



OWASP 2023
GLOBAL
AppSec

WASHINGTON

DC

OCT 30 • NOV 3





OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3



OWASP Low-Code / No-Code Top 10

Michael Bargury (Zenity), Ory Segal (Palo Alto Networks), Don Willits (Microsoft), John McTiernan (DT Group), Yianna Paris (Xebia), Ziv Daniel Hagbi (Zenity) and many more!

@OWASPNoCode



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30 - NOV 3

OWASP LCNC Top 10

@OWASPNoCode

OWASP TOP 10



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3

Why LCNC? Why new?

@OWASPNoCode

Tree view

Screens Components

Search

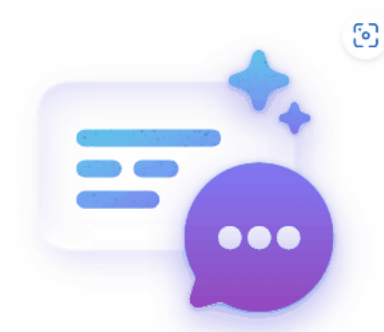
+ New screen

> App

- Screen1

Add an item from the Insert pane or connect to data

Copilot PREVIEW



What do you want to do?

Describe what you want to do with this app, and AI will do it for you.

- Add a text label
- Add a gallery
- Add a button
- Add an email screen

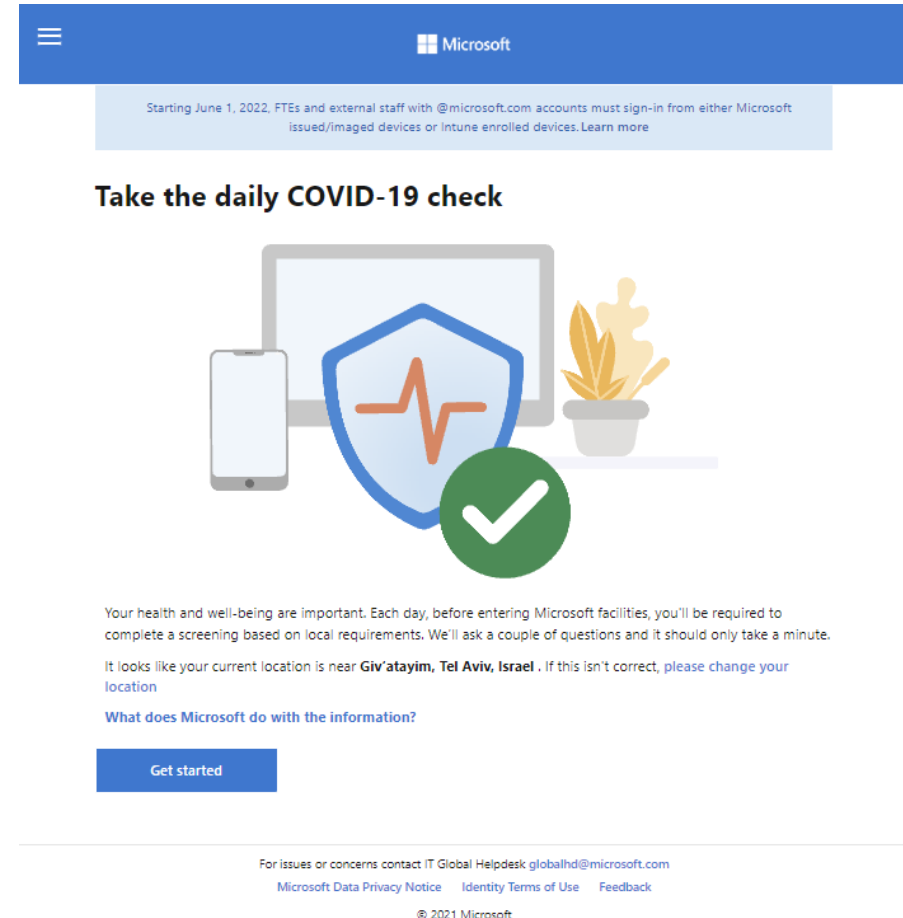
What do you want to do with this app?

[Send icon]

Make sure AI-generated content is accurate and appropriate before using. [See terms](#)

