SGTS Product Overview

A Product of GDS, GovTech

Singapore Government
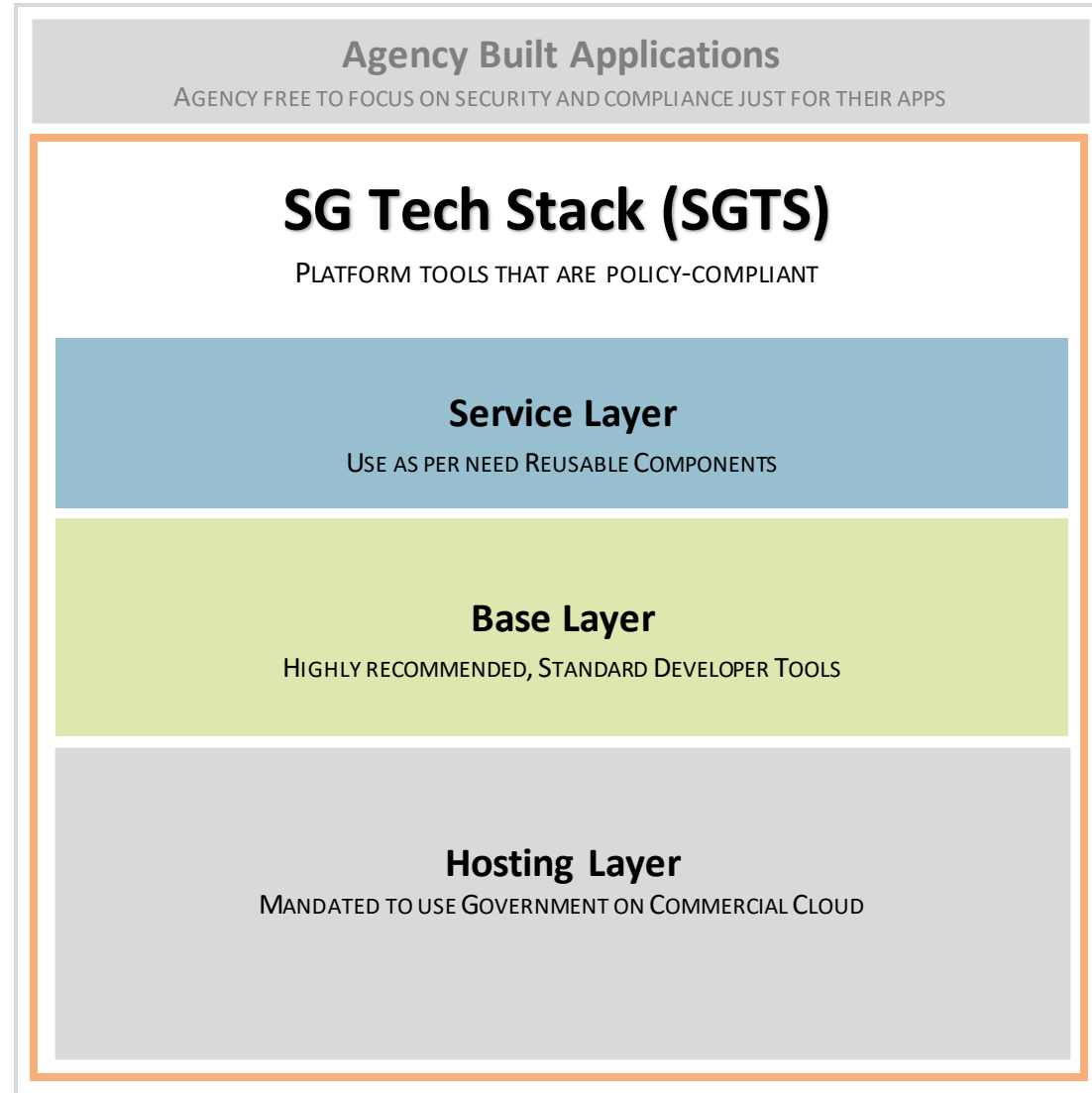# Tech Stack (SGTS)

