



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

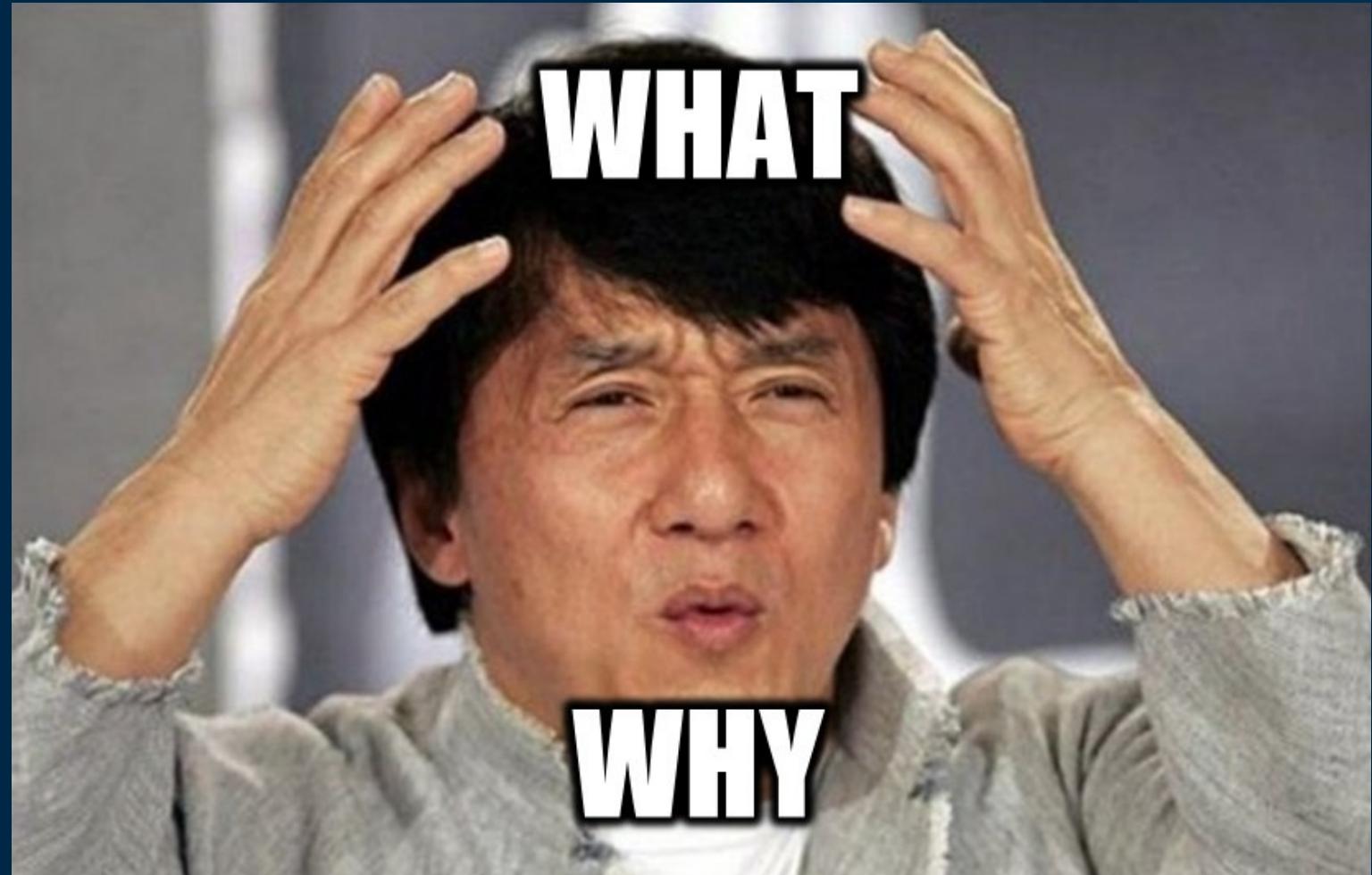


55K devs
90K copilots
500K apps
1.1M automations



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

our 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 Excel 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... Beginner

@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?](#)

[Get started](#)

For issues or concerns contact IT Global Helpdesk globalhd@microsoft.com
[Microsoft Data Privacy Notice](#) [Identity Terms of Use](#) [Feedback](#)
© 2021 Microsoft

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



servicenow™



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”



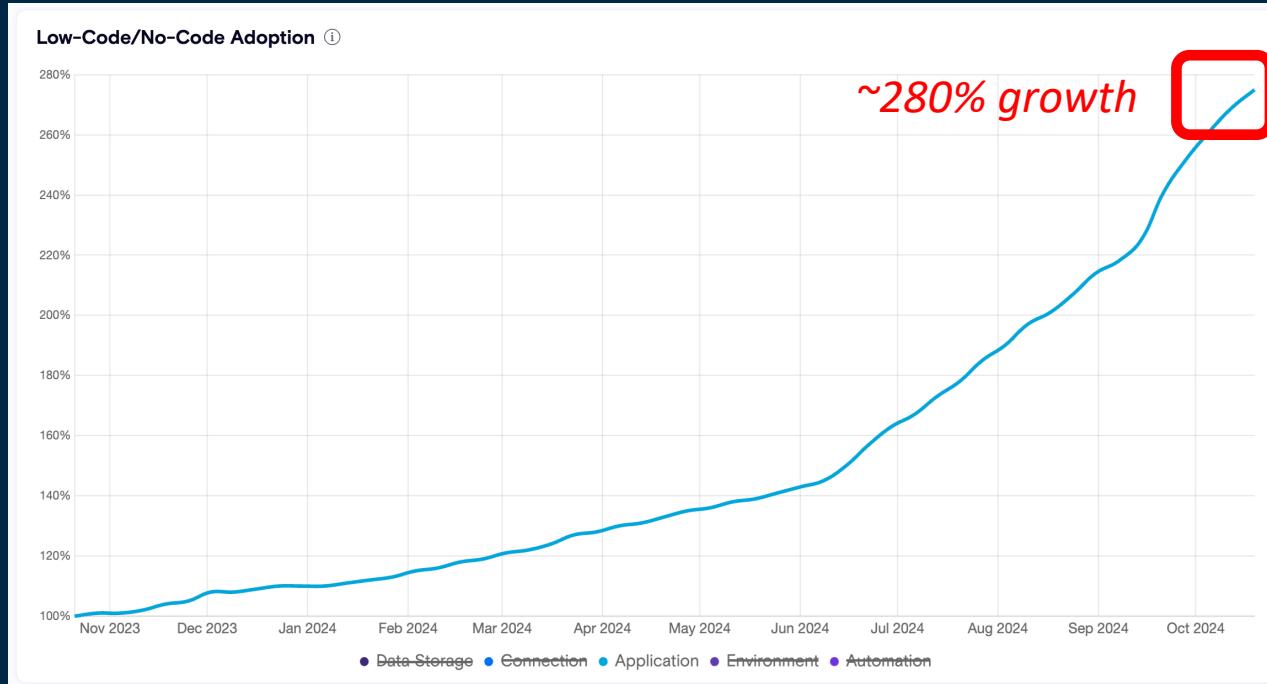
LCNC → “500M apps by 2023”

Enters GenAI.



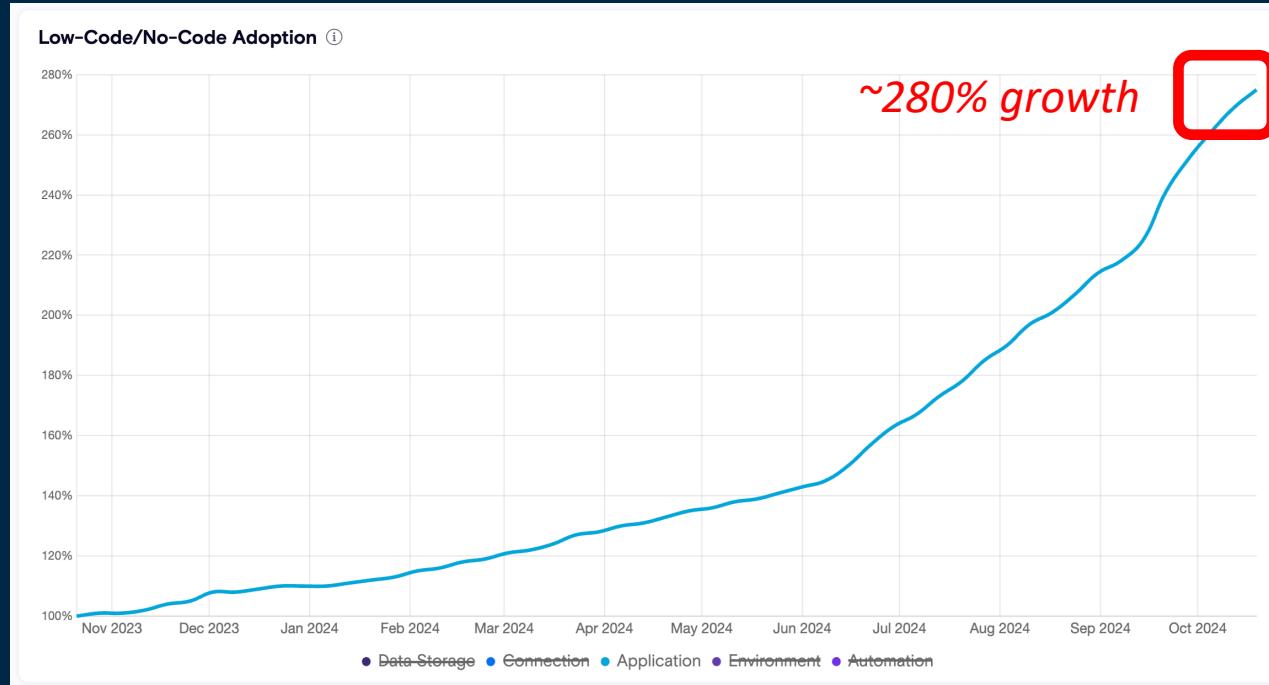
LCNC → “500M apps by 2023”

Enters GenAI.

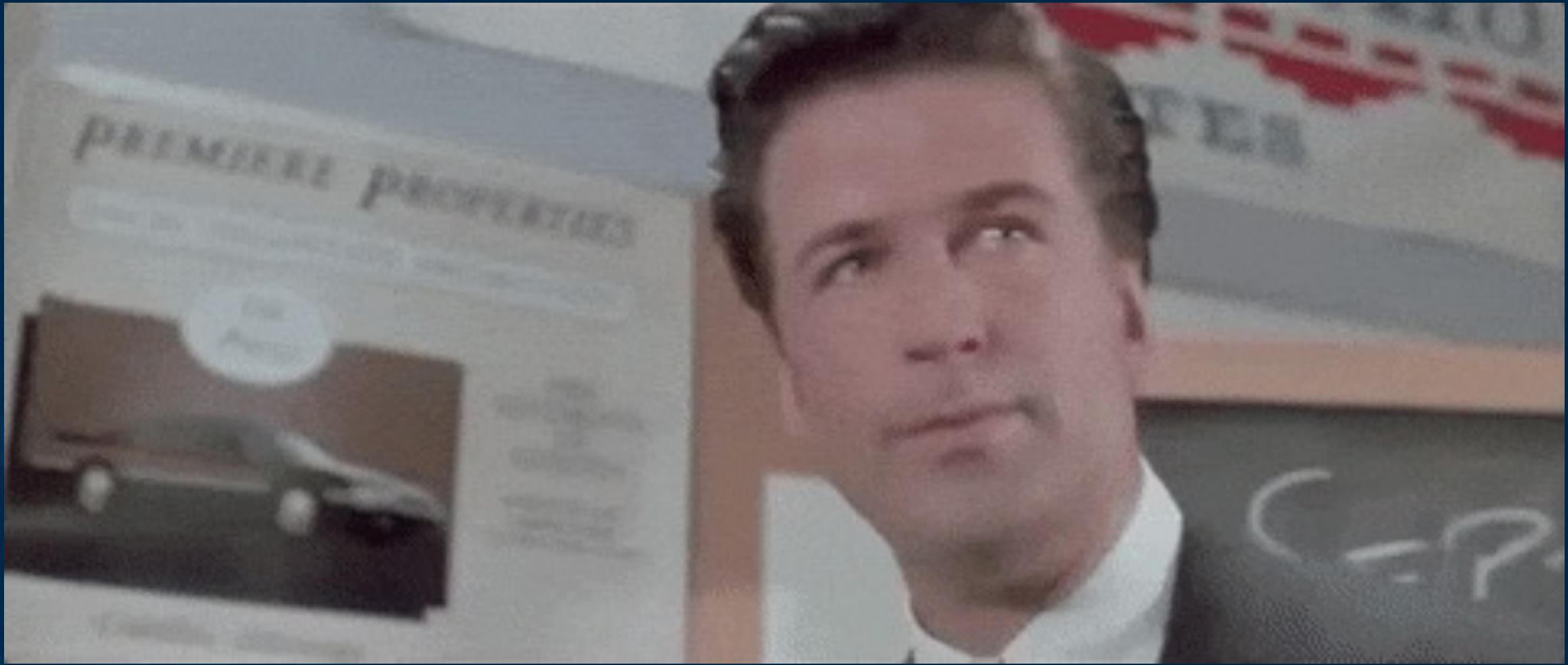


LCNC → “500M apps by 2023”

Enters GenAI.



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



@mbrg0
@donwillits66
#BLUEHAT

WHY are these important?

Story #1 – Community website

[← Back](#)



[Help & Training](#)

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.

@mbrg0
@donwillits66
#BLUEHAT

PwnRobotsSpareParts

About Us Products Partners

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.

[Success Stories](#)

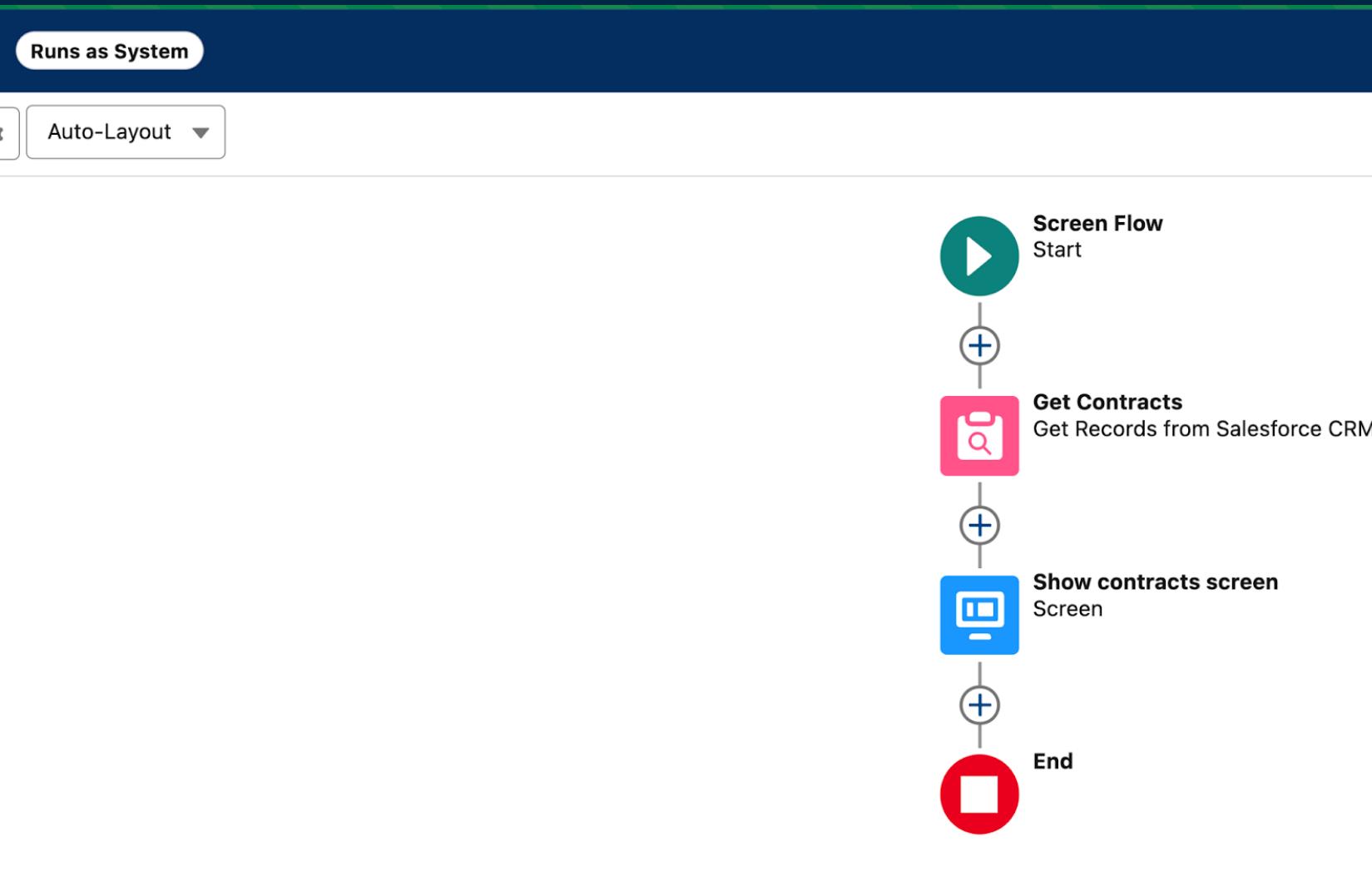
© 2024 PwnRobotsSpareParts. All rights reserved.

