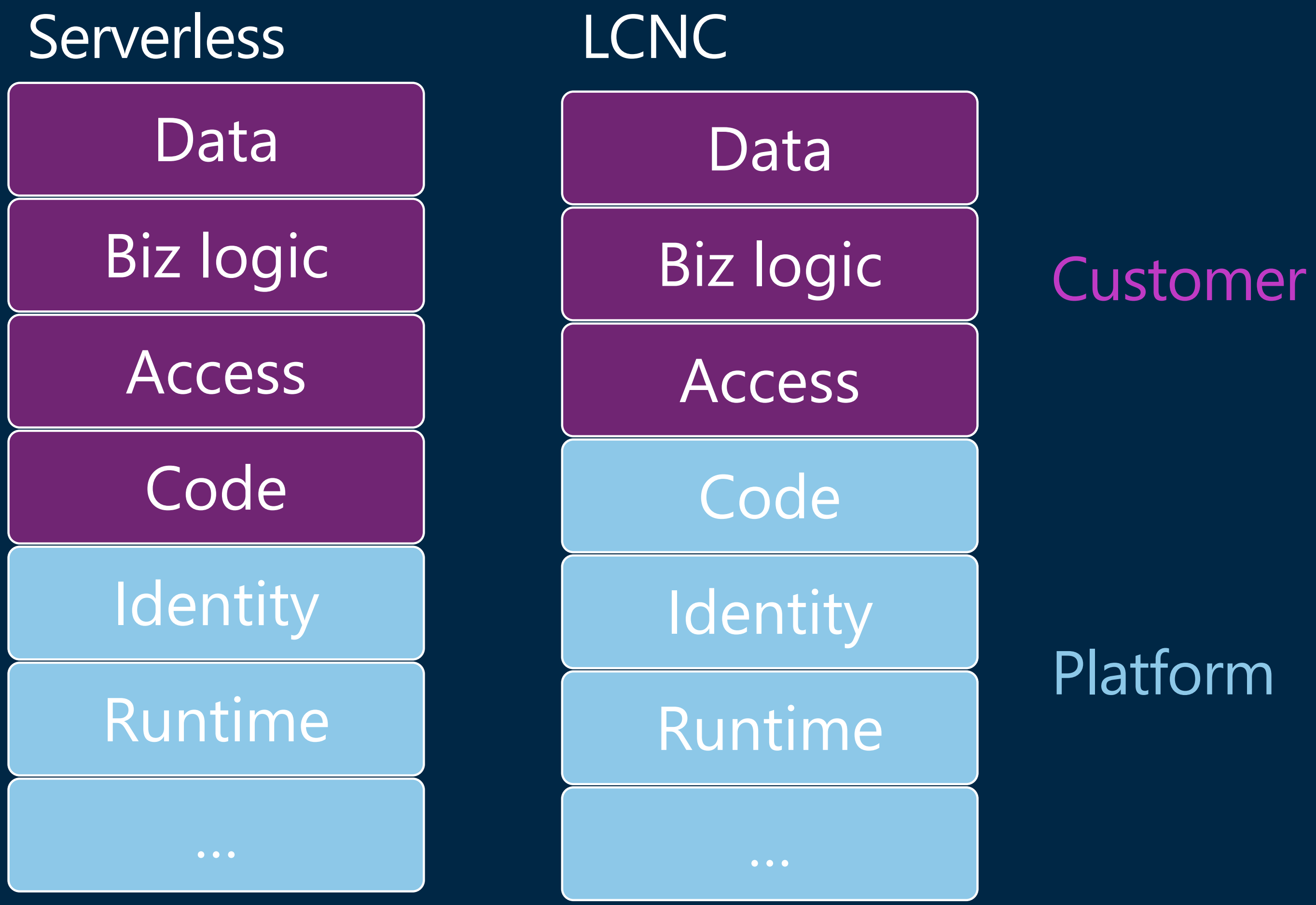
Runtime

…

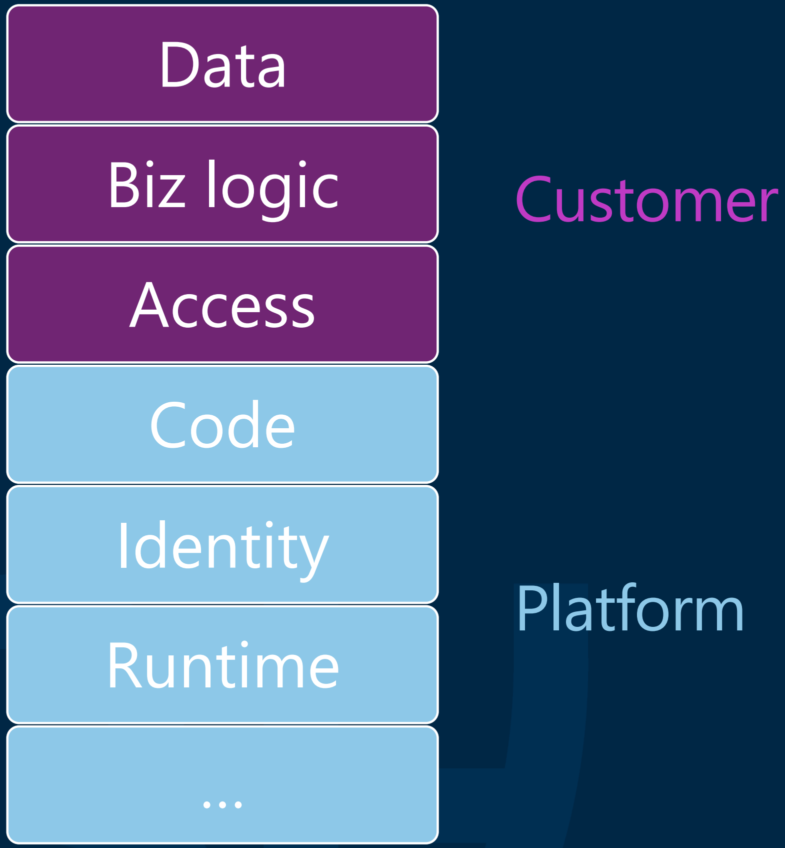
Customer

Platform

We must own our side of the Shared Responsibility Model



Sure, let business users build they own. What could go wrong?



