zenity

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

Automated Security Governance

Workato Community Event 2023
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

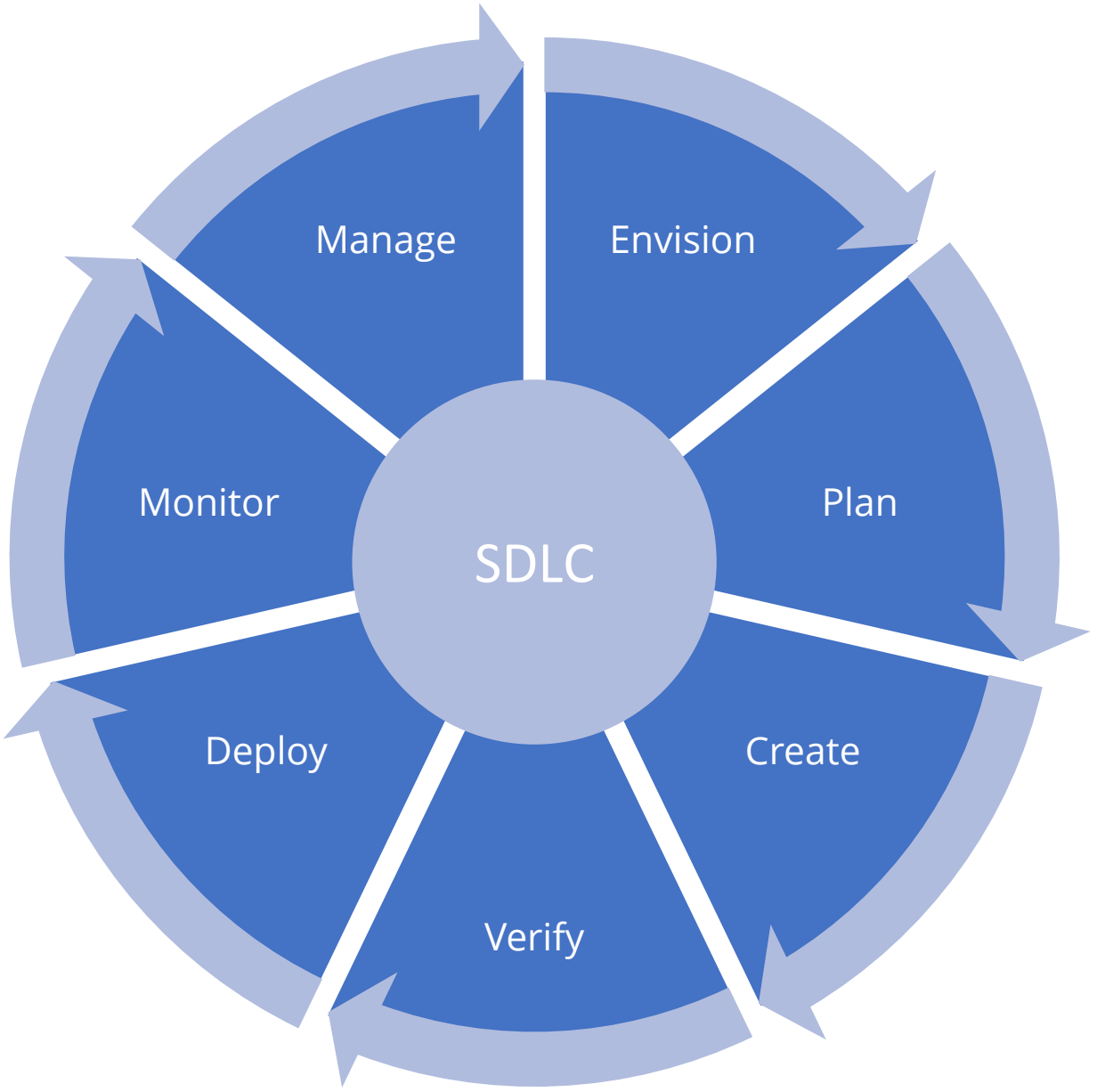
Outline

- LCNC SDLC and AppSec
- A security perspective on Citizen Integrators
- Security governance to enable Citizen Integrators and LCNC AppSec
- Learn more