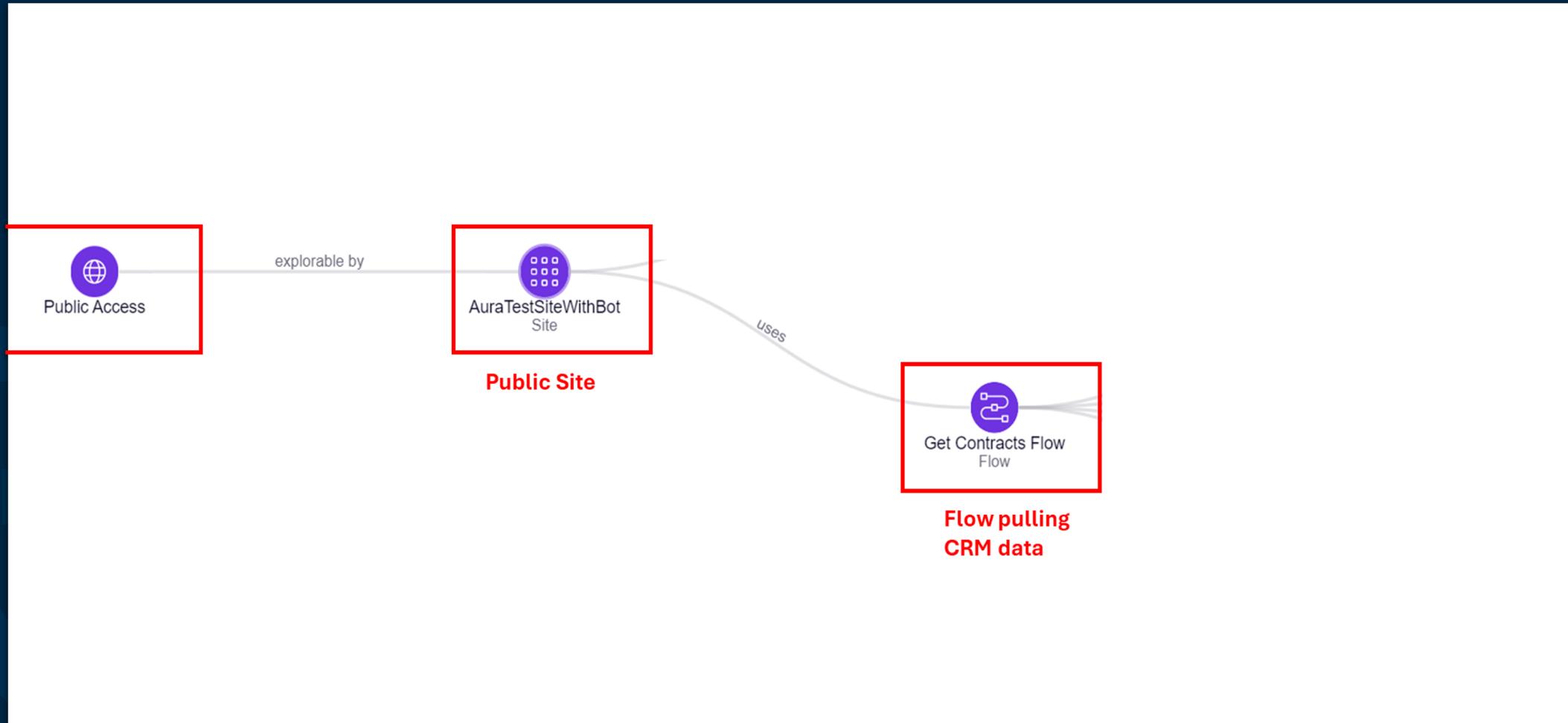
@mbrg0
@donwillits66
#BLUEHAT

The screenshot shows the Site Settings General page. On the left, a sidebar lists various settings categories: General (selected), Theme, Languages, Navigation, Mobile Publisher, SEO, CMS Connect, Advanced, Security & Privacy, Developer, Updates, and Change History. The main content area is titled "General" and describes viewing and editing site properties. It includes sections for "Site Details" (Template: Build Your Own), "Public Access" (checkbox checked, "Guest users can see and interact with the site without logging in"), "Site Title" (set to "AuraTestSiteWithBot"), "Published Status" (published at "https://zenity.my.site.com/AuraTestSiteWithBot/s"), and "Guest User Profile" (link to "AuraTestSiteWithBot Profile").



@mbrg0
@donwillits66
#BLUEHAT





Flow Builder Get Contracts Flow - V4 Runs as System

Edit version properties

* Flow Label: Get Contracts Flow * Flow API Name: Get_Contracts_Flow

Description:

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}

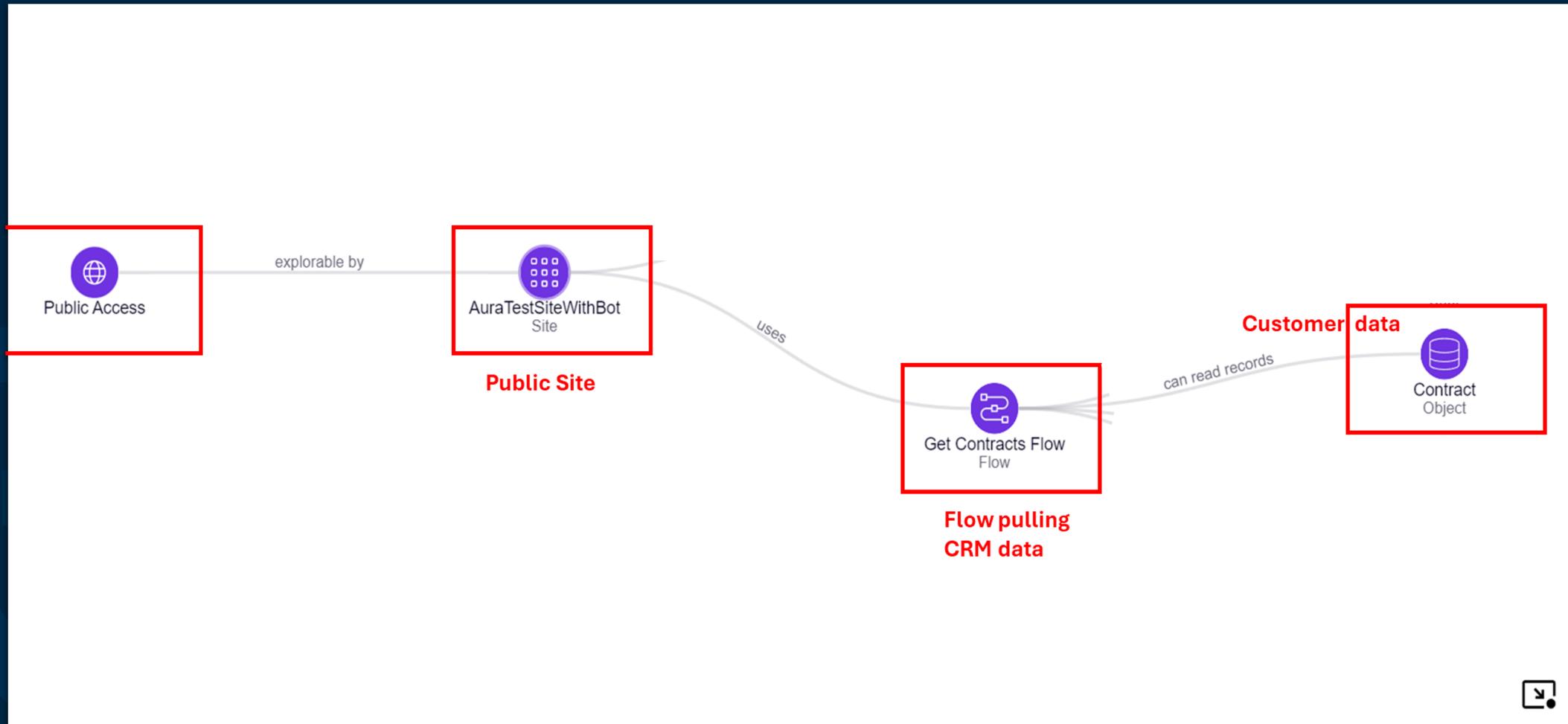
Last Modified: 28.2.2024, 15:01 by Ofer Chacham

Hide Advanced

Cancel Done

The "How to Run the Flow" section is highlighted with a red box.

@mbrg0
@donwillits66
#BLUEHAT



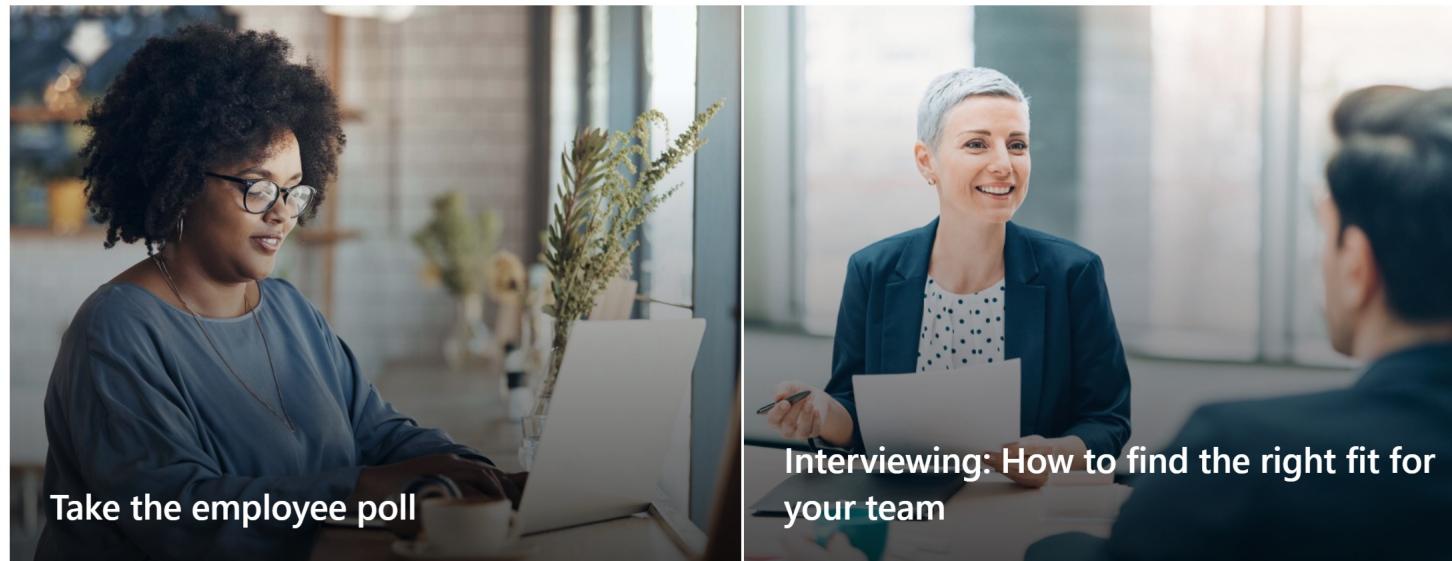
Get Contracts Flow

3 of 3 items • 0 items selected

 Search this list...

<input type="checkbox"/> Contract Number	Description	<input type="checkbox"/> PresentInSite
<p>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."</p>		
<input type="checkbox"/> 00000108		SensitiveCustomer
	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.	
<input type="checkbox"/> 00000106	Shipping Contract - Global Logistics	SuccessStory
<input type="checkbox"/> 00000105	Service Agreement - Acme Corp	SuccessStory

Story #2 – AskHR Copilot



Take the employee poll

Interviewing: How to find the right fit for your team



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

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

[Skip to configure](#)[Create](#)

...

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

What should I say?

Type your message



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

[Edit language](#)

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

AskHR Copilot



@mbrg0
@donwillits66
#BLUEHAT

Security - Ask HR Copilot | Microsoft Copilot Studio

copilotstudio.microsoft.com/environments/9f39c593-708b-e141-8f24-d89573503212/bots/badea132-d994-ee11-be37-6045bddba096/main

Copilot Studio | Ask HR Copilot

Test copilot

Track between topics

Chat

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?

Type your message

Security

Set up additional security measures for the copilot.

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](#)

Save Close

11:48
07/12/2023

- 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

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

...

×

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

Type your message ➤

Security

Set up additional security measures for

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](#)

[Save](#) [Close](#)

AskHR Copilot



@mbrg0
@donwillits66
#BLUEHAT

**Copilots**

▼ Custom copilots



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

**knowl**

ces to info

[+ Add k](#)**Dataverse (preview)**

Customize and deploy structured data tables

The screenshot shows the Microsoft Fabric AI Skills interface. On the left, a sidebar menu includes Home, Create, Browse, OneLake data hub, Monitoring hub, Workspaces, and a workspace named Contoso Outdoors Sales. The main area displays a 'New' section with a message about the current workspace: 'Contoso Outdoors Sales'. Below this are 'Recommended' sections for 'My workspace', 'Notebook 6', and 'Copilot Demo', each with an 'Open' button. A 'Quick access' section at the bottom shows a recent workspace named 'Contoso Outdoors Sales' and a 'Filter by keyword' search bar. A central modal window titled 'Create AI skill' is open, prompting for a 'Name' which is currently 'LoyaltyMemberSupportInsights'. It also features 'Create' and 'Cancel' buttons.

