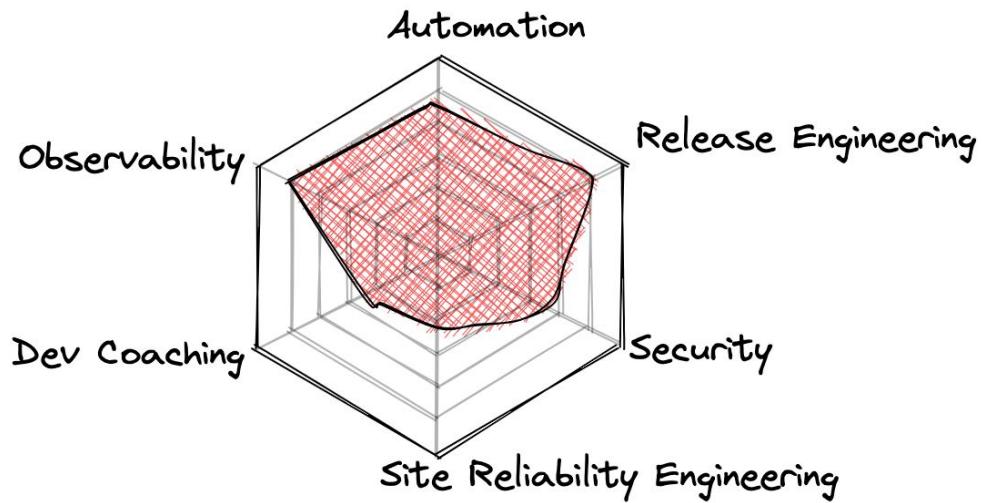


Platform Engineering



Jirayut Nimsaeng (Dear)

CEO & Founder, Opsta (Thailand) Co.,Ltd.

Dev Mountain Tech Festival

March 19, 2021

<https://bit.ly/opsta-dmtf-platform-engineering>



#whoami

Jirayut Nimsaeng (Dear)

Jirayut has been involved in DevSecOps, Container, Cloud Technology and Open Source for over 10 years. He has experienced and succeeded in transforming several companies to deliver greater values and be more agile.

- **He is Founder and CEO of Opsta (Thailand) Co.,Ltd.**
- **He is Cloud/DevSecOps Transformation Consultant and Solution Architecture**
- **He is the first Certified Kubernetes Security Specialist (CKS) and Certified Kubernetes Administrator (CKA) in Thailand**
- **He is first Thai Google Cloud Developer Expert (GDE) in Thailand**
- **Google Cloud Certified - Professional Cloud Architect and Associate Cloud Engineer**



What are we going to talk about today

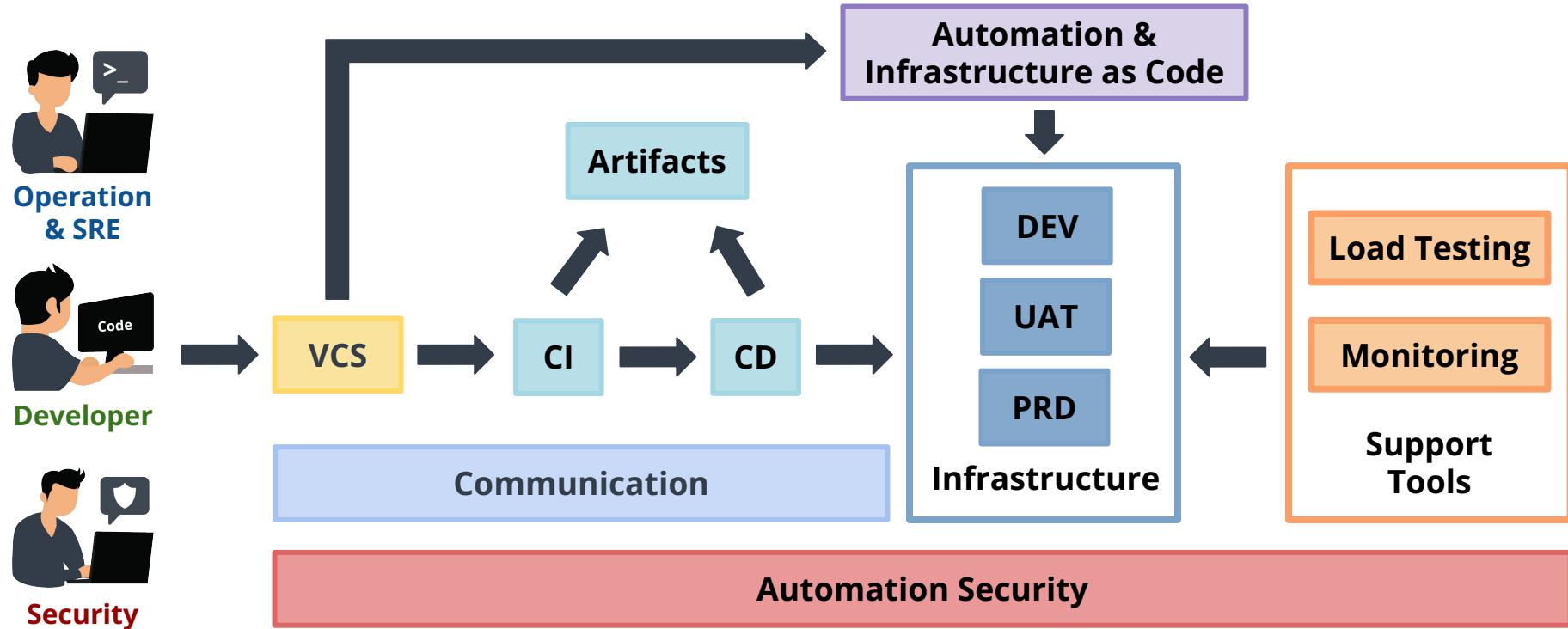
- Why Platform?
- What is Platform Engineering?
- How to build Platform Engineering
- Platform Engineering Self-Service
- Demo
- Wrap up & Q/A



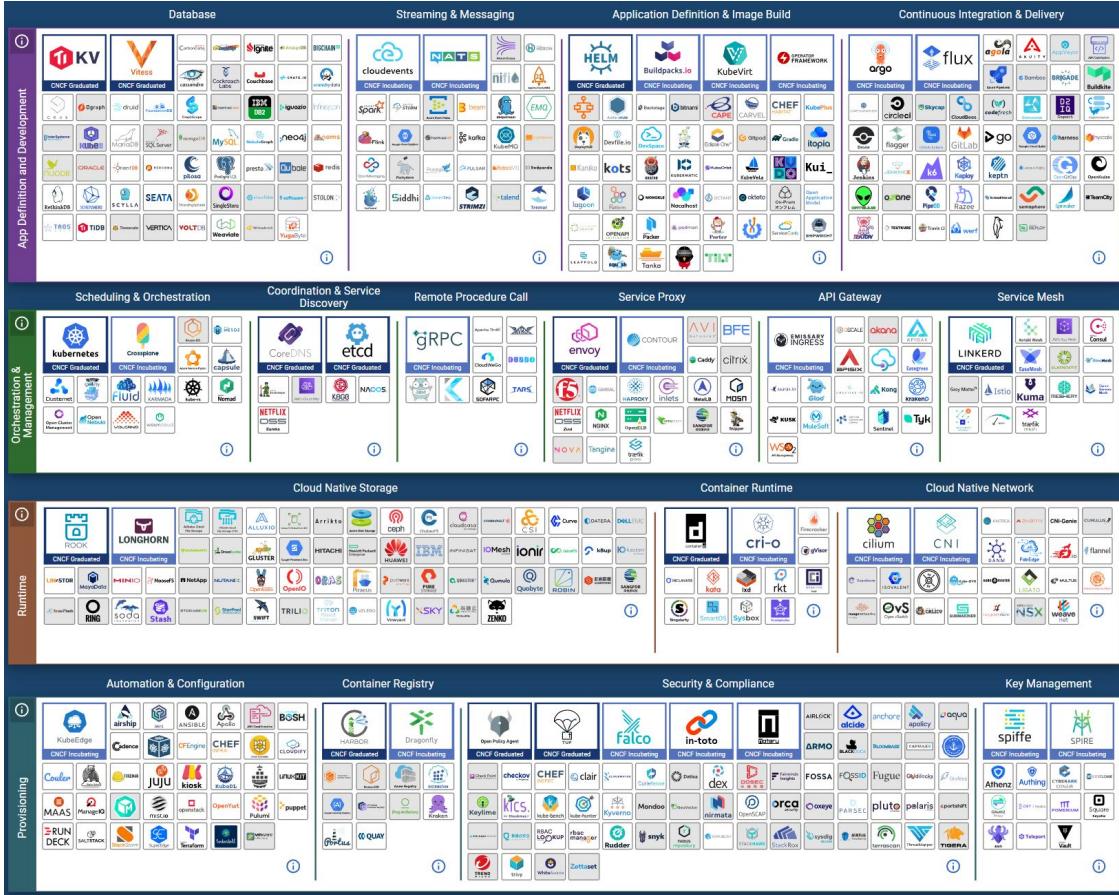
Why Platform?