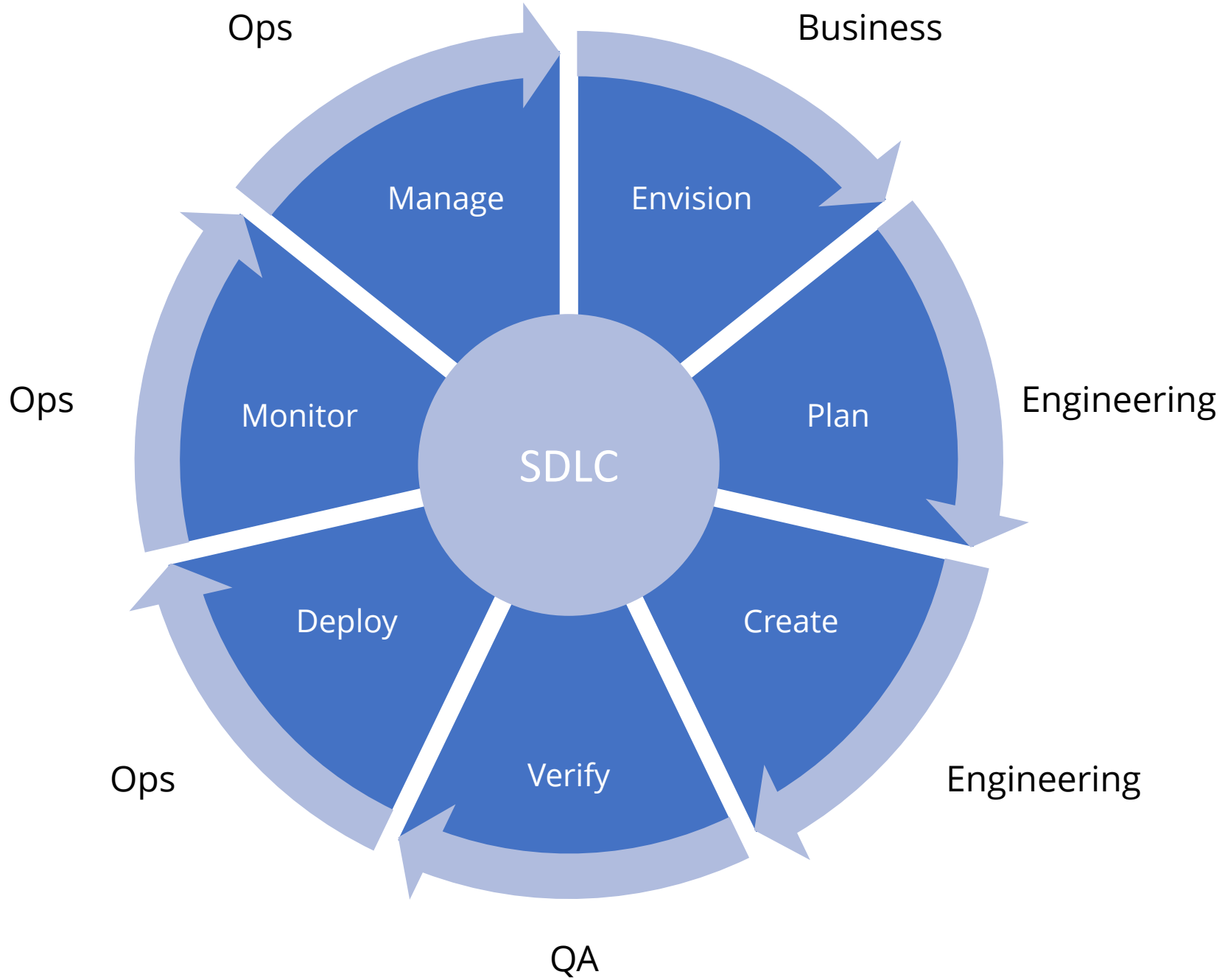
zenity

Low-Code/No-Code SDLC

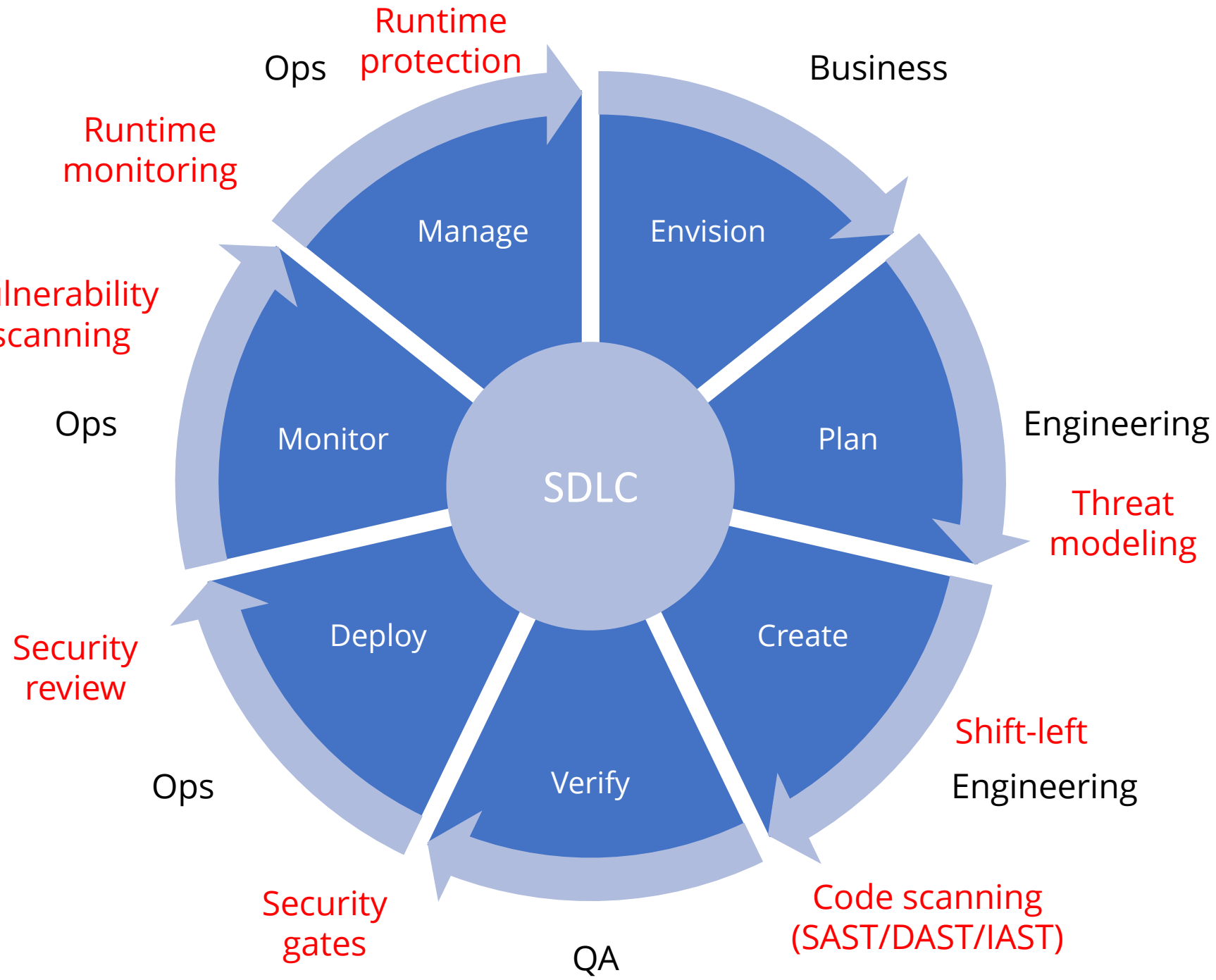
Software Development Lifecycle



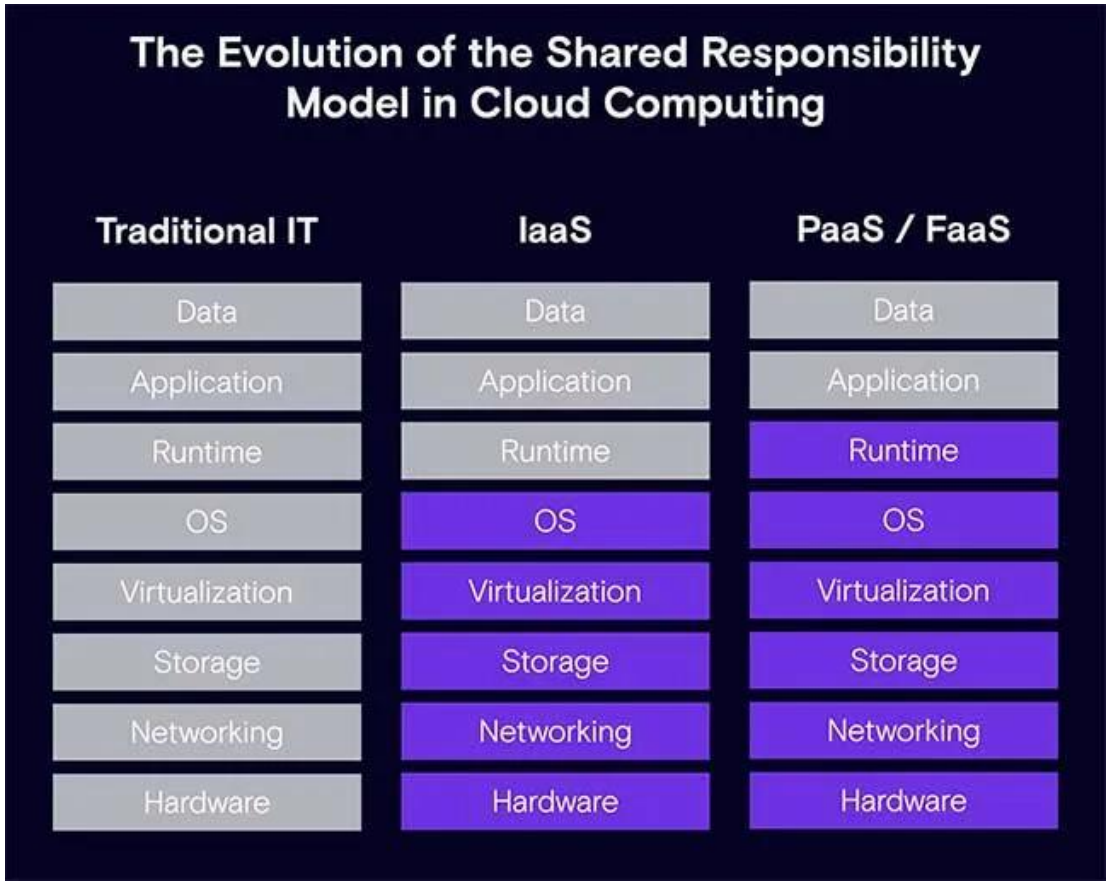
Software Development Lifecycle



Secure Software Development Lifecycle

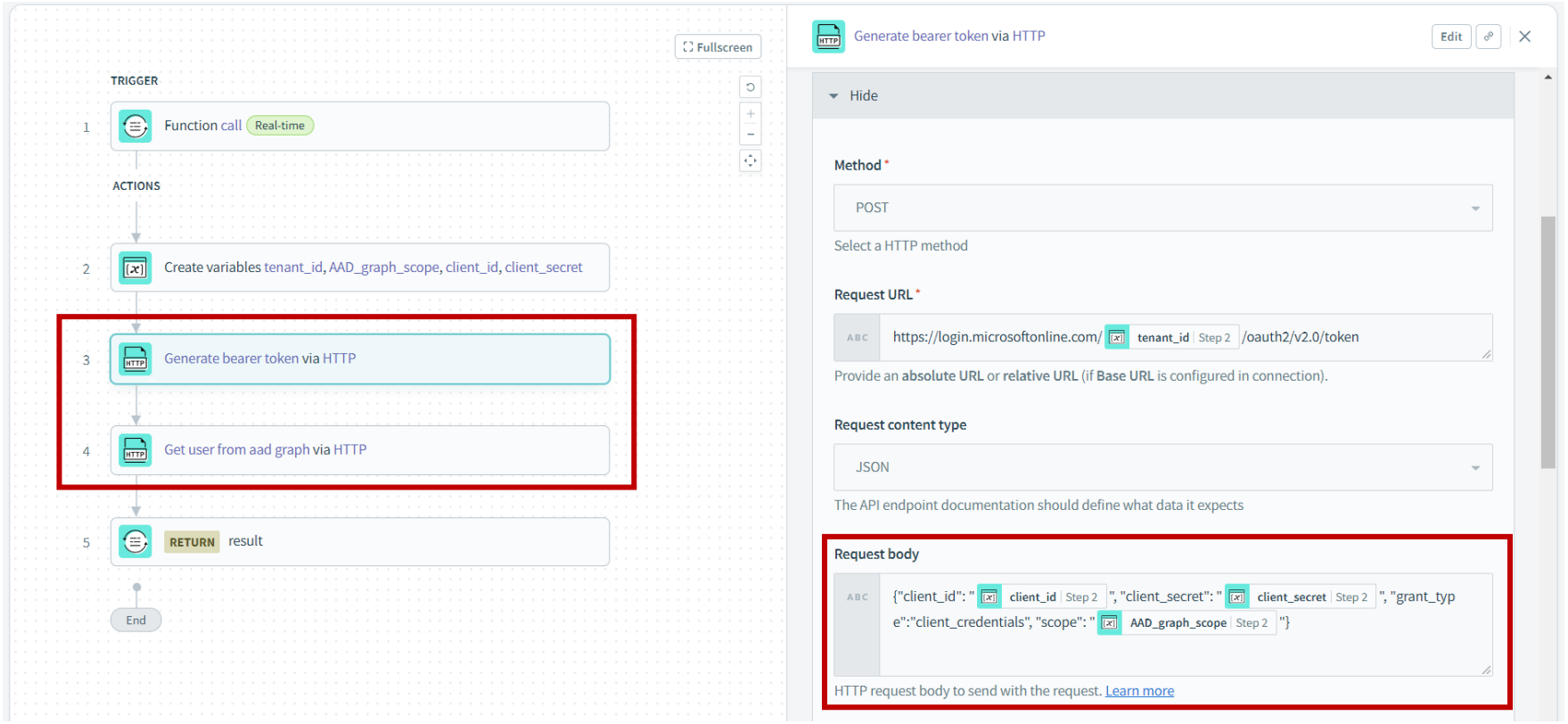


The Shared Responsibility Model



