

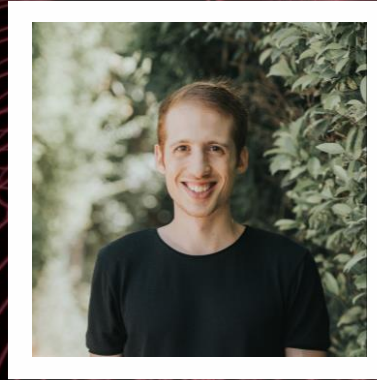


OWASP

Virtual AppSec

APAC

2022



Michael Bargury (@mbrg0)

## No Code Risk: What Happens When We Leave No Code up for Grabs

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

Zenity

# Abstract

Business professionals are no longer waiting for IT to address their needs. Instead, they are increasingly building their own applications with Low-Code/No-Code platforms. Recent surveys show that most enterprise apps are now built outside of IT by business professionals who hold no previous experience in building software.

And so, enterprises are placing \*developer-level power\* in the hands of 100x \*new\* business developers.. What could go wrong?

In short, everything.

In this presentation, we will share extensive research on the security of Low-Code applications based on scanning >100K applications across hundreds of enterprise environments. We will demonstrate how most applications get identity, access and data flow wrong, cover a wide range of security issues found in real environments, and share their backstories and implications.

Next, we will share the first-ever security framework for categorization and mitigation of common Low-Code security issues. We will illustrate why the involvement of AppSec teams is desperately missing from business-led development, and share stories about organizations that got it right.

Finally, we will leave you with an open-source low-code “goat” application, so you can try it out for yourselves and help educate others and become a low-code security champion in your organization.

# About me

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



@mbrg0



[bit.ly/lcsec](https://bit.ly/lcsec)

# Outline

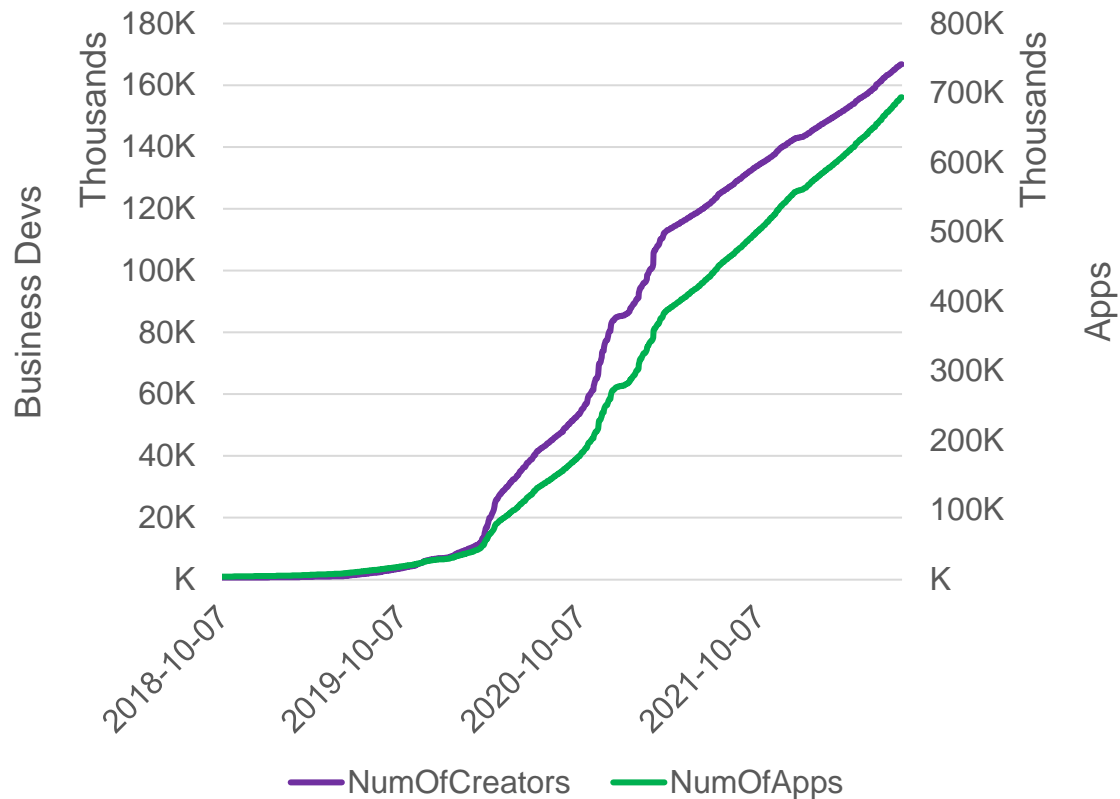
- How pervasive is it?
- Low Code / No Code growth and evolution
- The “hit-save” SDLC
- OWASP Top 10 LCNC Security Risks
- Learn more