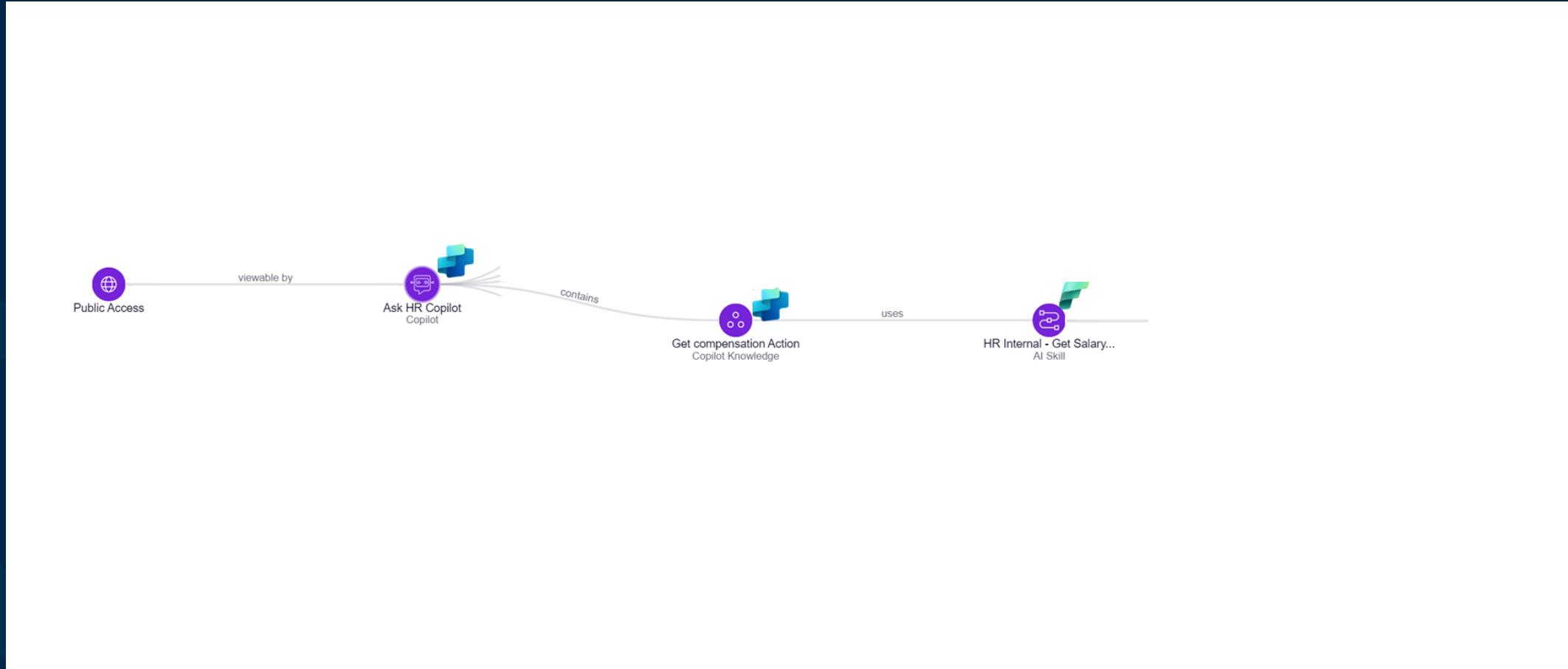
Publish AI skill

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

 Publish

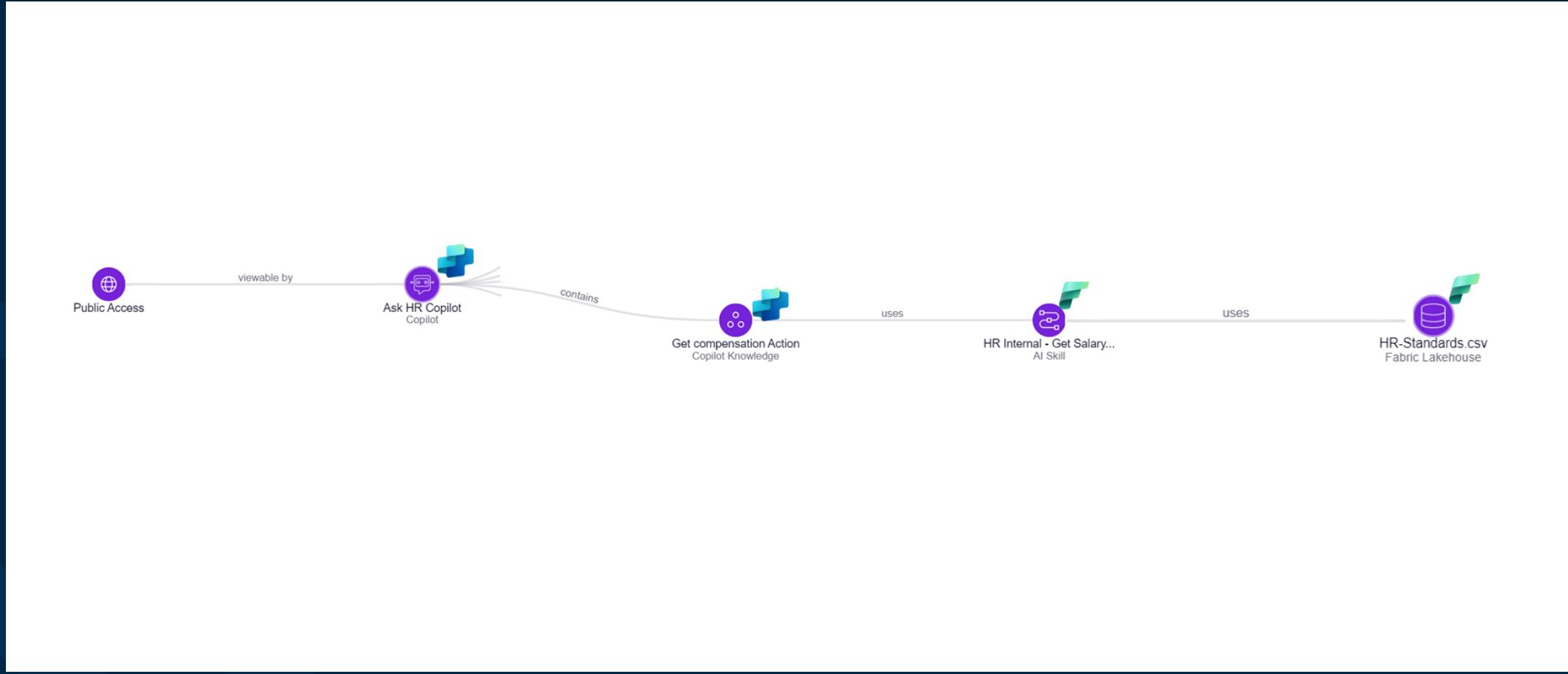
Cancel

AskHR Copilot



@mbrg0
@donwillits66
#BLUEHAT

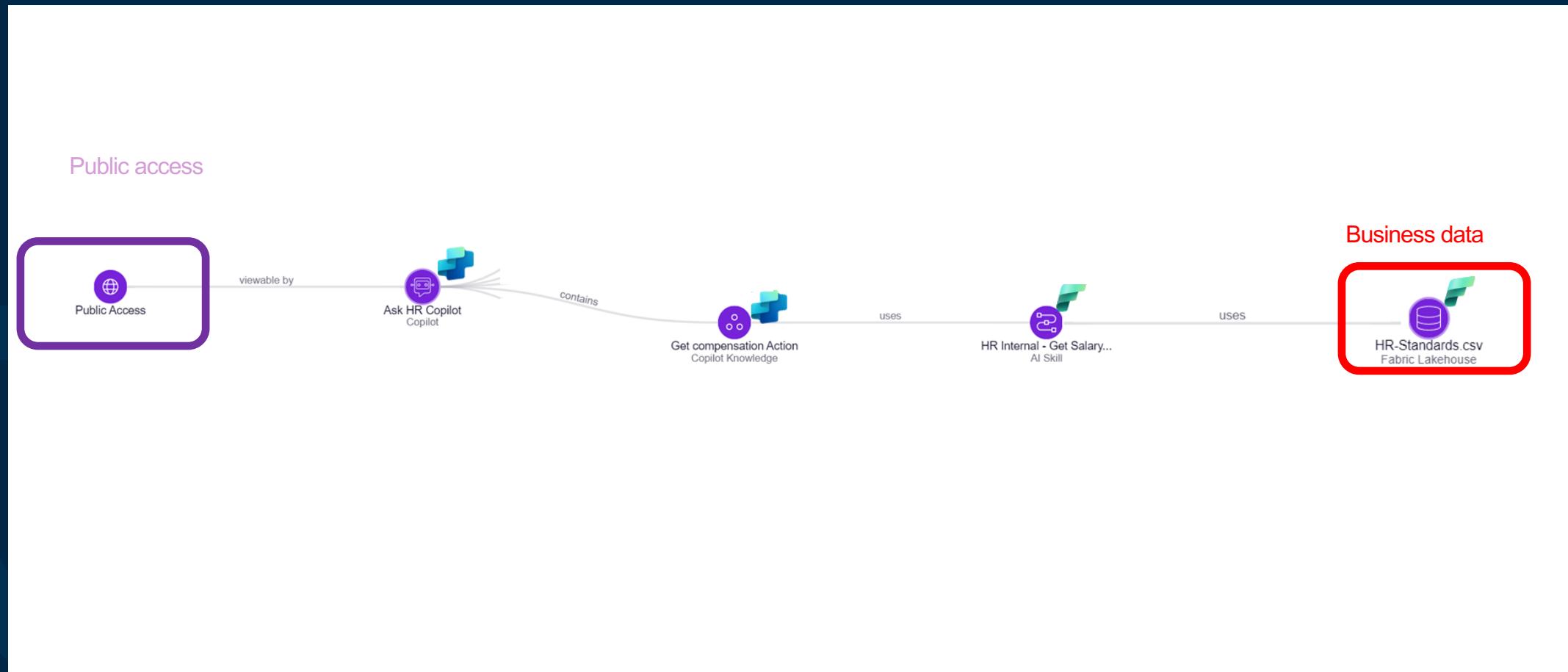
AskHR Copilot



@mbrg0
@donwillits66
#BLUEHAT

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
```



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

Power Automate

Search

Environments
Zenity Stage (default)

?

KS

Sync Outlook to Gmail

Undo Redo Comments Save Flow checker Test

Home Approvals My flows Create Templates Connectors Data Monitor AI Builder Process mining

When a new email arrives (V3)

Send email (V2)

To: Kris Smith

Subject: Subject

Body: Body

Attachments: Attachments

A red square icon with a white figure sitting at a desk is located in the bottom right corner.

```
graph TD; A[When a new email arrives (V3)] --> B[Send email (V2)]; B --> C[Body]; C --> D[Attachments]
```

Productivity sync – findings



@mbrg0
@donwillits66
#BLUEHAT

Productivity sync – findings

- Business data to personal account (Data Leakage)



← Back | ↎ | √ | 🗑️ | √ | + Insert √ Open Sans √ 15 Semibold √ ...

Editing | |

OnSelect = *fx* SyncOutlookhistorytoGmail.Run(*NumberInput*,*EmailInput*)

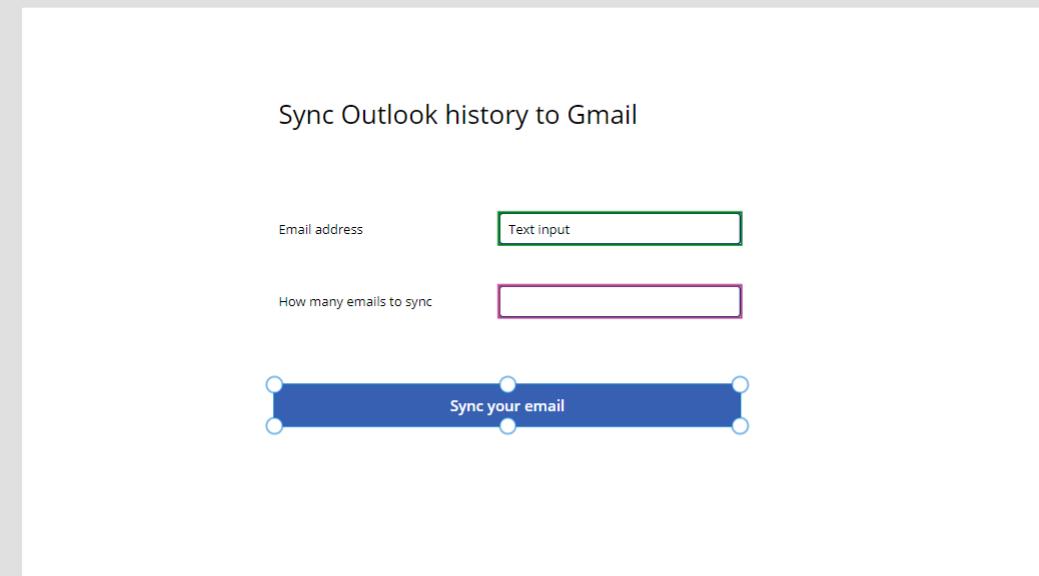
Power Automate

 Search

+ Add flow

✓ In your app

 Sync Outlook history to Gmail
SyncOutlookhistorytoGmail



BUTTON ?

Button1

Properties Advanced Ideas

Search for a property ...

ACTION

OnSelect

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

DATA

Text

"Sync your email"





Sync Outlook history to Gmail

Email address

Text input

How many emails to sync

Text input

Sync your email



Power Automate

Search

Environments
Zenity Stage (default)

?

KS

Sync Outlook history to Gmail

Undo Redo Comments Save Flow checker Test

Home Approvals My flows Create Templates Connectors Data Monitor AI Builder Process mining Solutions Learn

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:

Font: 12pt B I U

```
graph TD; A[PowerApps (V2)] --> B[Get last X emails with attachments]; B --> C[For each email]; C --> D[Send email to myself];
```

Power Apps

Search

Edit Play Share

Apps > Set up your en

Details

Versions

Connec

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



Everyone in CloudCore



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.

Upload

Select or add a user to set their permissions



Send an email invitation to new users

Power Apps

Search

Edit Play Share

Apps > Set up your en

Details Versions Connect

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



Everyone in CloudCore
User



Kris Smith
Owner

Shared with

Sort by Name ▾

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

Upload

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.



Logic flows



Office 365 Outlook

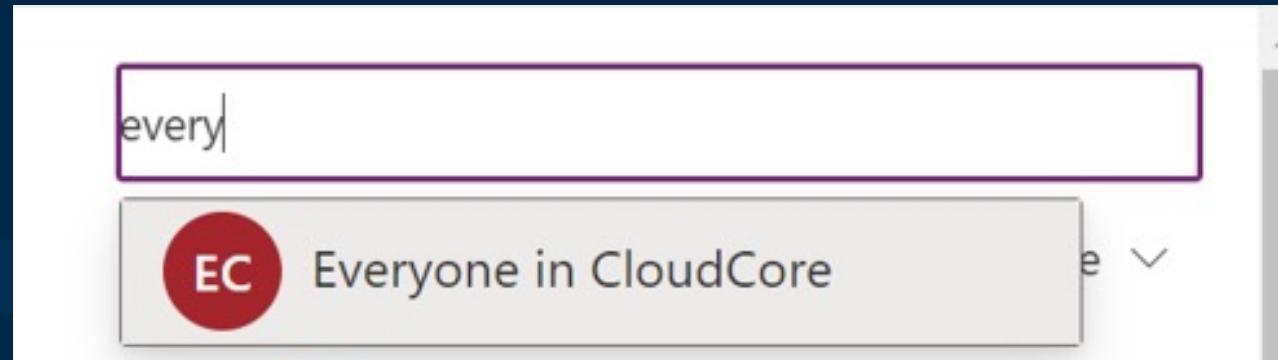


Gmail



Productivity sync – findings

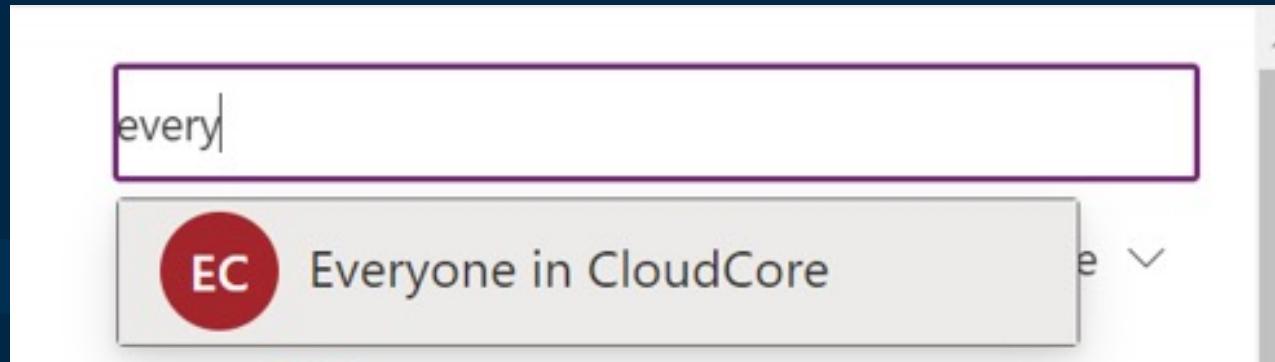
- Business data to personal account (Data Leakage)
- Share with Everyone (Authorization Misuse)



Everyone means EVERYONE,
including guests by-default

Productivity sync – findings

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



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](#)

[Switch account](#)



Gmail

maortzury@gmail.com

Signed in

[Switch account](#)

Allow

Don't Allow



Sync Outlook history to Gmail

Email address

maortzury@gmail.com

How many emails to sync

20

Sync your email



Power Automate

Search

Environments
Zenity Stage (default)

Resubmit Cancel Edit Help

Home Approvals My flows Create Templates Connectors Data Monitor AI Builder Process mining Solutions Learn

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

The screenshot shows the Microsoft Power Automate interface. On the left is a navigation bar with various options like Home, Approvals, My flows (which is selected), Create, Templates, Connectors, Data, Monitor, AI Builder, Process mining, Solutions, and Learn. The main area displays a flow titled "Sync Outlook history to Gmail" that ran at 8/8/2023 1:48:09 AM. The flow consists of three steps: 1. PowerApps (V2) which completed in 0s. 2. Get last X emails with attachments which completed in 2s. 3. For each email which completed in 32s. Each step has a status icon and a green checkmark.

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

 Resubmit

 Cancel

 Edit

 Home

⌚ Approvals

My flows

+ Create

Templates

Connectors

>Data

Monitor

 AI Builder

 Process mining

Solutions

 Learn

 For each email

< Previous

5s

INPUTS

Show raw inputs >

To

imkrissmith@gmail.com

Subject

Admin Admin1 has shared the Weekly Timesheet app with you

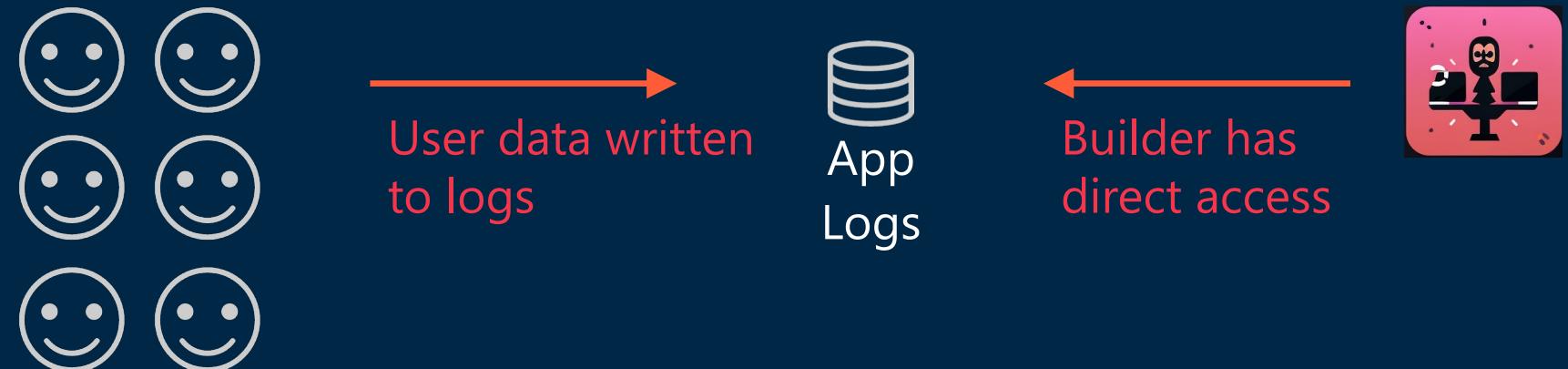
Page
3