LCNC-SEC-08: Data and Secret Handling Failures

Low-code/no-code applications can 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.



OWASP Top 10 Security Risks for LCNC

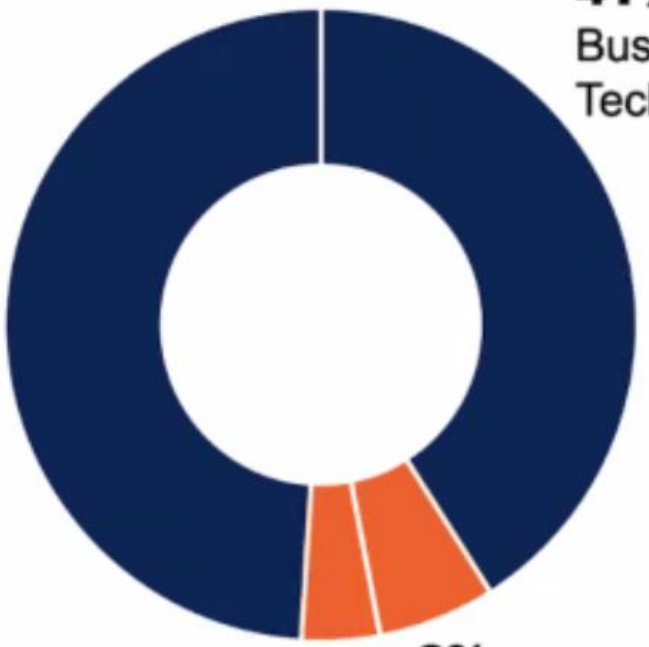
1. LCNC-SEC-01: Account Impersonation
2. LCNC-SEC-02: Authorization Misuse
3. LCNC-SEC-03: Data Leakage and Unexpected Consequences
4. LCNC-SEC-04: Authentication and Secure Communication Failures
5. LCNC-SEC-05: Security Misconfiguration
6. LCNC-SEC-06: Injection Handling Failures
7. LCNC-SEC-07: Vulnerable, 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

zenity

A Security Perspective on Citizen Integrators

The rise of Business Technologists



41%
Business Technologists

49%
Technology "End Users"