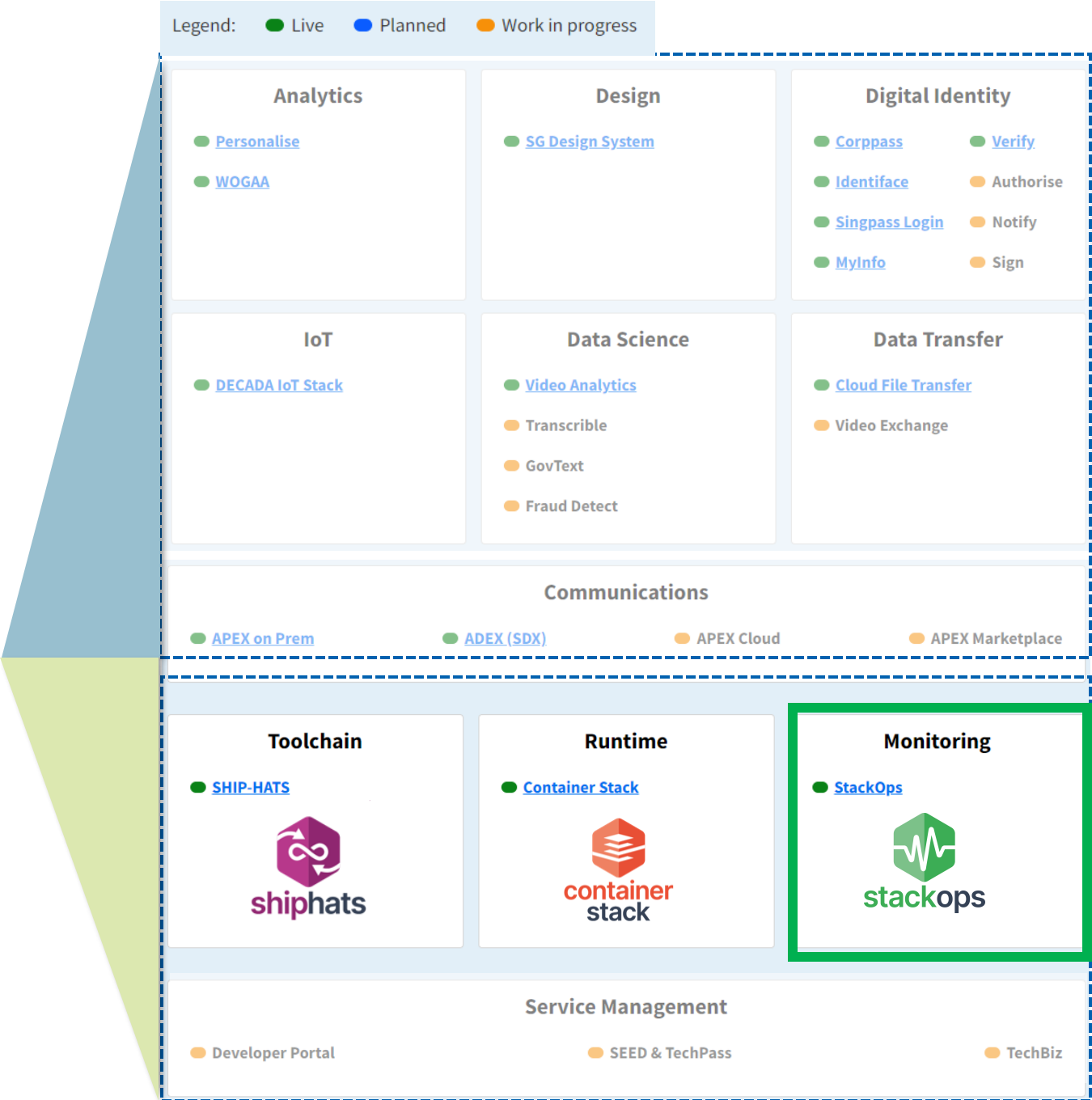