zenity

Learn more: github.com/mbrg/talks
Twitter: @mbrg0

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

Michael Bargury @ Zenity

BSidesSF 2023

About me

- CTO and co-founder @ Zenity
- Ex MSFT cloud security
- OWASP *'Top 10 LCNC Security Risks'* project lead
- Dark Reading columnist

@mbrg0

DR bit.ly/lcsec

Outline

- Low-Code / No-Code in a nutshell
- The “hit-save” SDLC
- OWASP Top 10 LCNC Security Risks
- Learn more

zenity

Twitter: @mbrg0

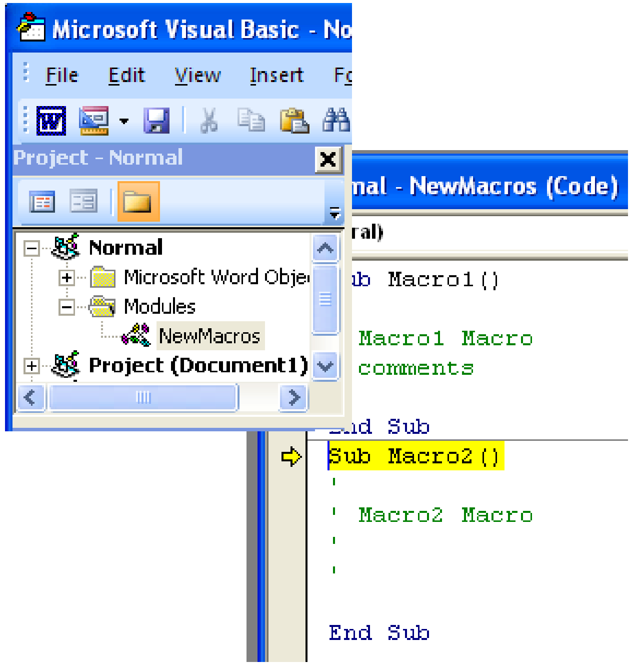
Low-Code / No-Code in a Nutshell: EVERYONE is a Developer

Business Needs ⋙ IT Capacity

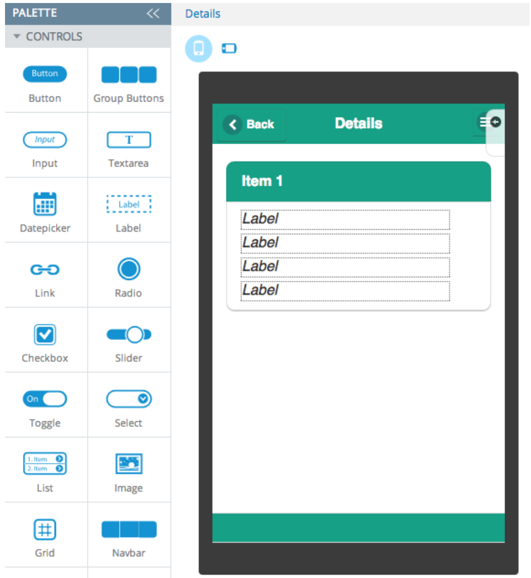
ASKED IT FOR A NEW TOOL
NEXT QUARTER
NEXT YEAR

If it sounds familiar, its because it is

Windows Series
For disk size contained in this package, see top of package.
Requires Microsoft Windows version 3.0
The Microsoft Office for Windows
The essential productivity applications
Microsoft Word for Windows
r Windows
PowerPoint for Windows
GhostMouse
File
Help
Record
Stop
Play

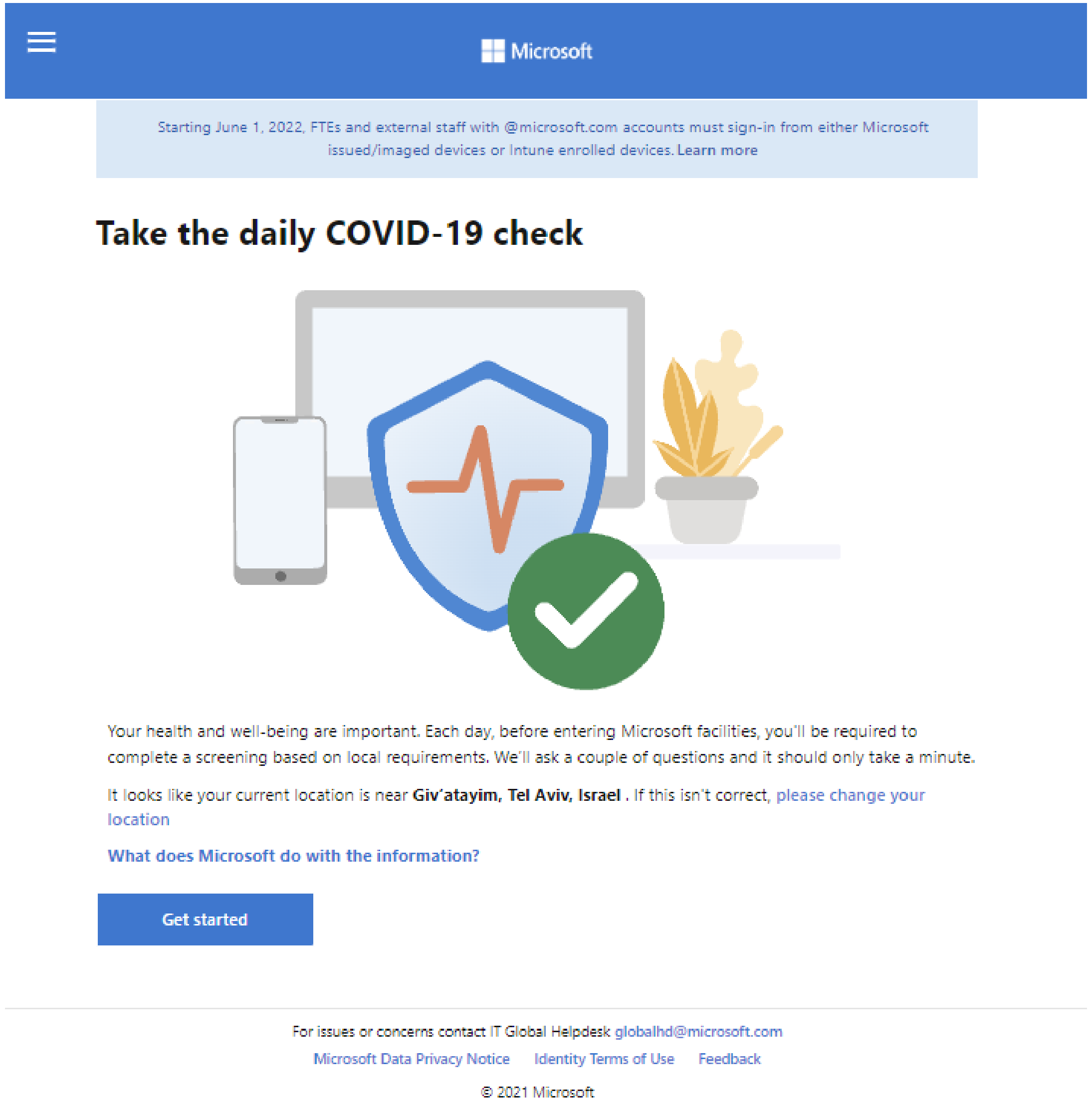


```
ral)
ub Macro1()

 Macro1 Macro
 comments

End Sub
Sub Macro2()
'
' Macro2 Macro
'
'

End Sub
```



Tech evolution

COVID health check app by Microsoft



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

Take the daily COVID-19 check

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

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

What does Microsoft do with the information?

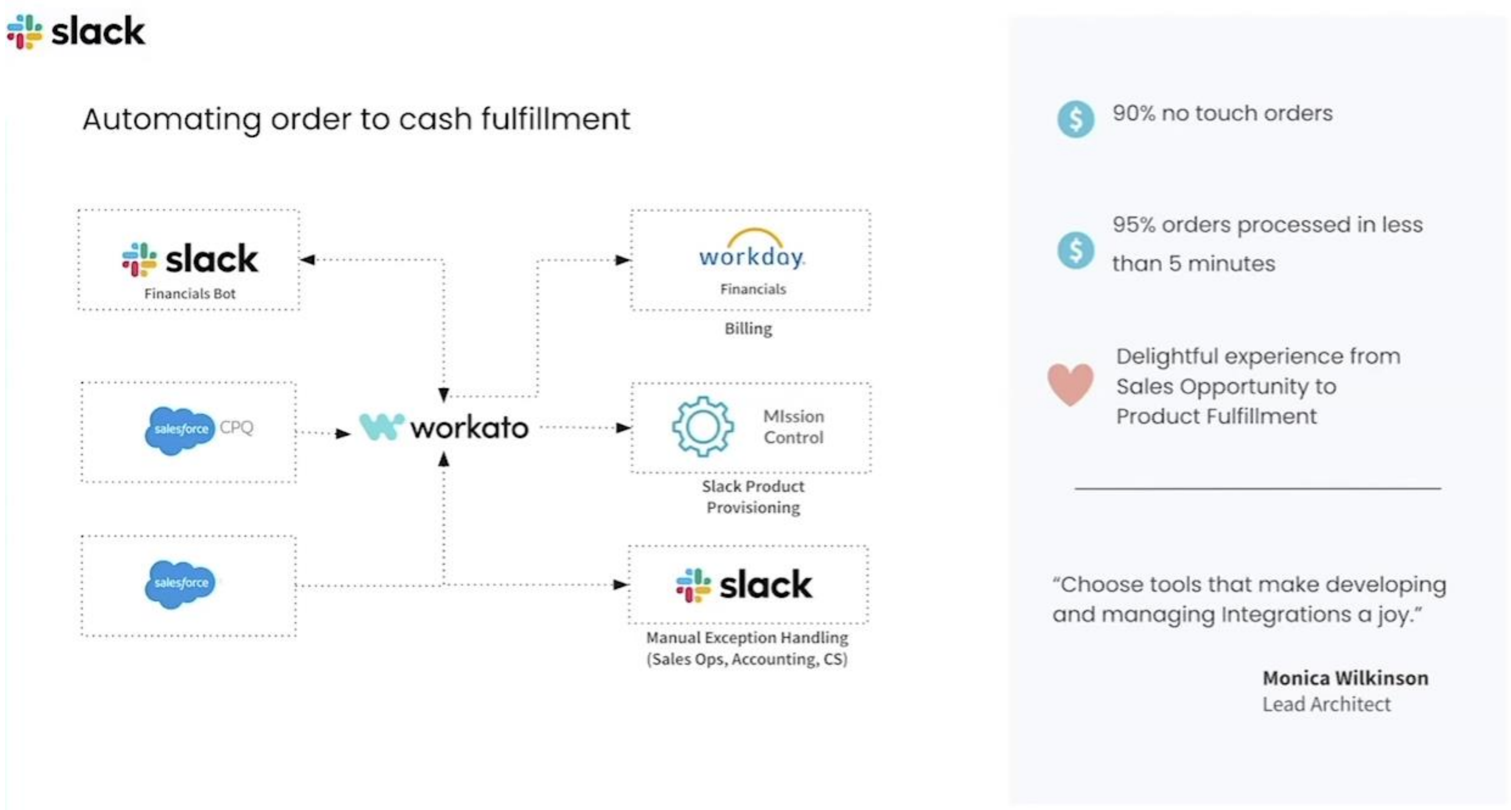
For issues or concerns contact IT Global Helpdesk globalhd@microsoft.com

Microsoft Data Privacy Notice Identity Terms of Use Feedback

© 2021 Microsoft

https://aka.ms/healthcheck

Order-to-cash automation by Slack



slack

Automating order to cash fulfillment

slack
Financials Bot

salesforce CPQ

salesforce

workato

workday.
Financials
Billing

MIssion Control
Slack Product Provisioning

slack
Manual Exception Handling (Sales Ops, Accounting, CS)

90% no touch orders

95% orders processed in less than 5 minutes

Delightful experience from Sales Opportunity to Product Fulfillment

"Choose tools that make developing and managing Integrations a joy."

