ADDO
ALL DAY DEVOPS | 4.17.20
SPRING BREAK EDITION

APRIL 17, 2020

Michael Fraser | CEO | Refactr

CI/CD Pipelines for DevSecOps With Hybrid Cloud

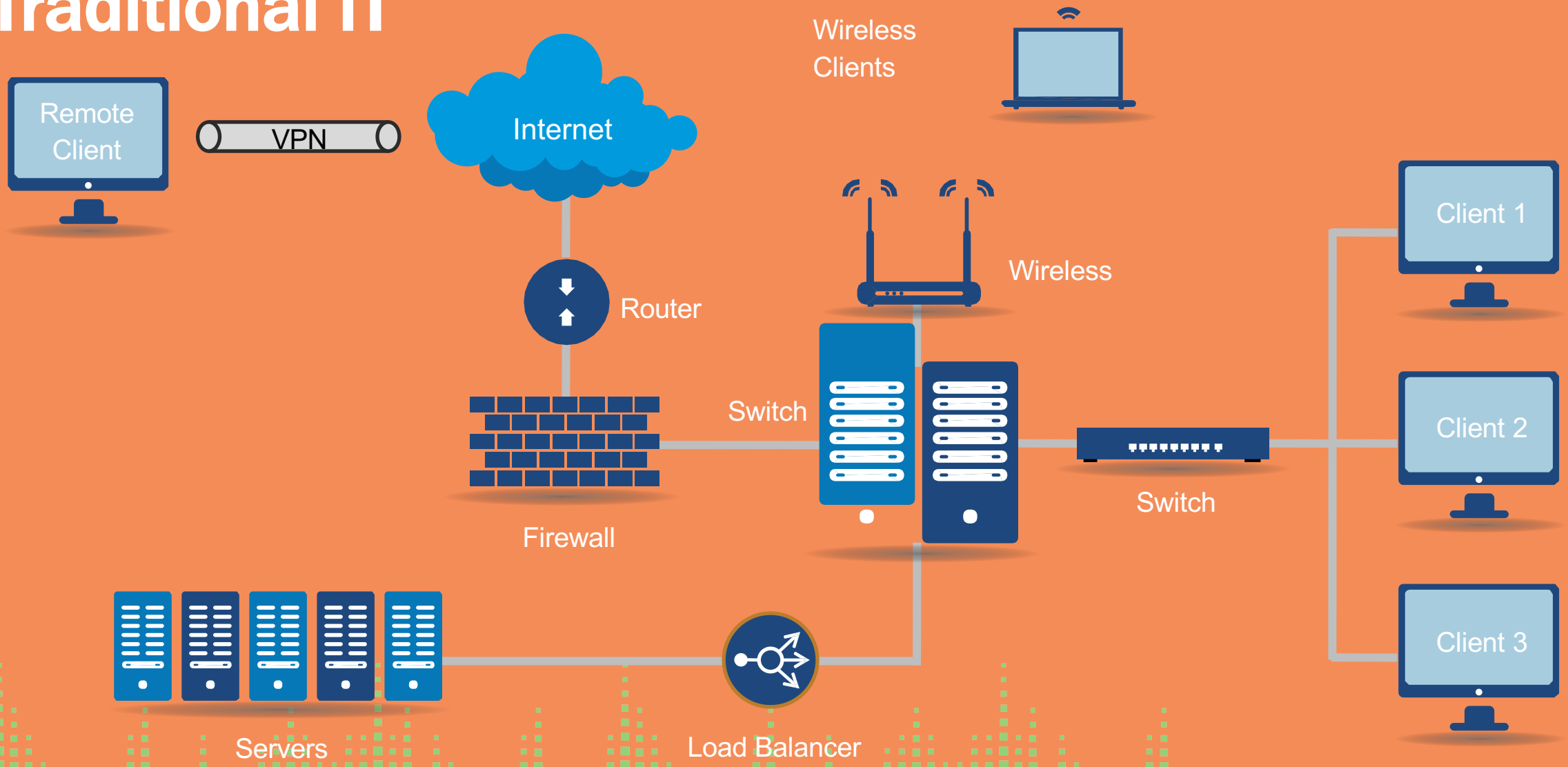
Intro

- US Air Force Veteran
  - F-15 C/D Armament Specialist
  - Cybersecurity Engineer
- Refactr
  - Co-Founder | CEO
- Master of Computer Science
  - Seattle University
- Adjunct Instructor
  - Seattle Central College
- Thought Leader | Speaker
  - All Day DevOps
  - DevOps Days Tampa
  - RedHat AnsibleFest

