



AUGUST 9-10, 2023

BRIEFINGS

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

Michael Bargury @mbrg0

Zenity



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



darkreading.com/author/michael-bargury



Agenda

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



The background of the slide features a dark blue gradient with a complex, glowing network of blue and white lines and dots, resembling a digital or quantum state.

Enterprise LCNC – **EVERYONE** is a developer

@mbrg0

#BHUSA @BlackHatEvents

Business Needs

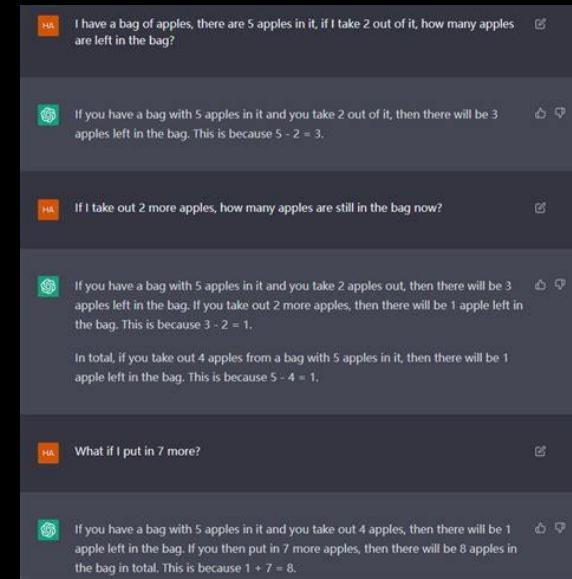
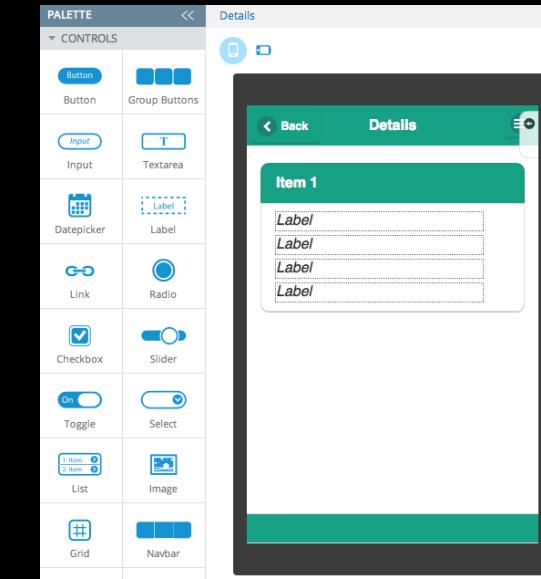
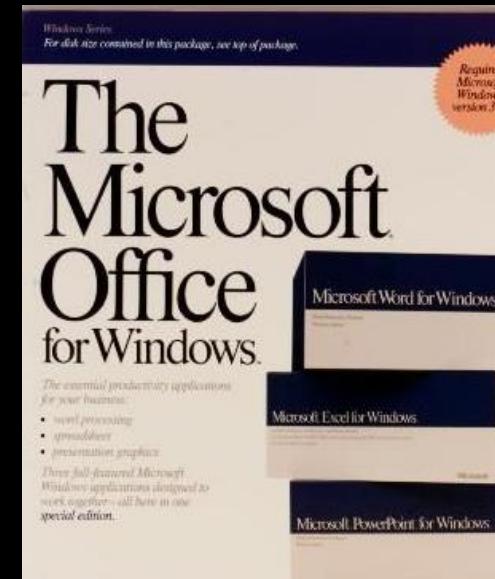


IT Capacity





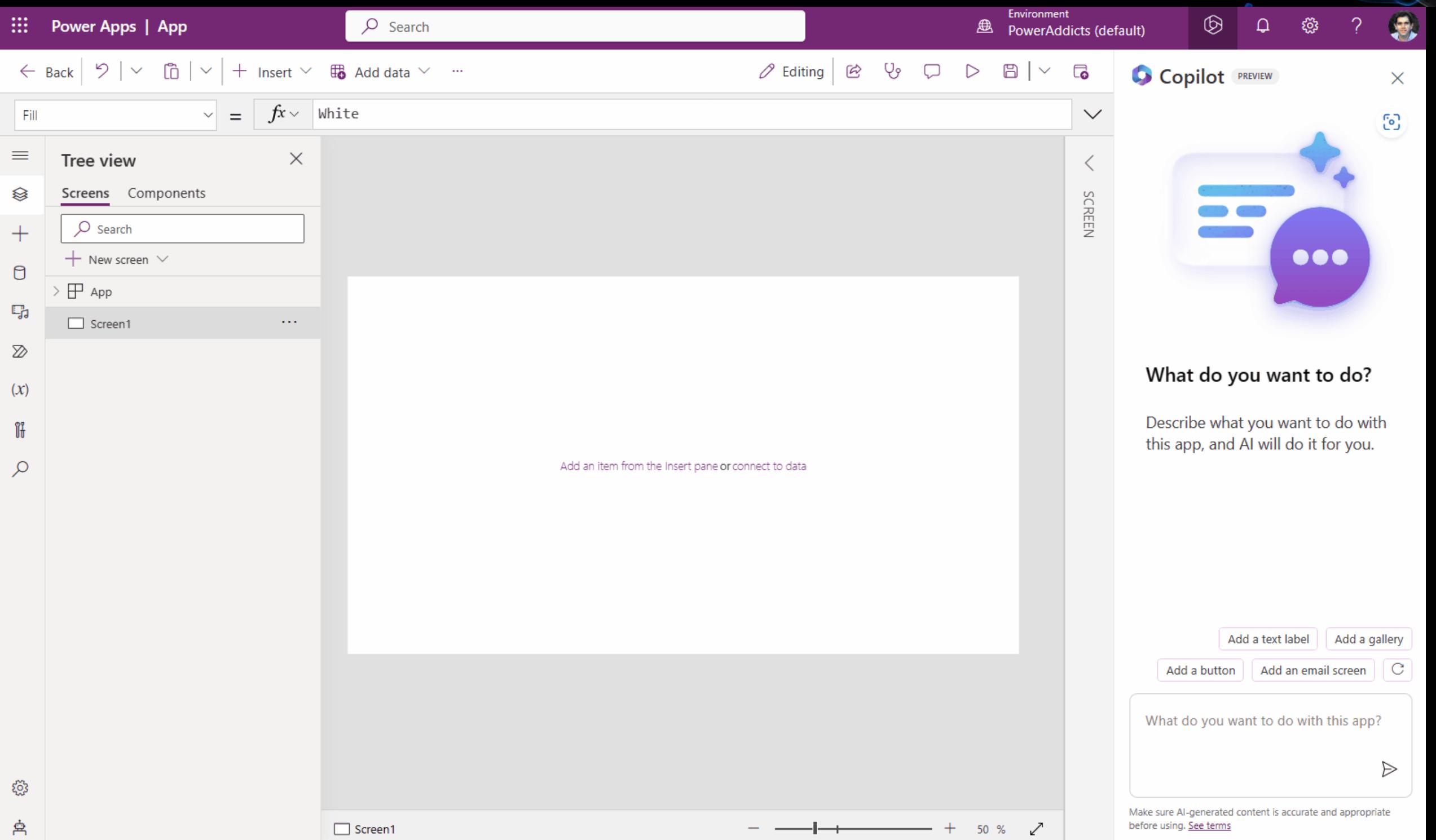
If this sounds familiar, its because it is



Tech evolution

@mbrg0

#BHUSA@BlackHatEvents



A screenshot of the Microsoft Power Apps studio interface. The top navigation bar shows "Power Apps | App" and "Search". The environment is set to "PowerAddicts (default)". The main workspace is titled "Screen" and contains a large, empty white area with the placeholder text "Add an item from the Insert pane or connect to data". To the left, a "Tree view" sidebar shows a "Screens" tab selected, with a search bar and a "New screen" button. Below it, there's a section for "App" and "Screen1". The bottom of the workspace shows a progress bar at 50% completion. On the right side of the screen, a "Copilot" preview window is open, featuring a purple speech bubble icon and the text "What do you want to do?". It also includes buttons for "Add a text label", "Add a gallery", "Add a button", "Add an email screen", and a "Copilot" button. A message at the bottom of the Copilot window reads: "Make sure AI-generated content is accurate and appropriate before using. [See terms](#)".

Source:
@RezaDorrani

@mbrg0

#BHUSA@BlackHatEvents

COVID health check app by Microsoft

<https://aka.ms/healthcheck>

The screenshot shows the Microsoft COVID-19 check app landing page. At the top, there's a blue header bar with the Microsoft logo and a message about sign-in requirements starting June 1, 2022. Below the header, a large heading says "Take the daily COVID-19 check". There's an illustration of a smartphone connected to a computer monitor displaying a shield with a heart rate graph, and a green circle with a checkmark. Below the illustration, text explains the purpose of the check and displays the user's current location as Giv'atayim, Tel Aviv, Israel. A "Get started" button is at the bottom left, and footer links and copyright information are at the bottom right.

@mbrg0

#BHUSA@BlackHatEvents



 Microsoft | Inside Track Search content Audience ▾ Topic ▾ Content Suites Videos Blog Careers

How citizen developers modernized Microsoft product launches

Mar 20, 2020 | Serah Delaini

[f](#) [t](#) [in](#) [p](#)



Product launch management

* This is an example of a business-critical app built by a citizen developer. We did not search for or identify any security vulnerabilities in this app.

<https://www.microsoft.com/insidetrack/blog/how-citizen-developers-modernized-microsoft-product-launches/>

@mbrg0

#BHUSA@BlackHatEvents



Financial risk management

- Facilitates the process of credit assignment
- Determines whether or not a person is assigned credit
- Streamlines risk assessment and decision-making

* This is an example of a business-critical app built by a citizen developer. We did not search for or identify any security vulnerabilities in this app.



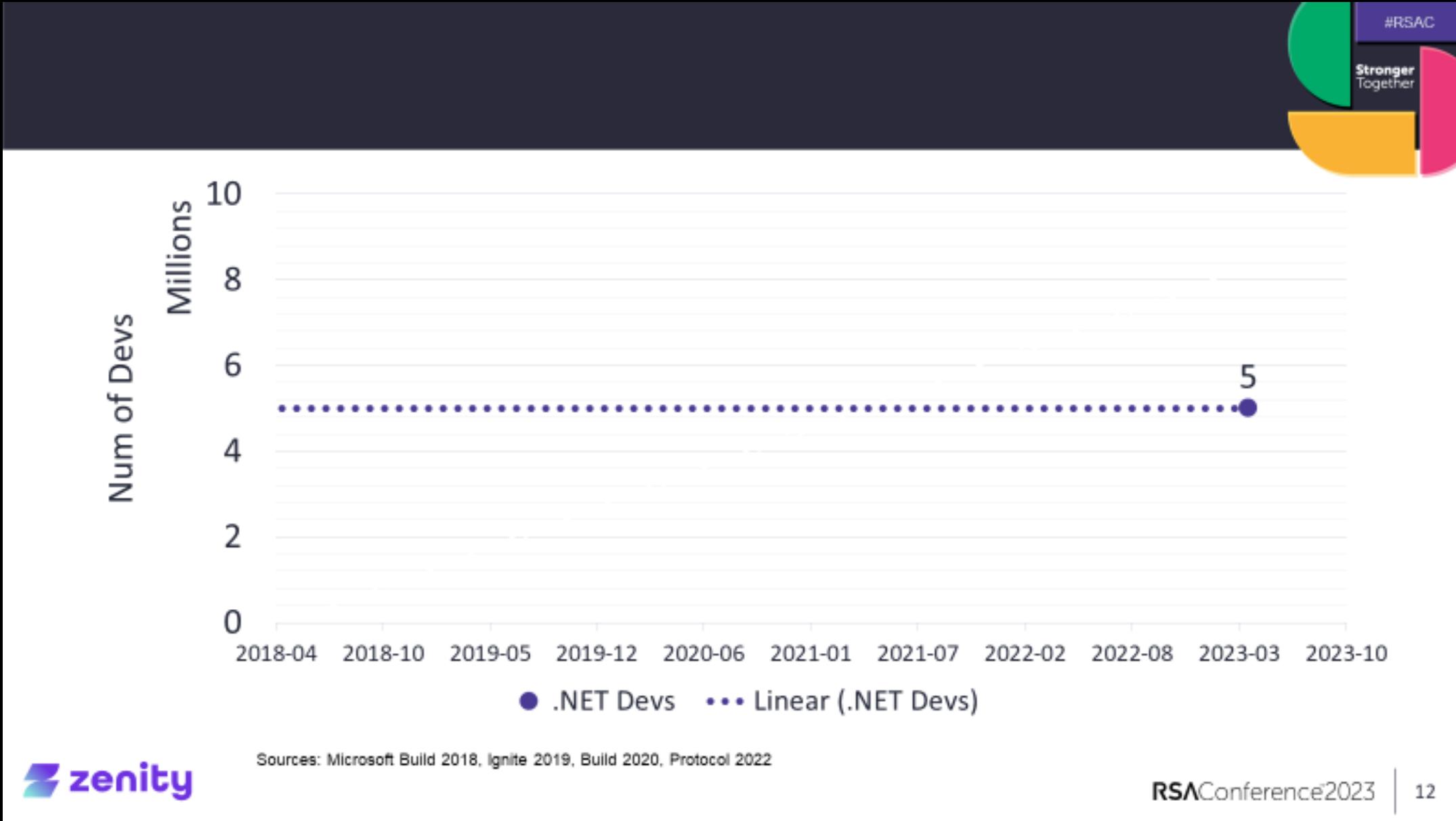
Your business is already there, it's time for security to keep up.