Monica Wilkinson
Lead Architect

https://www.workato.com/the-connector/how-slack-automated-order-to-cash/

Business users become business developers

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

How citizen developers modernized Microsoft product launches

Mar 20, 2020 | Serah Delaini

"… A Business Operations program manager, and her team, were searching for a way to optimize the launch process for the 150 employees who ran product launches across the company.
… Within months, the app would become a widely used internal tool"

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

Available in every major enterprise

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

The vast majority of enterprise apps

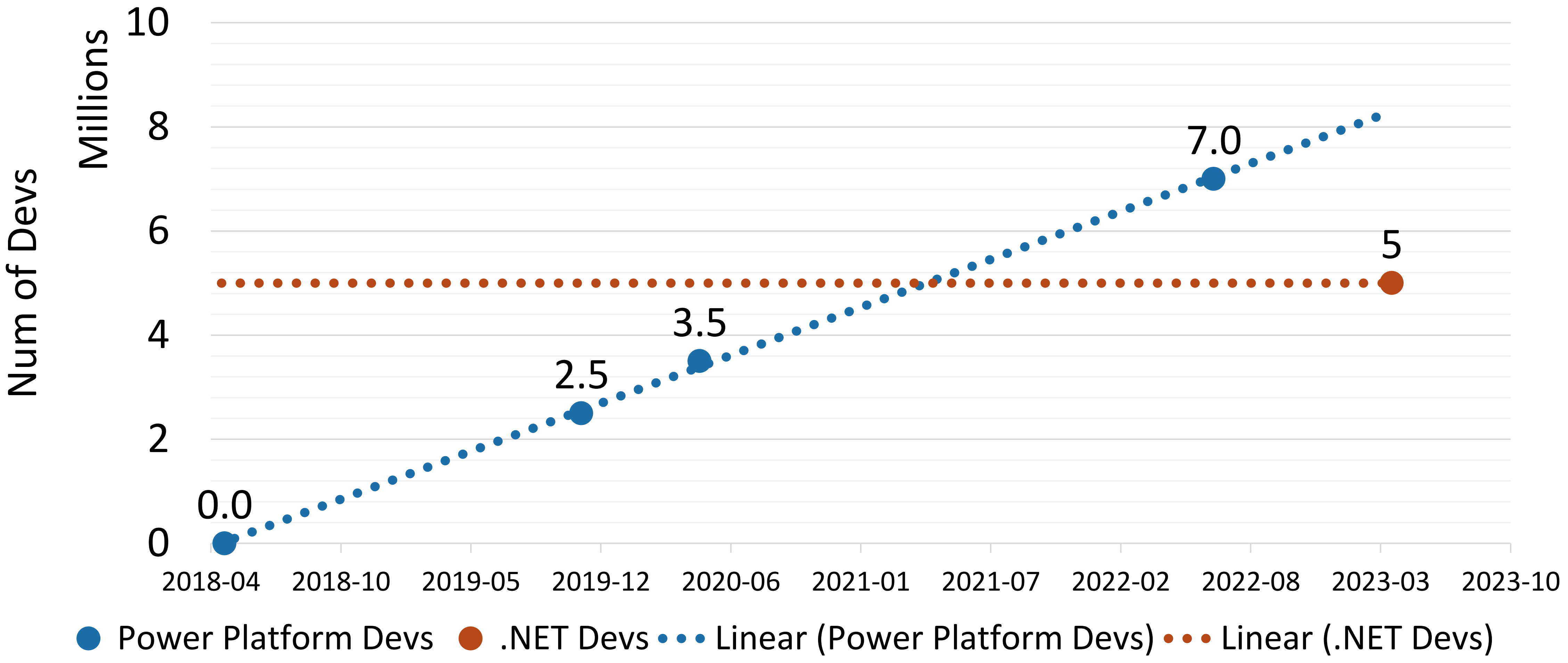
- *“By 2025, 70% of new applications deployed for the enterprise will use low-code or no-code tools”*
- *“By 2023, the number of active citizen developers at large enterprises will be at least four times the number of professional developers.”*

Gartner 2021

- *“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.”*

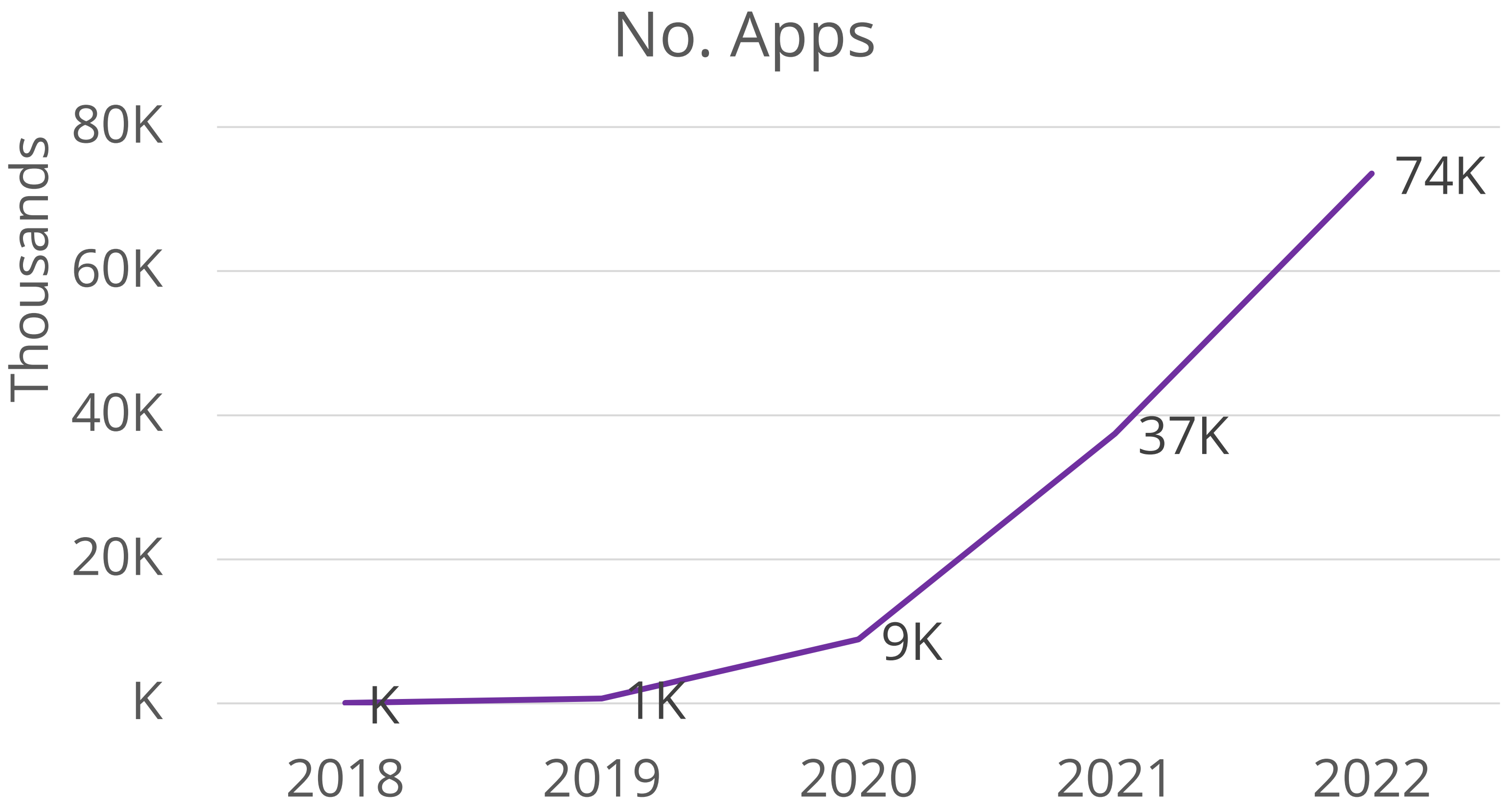
Satya Nadella, Microsoft Ignite 2019

More MSFT low-code devs than .NET devs, today!



Sources: Microsoft Build 2018, Ignite 2019, Build 2020, Protocol 2022

Exponential Growth in Business Development



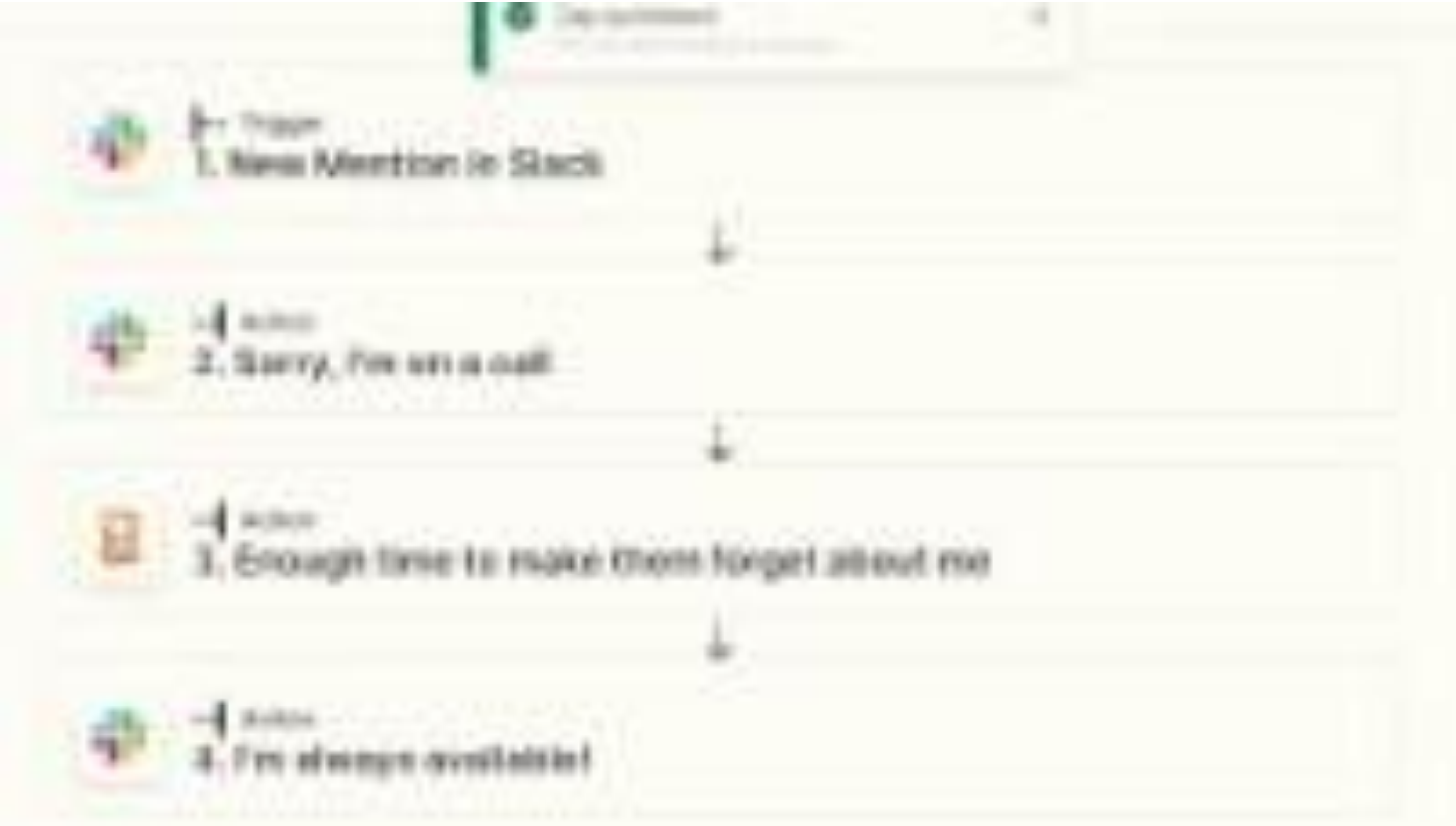
Recap: you can’t opt out of citizen development