Building

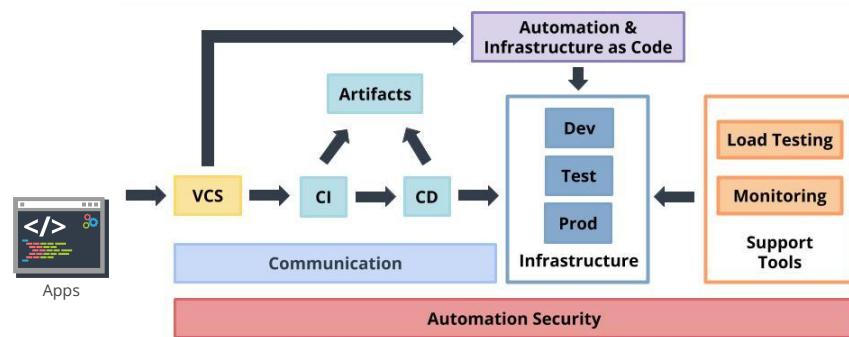
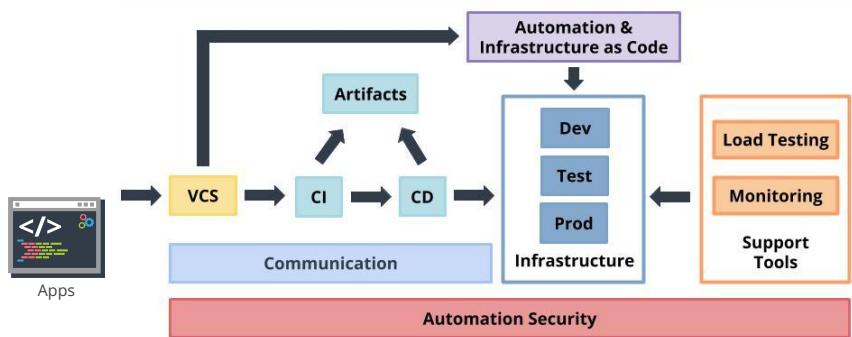
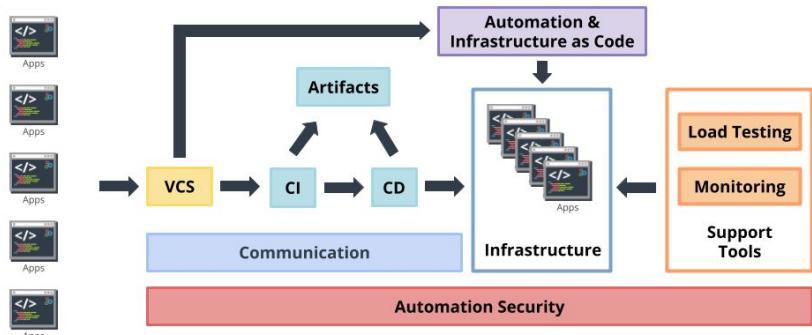
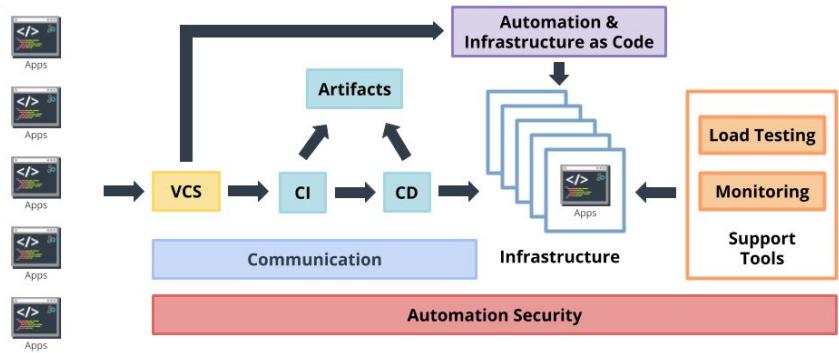


A lot of tools

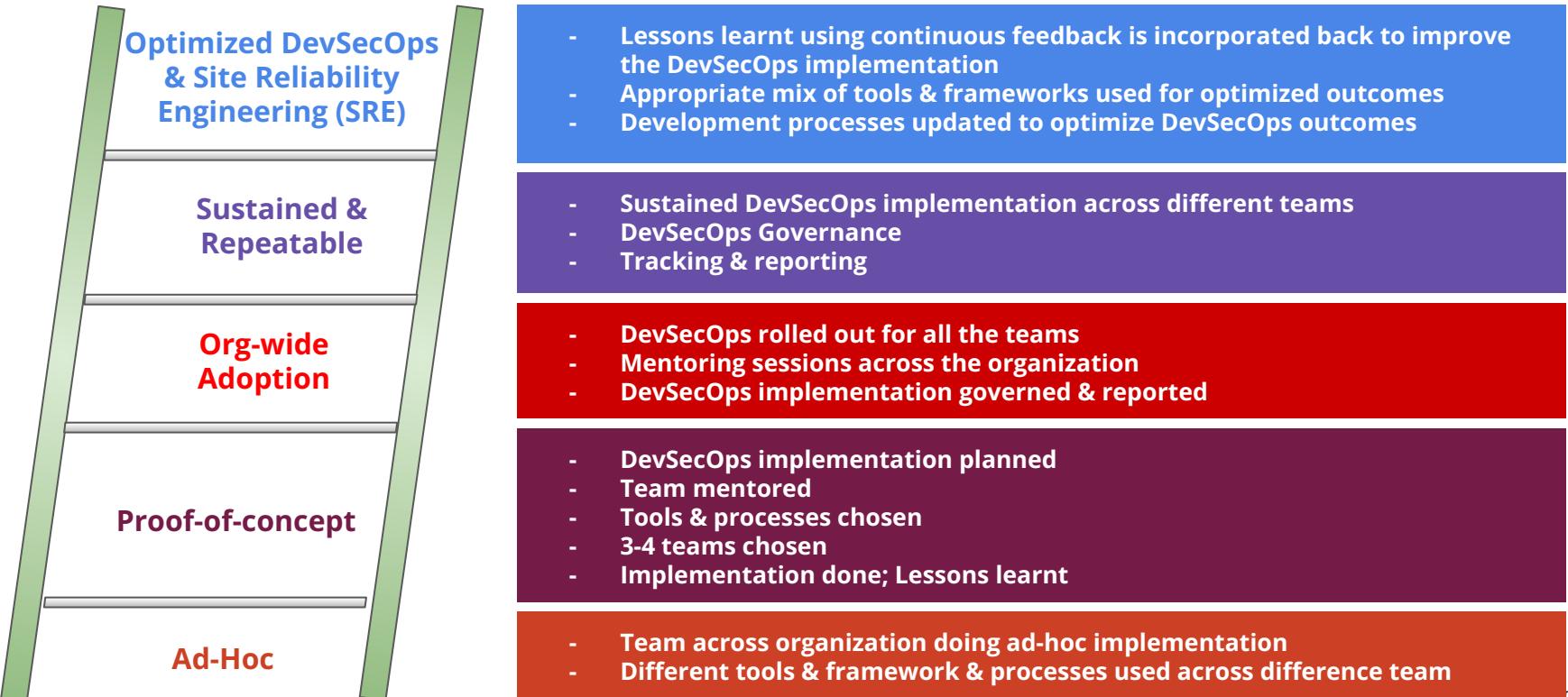


<https://landscape.cncf.io>

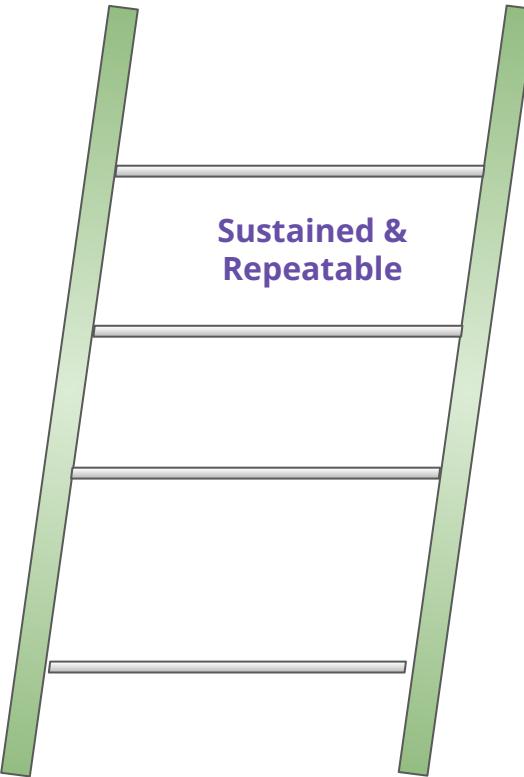
Too many variations



DevSecOps Maturity Levels



DevSecOps Maturity Levels



- Sustained DevSecOps implementation across different teams
- DevSecOps Governance
- Tracking & reporting

This is Platform



When we need Platform?

