



Learn more: [github.com/mbrg/talks](https://github.com/mbrg/talks)  
Twitter: @mbrg0

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

Michael Bargury @ Zenity  
BSidesLV 2023

# Hi there

- CTO and Co-founder @ Zenity
  - OWASP LCNC Top 10 project lead
  - Dark Reading columnist
  - Defcon, BSides, RSAC, OWASP
- 
- Hiring top researchers, engs & pms!



@mbrg0



[github.com/mbrg](https://github.com/mbrg)



[darkreading.com/author/michael-bargury](https://darkreading.com/author/michael-bargury)

# Agenda

1. Business users are building their own
2. What could go wrong?
3. How can we fix it?



Twitter: @mbrg0

# Enterprise LCNC - **EVERYONE** is a Developer

# Business Needs



IT Capacity



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

@mbrg0  
BSideLV 2023

The screenshot shows the Microsoft Power Apps studio interface. On the left, there's a tree view pane titled "Screens" with "Screen1" selected. The main workspace is a large white area with the placeholder text "Add an item from the Insert pane or connect to data". At the top, the ribbon includes "Power Apps | App", "Search", "Environment PowerAddicts (default)", and user profile icons. Below the ribbon, there are standard navigation and insert tools. A "Copilot" feature window is open on the right, featuring a purple speech bubble icon and the text "What do you want to do? Describe what you want to do with this app, and AI will do it for you." It also lists options like "Add a text label", "Add a gallery", "Add a button", and "Add an email screen". The bottom of the screen shows a footer with "Screen1" and a zoom control.

Source:  
@RezaDorrani

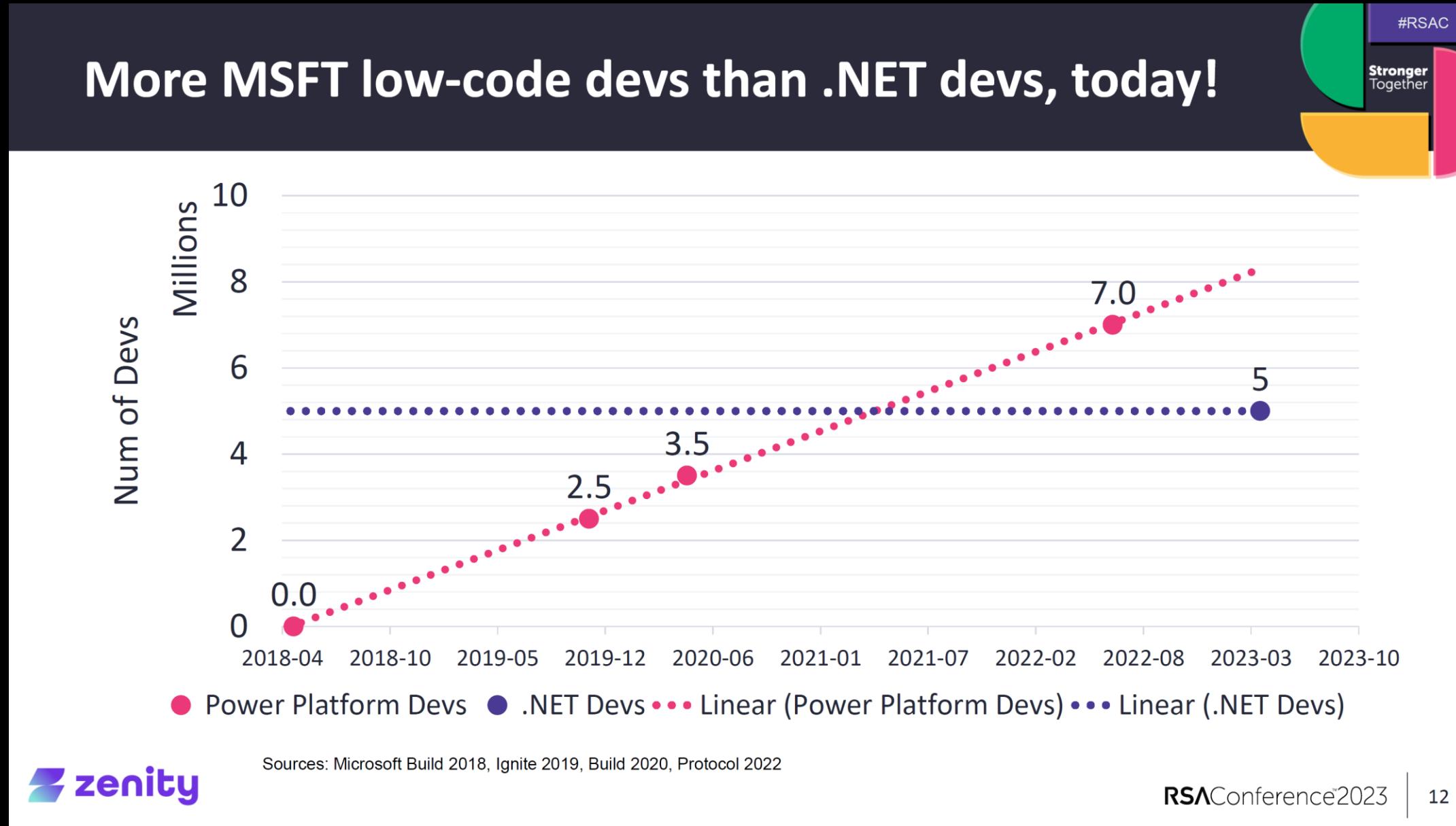
@mbrg0

#BHUSA@BlackHatEvents

# Is this actually being used?



# ~8M active Power devs today!



*Credential  
Sharing as a  
Service: The Dark  
Side of No Code*

Michael Bargury  
RSAC 2023



Twitter: @mbrg0

# What could go wrong?

# OWASP LCNC Top 10

- LCNC-SEC-01: Account Impersonation
- LCNC-SEC-02: Authorization Misuse
- LCNC-SEC-03: Data Leakage and Unexpected Consequences
- LCNC-SEC-04: Authentication and Secure Communication Failures
- LCNC-SEC-05: Security Misconfiguration
- LCNC-SEC-06: Injection Handling Failures
- LCNC-SEC-07: Vulnerable and Untrusted Components
- LCNC-SEC-08: Data and Secret Handling Failures
- LCNC-SEC-09: Asset Management Failures
- LCNC-SEC-10: Security Logging and Monitoring Failures





Twitter: @mbrg0

# Real-world stories



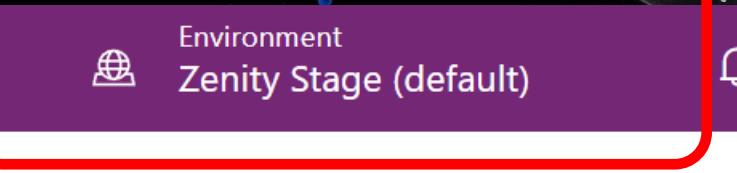
Twitter: @mbrg0

# Story #1 - employee onboarding

Power Apps    Search    Environment Zenity Stage (default)   

Start from

<b>Blank app</b> Create an app from scratch and then add your data 	<b>Dataverse</b> Start from a Dataverse table to create a three-screen app 	<b>SharePoint</b> Start from a SharePoint list to create a three-screen app 
<b>Excel</b> Start from an Excel file to create a three-screen app 	<b>SQL</b> Start from a SQL data source to create a three-screen-app 	<b>Image</b> Upload an image of an app and we'll convert it into an app 

Power Apps    Search    Environment Zenity Stage (default)    

Start from

-  **Blank app**  
Create an app from scratch and then add your data  
 Watch video
-  **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 file to create a three-screen app  
 Watch video
-  **SQL**  
Start from a SQL data source to create a three-screen-app  
 Watch video
-  **Image**  
Upload an image of an app and we'll convert it into an app  


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

@mbrgO  
BSideLV 2023

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

@mbrg0  
BSideLV 2023

Power Apps | Employee Onboarding

Search

Back | ↺ | ↻ | Insert | Add data | ...

