SO…WHY DOES KEVIN CARE?

ENTER SECURITY, STAGE LEFT

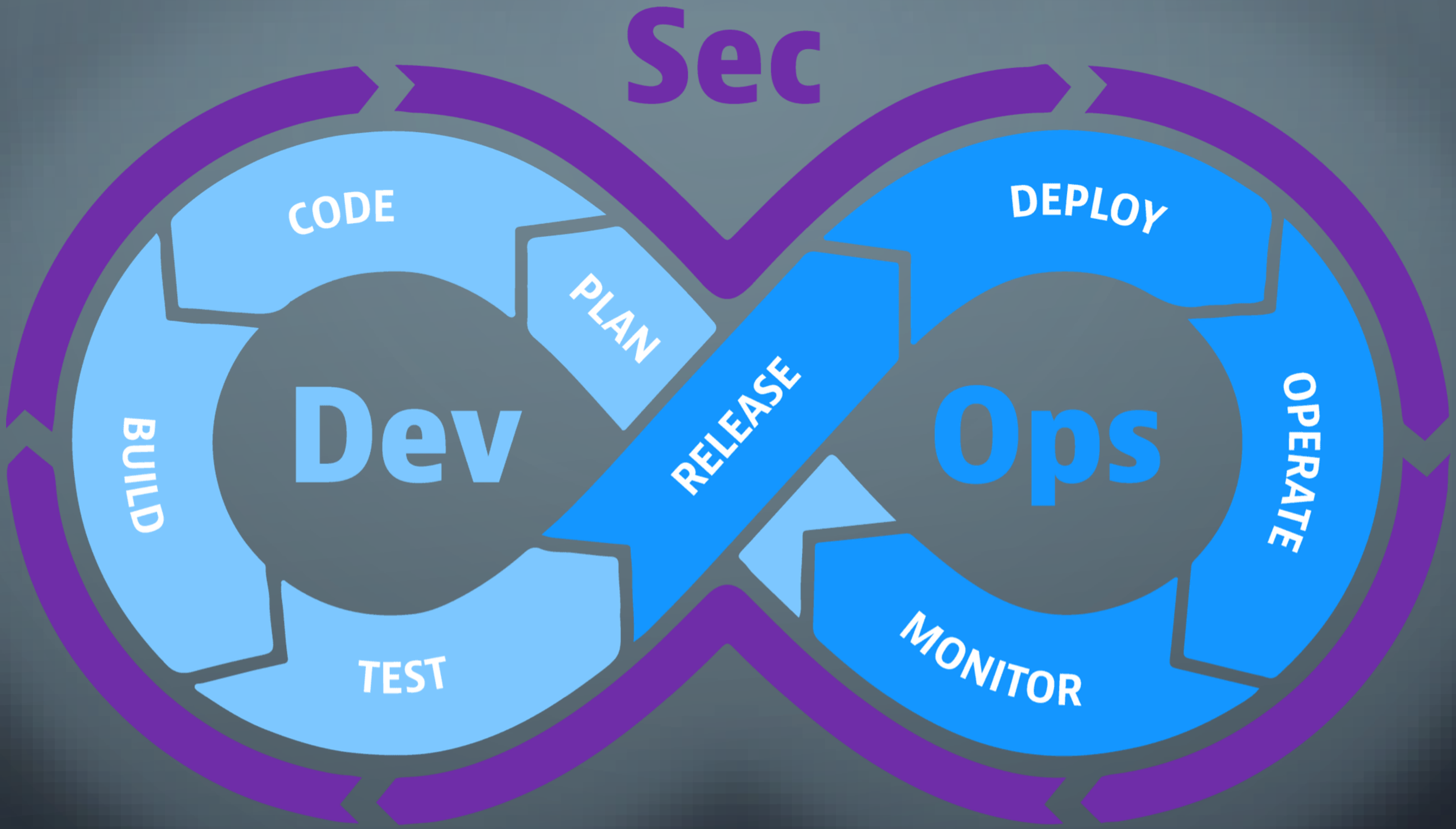
- I’m Kevin (Schwantje)
- He/him
- Settler on stolen land
- Almost 10 years in cybersecurity (>3 years at WSBC)
- Sysadmin, systems engineering (in space), architecture, network security, red team, blue team, purple team, and now – **web application and cloud security**
- I care most about standardization, consistency, collaboration, communication, inclusiveness, respect, and the “human factor” of security (which may not be what you think!)