- 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
- Tens of thousands of apps in a large enterprise

zenity

Twitter: @mbrg0

No Code No SDLC?



Zap published

[illegible]

Trigger

1. New Mention in Slack

Action

2. Sorry, I'm on a call

Action

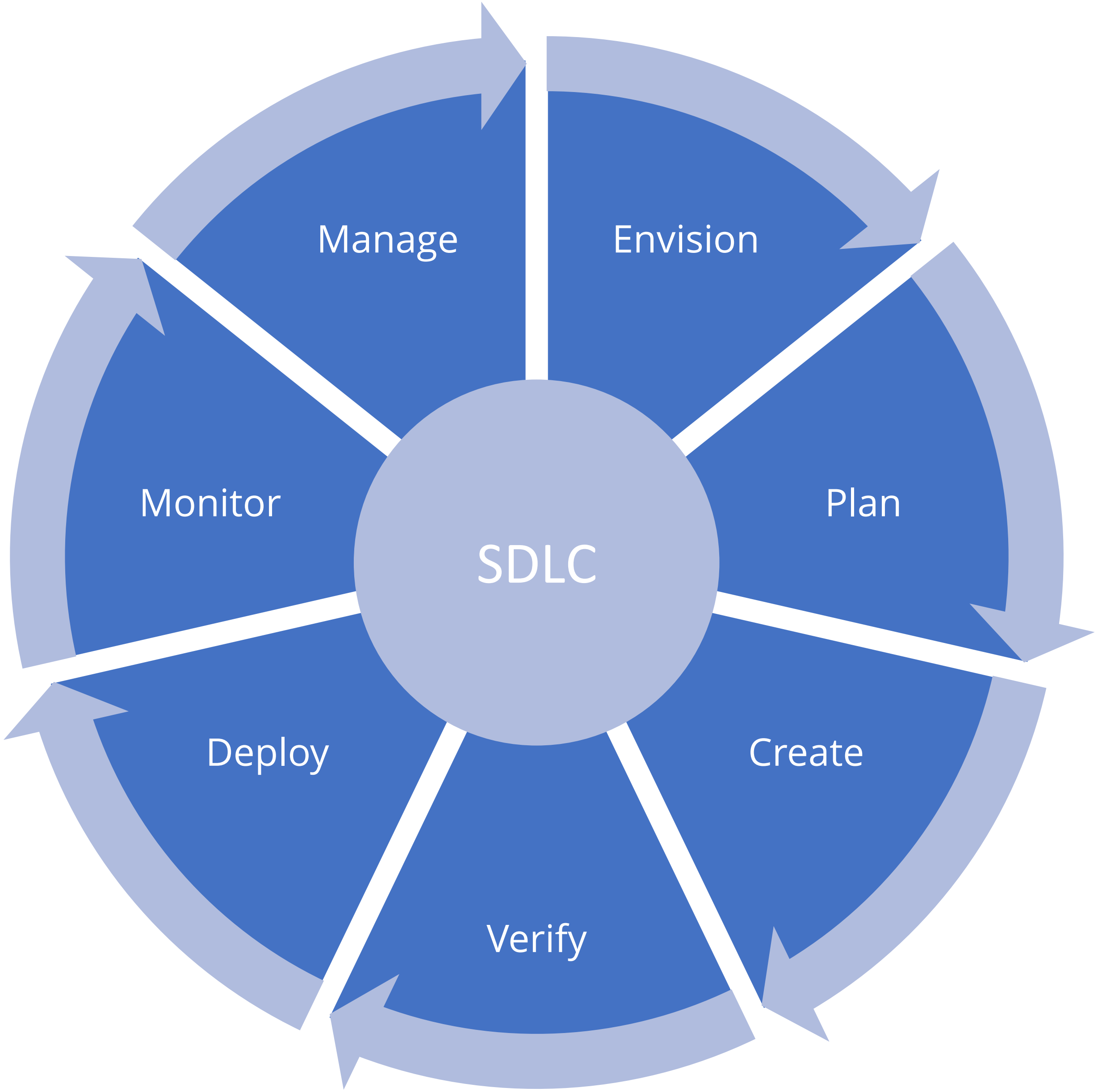
3. Enough time to make them forget about me

Action

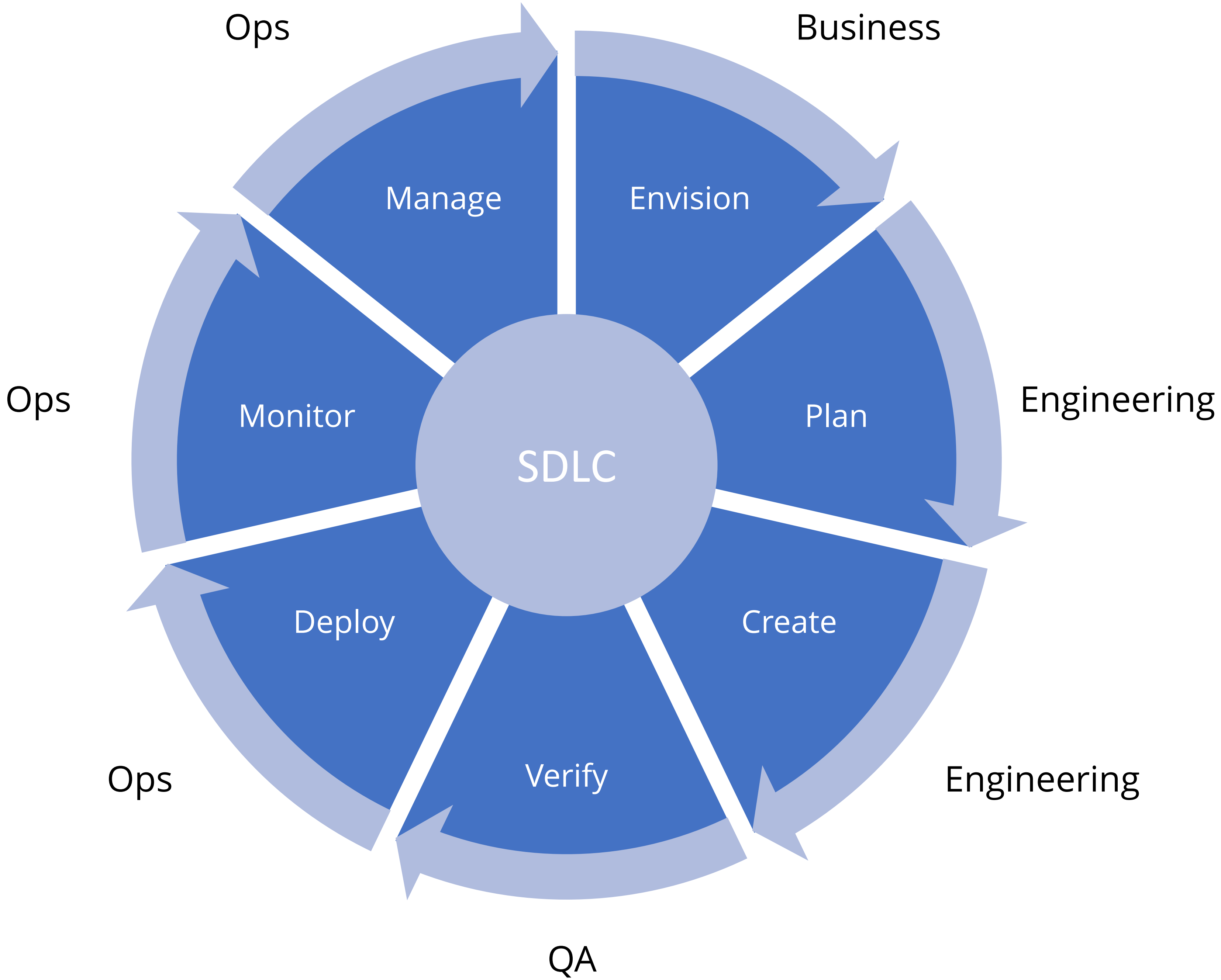
4. I'm always available!