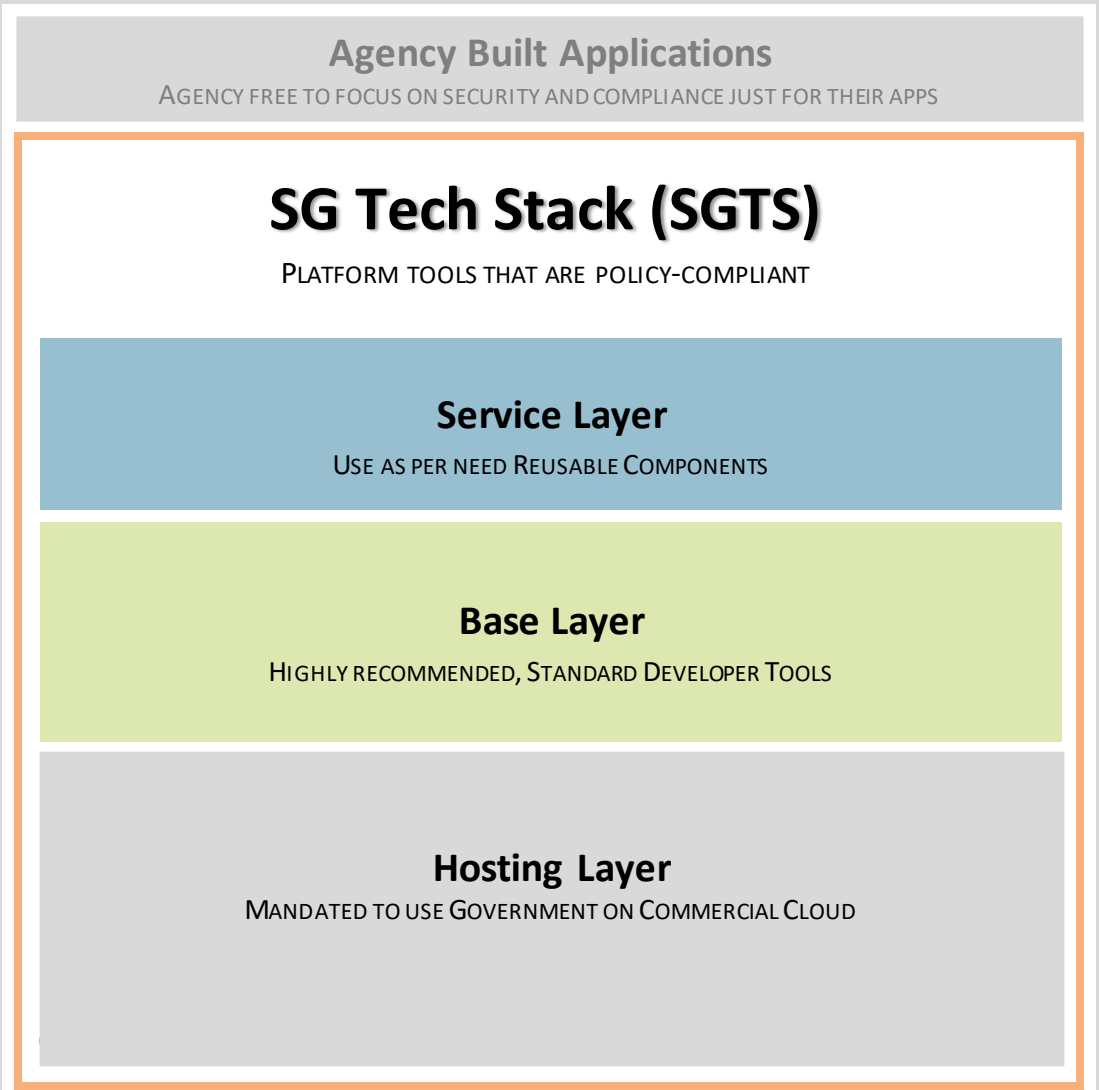**stackops**