01

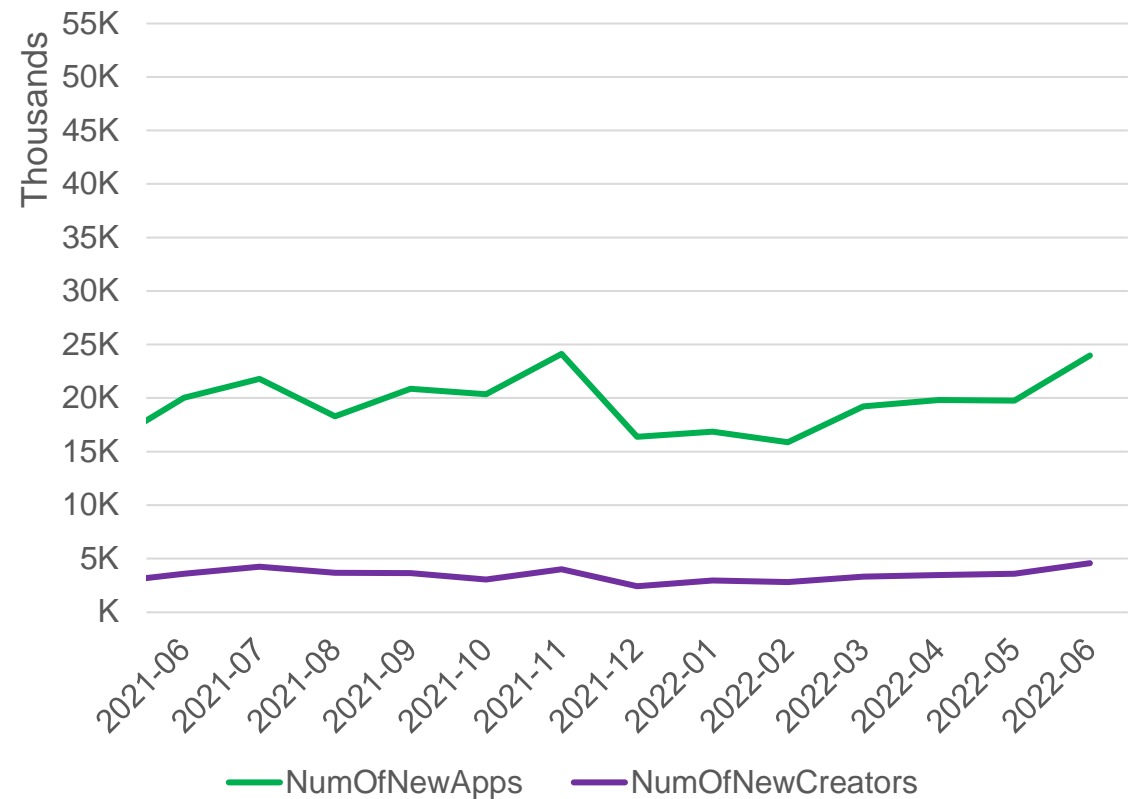
Business-Led Development Is Here

# Exponential Growth in Business Development

Apps/Devs Over Time



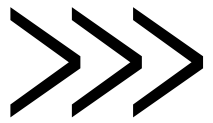
New Apps/Devs Introduced Monthly



02

The Low-Code/No-Code Evolution:  
How did we get here?

# Business Needs



# IT Capacity



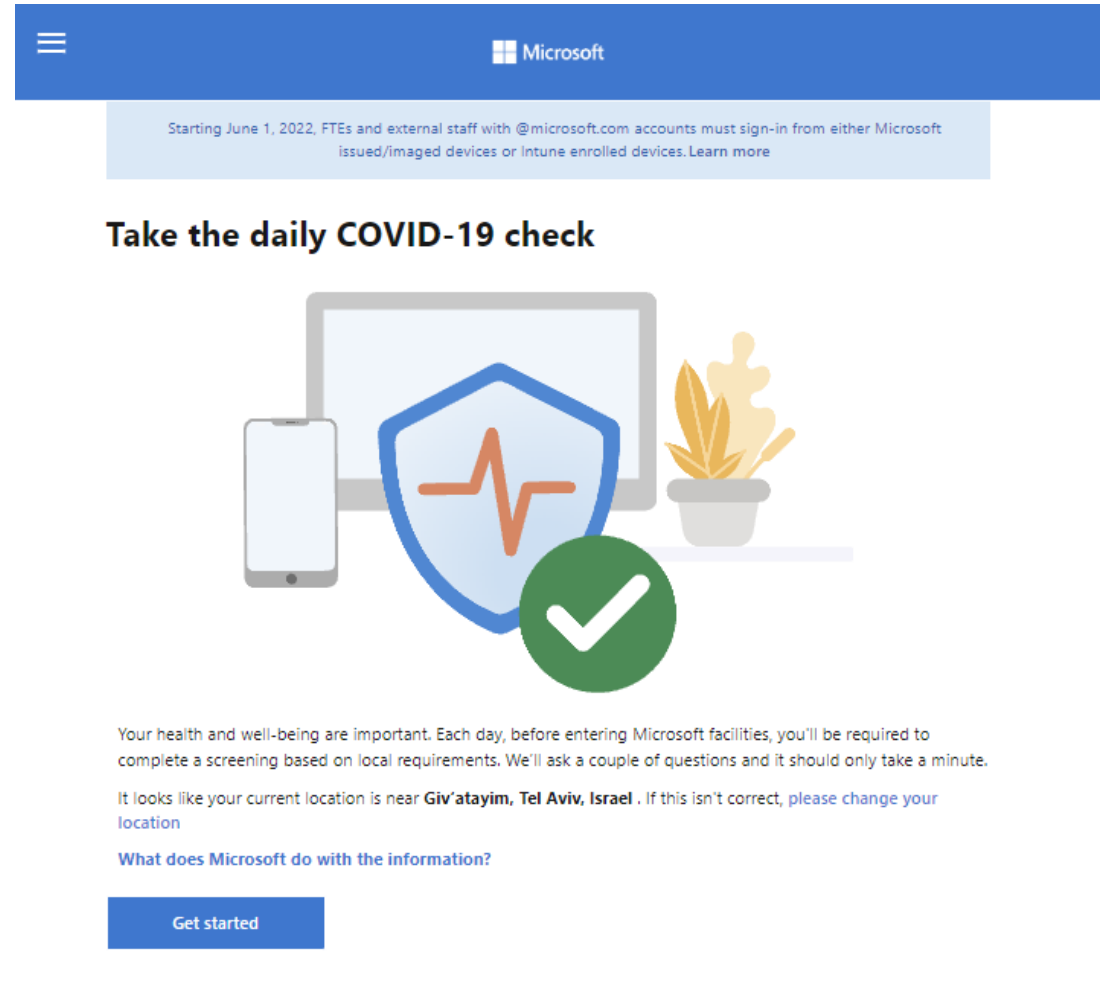


# Build Business Apps Faster

How low code / no node accelerates development:

- Ease of use lowers barrier to entry
- Off-the-shelf integrated components
- Key app features are baked-in (AuthN, AuthZ, ..)
- Connectors to on-prem, cloud and SaaS
- “Save” to deploy
- No infra to maintain