ADDO
ALL DAY DEVOPS

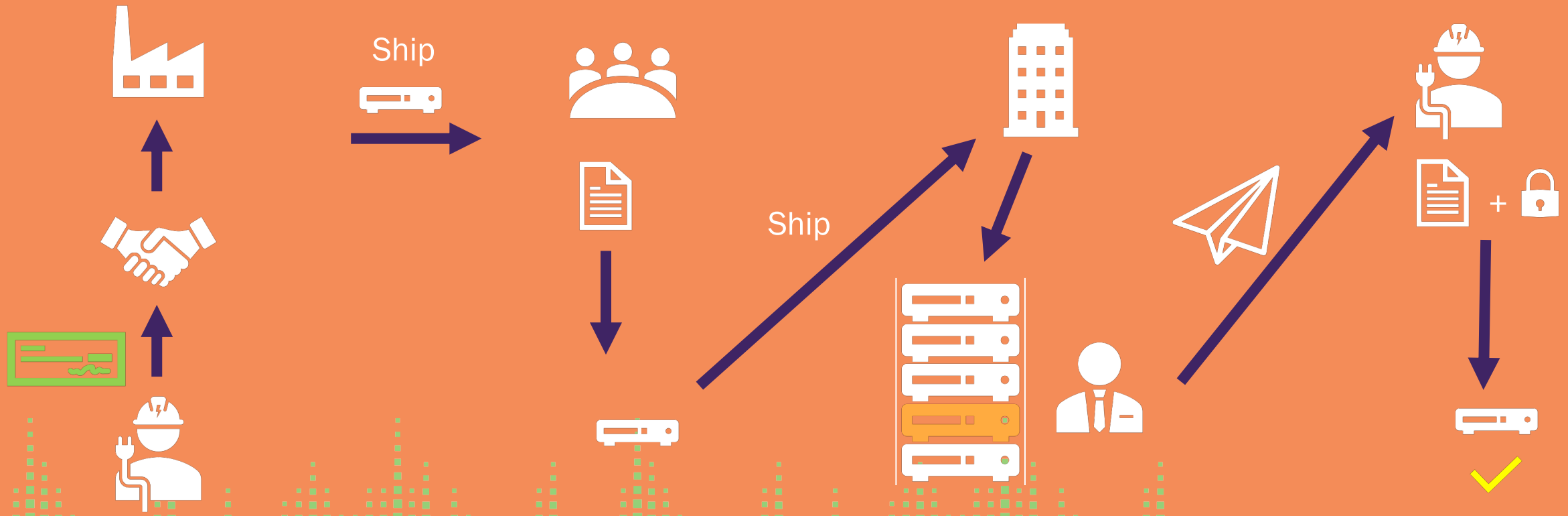
DEVOPS DAYS TAMPA BAY

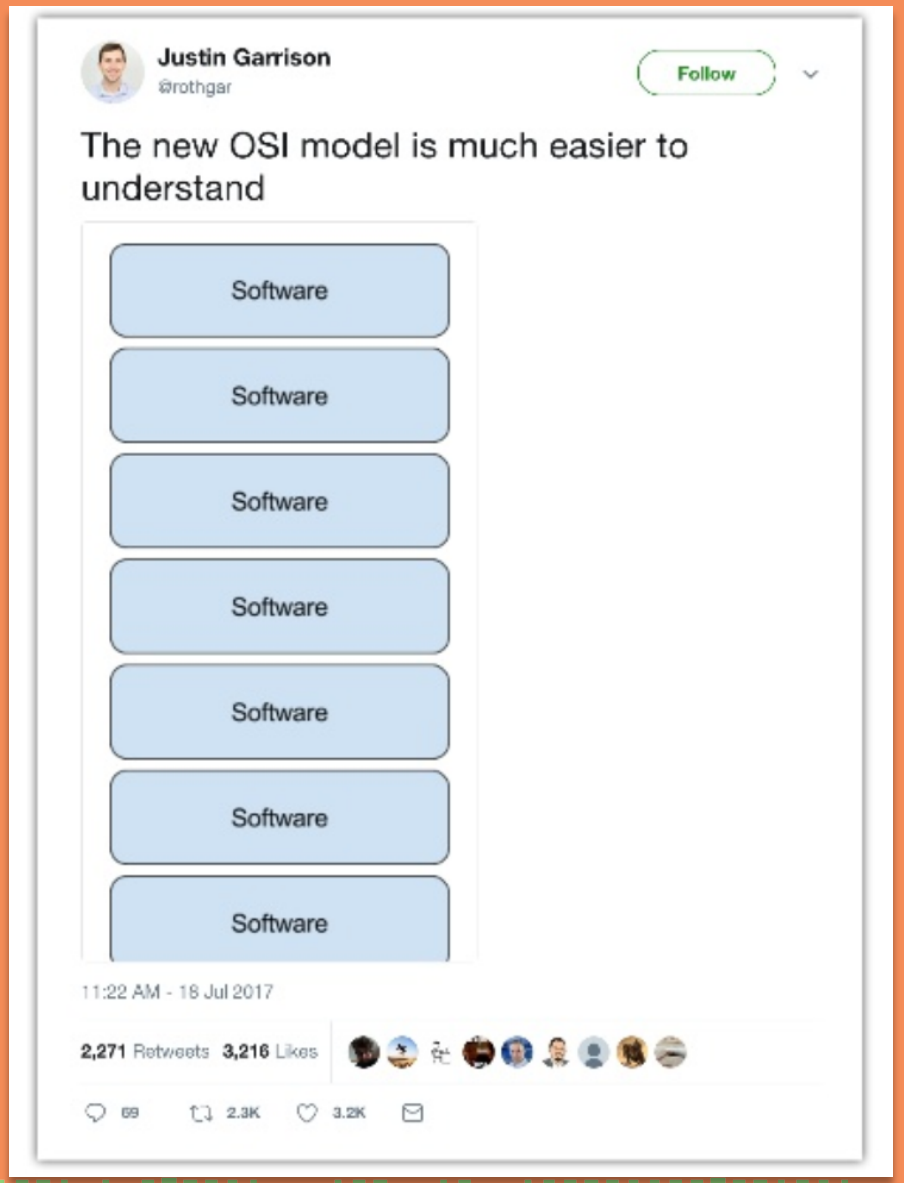
Traditional IT



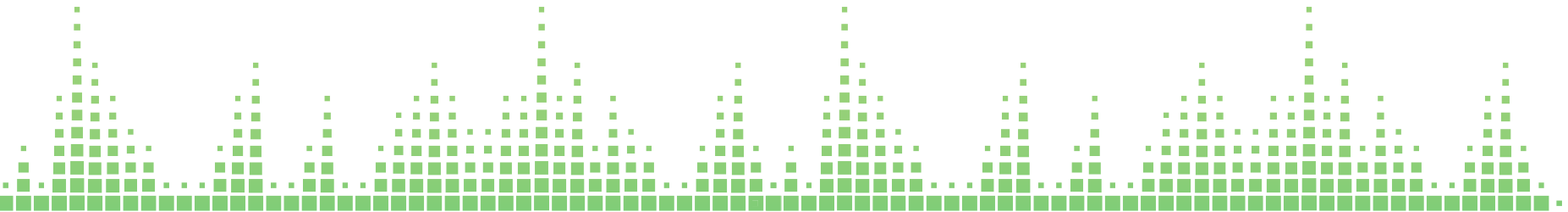
Deploying Traditional IT

Procure → Pre-configure → Rack & Stack → Final Configuration

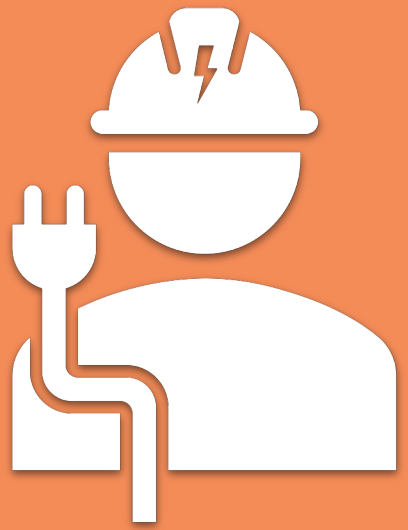



Justin Garrison
@rothgar
Follow
The new OSI model is much easier to understand
Software
Software
Software
Software
Software
Software
Software
11:22 AM - 18 Jul 2017
2,271 Retweets 3,216 Likes
69
2.3K
3.2K

TRADITIONAL IT = LEGACY



What is IT as Code?