Editing

Fill = fx White

Data

Search

Add data

Sensitive Inputs

Microsoft Dataverse - Current environment

Employee onboarding form

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security Number

Save

SCREEN

Screen1

Properties Advanced Ideas

Fill

Background image

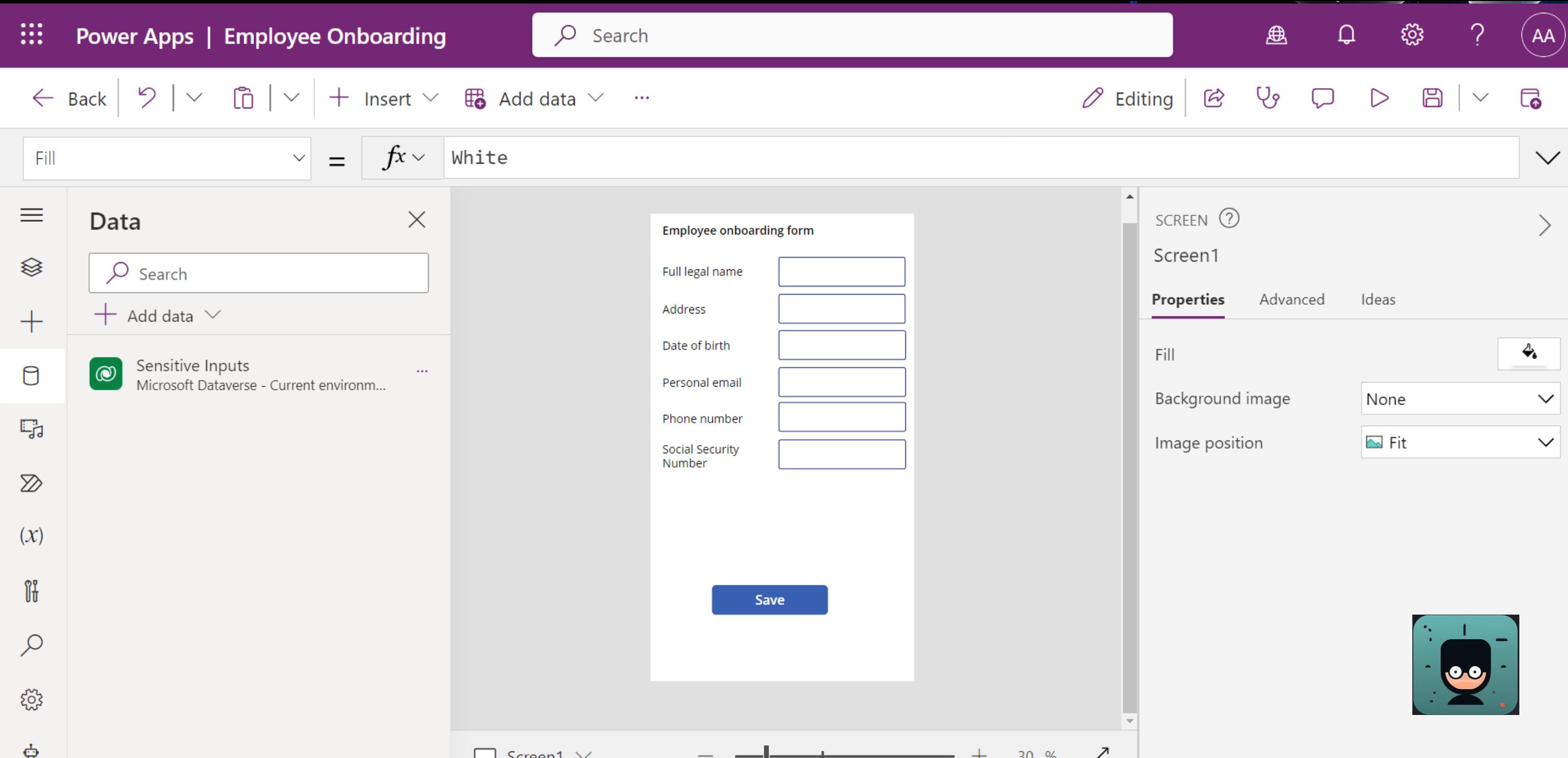
Image position

None

Fit

Screen1

30 %



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

@mbrg0  
BSideLV 2023

Power Apps | Employee Onboarding

Search

Back | ↺ | ↻ | Insert | Add data | ...

Editing

Fill = fx White

**Data**

Search

Add data

Sensitive Inputs Microsoft Dataverse - Current environment...

**Employee onboarding form**

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security Number

Save

SCREEN ?

Screen1

Properties Advanced Ideas

Fill

Background image

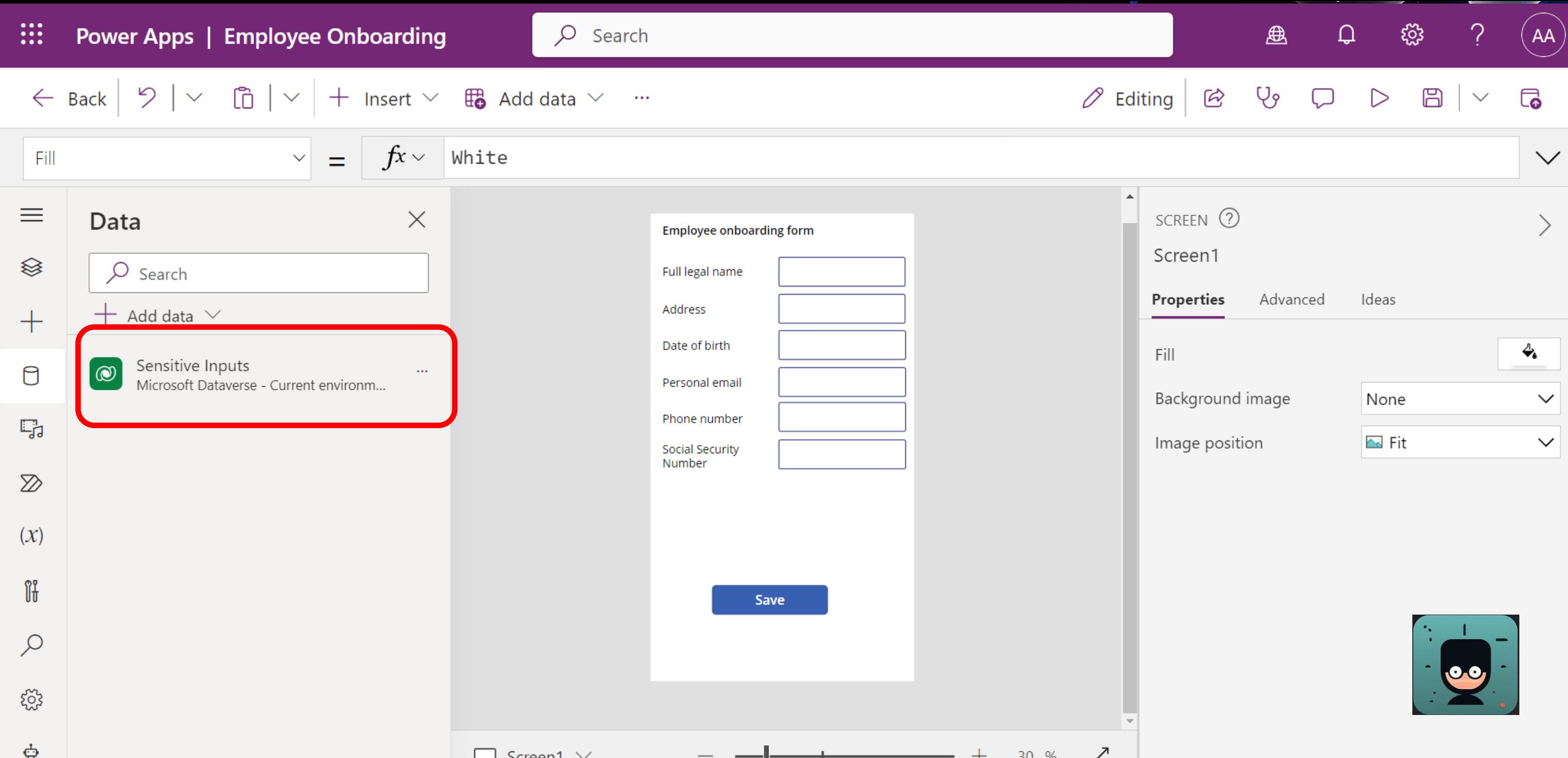
Image position

None Fit

Screen1

Save

30 %



Power Apps | Employee Onboarding

Search

Back | ↺ | ↻ | Insert | Add data | ...

Editing

Fill

Data

Search

Add data

Sensitive Inputs Microsoft Dataverse

Ideas

None

Fit

Microsoft Power Platform

The low code platform that spans Microsoft 365, Azure, Dynamics 365, and standalone apps.

Power BI Business analytics

Power Apps App development

Power Automate Process automation

Power Virtual Agents Intelligent virtual agents

Power Pages External-facing websites

Data connectors

AI Builder

Dataverse

AI Assistant

This screenshot shows the Microsoft Power Platform home page. The top navigation bar includes 'Power Apps | Employee Onboarding', a search bar, and various icons for globe, notifications, settings, and help. The left sidebar has a 'Data' section with 'Sensitive Inputs Microsoft Dataverse'. The main content area features the 'Microsoft Power Platform' logo and a description: 'The low code platform that spans Microsoft 365, Azure, Dynamics 365, and standalone apps.' Below this are five service cards: Power BI (Business analytics), Power Apps (App development), Power Automate (Process automation), Power Virtual Agents (Intelligent virtual agents), and Power Pages (External-facing websites). At the bottom, there are three additional icons: Data connectors, AI Builder, and Dataverse. A vertical sidebar on the right contains sections for 'Ideas', 'None', and 'Fit', along with a large 'AI Assistant' icon.

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

@mbrgO  
BSideLV 2023

The screenshot shows the Microsoft Power Automate interface. On the left, the navigation bar includes 'Power Automate', 'Search' (with a magnifying glass icon), 'Environments' (set to 'Zenity Stage (default)'), and various global icons like gear, question mark, and language (ZH).

The main workspace displays a flow titled 'Update Employee Info in HR system'. The flow consists of two steps:

- When a row is added, modified or deleted** (trigger step)
- Send email (V2)** (action step)

The 'Send email (V2)' step is currently selected. Its configuration includes:

- To:** hrorg@cloudcore.com
- Subject:** New Employee Update info
- Body:** A rich text editor with a font size dropdown set to 12, bold (B), italic (I), underline (U), and a toolbar below.
- Attachments:** A section for attachments with fields for Name, Content, and Type.
- Advanced Options:** A 'Show advanced options' button.

At the bottom of the workspace, there are buttons for '+ New step' and 'Save'. A blue circular icon in the bottom right corner says 'Ask a chatbot'.

# Employee onboarding – findings

Power Apps | Employee Onboarding

Search

Employee onboarding form

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security Number

Save

KS

A small icon in the bottom right corner depicts a person sitting at a desk with two computer monitors, set against a pink gradient background.

