



A Billion Decisions A Day: MLOps
Powering DOD Scale Missions



Kyle Fox

SOSi CTO

First Chief Software Engineer DAF

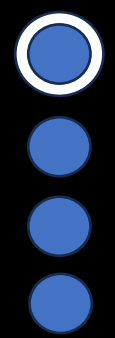
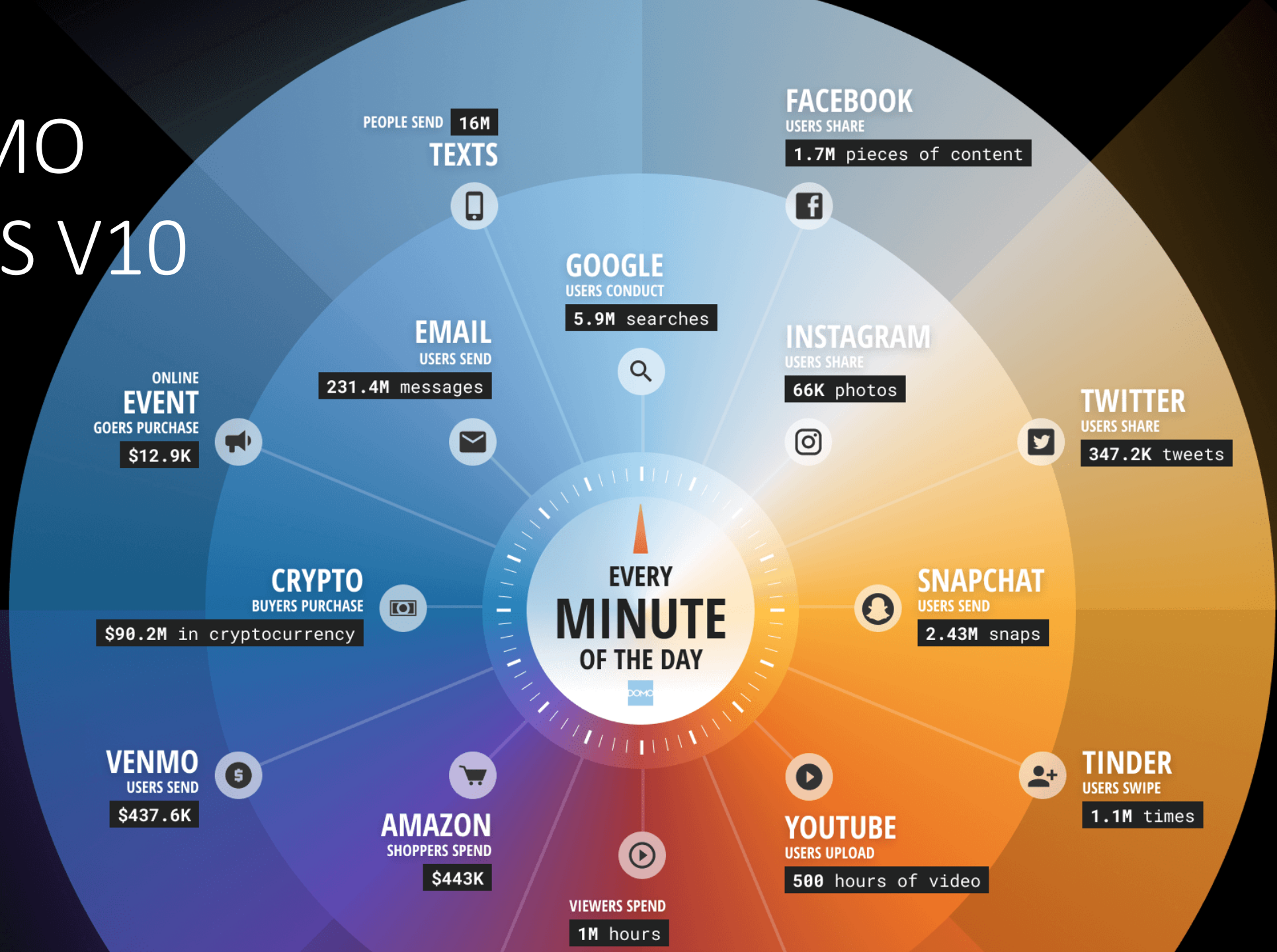
Delivered Cloud Native Nuclear Weapons