Data

Biz logic

Access

Code

Identity

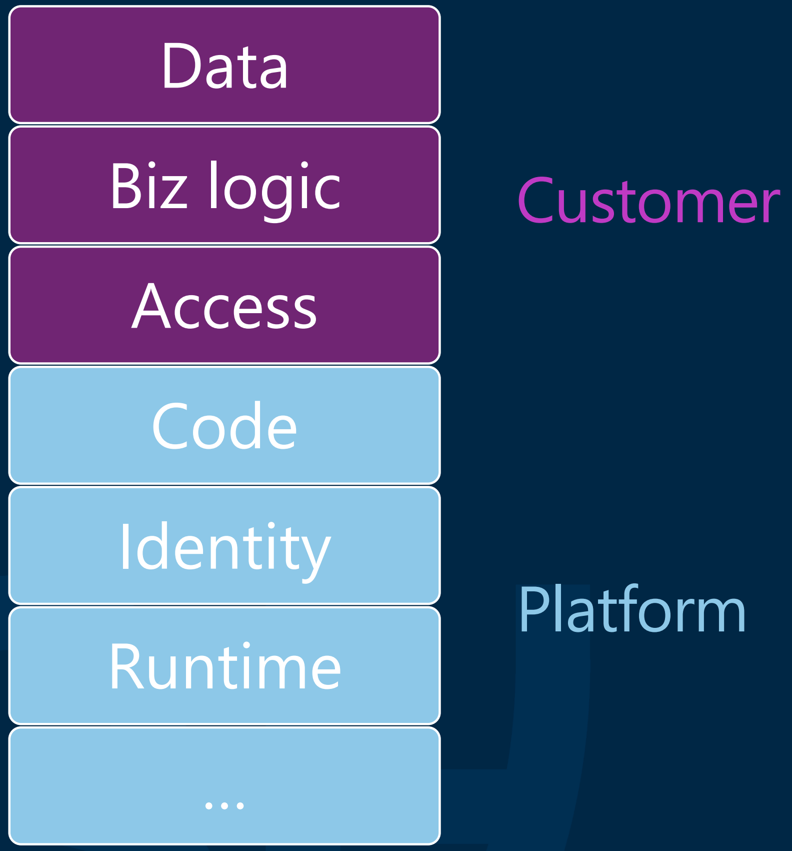
Runtime

…

Customer

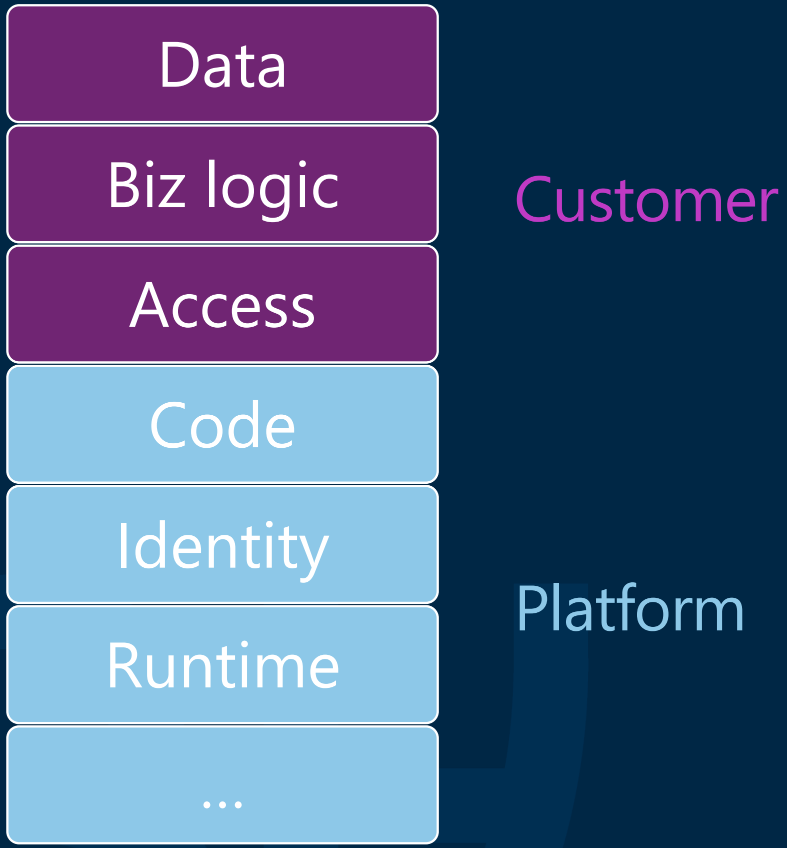
Platform

Sure, let business users build they own. What could go wrong?



- Are apps moving data outside of the corp boundary?
- Are users over-sharing data?
- Are we allowing external access?
- Are we properly handling secrets and sensitive data?
- Do apps have business logic vulns?
- …

Sure, let business users build they own. What could go wrong?



Data

Biz logic

Access

Customer

Code

Identity

Runtime

…

Platform

- Are apps moving data outside of the corp boundary?
- Are users over-sharing data?
- Are we allowing external access?
- Are we properly handling secrets and sensitive data?
- Do apps have business logic vulns?
- …

Who owns AppSec for apps built by business users?

Shared Responsibility Model for LC/NC

		Role Accountability			
Domain	**Responsibility**	**LC/NC Dev.**	**LC/NC Admin**	**Security Team**	**LC/NC Platform**
Access Control	Identity, Access Control	√			
Access Control	Sharing, Ownership	√			
Business Logic	Connectivity, Integration, Plugins, & Agents	√			
Business Logic	Data flows, Control Flows, Integration	√			
Data Management	Data and Secret Handling	√			●
Data Management	Data Governance	√			
Data Management	Encryption	√			●
Governance	Application Security / Risk Assessment	○	●	√	
Governance	Developer Lifecycle Governance	○	●	√	
Governance	Developer Training and accountability	○	●	√	
LC/NC Platform	Hygiene Management		●		√
LC/NC Platform	LC/NC Platform configuration, policies, settings, security controls		●	●	√
Platform(s)	Harden other services besides LC/NC Platform		<Other Admins>	○	

√	Directly accountable/responsible
●	Responsible (in partnership)
○	Consulted/Informed, may take some action

What are the priorities?