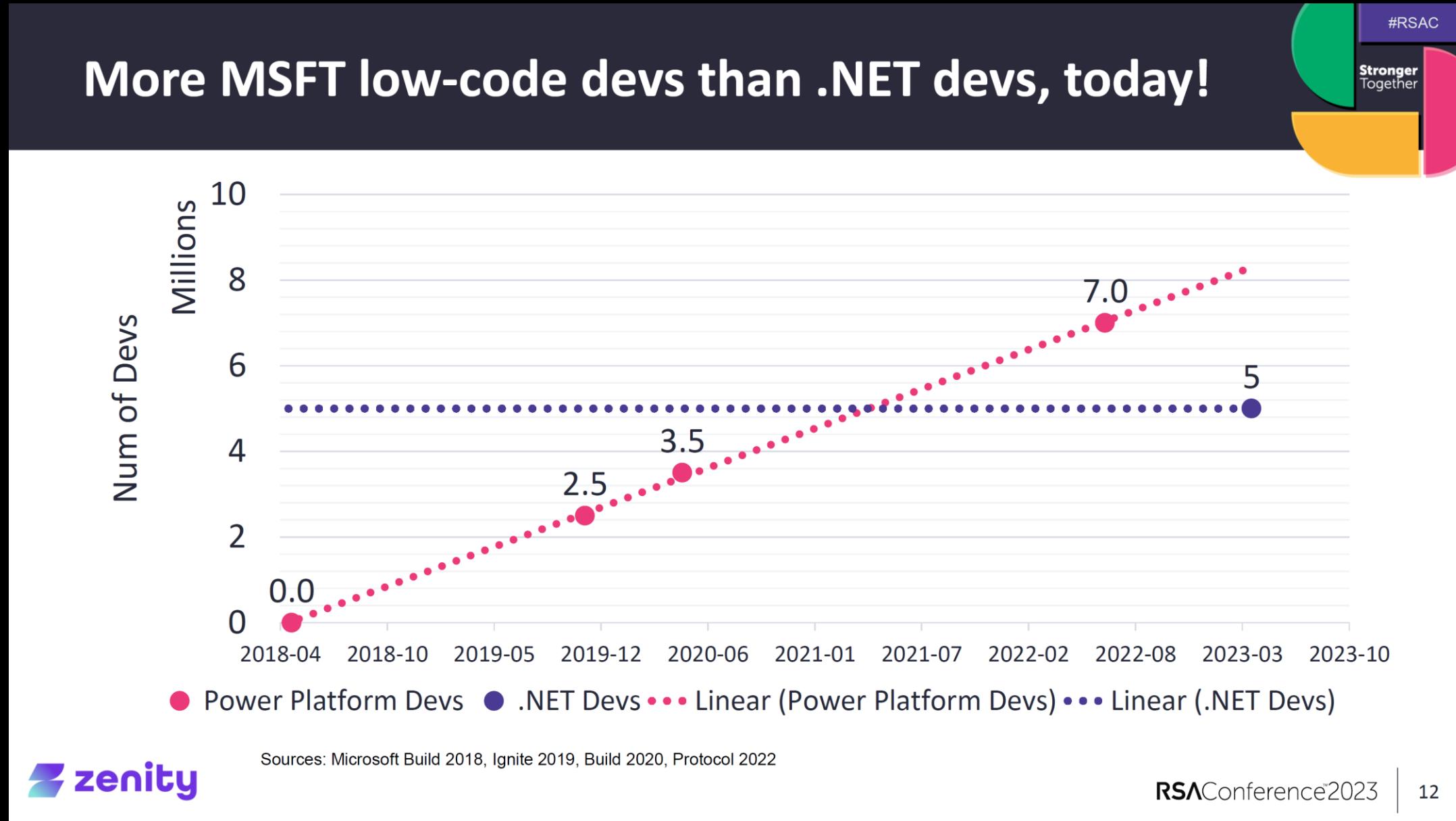
@mbrg0

#BHUSA@BlackHatEvents

Is this actually being used?



~8M active Power devs today!



A single F500 organization

Exponential Growth in Business Development



Michael Bargury
BSidesSF 2023

@mbrg0



Recap: You can't opt out of citizen development

- The next big productivity boost (Excel-level impact)
- Powers critical business workflows, predicted to power 70% of enterprise apps by 2025
- Available on every major enterprise, yours too
- Millions of new (business) developers and growing fast



A large, abstract graphic in the upper right corner consists of glowing blue and white lines forming a complex, organic shape against a dark background. Small orange dots are scattered throughout the lines.

What could go wrong?

@mbrg0

#BHUSA @BlackHatEvents



OWASP LCNC Top 10

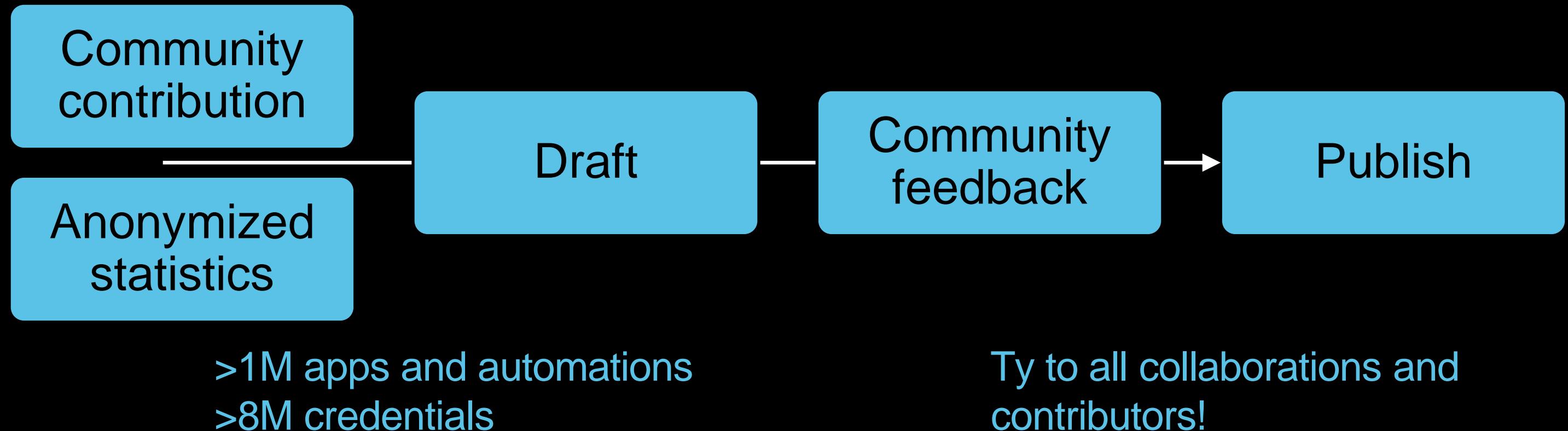
- LCNC-SEC-01: Account Impersonation
- LCNC-SEC-02: Authorization Misuse
- LCNC-SEC-03: Data Leakage and Unexpected Consequences
- LCNC-SEC-04: Authentication and Secure Communication Failures
- LCNC-SEC-05: Security Misconfiguration
- LCNC-SEC-06: Injection Handling Failures
- LCNC-SEC-07: Vulnerable 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



@mbrg0

#BHUSA@BlackHatEvents

Methodology loop





Real-world stories

@mbrg0

#BHUSA @BlackHatEvents



Story #1 - employee onboarding

@mbrg0

#BHUSA @BlackHatEvents

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

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



SQL

Start from a SQL data source to create a three-screen-app



Image

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





Home

Create

Learn

Apps

Tables

Connections

Solutions

Flows

More

Power Platform

Ask a virtual agent

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



SQL

Start from a SQL data source to create a three-screen-app



Image



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



Power Apps | Employee Onboarding

 Search



← Back ⌂ | ▼ | 🗑️ | ▼ | + Insert ▼ | 📈 Add data ▼ ...

Editing |

Fill \vee \equiv \neg $fx \vee$ White

▽

Tree view

Screens Components

 Search

+ New screen ▾

>  App

Screen1

Label2_4

TextInput1_5

 Textinput_1

 LblAppName3_1

A small icon consisting of a red heart above a green checkmark, with a circular arrow symbol to the right.

IconCancel1_1

Label2 3

Employee onboarding form

Full legal name	<input type="text"/>
Address	<input type="text"/>
Date of birth	<input type="text"/>
Personal email	<input type="text"/>
Phone number	<input type="text"/>
Social Security Number	<input type="text"/>

Save

SCREEN ?

Screen1

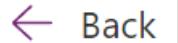
Properties

Fill

Background image

Image position

A teal rounded square containing a black cartoon character with large white eyes and a small orange mouth.

 Back |  |  |  Insert |  Add data | ... Editing |      |  

Fill ▾

= fx ▾

White

▼



Data



+ 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

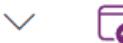
None



Image position

Fit



 Back    Insert  Add data  Editing      Fill  =  White

Data

 Search

 Add data 

 Sensitive Inputs
Microsoft Dataverse - Current environment

Employee onboarding form

Full legal name	<input type="text"/>
Address	<input type="text"/>
Date of birth	<input type="text"/>
Personal email	<input type="text"/>
Phone number	<input type="text"/>
Social Security Number	<input type="text"/>

Save

SCREEN 

Screen1

Properties

Advanced

Ideas

Fill

None

Background image

Fit

Image position



[← Back](#) | | | | | Insert | Add data | ...

Editing | |

Fill

Data

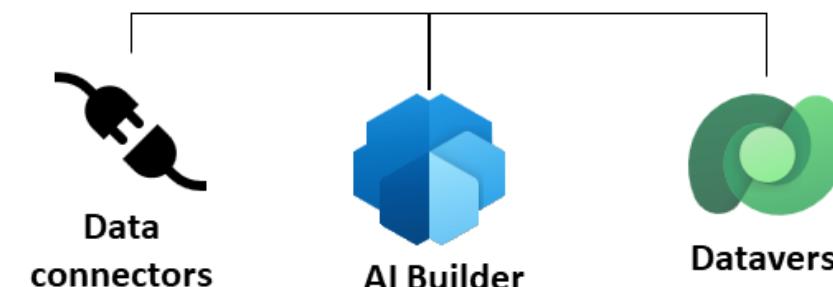
Search

Add data

 Sensitive Inputs
Microsoft Dataverse

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

Ideas



None



Fit





Power Automate

Search

Environments
Zenity Stage (default)

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Ask a chatbot

Update Employee Info in HR system

When a row is added, modified or deleted

Send email (V2)

To: hrorg@cloudcore.com

Subject: New Employee Update info

Body:

Font: 12, B, I, U,

SSN, Contact, Email, Address, Employee Name

Attachments Name - 1: Title of the attachment.

Attachments Content - 1: Body of the attachment.