youtu.be/5naPxs0fEJc

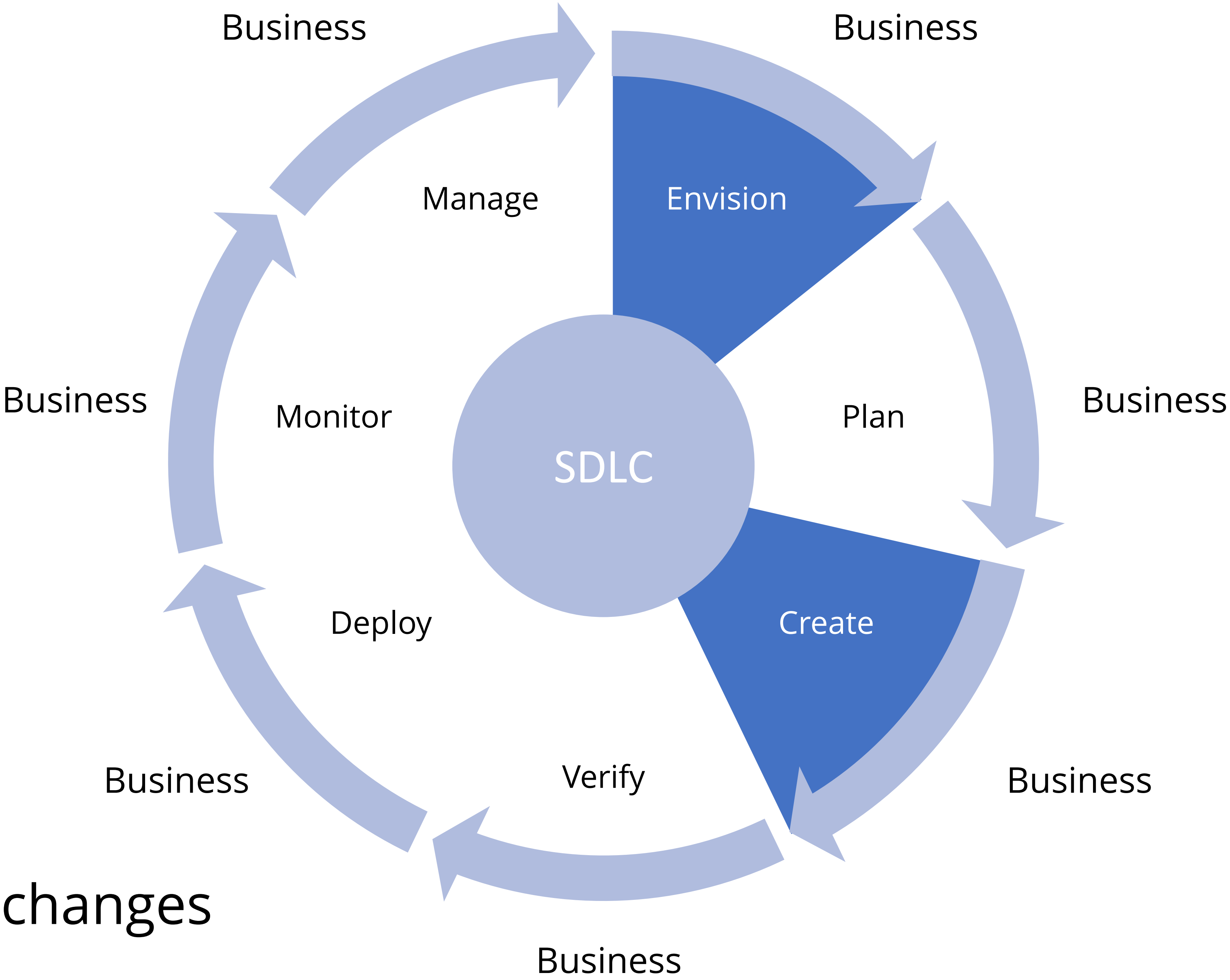
Software Development Lifecycle



Software Development Lifecycle

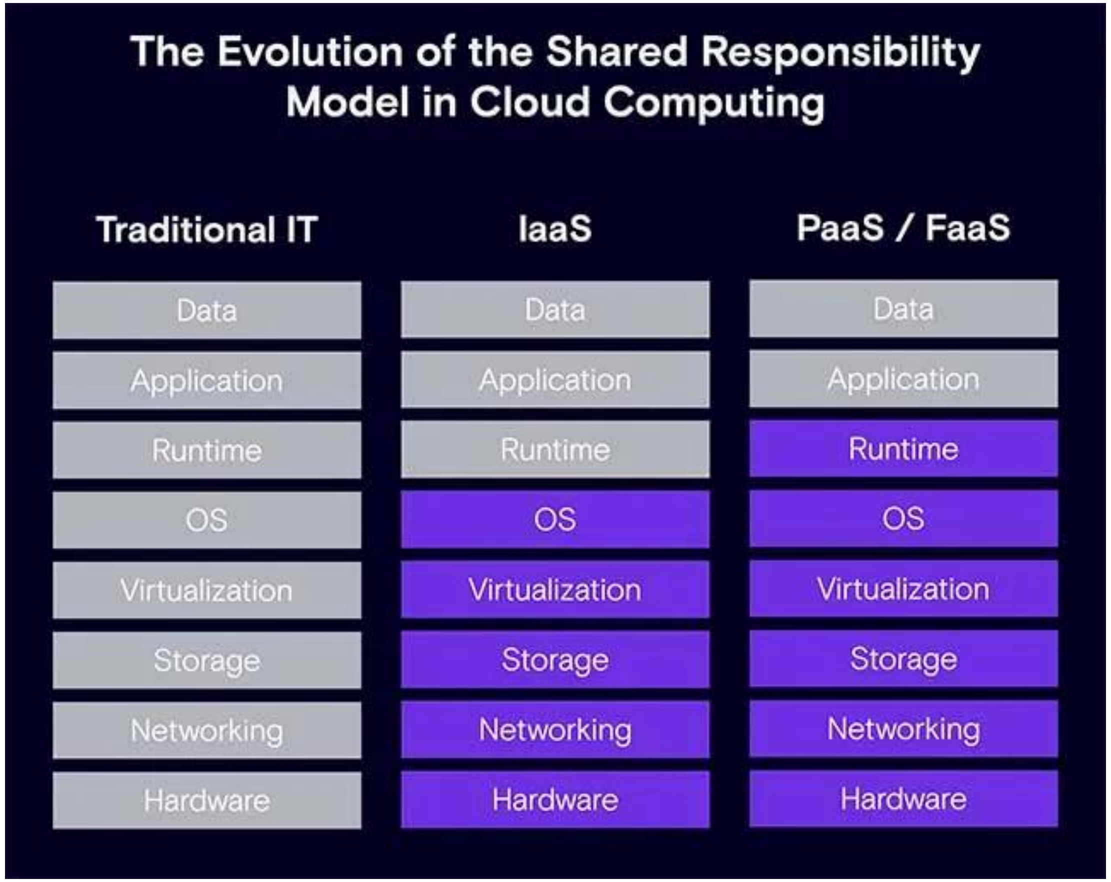


No Code SDLC?



Hit Save to deploy changes

The Shared Responsibility Model



The Evolution of the Shared Responsibility Model in Cloud Computing

Traditional IT	IaaS	PaaS / FaaS
Data	Data	Data
Application	Application	Application
Runtime	Runtime	Runtime
OS	OS	OS
Virtualization	Virtualization	Virtualization
Storage	Storage	Storage
Networking	Networking	Networking
Hardware	Hardware	Hardware

zenity

Twitter: @mbrg0

OWASP Top 10 Low-Code/No-Code Security Risks

OWASP
low-code/no-code

Top 10 Security Risks

https://owasp.org/www-project-top-10-low-code-no-code-security-risks

OWASP Top 10 Security Risks for LCNC

1. LCNC-SEC-01: Account Impersonation
2. LCNC-SEC-02: Authorization Misuse
3. LCNC-SEC-03: Data Leakage and Unexpected Consequences
4. LCNC-SEC-04: Authentication and Secure Communication Failures
5. LCNC-SEC-05: Security Misconfiguration
6. LCNC-SEC-06: Injection Handling Failures
7. LCNC-SEC-07: Vulnerable, Unmanaged and Untrusted Components
8. LCNC-SEC-08: Data and Secret Handling Failures
9. LCNC-SEC-09: Asset Management Failures
10. LCNC-SEC-10: Security Logging and Monitoring Failures

https://owasp.org/www-project-top-10-low-code-no-code-security-risks

LCNC-SEC-01: Account Impersonation

Low-code/no-code applications can be embedded with user identities which are used implicitly by any application user. This creates a direct path towards Privilege Escalation, allows an attacker to hide behind another user's identity, and circumvents traditional security controls.

Better Customer Care – The Problem

The Customer Care team at a large eCommerce company wanted to improve customer service.

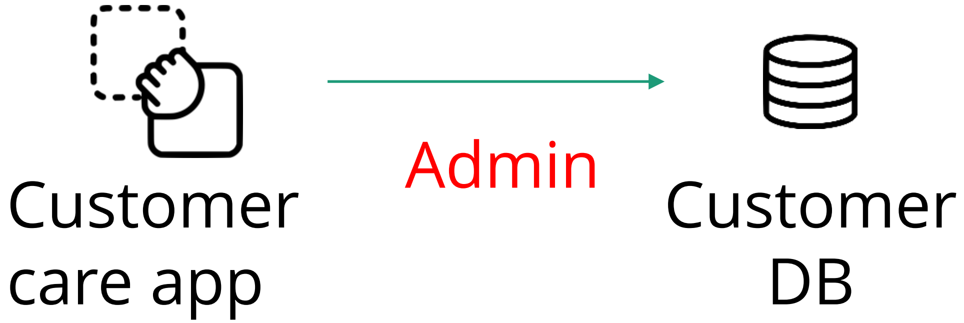
- Goal: improve customer service
- Method: build an app that lets relevant company employees view customer support history and latest purchases
- Challenge: employees don’t have permissions to the customer database

Customer care app

Better Customer Care – The Solution

Impact:

- ✓Employees are happy
- ✓Customers are happy
- ✓Customer Care team is happy



Customer care app

Admin

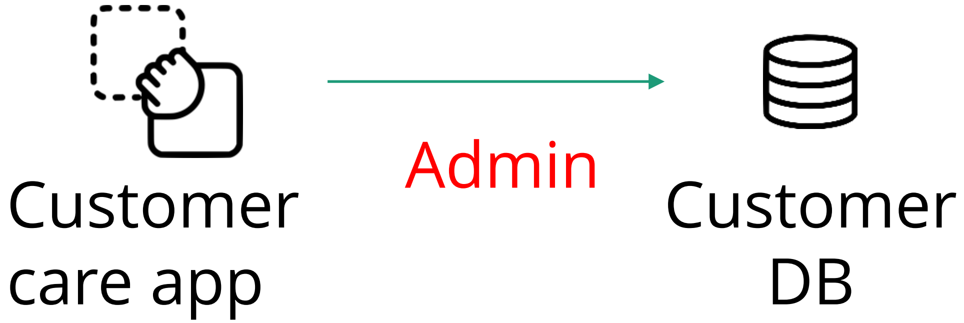
Customer DB

Better Customer Care – The Solution

Impact:

✓Employees are happy
✓Customers are happy
✓Customer Care team is happy

✓SOC team panics



Customer care app

Admin

Customer DB

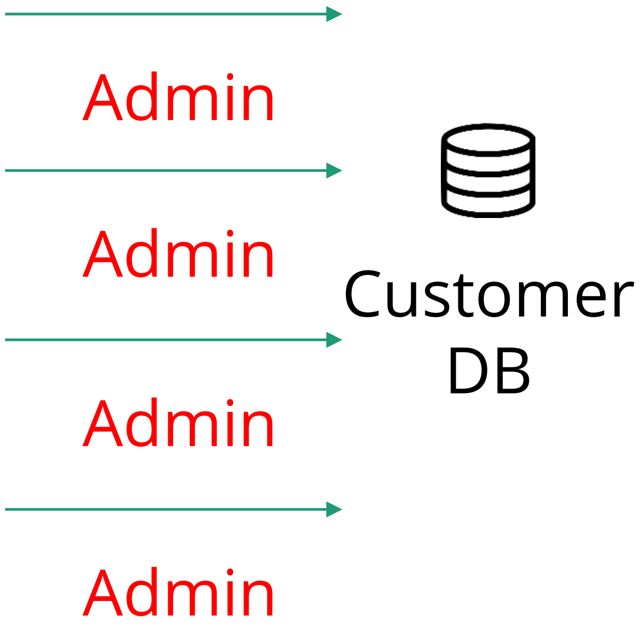
Meanwhile, At the SOC

Abnormal activity detected:

Customer DB is being scraped?