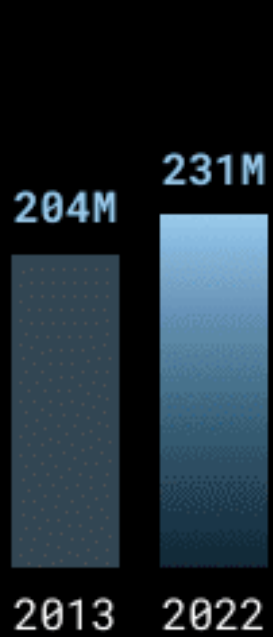


Game Plan

- 1 Data dominance gaps are lethal
- 2 DevSecOps is not enough
- 3 Trusted decisions at scale
- 4 #LetsGo!

DOMO D.N.S V10





EMAILS
EMAILS SENT



YOUTUBE
HOURS UPLOADED



63%

97ZB
In 2022

181ZB
By 2025



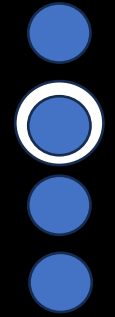
Gaps are Lethal

A high-angle, wide shot of a densely packed urban area, likely a slum or a city under conflict. The buildings are multi-story and closely packed. The sky is filled with thick, dark grey smoke, suggesting a recent explosion or fire. In the middle ground, a bright orange and yellow fire is visible, with a white horizontal line drawn across it. The overall atmosphere is one of devastation and danger.


```
3 require File.expand_path("../..//config/environment.rb", __FILE__)
4 # Prevent database truncation if the environment is production
5 abort("The Rails environment is running in production mode!") if Rails.env.production?
6 require 'spec_helper'
7 require 'rspec/rails'
8
9 require 'capybara/rspec'
10 require 'capybara/rails'
11
12 Capybara.javascript_driver = :webkit
13 Category.delete_all; Category.create(:name => "Category")
14 Shoulda::Matchers.configure do |config|
15   config.integrate do |that|
16     that.with.test_framework :rspec
17     that.with.library :rails
18   end
19 end
20
21 # Add additional requires below this line. Please do not require files that
22 # require supporting ruby files with dependencies on ActiveSupport.
23 # spec/support/ and its subdirectories. This directory is automatically
24 # run as spec files by default. This directory is also automatically
25 # in _spec.rb will both be required and run. This directory is also
26 # run twice. It is recommended that you do not require files in
27 # end with _spec.rb. You can configure the behavior of this
28 # option in the command line or in the configuration file.
29 # rails spec --require spec_helper --require spec_helper
30 # rails spec --require spec_helper --require spec_helper
```



2009 - DevOps



```
3 require File.expand_path("../test/spec_helper", __FILE__)
4 # Prevent database truncation if the environment is production
5 abort("The Rails environment is running in production mode!")
6 require "spec_helper"
7 require "rspec/rails"
8
9 require "capybara/rspec"
10 require "capybara/rails"
11
12 Capybara.javascript_driver = :webkit
13 Category.delete_all; Category.create
14 Shoulda::Matchers.configure do |config|
15   config.integrate do |test|
16     with.test_framework :rspec
17     with.library :rails
18   end
19 end
20
21 # Add additional requires below this line. This is not required to run
22 # your tests, but it allows you to capture some common test methods.
23 # Requires supporting ruby files with support/ or spec/support/ and its
24 # spec/support/ and its subdirectories. Files ending in *_spec.rb are
25 # run as spec files by default. This means that you can use
26 # in _spec.rb will both be required and run as spec files. It is
27 # run twice. It is recommended that you use the *_spec.rb
28 # end with _spec.rb. You can configure this behavior by using
29 # in *_spec.rb. You can configure this behavior by using
30 # in *_spec.rb. You can configure this behavior by using
```



2013 - DevSecOps





Cloud took off..

In 2013 \$131B

In 2023 **\$600B**

...with an estimated
30% waste!