# COVID health check app by Microsoft

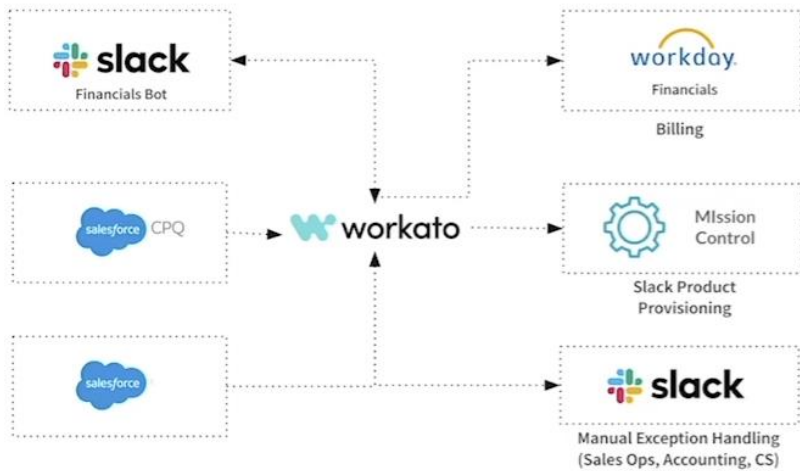


The screenshot shows the Microsoft COVID-19 health check app interface. At the top, there is a blue header with a hamburger menu icon on the left and the Microsoft logo on the right. Below the header, a light blue banner contains the text: "Starting June 1, 2022, FTEs and external staff with @microsoft.com accounts must sign-in from either Microsoft issued/imaged devices or Intune enrolled devices. Learn more". The main heading is "Take the daily COVID-19 check". Below this is an illustration featuring a laptop, a smartphone, a shield with a red heartbeat line, and a green checkmark in a circle. The text below the illustration reads: "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](#)". Below this is a section titled "What does Microsoft do with the information?" followed by a blue "Get started" button.

<https://aka.ms/healthcheck>



### Automating order to cash fulfillment



💰 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

# Order-to-cash automation by Slack

# 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”*

# A Humble Beginning – Low Code as Extensibility

*“With Dynamics, ..., we also launched this very powerful platform, the Power Platform -- ... which acts as the extensibility framework for Microsoft Graph, extensibility framework for Dynamics, as well as Microsoft 365, and embeddable by every SaaS ISV.”*

*Satya Nadella, Microsoft Build 2018*

# Shift to Empowerment of Business Users

*“Anyone can be a developer, completely transforming how your business operates”*

*“... we need to empower citizen developers with tools that are low-code/no-code tools so that they can build out these applications .... In fact, there are already 2.5 million citizen developers using Power Platform ...”*

*“Once Excel was introduced, a lot of people were able to build spreadsheets and become numerical and analytical ... think about all the white-collar-ish jobs that were created ... we want the same thing to happen with low-code/no-code.”*

*Satya Nadella, Microsoft Ignite 2019*

# Business Users are Leading The Way

*“By 2025, 70% of new applications deployed for the enterprise will use low-code or no-code tools, up from less than 25% in 2020.”*

*“With Power Platform, we have the leading business process automation and productivity suite for domain experts in every industry, with 20 million monthly active users.”*

*Satya Nadella, Microsoft Inspire 2022*

# The Focus Has Shifted To Business Users







# The Race for a New Excel

Big vendors have a strong incentive to empower business users



Companies are lacking IT resources and need a solution for accelerated development