4%
Corporate IT Staff Reporting Into the CIO

6%
Business Unit IT Staff Reporting Into Divisional or BU CIOs

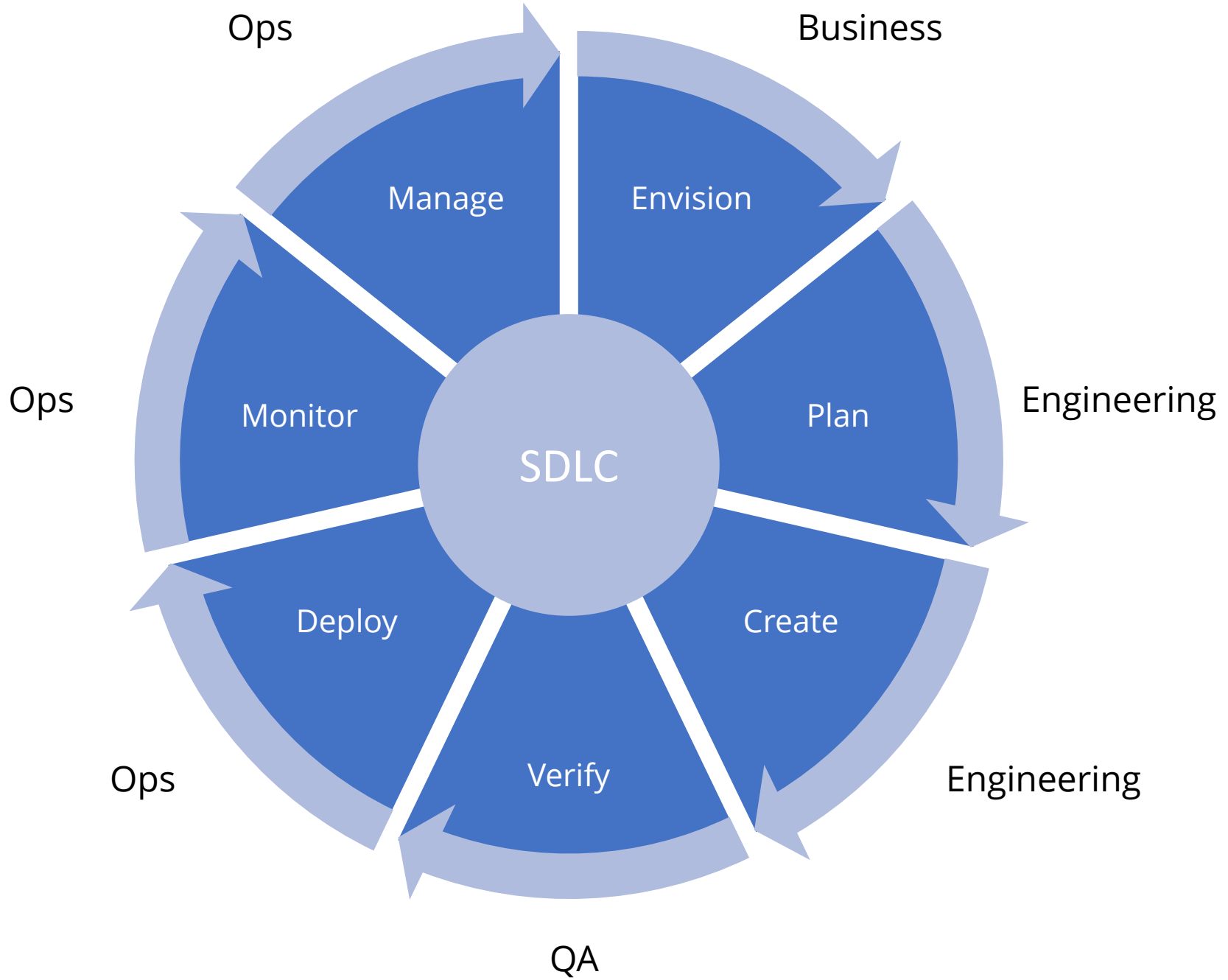
Business Technologists: Employees who report outside of IT departments and create technology or analytics capabilities for internal or external use.

- ✓ Citizen Developers
- ✓ Citizen Data Scientist
- ✓ Citizen Designer
- ✓ **Citizen Automators**
- ✓ **Citizen Integrators**