Source:
@RezaDorrani

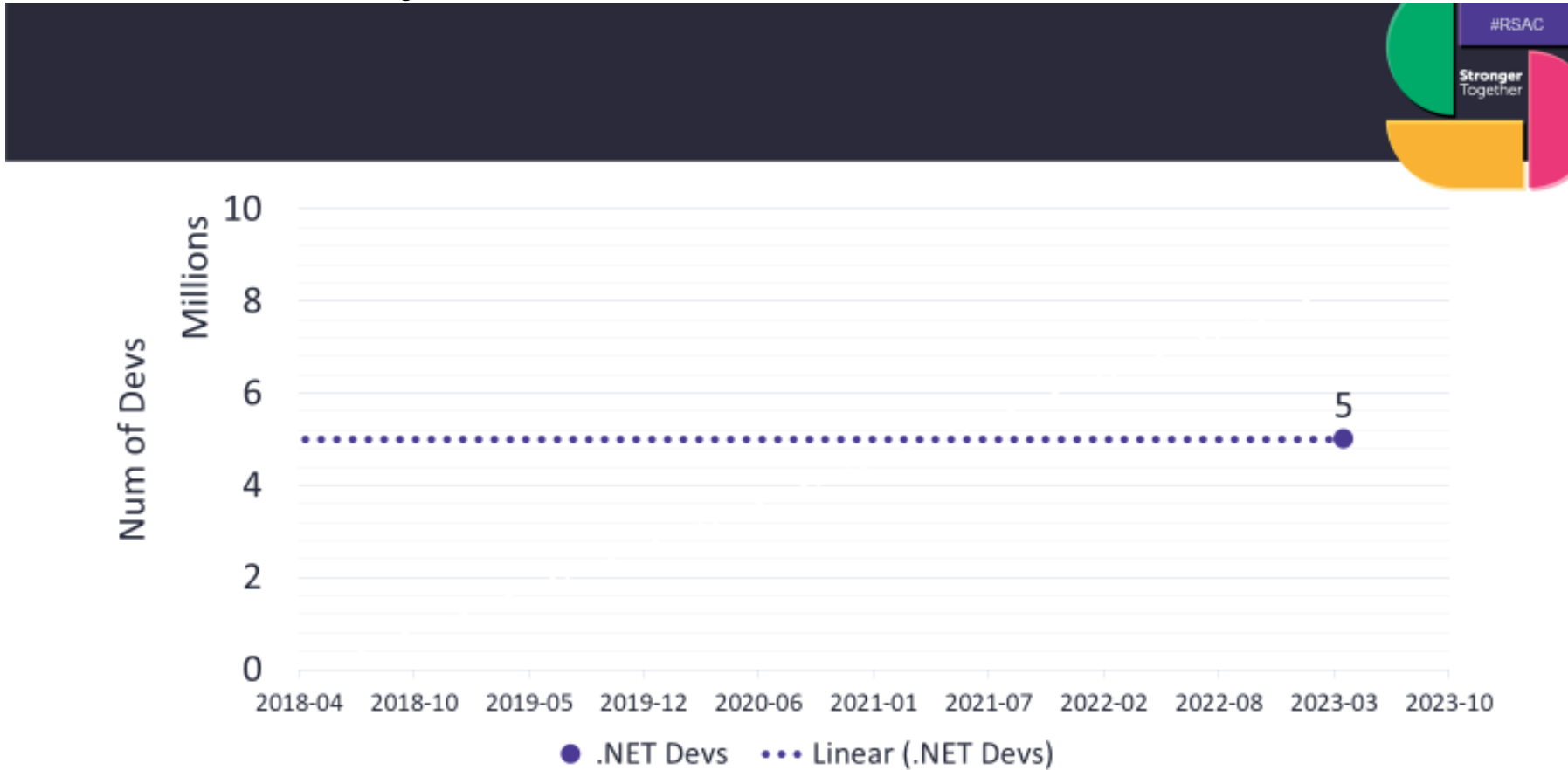
COVID health check app by Microsoft



The screenshot shows the Microsoft COVID-19 health check app interface. At the top, there is a blue header with the Microsoft logo and a hamburger menu icon. 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/imagined 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 link: "What does Microsoft do with the information?". At the bottom of the main content area is a blue button labeled "Get started". The footer contains the text: "For issues or concerns contact IT Global Helpdesk globalhd@microsoft.com", "Microsoft Data Privacy Notice", "Identity Terms of Use", "Feedback", and "© 2021 Microsoft".