- Lots of queries
- Multiple IPs and hosts
- Spread across time

An investigation shows that all connections use single account. Was it compromised?



Admin

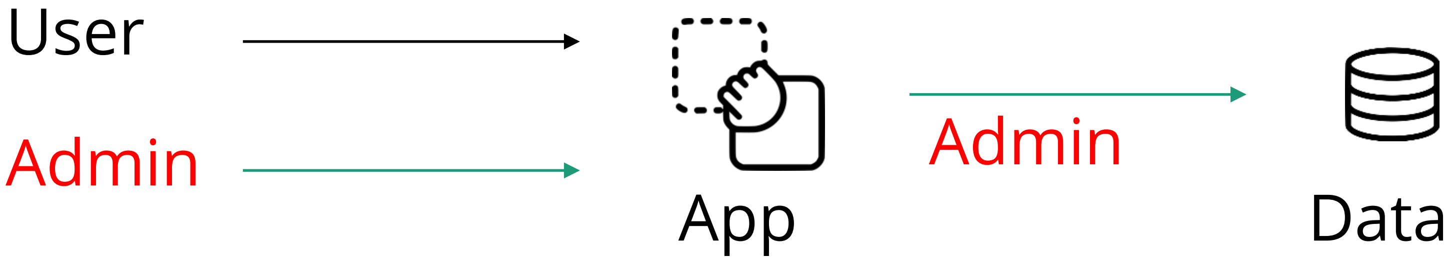
Admin

Admin

Admin

Customer DB

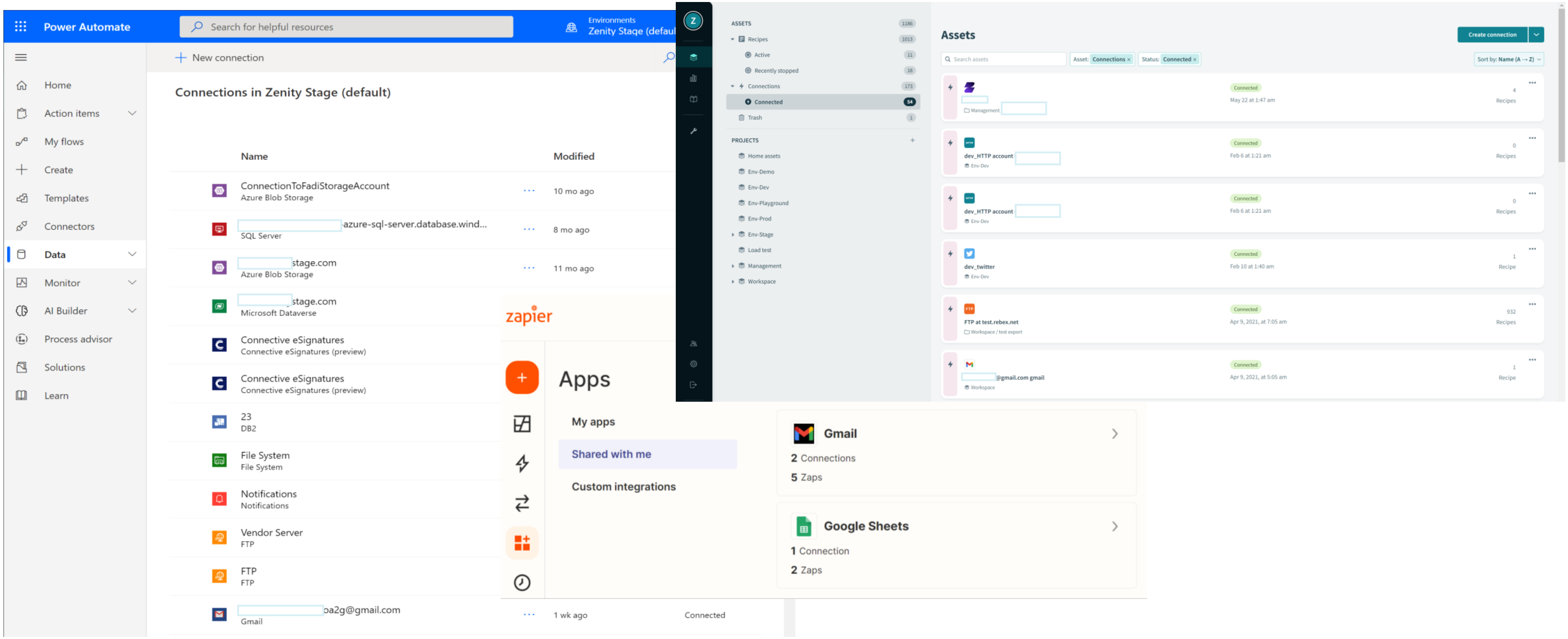
Better Customer Care – Summary



LCNC-SEC-02: Authorization Misuse

Service connections are first class objects in most low-code/no-code platforms. This means they can be shared between applications, with other users or with entire organizations.

Credential Sharing as a Service



Connections in Zenity Stage (default)

Name	Modified	
ConnectionToFadiStorageAccount Azure Blob Storage	10 mo ago	
[redacted]azure-sql-server.database.wind... SQL Server	8 mo ago	
[redacted]stage.com Azure Blob Storage	11 mo ago	
[redacted]stage.com Microsoft Dataverse		
Connective eSignatures Connective eSignatures (preview)		
Connective eSignatures Connective eSignatures (preview)		
23 DB2		
File System File System		
Notifications Notifications		
Vendor Server FTP		
FTP FTP		
[redacted]oa2g@gmail.com Gmail	1 wk ago	Connected

Assets

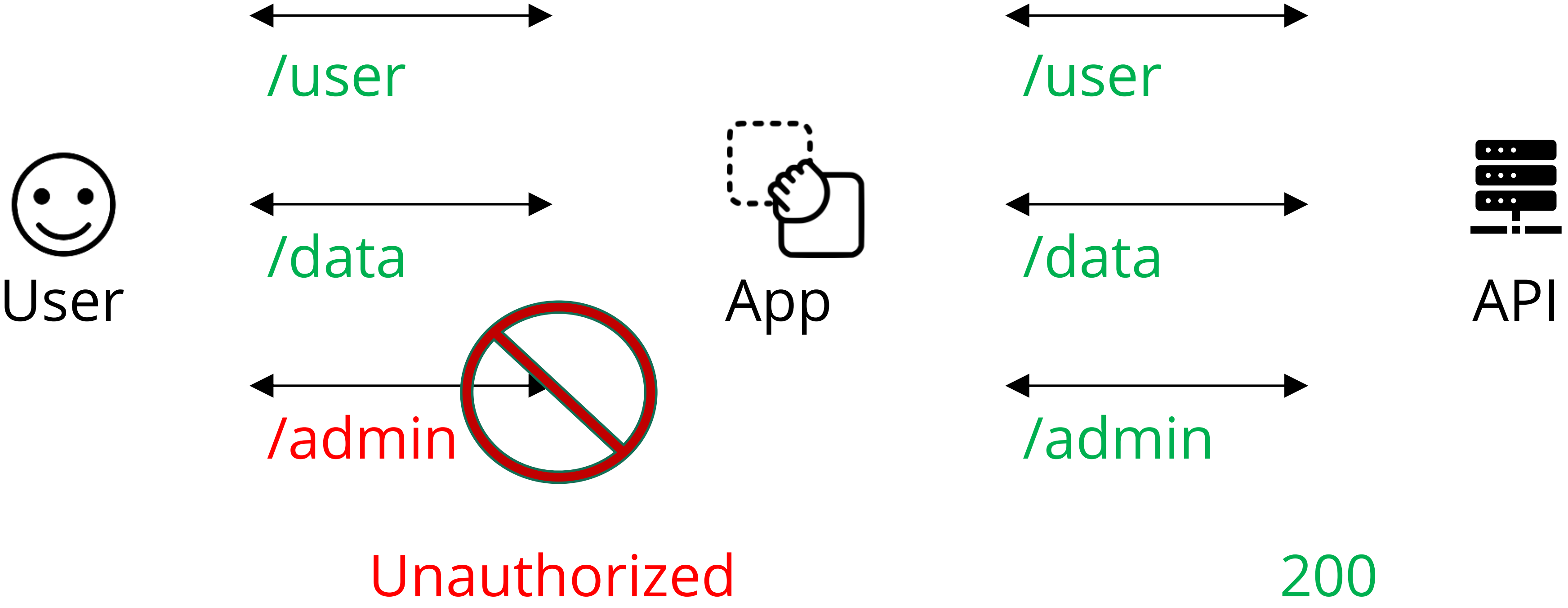
[redacted] Management [redacted]	Connected	May 22 at 1:47 am	4 Recipes
dev_HTTP account [redacted] Env-Dev	Connected	Feb 6 at 1:21 am	0 Recipes
dev_HTTP account [redacted] Env-Dev	Connected	Feb 6 at 1:21 am	0 Recipes
dev_twitter Env-Dev	Connected	Feb 10 at 1:40 am	1 Recipe
FTP at test.rebex.net Workspace / test export	Connected	Apr 9, 2021, at 7:05 am	932 Recipes
[redacted]@gmail.com gmail Workspace	Connected	Apr 9, 2021, at 5:05 am	1 Recipe

Gmail
2 Connections
5 Zaps

Google Sheets
1 Connection
2 Zaps

App Reader <> API Admin

Authorization as front-end logic



User

/user

/data

/admin

Unauthorized

App

/user

/data

/admin

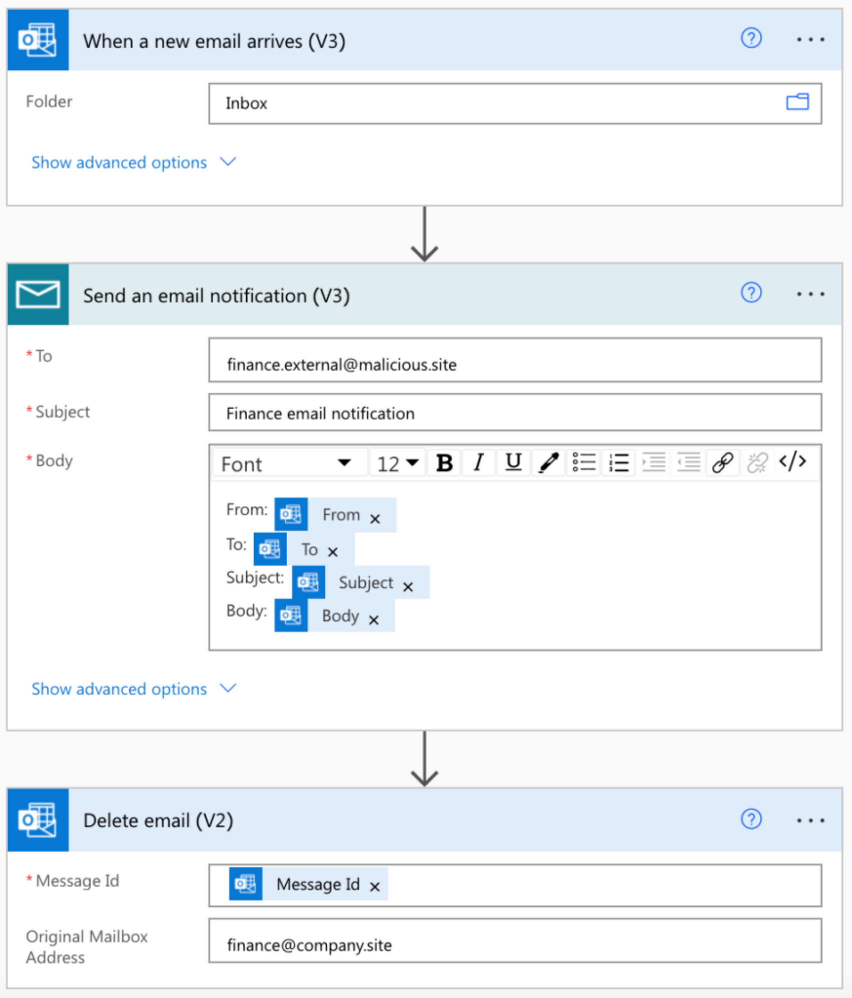
200

API

LCNC-SEC-03: Data Leakage and Unexpected Consequences

Low-code/no-code applications often sync data or trigger operations across multiple systems, which creates a path for data to find its way outside the organizational boundary. This means that operations in one system can have unexpected consequences in another.