✓Leverage industry-standard security risk categorization

✓Prioritize what we want to fix first

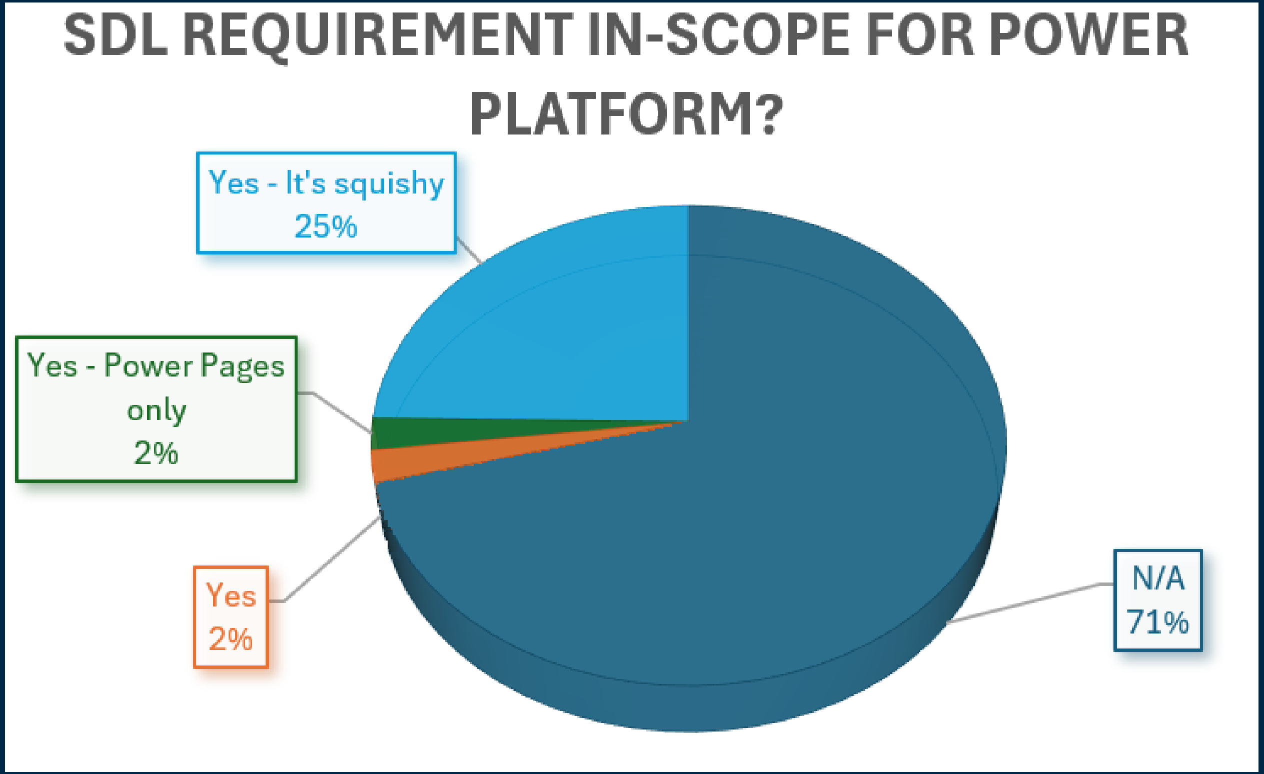
✓Shared Responsibility Model

- De-facto SDL enforcement

Remember this gap analysis?

- Successful SDL uses automation for the more technical requirements

- Our processes give us “de-facto” SDL across our corporate network
  - Sorry, no Threat Models. ☹



@mbrg0
@donwillits66
#BLUEHAT

What did we learn from this?

✓Leverage industry-standard security risk categorization

✓Prioritize what we want to fix first

✓Shared Responsibility Model

✓De-facto SDL enforcement

Conclusion

Resources

- Product docs
- SDL: microsoft.com/en-us/securityengineering/sdl
- Top 10 for LC/NC: owasp.org/lowcodenocode
- Top 10 for LLM: llm.owasp.org
- LCNC Shared Responsibility Model Whitepaper (forthcoming)

Full writeup labs.zenity.io/p/bluehat24

In conclusion…

Low-Code/No-Code is a powerful and prolific tool in an Enterprise

- But the shared responsibility model is not necessarily recognized

You CAN build a successful program at scale

- We happened to use Zenity, but that's not a prerequisite

You can get both Productivity and improved Security

- Greater parity with the SDL is possible

Microsoft

Thank you

@mbrg0
@donwillits66
#BLUEHAT