- Want a dedicated team focused on constant innovation of how applications are deployed and operated in production
- Want application teams to focus on building the business features for end-users
- Aligning how various teams deploy and operate applications across the organization
- Teams lack the skills to self-manage deployment and operations

<https://shahadarsh.com/2020/10/12/platform-engineering/>

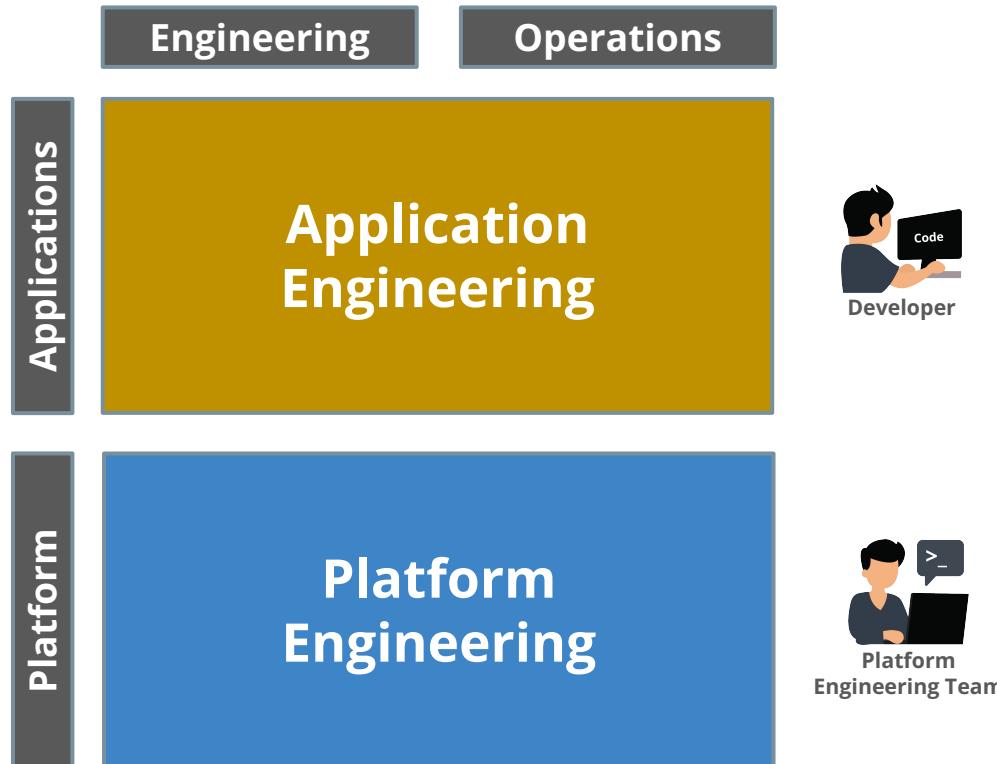
What is Platform Engineering?



What is Platform Engineering?

Platform Engineering is a practice of building and operating a common platform as a product for technology teams. It reduces time to market and complexity by providing **self-service** deployments for infrastructure and application and ease of operating applications in production. The team building and operating the common platform constantly innovates and provides best practices implementation, tools, and automation.

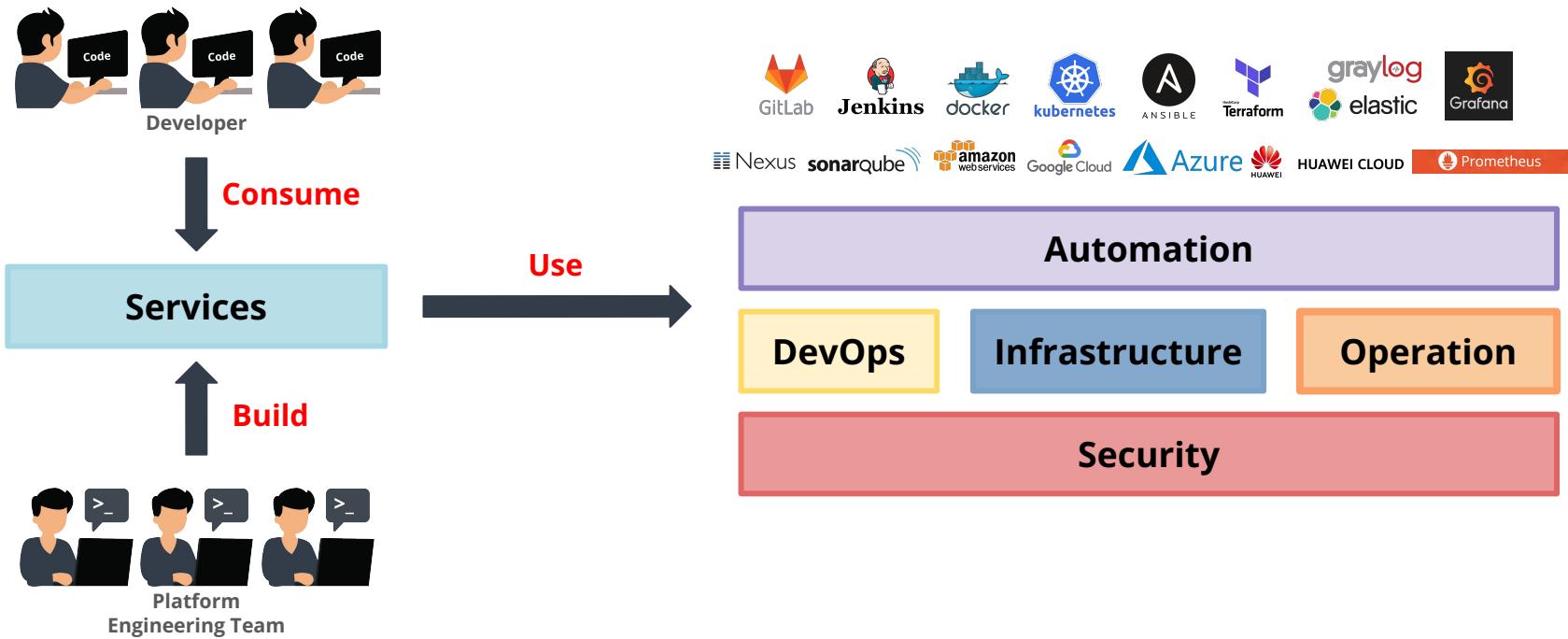
Platform Engineering



<https://docs.aws.amazon.com/wellarchitected/latest/operational-excellence-pillar/separated-aeo-and-ieo-with-centralized-governance.html>



Internal Developer Platform (IDP)



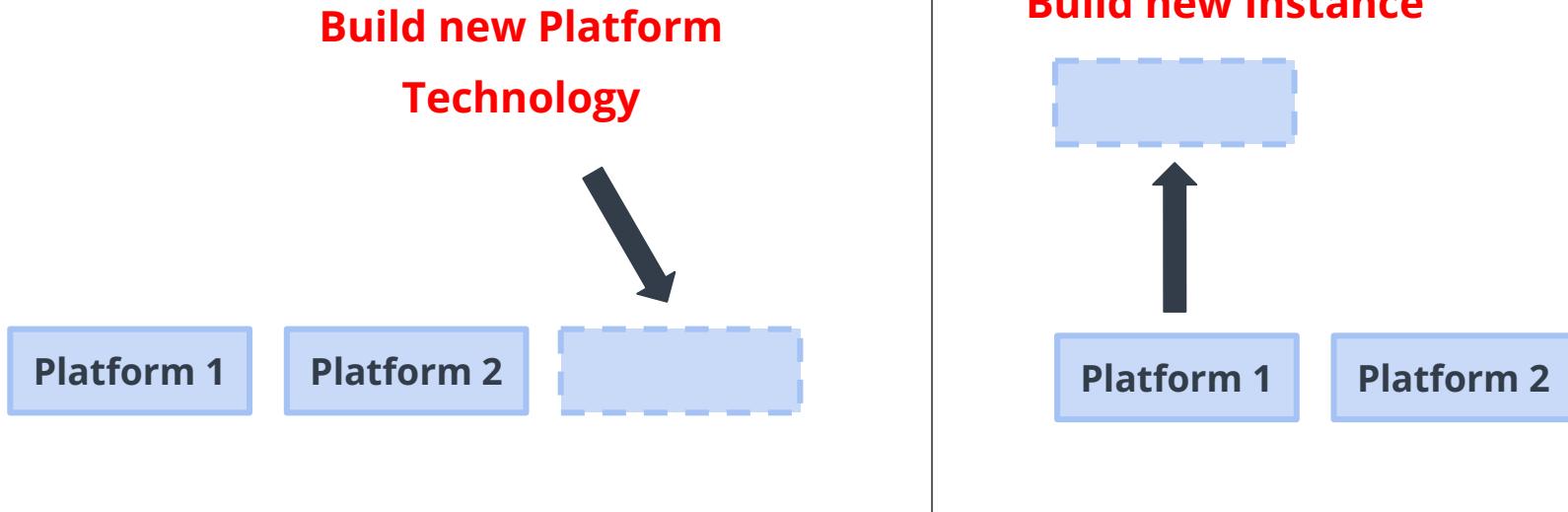
Platform Engineering is a new product

- **[Customers] For** Application Development, Information Security, Compliance, and Infrastructure Teams
- **[Goal] Who Need** to deploy & operate applications in Production
- **[Solution] We Are Providing** Scalable, Secure, Reusable, and Self Service Platform
- **[Key Outcome] That can enable** out of the box complex deployments & operations using industry best practices
- **[Key Differentiator] Which is** declarative, extendable & a comprehensive plug & play solution
- **[Value] So that** they get a competitive advantage by reducing Time to Market & Complexity

<https://shahadarsh.com/2020/10/12/platform-engineering/>



What Platform Engineering Team Do?