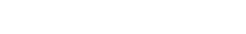
Power Apps    Search    Environment Zenity Stage (default)    

+ New table    Import    Export    Search

Home    Create    Learn    Apps

Tables

Recommended    Custom    All

Table ↑	Name	Type	Managed	Customizable	Tags
Account	account	Standard	Yes	Yes	Core
Address	customeraddress	Standard	Yes	Yes	Standard
AppFlow Relation	cr6e4_appflowrel...	Standard	No	Yes	Custom
Appointment	appointment	Activity	Yes	Yes	Productivit
asjs	cr6e4_asjs	Standard	No	Yes	
Attachment	activitymimeatta...	Standard	Yes	Yes	

... More

Power Platform    Ask a virtual agent

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

@mbrg0  
BSideLV 2023

Power Apps    Search    Environment Zenity Stage (default)    KS

+ New table    Open    Edit    Import    Export    Properties    ...    Search

	Position	⋮	position	Standard	Yes	Yes	System
+	Query	⋮	cr6e4_querytest	Standard	No	Yes	Custom
+	Recurring Appointment	⋮	recurringappoint...	Activity	Yes	Yes	Standard
+	res	⋮	cr6e4_res	Standard	No	Yes	Custom
+	Sensitive Input	⋮	cr6e4_sensitivein...	Standard	No	Yes	Custom
+	table_for_app_with_im...	⋮	cr6e4_table_for_...	Standard	No	Yes	Custom
+	Task	⋮	task	Activity	Yes	Yes	Productivit
+	Team	⋮	team	Standard	Yes	Yes	System
+	Team template	⋮	teamtemplate	Standard	Yes	Yes	
+	ttv	⋮	cr6e4_ttv	Standard	No	Yes	
+	User	⋮	systemuser	Standard	Yes	Yes	Standard

Home    Create    Learn    Apps    Tables    Connections    Solutions    Flows    More    Power Platform    Ask a virtual agent



Power Apps    Search    Environment Zenity Stage (default)    KS

Back | New row | New column | Refresh | Create an app | Edit table properties | Update forms and views

### Sensitive Inputs

Data saved

Employee Name*	SSN	Address	Contact	+19 more	
Jamie Reading	209-97-1111	jamier@zenitydemo.OnMicrosoft.com			
Brooklyn Gonzalez	209-97-9876	brooklynd@zenitydemo.OnMicrosoft.com			
Henry Mitchell	209-97-0987	henryd@zenitydemo.OnMicrosoft.com			
Savannah Perez	209-97-7890	savannahp@zenitydemo.OnMicrosoft.com			
Ella Gonzalez	209-97-9876	ellaq@zenitydemo.OnMicrosoft.com			
Riley Mitchell	209-97-0987	rileyp@zenitydemo.OnMicrosoft.com			
Nathan Perez	209-97-7890	nathanh@zenitydemo.OnMicrosoft.com			
Daniel Martin	209-97-6789	danielm@zenitydemo.OnMicrosoft.com			
Layla Gonzalez	209-97-9876	laylam@zenitydemo.OnMicrosoft.com			



# Employee onboarding – findings

- Data accessible to all (Authorization Misuse)



# Employee onboarding – findings

- Data accessible to all (Authorization Misuse)
- Sensitive data in plain text (Data and Secret Handling Failures)



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

@mbrg0  
BSideLV 2023

Power Apps | Employee Onboarding

Environment  
Zenity Stage (default)



## Employee onboarding form

Full legal name	Daniel Wood
Address	New York 3rd street
Date of birth	11 Jan 1990
Personal email	Danielw124@gmail.co
Phone number	202-555-0117
Social Security Number	78-05-1120



Save



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

@mbrgO  
BSideLV 2023

The screenshot shows the Microsoft Power Automate interface. On the left, the navigation bar includes 'Power Automate', 'Search' (with a magnifying glass icon), 'Environments' (set to 'Zenity Stage (default)'), and various global icons like gear, question mark, and language (ZH).

The main workspace displays a flow titled 'Update Employee Info in HR system'. The flow consists of two steps:

- When a row is added, modified or deleted** (trigger step)
- Send email (V2)** (action step)

The 'Send email (V2)' step is currently selected. It has the following configuration:

- To:** hrorg@cloudcore.com
- Subject:** New Employee Update info
- Body:** Includes a rich text editor with font size 12, bold, italic, underline, and other styling options. It also includes placeholder fields for SSN, Contact, Email, Address, and Employee Name.
- Attachments Name - 1:** Title of the attachment.
- Attachments Content - 1:** Body of the attachment.
- Attachments Content-Tune - 1:** Type of content in the attachment.

At the bottom of the email step, there is a button labeled '+ Add new item' and a link 'Show advanced options'.

At the bottom of the Power Automate screen, there are buttons for '+ New step' and 'Save'. A blue circular icon with a white question mark and the text 'Ask a chatbot' is located at the bottom left. A green circular icon with a cartoon character face is at the bottom right.

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

@mbrgO  
BSideLV 2023

Power Automate    Search    Environments Zenity Stage (default)    ? ZH

Update Employee Info in HR system • Ran at 8/7/2023 7:40:51 PM

Your flow ran successfully.

When a row is added, modified or deleted

When a row is added, modified or deleted

Change type: 4

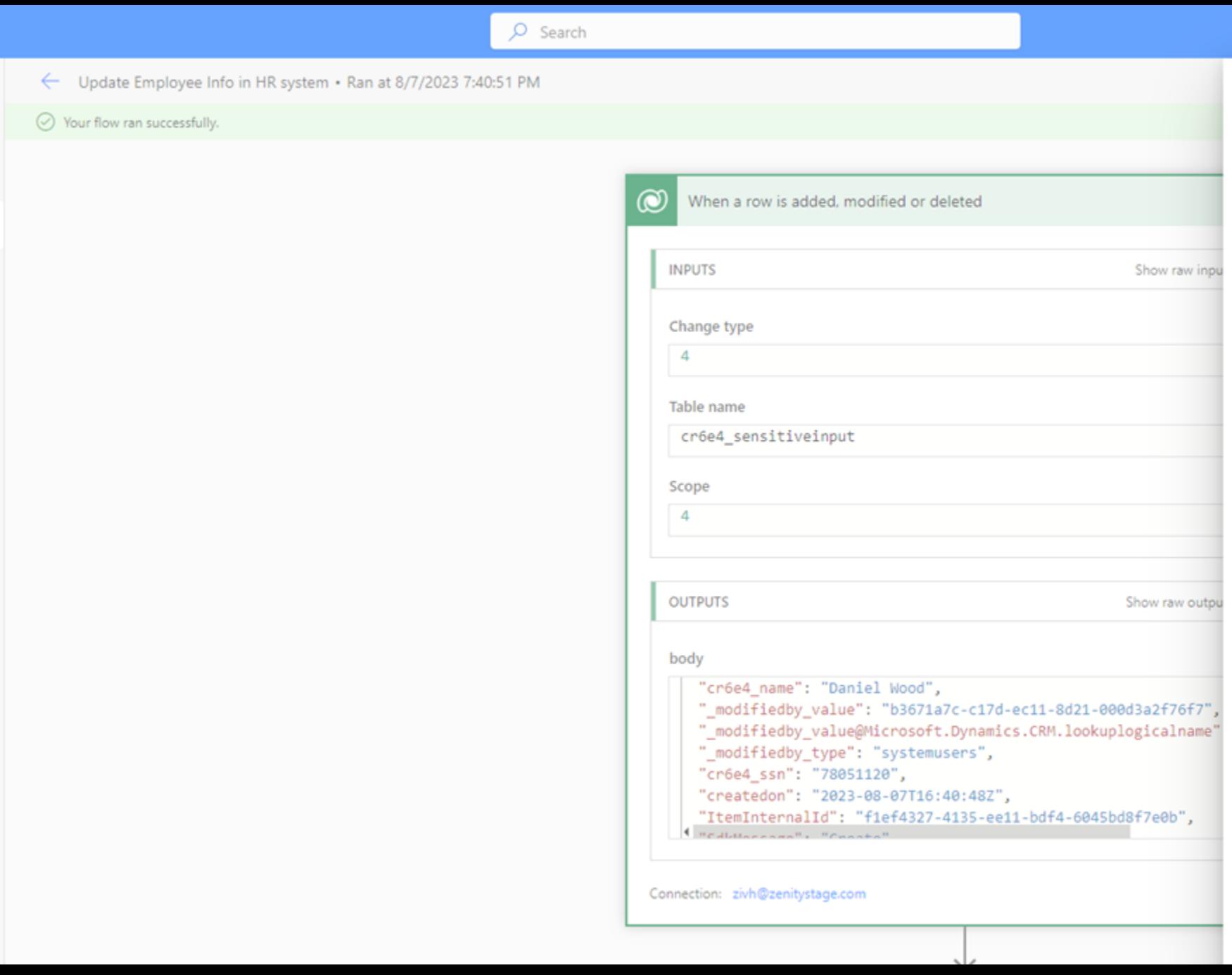
Table name: cr6e4\_sensitiveinput

Scope: 4

body

```
{
  "headers": {
    "Expect": "100-continue",
    "Host": "prod-52.westeurope.logic.azure.com",
    "x-ms-correlation-request-id": "d7b3daa4-0bba-4724-918b-4523e1bb2e75",
    "x-ms-client-request-id": "d7b3daa4-0bba-4724-918b-4523e1bb2e75",
    "x-ms-user-id": "7cb2f429-a54a-46c3-8e4f-df3a3032f249",
    "Content-Length": "1258",
    "Content-Type": "application/json"
  },
  "body": [
    "cr6e4_email": "daniel1ds@gmail.com",
    "_owningbusinessunit_value": "edfdf52a-e501-ec11-94ee-002248800bc",
    "_owningbusinessunit_value@Microsoft.Dynamics.CRM.lookuplogicalname": "bu",
    "_owningbusinessunit_type": "businessunits",
    "statecode": 0,
    "_statecode_label": "Active",
    "cr6e4_sensitiveinputid": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",
    "statuscode": 1,
    "_statuscode_label": "Active",
    "cr6e4_contact": "202-555-0117",
    "_createdby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "_createdby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",
    "_createdby_type": "systemusers",
    "cr6e4_dateofbirth": "10.10.1990",
    "_ownerid_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "_ownerid_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",
    "_ownerid_type": "systemusers",
    "modifiedon": "2023-08-07T16:40:48Z",
    "cr6e4_address": "116 E 60TH ST NEW YORK USA",
    "cr6e4_name": "Daniel Wood",
    "_modifiedby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "_modifiedby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",
    "_modifiedby_type": "systemusers",
    "cr6e4_ssn": "78051120",
    "createdon": "2023-08-07T16:40:48Z",
    "ItemInternalId": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",
    "SdkMessage": "Create",
    "RunAsSystemUserId": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7"
  ]
}
```

