WALKOFF

SECURITY, ORCHESTRATION, AUTOMATION, & RESPONSE (SOAR)

EASY-TO-USE

FLEXIBLE

MODULAR

LIGHTWEIGHT

TIMELINE

1. What is **WALKOFF**?
2. The History of WALKOFF
3. Capabilities Overview
4. Architecture Deep-Dive
5. *Break*
6. Guided Installation
7. WALKOFF Scavenger Hunt
8. Workflow Development
9. *Final Questions and Survey*

WHAT IS **WALKOFF**?

- WALKOFF is a flexible, easy-to-use, **automation framework** allowing users to integrate their capabilities and devices to cut through the repetitive, tedious tasks slowing them down.

WALKOFF HISTORY

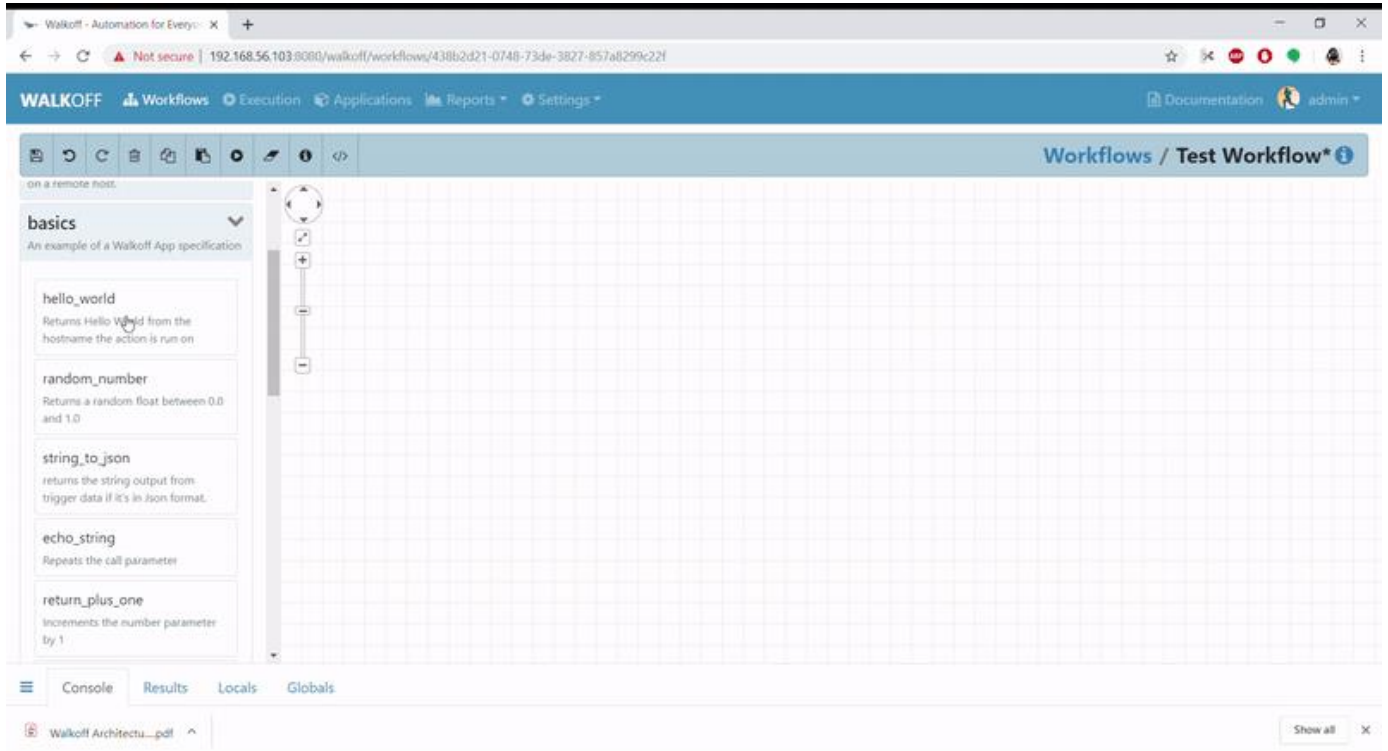
- Started with National Security Agency
- Prototype and Pilot at USINDOPACOM in 2018.
- Moved under ARD's Analytics Portfolio at USCYBERCOM

PACOM PILOT

- **Goal:** demonstrate value of automation to leadership.
- Automation-enabled team outperformed team following manual TTPs/SOPs.