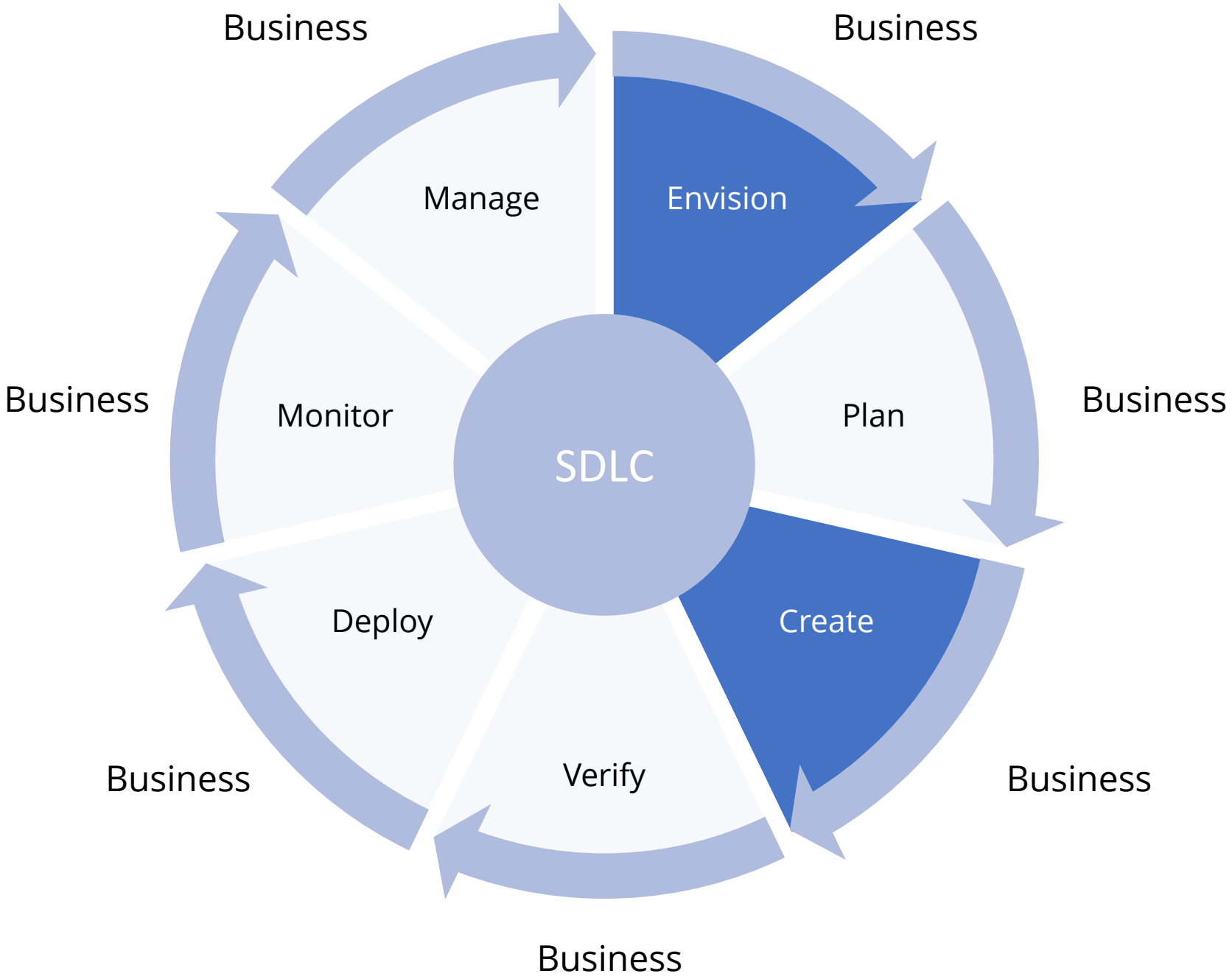
Gartner

workato

Software Development Lifecycle

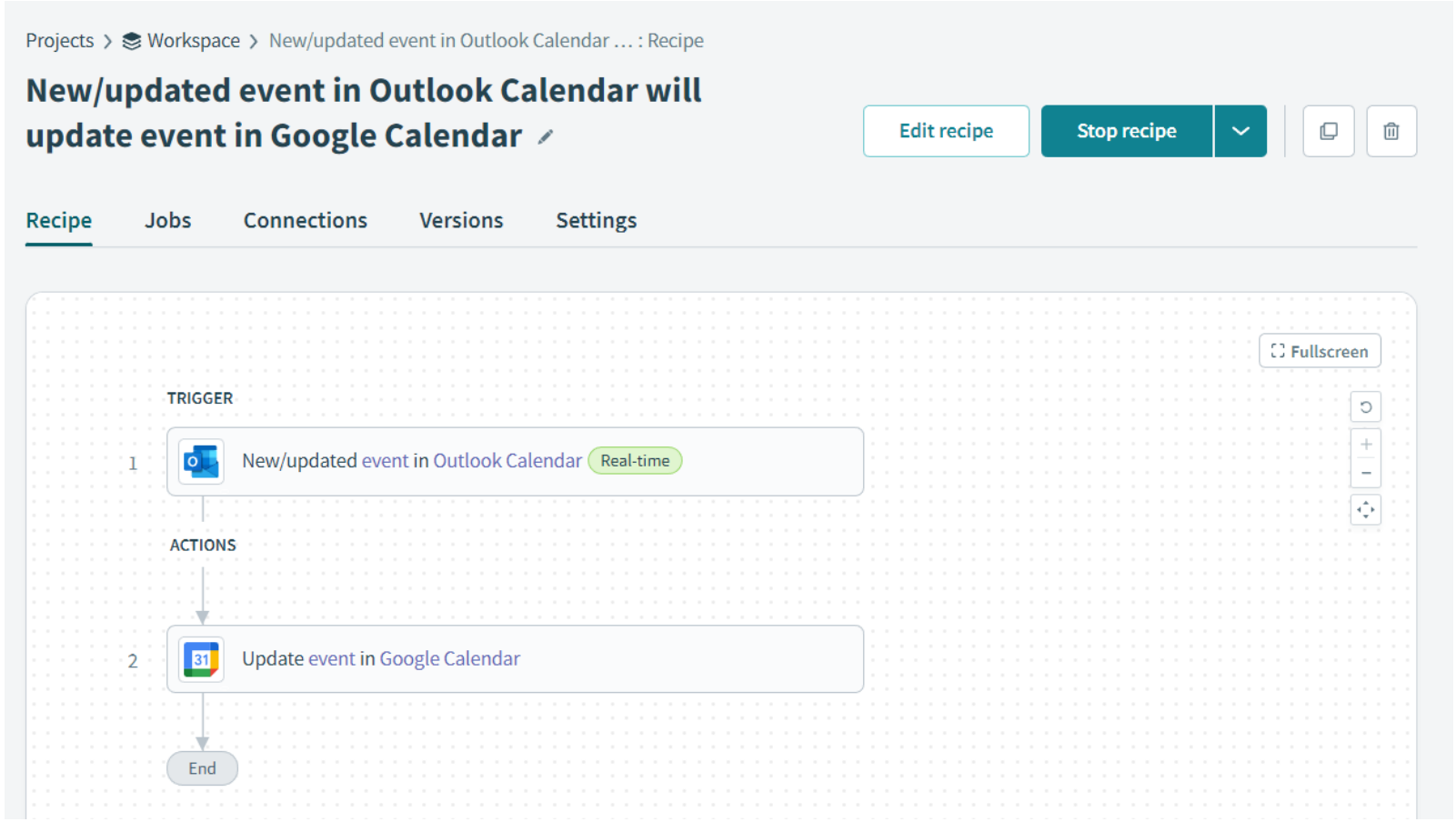


No Code SDLC?