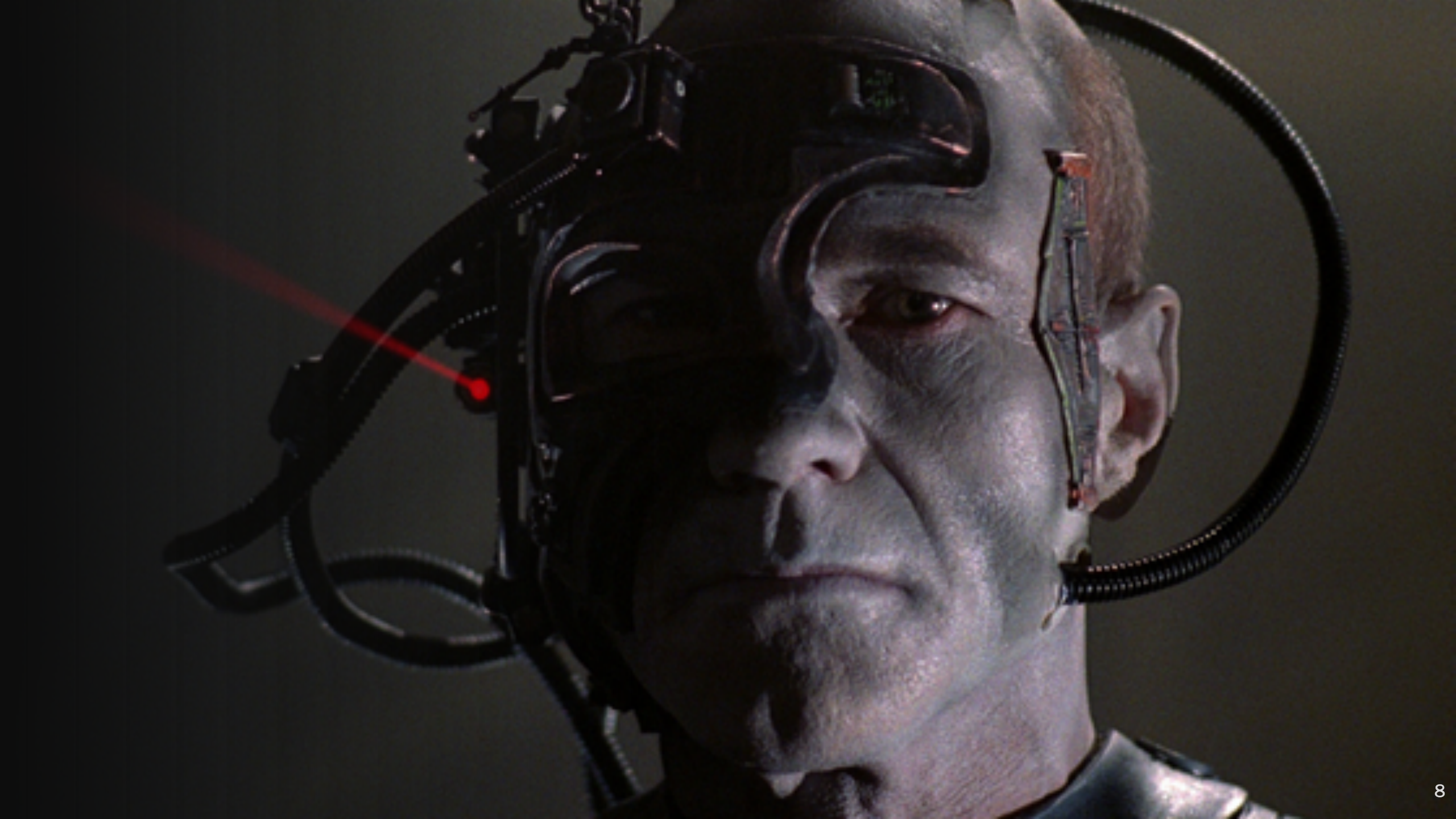


Traditional IT

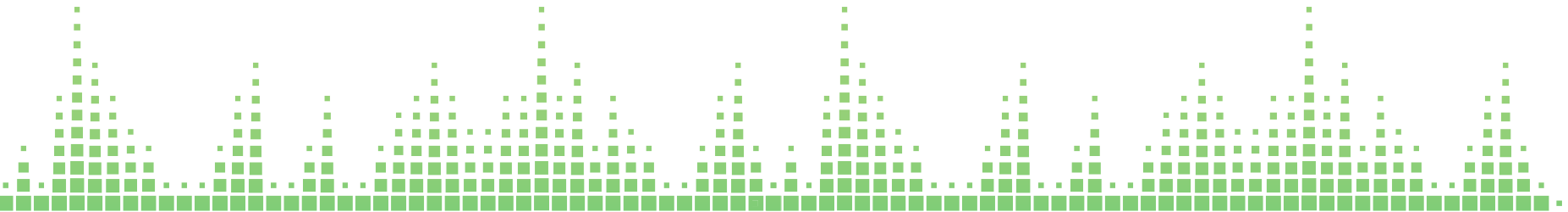
VS.

IT as Code

The primary difference between traditional IT and IT as Code is the mindset, method, and tools used to solve IT problems, deploy new solutions, and to deliver solutions in an agile approach.

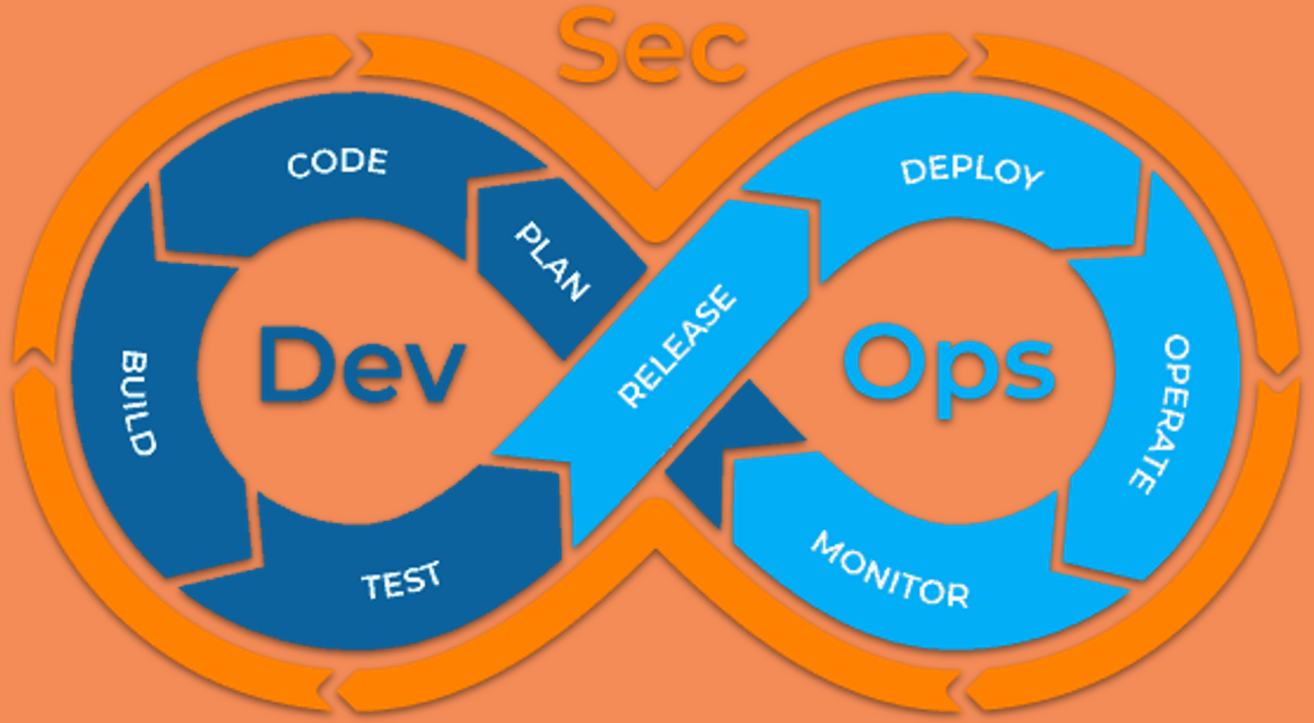


RESISTANCE IS FUTILE, AUTOMATE



IT as Code Requires DevSecOps

Dev Team



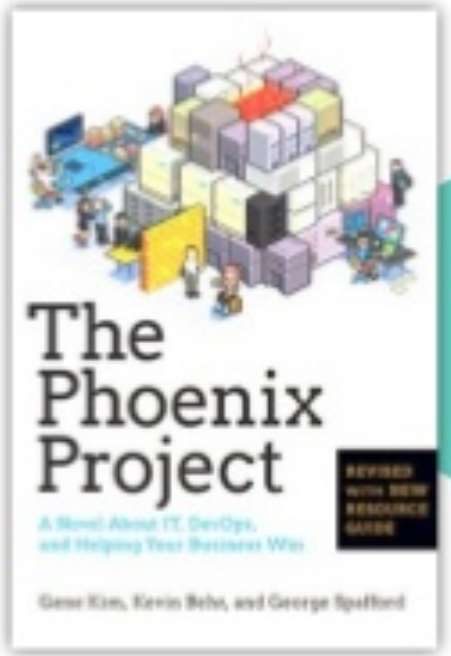
Ops Team

Security Team

DevSecOps added agile infrastructure [as code] to agile software development

DevSecOps added agile security [as code] to DevOps.