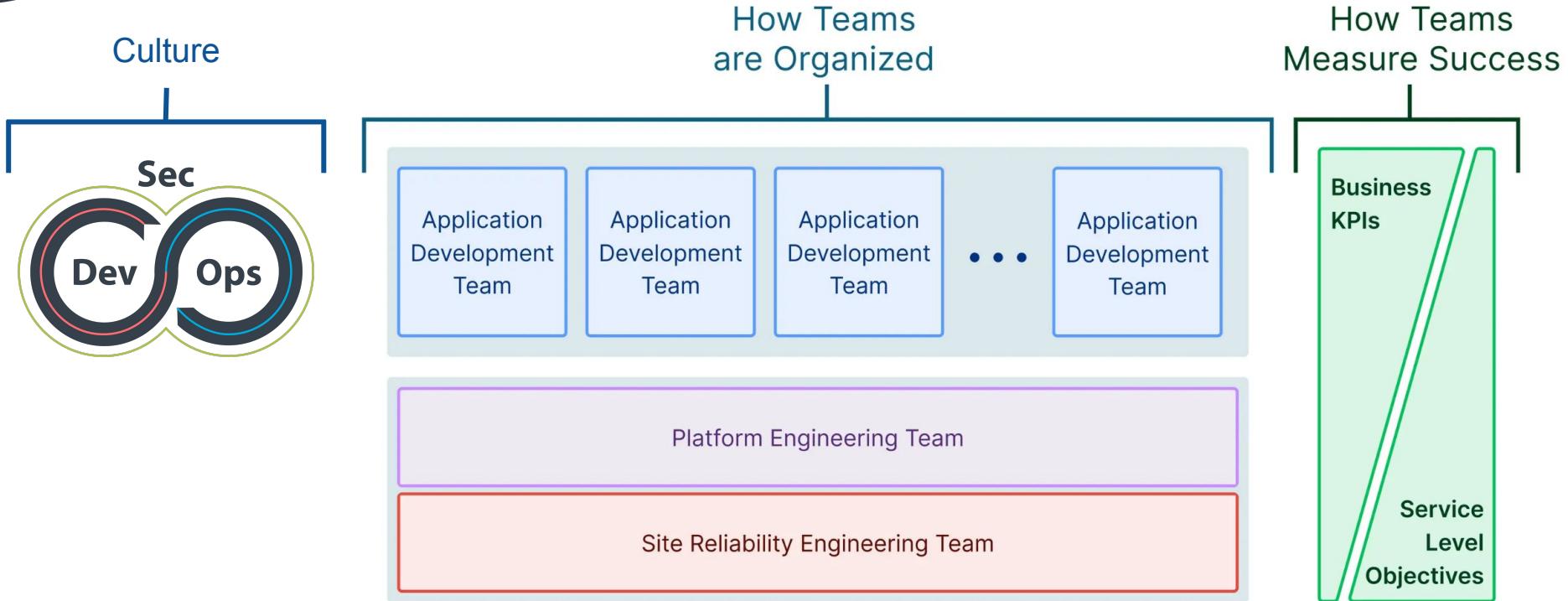
Benefit of Platform Engineering

- Reduce the toil of software development
- Improve Engineering Productivity
- Provide Consistency & Confidence
- Help Scale Teams

Team Topologies



DevSecOps, SRE, and Platform Engineering



How to build Platform Engineering



Treat Platform Engineering as Product

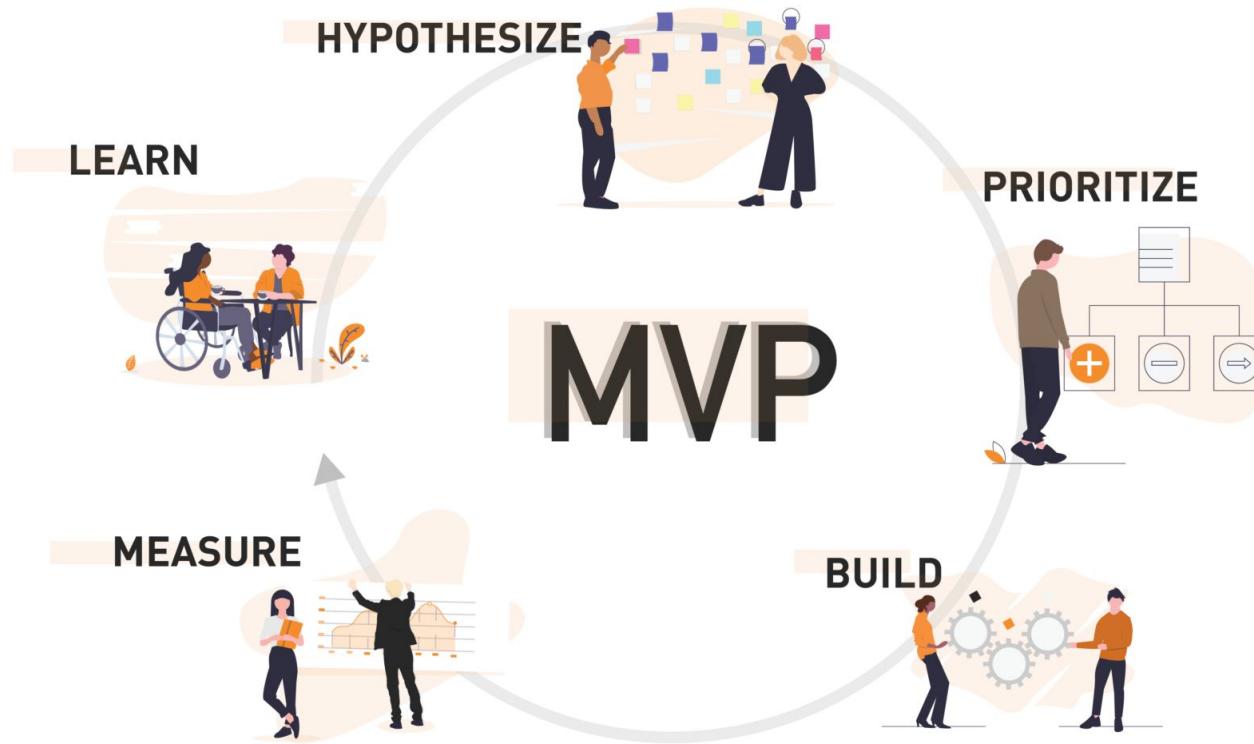
- Requirements
- Product Manager
- Planning
- Onboarding
- Feedback

Platform Engineering Sample Features

- Infrastructure Provisioning
- Container Platform
- Self-service Pipelines
- Change & Release Management
- Observability Tools
- Identity Management
- Secret Management
- Security Baseline
- Automation Security Integration
- Load Testing Platform



Treat Platform as Most Viable Product



Create Platform Tech Stacks

Project Management	Frontend	Backend	Testing	API Gateway
Jira Software	React 	.NET  Java	 Robot Framework	 Kong
Relation Database	NoSQL Database	Un-structure Database	In-memory Database	Messaging & Streaming
ORACLE DATABASE 		elasticsearch	redis	RabbitMQ 
Communication	Version Control	CI/CD	Artifacts Server	Load Testing
Microsoft Teams	GitLab	Jenkins	Sonatype Nexus	APACHE JMeter™ 
Metric Monitoring	Log Centralized	APM	Security	Secret Manager
Grafana  Thanos 	graylog kibana	JAEGER 	anchore sonarqube 	HashiCorp Vault
Container Platform	Infrastructure as Code	Automation	Public Cloud	Private Cloud
kubernetes  		 ANSIBLE	amazon web services	vmware 

Use Cloud

Private Cloud



Public Cloud



Hybrid Cloud



Build Container Platform

Installation Tools



minikube



kops



K3S



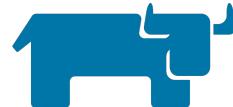
Commercial



OPENSHIFT



VMware Tanzu



RANCHER®

Public Cloud



Amazon EKS



**IBM Cloud
Container Service**

Build Kubernetes Multi-Tenancy

- **Access Control**

Use policies to ensure that tenants can access only what they should have access to