<https://aka.ms/healthcheck>

C# devs today



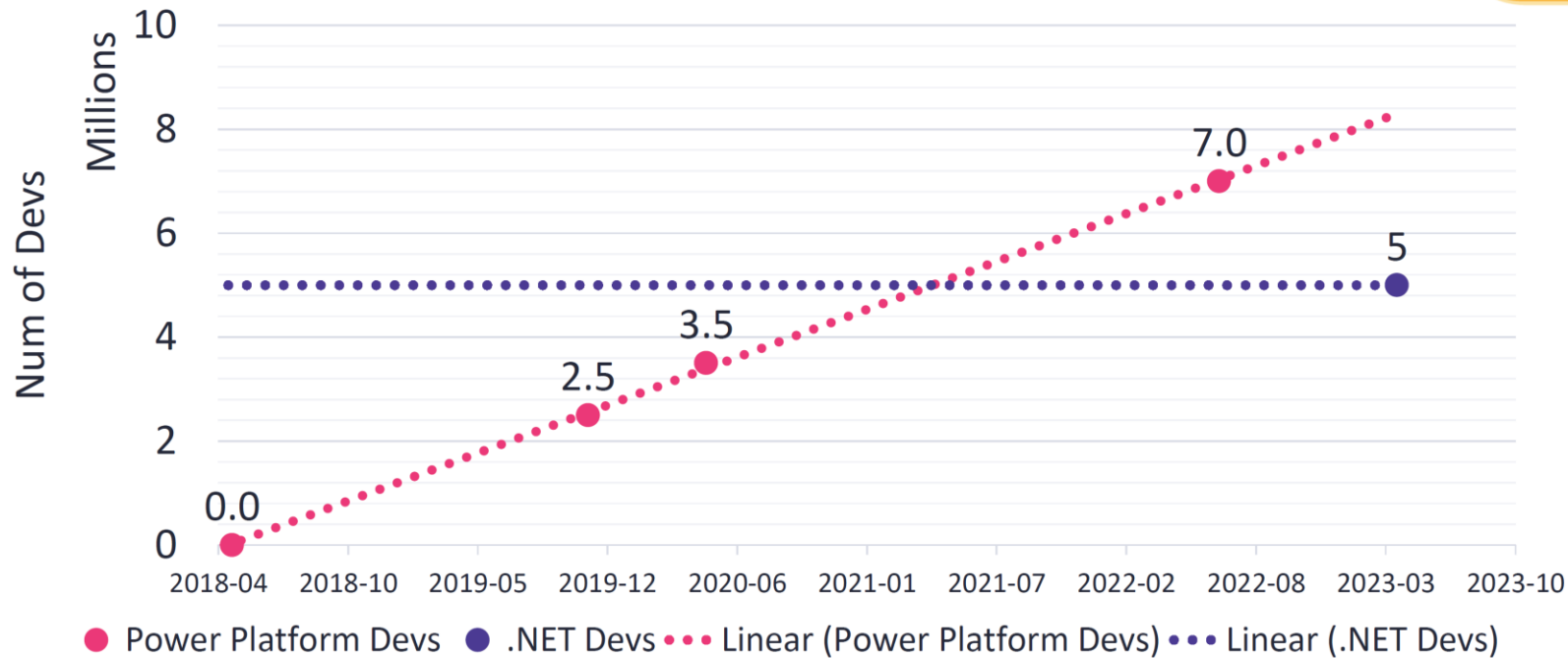
Sources: Microsoft Build 2018, Ignite 2019, Build 2020, Protocol 2022

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

Michael Bargury
RSAC 2023

~8M active Power devs today!

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



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

Michael Bargury
RSAC 2023

AI implies No Code apps become more complex and more useful

Press release

14 Jun 2023 | London, GB

EY unlocks Microsoft Azure OpenAI Service to empower EY Tax professionals globally with EY Tax Copilot

Press contact



Barbara Dimajo

Assistant Director, Media Relations and Social Media Ecosystems, Ernst & Young LLP



Related topics

- **The EY Tax Copilot program is designed to accelerate how the EY organization innovates, delivers services and provides value to teams and clients**

EY today announces the launch of EY Tax Copilot, an education and enablement program to prepare EY Tax professionals across the globe for the future of low-code technologies powered by generative AI. EY Tax Copilot was created with Microsoft to provide a framework to take advantage of Microsoft Azure OpenAI Service, Power Platform and other Microsoft technologies to improve EY Tax platforms, including EY Global Tax Platform, EY Mobility Pathway, EY Global Payroll Operate, EY Tax FS, and EY Indirect Tax, as well as support tax professionals and clients.

Tailored to one's skills and career path, this program will focus on building design and development capabilities that are appropriate for each individual's role at the EY organization and future as a tax or tax-law professional. Some professionals will focus on value creation and design, while others will be enabled to utilize **Microsoft Power Platform** to quickly create solutions. EY Fabric, which underpins EY Tax's platforms, is one of the largest B2B technology platforms in the world, analyzing over 1 trillion lines of financial data annually.

In collaboration with EY Tax Copilot, EY Fabric will allow EY Tax teams to not only leverage **Microsoft Power Platform** with EY accelerators, but also connect their efforts to other technology and data assets being built across the organization, reducing duplication across the organization and improving technology value for all. EY Tax professionals will be able to efficiently provide technology-based value as trusted tax advisors by taking advantage of EY Fabric's one-of-a-kind global deployment and governance capabilities.