- **WALKOFF** was able to:
  - query the commercial sensors
  - act to take actions based on the information from the commercial sensors
  - function as an orchestrator
  - perform basic response actions based on triggers

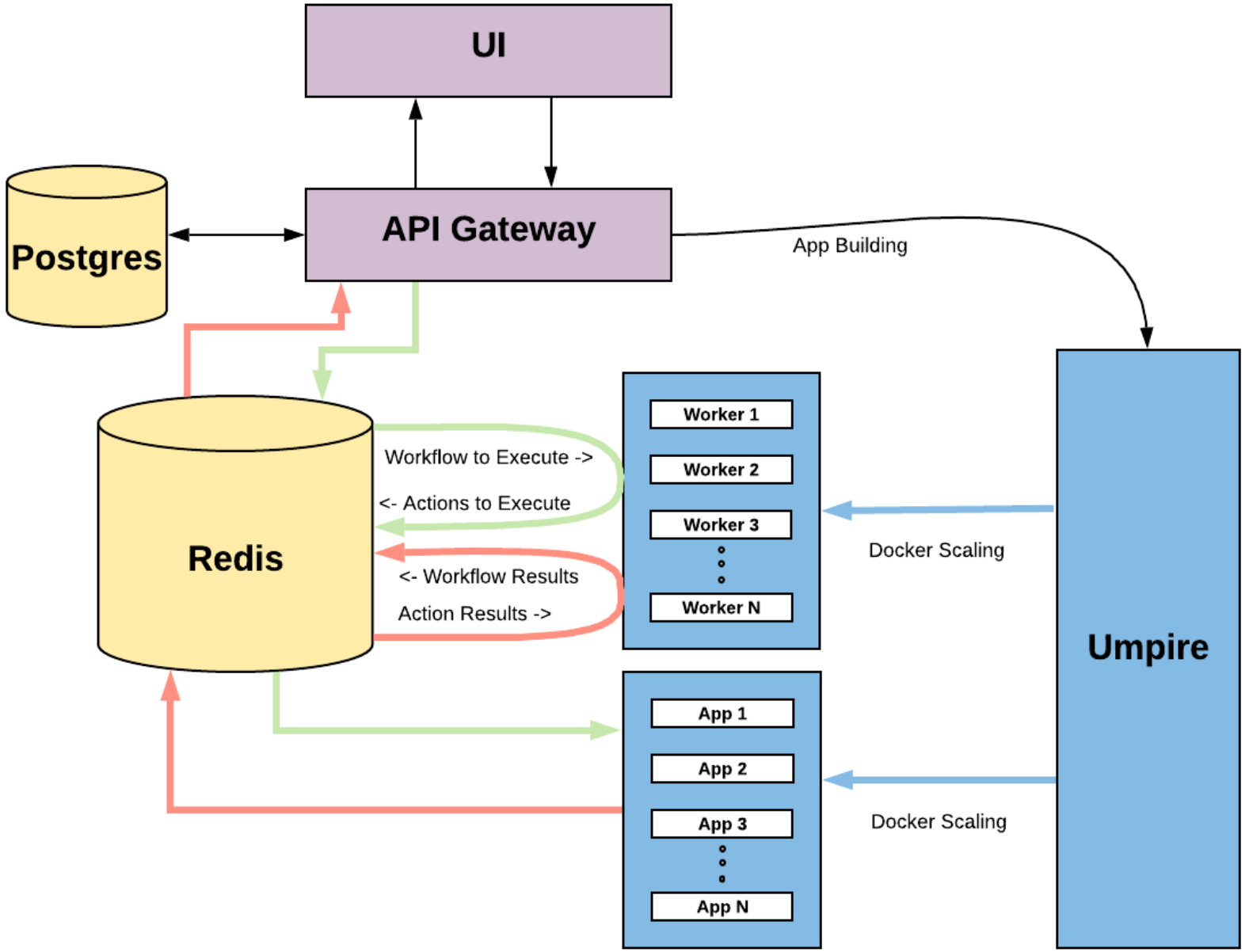
WHAT WE OFFER – EASE OF USE



Drag-and-drop workflow editor. Sharable apps and workflows

WHAT WE OFFER

- ***Flexibility***: Deployable on Windows or Linux.
- ***Modularity***: Plug-and-play integration of almost any technology with easy-to-develop apps.
- ***Lightweight***: Containerized Docker architecture allows for compact offline deployment.


UI
Postgres
API Gateway
App Building
Redis
Workflow to Execute ->
<- Actions to Execute
<- Workflow Results
Action Results ->
Worker 1
Worker 2
Worker 3
Worker N
Docker Scaling
Umpire
App 1
App 2
App 3
App N
Docker Scaling

INSTALLATION AND Q&A

Code at www.github.com/nsacyber/WALKOFF

Documentation at www.walkoff.readthedocs.io