- *RBAC*

- **Fair Sharing**

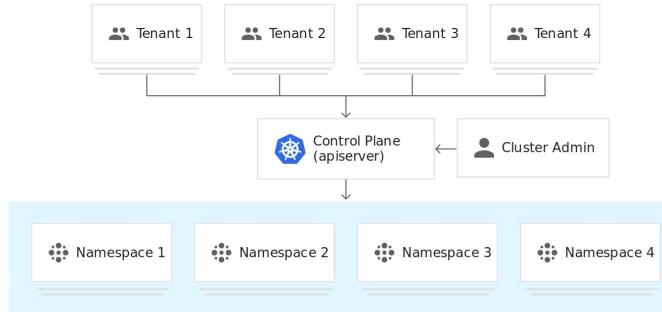
Enforce limits per tenant

- *Resource Quota*
- *Pod Priority*
- *Quality of Service*
- *Taints & Tolerations*
- *Pod Affinity / Anti-affinity*

- **Isolation**

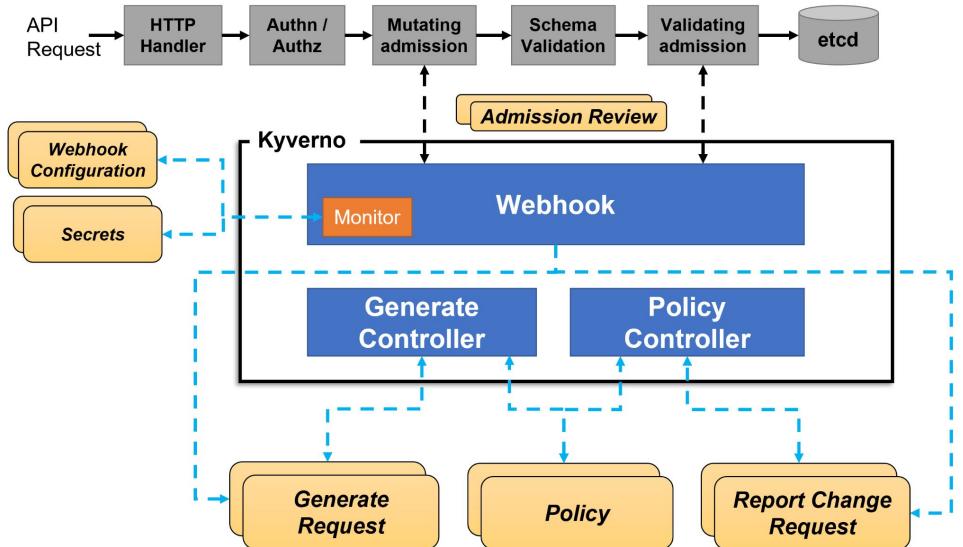
Ensure tenants cannot access each others' workloads, secrets, etc.

- *Namespace*
- *Pod Security Policy*
- *Network Policy*
- *Sandbox*

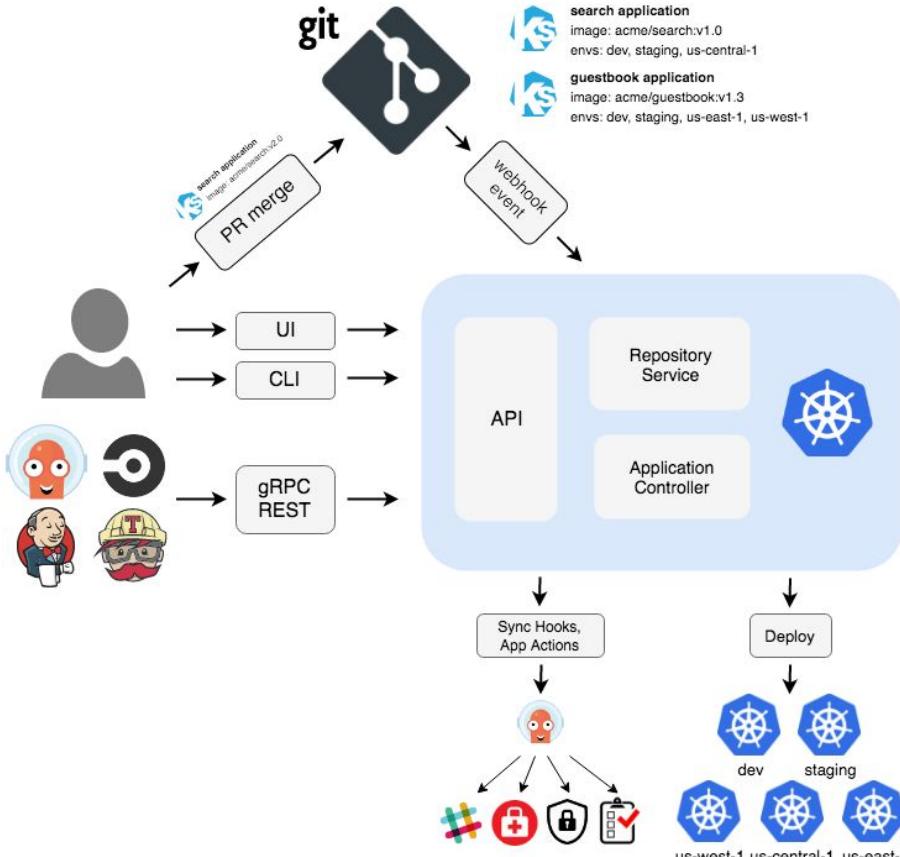


Kubernetes Policies

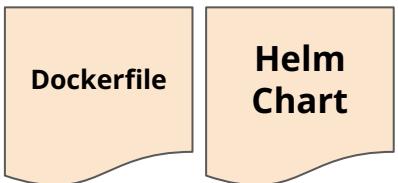
- Disallow Capabilities (Strict)
- Disallow Privilege Escalation
- Require Run As Non-Root User
- Require runAsNonRoot
- Restrict Volume Types
- Add Network Policy
- Add Quota
- Disallow Default Namespace



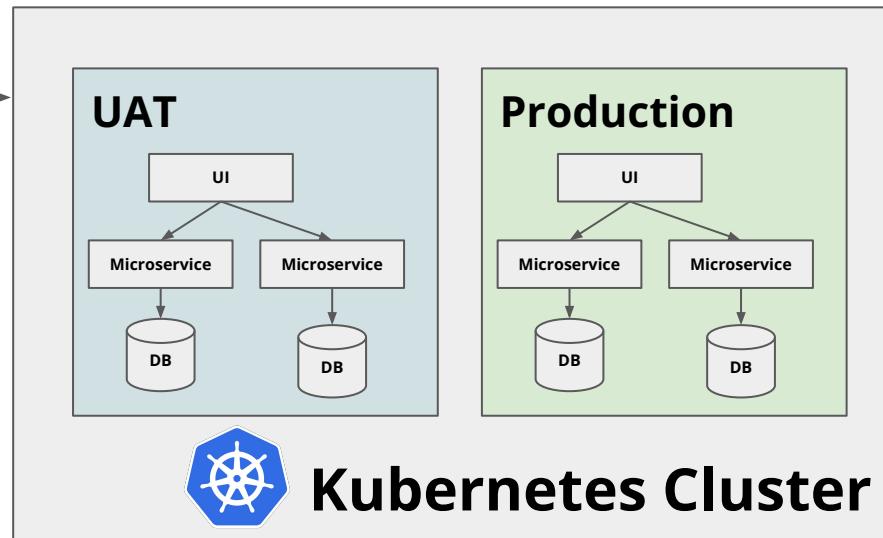
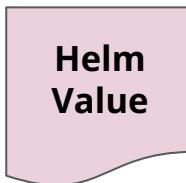
Build Everything with GitOps