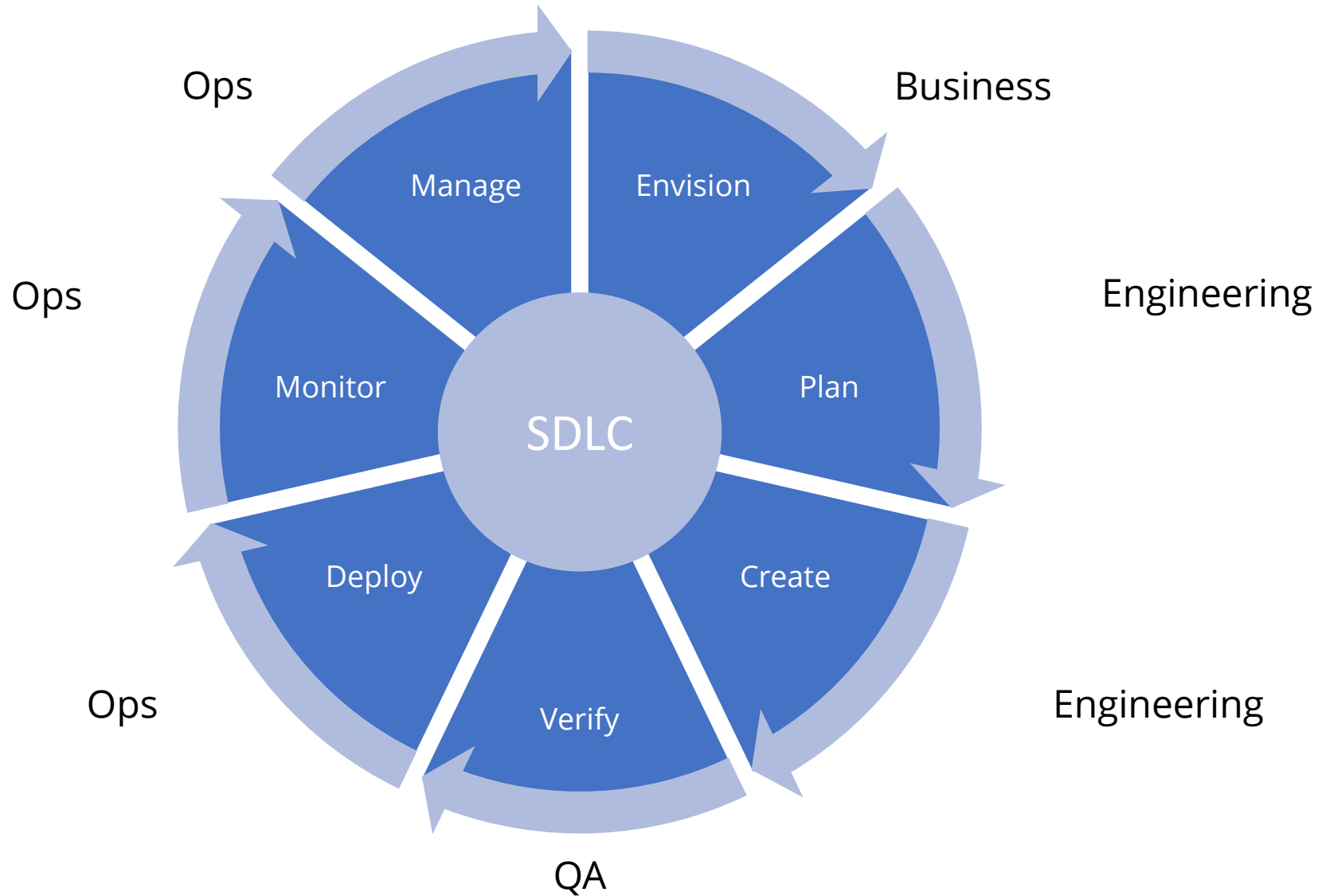
OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3