Attachments Content - Type - 1: Type of content in the attachment.

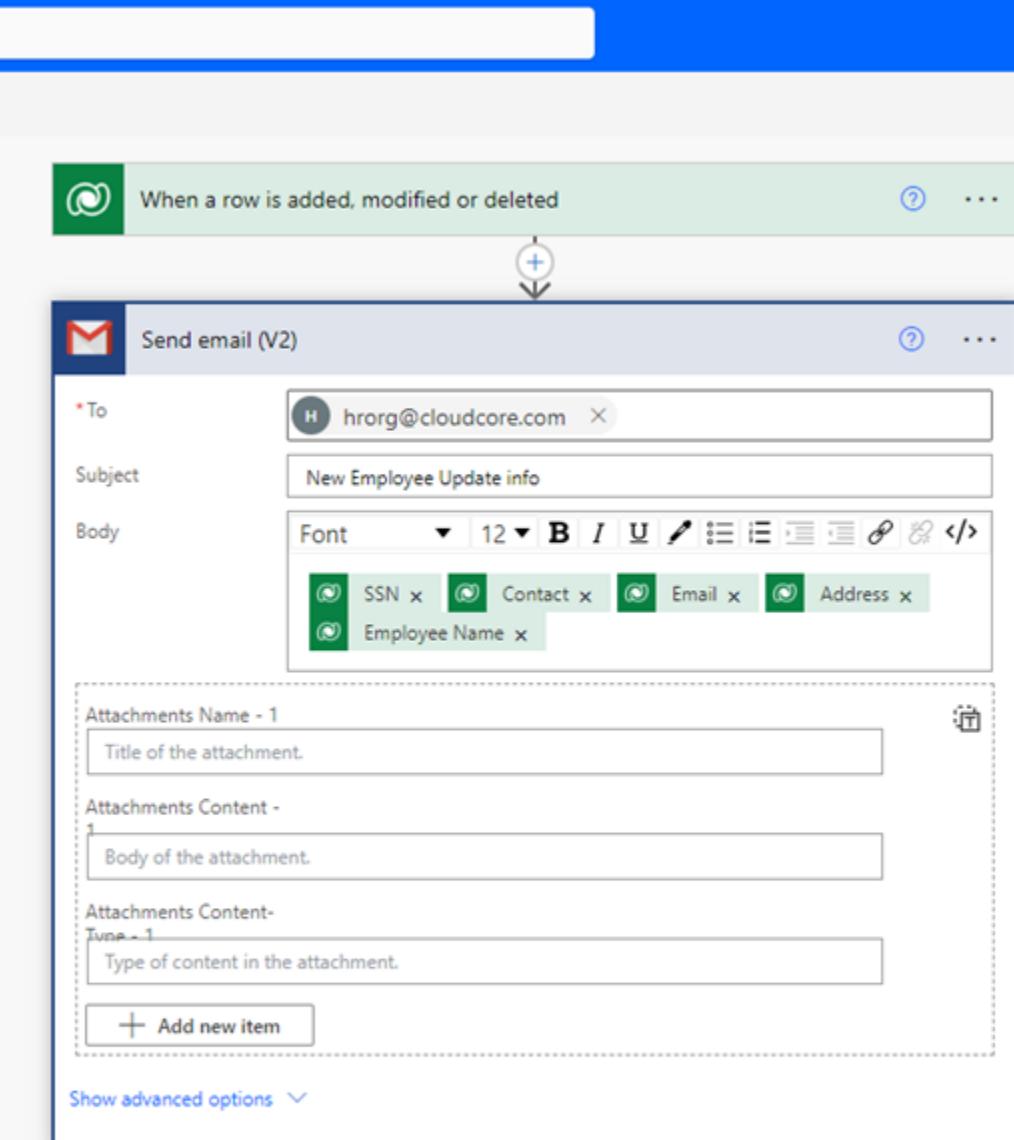
+ Add new item

Show advanced options

+ New step

Save

Undo Redo Comments Save Flow checker Test





Employee onboarding – findings



Employee onboarding form

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security
Number



Save





Power Apps

Search

Environment
Zenity Stage (default)

New table Import Export

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	

Ask a virtual agent



Power Apps

Search

Environment
Zenity Stage (default)

KS

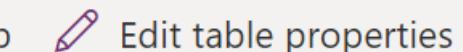
[+ New table](#) [Open](#) [Edit](#) [Import](#) [Export](#) [Properties](#) [...](#)

Search

[Home](#)[Create](#)[Learn](#)[Apps](#)[Tables](#)[Connections](#)[Solutions](#)[Flows](#)[More](#)[Power Platform](#)[Ask a virtual agent](#)

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



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

Data saved

 Abc Employee Name * ↑ ↓ Abc SSN ↓ Abc Address ↓ Abc 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)





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





Power Automate

Search

Environments
Zenity Stage (default)

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Ask a chatbot

Update Employee Info in HR system

When a row is added, modified or deleted

Send email (V2)

To: hrorg@cloudcore.com

Subject: New Employee Update info

Body:

Font: 12, B, I, U,

SSN, Contact, Email, Address, Employee Name

Attachments Name - 1: Title of the attachment.

Attachments Content - 1: Body of the attachment.

Attachments Content - Type - 1: Type of content in the attachment.