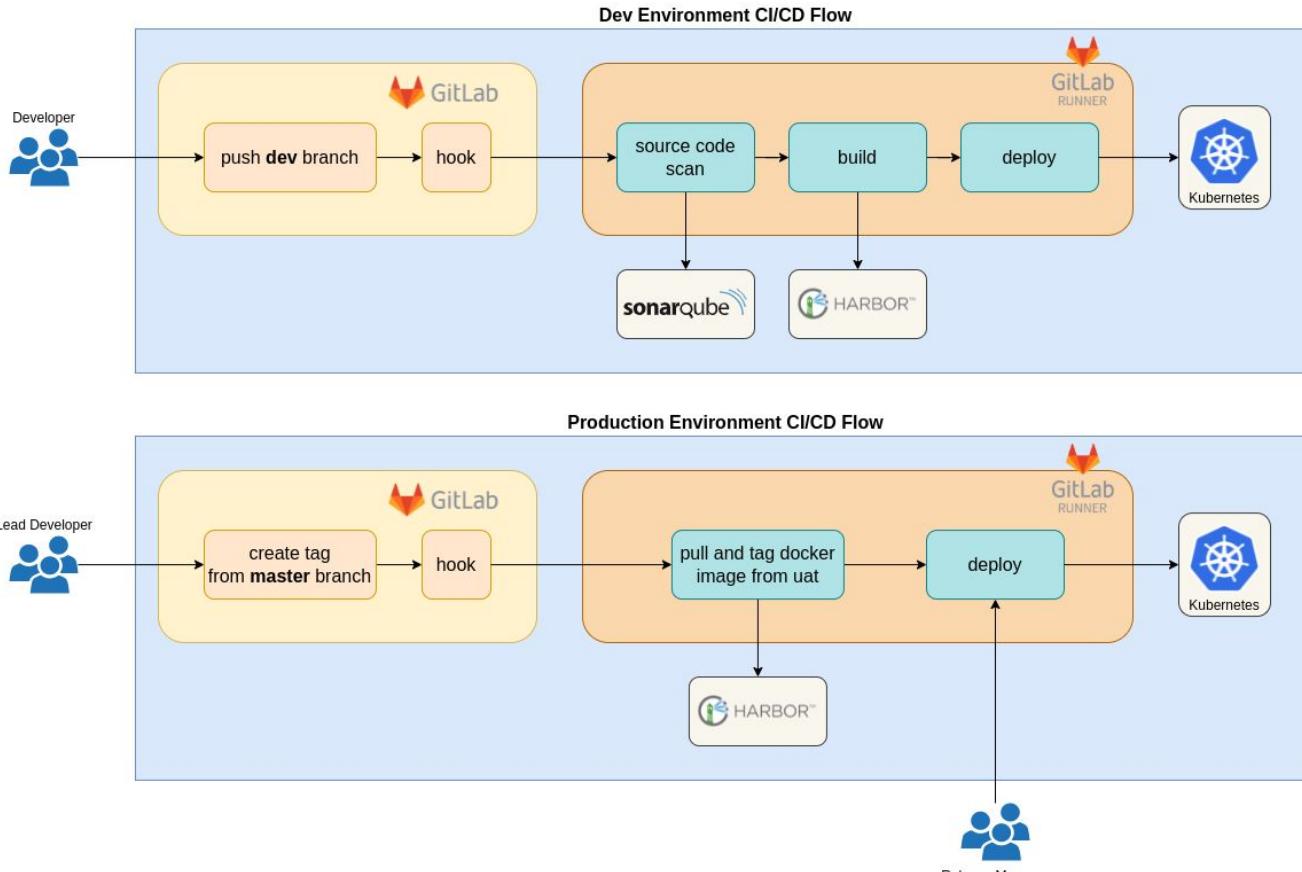
Develop Deployment Pattern



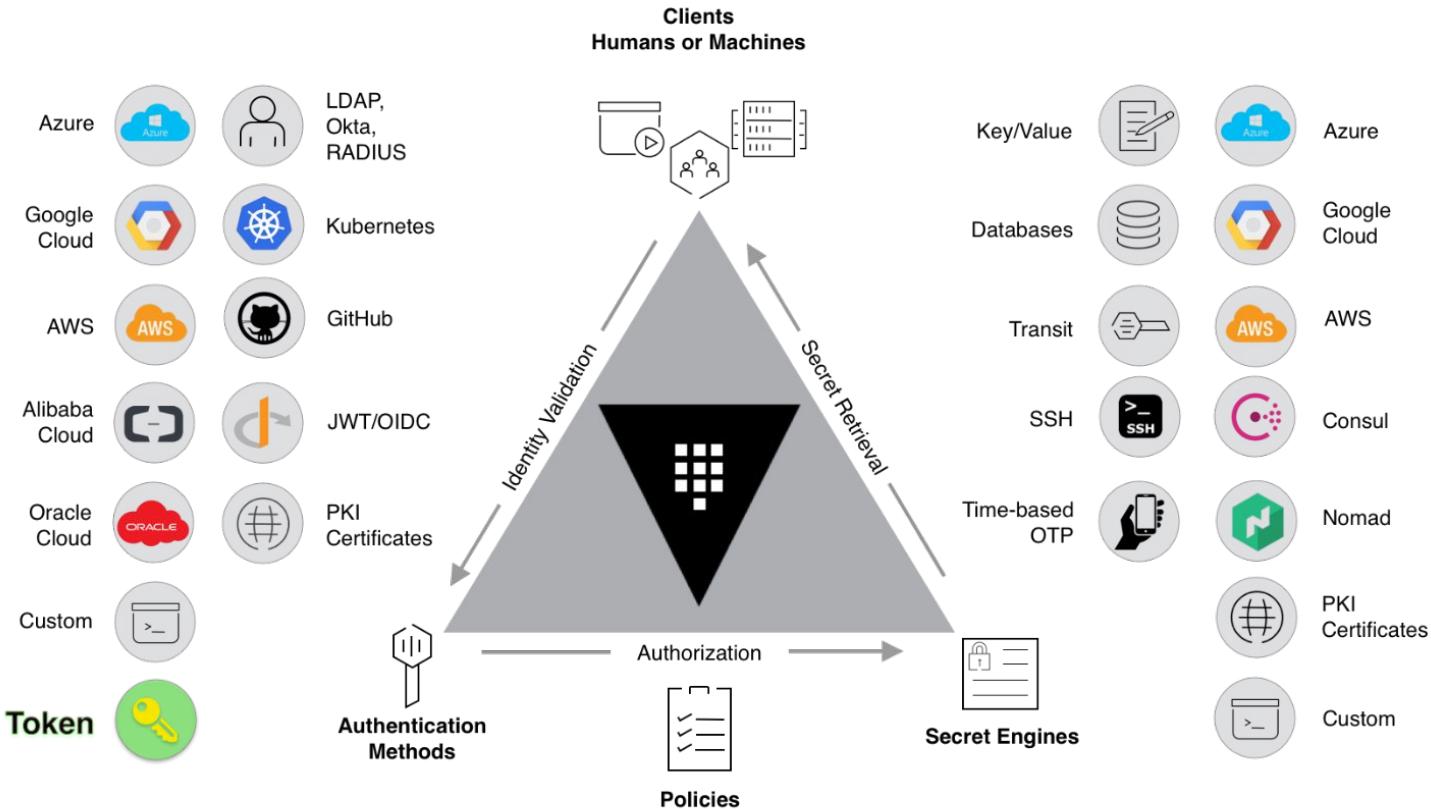
```
app:  
  image: app-a  
  tag: dev  
  replicas: 2  
  healthCheck: "/health"  
  
ingress:  
  host: app-a.example.com  
  
env:  
  DB_URL: db-dev:5432
```