Connection: zivh@zenitystage.com



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

@mbrg0  
BSideLV 2023

Power Automate

Search

Environments  
Zenity Stage (default)

Edit

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Ask a chatbot

Update Employee Info in HR system

Owners

Adding an owner gives them full control of this flow, so make sure you only share with people you trust. They'll be able to add or remove other users as owners, access the run history, and can update, edit or delete this flow.

[Learn more](#)

Add a user or group as owner

Enter names, emails, or user groups

Ziv Hagbi

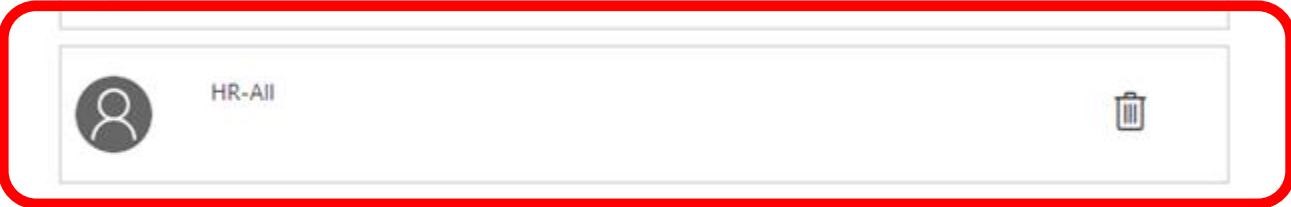
HR-All

Connections in use

Connections listed are actively being used in this flow. [Manage connections](#)

 zivh@zenitystage.com  
✓ Microsoft Dataverse

 maortzury@gmail.com  
✓ Gmail



# Employee onboarding – findings

- Data accessible to all (Authorization Misuse)
- Sensitive data in plain text (Data and Secret Handling Failures)
- Sensitive data written to logs (Data Leakage)

```
        "body": {  
            "cr6e4_email": "danielids@gmail.com",  
            "_owningbusinessunit_value": "edfdf52a-e501-ec11-94ee-0022488300bc",  
            "_owningbusinessunit_value@Microsoft.Dynamics.CRM.lookuplogicalname": "bu",  
            "_owningbusinessunit_type": "businessunits",  
            "statecode": 0,  
            "statecode_label": "Active",  
            "cr6e4_sensitiveinputid": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",  
            "statuscode": 1,  
            "statuscode_label": "Active",  
            "cr6e4_contact": "202-555-0117",  
            "createdby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",  
            "createdby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",  
            "createdby_type": "systemusers",  
            "cr6e4_dateofbirth": "10.10.1990",  
            "ownerid_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",  
            "ownerid_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",  
            "ownerid_type": "systemusers",  
            "modifiedon": "2023-08-07T16:40:48Z",  
            "cr6e4_address": "116 E 60TH ST NEW YORK USA",  
            "cr6e4_name": "Daniel Wood",  
            "modifiedby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",  
            "modifiedby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",  
            "modifiedby_type": "systemusers",  
            "cr6e4_ssn": "78051120",  
            "createdon": "2023-08-07T16:40:48Z",  
            "ItemInternalId": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",  
            "SdkMessage": "Create",  
            "RunAsSystemUserId": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",  
            "RowVersion": "12774383"  
        }  
    }  
}
```

# Employee onboarding – findings

- Data accessible to all (Authorization Misuse)
- Sensitive data in plain text (Data and Secret Handling Failures)
- Sensitive data written to logs (Data Leakage)



Twitter: @mbrg0

## Story #2 – productivity sync

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

@mbrg0  
BSideLV 2023

Power Automate    Search    Environments    Zenity Stage (default)         

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:

Font: 12pt, Bold, Italic, Underline,

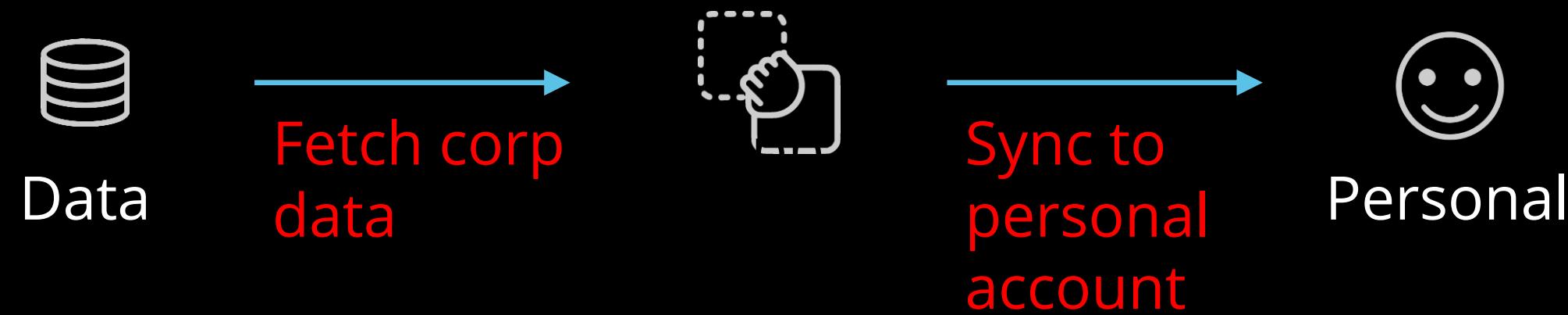
Attachments:



# Productivity sync – findings

# Productivity sync – findings

- Business data to personal account (Data Leakage)



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

@mbrg0  
BSideLV 2023

Power Apps | Set up your email sync

Environment  
Zenity Stage (default)

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

Sync Outlook history to Gmail

Email address

Text input

How many emails to sync

Sync your email

**Button**

Button1

Properties Advanced Ideas

Search for a property ...

**ACTION**

OnSelect

SyncOutlookhistorytoGmail.Run( NumberInput , EmailInput )

**DATA**

Text

"Sync your email"

Tooltip

""

Icon: A cartoon character sitting at a desk with multiple computer monitors.



KS

## Sync Outlook history to Gmail

Email address

Text input

How many emails to sync

Text input

Sync your email



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

@mbrgO  
BSideLV 2023

Power Automate

Search

Environments  
Zenity Stage (default)

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Sync Outlook history to Gmail

Undo Redo Comments Save Flow checker Test

PowerApps (V2)

Get last X emails with attachments

For each email

Send email to myself

To: MyEmailAddress

Subject: Subject

Body:

Font: 12pt B I U

Body:

?

KS

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

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

@mbrg0  
BSideLV 2023

Power Apps

Search

Edit Play Share

Apps > 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

Kris Smith Owner

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



Send an email invitation to new users

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

KS Kris Smith Owner

Share Set up your email sync

Send an email invitation to new users



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

@mbrgO  
BSideLV 2023

Power Apps

Search

Edit Play Share

Apps > 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

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

Send an email invitation to new users

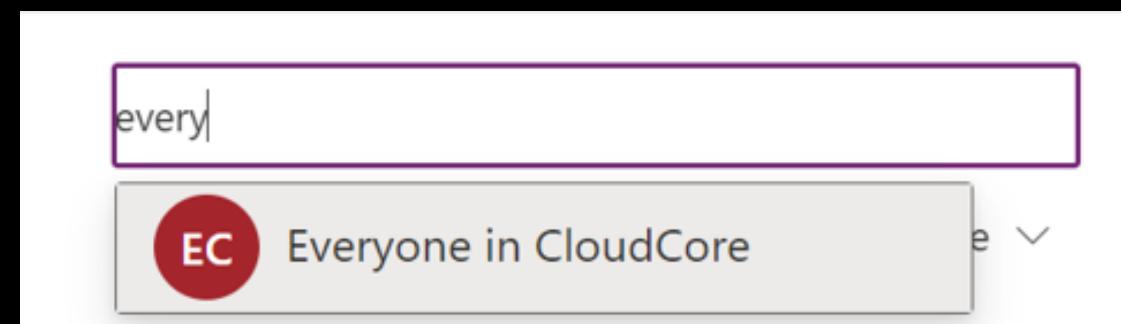
Home Create Learn Apps Tables Flows Chatbots AI models Solutions Cards Choices Connections Dataflows More