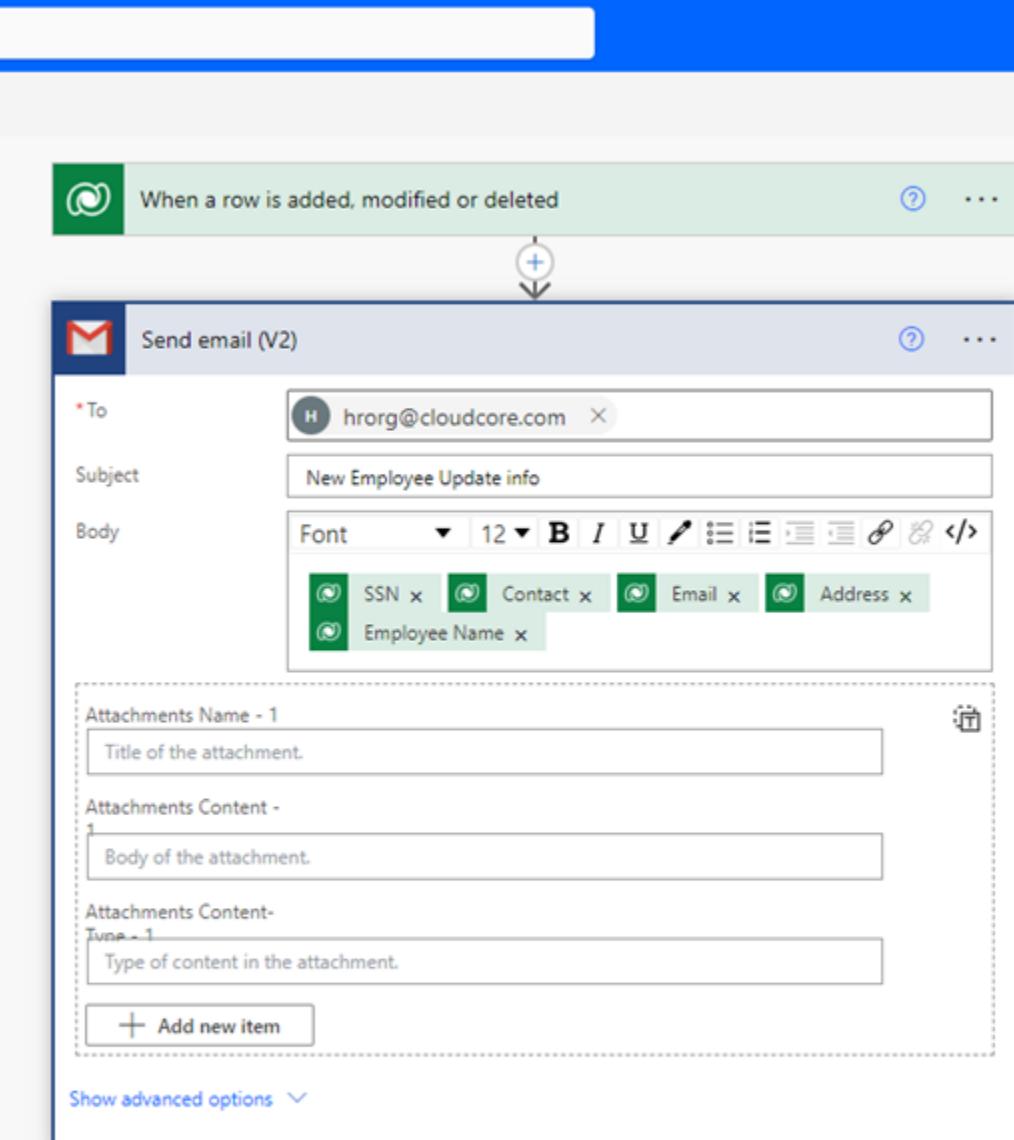
+ Add new item

Show advanced options

+ New step

Save

Undo Redo Comments Save Flow checker Test





Power Automate Search Environments Zenity Stage (default) ? ZH

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

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

Outputs:

```
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



Power Automate

Search

Environments
Zenity Stage (default)

?

ZH

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

Ask a chatbot

Update Employee Info in HR system

Edit

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

A red rectangular box highlights the "HR-All" entry in the "Add a user or group as owner" section.





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": "daniel1ds@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)



Story #2 – productivity sync

@mbrg0

#BHUSA @BlackHatEvents



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 X

Subject



Subject X

Body



Font



Body X

Attachments



Attachments X

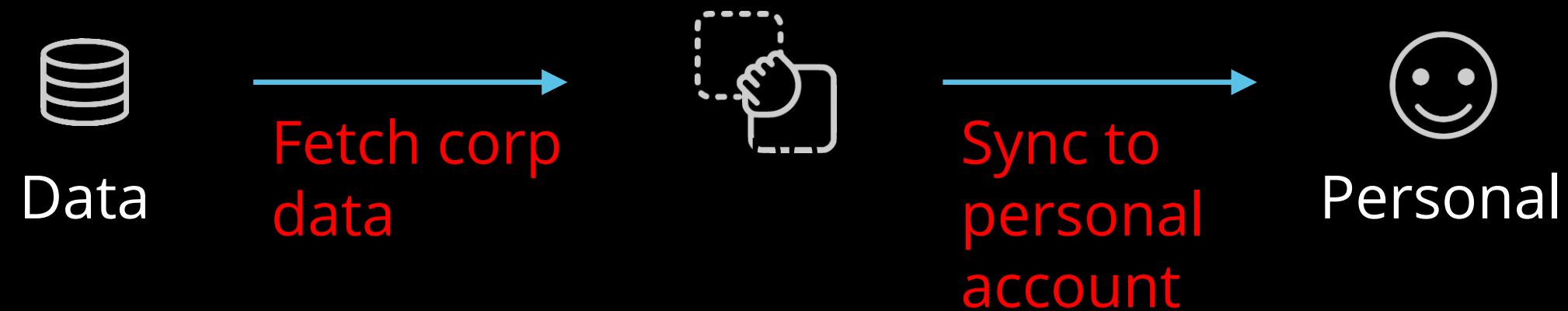




Productivity sync – findings

Productivity sync – findings

- Business data to personal account (Data Leakage)





Back | ↻ | ⏪ | ⏩ | + Insert | Open Sans | 15 | Semibold | ...

Editing |       | 

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

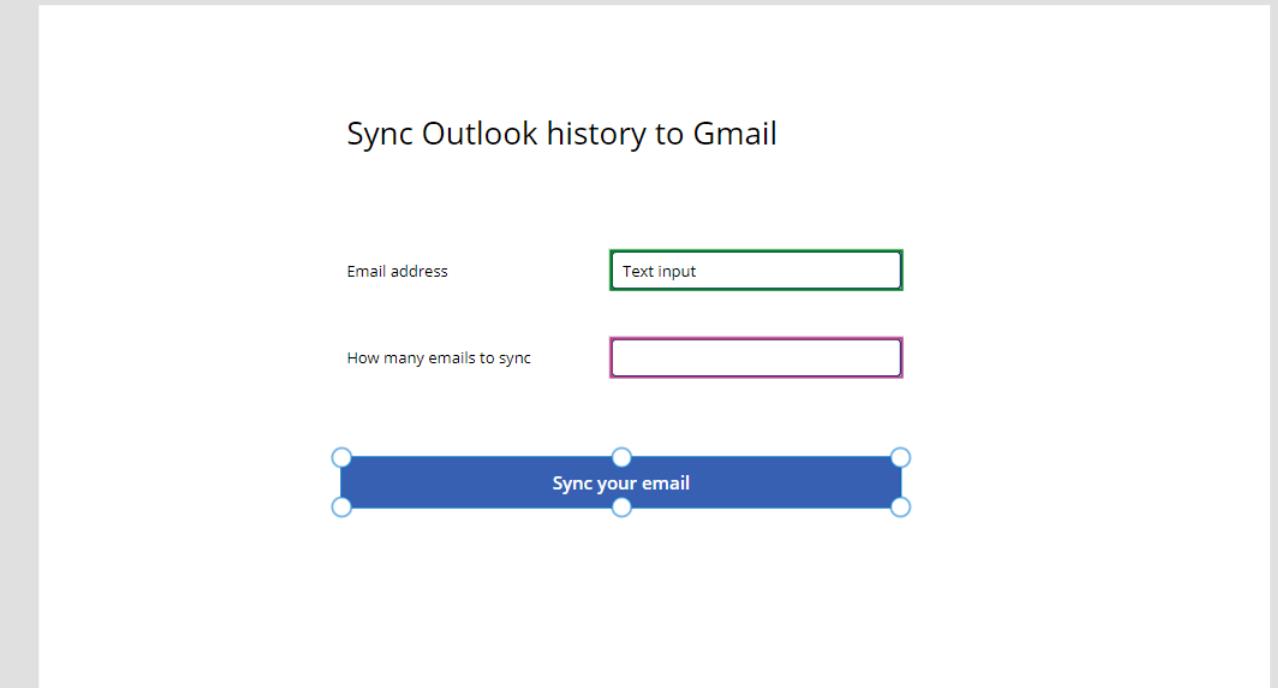
Power Automate X

Search

Add flow

In your app

Sync Outlook history to Gmail



BUTTON ? >

Button1

Properties Advanced Ideas

Search for a property ...

ACTION

OnSelect

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

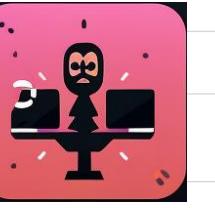
DATA

Text

"Sync your email"

Tooltip

""





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

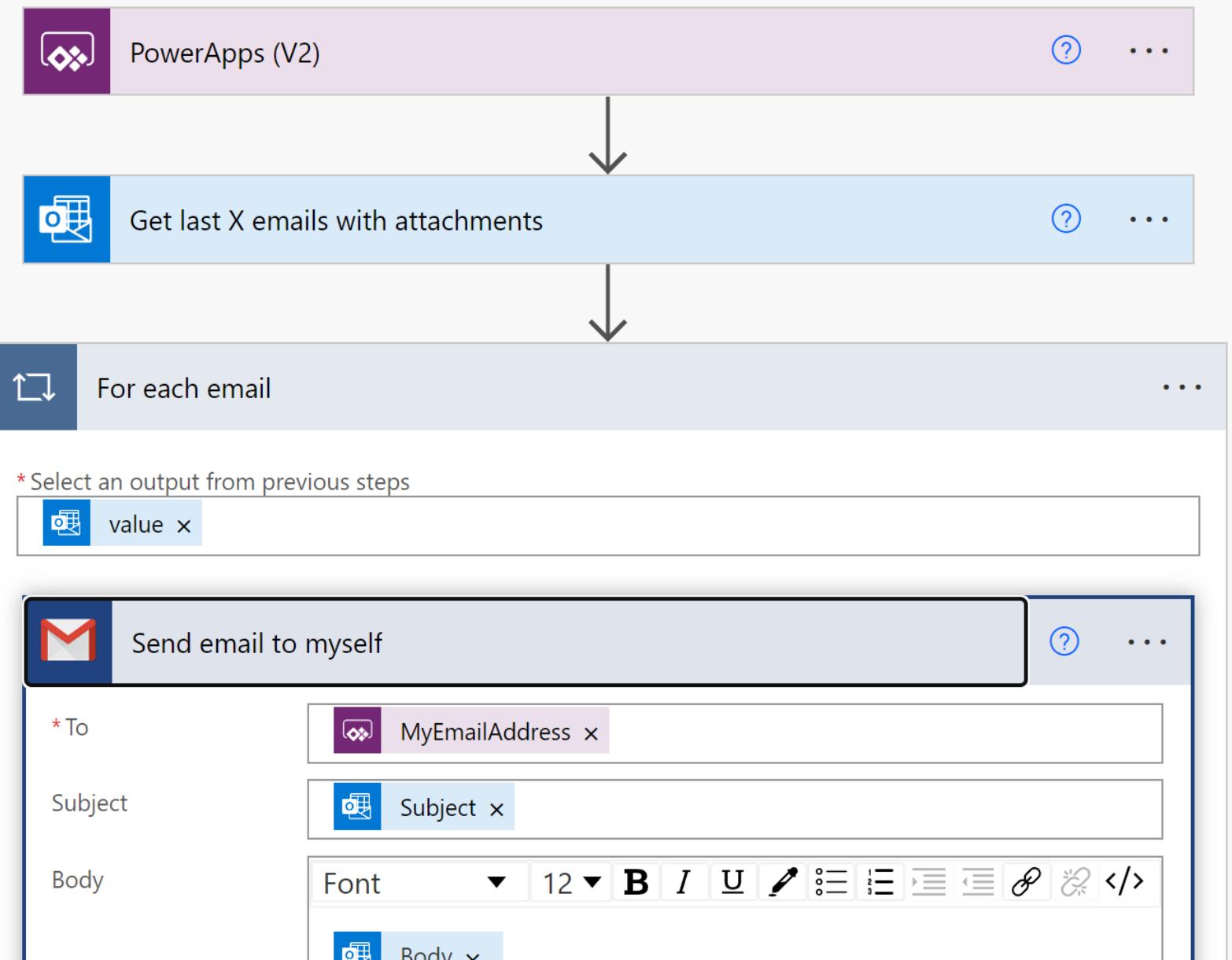
Monitor

AI Builder

Process mining

Solutions

Learn







Power Apps

Search

Edit Play Share

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

Apps > Set up your email sync

Details Versions Owner Kris Smith

Description Not provided

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

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

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

Mobile QR code



Share Set up your email sync

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

Enter a name, email address, or Everyone

New users

EC Everyone in CloudCore User

Shared with

Kris Smith Owner

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 *i*

Logic flows

Office 365 Outlook

Gmail

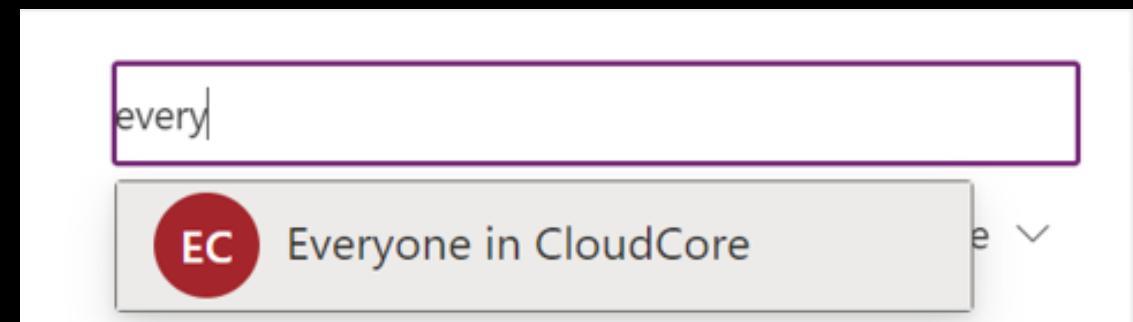
Send an email invitation to new users



Productivity sync – findings

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

Everyone means
EVERYONE, including
guests by-default



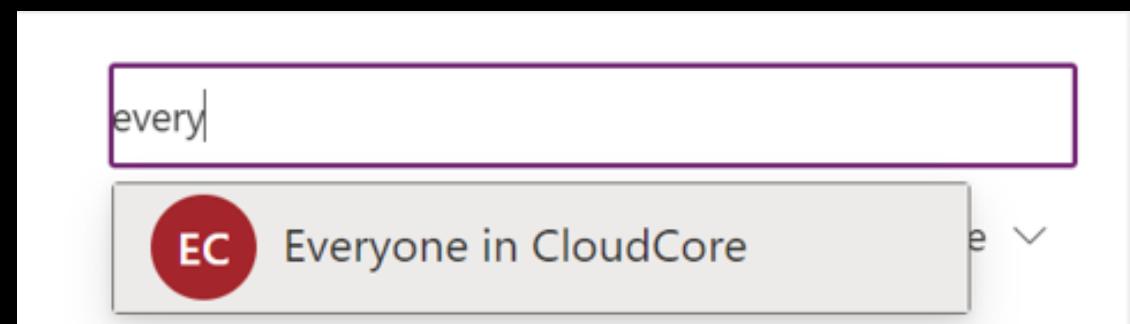


Productivity sync – findings

- 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!





Almost there ...

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



Office 365 Outlook
admin@zenitystage.com
Signed in [View permissions](#)



Gmail
maortzury@gmail.com
Signed in

[Switch account](#)

[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





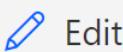
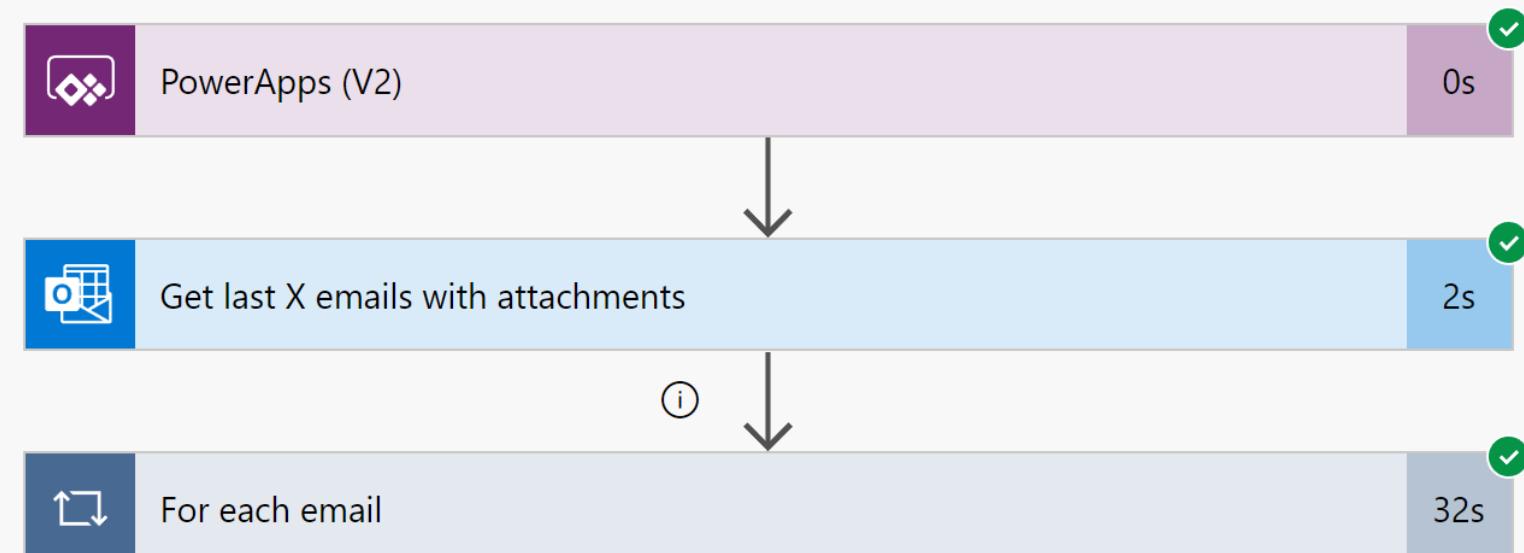
Power Automate

Search

Environments
Zenity Stage (default)

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



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

Home

Approvals

My flows

Create

Templates

Connectors

Data

Monitor

AI Builder

Process mining

Solutions

Learn

For each email 5s

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

 Send email to myself 1s

INPUTS Show raw inputs >

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
}
```



Productivity sync – findings

- Data 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](#)



Gmail
maortzury@gmail.com
Signed in

[Switch account](#)

[Switch account](#)

[Allow](#) [Don't Allow](#)



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)



Story #3 – self-service

@mbrg0

#BHUSA @BlackHatEvents



What happens when a maker leaves the org?