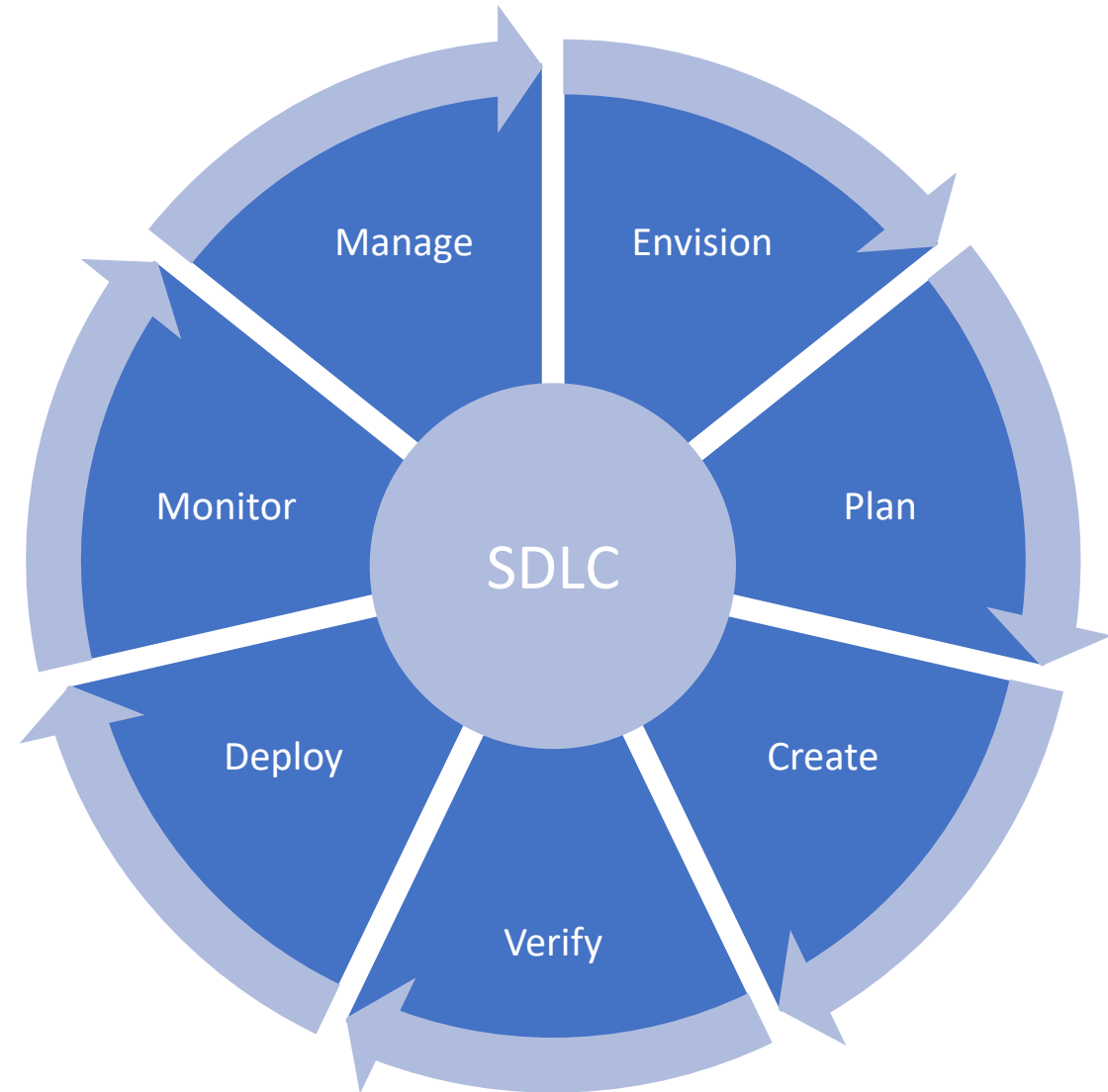


The tech is already there – business users are actually using it

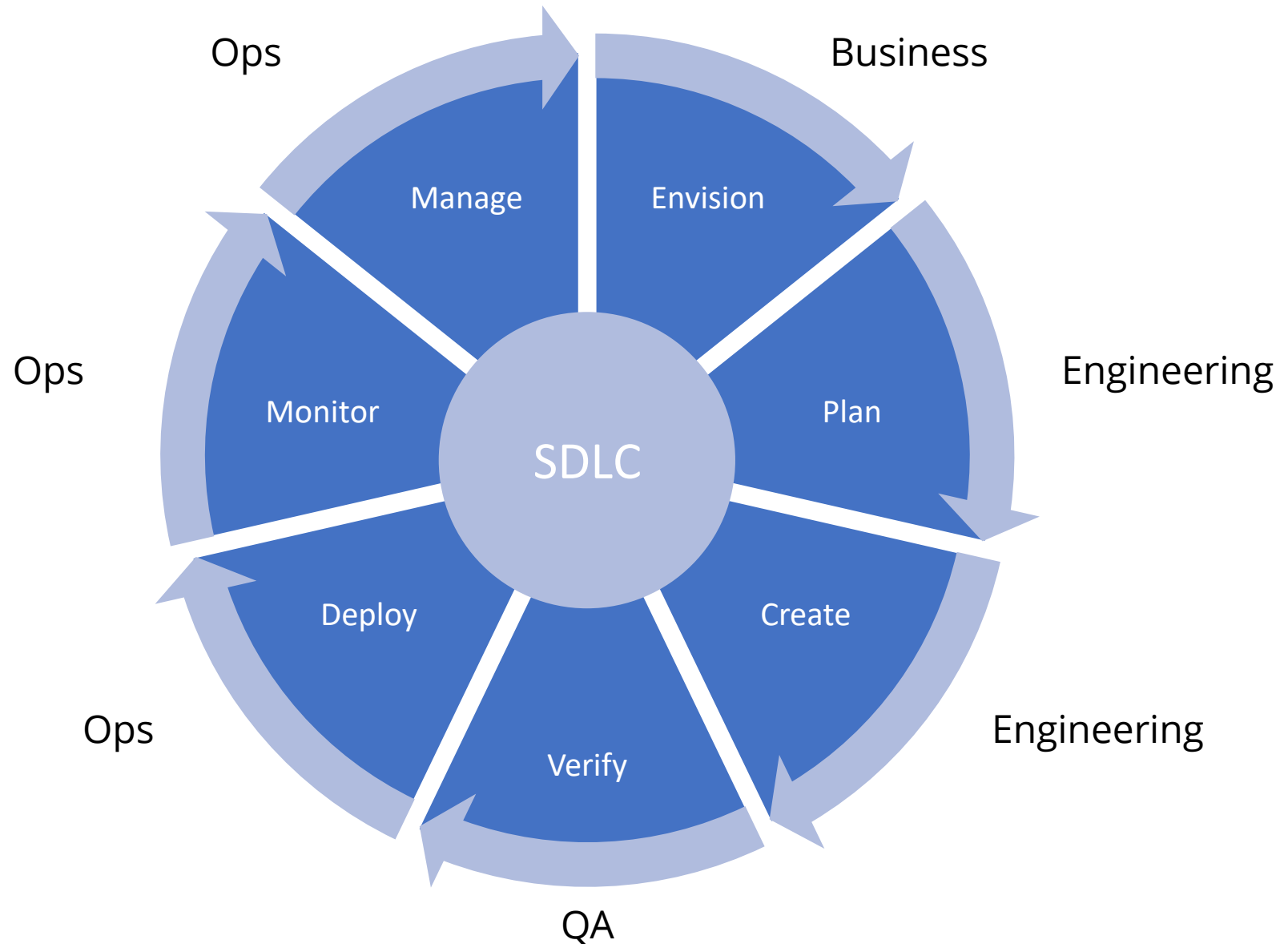
03

# No Code No SDLC?

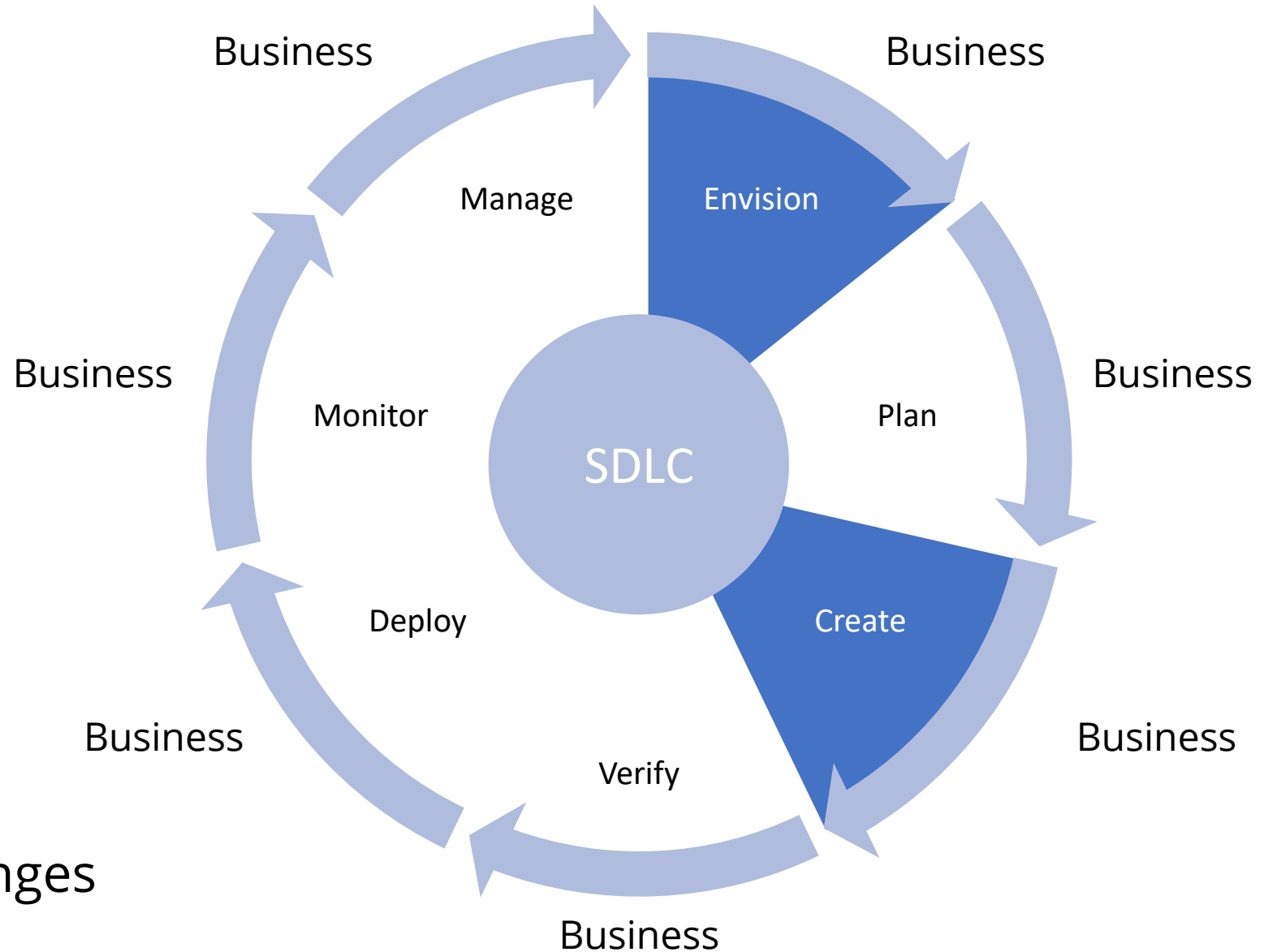
# Software Development Lifecycle



# Software Development Lifecycle

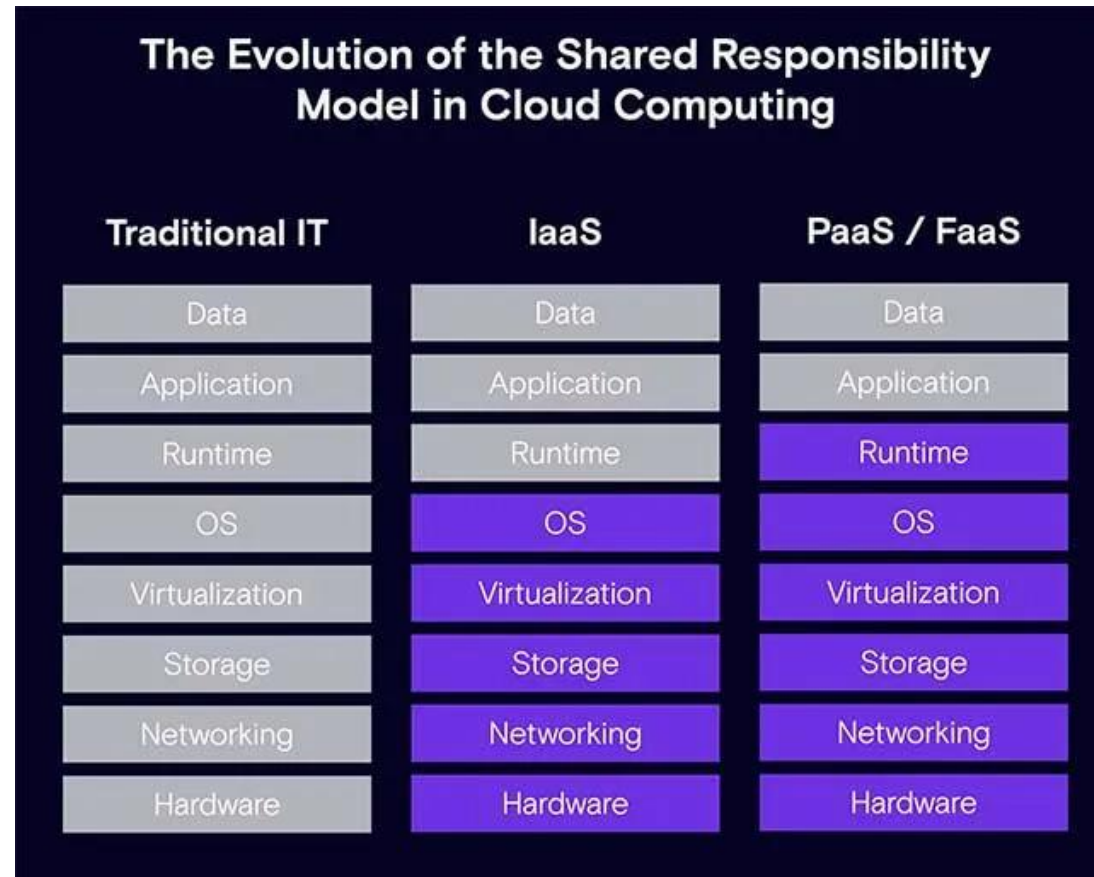


# No Code SDLC?



Hit Save to deploy changes

# The Shared Responsibility Model



04

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





**OWASP**  
low-code/no-code

# Top 10 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](#)



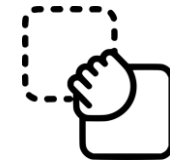
# LCNC-SEC-01: Account Impersonation

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