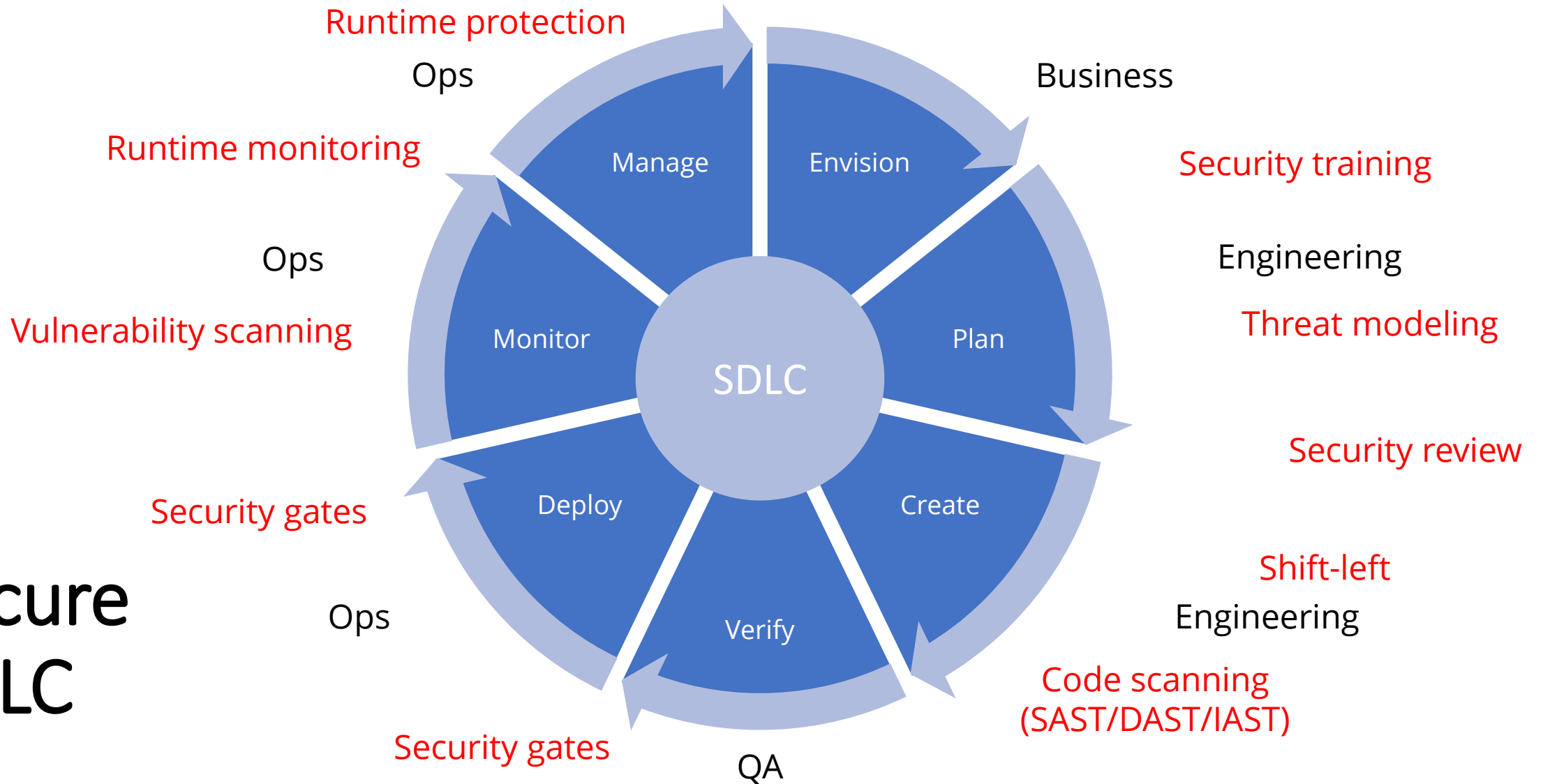
No Code No SDLC

@OWASPNoCode

The SDLC

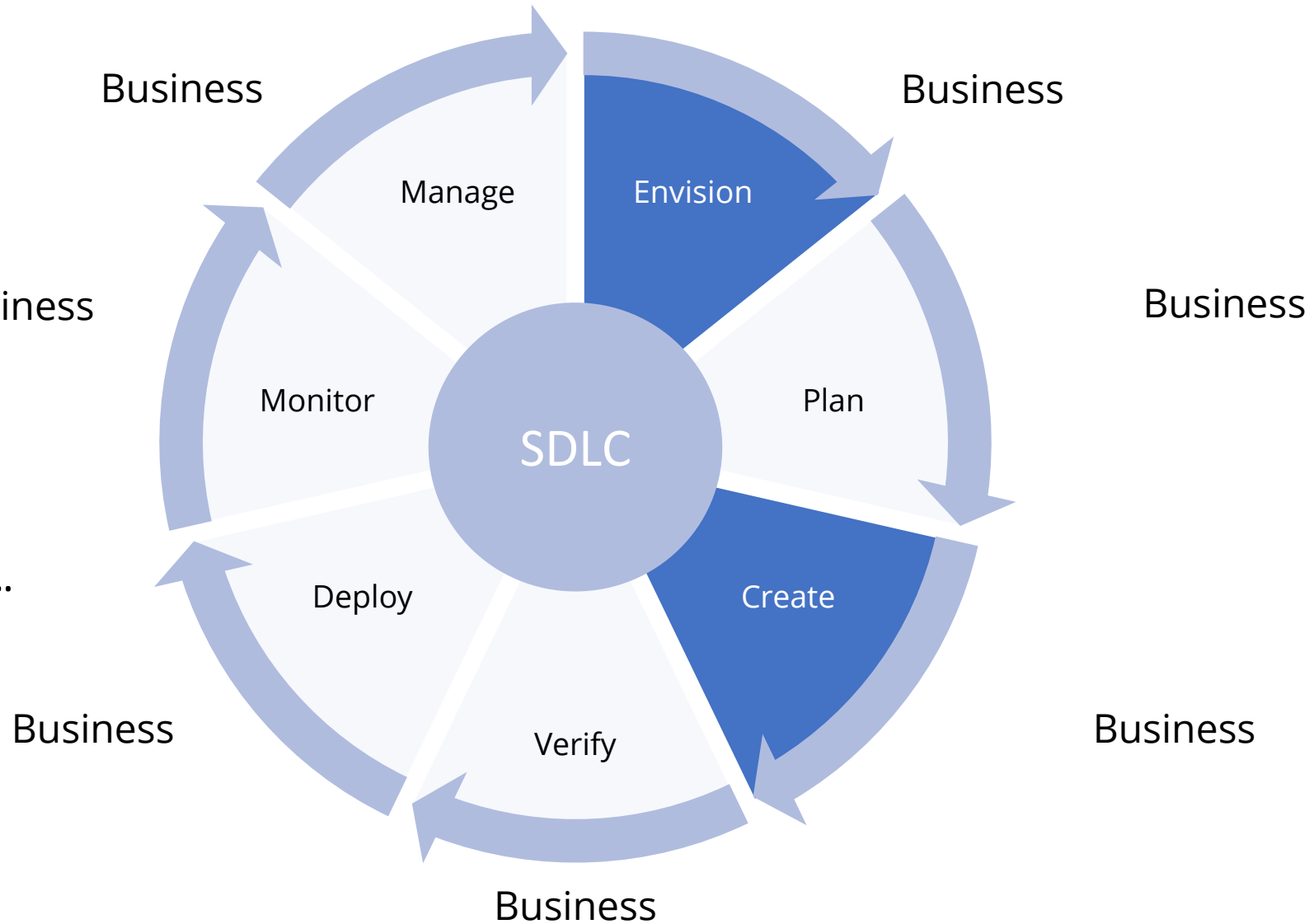


Secure SDLC



No Code No SDLC

Hit Save to deploy...



Lacking security controls

Existing security control	Low-code / no-code
Security training	Can we expect business users to be security savvy?
Threat modeling	Can't scale to 000s apps/year
Security review	Can't scale to 000s apps/year
Code scanning	No code to scan
Artifact scanning	Mostly unavailable, overwhelming FPs
Security gates	Lacking CI/CD
Vulnerability scanning	No awareness to low-code leads to overwhelming FPs
Runtime monitoring	Lacking logs
Runtime protection	Lacking instrumentation



Recap – security process and controls are severely lacking

- Has access to business, health, financial data
- Runs as SaaS
- Lacking SDLC
- Lacking security controls
- Developers with no security savviness
- 10-100x the scale of application development



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3

OWASP LCNC Top 10

@OWASPNoCode



Unique about LCNC

- Devs can be anyone from a pro dev to a citizen dev
- No SDLC
- No security controls
- 10-100x scale of app development
- Code is generated (platform owns code-gen vulns)
- Focused on logical vulns

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



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





OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30 - NOV 3

OWASP LCNC Top 10

@OWASPNoCode

LCNC-SEC-01: Account Impersonation

LCNC-SEC-01: Account Impersonation

The Gist

A short description for security pros

Low-code/no-code applications can be embedded with a developer account which is used implicitly by any application user. This creates a direct path towards Privilege Escalation, allowing an attacker to hide behind another user's identity, circumventing traditional security controls.

Business User Description

A critical component of any system is tracking what user is taking actions in that system. When account impersonation occurs it "looks" like actions taken by one user are being done by another.