Say Hello to
SGTS

Agency Built Applications
AGENCY FREE TO FOCUS ON SECURITY AND COMPLIANCE JUST FOR THEIR APPS

SG Tech Stack (SGTS)
PLATFORM TOOLS THAT ARE POLICY-COMPLIANT

Service Layer
USE AS PER NEED REUSABLE COMPONENTS

Base Layer
HIGHLY RECOMMENDED, STANDARD DEVELOPER TOOLS

Hosting Layer
MANDATED TO USE GOVERNMENT ON COMMERCIAL CLOUD

GOVTECH SINGAPORE

SGTS - Unpacked

Agency Built Applications
AGENCY FREE TO FOCUS ON SECURITY AND COMPLIANCE JUST FOR THEIR APPS

SG Tech Stack (SGTS)
PLATFORM TOOLS THAT ARE POLICY-COMPLIANT

Service Layer
USE AS PER NEED REUSABLE COMPONENTS

Base Layer
HIGHLY RECOMMENDED, STANDARD DEVELOPER TOOLS

Hosting Layer
MANDATED TO USE GOVERNMENT ON COMMERCIAL CLOUD

Legend: ● Live ● Planned ● Work in progress

Analytics
- ● Personalise
- ● WOGAA

Design
- ● SG Design System

Digital Identity
- ● Corppass
- ● Identiface
- ● Singpass Login
- ● MyInfo
- ● Verify
- ● Authorise
- ● Notify
- ● Sign

IoT
- ● DECADA IoT Stack

Data Science
- ● Video Analytics
- ● Transcrible
- ● GovText
- ● Fraud Detect

Data Transfer
- ● Cloud File Transfer
- ● Video Exchange

Communications
- ● APEX on Prem
- ● ADEX (SDX)
- ● APEX Cloud
- ● APEX Marketplace

Toolchain
- ● SHIP-HATS

shiphats

Runtime
- ● Container Stack

container stack

Monitoring
- ● StackOps

stackops

Service Management
- ● Developer Portal
- ● SEED & TechPass
- ● TechBiz

Benefits to
SGTS

Engineers

Access to templates, and self-service capabilities with **automated** infrastructure operations that are IM-compliant, to **reduce cognitive workload** on engineers.

PMs, Leads & CIOs

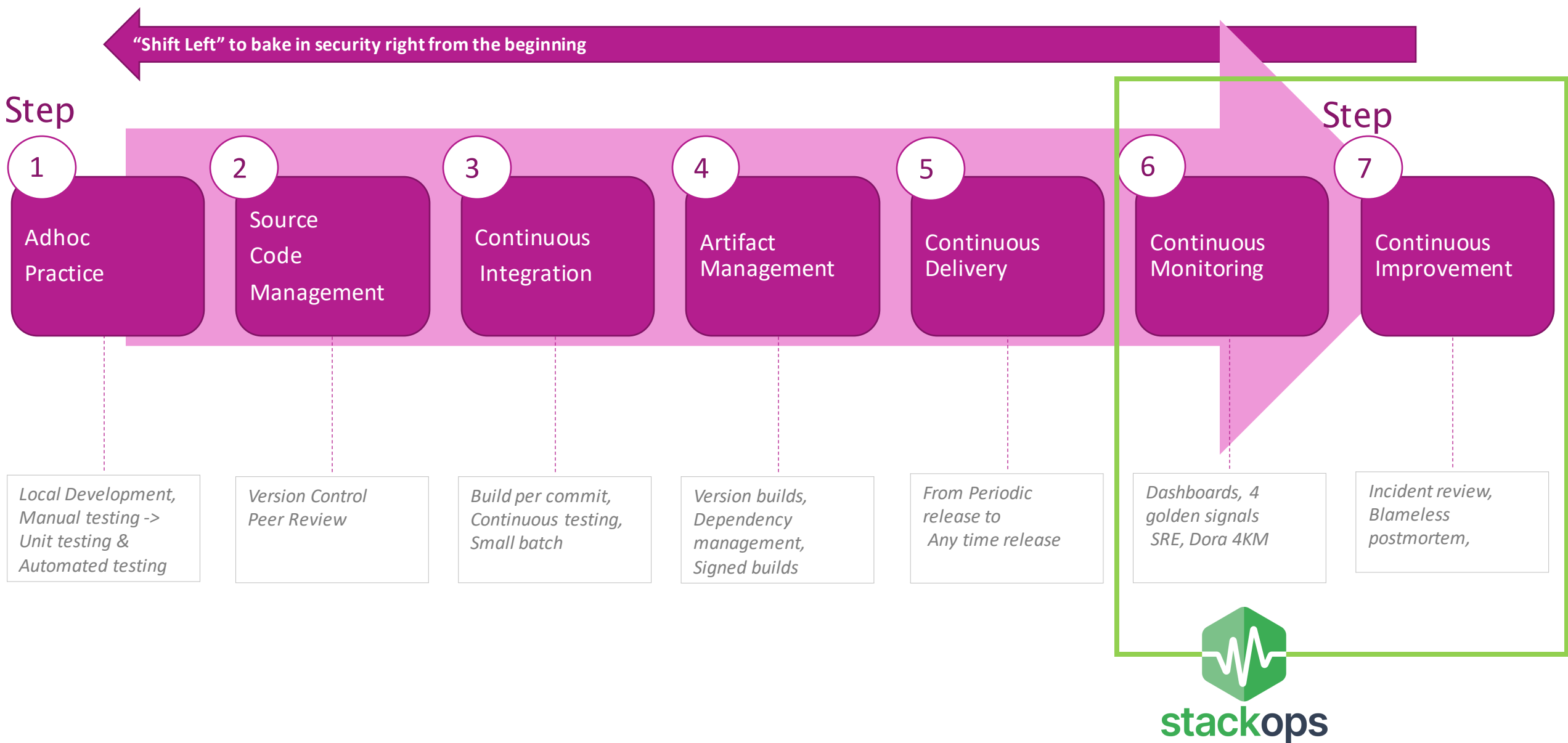**Increased transparency** into the development process, and greater operational insights