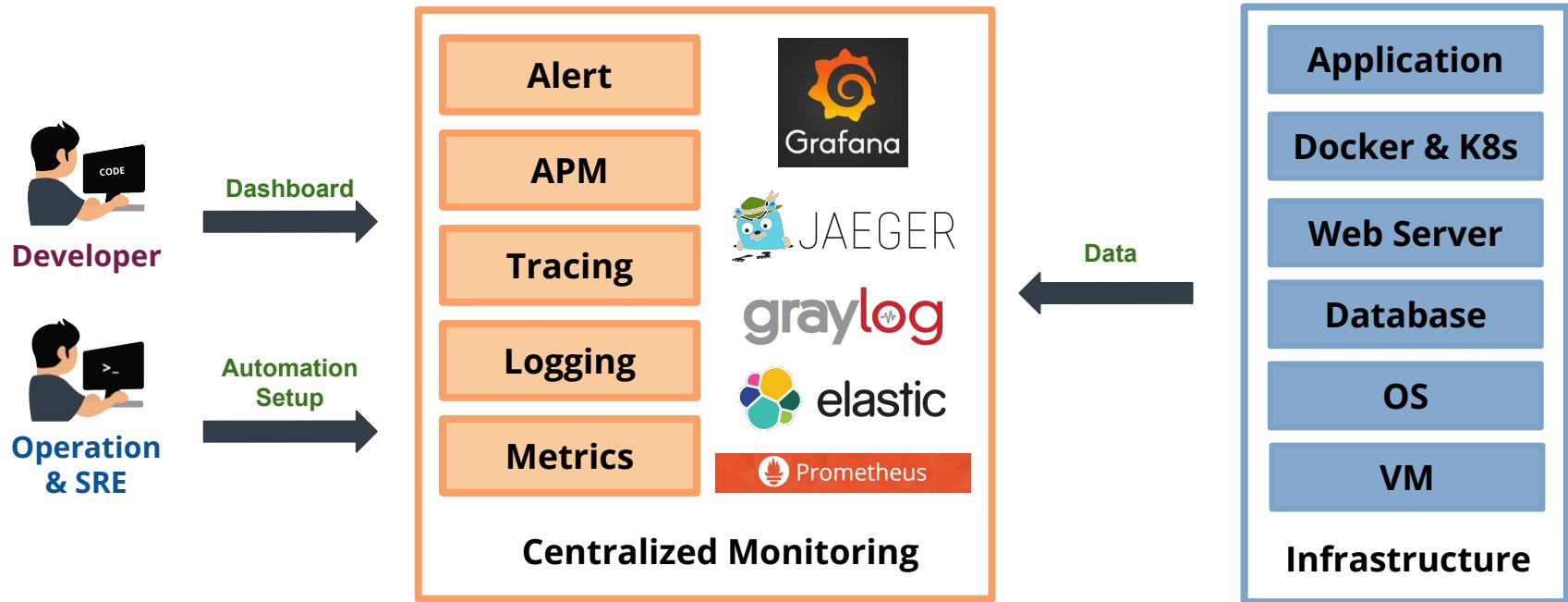
Standardized & Reused Pipeline



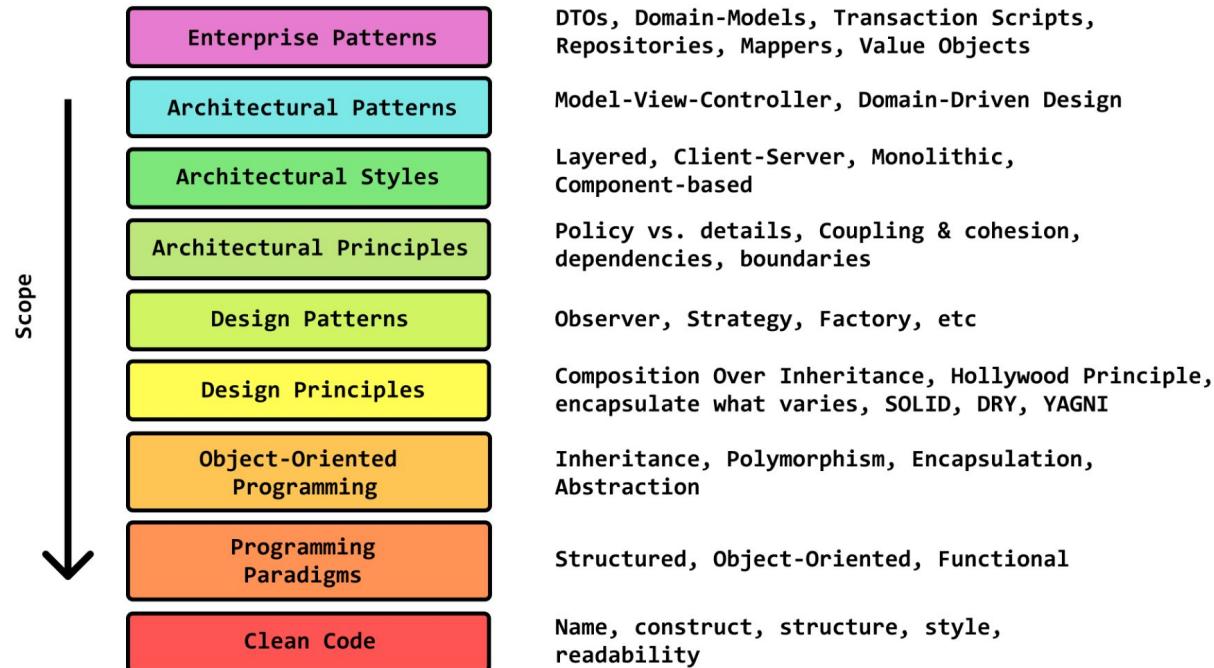
Secret Management



Observability



Development Reuse Pattern



Application Pattern



Documentation & How-to

- Twelve-Factor Guideline
- Secure Coding
- Coding Standard
- Standard Framework and Library
- Naming Convention
- Log Format

Platform Engineering Self-Service



Self-service interfaces

- High performance
 - CLI
 - APIs
 - GitOps
 - ChatOps
- **Composable into higher level workflows**

Components List & SSO

The screenshot shows the Opstella platform interface. At the top, there is a navigation bar with tabs: Services, Components (which is the active tab), and Users. On the far right of the header, there is a user profile icon with the letter 'D'.

The main content area is divided into two main sections:

- Services** (left sidebar):
 - Search bar: "Search Serv"
 - Pinned Services: vaccination
 - All Services: vaccination
- Components** (right sidebar):
 - Owner: 0 O 0 D 0 D
 - Components (3 Components):
 - web**: Endpoint: <https://pandora.vaccination-web.develop.opstella.in.th>, Latest update: 17/02/2022
 - backend**: Endpoint: <https://pandora.vaccination-backend.develop.opstella.in.th>, Latest update: 17/02/2022
 - gobackend**: Endpoint: <https://pandora.vaccination-gobackend.develop.opstella.in.th>, Latest update: 08/03/2022

Dashboard with Mirantis Lens IDE

The screenshot shows the Mirantis Lens IDE interface. On the left, there's a sidebar with a 'GOD' button, a cluster dropdown set to 'gke_opstella-dev_asia-southeast1...', and a navigation menu with 'Nodes' selected. The main area is titled 'Nodes' and shows a table with 6 items. The table columns are: Name, CPU, Memory, Disk, Tai..., Roles, Version, Age, Conditions, and three vertical dots. Each row represents a node named 'gke-opstella-production-' followed by a short ID. The 'Conditions' column shows all nodes as 'Ready'. The 'Age' column shows all nodes as '52m'. The 'Disk' column has yellow progress bars indicating usage.

Name	CPU	Memory	Disk	Tai...	Roles	Version	Age	Conditions	⋮
gke-opstella-production-				0		v1.21.5-gke...	52m	Ready	⋮
gke-opstella-production-				0		v1.21.5-gke...	52m	Ready	⋮
gke-opstella-production-				0		v1.21.5-gke...	52m	Ready	⋮
gke-opstella-production-				0		v1.21.5-gke...	52m	Ready	⋮
gke-opstella-production-				0		v1.21.5-gke...	52m	Ready	⋮
gke-opstella-production-				0		v1.21.5-gke...	52m	Ready	⋮

CI/CD Pipeline with GitLab CI

The screenshot shows the GitLab web interface for a project named "web". The left sidebar is open, showing various project management sections like Project information, Repository, Issues, Merge requests, CI/CD, Pipelines (which is selected), Editor, Jobs, Schedules, Security & Compliance, Deployments, Monitor, Infrastructure, Packages & Registries, Analytics, Wiki, and Snippets. The main content area displays a pipeline run titled "Pipeline #177 triggered 10 hours ago by opstella opstella". The status is "passed". Below this, there's a section titled "Update .gitlab-ci.yml" which lists "4 jobs for develop in 3 minutes and 49 seconds (queued for 29 seconds)". A "latest" button is shown next to a commit hash "722b7e08". A note says "No related merge requests found." At the bottom, there's a summary table for the pipeline:

Needs	Jobs	Tests
1	4	0

Below the table, there are three tabs: Security, Build, and Deploy. Under Security, there's a job for "sonar-code-scan" which has passed. Under Build, there's a job for "build:kaniko" which has also passed. Under Deploy, there's a job for "deploy" which has passed.

AST with Sonarqube

The screenshot shows the Sonarqube web interface for the 'sonarqube' project. The top navigation bar includes links for Projects, Issues, Rules, Quality Profiles, and Quality Gates. A search bar and a 'DD' button are also present.

The main content area has tabs for Overview, Issues, Security Hotspots, Measures, Code, and Activity. The Overview tab is selected.

QUALITY GATE STATUS:
Some Quality Gate conditions on New Code were triggered because of the small number of New Lines.
Passed
All conditions passed.

MEASURES

Measure	Status	Score
New Code	Since February 17, 2022 Started 20 days ago	Reliability A
New Bugs	0	
New Vulnerabilities	0	Security A
New Security Hotspots	0	Security Review A
Added Debt	0	Maintainability A
New Code Smells	0	

ACTIVITY

Issues: 2 new code

Bugs: 0

Code Smells: 0

Vulnerabilities: 0

Coverage: 0.0% (Coverage on 1 New Lines to cover)

Duplications: 0.0% (Duplications on 2 New Lines)

Activity timeline from Sat 19 to Sat 05:

- March 8, 2022, 11:30 PM: Quality Gate Passed (not provided)
- March 8, 2022, 8:38 PM: Quality Gate Passed
- February 17, 2022, 2:52 PM: Quality Gate Failed

SonarQube™ technology is powered by SonarSource SA
Community Edition - Version 8.9.6 (build 50800) - LGPLv3 - Community - Documentation - Plugins - Web API - About

Container Registry with Harbor

The screenshot shows the Harbor Container Registry interface. At the top, there is a navigation bar with the Harbor logo, a search bar containing "Search Harbor...", a language selector for English, and a user dropdown for "dev1". Below the navigation bar, the main title "Projects" is displayed, along with summary statistics: 3 PRIVATE PROJECTS and 1 PUBLIC PROJECT, and 3 PRIVATE REPOSITORIES and 0 PUBLIC REPOSITORIES. There are buttons for "+ NEW PROJECT" and "X DELETE". A filter dropdown shows "All Projects" and a search bar. The main content area is a table listing five projects:

<input type="checkbox"/>	Project Name	Access Level	Role	Type	Repositories Count	Chart Count	Creation Time
<input type="checkbox"/>	library	Public	-	Project			11/22/21, 4:36 PM
<input type="checkbox"/>	pandora-[REDACTED]vaccination-backend	Private	Project Admin	Project	1		2/17/22, 11:55 AM
<input type="checkbox"/>	pandora-[REDACTED]vaccination-gobackend	Private	Project Admin	Project	1		3/8/22, 10:20 PM
<input type="checkbox"/>	pandora-[REDACTED]vaccination-web	Private	Project Admin	Project	1		2/17/22, 11:14 AM

At the bottom right of the table, there are pagination controls for "Page size" (set to 15) and "1 - 4 of 4 items".