A longer description for security pros

A short description for business users

contribution by John McTiernan, DT Group and Yianna Paris @punk_fairybread, Xebia

Description

Identities are embedded within each built application, and multiple users can use that application. This creates a direct path for application users to escalate privileges, which is atypical and should be avoided whenever possible.

Low-code/no-code applications can take advantage of embedded user accounts rather than having their own application identity. Embedded identities can belong to the application creator, or they could be a common identity shared by teams, such as database credentials. They could also be service accounts or shared identities.

The lack of application identity hides the application's existence from monitoring systems outside of the low-code/no-code platform. As an outside viewer, any user that uses the application is impersonating the application's creator, and there is no way to distinguish between the application and its creator. The problem becomes even more acute when applications use different identities to operate on various platforms. In such a case, one user could be used to store files on a file-sharing SaaS and another user to retrieve on-premise data.

LCNC-SEC-01: Account Impersonation

Attack and misuse scenarios for both security pros and business users

Example Attack Scenarios

Scenario #1

A developer creates a simple application to view records from a database. They use their identity to log into the database, creating a connection embedded within the application. Every action that any user performs in this application ends up querying the database using the developer's identity. A malicious user takes advantage of this and uses the application to view, modify or delete records they should not have access to. Database logs indicate that all queries were made by a single user, the trusted developer.

Scenario #2

A developer creates a business application that allows employee responses, the developer uses their personal email account. Using the developer's personal account.