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

LCNC-SEC-03: Data Leakage and Unexpected Consequences

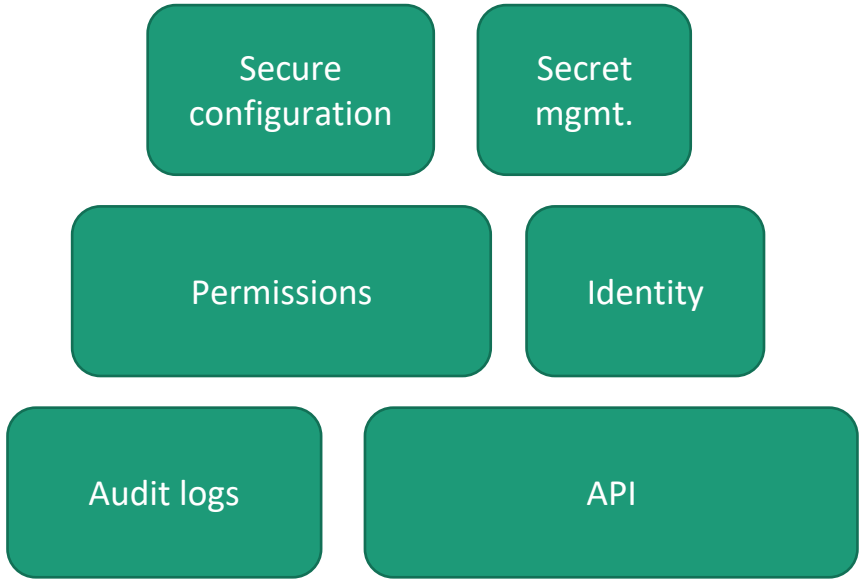
Low-code/no-code applications can sync data or trigger operations across multiple systems, which creates a path for data to find its way outside the organizational boundary. This means that operations in one system can have unexpected consequences in another.



Security should drive LCNC adoption

Extended visibility into an existing problem

- “Copy-paste” integration leads to the Shadow-IT problem
- LCNC replaces manual processes with automated workflows
- The potential for improved visibility is huge
- Security teams and LCNC leaders need for a common language to seize this opportunity



zenity

Security Governance to Enable Citizen Integrators and LCNC AppSec

Security governance strategy

Green zone –playground and personal productivity

Red zone – Production, managed centrally, policy enforced

Security governance strategy

Green zone – playground and personal productivity

- No business connectors or data
- Vendors can access
- No custom components
- Permissive roles
- OWASP top 10 security controls enforced with grace period (alert mode)

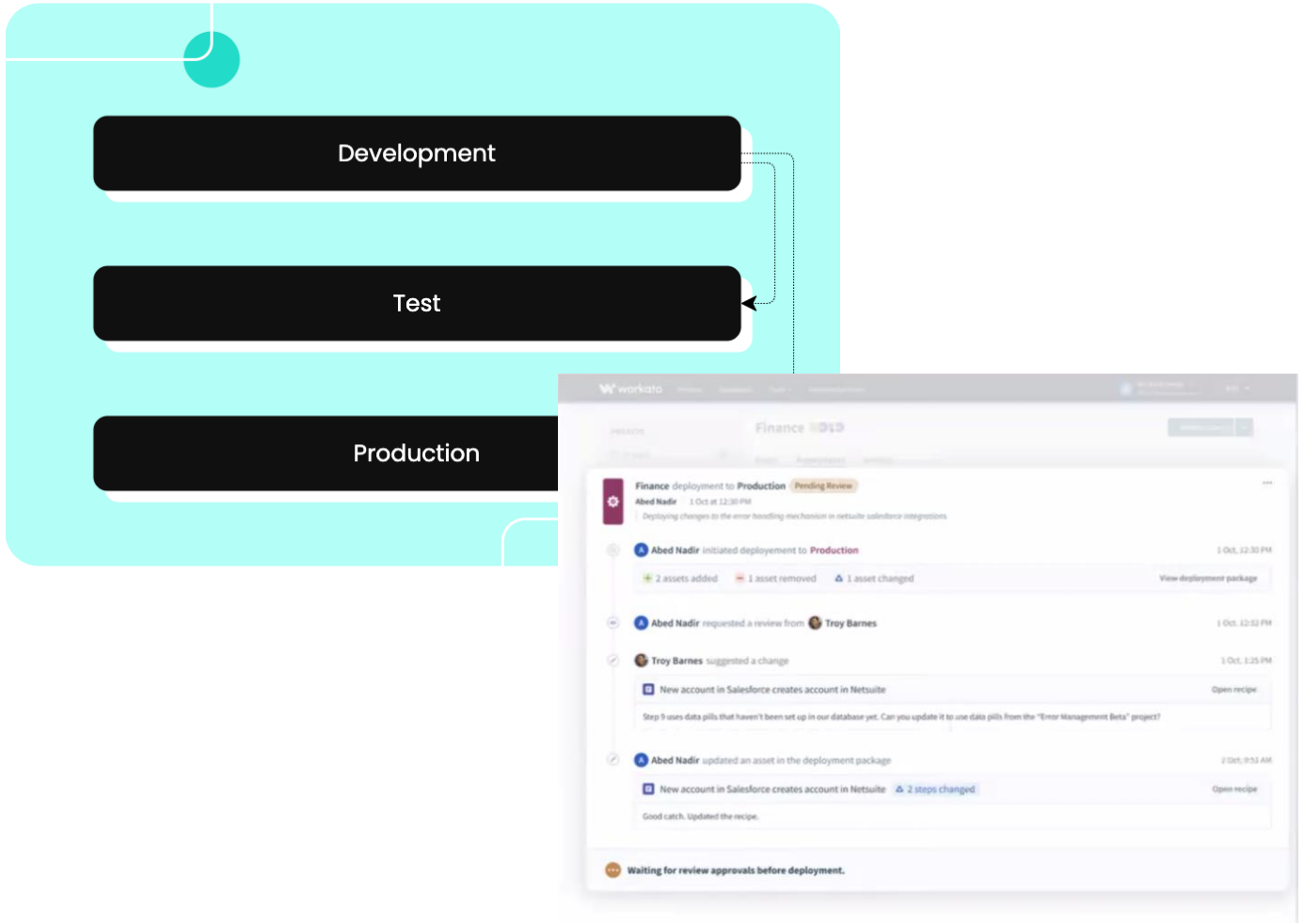
Red zone – production, managed centrally, policy enforced