What happens when a maker leaves the org?

- Asset Management Failures



Power Apps | Management App

Search



ZH

My Management App

My Employees

Kris Smith



Get Access



This app allows you as a manager to take access employee Apps, including employees who have left the organization and reassign them.





Power Automate

Search

Environments
Zenity Stage (default)

Undo Redo Comments Save Flow checker Test

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

Get Access to Employee Apps

PowerApps (V2)

Email Please enter an e-mail address

+ Add an input

Get Apps

Apply to each 2

Apply to each 3

+ New step Save

Ask a chatbot

A small teal icon with a white cartoon face and a speech bubble is located in the bottom right corner.

```
graph TD; PowerApps[PowerApps (V2)] --> GetApps[Get Apps]; GetApps --> Apply1[Apply to each 2]; Apply1 --> Apply2[Apply to each 3]
```



Power Automate

Search

Environments
Zenity Stage (default)

Undo Redo Comments Save Flow checker Test

Get Access to Employee Apps

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

Apply to each

Set App Owner

*Environment Name properties/envi... x

*PowerApp Name name x

API Version 2016-11-01

Content Type application/json

Role For Old App Owner CanView

New PowerApp Owner email x

Add an action





Power Automate Search Environments Zenity Stage (default)   

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

Get Access to Employee Apps

PowerApps (V2) Email Add an input

Apply to each 3 Select an output from previous steps value

Apply to each Select an output from previous steps value email

Set App Owner Environment Name: properuseenv... 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

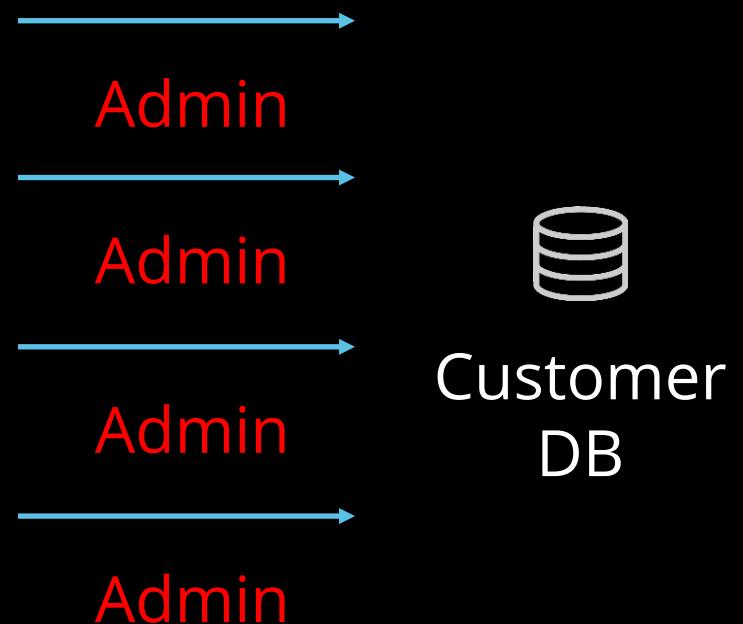
A red box highlights the "Set App Owner" step.



Self-service – findings

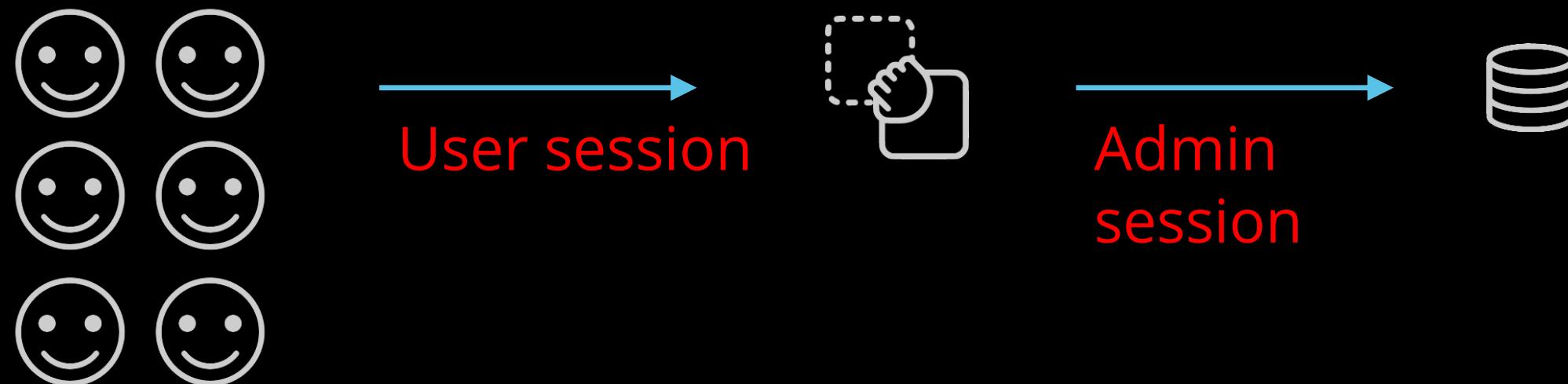
Self-service – findings

SOC Panics!



Self-service – findings

- App embedded with admin ID
(Account Impersonation)





Power Apps | Management App

Search



ZH

My Management App

My Employees

Kris Smith



Get Access



This app allows you as a manager to take access employee Apps, including employees who have left the organization and reassign them.



Screenshot of the Network tab in the Chrome DevTools developer console, showing a request to the endpoint `/api/apim/logicflows/f818501a-d1ce-42db-873a-5f5261671cc7/triggers/manual/run?api-version=2015-02-01-preview`.

The Headers section shows the following details:

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

A red box highlights the `X-Ms-Request-Url` header value.



My Management App

Elements Console Sources **Network** Performance Memory Application Lighthouse Security Recorder   19  5  71  

Search     Preserve log Disable cache No throttling  Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other
 Has blocked cookies Blocked Requests 3rd-party requests

Timing: 500 ms 1000 ms 1500 ms 2000 ms 2500 ms 3000 ms 3500 ms 4000 ms 4500 ms

Path	Headers	Payload	Preview	Response	Initiator	Timing
<input type="checkbox"/> /invoke <input type="checkbox"/> /Collector/3.0		 view source	 ▼ {email: "zivh@cloudcore.com"} email: "zivh@cloudcore.com"			

2 requests | 1.4 kB transferred | 0 B resources



Self-service – findings

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





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

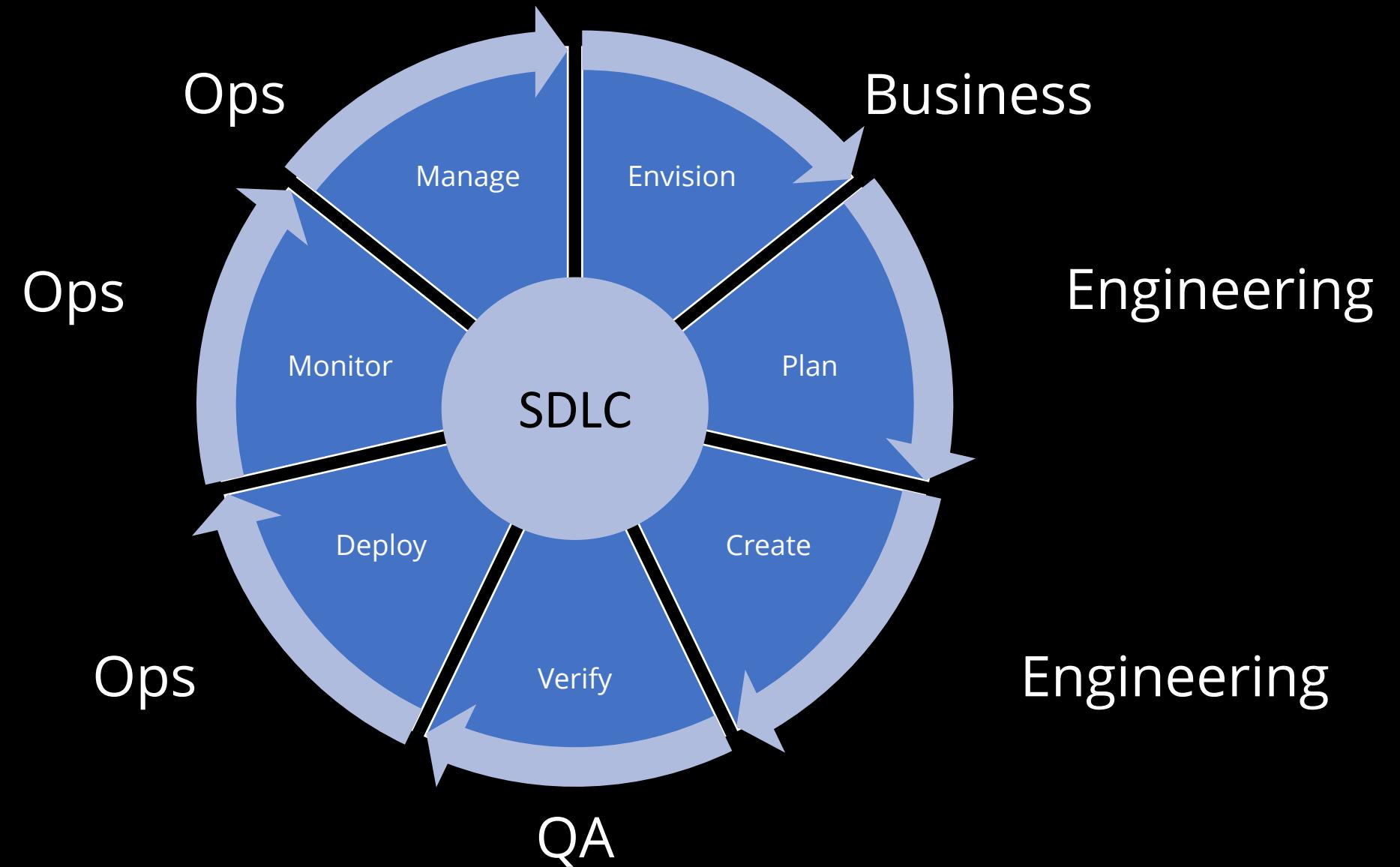


Why does it go wrong?