# Better Customer Care - The Solution

Impact:

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



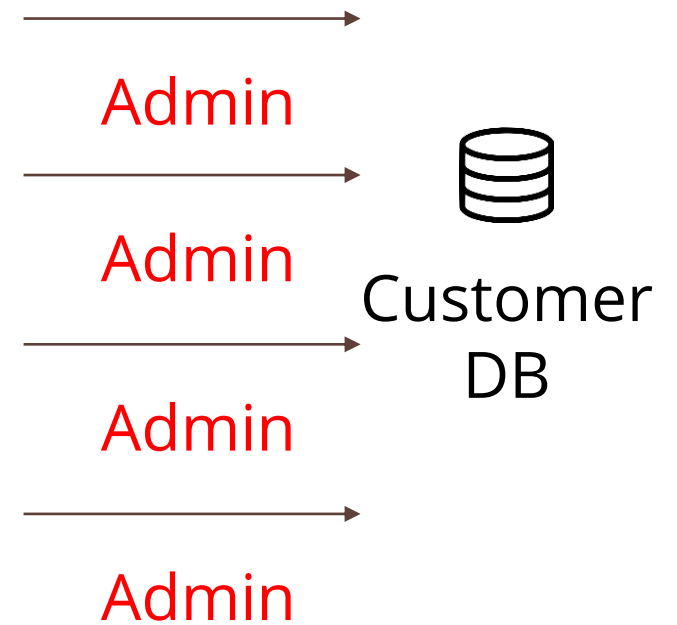
# Meanwhile, At the SOC

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?



# 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

The image displays two overlapping software interfaces: Power Automate on the left and Zapier on the right. The Power Automate interface shows a list of connections in the 'Zenity Stage (default)' environment. The connections table includes:

Name	Modified
ConnectionToFadStorageAccount 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]ba2g@gmail.com Gmail	1 wk ago Connected

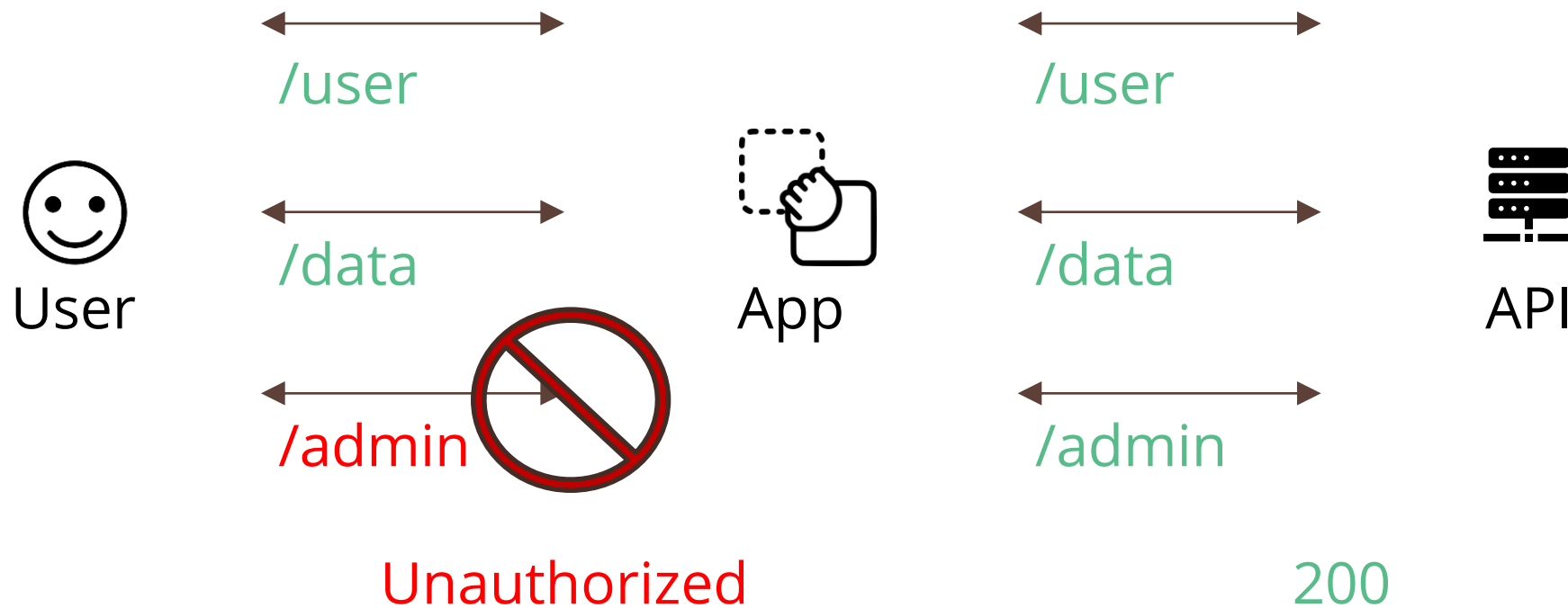
The Zapier interface shows a list of 'Assets' with columns for Name, Status, and Recipes. Assets include:

- Management (Connected, May 22 at 1:47 am, 4 Recipes)
- dev\_HTTP account (Connected, Feb 6 at 1:21 am, 0 Recipes)
- dev\_HTTP account (Connected, Feb 6 at 1:21 am, 0 Recipes)
- dev\_twitter (Connected, Feb 10 at 1:40 am, 1 Recipe)
- FTP at test.rebox.net (Connected, Apr 9, 2021, at 7:05 am, 932 Recipes)
- [redacted]@gmail.com gmail (Connected, Apr 9, 2021, at 5:05 am, 1 Recipe)

Below the Zapier interface, there are summary cards for 'Gmail' (2 Connections, 5 Zaps) and 'Google Sheets' (1 Connection, 2 Zaps). A 'zapier' logo and 'Apps' section are also visible in the center of the image.