```
<p><html lang="en" style="min-height:100%; background:#ffffff"><head>
<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)



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](#)

[Switch account](#)



Gmail

maortzury@gmail.com

Signed in

[Switch account](#)

Allow

Don't Allow



```
C:\powerpwn-blackhat>powerpwn phishing install-app --tenant "fc993b0f-345b-4d01-9f67-9ac4a140dd43" -e "Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43" --input "C:\Users\User\Downloads\Shoutout_20230729151109.zip" -n "Shoutouts"
```



```
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

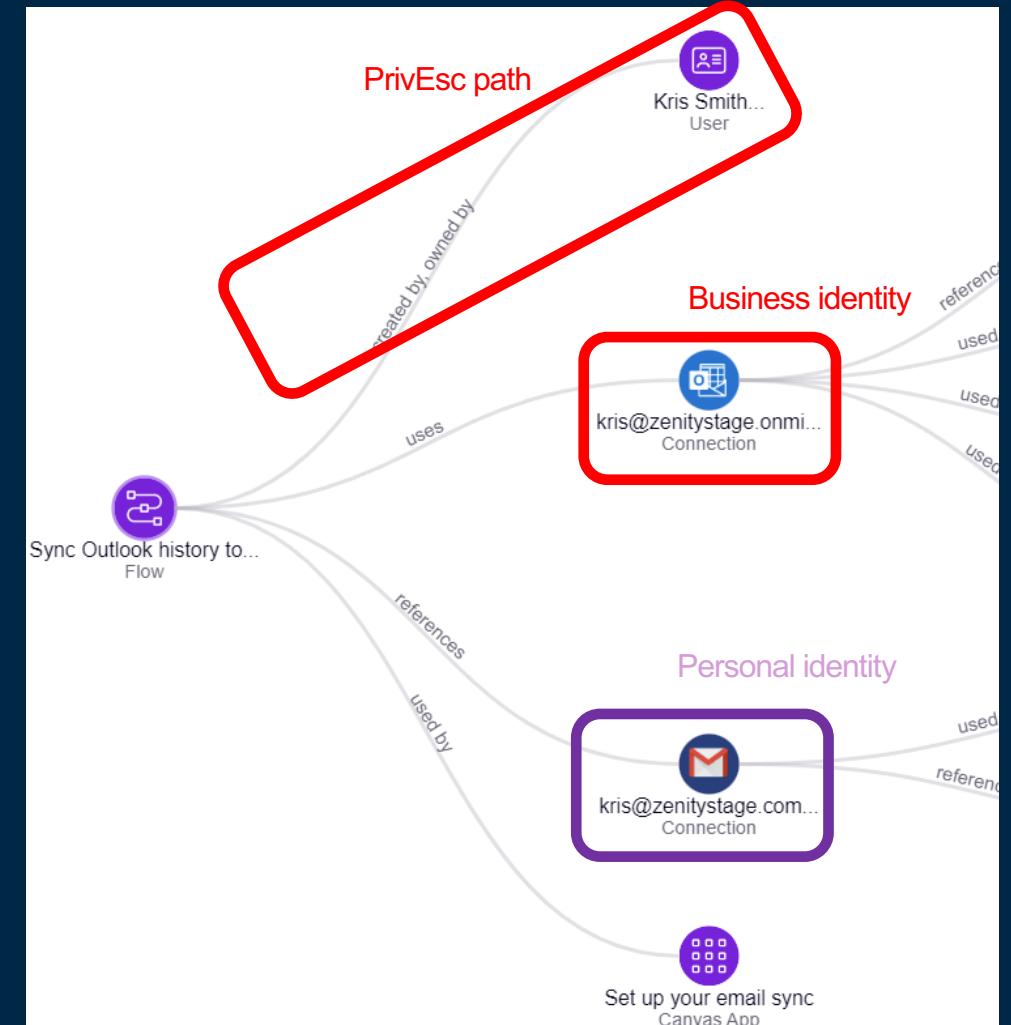


Productivity sync – findings

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

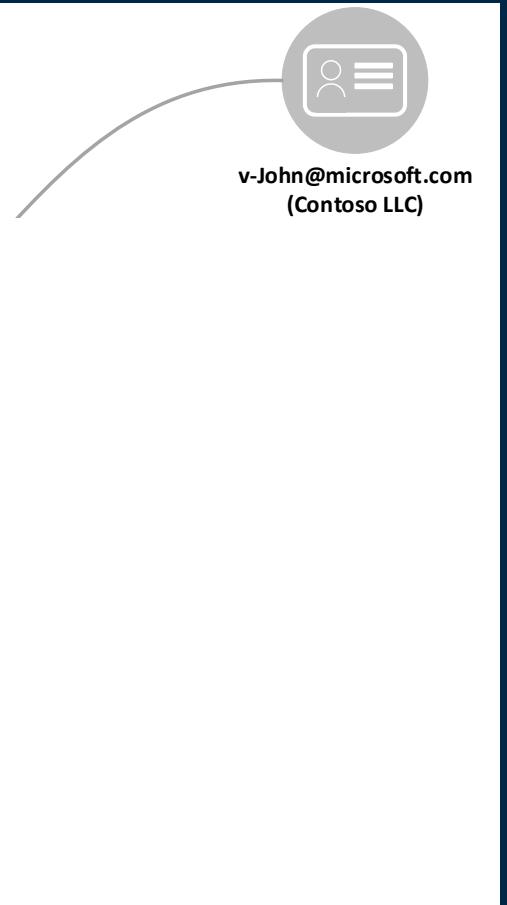
Productivity sync – findings

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

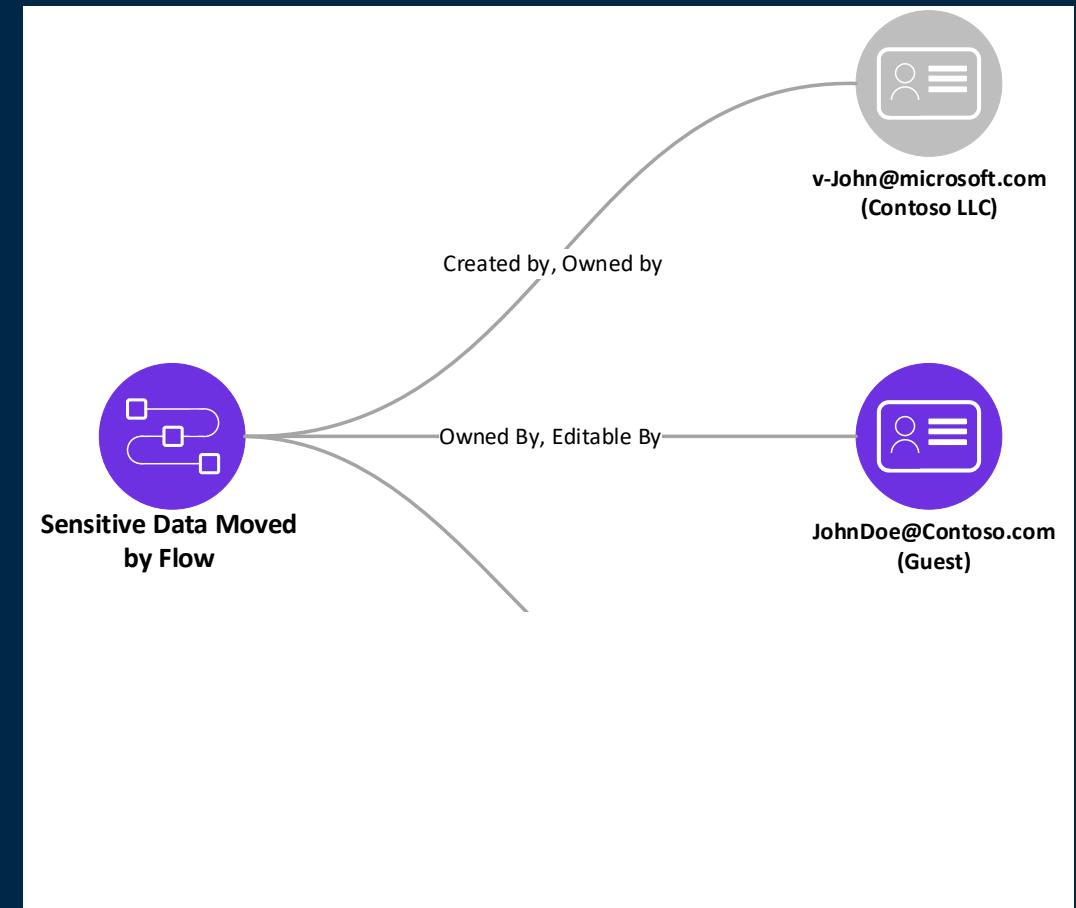


Story #4 – a persistent vendor

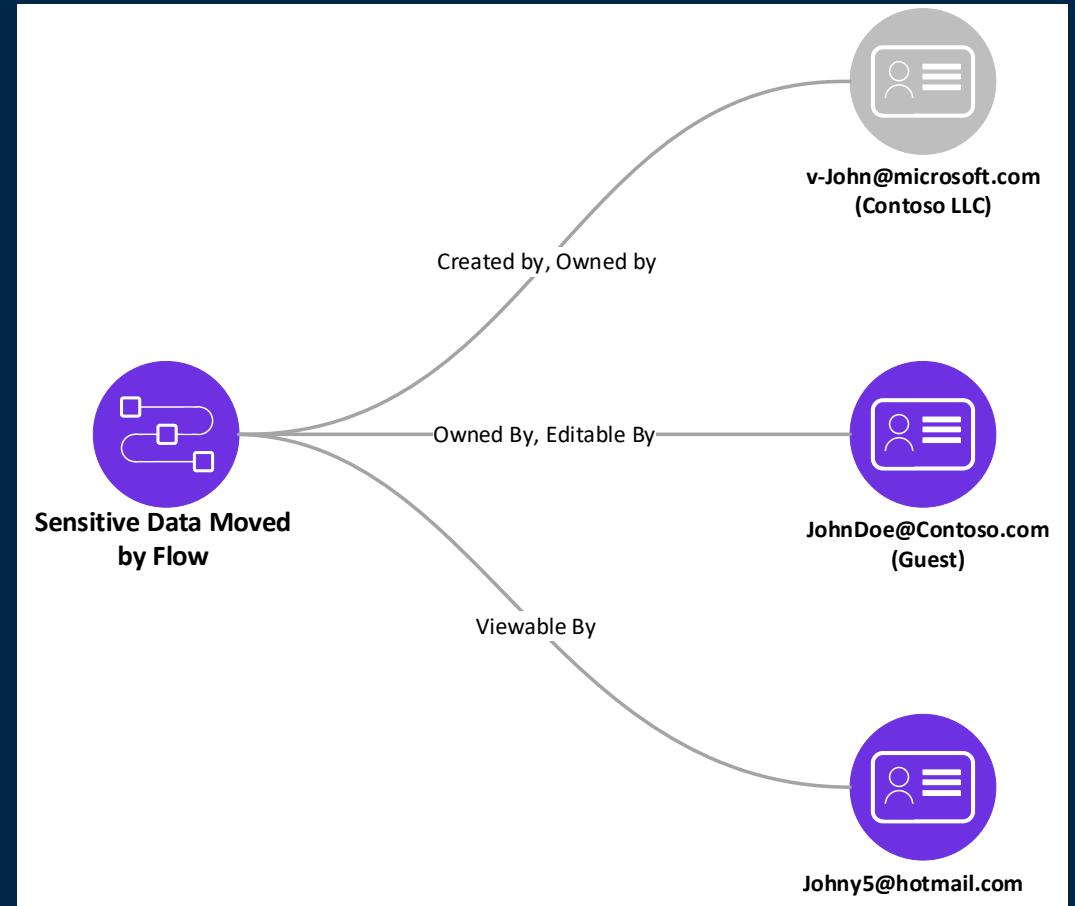
- Vendor John's contract has expired, Entra ID account disabled



- 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

(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

EntralD 130K

OneDrive 125K

Azure DevOps 124K

...

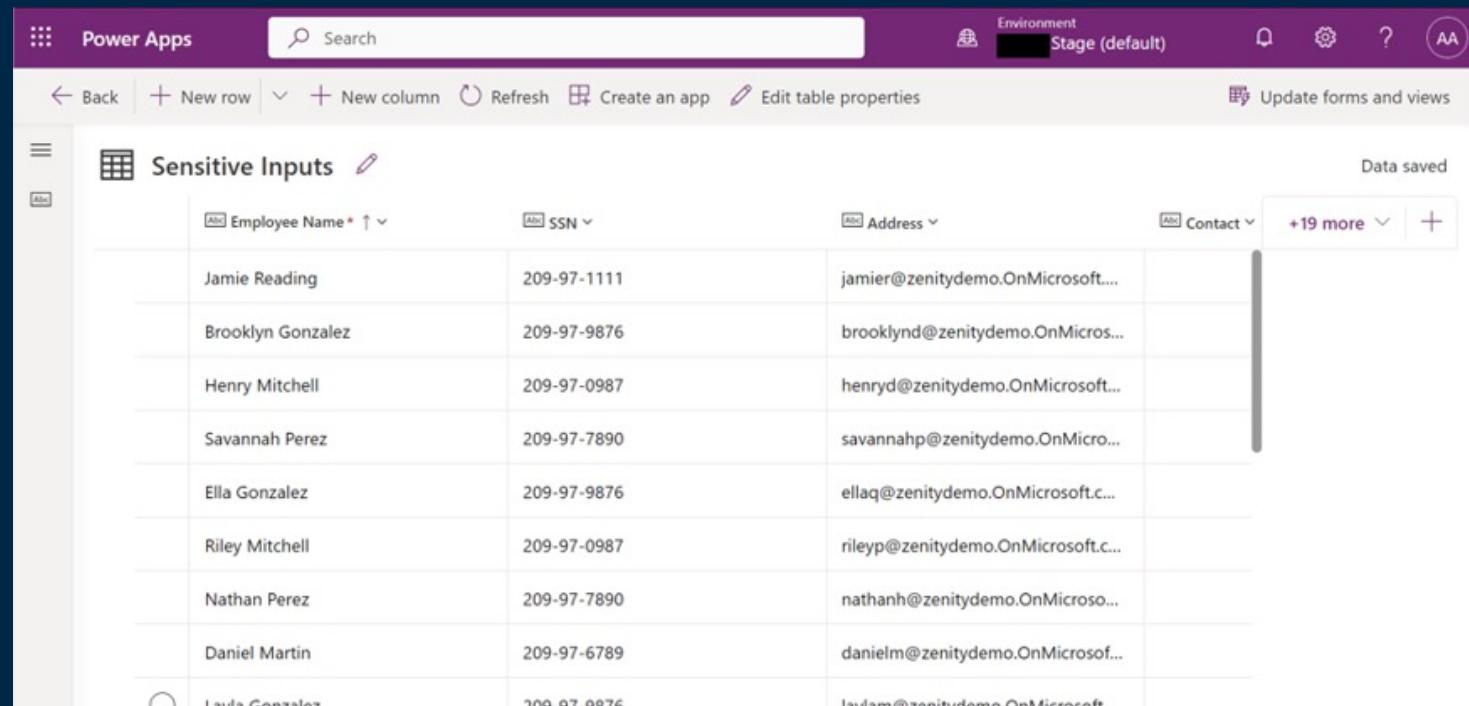
Application Security Best Practice

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?



Employee Name*	SSN	Address	Contact
Jamie Reading	209-97-1111	jamier@zenitydemo.OnMicrosoft...	
Brooklyn Gonzalez	209-97-9876	brooklynd@zenitydemo.OnMicro...	
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.OnMicroso...	
Laura Gonzalez	209-97-9876	lauram@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

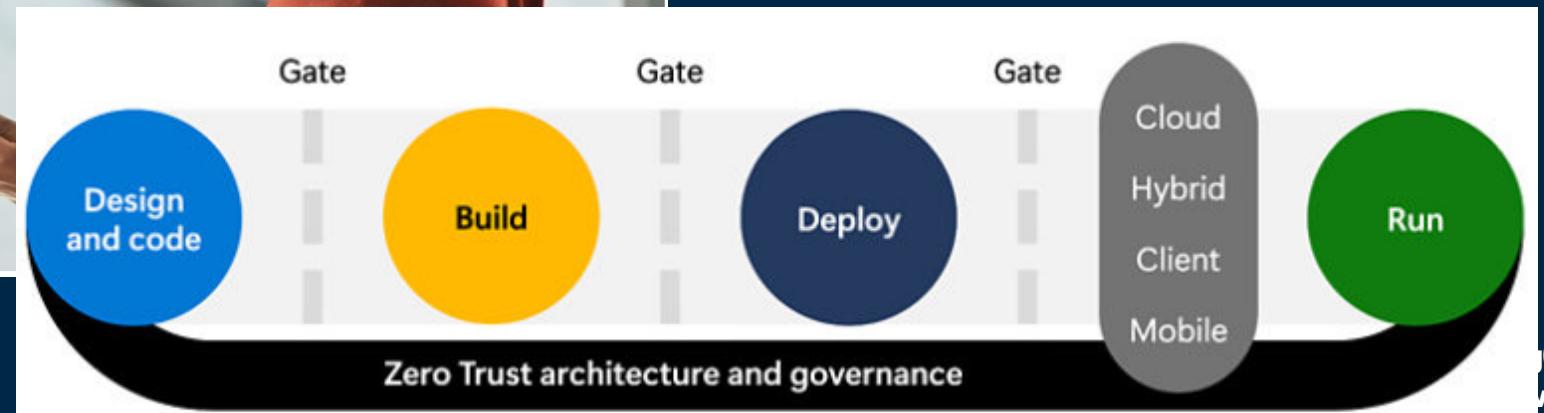
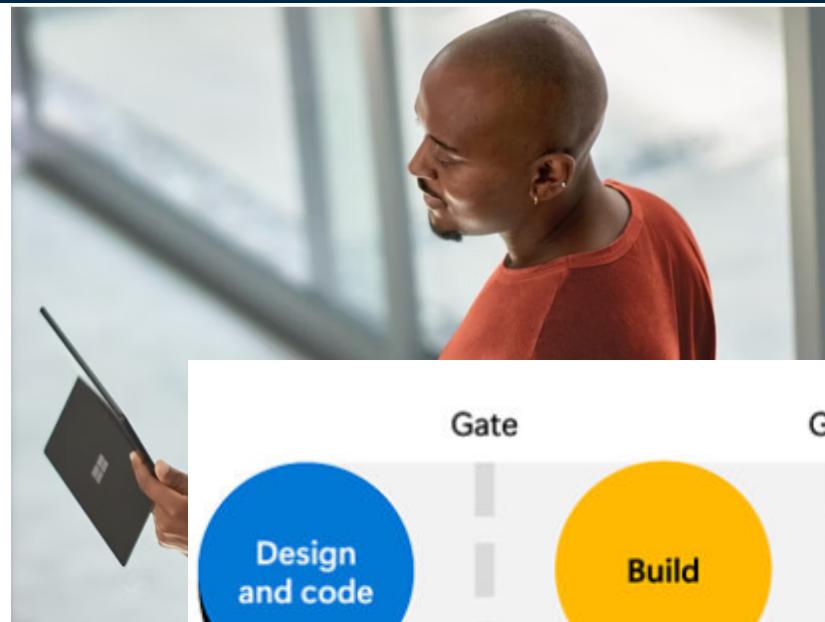
1. Focus on crown jewels
2. Get developer buy-in
3. Secure Development Lifecycle (SDL)



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.



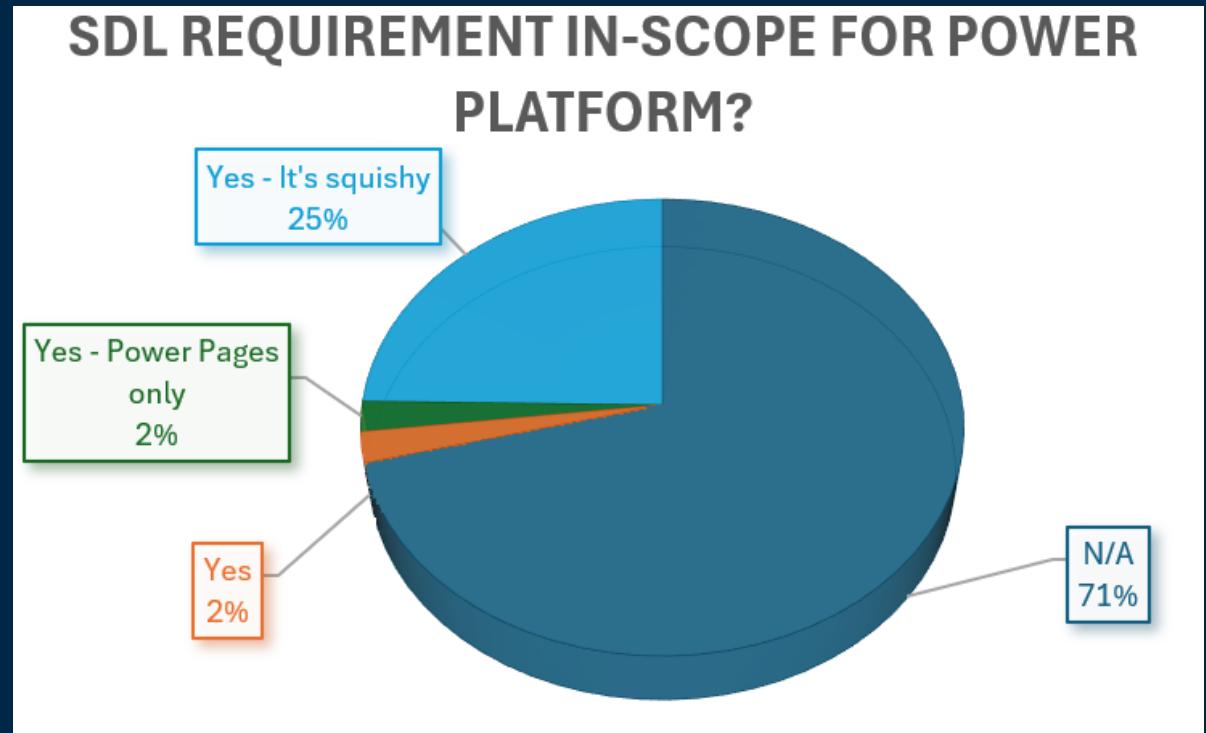