Scenario #3

A developer creates a business application and shares it with a user's identity. Aside from its stated purpose, the app also uses the user's identity. Once the admin uses the app, they inadvertently elevate the developer's permissions.

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.

LCNC-SEC-01: Account Impersonation

What can you do about it?

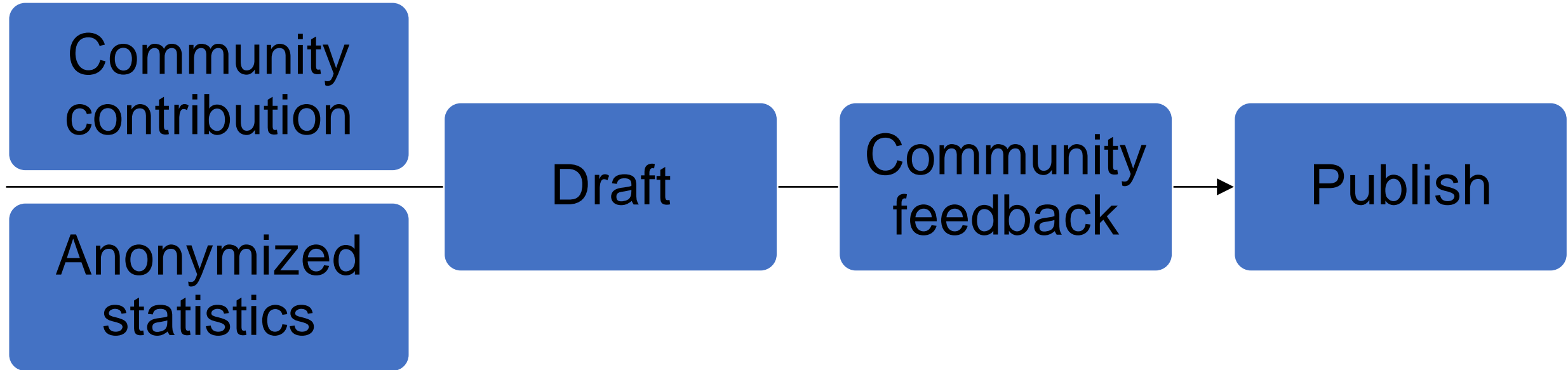
How to Prevent

- Adhere to the principle of least privilege when provisioning connections to databases/services/SaaS
- Ensure applications use dedicated service or application accounts rather than user accounts
- Ensure applications use a single consistent identity across all their connections, rather than a different identity for each.
Use a dedicated service or application account for those connections
- Ensure a proper audit trail is maintained to identify the actor behind actions performed through the shared connection, whether those connections are shared by virtue of users using the application or by granting users access to that connection directly

References

- [Low Code High Risk - Enterprise Domination via Low Code Abuse, DEF CON 2022](#)
- [Watch Out for User Impersonation in Low-Code/No-Code Apps](#)
- [Do low-code / no-code platforms pose a security risk?](#)
- [Credential Sharing as a Service: The Hidden Risk of Low-Code/No-Code](#)

Methodology loop



>1M apps and automations
>8M credentials

Ty to all collaborations
and contributors!



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3

Real-world example – employee onboarding

@OWASPNoCode


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

Search

Environment
Zenity Stage (default)

⌂ ⚙️ ? AA


Start from



Blank app

Create an app from scratch and then add your data


▶ Watch video



Dataverse

Start from a Dataverse table to create a three-screen app


▶ Watch video



SharePoint

Start from a SharePoint list to create a three-screen app


▶ Watch video



Excel

Start from an Excel file to create a three-screen app


▶ Watch video



SQL


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

▶ Watch video



Image

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



- 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
[Watch video](#)

SQL
Start from a SQL data source to create a three-screen app
[Watch video](#)

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



Fill ▾ = fx ▾ White ▾

Tree view [Close]

Screens Components

Search

+ New screen ▾

> App

▾ Screen1 ...

- ✎ Label2_4
- 📄 TextInput1_5
- ✎ Textinput_1
- ✎ LblAppName3_1
- 📄 IconAccept1_1
- 📄 IconCancel1_1
- ✎ Label2_3

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 ▾



Fill ▾ = fx ▾ White ▾

Data [Close]

Search

+ Add data ▾

Sensitive Inputs
Microsoft Dataverse - Current environm...

Employee onboarding form

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security Number

SCREEN [?] >

Screen1

Properties Advanced Ideas

Fill

Background image None ▾

Image position Fit ▾

Fill ▾ = fx ▾ White ▾

Data [Close]

Search

+ Add data ▾

Sensitive Inputs
Microsoft Dataverse - Current environm...