DEVSECOPS IS VERY PROMISING...



DEVOPS

1. Establish work flow

2. Ensure instant feedback

3. Culture of experimentation

DEVSECOPS

1. Establish security work flow

2. Ensure instant security feedback

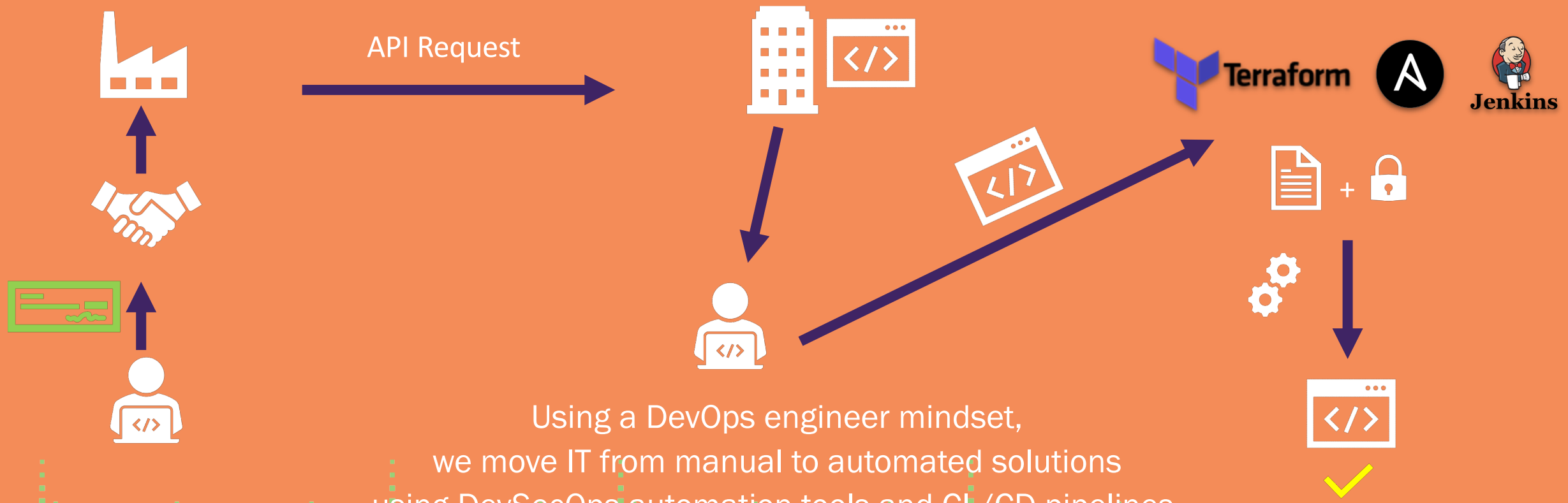
3. Build a security culture

Principles of DevSecOps

Instead of	configuring by hand	we	automate.
Instead of	manually responding to alerts and events	we	create automation that helps cut down on labor overhead and eliminates human error.
Instead of	being reactive	we	are proactive and use automation to deliver IT as Code solutions in an agile approach.
Instead of	configuring security manually	we	enforce security controls programmatically.

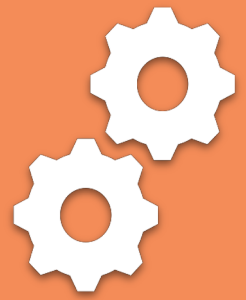
IT as Code via DevSecOps Automation Pipeline

Procure → IT as Code → Run Job



Using a DevOps engineer mindset,
we move IT from manual to automated solutions
using DevSecOps automation tools and CI/CD pipelines.