How well does SDL Guidance fit?



@mbrg0
@donwillits66
#BLUEHAT

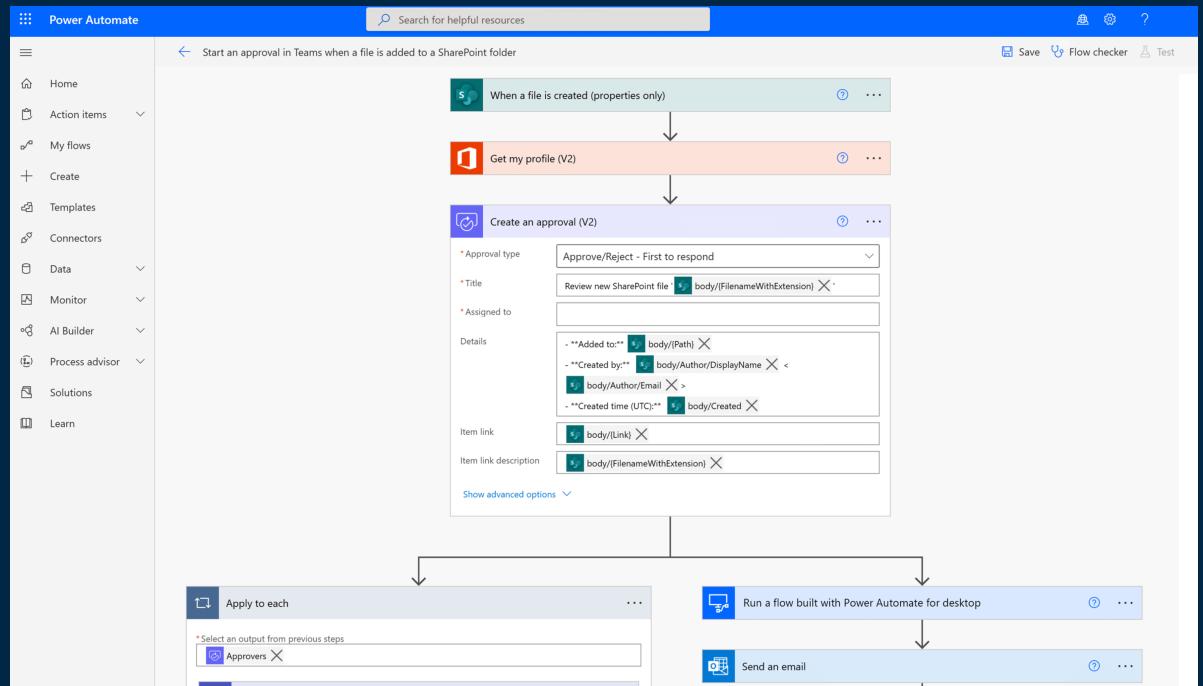
How well does SDL Guidance fit?

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



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



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 development 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 guidance.

Additionally, you should define and publish a list of approved tools and strive to use the latest version of approved tools.

2.1 Identity - Ensure users are using strong authentication and only have the level of permissions suitable for their role.

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](#)

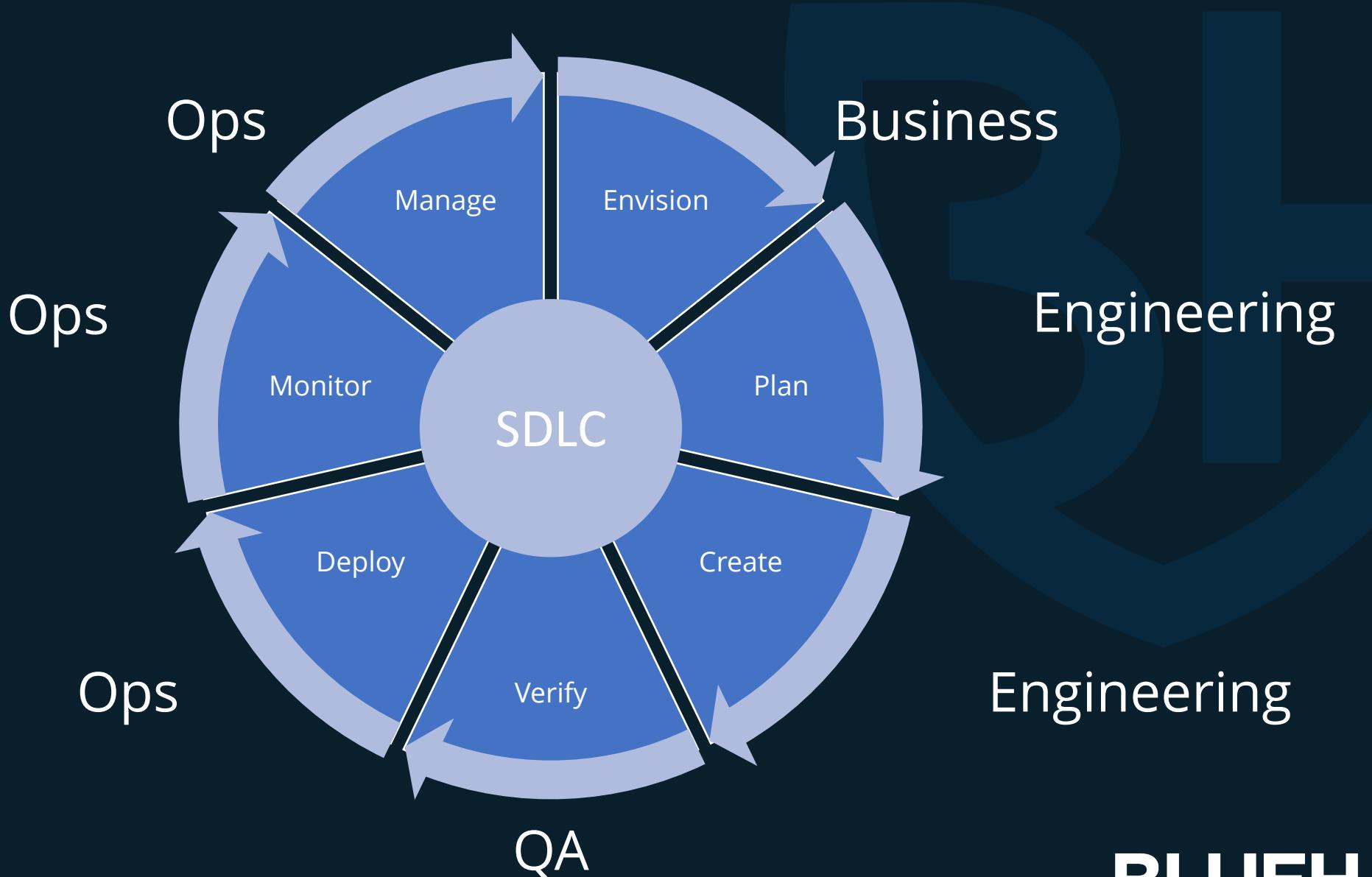
Secure Credential Storage (KeyVault / HSM)- Implement a mechanism to inventory, monitor, maintain, and audit sensitive configuration information in code or configuration files of the code. Never store passwords or other sensitive information in plain text or in unprotected locations. Production secrets 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 to easily and securely access Microsoft Graph, other Microsoft APIs, third-party web APIs, or your own APIs.

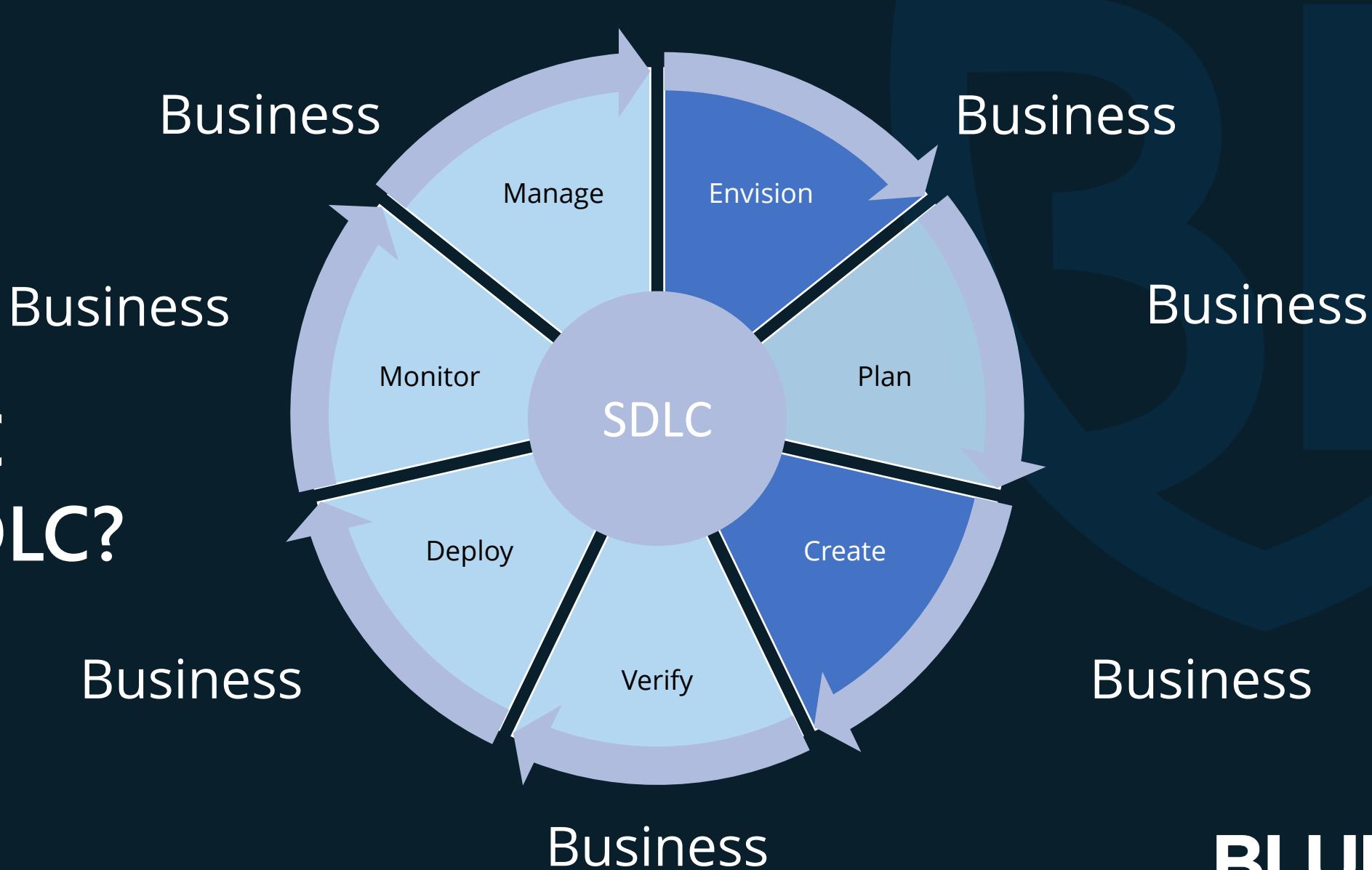
- Microsoft Learn: [Overview of the Microsoft Authentication Library \(MSAL\)](#)
- Microsoft Learn: [Public client and confidential client applications](#)
- Microsoft Learn: [Acquire and cache tokens using the Microsoft Authentication Library \(MSAL\)](#)

Pro
Code
SDLC



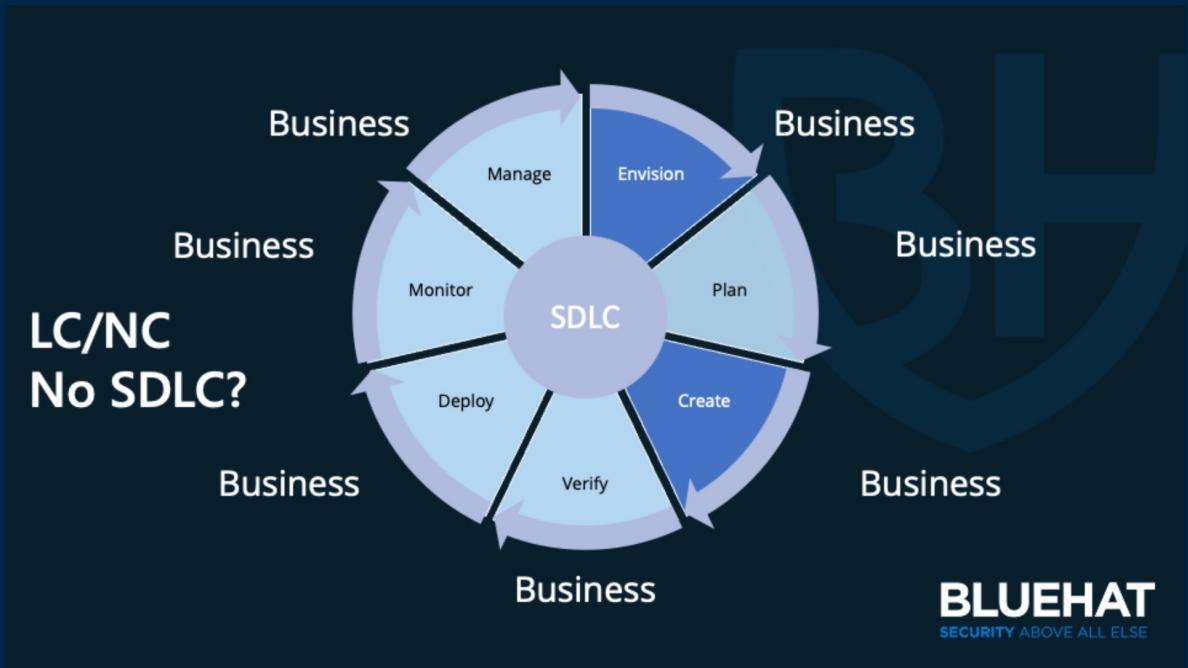
BLUEHAT
SECURITY ABOVE ALL ELSE

**LC/NC
No SDLC?**



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!)

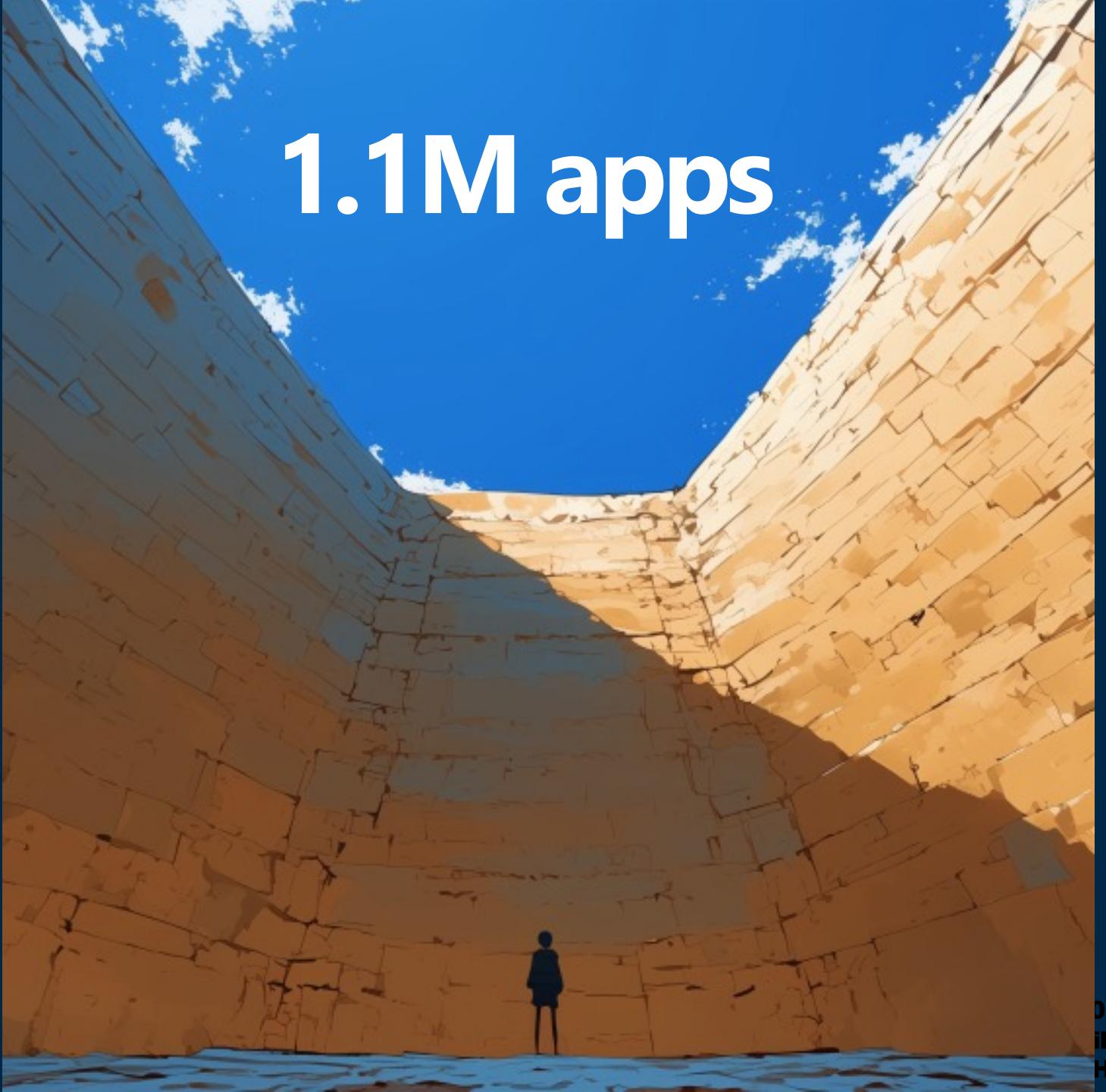


Sure, Let Business Users Build Their Own. What Could Go Wrong?

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

our 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 Excel 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... Beginner