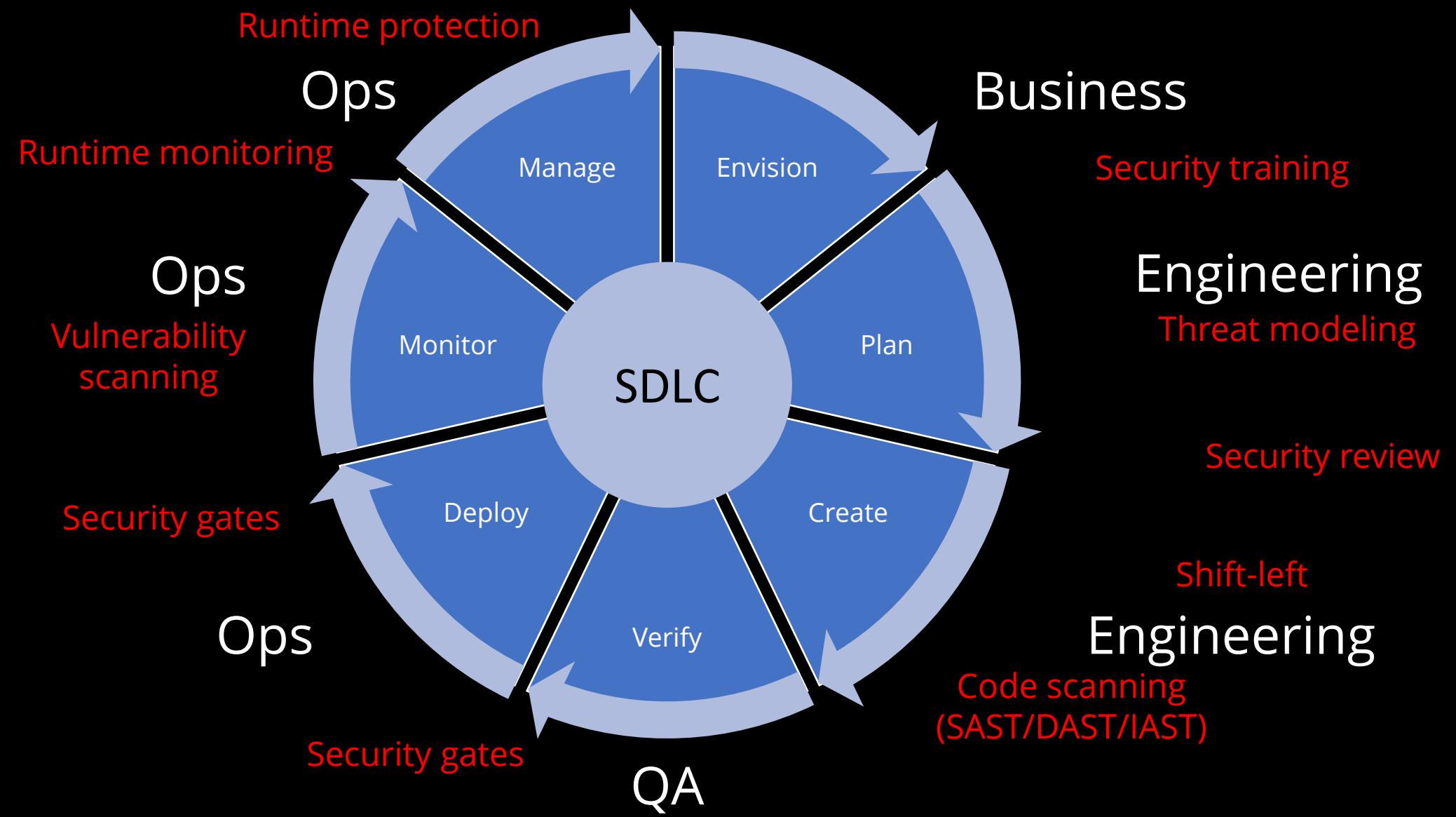
@mbrg0

#BHUSA @BlackHatEvents

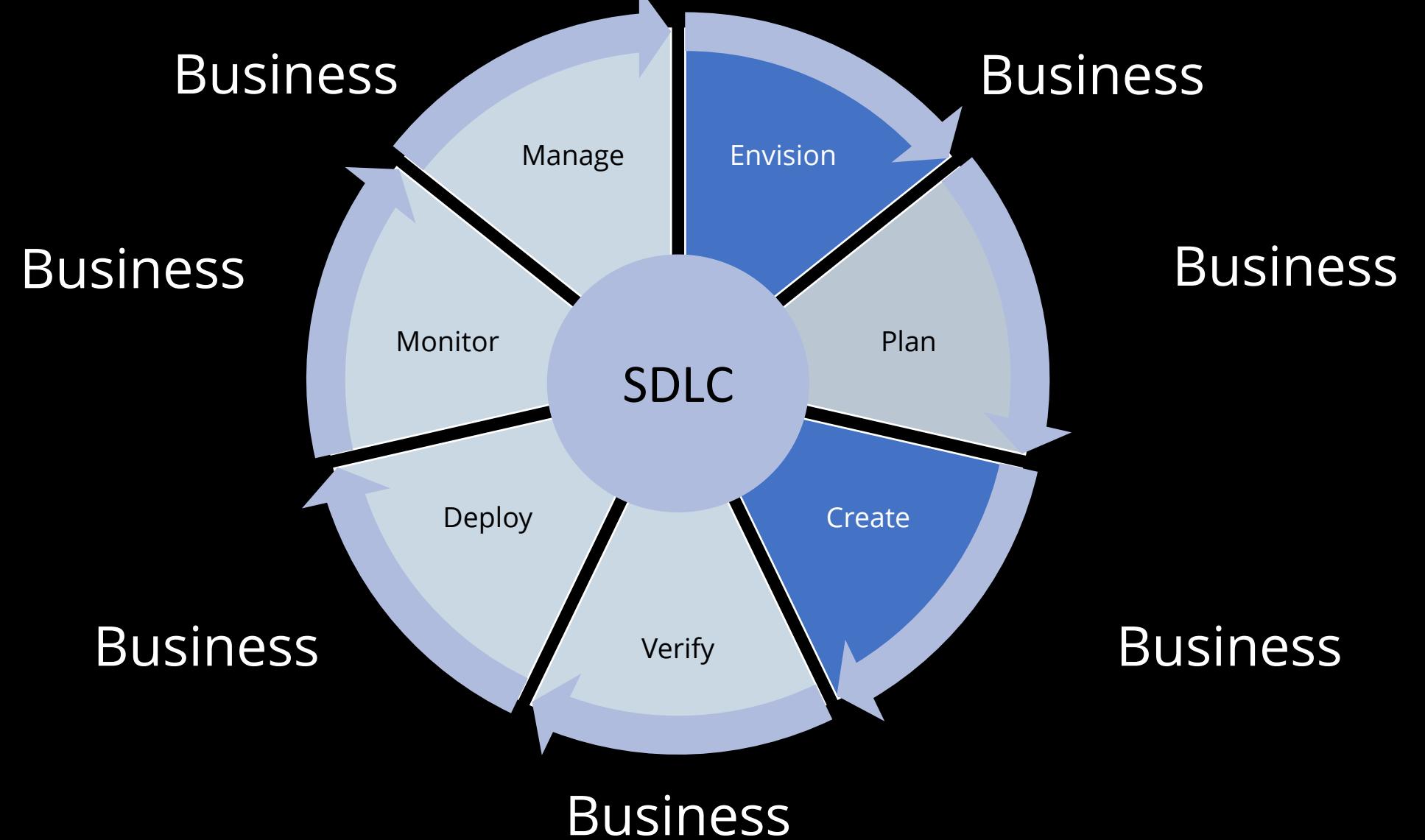
Pro Code SDLC



Pro Code SDLC



No Code No SDLC?





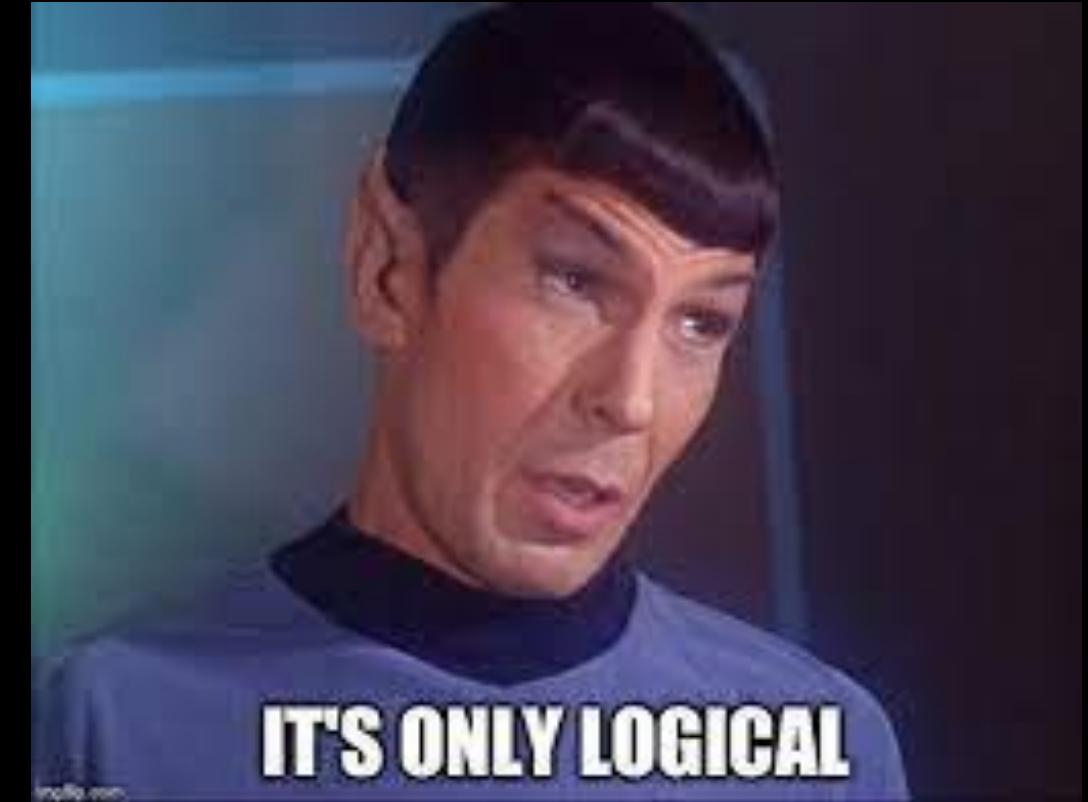
We've given business users:

- **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?