QR code

# Productivity sync – findings

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

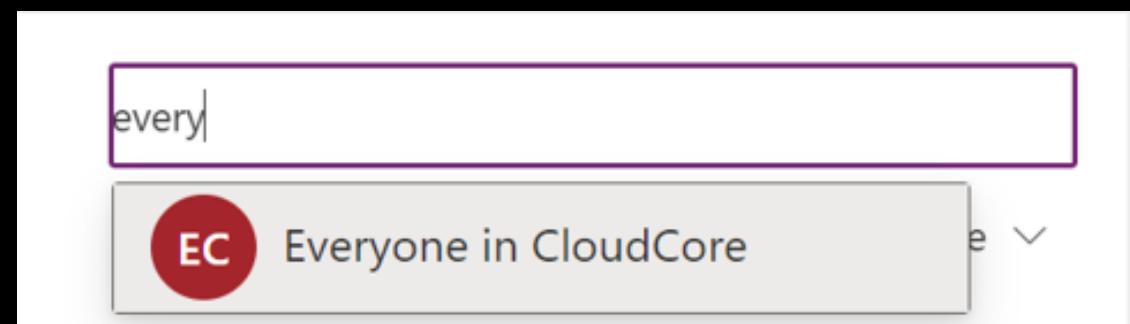
Everyone means EVERYONE, including guests by-default



# Productivity sync – findings

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

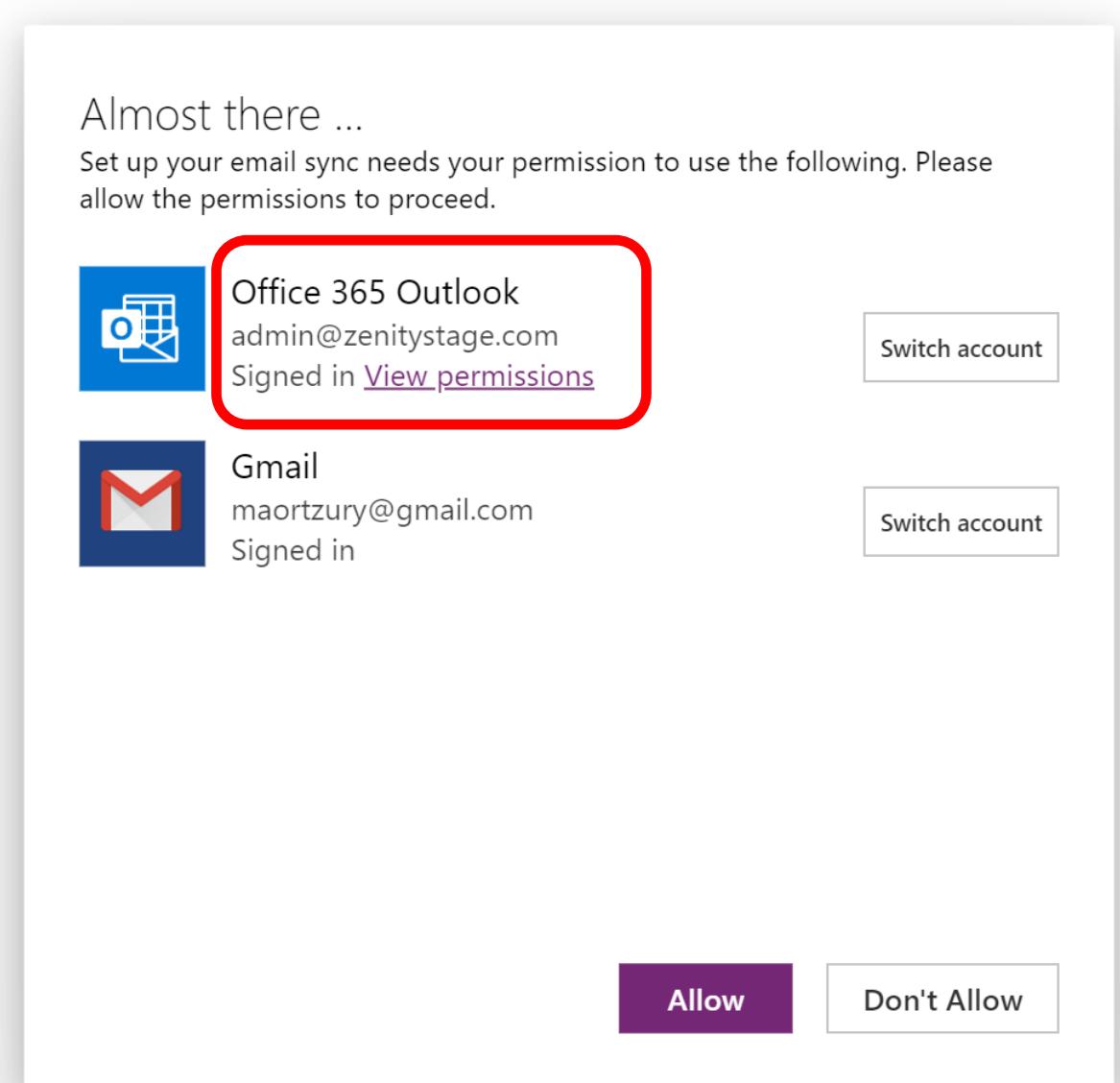
Everyone means EVERYONE, including guests by-default



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

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

@mbrgO  
BSideLV 2023



## Sync Outlook history to Gmail

Email address

maortzury@gmail.com

How many emails to sync

20

Sync your email



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

@mbrg0  
BSideLV 2023

Power Automate    Search    Environments    Zenity Stage (default)    Ks

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

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

PowerApps (V2)    0s

Get last X emails with attachments    2s

For each email    32s

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

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

@mbrgO  
BSideLV 2023

Power Automate    Search    Environments    Zenity Stage (default)    Resubmit    Cancel    Edit

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

For each email    5s

< Previous    < Previous failed    Show 1 of 5    Next failed >    Next >

Send email to myself    1s

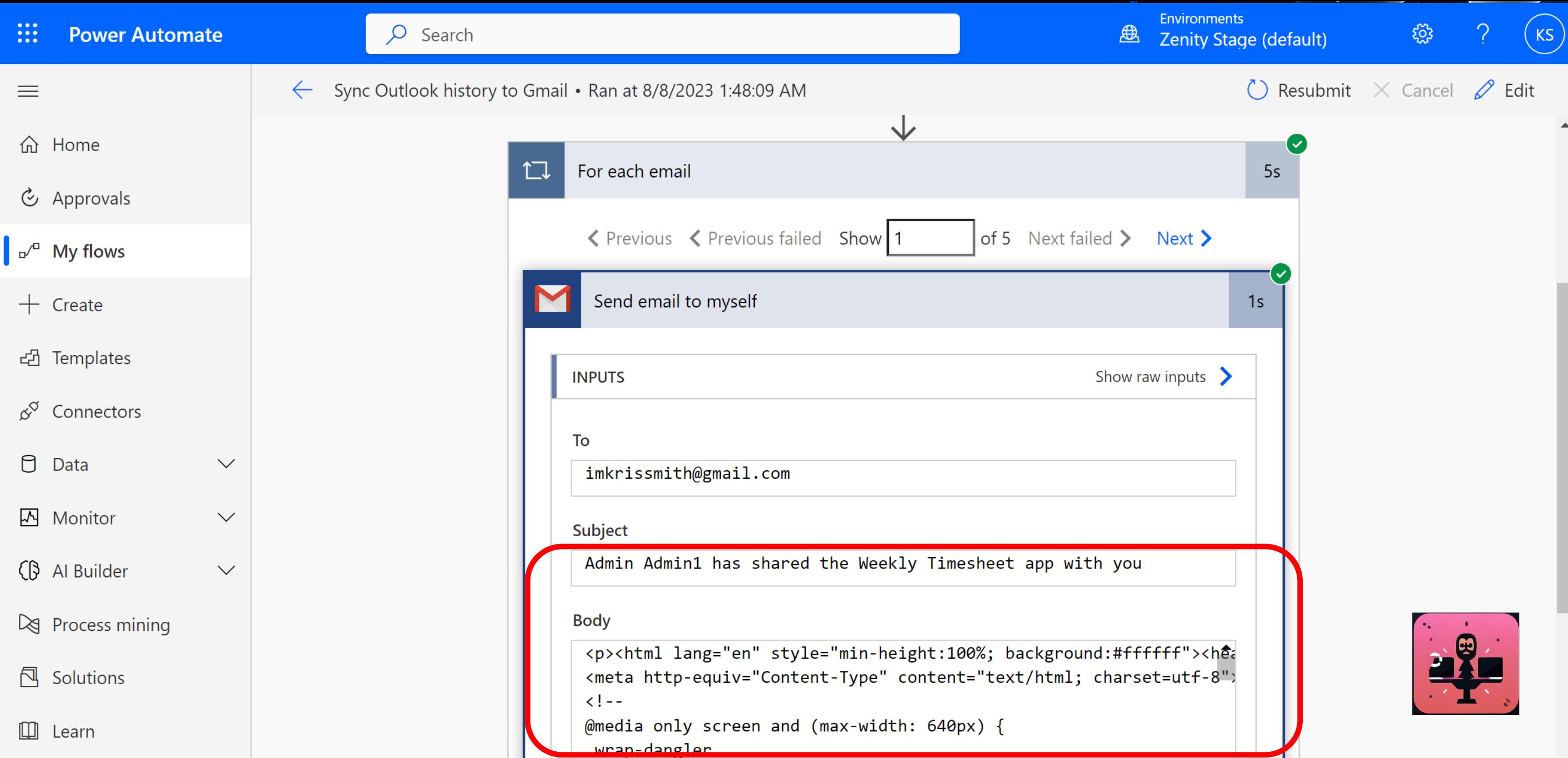
To: imkriissmith@gmail.com

Subject: Admin Admin1 has shared the Weekly Timesheet app with you

Body:

```
<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
}
```

A red box highlights the "Body" section of the email template.