@mbrg0
@donwillits66
#BLUEHAT

If building is easy, shouldn't
fixing vulns be easy too...?

AUTO-FIX

Sanitize inputs

Turn on logs

Remove unused
credentials

Use secure
properties

Sanitize logs

Change configs

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

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

The image consists of three vertically stacked screenshots from a Microsoft Power Platform interface. The top screenshot shows a navigation bar with a 'Share' button highlighted by a red box. The middle screenshot shows a 'Users (1) [sharepoint.com]' dialog box with a user listed, also with a red box highlighting the 'X' button next to the user name. The bottom screenshot shows the same dialog box after the user has been removed, with the user list now empty.

- 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”



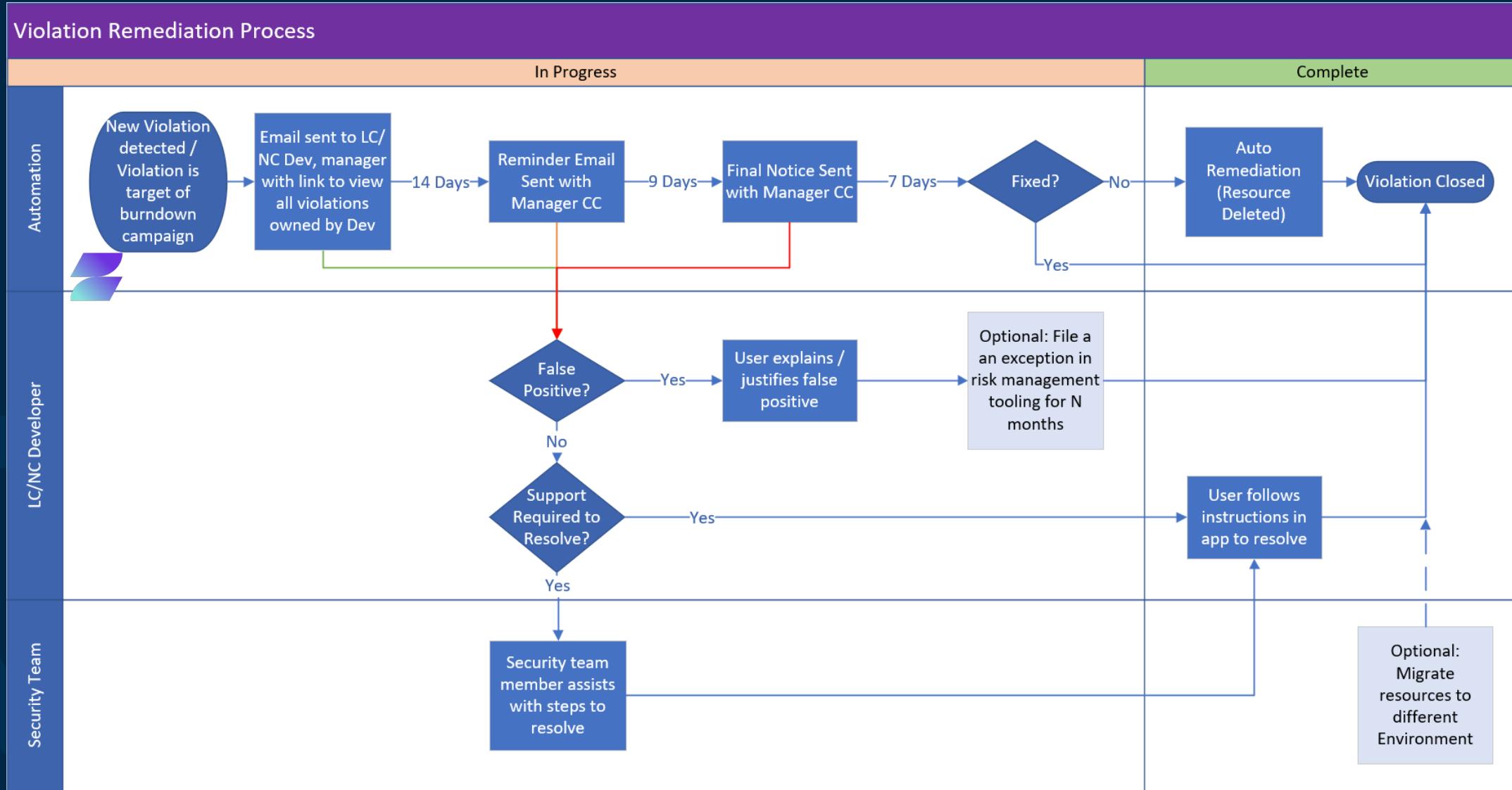
Minimum Viable Product

- 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



Self Service – SharePoint List of Instructions

SharePoint

Information Protection - Power Platform DLP Admins

+ Add new item Exit grid view Undo Share Export Forms Automate Integrate ... Manage access

ZenithBurndownRemediationSteps

All Items* By Rule InstructionApp + Add view

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 authentication.
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. If you are using a connection from a different environment, update the connection settings to use the new environment.
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".

Add new item

Self Service – Step-by-Step Instructions

SharePoint

Information Protection - Power Platform DLP Admins

Home + Add new item Edit in grid view Undo Share Export Forms Automate Integrate ... Manage access

ZenityBurndownRemediationSteps

By Rule All Items InstructionApp + Add view