# App Reader $\leftrightarrow$ API Admin

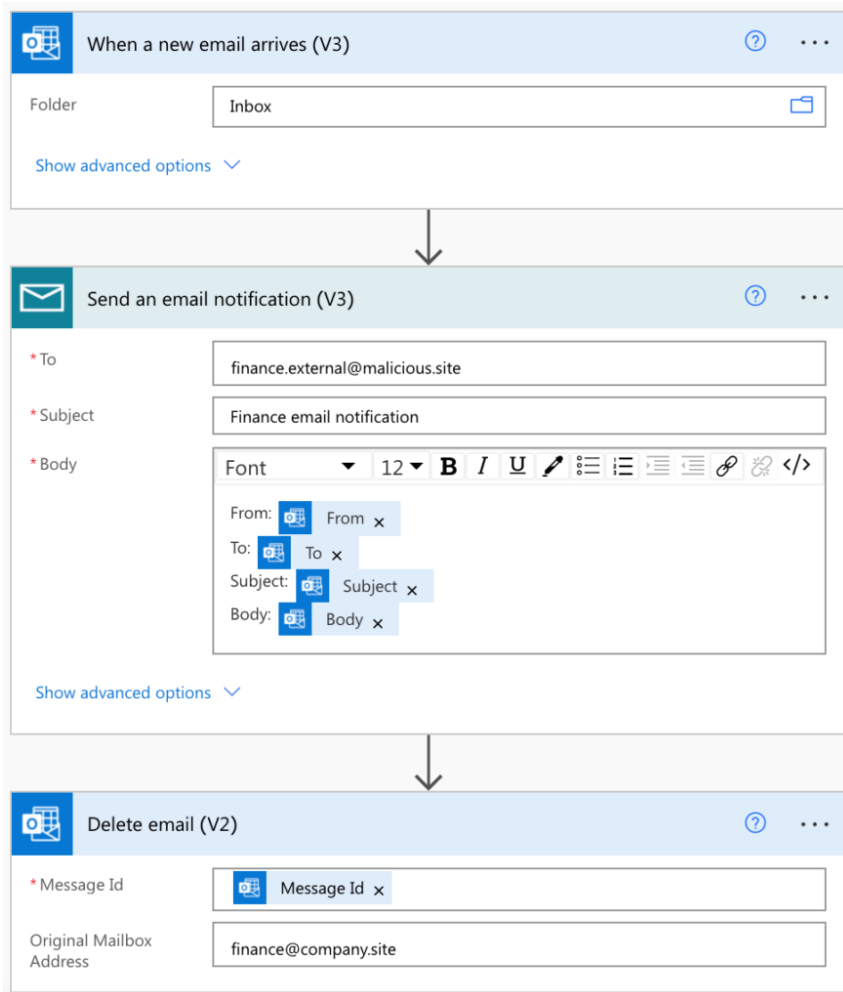
Authorization as front-end logic



# 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

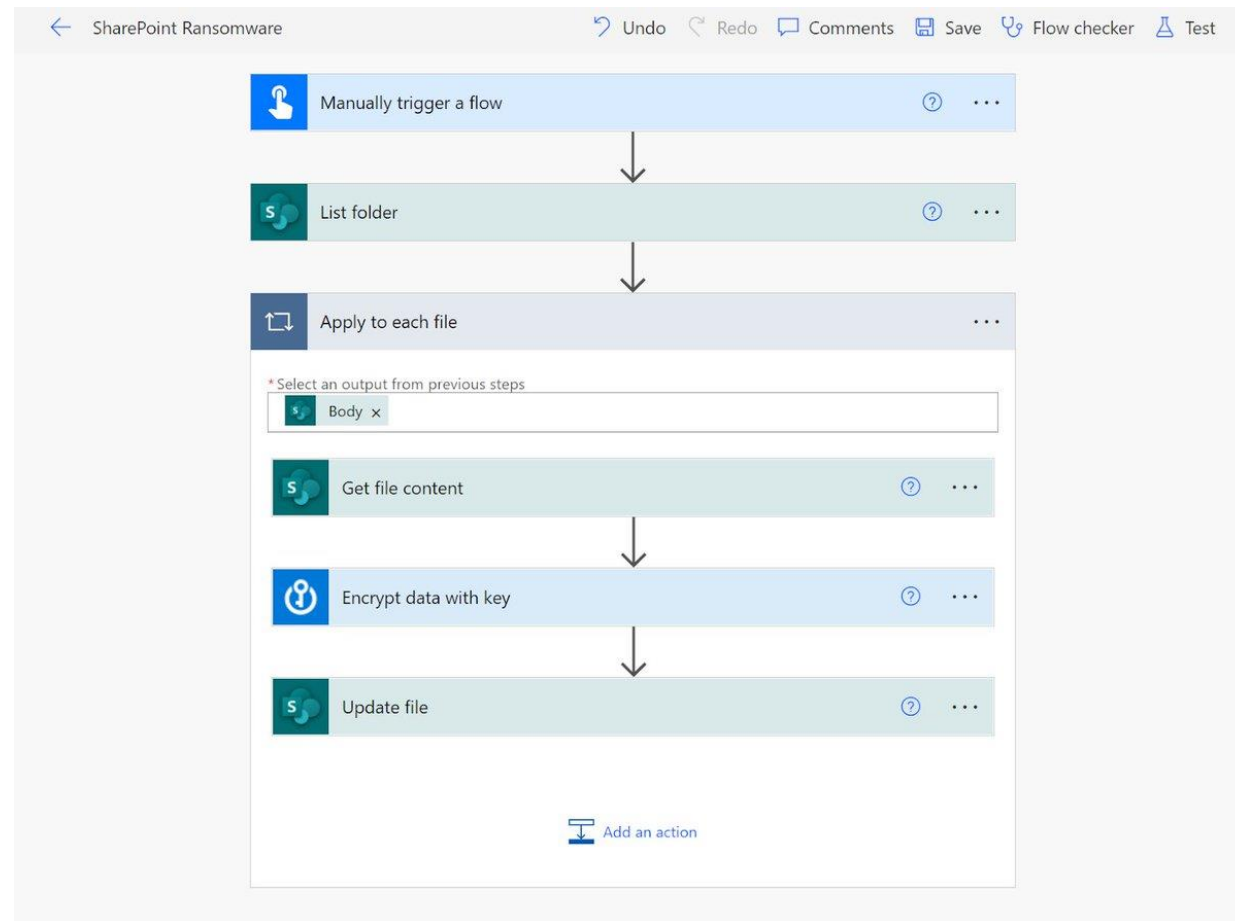


Data is being copied between two separate services using two separate identities – existing defense mechanisms fail

# LCNC-SEC-03: Data Leakage and Unexpected Consequences

If <file found>

Then <encrypt file>



# 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.

The screenshot shows a web interface for configuring a connection. The breadcrumb path is 'Projects > New connection > Connect to FTP/FTPS'. The main heading is 'Connect to FTP/FTPS'. The form contains three sections: 'Connection name' with a text input field containing 'Shared Drive' and a help icon; 'Location' with a dropdown menu showing 'Home assets'; and 'Server type' with a dropdown menu showing 'FTP-S' and 'FTP' (which is highlighted).

# 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



## 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](https://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](https://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/](https://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]
```

```
[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.