LCNC-SEC-03: Data Leakage and Unexpected Consequences



When a new email arrives (V3)

Folder: Inbox

Show advanced options

Send an email notification (V3)

*To: finance.external@malicious.site

*Subject: Finance email notification

*Body:

From: From
To: To
Subject: Subject
Body: Body

Show advanced options

Delete email (V2)

*Message Id: Message Id

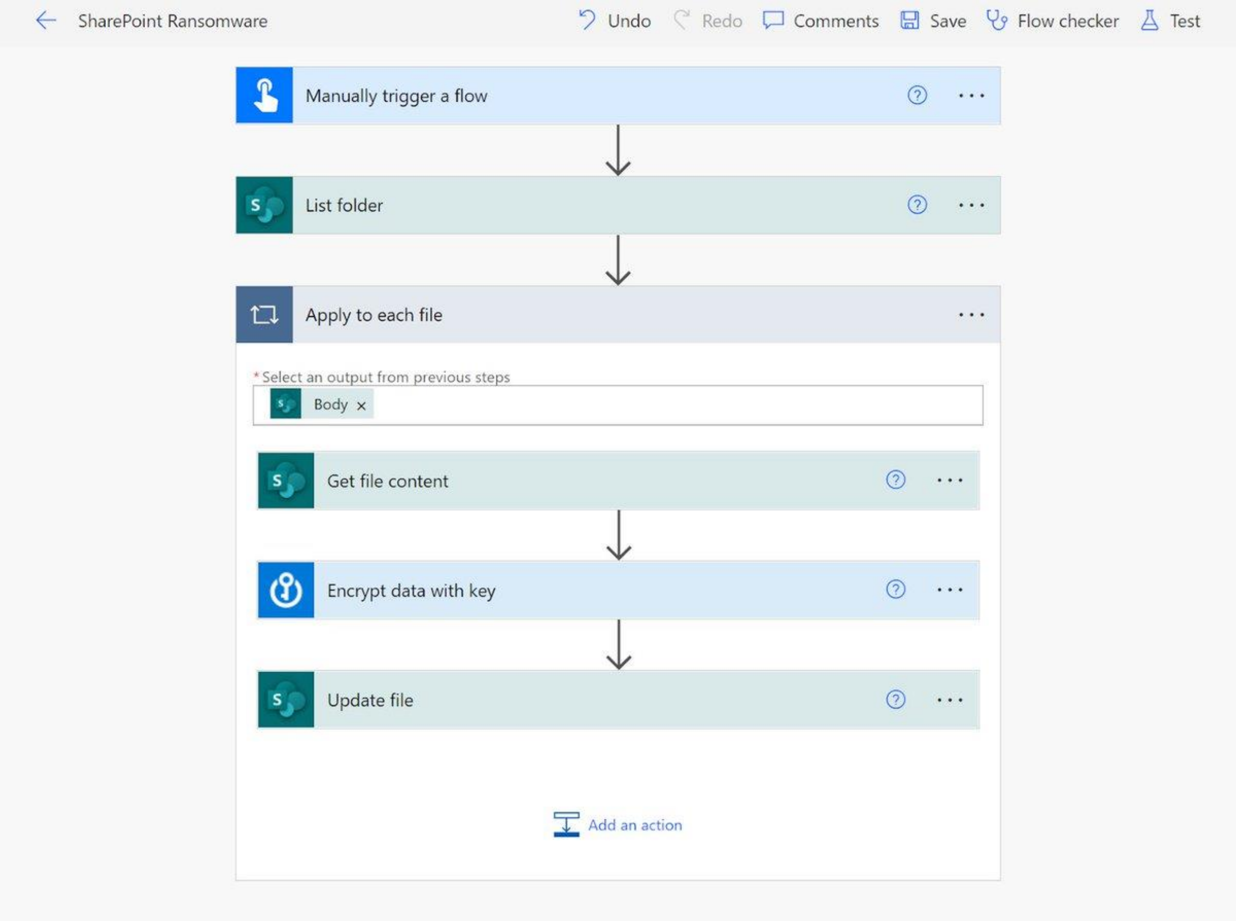
Original Mailbox Address: finance@company.site

Data is being copied between two separate services using two separate identities – existing defense mechanisms fail

LCNC-SEC-03: Data Leakage and Unexpected Consequences

If <file found>

Then <encrypt file>



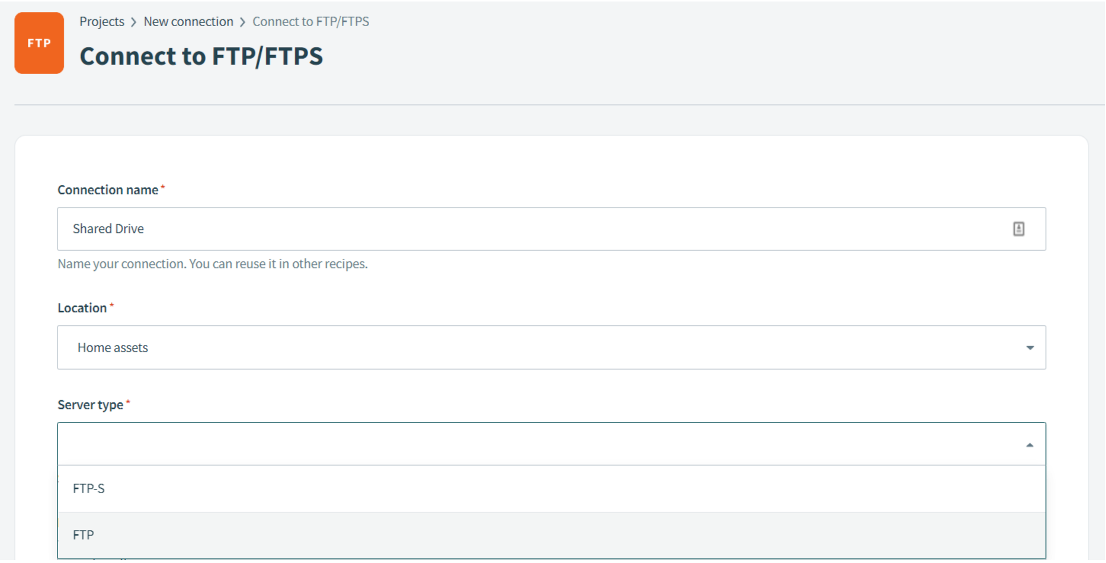
1. Manually trigger a flow
2. List folder
3. Apply to each file

   * Select an output from previous steps: Body

   1. Get file content
   2. Encrypt data with key
   3. Update file

LCNC-SEC-04: Authentication and Secure Communication Failures

Low-code/no-code applications typically connect to business-critical data via connections set up by business users, which can often result in insecure communication.



Projects > New connection > Connect to FTP/FTPS

Connect to FTP/FTPS

Connection name *

Shared Drive

Name your connection. You can reuse it in other recipes.

Location *

Home assets

Server type *

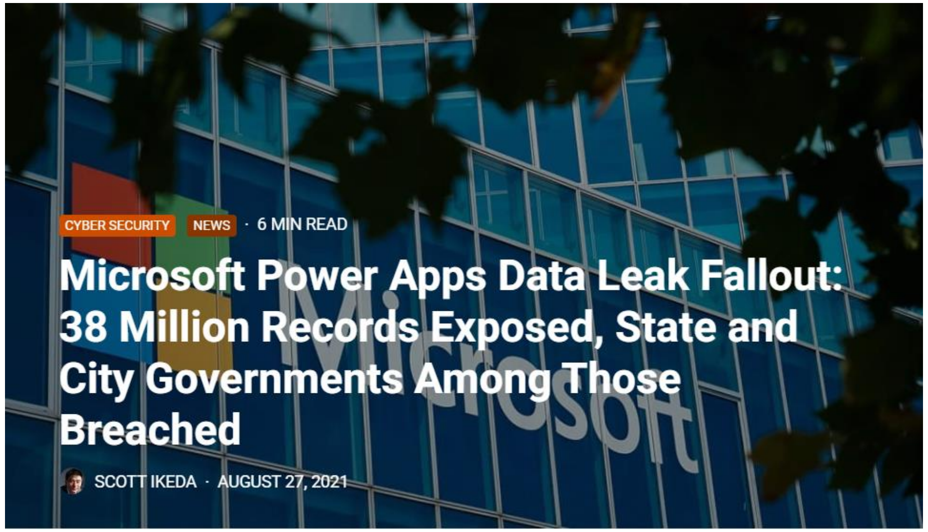
FTP-S

FTP

LCNC-SEC-05: Security Misconfiguration

Misconfigurations can often result in anonymous user access to sensitive data or operations, unprotected public endpoints, unprotected secrets and oversharing.

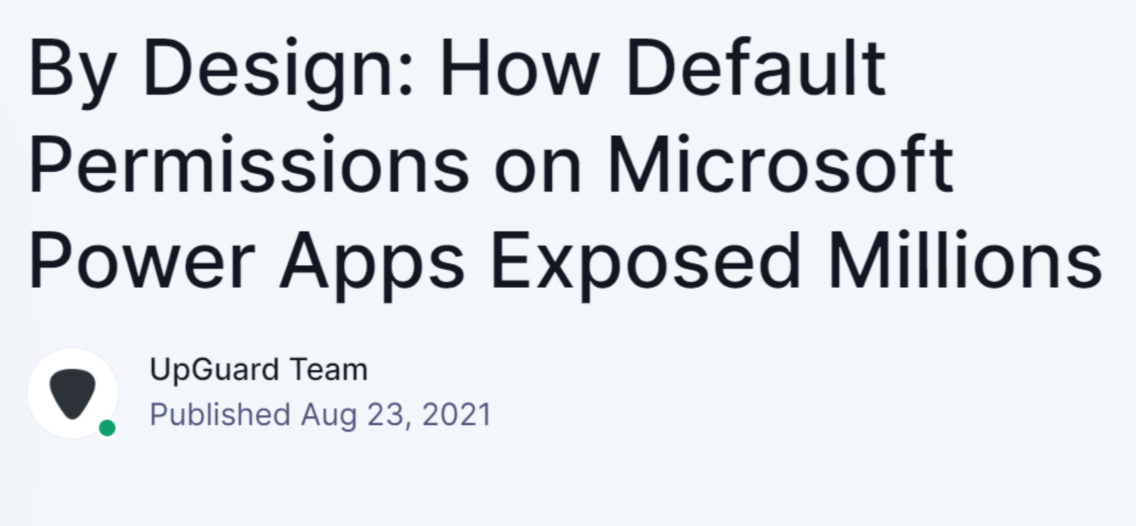
LCNC-SEC-05: Security Misconfiguration



CYBER SECURITY NEWS · 6 MIN READ

Microsoft Power Apps Data Leak Fallout: 38 Million Records Exposed, State and City Governments Among Those Breached

SCOTT IKEDA · AUGUST 27, 2021



By Design: How Default Permissions on Microsoft Power Apps Exposed Millions

UpGuard Team
Published Aug 23, 2021

Anonymous API Access

“An open protocol to allow the creation and consumption of queryable and interoperable RESTful APIs in a simple and standard way.”