Data Science Crash Course (1/2)



Turning data into insights



Artificial Intelligence (AI) = Algorithms that can infer, reason, and adapt



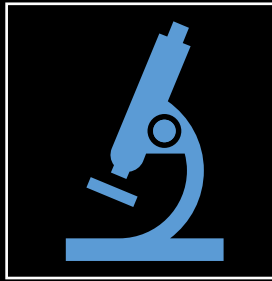
Machine Learning (ML) = Subset of AI focused on Algorithms who perform better as they are exposed to additional data



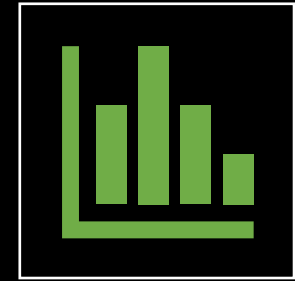
Deep Learning = Subset of ML that uses Algorithms inspired by human brain topology (e.g. Neural Networks)



Data Science Crash Course (2/2)



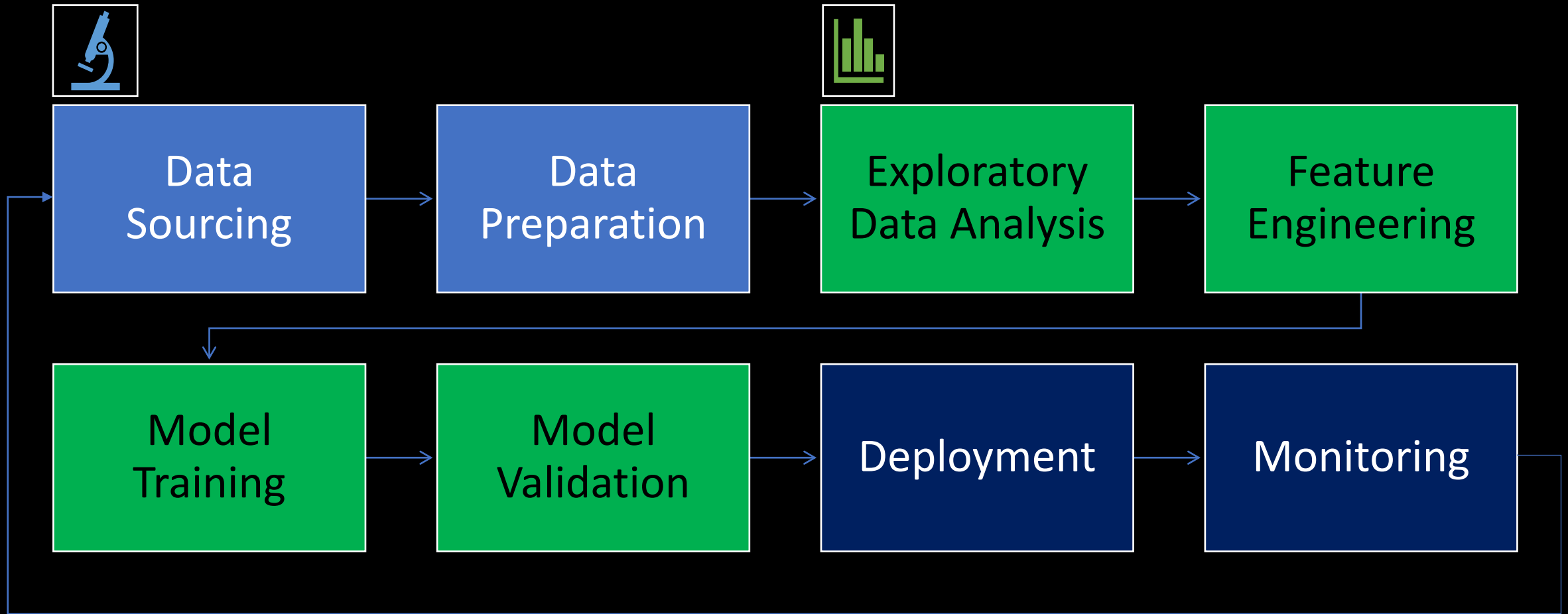
Data Scientists focus on
Algorithms and Experiments