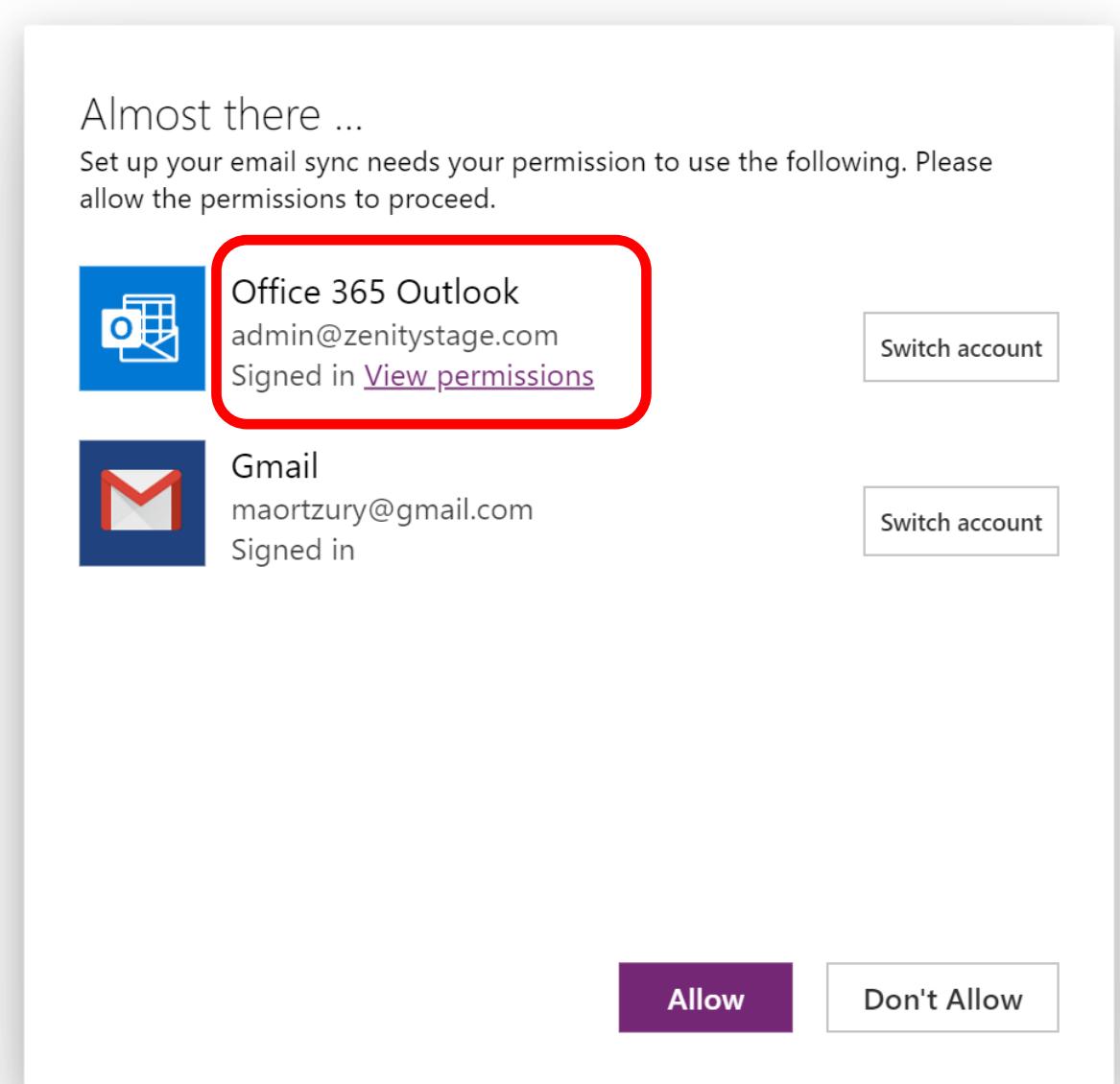
# Productivity sync – findings

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



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

@mbrgO  
BSideLV 2023



# Phishing made easy

Can we fool users to create connections for us?

- Set up a bait app that does something useful
- Generate connections on-the-fly
- Fool users to use it
- Pwn their connection (i.e. account)

***Low Code High Risk:  
Enterprise Domination via  
Low Code Abuse***

Michael Bargury  
DEFCON 30

Check out [power-pwn](#)  
on GitHub!



Account takeover

# Productivity sync – findings

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

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

@mbrg0  
BSideLV 2023



# Story #3 – self-service

@mbrg0

#BHUSA @BlackHatEvents



Twitter: @mbrg0

## Story #3 – self-service

# What happens when a maker leaves the org?

# What happens when a maker leaves the org?

- Asset Management Failures

The screenshot shows a Microsoft Power Apps interface. At the top, there's a purple header bar with the text "Power Apps | Management App" on the left, a search bar in the center containing a magnifying glass icon and the word "Search", and several icons on the right including a globe, a bell, a gear, a question mark, and a language switch set to "ZH". Below the header, the main title "My Management App" is displayed in large black font. Underneath it, the section "My Employees" is shown in a larger font. To the left of this section is a dropdown menu showing "Kris Smith" and a blue "Get Access" button. On the right side, there's a vertical sidebar with icons for a list, a phone, and a calendar, along with a small circular profile picture of a cartoon character at the bottom. A descriptive text at the bottom states: "This app allows you as a manager to take access employee Apps, including employees who have left the organization and reassign them."

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

@mbrgO  
BSideLV 2023

Power Automate    Search    Environments Zenity Stage (default)    ? ZH

Get Access to Employee Apps    Undo    Redo    Comments    Save    Flow checker    Test

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

Ask a chatbot

```
graph TD; A[PowerApps (V2)] --> B[Get Apps]; B --> C[Apply to each 2]; C --> D[Apply to each 3]
```

+ New step    Save

A cartoon character icon is located in the bottom right corner.

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

@mbrgO  
BSideLV 2023

Power Automate    Search    Environments    Zenity Stage (default)    ?    ZH

Get Access to Employee Apps

Undo    Redo    Comments    Save    Flow checker    Test

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

Ask a chatbot

PowerApps (V2)

Email

Add an input

Get Apps

Apply to each

Set App Owner

\* Environment Name: properties/environment

\* PowerApp Name: name

API Version: 2016-11-01

Content Type: application/json

Role For Old App Owner: CanView

New PowerApp Owner: email

Add an action

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

@mbrgO  
BSideLV 2023

The screenshot shows a Microsoft Power Automate flow titled "Get Access to Employee Apps". The flow consists of the following steps:

- A "PowerApps (V2)" connector action labeled "Email".
- An "Apply to each 3" loop.
- A "Get Apps" connector action.
- An "Apply to each" loop.
- A "Set App Owner" connector action, which is highlighted with a red box.
- An "Apply to each" loop.
- An "Apply to each" loop.

The "Set App Owner" step has the following configuration:

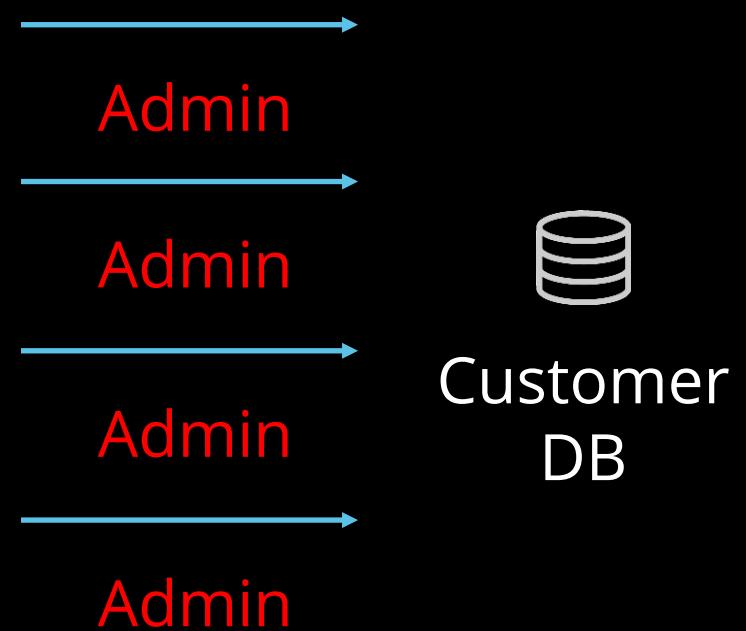
- Environment Name: properuseenv... (with a warning icon)
- \*PowerApp Name: name (with a warning icon)
- API Version: 2016-11-01
- Content Type: application/json
- Role For Old App Owner: CanView
- New PowerApp Owner: email (with a warning icon)

At the bottom of the flow, there is a button labeled "Add an action".