DevSecOps CI/CD Pipeline Requirements



Automation

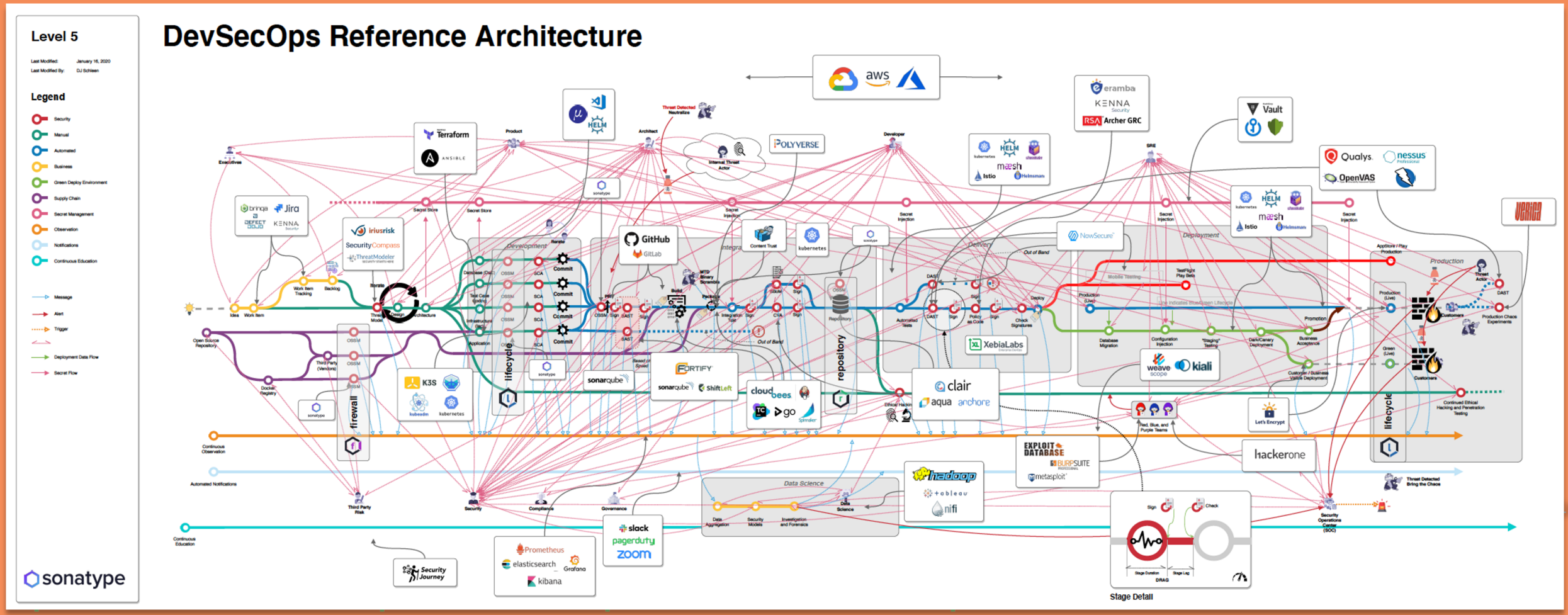
Integration

Agile Delivery

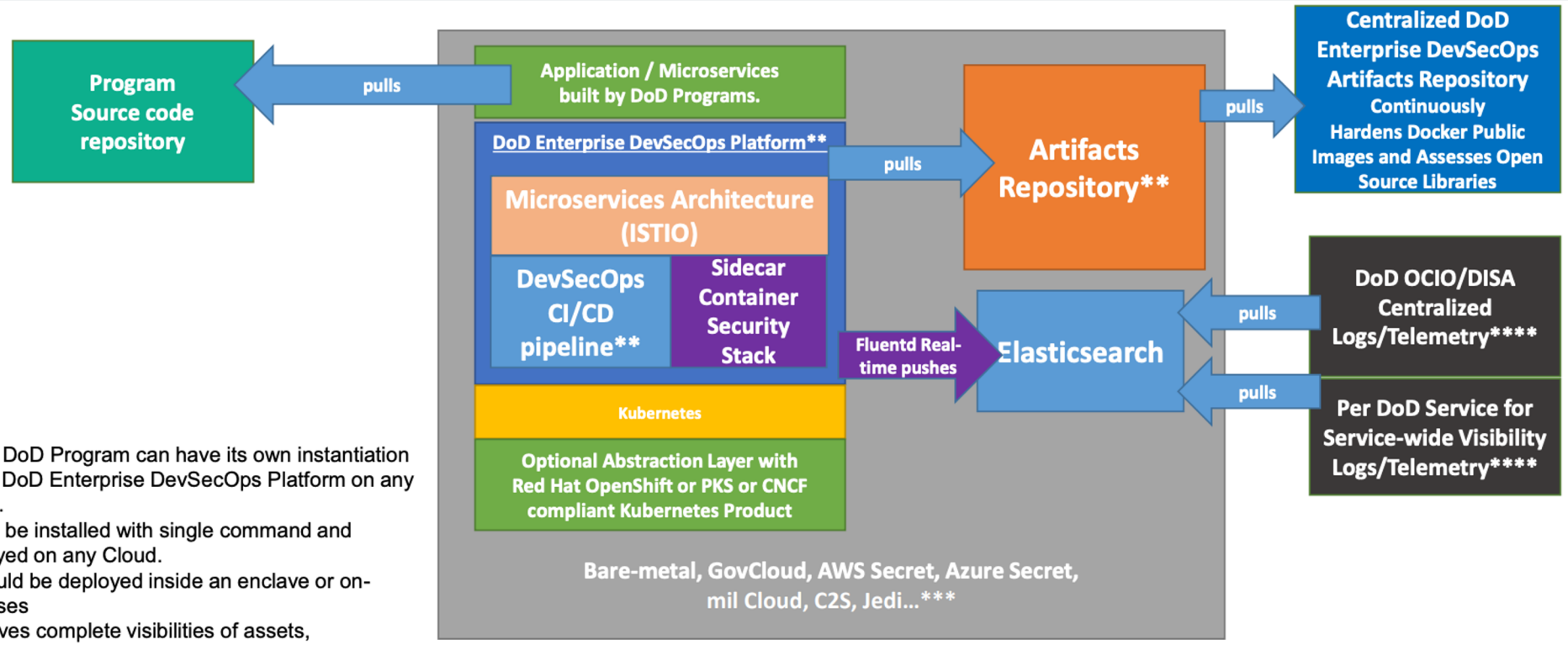
Security

SOUNDS EASY?

DevSecOps Reference Architecture



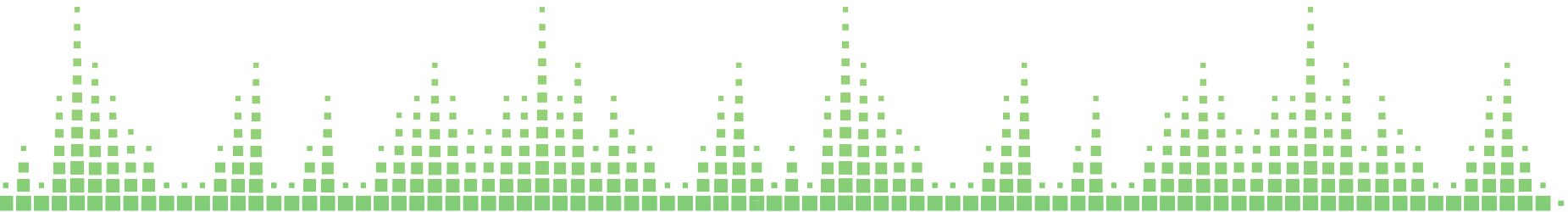
DoD Enterprise DevSecOps Architecture*

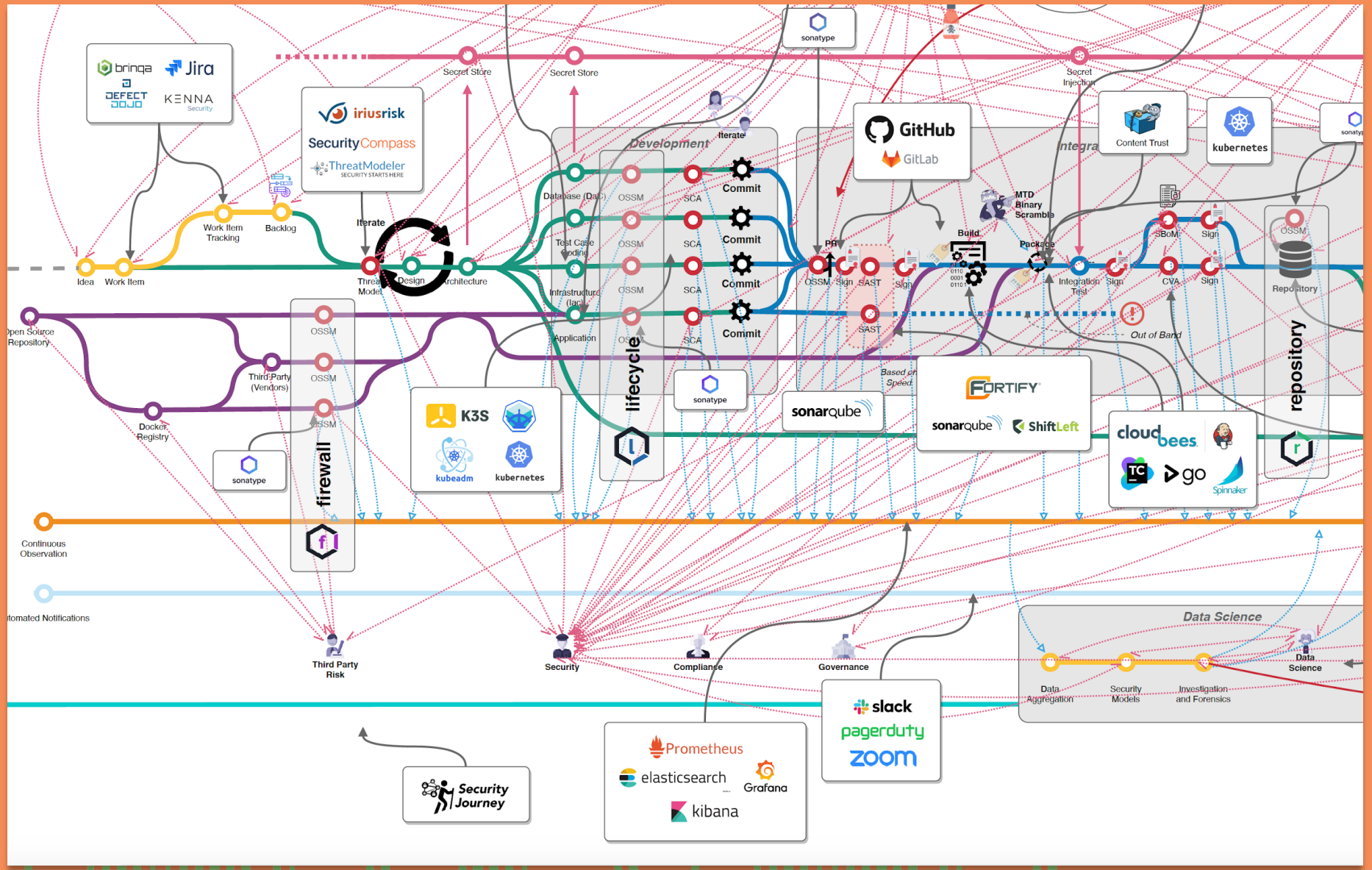


*each DoD Program can have its own instantiation of the DoD Enterprise DevSecOps Platform on any Cloud.
** can be installed with single command and deployed on any Cloud.
*** could be deployed inside an enclave or on-premises
**** gives complete visibilities of assets, security/vulnerability state etc. can be integrated to existing cybersecurity shared services.