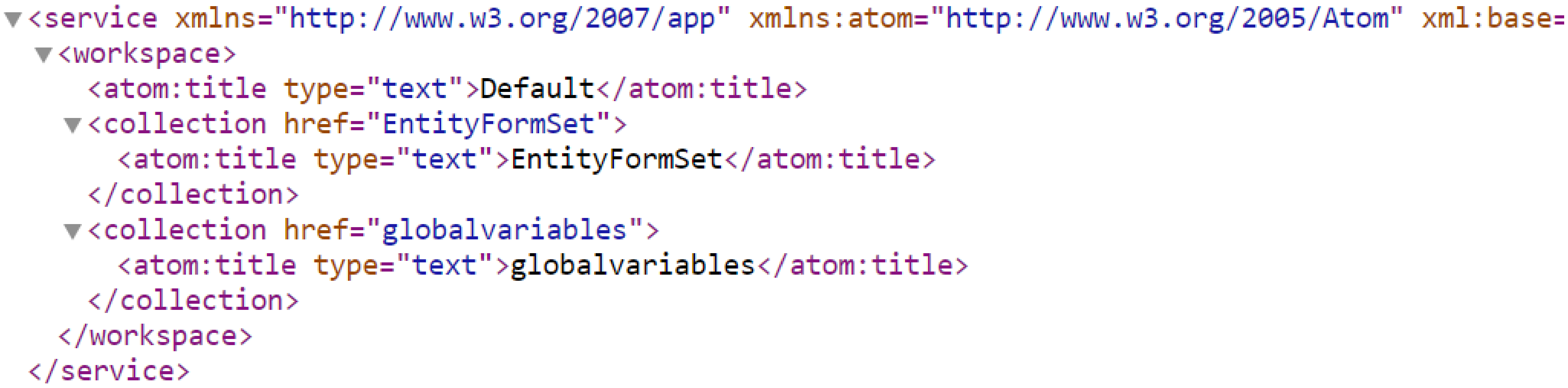
Power portals can be configured to provide access to SQL tables through ODATA using a specific URL:

portal.powerappsportals.com/_odata

Anonymous API Access

Power portals can be configured to provide access to SQL tables through ODATA using a specific URL:

portal.powerappsportals.com/_odata

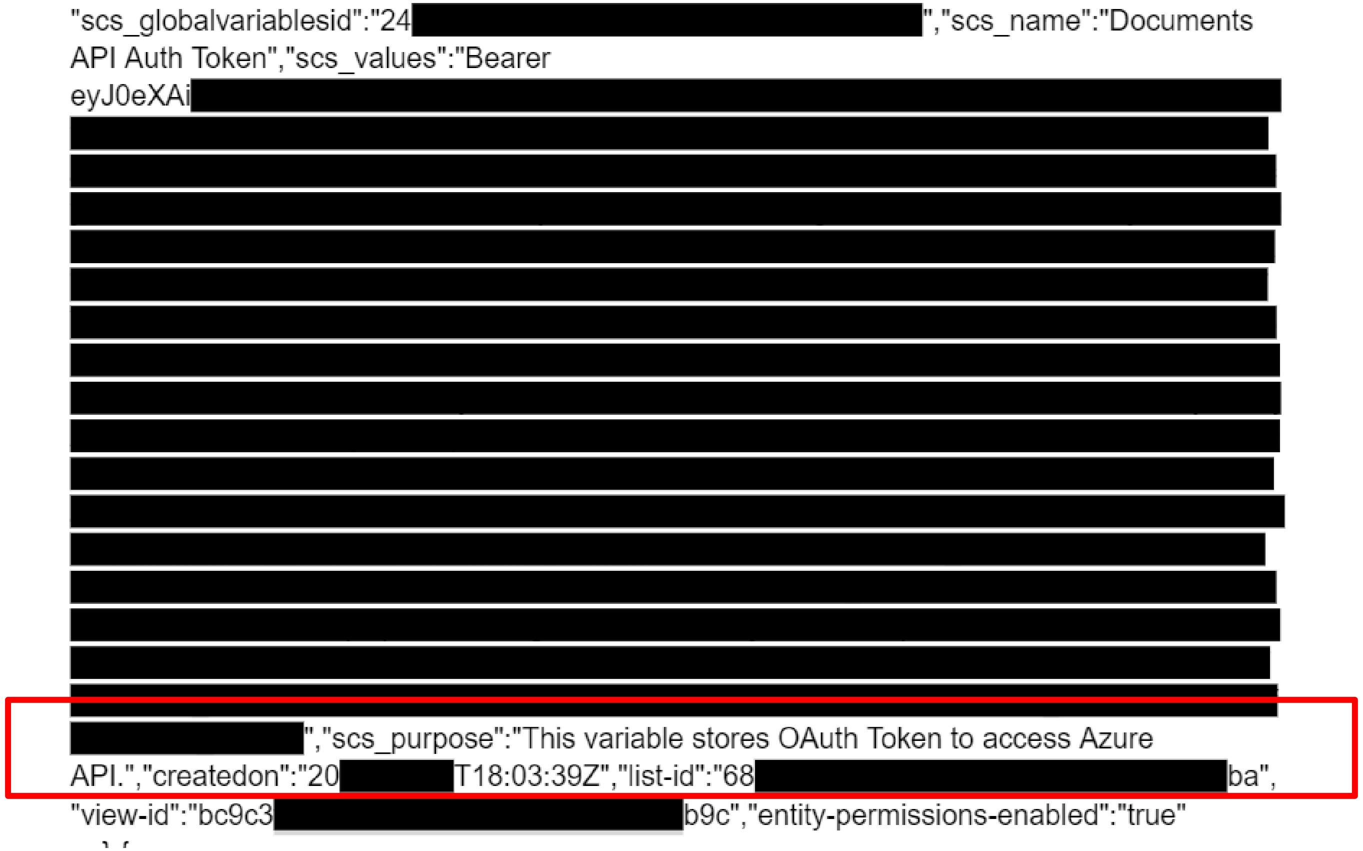


```
▼<service xmlns="http://www.w3.org/2007/app" xmlns:atom="http://www.w3.org/2005/Atom" xml:base=
  ▼<workspace>
     <atom:title type="text">Default</atom:title>
   ▼<collection href="EntityFormSet">
       <atom:title type="text">EntityFormSet</atom:title>
     </collection>
   ▼<collection href="globalvariables">
       <atom:title type="text">globalvariables</atom:title>
     </collection>
   </workspace>
 </service>
```

zenity.io/blog/the-microsoft-power-apps-portal-data-leak-revisited-are-you-safe-now/

Nothing to see here

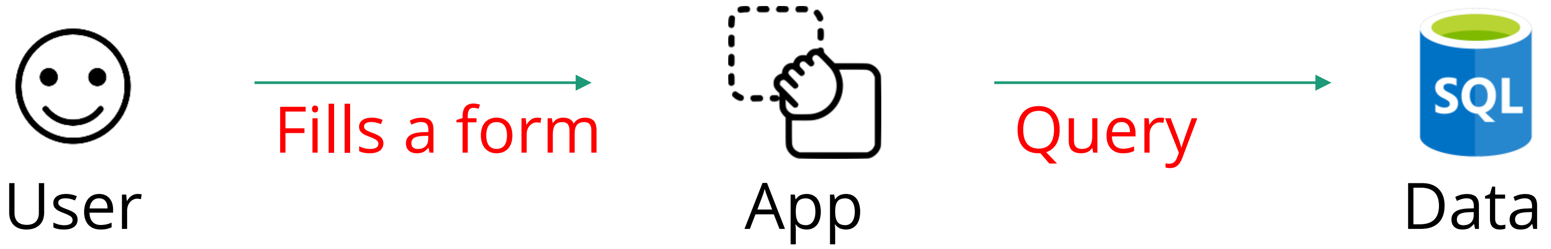
/_odata/globalvariables:



```
"scs_globalvariablesid":"24[redacted]","scs_name":"Documents
API Auth Token","scs_values":"Bearer
eyJ0eXAi[redacted]","scs_purpose":"This variable stores OAuth Token to access Azure
API.","createdon":"20[redacted]T18:03:39Z","list-id":"68[redacted]ba",
"view-id":"bc9c3[redacted]b9c","entity-permissions-enabled":"true"
```

LCNC-SEC-06: Injection Handling Failures

Low-code/no-code applications ingest user provided data in multiple ways, including direct input or retrieving user provided content from various services. Such data can contain malicious payloads that may introduce risk to the application.



User

Fills a form

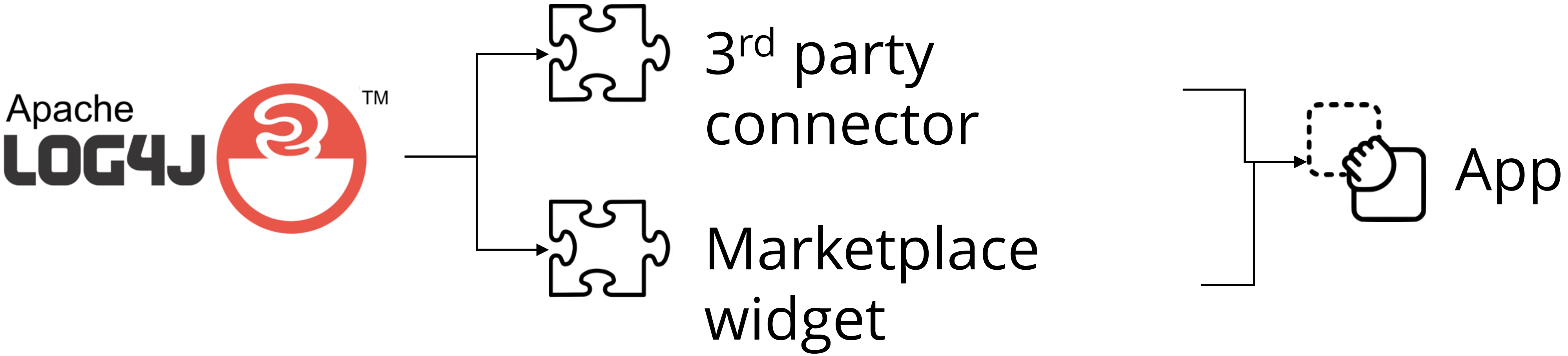
App

Query

Data

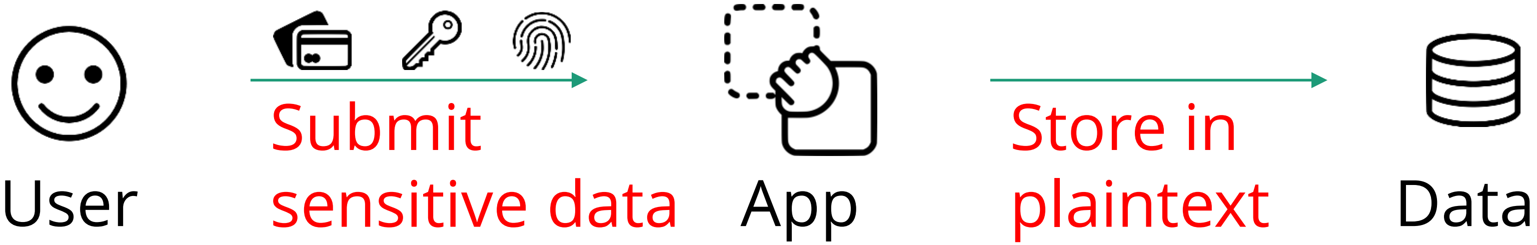
LCNC-SEC-07: Vulnerable, Unmanaged and Untrusted Components

Low-code/no-code applications rely heavily on ready-made components out of the marketplace, the web or custom connectors built by developers. These component are often unmanaged, lack visibility and expose applications to supply chain-based risks.