# Self-service – findings

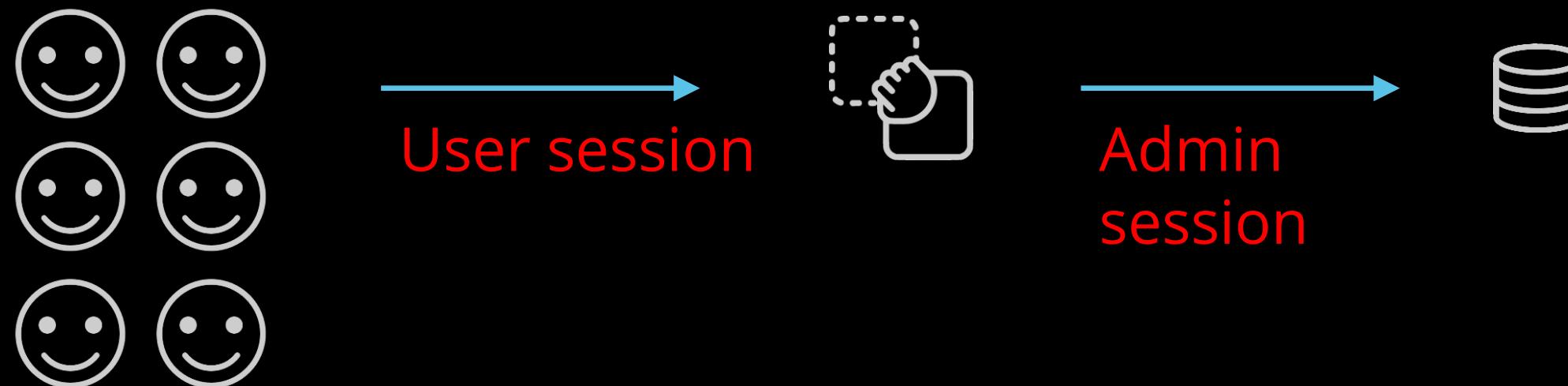
# Self-service – findings

SOC Panics!



# Self-service – findings

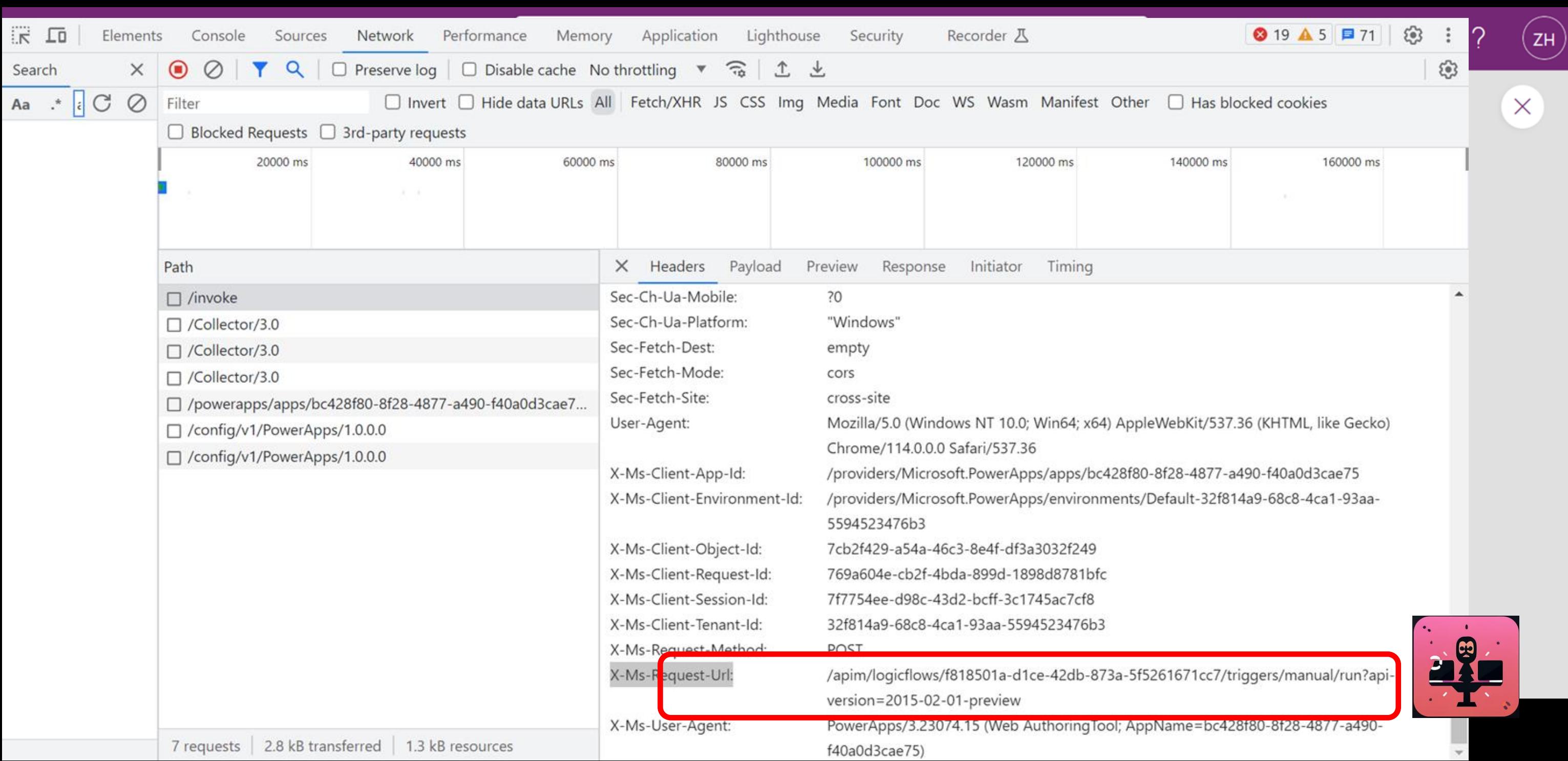
- App embedded with admin ID  
(Account Impersonation)



The screenshot shows a Microsoft Power Apps interface. At the top, there's a purple header bar with the text "Power Apps | Management App" on the left, a search bar in the center containing a magnifying glass icon and the word "Search", and several icons on the right including a globe, a bell, a gear, a question mark, and a language switch set to "ZH". Below the header, the main title "My Management App" is displayed in large black font. Underneath it, a section titled "My Employees" is shown. On the left side of this section is a dropdown menu with "Kris Smith" selected. To the right of the dropdown is a blue "Get Access" button. On the far right, there's a vertical sidebar with icons for a list, a phone, and a calendar, along with a small circular "X" icon. At the bottom of the page, a descriptive text block states: "This app allows you as a manager to take access employee Apps, including employees who have left the organization and reassign them." To the right of this text is a small red square icon featuring a cartoon character sitting at a desk with two monitors.

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

@mbrgO  
BSideLV 2023



The screenshot shows the Network tab of the Google Chrome DevTools. A specific request to the URL `/api/logicflows/f818501a-d1ce-42db-873a-5f5261671cc7/triggers/manual/run?api-version=2015-02-01-preview` is selected. The Headers section is expanded, showing various headers including `X-Ms-Request-Url`, which is highlighted with a red box.

Path	Headers	Payload	Preview	Response	Initiator	Timing
<code>/invoke</code>	<code>Sec-Ch-Ua-Mobile:</code>	<code>?0</code>				
<code>/Collector/3.0</code>	<code>Sec-Ch-Ua-Platform:</code>	<code>"Windows"</code>				
<code>/Collector/3.0</code>	<code>Sec-Fetch-Dest:</code>	<code>empty</code>				
<code>/Collector/3.0</code>	<code>Sec-Fetch-Mode:</code>	<code>cors</code>				
<code>/powerapps/apps/bc428f80-8f28-4877-a490-f40a0d3cae7...</code>	<code>Sec-Fetch-Site:</code>	<code>cross-site</code>				
<code>/config/v1/PowerApps/1.0.0.0</code>	<code>User-Agent:</code>	<code>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)</code>				
<code>/config/v1/PowerApps/1.0.0.0</code>	<code>Chrome/114.0.0.0 Safari/537.36</code>					
	<code>X-Ms-Client-App-Id:</code>	<code>/providers/Microsoft.PowerApps/apps/bc428f80-8f28-4877-a490-f40a0d3cae75</code>				
	<code>X-Ms-Client-Environment-Id:</code>	<code>/providers/Microsoft.PowerApps/environments/Default-32f814a9-68c8-4ca1-93aa-5594523476b3</code>				
	<code>X-Ms-Client-Object-Id:</code>	<code>7cb2f429-a54a-46c3-8e4f-df3a3032f249</code>				
	<code>X-Ms-Client-Request-Id:</code>	<code>769a604e-cb2f-4bda-899d-1898d8781bfc</code>				
	<code>X-Ms-Client-Session-Id:</code>	<code>7f7754ee-d98c-43d2-bcff-3c1745ac7cf8</code>				
	<code>X-Ms-Client-Tenant-Id:</code>	<code>32f814a9-68c8-4ca1-93aa-5594523476b3</code>				
	<code>X-Ms-Request-Method:</code>	<code>POST</code>				
	<code>X-Ms-Request-Url:</code>	<code>/api/logicflows/f818501a-d1ce-42db-873a-5f5261671cc7/triggers/manual/run?api-version=2015-02-01-preview</code>				
	<code>X-Ms-User-Agent:</code>	<code>PowerApps/3.23074.15 (Web Authoring Tool; AppName=bc428f80-8f28-4877-a490-f40a0d3cae75)</code>				

The screenshot shows the Microsoft Edge DevTools Network tab for a "Management App". The title bar includes icons for Power Apps, a search bar, and global navigation.

The main content area displays the title "My Management App". Below it is the Network tab of the DevTools interface. The "Payload" section of a request is highlighted with a red box, showing the JSON content:

```
{email: "zivh@cloudcore.com"}  
email: "zivh@cloudcore.com"
```

The sidebar on the right contains collapsed sections and a small icon at the bottom right.