# 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.



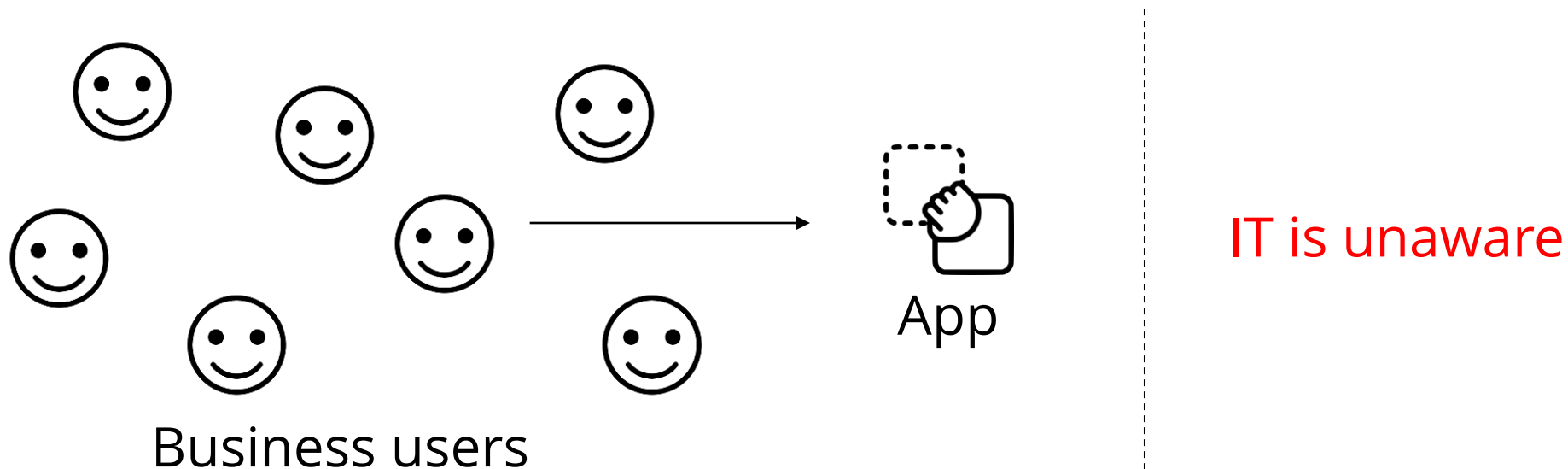
# Give-Aware Campaign

- 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 applications 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.



# 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.

The image displays a no-code workflow interface. On the left, a workflow titled "When a new email arrives" is shown with a "0s" duration and a green checkmark. The "INPUTS" section shows a "Label" field set to "INBOX". The "OUTPUTS" section shows an email template with fields for "From" (admin@zentoso.com), "Sender's Name" (Zentoso), and "To" (kris@zenitystage.com). The email body contains HTML code for a password reset instruction, including a title and a snippet: "You recently requested to reset the password for your Zentoso acco".

On the right, a "28-day run history" table shows the execution status of the workflow. The table has three columns: "Start", "Duration", and "Status". All 12 entries show a "Succeeded" status.

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

05

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

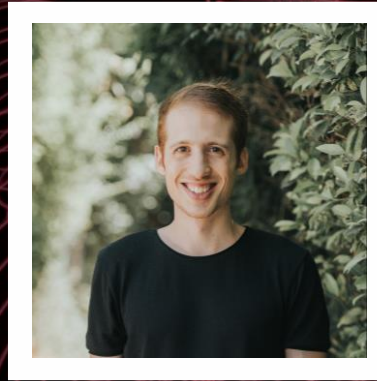


OWASP

Virtual AppSec

APAC

2022



Michael Bargury (@mbrg0)

No Code Risk: What Happens  
When We Leave No Code up for  
Grabs

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

Zenity