Container Image Scan with Trivy

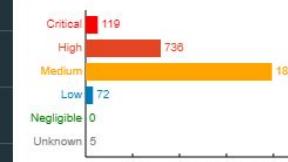
Harbor Search Harbor... English dev1 Projects Logs web Info Artifacts SCAN ACTIONS ▾

Projects < pandora/vaccination-web

web

Artifacts	Pull Command	Tags	Size	Vulnerabilities	Annotations	Labels	Push Time
sha256:f4738d5c	develop-	398.49MB	C 2758 Total - 12 Fixable	3/8/22, 11:26 PM			
sha256:9b2b6783	latest	398.50MB	C 2758 Total - 12 Fixable				
sha256:9d34f406	master-9	398.50MB	C 2758 Total - 12 Fixable				
sha256:6d757e44		398.50MB	C 2758 Total - 12 Fixable				
sha256:d3f7889c	master-0	398.50MB	C 2758 Total - 12 Fixable				
sha256:ad45718a	develop-	398.50MB	C 2758 Total - 12 Fixable				
sha256:430a2ee9	develop-	398.50MB	C 2758 Total - 12 Fixable	3/8/22, 8:39 PM			

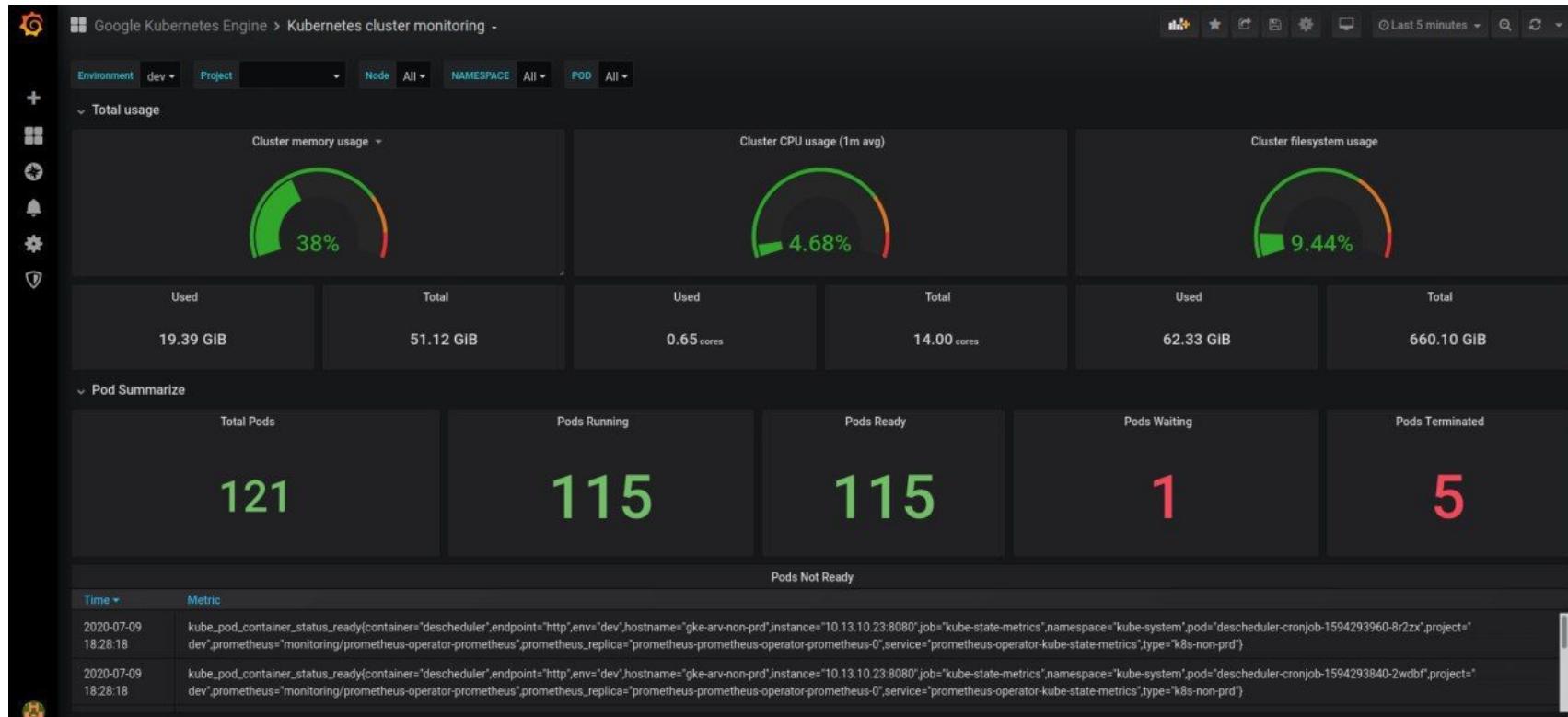
Vulnerability Severity: Critical



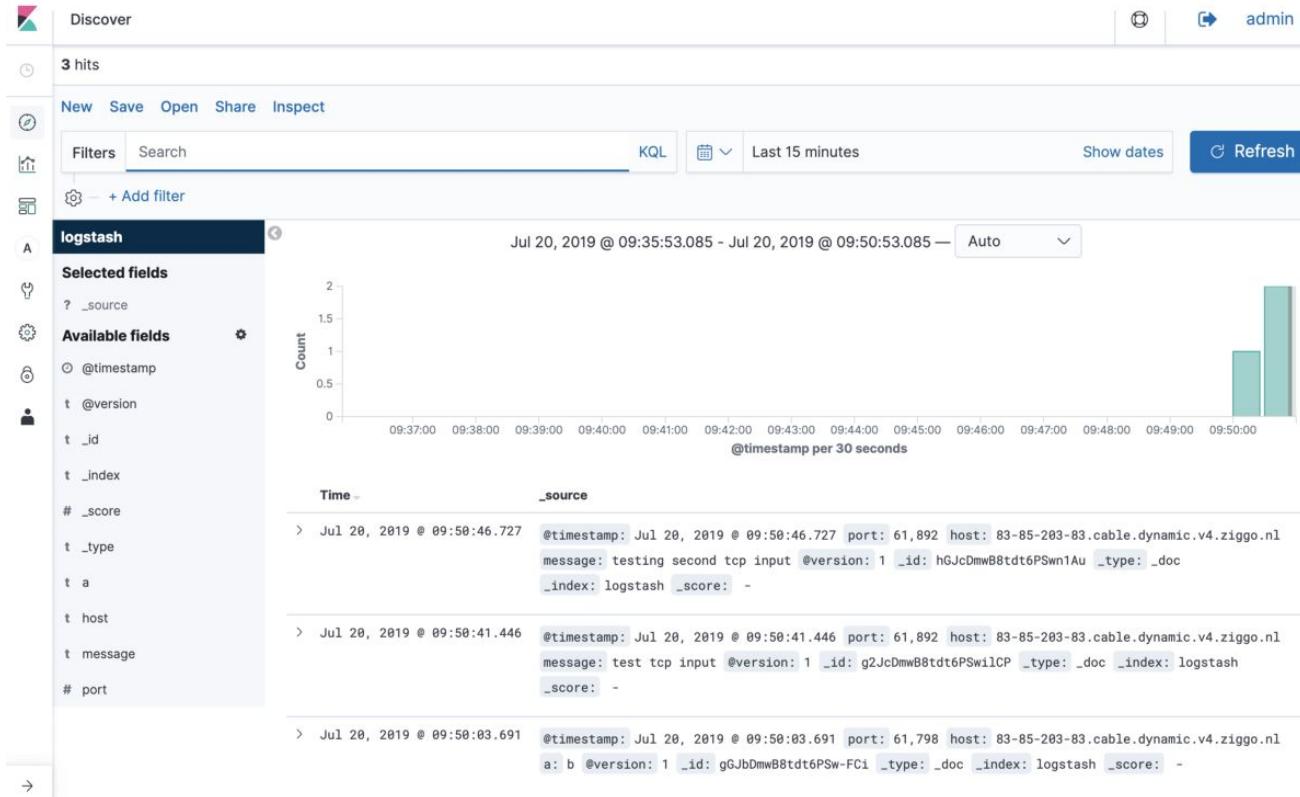
Severity	Count
Critical	119
High	738
Medium	1826
Low	72
Negligible	0
Unknown	5

Scanned by: Trivy@v0.16.0
Duration: 15 sec
Scan completed time: 3/8/22, 11:36 PM

Grafana Integration



OpenSearch Integration



Performance Load Testing

 LOCUST

HOST
https://pandora-vaccination-gobackend.develop.opstela.in.th

STATUS STOPPING
New test

WORKERS 160 RPS 52935.1 FAILURES 0%

Statistics											
Type	Name	# Requests	# Fails	Median (ms)	90%ile (ms)	Average (ms)	Min (ms)	Max (ms)	Average size (bytes)	Current RPS	Current Failures/s
POST	/	1763416	0	7	13	9	2	255	51	52935.2	0
Aggregated		1763416	0	7	13	9	2	255	51	52935.1	0

Demo



Q&A



More questions?



jirayut@opsta.co.th

Jirayut Nimsaeng
CEO & Founder
Opsta (Thailand)
086-069-4042



Facebook