@604kev

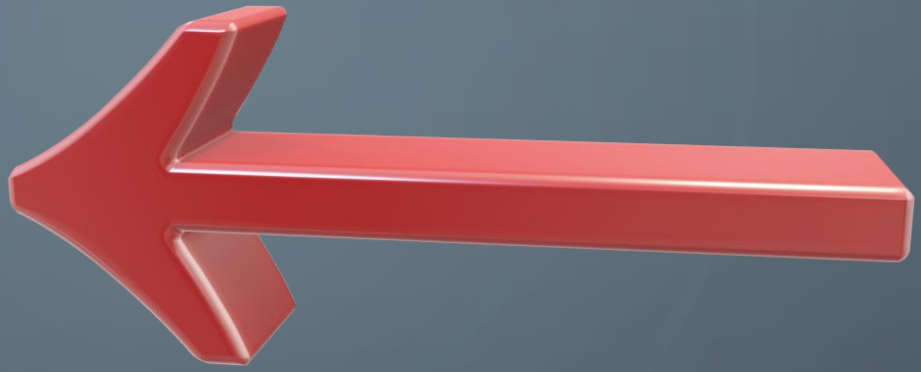
THE PROBLEM

- 3000+ unique pipeline definitions means no standardization, consistency, etc.
- Vulnerabilities ***everywhere*** ☹
- Sketchy approval situation
- Stuck on old technology and implementations
- Lack of true awareness of risk!

WHAT IS “DEVSECOPS”?