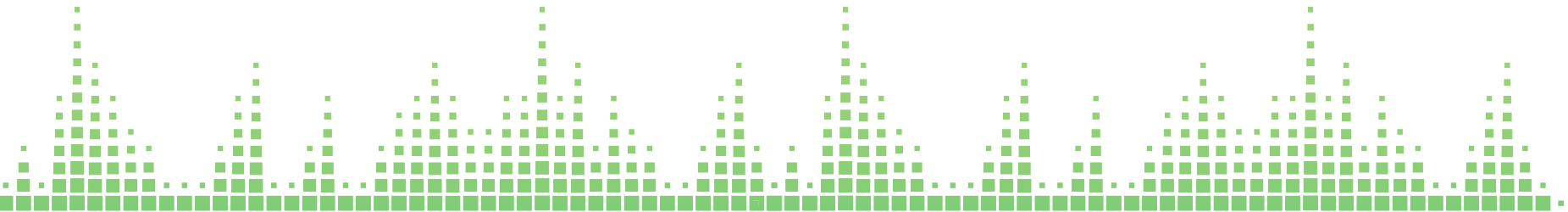
https://software.af.mil/wp-content/uploads/2019/12/DoD-Enterprise-DevSecOps-Initiative-Keynote-v1.7.pdf

DEVSECOPS IS COMPLICATED

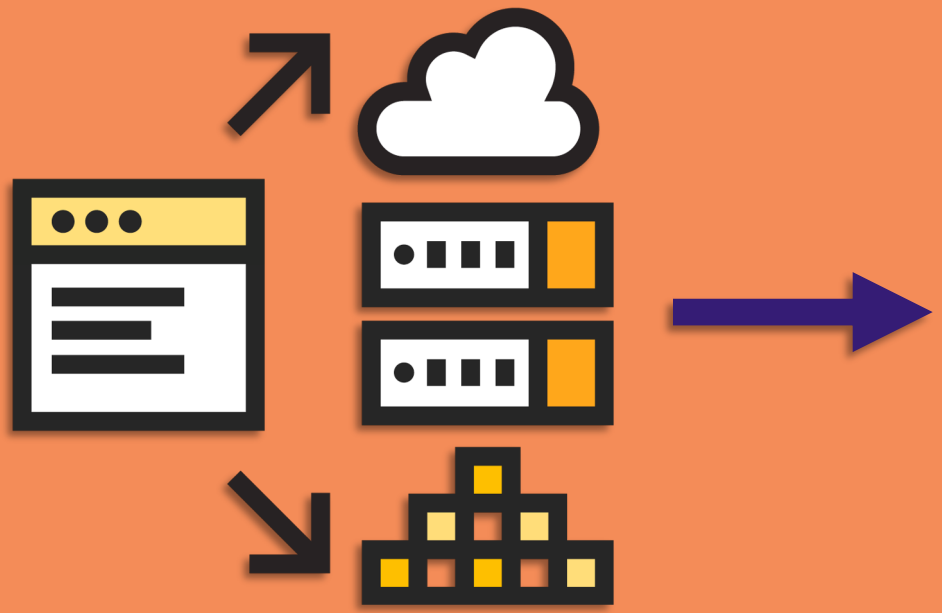



bringa
Jira
DEFECT DOJO
KENNA Security
iriusrisk
SecurityCompass
ThreatModeler
SECURITY STARTS HERE
Secret Store
Secret Store
sonatype
Secret Injection
GitHub
GitLab
Content Trust
kubernetes
Development
Iterate
Work Item Tracking
Backlog
Iterate
Idea
Work Item
Threat Model
Design
Architecture
Database (DaC)
Test Case Coding
Infrastructure (IaC)
Application
OSSM
SCA
Commit
PR
OSSM
Sign
SAST
Sign
Build
MTD Binary Scramble
Package
Integration Test
Sign
SBoM
Sign
CVA
Sign
OSSM
Repository
Integra
Open Source Repository
Third Party (Vendors)
Docker Registry
OSSM
OSSM
OSSM
firewall
sonatype
K3S
kubeadm
kubernetes
lifecycle
sonatype
sonarqube
SAST
Out of Band
Based on Speed
FORTIFY
sonarqube
ShiftLeft
cloudbees
go
Spinnaker
repository
Continuous Observation
Automated Notifications
Third Party Risk
Security
Compliance
Governance
Data Science
Data Aggregation
Security Models
Investigation and Forensics
Data Science
slack
pagerduty
zoom
Prometheus
elasticsearch
Grafana
kibana
Security Journey