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".

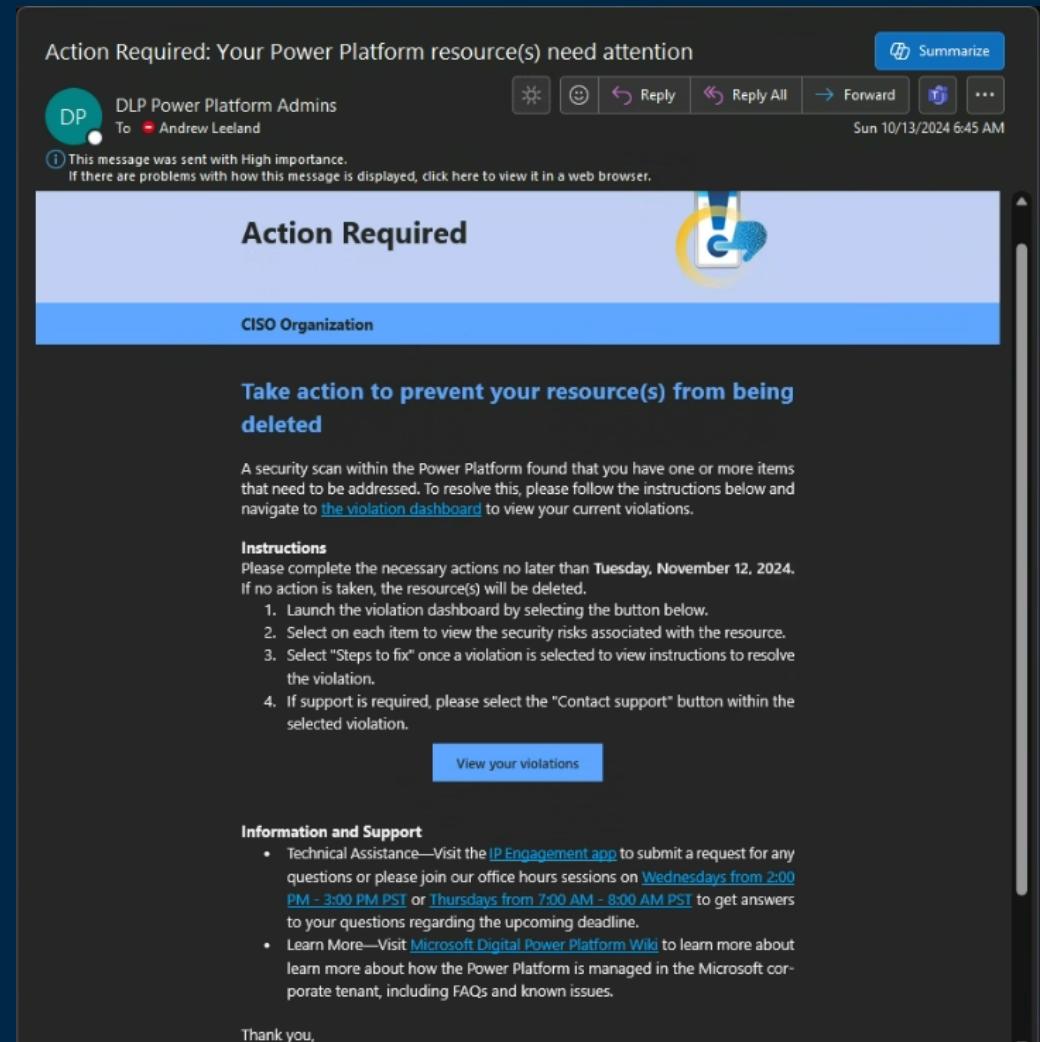
ZN_P00095

4 Enable the "Secure Outputs" and "Secure Inputs" options and then select "Done." Save the Flow to retain changes.

Return to classic SharePoint

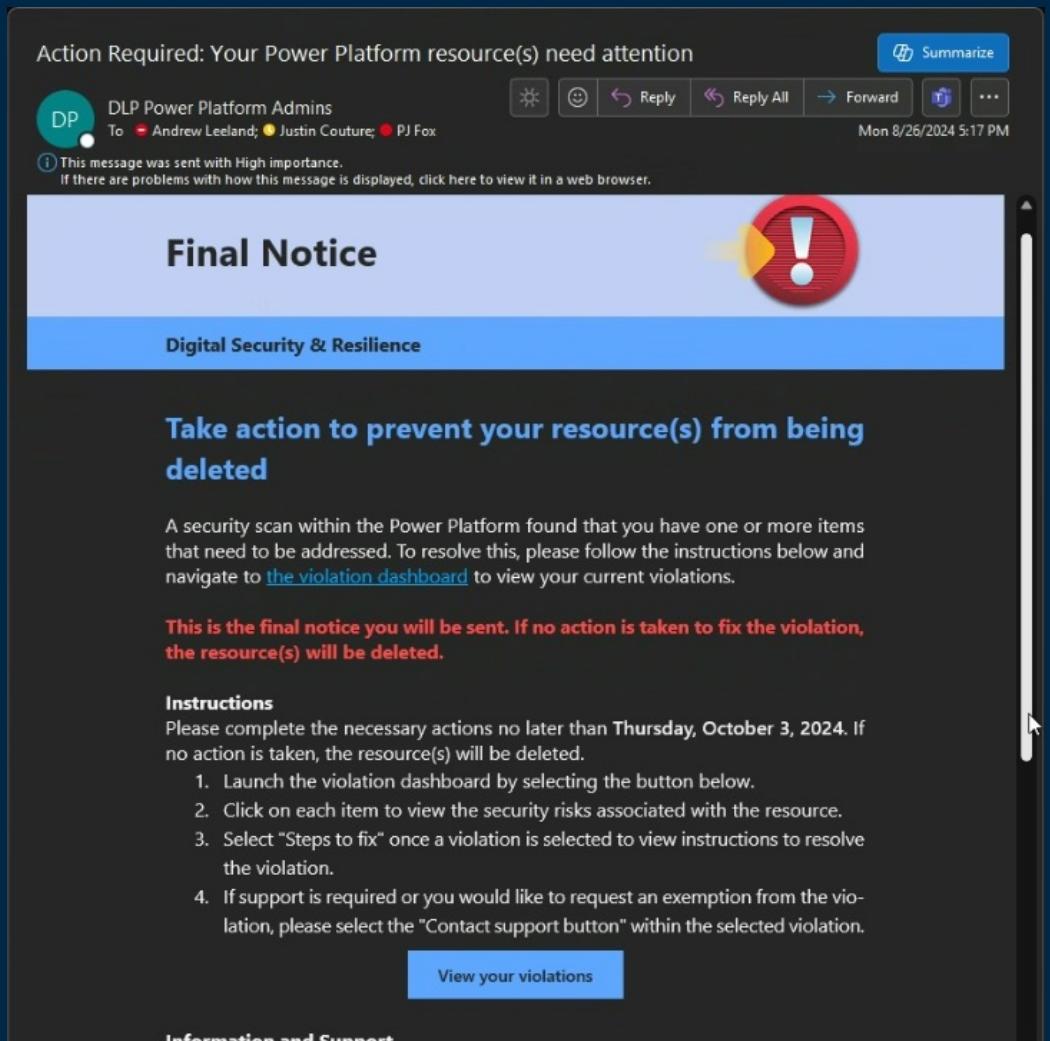
Self Service – Email

- 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



Self Service – Final Email

- Final Warning mail



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 ▾ 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.

RESOLVE BY: 11/12/2024 X

Open	Resource Type	Environment	Due Date Set	Sort by
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	>
AZ [REDACTED] Prod	Connection is using a shareable authentication method		● Due Date: 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 Description Steps to Fix Violation Activity

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.

[View Connection](#) [Delete Connection](#) [Contact Support](#) [Report as False Positive](#) [Request Exemption](#)

Microsoft 3 violations detected [REDACTED] Set User Give feedback v.20241008.2 66 #BLUEHAT

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 [REDACTED] RESOLVE BY: 11/12/2024 X

Open Resource Type 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 >

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 Description Steps to Fix Violation Activity

Steps to Fix

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

+ New connection Edit Share Switch account Delete Details

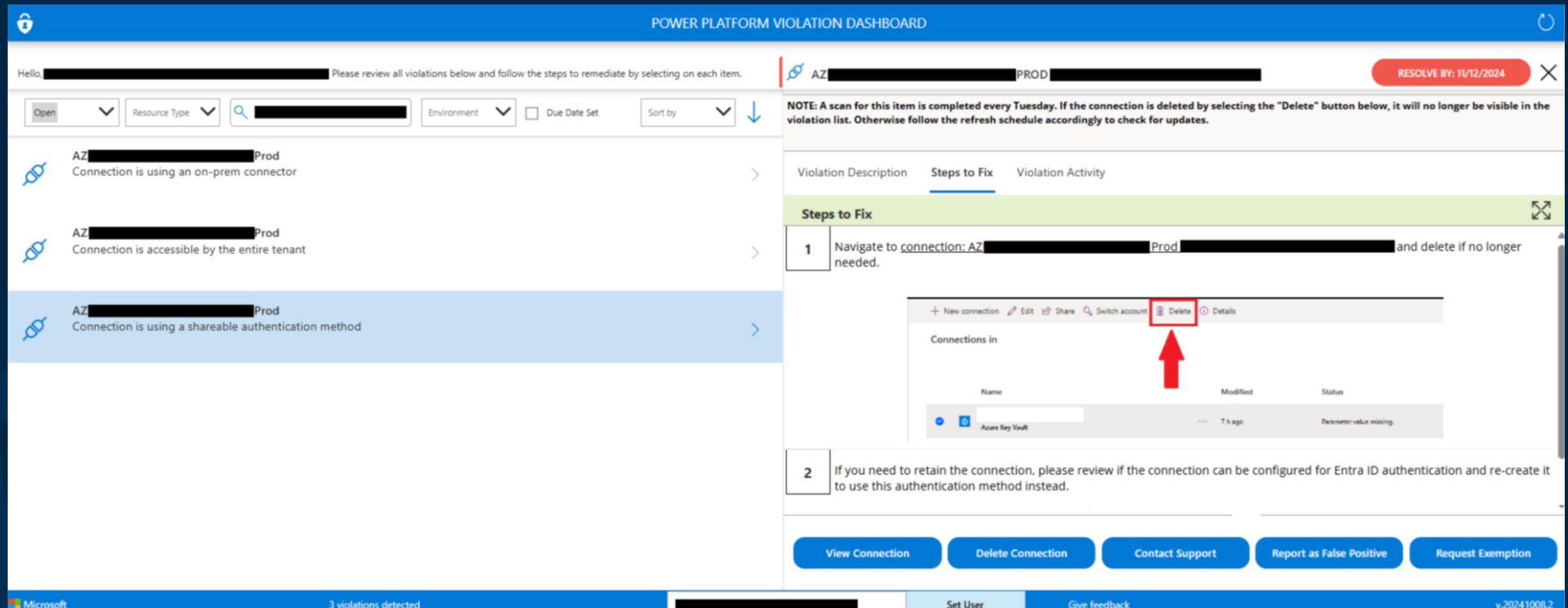
Connections in

Name	Modified	Status
Azure Key Vault	7 h ago	Parameter value missing.

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.

View Connection Delete Connection Contact Support Report as False Positive Request Exemption

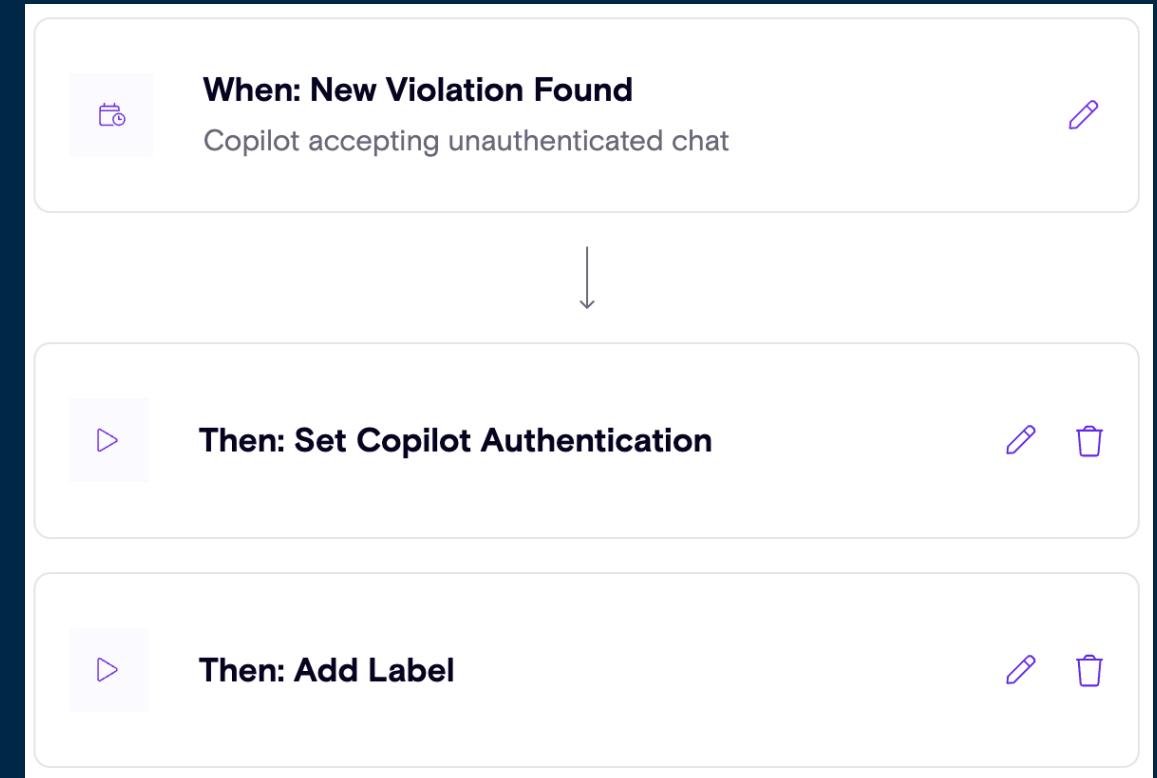
Microsoft 3 violations detected [REDACTED] Set User Give feedback v.20241008.2



@mbrg0
@donwillits66
#BLUEHAT