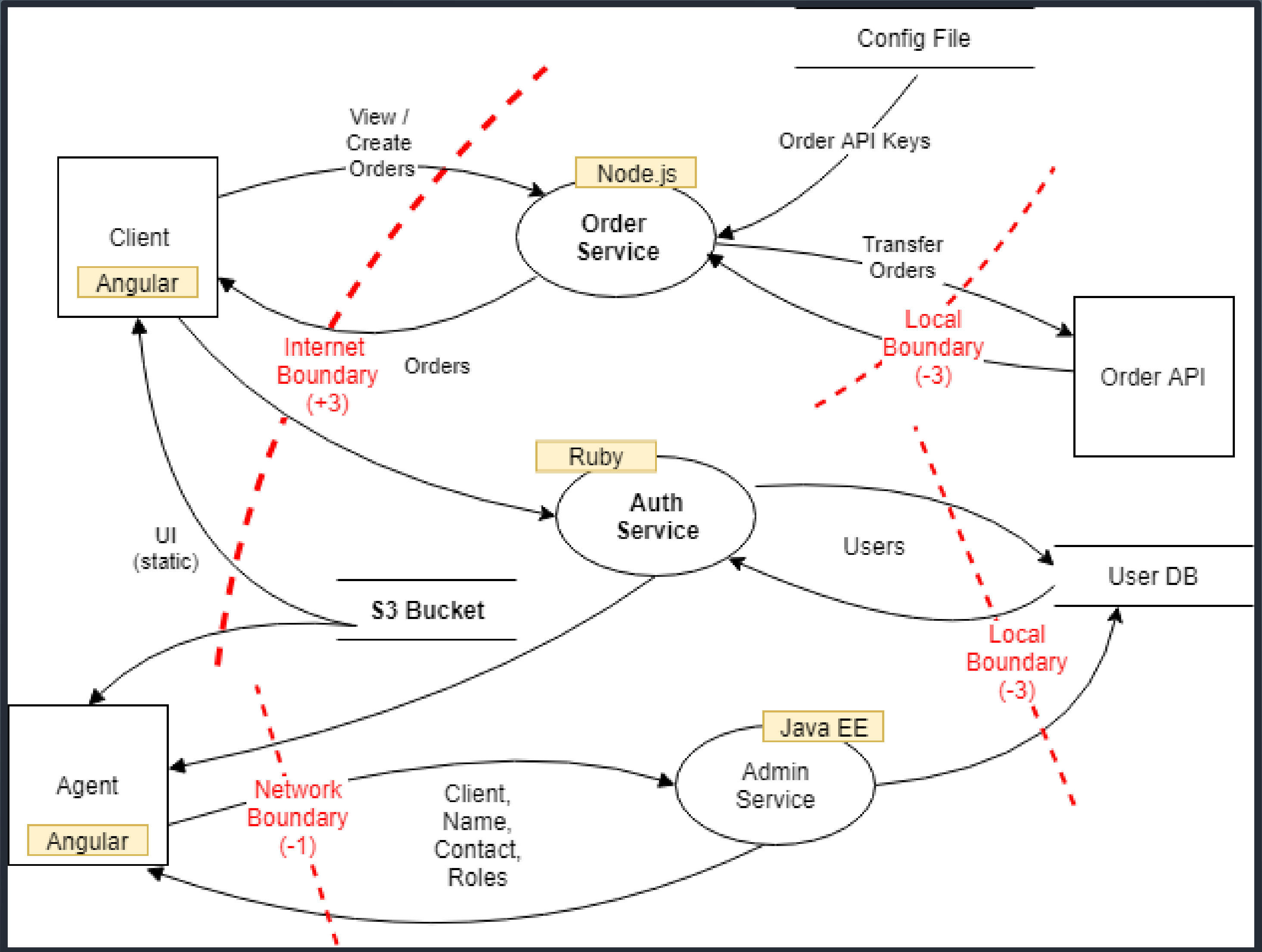

Sec
CODE
PLAN
BUILD
Dev
TEST
RELEASE
DEPLOY
Ops
OPERATE
MONITOR

- “Shifting Left”



- Bake in security from day one
- Security is **everyone’s** responsibility
  - Business, executive, developers – everyone
- Teach, train, educate, and share

- Automate! Automate! Automate!
  - Run tasks on machines, not people
  - Take human error out of the equation
- Continuous detection and response
  - No more “one and done” audit scans
- Threat Modelling
  - Collaborate with all parties and gain insight into potential risks
  - A critically important exercise to truly understand an application!
  - It looks something like this…


Config File
View / Create Orders
Order API Keys
Node.js
Order Service
Client
Angular
Transfer Orders
Local Boundary (-3)
Order API
Internet Boundary (+3)
Orders
Ruby
Auth Service
Users
User DB
UI (static)
S3 Bucket
Local Boundary (-3)
Java EE
Admin Service
Agent
Angular
Network Boundary (-1)
Client, Name, Contact, Roles

And, most importantly…

The definition of quality must include “secure”

PIPELINES ARE THE SOLUTION!

- Reusable standardized templates are more secure – no snowflakes!
- We can now implement proper guardrails!
  - Just a few ways of doing things – not 3000+
  - Centralized and vetted
  - Repeatable ad infinitum
  - Contain required steps and approvals!

- Automate everything that you can
  - Taking the human out of the equation is actually the human-friendly and human-centric thing to do
- Objective risk assessment and understanding is now possible
  - We can guarantee standard scans and tests will be run every single time

THE FUTURE

- Self-Service – more automation!
  - Give power to the engineers (within limits)
- More (and better) security scans and steps
  - Let the tools speak for themselves, to all users (don’t hide information)
- ***Never*** stop shifting left
  - Work with projects at their inception, implement the standards before anything else

THANK YOU!