@mbrg0

#BHUSA@BlackHatEvents



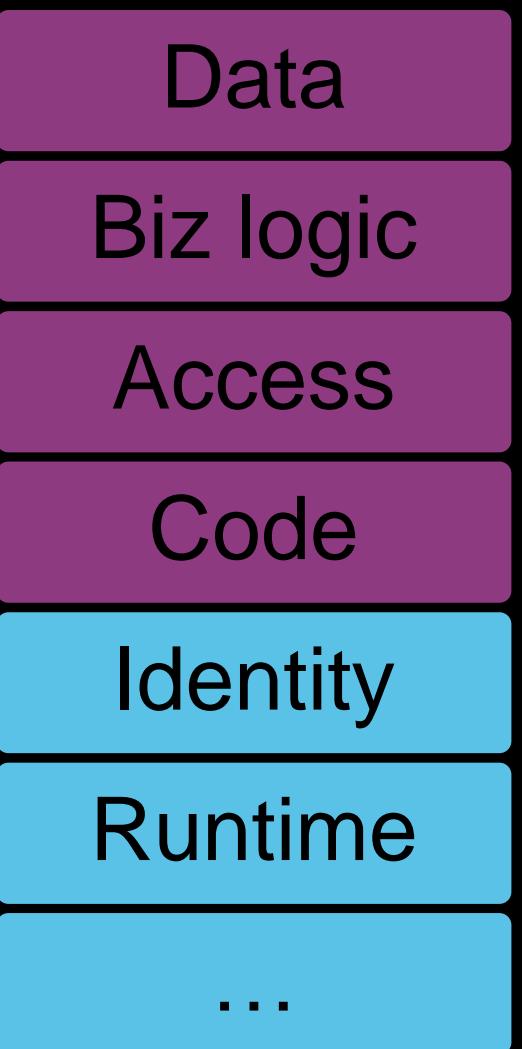
The LCNC Shared Responsibility Model

@mbrg0

#BHUSA @BlackHatEvents



Serverless

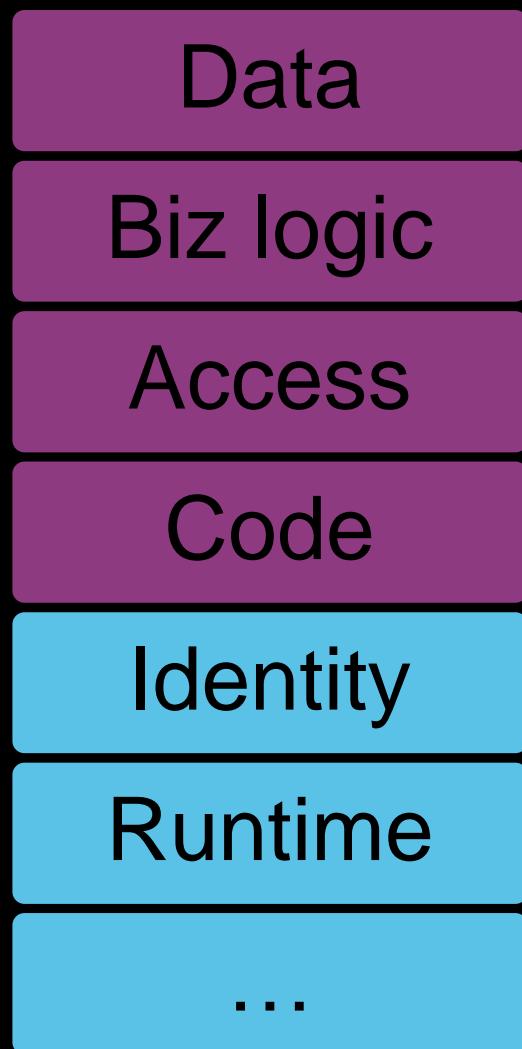


Customer

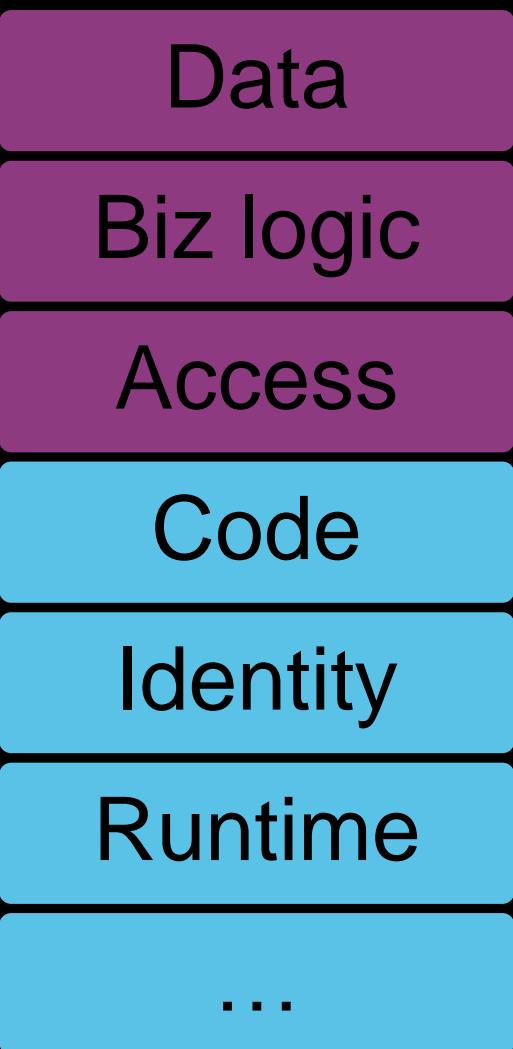
Platform



Serverless



LCNC



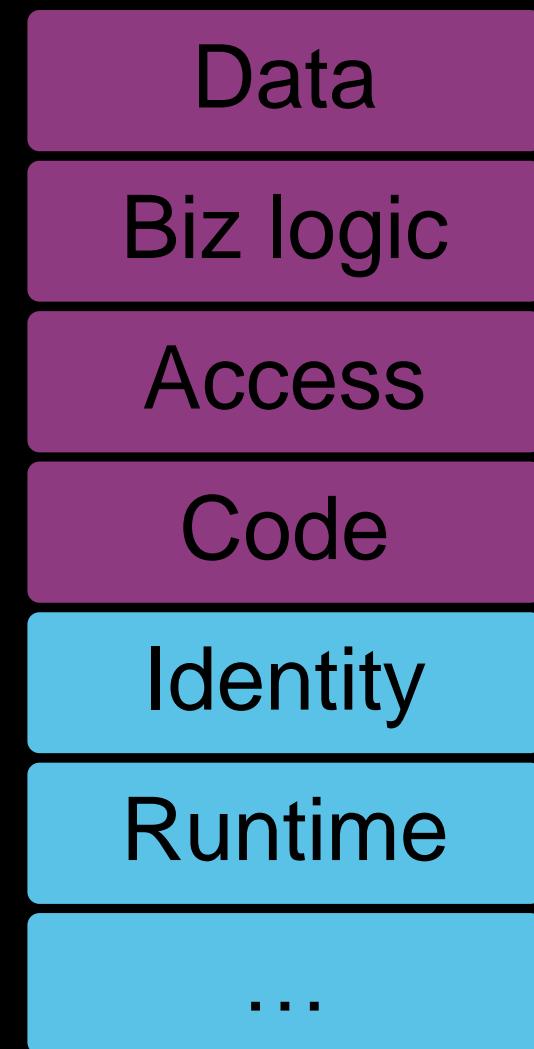
Customer

Platform

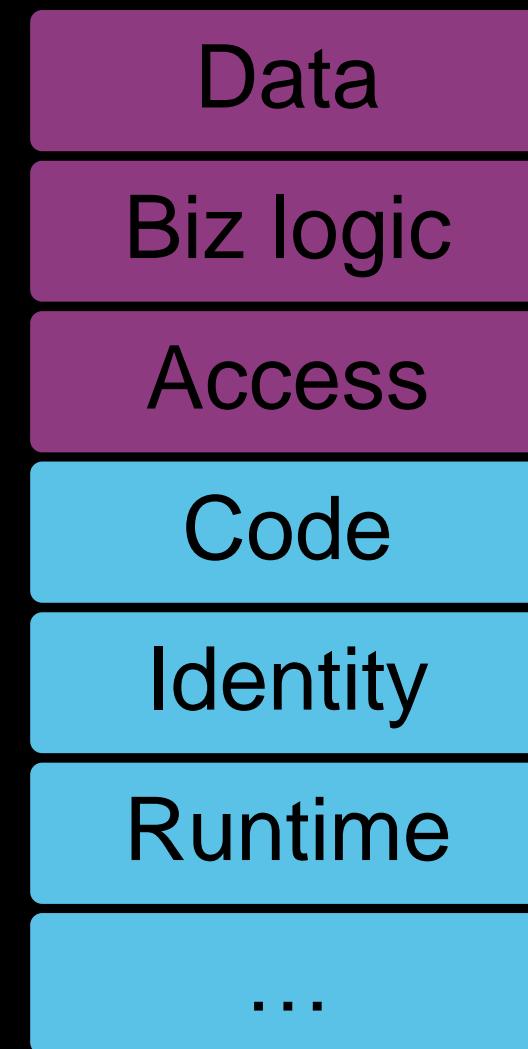


**We must own
our side of the
Shared
Responsibility
Model**

Serverless

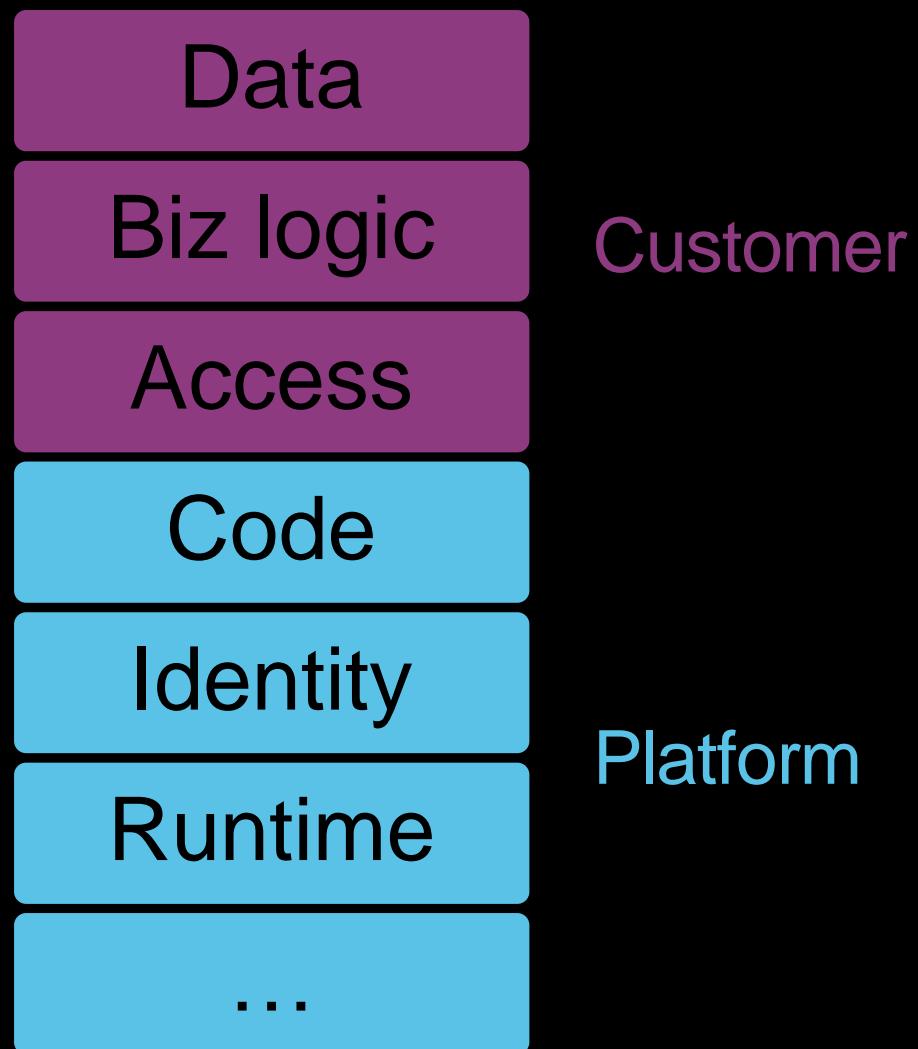


LCNC



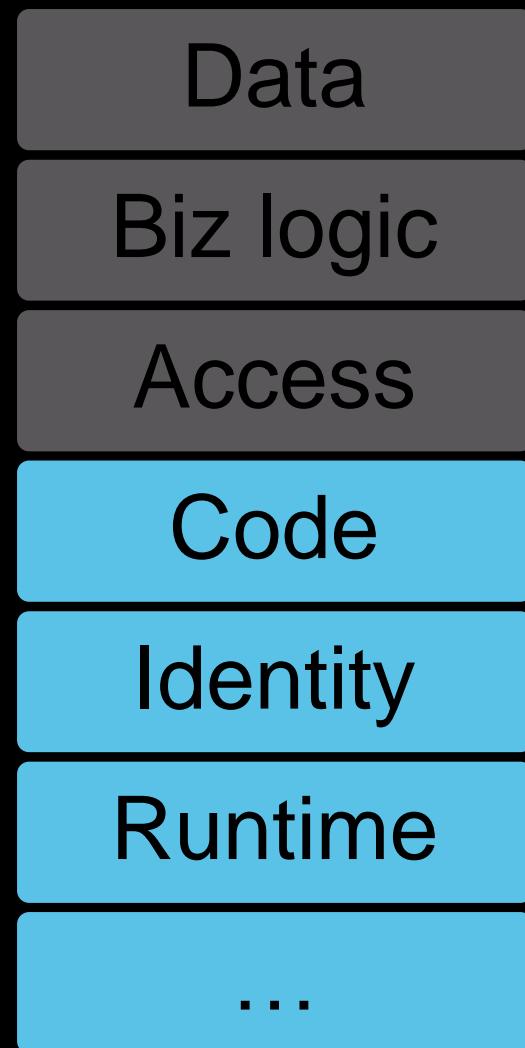


LCNC





Platforms have to step up



Customer

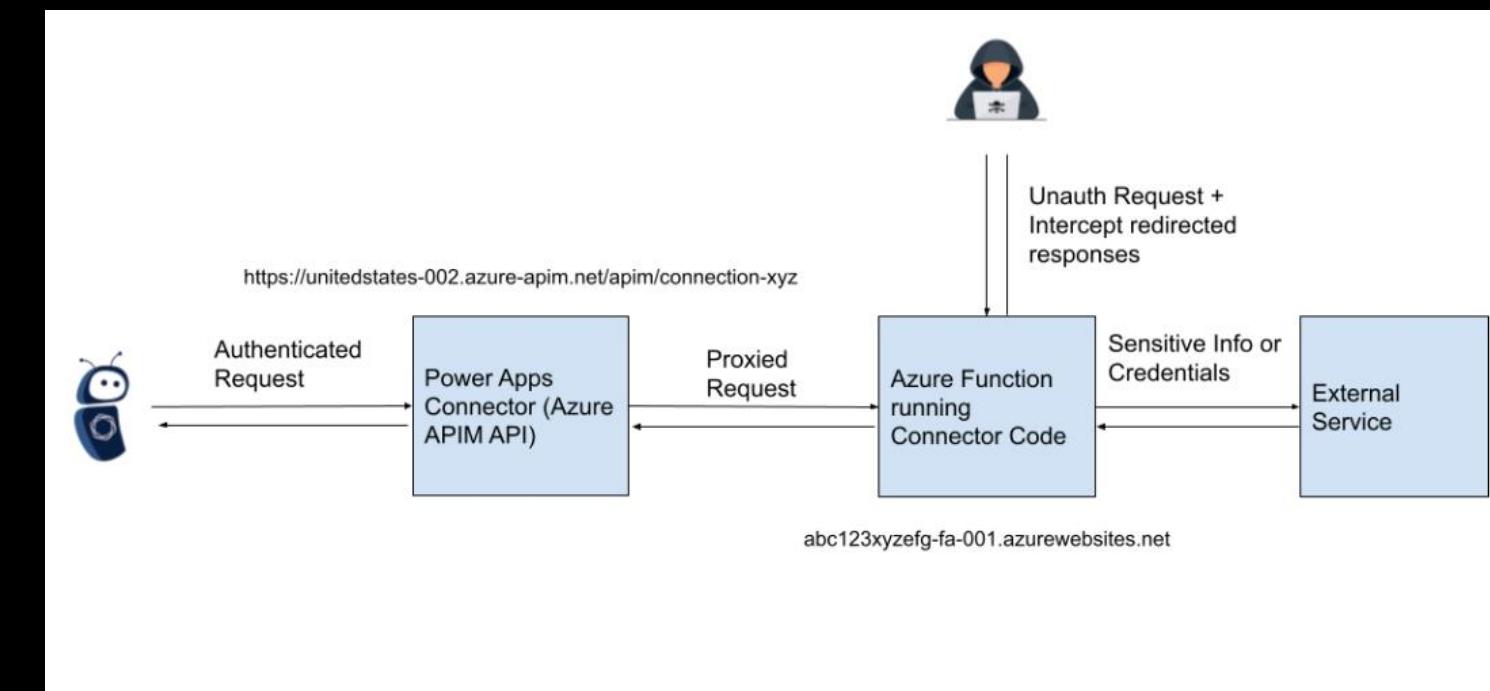
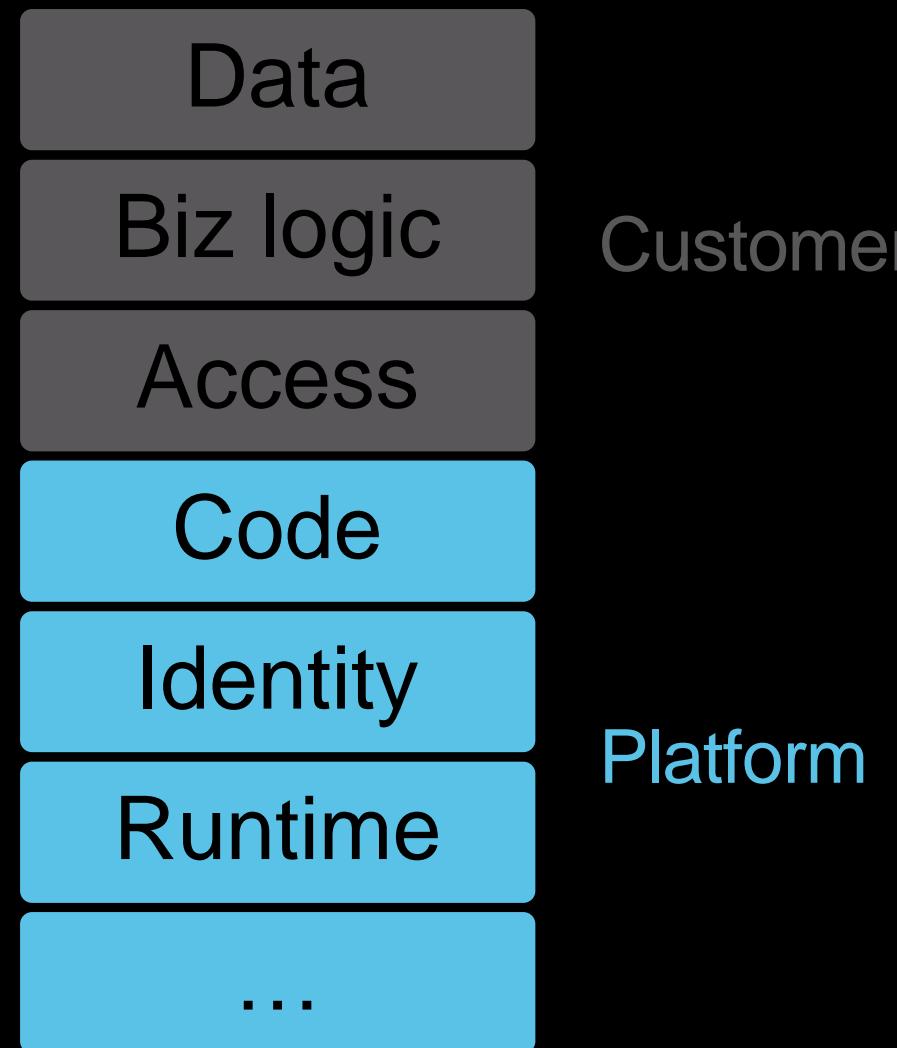
Every SaaS is a Low-Code/No-Code platform today.

They need to own the code running on their platforms, in addition to the rest of the Shared Responsibility Model.