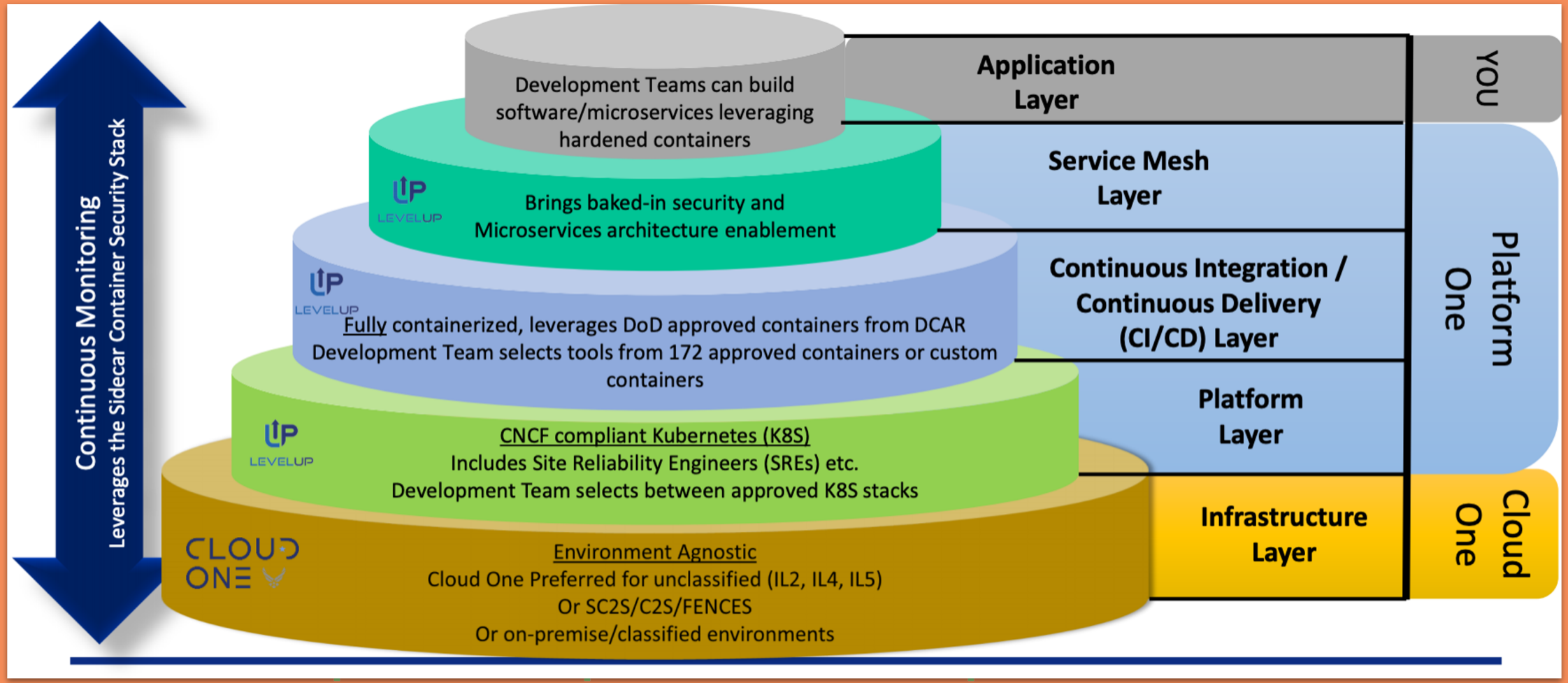
SECURITY TOUCHES EVERYTHING



DevSecOps Technology Stack

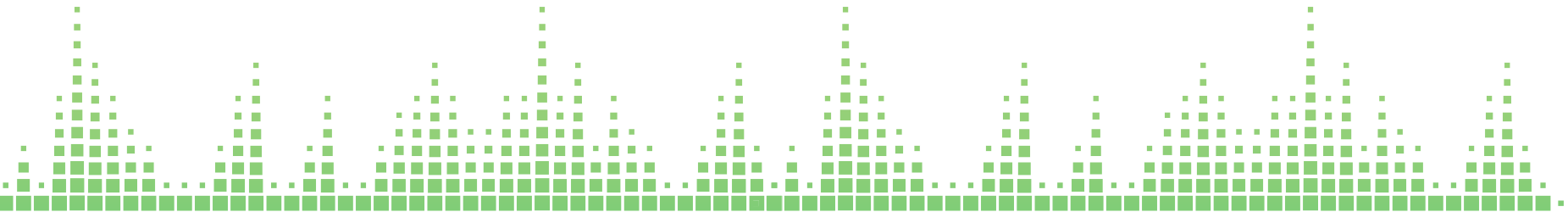


- Infrastructure as Code (“IaC”)
- Configuration Management
- API Integrations
- Security as Code
- Source Control



https://software.af.mil/wp-content/uploads/2019/12/DoD-Enterprise-DevSecOps-Initiative-Keynote-v1.7.pdf

MANY LAYERS OF DEVSECOPS



Git

AWS CFT

Azure ARM

Ansible

Google Cloud

Kubernetes

Terraform

Python

Powershell

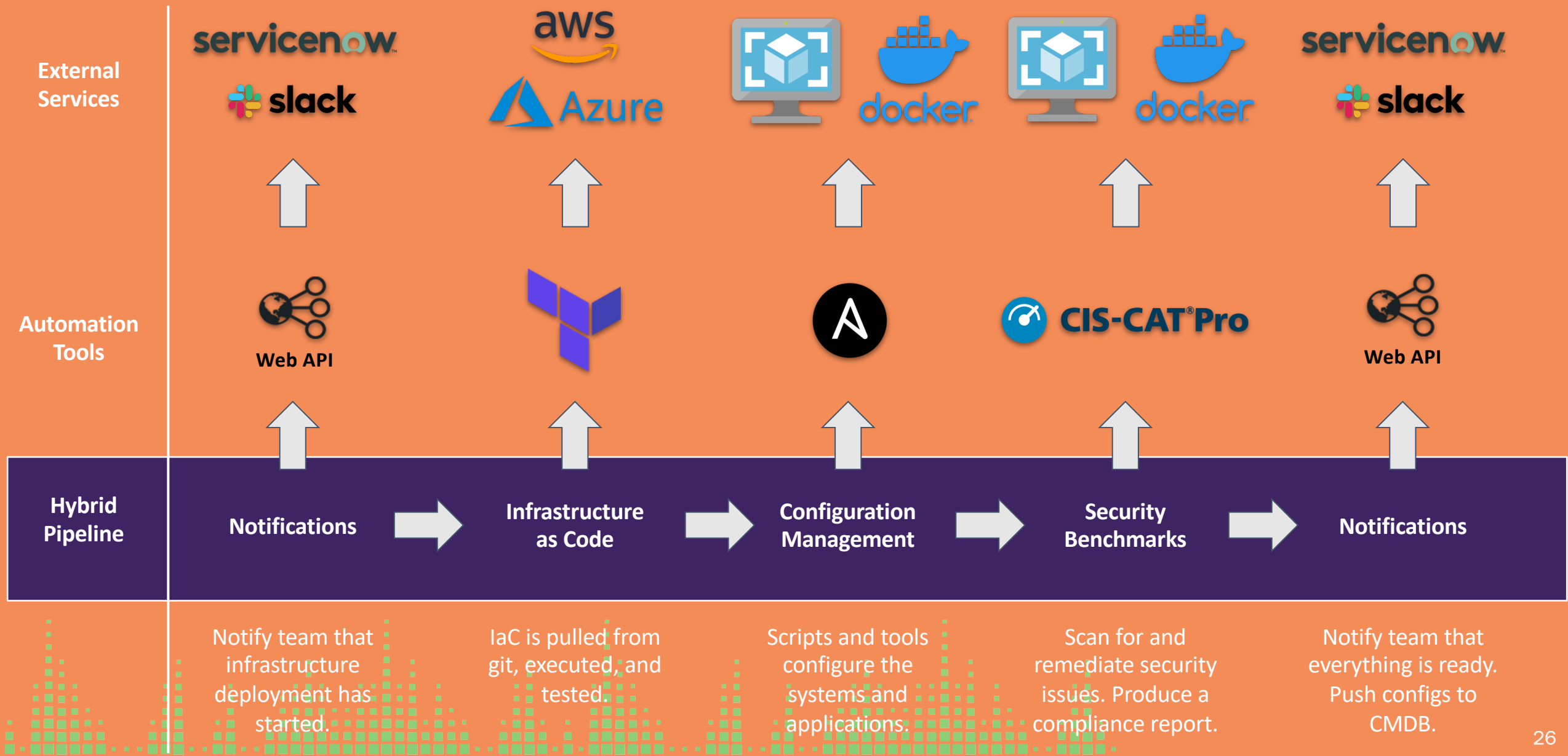
OpenSCAP

Open Policy Agent

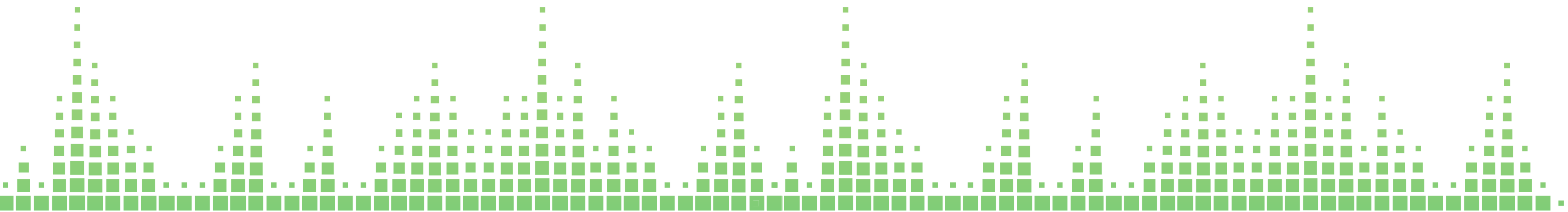
And many more!