- No personal connectors, data or accounts
- No vendor access
- Custom components allowed
- Strict roles
- OWASP top 10 security controls strictly enforced (block mode)

Security governance strategy

Secure CI/CD

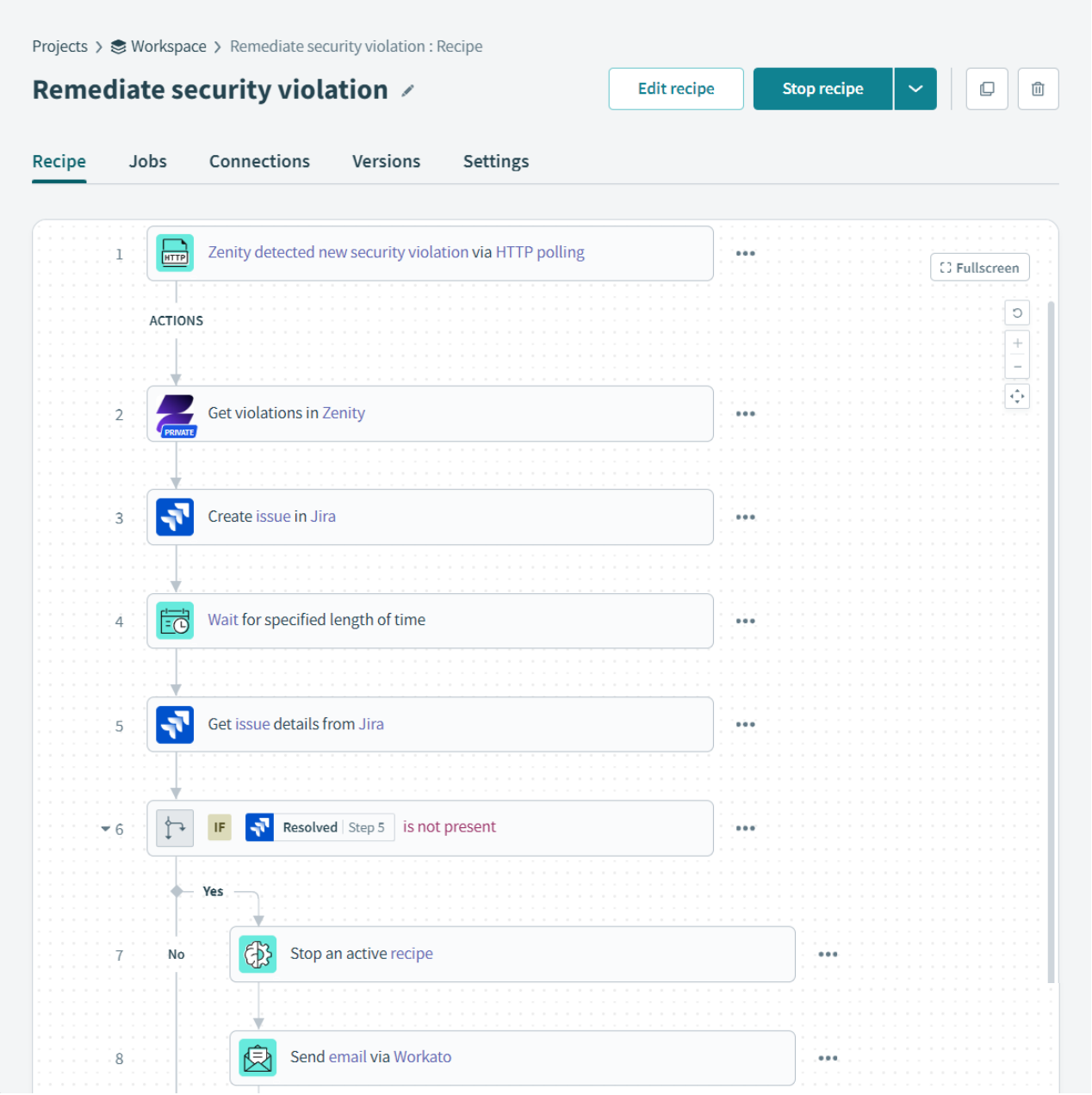
- Incorporate security review into the Peer Review process
- Leverage security scanning to support approval decision
- Security controls as deployment gates



Remediation

Facilitate a remediation process with **RecipeOps**

- Notify developer / security
- Wait for mitigation
- Stop recipe if not resolved in allocated time



zenity

Summary

What have we seen

- Low Code / No Code SDLC
    - Security needs to be built into the process
    - The builder’s part of the Shared Responsibility Model
- OWASP Top 10 LCNC Security Risks
- Enable Citizen Integrators with Security Governance
    - Security should drive wide LCNC adoption
    - Security governance strategy
    - Implement governance with automation

zenity

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

Automated Security Governance

Workato Community Event 2023
Michael Bargury @ Zenity