Data Engineers focus on Data
Operations



Simplified ML Workflow





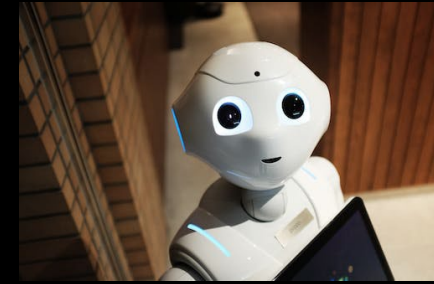
AIOps

- AI Enabled Log Analysis
- Emphasis is on optimizing SDLC and teams



FinOps

- AI Enabled Log Analysis
- Emphasis is on reducing OPEX

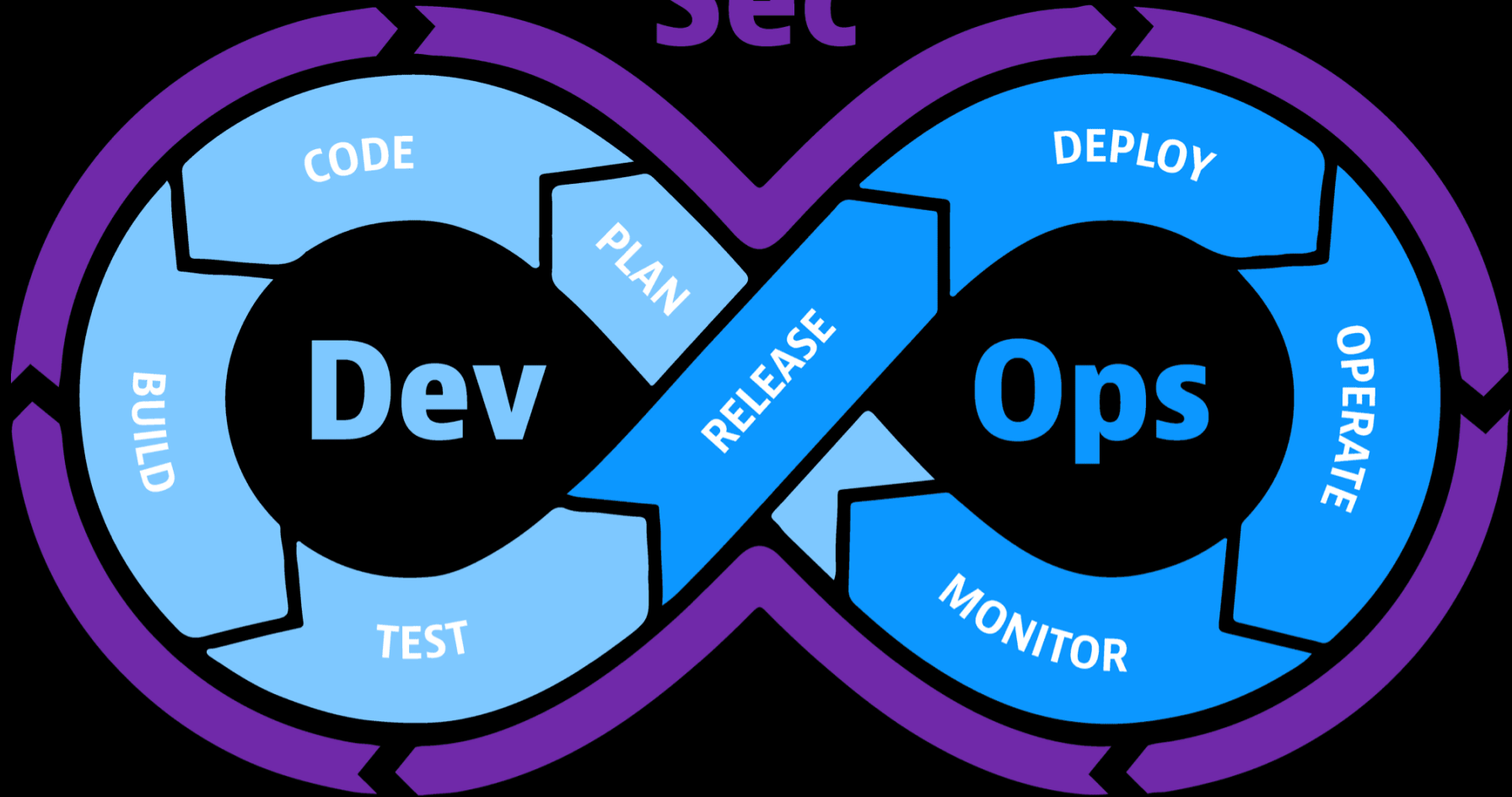


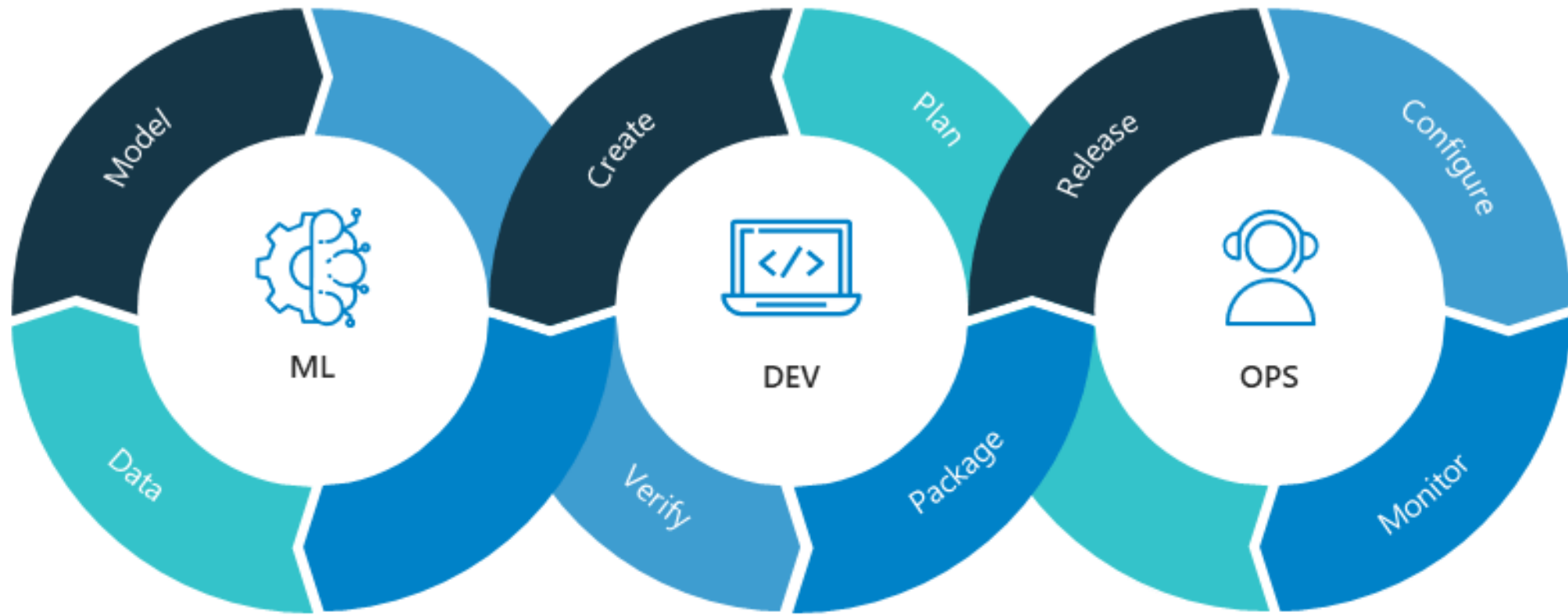
MLOps

- Serving AI/ML Models
- Emphasis is on productionizing data science workloads



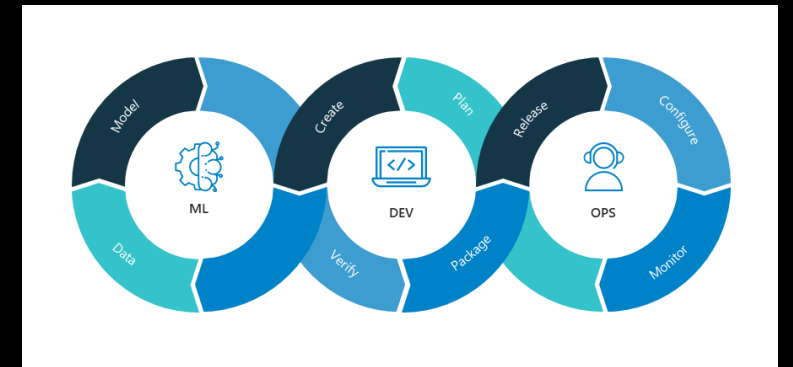
Sec



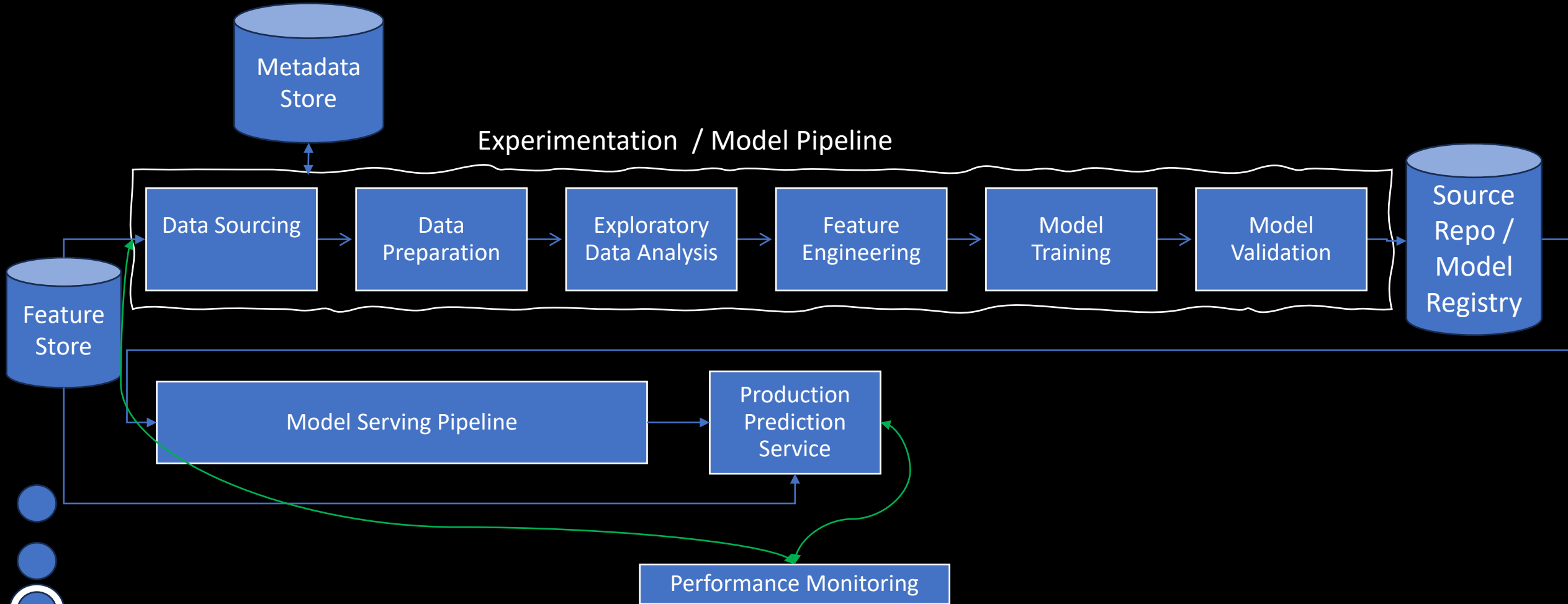


MLOps for DSO veteran's takeaways

- CI now tests and validates more than code but also includes model data schemas, models, and related verification data
- CD is now not about delivering a single service but instead a training pipeline that then deploys a predictive service
- New is Continuous Testing (CT) which enables continuous retraining and redeployment with updated datasets or other conditions



MLOps Workflow



MLOps in high assurance environments

- Trustworthy AI / Explainable AI (XAI) → Human friendly outputs
- Disconnected Environments → Many pain points but tools are maturing
- High Side Cloud → Many pain points but platforms rapidly maturing



Open Challenges / Call to Action

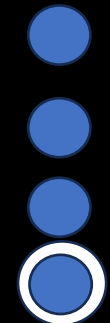
- Disconnected is a 2nd class citizen, please contribute to OSS projects like Leapfrog



- Some Models such as the large foundation model LLMs are NOT OSS and there is extremely limited insight into their makeup ... places significant burden on test for trustworthy AI



- Skills and Culture Gap acute in DOD. Critical to form teams that comprise Analysts, Data Engineers, Data Scientists, and DSO engineering roles and start experimenting!



Questions?