Example DevSecOps CI/CD Pipeline

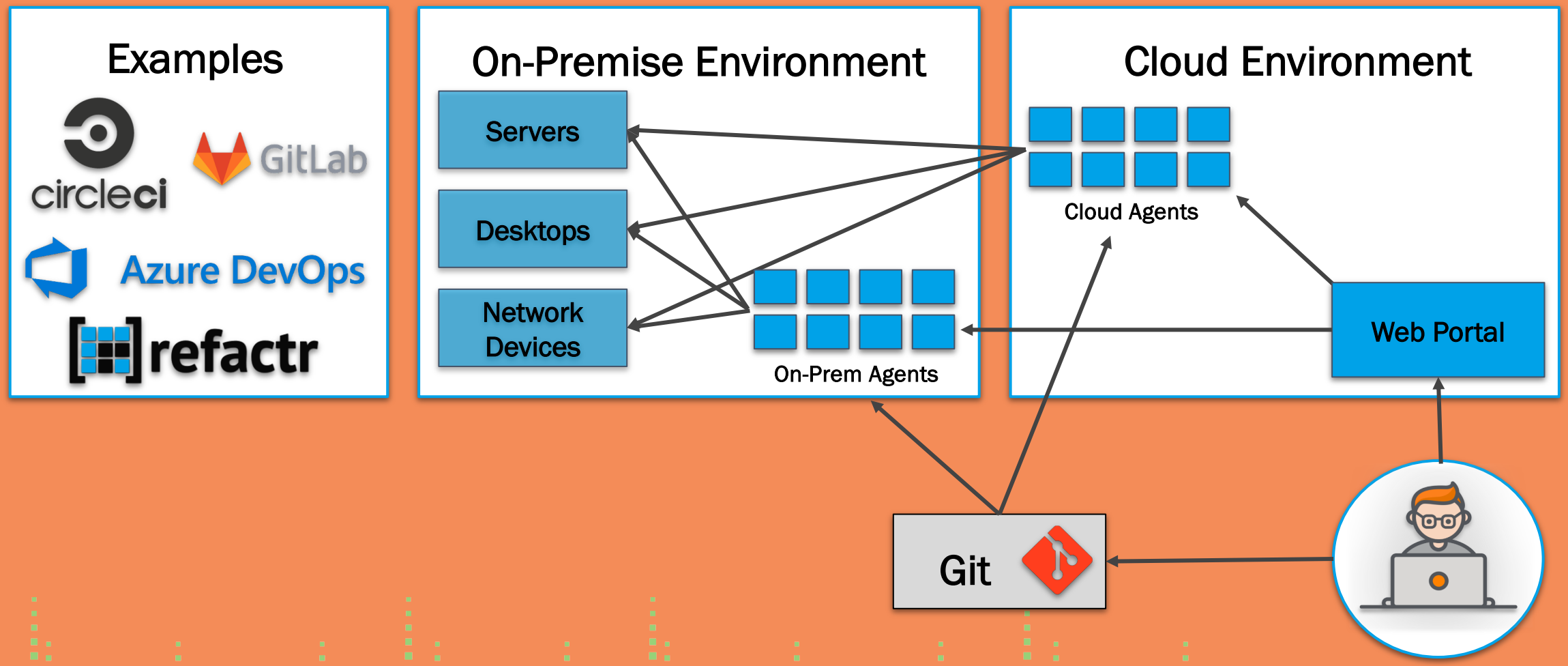
Source Code	Build & Test	IaC	Configuration	Code Deploy	Security Scans & Reporting
GitLab	Jenkins	HashiCorp Terraform	ANSIBLE	docker	CIS-CAT Pro
Node.js	Jenkins Pipeline Mocha	AKS Load Balancers S3 Bucket VMWare	Apache RHEL Config K8S Config	Docker Images Dockerhub	XCCDF Scans XCCDF Reports Upload to S3


External Services
servicenow
slack
aws
Azure
docker
docker
servicenow
slack
Automation Tools
Web API
CIS-CAT Pro
Web API
Hybrid Pipeline
Notifications
Infrastructure as Code
Configuration Management
Security Benchmarks
Notifications
Notify team that infrastructure deployment has started.
IaC is pulled from git, executed, and tested.
Scripts and tools configure the systems and applications.
Scan for and remediate security issues. Produce a compliance report.
Notify team that everything is ready. Push configs to CMDB.

PURPOSE-BUILT PIPELINES

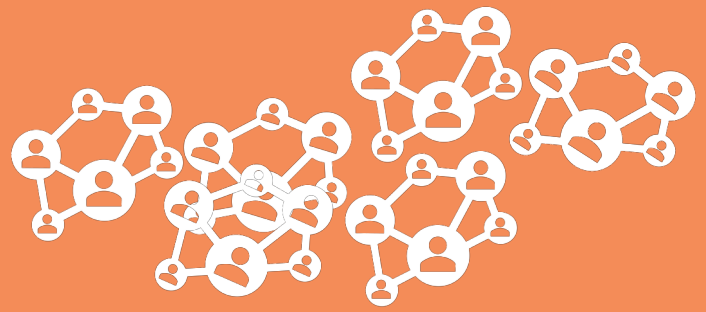


CI/CD Platform – Hybrid Architecture

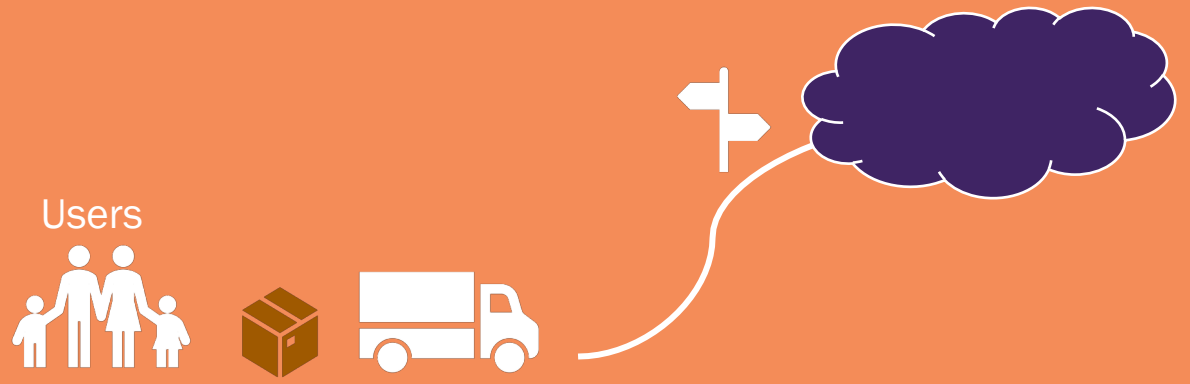


Why CI/CD Pipelines for DevSecOps with Hybrid Cloud?

IT is shifting to software-defined everything, not there yet



Shift Toward Everything-as-a-Service
Most organization not even close to 100% cloud



Moving to the cloud, still requires hybrid approach

Configuration Complexity with IT as Code
In Hybrid Cloud Enviroments

SEE YOU IN THE FALL!
November 12, 2020 | alldaydevops.com/register-2020
ADDO
ALL DAY DEVOPS