LCNC-SEC-08: Data and Secret Handling Failures

Low-code/no-code applications often store data or secrets as part of their "code" or on managed databases offered by the platform, which needs to be properly stored in compliance with regulation and security requirements.



User

Submit sensitive data

App

Store in plaintext

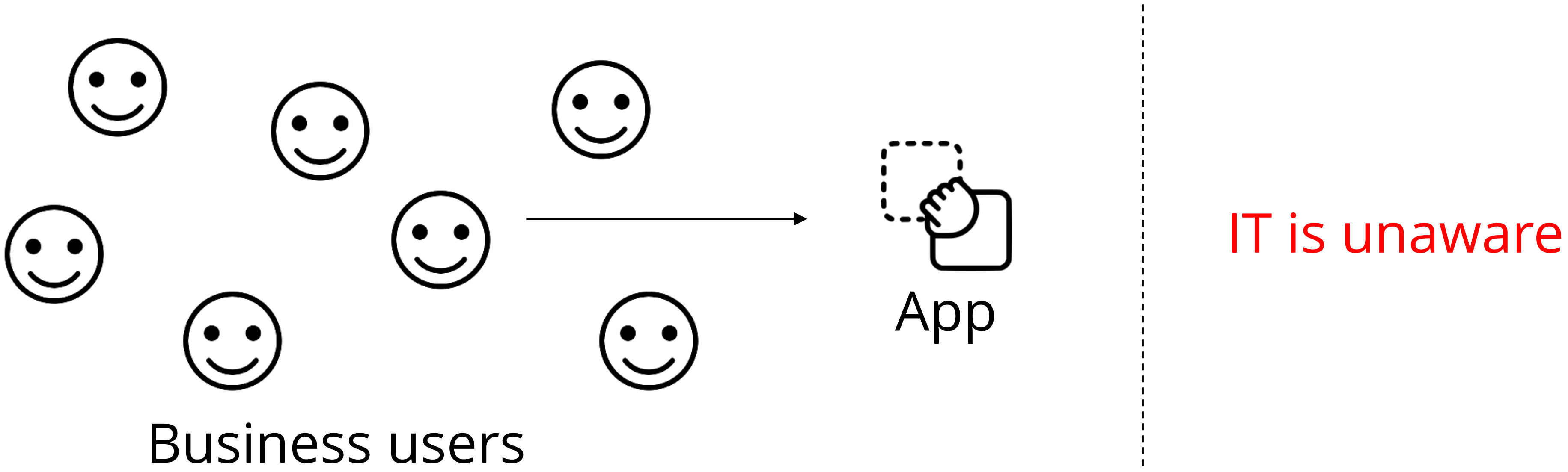
Data

Give-Aware Campaign

- HR team at a large IT company kicked off a Giveaway campaign
- App let’s you choose your donation, charity and plug in your credit card
- Cards are stored in plaintext on an environment available to everyone, including tenant guests
- Compliance audit

LCNC-SEC-09: Asset Management Failures

Low-code/no-code application are easy to create and have relatively low maintenance costs, which makes them prone to abandonment, while still remaining active. Furthermore, internal applications can gain popularity rapidly, without addressing business continuity concerns.



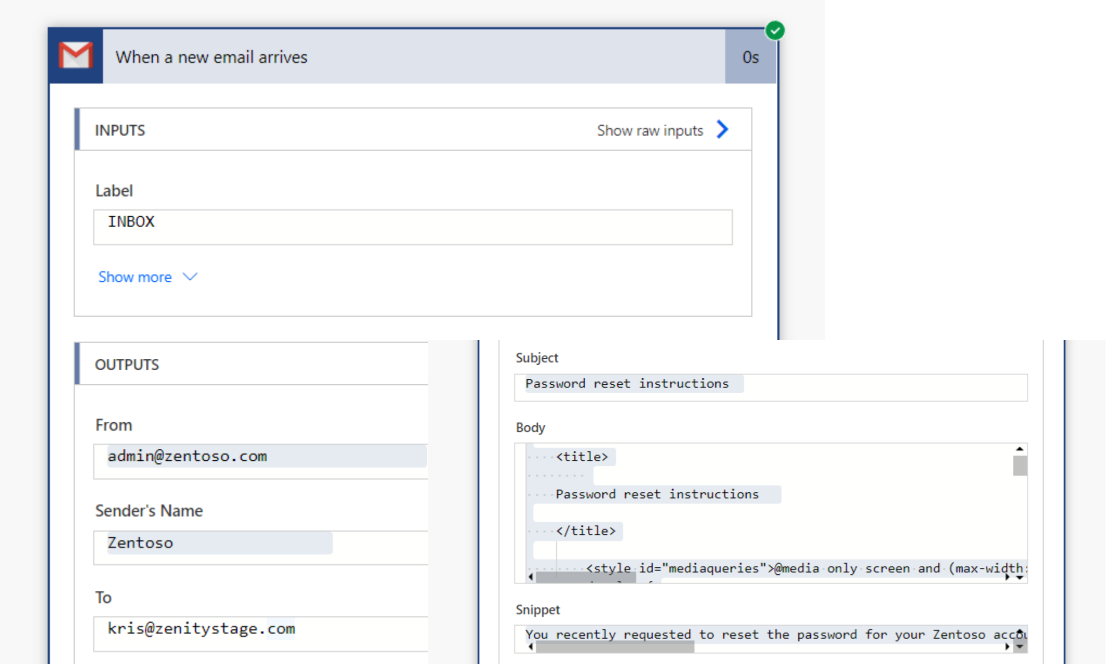
Business users

App

IT is unaware

LCNC-SEC-10: Security Logging and Monitoring Failures

Low-code/no-code applications often lack a comprehensive audit trail, produce none or insufficient logs, and fail to scrub sensitive data from logs.



When a new email arrives 0s

INPUTS Show raw inputs

Label: INBOX

Show more

OUTPUTS

From: admin@zentoso.com

Sender's Name: Zentoso

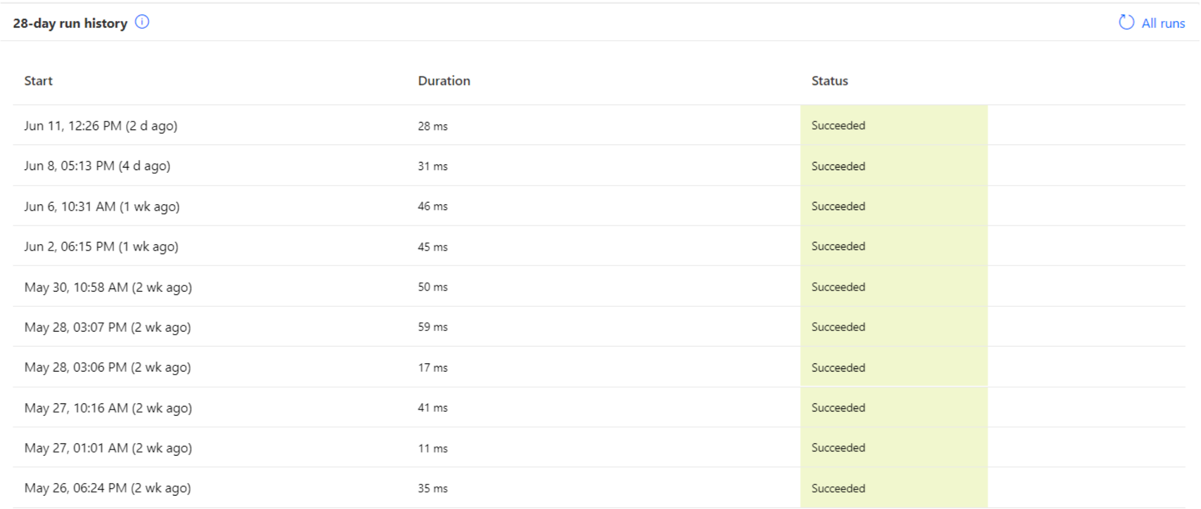
To: kris@zenitystage.com

Subject: Password reset instructions

Body:

```
    <title>
    Password reset instructions
    </title>
        <style id="mediaqueries">@media only screen and (max-width:
```

Snippet: You recently requested to reset the password for your Zentoso accou



28-day run history ⓘ All runs

Start	Duration	Status
Jun 11, 12:26 PM (2 d ago)	28 ms	Succeeded
Jun 8, 05:13 PM (4 d ago)	31 ms	Succeeded
Jun 6, 10:31 AM (1 wk ago)	46 ms	Succeeded
Jun 2, 06:15 PM (1 wk ago)	45 ms	Succeeded
May 30, 10:58 AM (2 wk ago)	50 ms	Succeeded
May 28, 03:07 PM (2 wk ago)	59 ms	Succeeded
May 28, 03:06 PM (2 wk ago)	17 ms	Succeeded
May 27, 10:16 AM (2 wk ago)	41 ms	Succeeded
May 27, 01:01 AM (2 wk ago)	11 ms	Succeeded
May 26, 06:24 PM (2 wk ago)	35 ms	Succeeded

zenity

Twitter: @mbrg0

Summary

What have we seen

- Low Code / No Code is growing rapidly
  - Probably already in your org
  - Shift focus to business users
- Missing SDLC
- OWASP Top 10 LCNC Security Risks
  - Get involved
  - Learn more

Opportunities - Champion Low Code / No Code AppSec in your org

- Create a Low Code / No Code Security Framework
- No Code SDLC
- Approved user cases
- Guide business users
- Join OWASP Top 10 LCNC Security Risks
- Reach out to be @mbrg0

zenity

Learn more: github.com/mbrg/talks
Twitter: @mbrg0

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

Michael Bargury @ Zenity
BSidesSF 2023