Playbooks

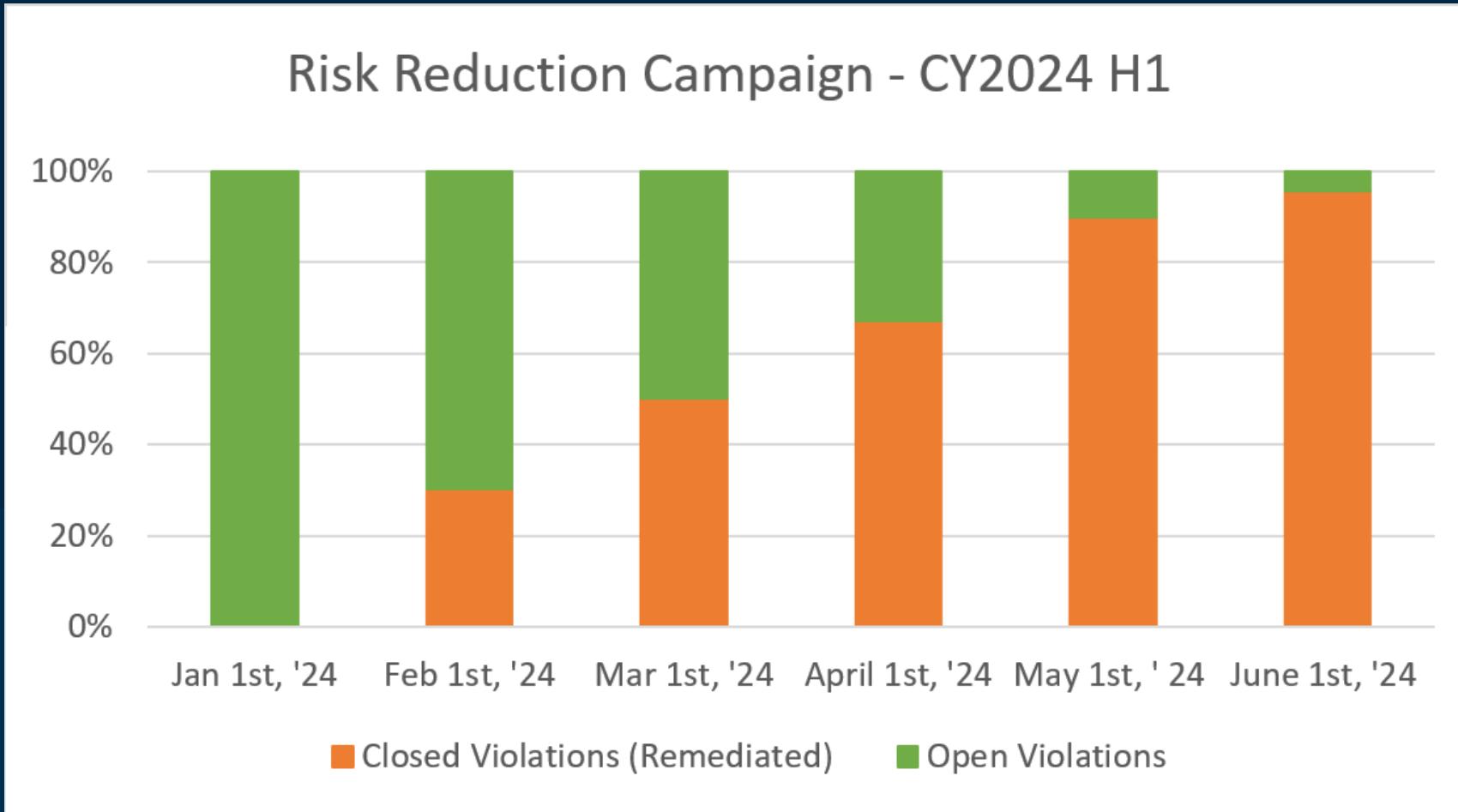
- Greenfield: As new violations come in...
- Brownfield: When we send out bulk emails to burn down pre-existing risk...
- If rule ID is XYZ, and other condition(s) are true...
...then take these actions



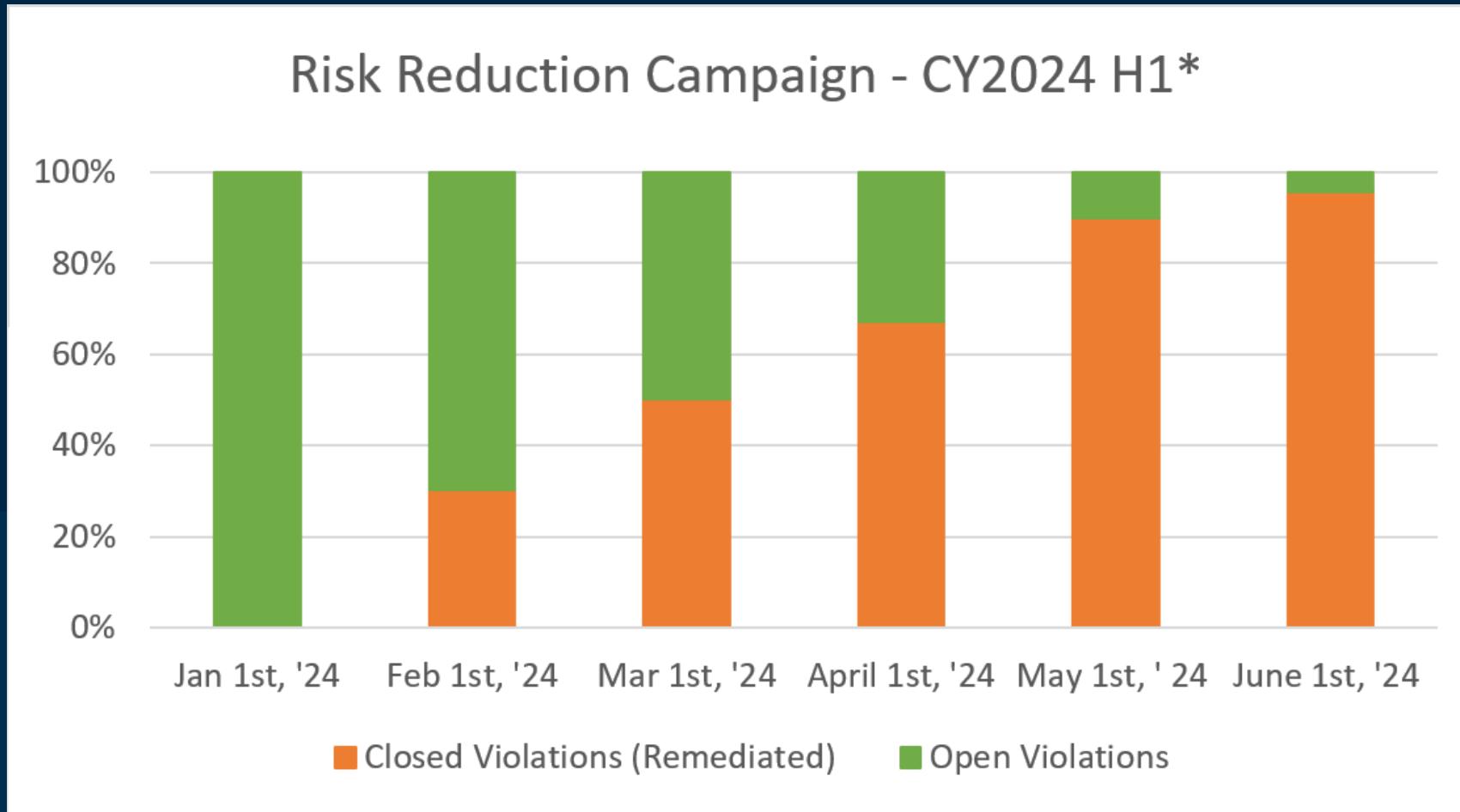
Results

- 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



SUCCESS



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



@mbrg0
@donwillits66
#BLUEHAT

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

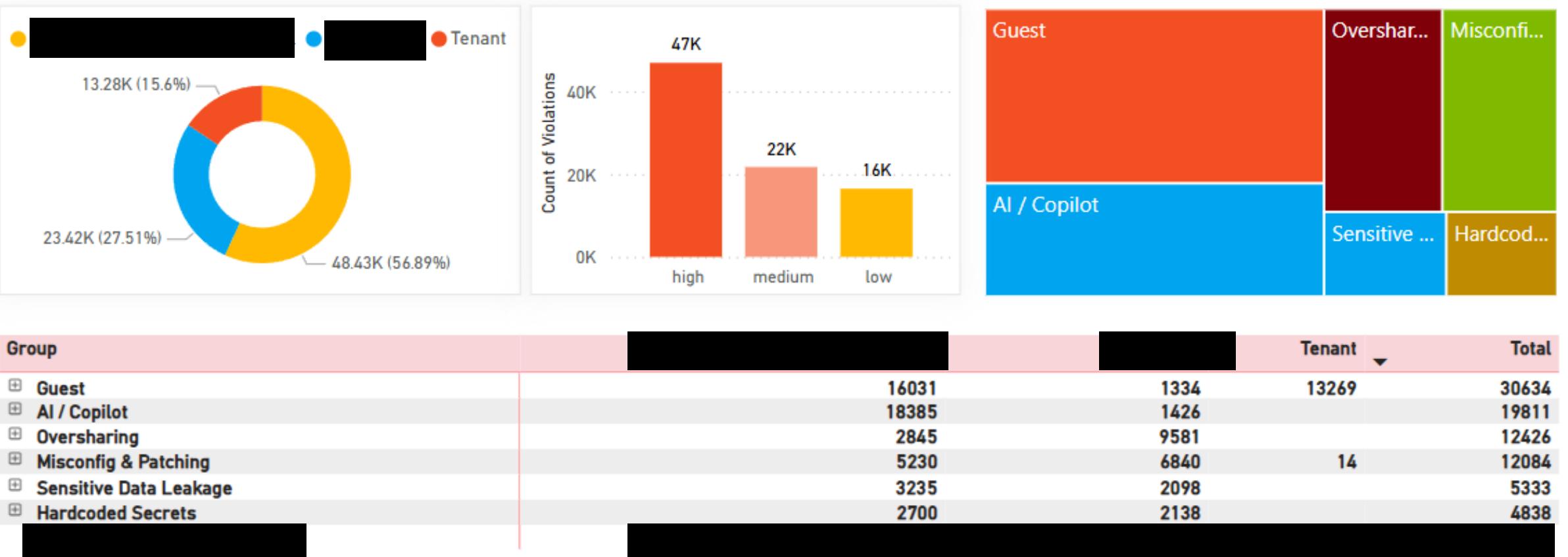
Merged similar OWASP Top 10 categories together & reviewed SDL gap analysis

- Also pivoted on Senior Leadership Team priorities

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

Campaigns included:

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



What did we learn from this?

- ✓ Leverage industry-standard security risk categorization
- ✓ Prioritize what we want to fix first
 - Shared Responsibility Model



Serverless



Customer

Platform

Serverless



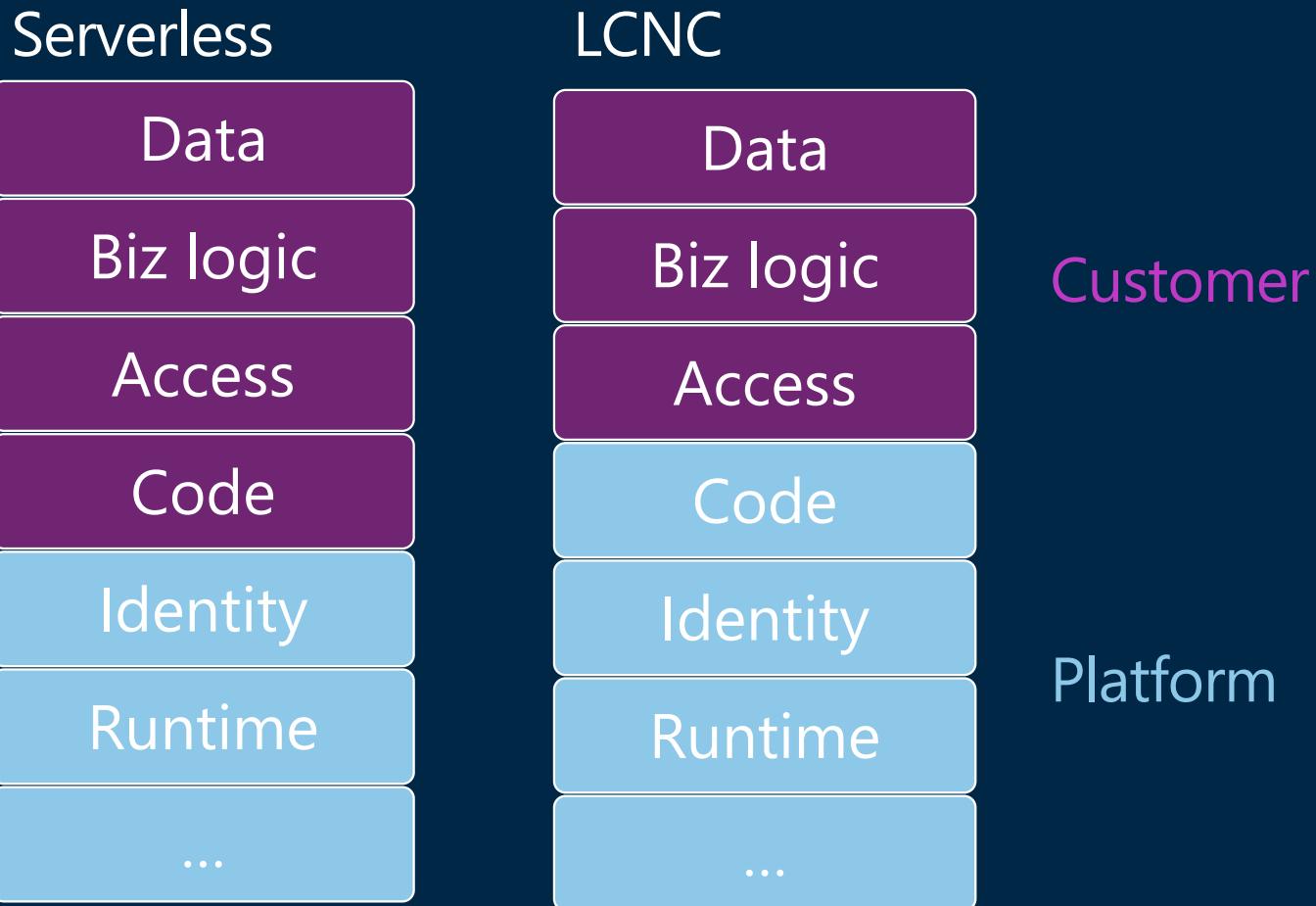
LCNC



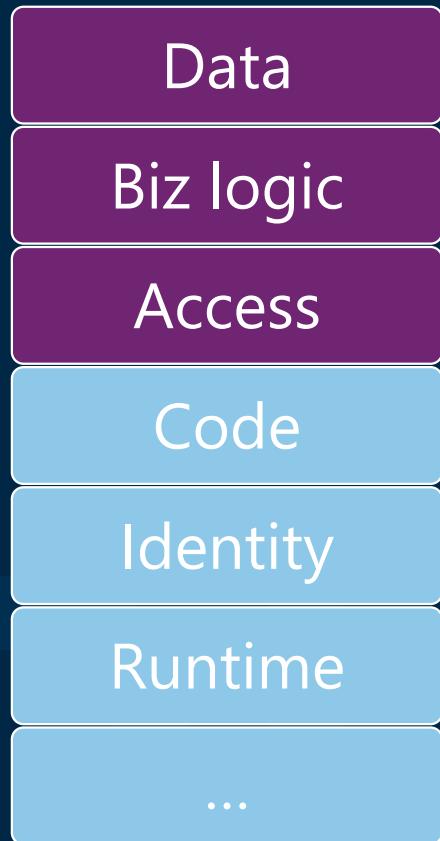
Customer

Platform

We must own our side of the Shared Responsibility Model



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



Customer

Platform

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



Customer
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?
- ...

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



Customer
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

Domain	Responsibility	Role Accountability			
		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>	○	

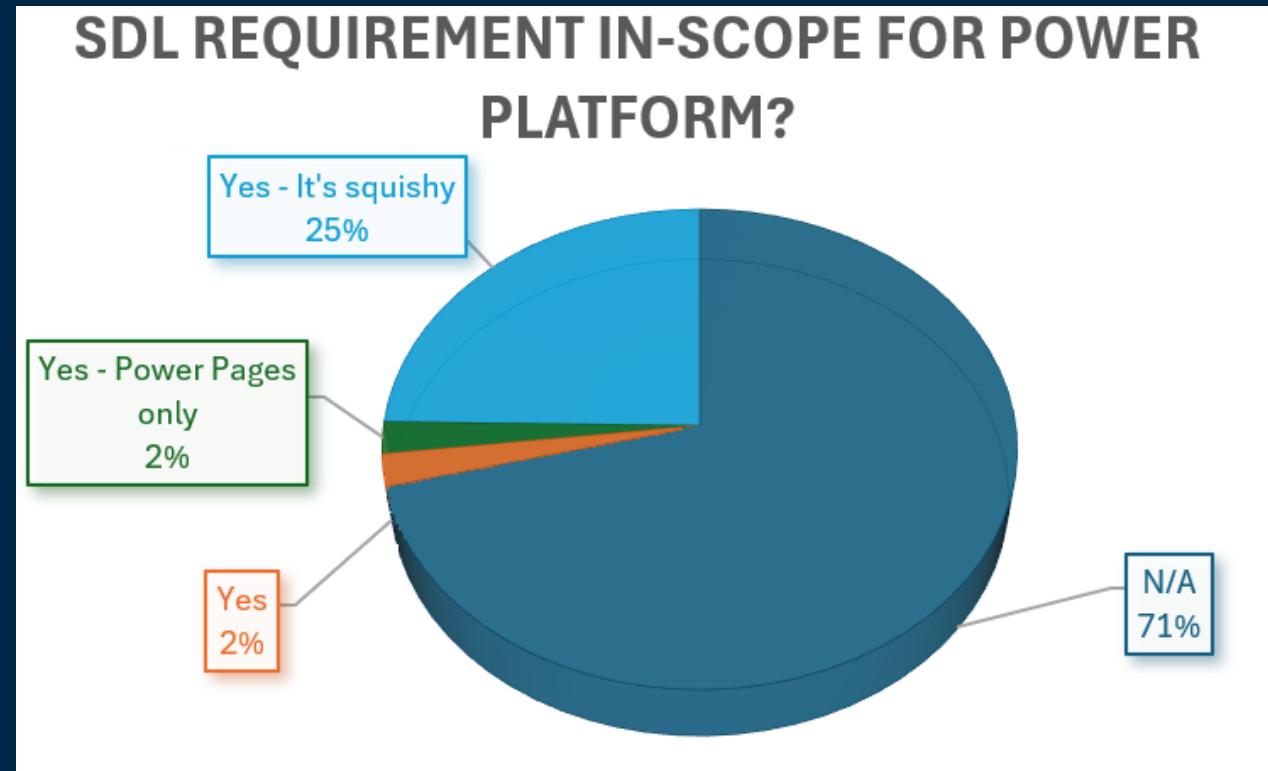
√	Directly accountable/responsible
●	Responsible (in partnership)
○	Consulted/Informed, may take some action

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. ☹



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



BLUEHAT

Thank you