# Self-service – findings

- App embedded with admin ID (Account Impersonation)
- IDOR (Injection handling failures)



Manipulates  
input

IDOR

# Self-service – findings

- App embedded with admin ID (Account Impersonation)
- IDOR (Injection handling failures)

# Recap:

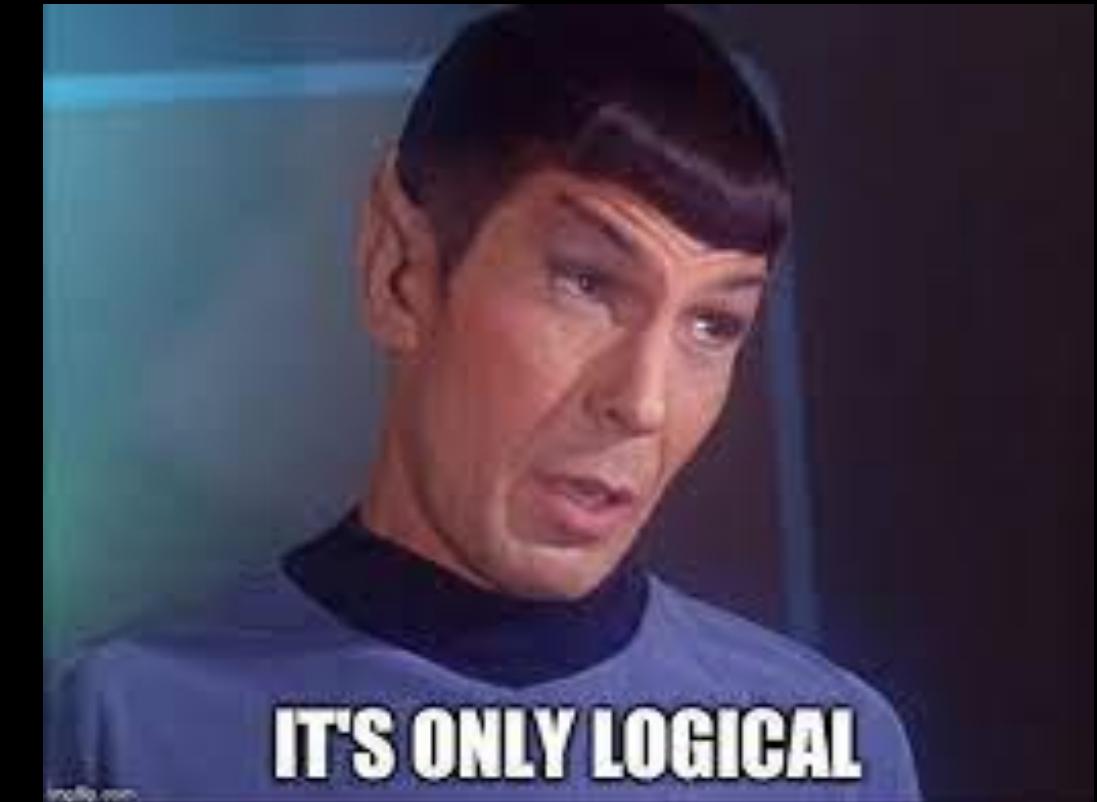
- We are leaving heavy security decisions in the hands of business users
- When choosing between productivity and security, the choice is obvious

## We've given business users:

- **Dev-level power**
- **Missing best practice**
- **No controls**
- **No guardrails**

## We've given business users:

- **Dev-level power**
- **Missing best practice**
- **No controls**
- **No guardrails**



## Could we really expect anything else?



Twitter: @mbrg0

How can we fix it? (Or: LCNC  
AppSec)

# LCNC AppSec is different

AppSec for, well, traditional apps    AppSec for LCNC apps

# LCNC AppSec is different

AppSec for, well, traditional apps

1. Pro devs w/ some awareness

AppSec for LCNC apps

1. Business users w/ no awareness

# LCNC AppSec is different

AppSec for, well, traditional apps

1. Pro devs w/ some awareness
2. Secure SDLC

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC

# LCNC AppSec is different

AppSec for, well, traditional apps

1. Pro devs w/ some awareness
2. Secure SDLC
3. Secure controls

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply

# LCNC AppSec is different

AppSec for, well, traditional apps

1. Pro devs w/ some awareness
2. Secure SDLC
3. Secure controls
4. Hundreds of apps / year

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year

# Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year

# Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year

## Example Attack & Misuse Scenarios - Business Users

### Scenario #1

A developer builds a No Code/Low Code Robotic Process Automation (RPA) application that connects to a database to update records. The connection uses the Admin's authentication (username and password) to log updates. Although 10 different users use this RPA process, all actions are being recorded as being done by the Admin. Logging systems can no longer track productivity, attribute errors to specific users, or identify malicious behavior.

### Scenario #2

A developer builds an application to help the sales team in the field. The developer uses their credentials (username and password) when writing the application, so all sales made through the application are attributed to the developer, not the sales person facilitating the sale.

OWASP LCNC Top 10 sections for business users by John McTiernan and Yianna Paris  
@punk\_fairybread

# Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year

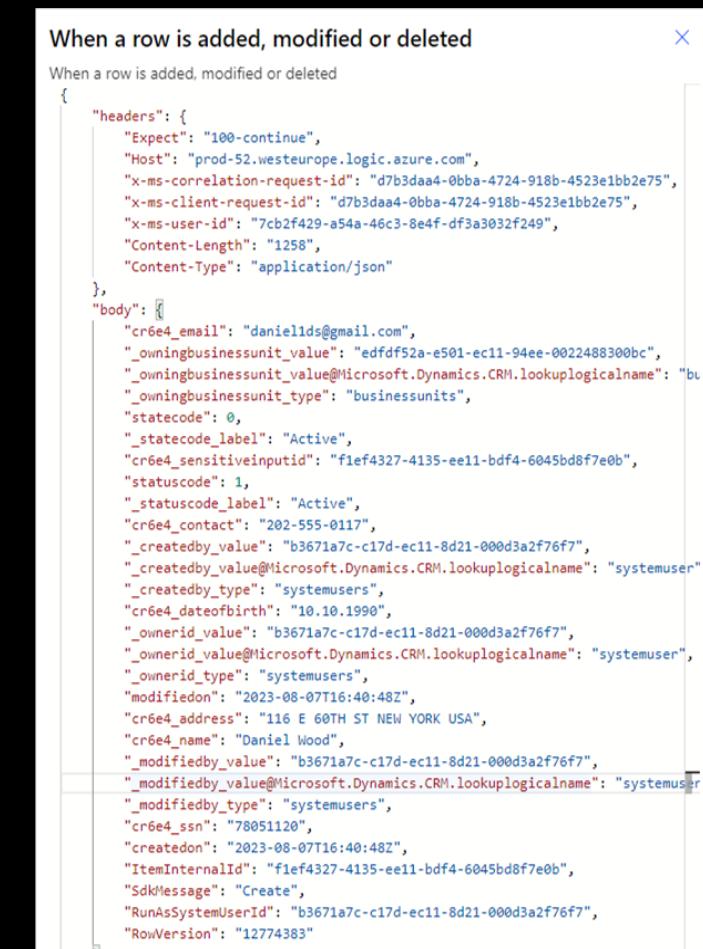
## LCNC Security Standard:

- Approved use cases
- SDLC
- Environments
- Testing
- Monitoring
- SBOM
- ...

# Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year



The screenshot shows a Logic App trigger configuration titled "When a row is added, modified or deleted". The trigger is set to run on a Microsoft Dynamics CRM entity. The JSON code for the trigger is as follows:

```
When a row is added, modified or deleted
{
  "headers": {
    "Expect": "100-continue",
    "Host": "prod-52.westeurope.logic.azure.com",
    "x-ms-correlation-request-id": "d7b3daa4-0bba-4724-918b-4523e1bb2e75",
    "x-ms-client-request-id": "d7b3daa4-0bba-4724-918b-4523e1bb2e75",
    "x-ms-user-id": "7cb2f429-a54a-46c3-8e4f-df3a3032f249",
    "Content-Length": "1258",
    "Content-Type": "application/json"
  },
  "body": {
    "cr6e4_email": "danielids@gmail.com",
    "_owningbusinessunit_value": "edffdf52a-e501-ec11-94ee-0022488300bc",
    "_owningbusinessunit_value@Microsoft.Dynamics.CRM.lookuplogicalname": "bu",
    "_owningbusinessunit_type": "businessunits",
    "statecode": 0,
    "_statecode_label": "Active",
    "cr6e4_sensitiveinputid": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",
    "statuscode": 1,
    "_statuscode_label": "Active",
    "cr6e4_contact": "202-555-0117",
    "_createdby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "_createdby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",
    "_createdby_type": "systemusers",
    "cr6e4_dateofbirth": "10.10.1990",
    "_ownerid_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "_ownerid_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",
    "_ownerid_type": "systemusers",
    "modifiedon": "2023-08-07T16:40:48Z",
    "cr6e4_address": "116 E 60TH ST NEW YORK USA",
    "cr6e4_name": "Daniel Wood",
    "_modifiedby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "_modifiedby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemuser",
    "_modifiedby_type": "systemusers",
    "cr6e4_ssn": "78051120",
    "createdon": "2023-08-07T16:40:48Z",
    "iteminternalid": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",
    "SdkMessage": "Create",
    "RunAsSystemUserId": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "RowVersion": "12774383"
  }
}
```

LCNC is an opportunity for more visibility than ever before

# Take the opportunity to champion LCNC security in your org

AppSec for LCNC apps

1. Business users w/ no awareness
2. No SDLC
3. Most controls don't apply
4. 10x-100x more apps / year





Learn more: [github.com/mbrg/talks](https://github.com/mbrg/talks)  
Twitter: @mbrg0

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

Michael Bargury @ Zenity  
BSidesLV 2023