Platform



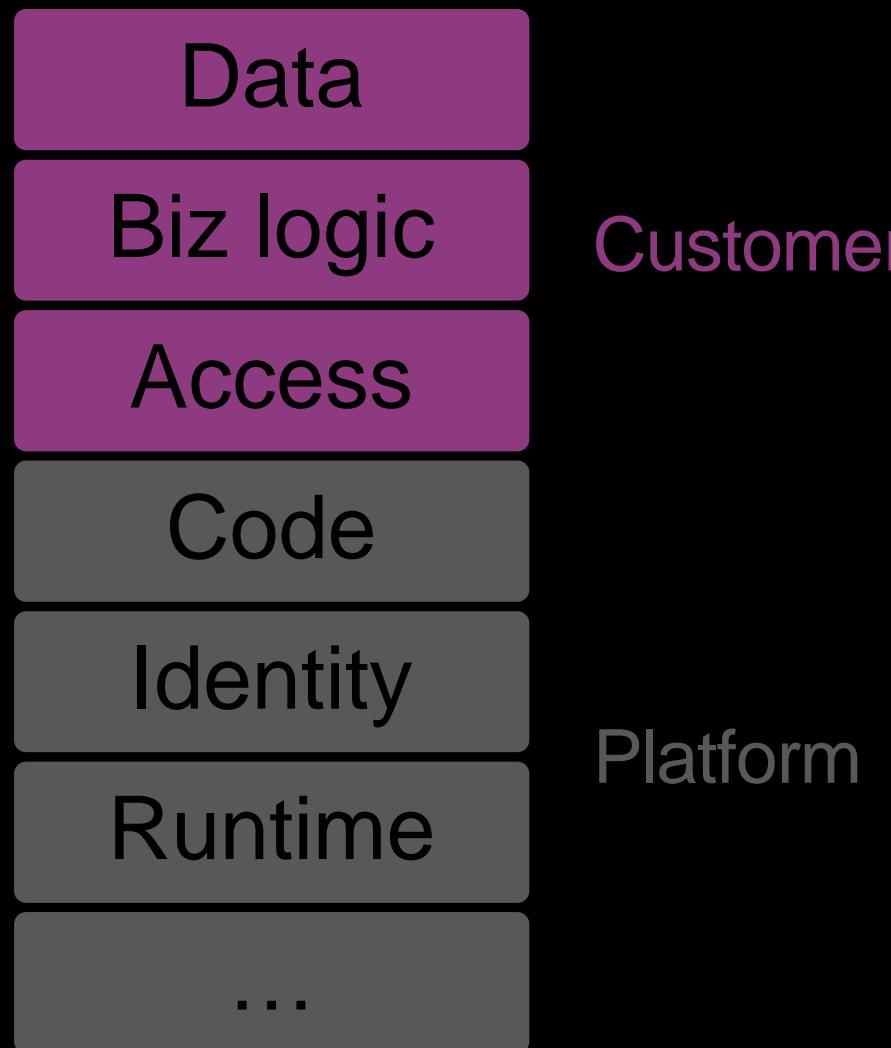
Platforms have to step up



<https://www.tenable.com/security/research/tra-2023-25>

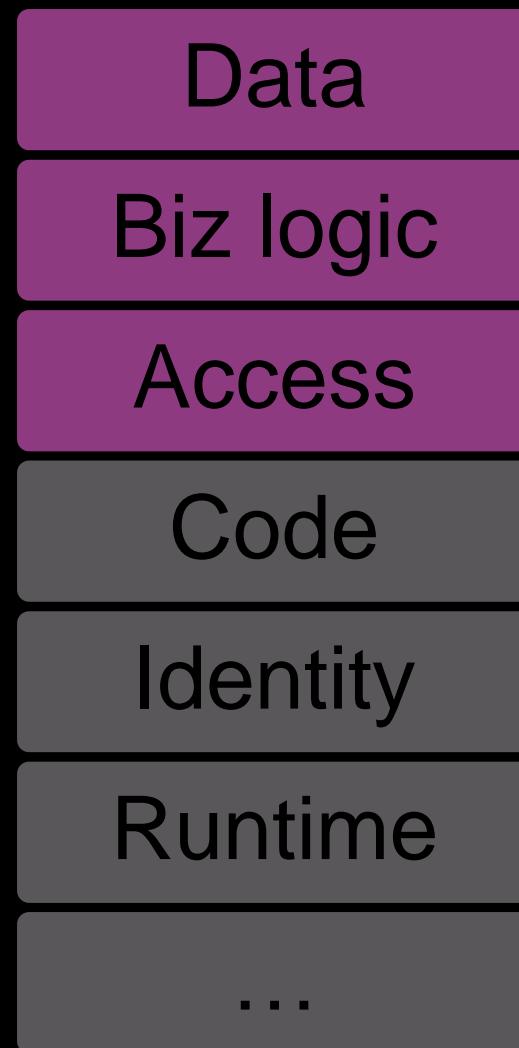


Sure, let business users build they own. What could go wrong?





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



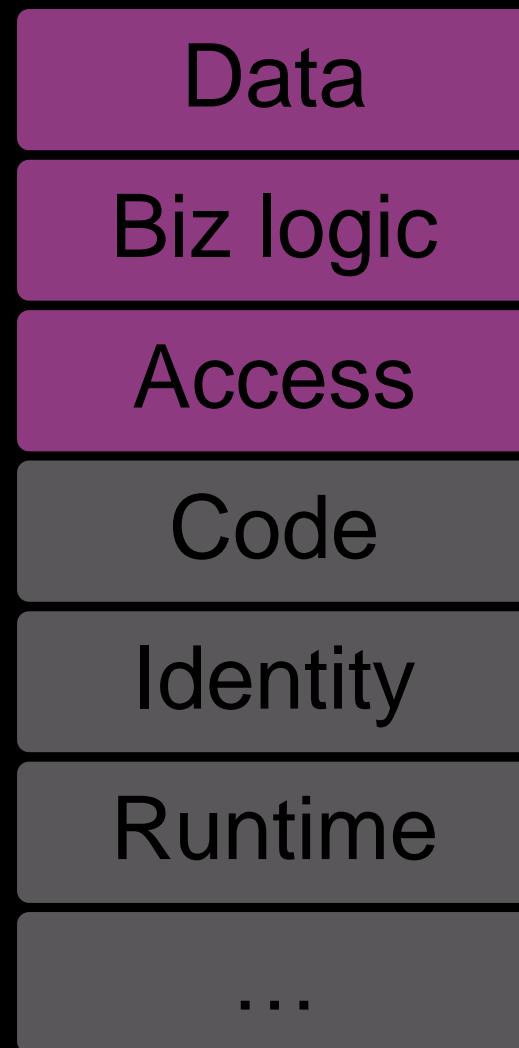
Customer

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?



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

@mbrg0

#BHUSA @BlackHatEvents



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

When a row is added, modified or deleted

```
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





AUGUST 9-10, 2023

BRIEFINGS

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

Michael Bargury @mbrg0

Zenity