Employee onboarding form

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security Number

Save

SCREEN [?] >


Screen1

Properties Advanced Ideas

Fill [Image icon]

Background image None ▾

Image position [Image icon] Fit ▾



Data

Search

+ Add data

Sensitive Inputs
Microsoft Dataverse

Navigation icons: Home, Layers, Plus, Data, Recent, (x), Tools, Search, Settings, Help

Microsoft Power Platform

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


- Power BI**
Business analytics
- Power Apps**
App development
- Power Automate**
Process automation
- Power Virtual Agents**
Intelligent virtual agents
- Power Pages**
External-facing websites

- Data connectors**
- AI Builder**
- Dataverse**

Ideas

None

Fit



Power Automate Search

Environments Zenity Stage (default)

Update Employee Info in HR system

Undo Redo Comments Save Flow checker Test

When a row is added, modified or deleted

Send email (V2)

To: hrorg@cloudcore.com

Subject: New Employee Update info

Body: 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.

+ New step Save

Ask a chatbot



Employee

- 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





OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30 - NOV 3

OWASP LCNC Top 10

@OWASPNoCode

Employee onboarding – findings

Search



Employee onboarding form

Full legal name

Address

Date of birth

Personal email

Phone number

Social Security Number



Save




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	



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
<input checked="" type="checkbox"/> 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

Table with columns: Employee Name, SSN, Address, Contact. Rows include Jamie Reading, Brooklyn Gonzalez, Henry Mitchell, Savannah Perez, Ella Gonzalez, Riley Mitchell, Nathan Perez, Daniel Martin, and Layla Gonzalez.



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)

Update Employee Info in HR system

Undo Redo Comments Save Flow checker Test

When a row is added, modified or deleted

Send email (V2)

To: hrorg@cloudcore.com

Subject: New Employee Update info

Body: 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.

+ New step Save

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

INPUTS Show raw inputs

Change type: 4

Table name: cr6e4_sensitiveinput

Scope: 4

OUTPUTS Show raw outputs

body

```
{
  "cr6e4_name": "Daniel Wood",
  "_modifiedby_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
  "_modifiedby_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemusers",
  "_modifiedby_type": "systemusers",
  "cr6e4_ssn": "78051120",
  "createdon": "2023-08-07T16:40:48Z",
  "ItemInternalId": "f1ef4327-4135-ee11-bdf4-6045bd8f7e0b",
  "SdkMessage": "Create"
}
```

Connection: zivh@zenitystage.com

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": "daniel1ds@gmail.com",
    "_owningbusinessunit_value": "eddf52a-e501-ec11-94ee-0022488300bc",
    "_owningbusinessunit_value@Microsoft.Dynamics.CRM.lookuplogicalname": "businessunits",
    "_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": "systemusers",
    "_createdby_type": "systemusers",
    "cr6e4_dateofbirth": "10.10.1990",
    "ownerid_value": "b3671a7c-c17d-ec11-8d21-000d3a2f76f7",
    "_ownerid_value@Microsoft.Dynamics.CRM.lookuplogicalname": "systemusers",
    "_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": "systemusers",
    "_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"
  }
}
```



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

Update Employee Info in HR system

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

Add a user or group as owner

- Ziv Hagbi
- HR-All**

Embedded connections
Everyone listed as an owner will have access to all these connections and will only be able to use them in this flow.
[Learn more](#)

Connections in use

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

- zivh@zenitystage.com Microsoft Dataverse
- maortzury@gmail.com Gmail



Employee onboarding – findings

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

```
"body": {
  "cr6e4_email": "daniellds@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)



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3

2023 recap and 2024 plans

@OWASPNoCode

2023 recap

- Lab project
- Stable 2023 Top 10 version
 - Better wording, better and more examples, clarity
- Virtual meetups → youtube.com/@owasplcnc
- Plain language for business users (contribution by John McTiernan, DT Group and Yianna Paris @punk_fairybread, Xebia) → youtube.com/watch?v=s3lZ8fsMDDQ

2024 plans

- Top 10 revamp
 - Another look on categories
 - A different treatment for Low Code / RPA / BPA / ..
 - CALL FOR DATA
- Translation to different languages
- Collaterals (deck, infographic, ..)
- Transparency
- Virtual meetups



GET INVOLVED!

michael.bargury@owasp.org

CALL FOR DATA

PLEASE SHARE YOUR STORIES!

JOIN THE DISCUSSION

Slack

bit.ly/owasp-lcnc-slack

Email group

bit.ly/owasp-lcnc-group

CONTRIBUTE

Share stories, review, translate, create graphics, help on social...



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3

Get involved!

Michael.Bargury@owasp.org

@OWASPNoCode

CALL FOR DATA

PLEASE SHARE YOUR STORIES!

JOIN THE DISCUSSION

Slack

bit.ly/owasp-lcnc-slack

Email group

bit.ly/owasp-lcnc-group

CONTRIBUTE

Share stories, review, translate, create graphics, help on social...