Agencies

Levelling up of DevSecOps maturity within agencies and across the government

Vendor Partners

Enhanced capabilities ready to partner various government agencies deliver apps using SGTS

GOVTECH
SINGAPORE

DevSecOps Maturity Model for Agencies

"Shift Left" to bake in security right from the beginning

Step

1 Adhoc Practice

2 Source Code Management

3 Continuous Integration

4 Artifact Management

5 Continuous Delivery

6 Continuous Monitoring

Step

7 Continuous Improvement

Local Development, Manual testing -> Unit testing & Automated testing

Version Control Peer Review

Build per commit, Continuous testing, Small batch

Version builds, Dependency management, Signed builds

From Periodic release to Any time release

Dashboards, 4 golden signals SRE, Dora 4KM

Incident review, Blameless postmortem,

stackops

Introducing StackOps

Product Vision

To be the service for WOG to embrace **Site Reliability Engineering** with **Automated** and **Easy-to-use** monitoring service which provides the user with the flexibility to monitor and track application output.

What is StackOps?

Monitoring tool for WOG to improve **observability** and embrace **Site Reliability Engineering**

- ✓ Provides **visibility across** your cloud **applications** and **infrastructure**.

- ✓ Monitors **all the components in your product** with a single agent and easy to use integrations

- ✓ **Aggregates, correlates** and visualizes all **operational data**

- ✓ Multi tenanted tool that can support multiple CSPs

- ✓ Shares data across products to have a **Central Log Monitoring solution for a division/agency**.

- ✓ Tool that comes with a Built-in **SIEM** and we are building a community around WOG to share SIEM rules
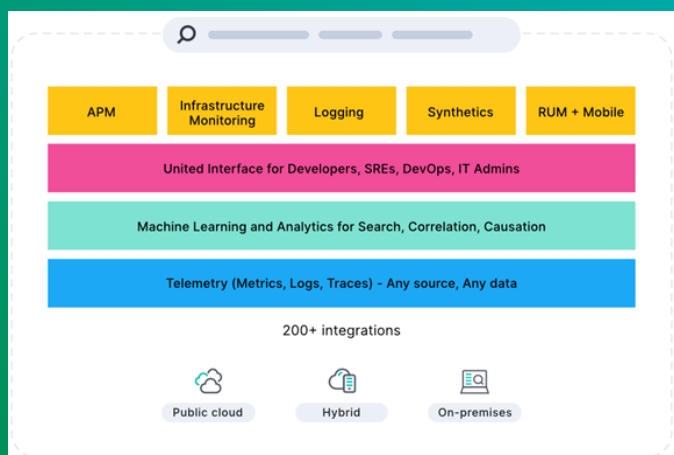
Who should use StackOps?

- For all **Agency Systems that are Restricted and below**
- Users can be **Public officers or Vendors**
  - L1 Ops
  - Central IT Team
  - Developers
  - SRE Team
  - Managers, CIOs
- Subscription **by Agencies**

Key Features

Metrics Monitoring

- Use prebuild dashboards to monitor metrics data coming from different sources
- Integrations that cover wide range of hosts and workloads.

Log & Trace Monitoring

- Queries over View logs with thresholds and set alerts.
- Alert configurations can be integrated with tools like Slack, Telegram etc.

Application Performance Monitoring

- Advance Application performance monitor to understand the service behavior.
- Effective visualization of the service dependencies and latencies.

SIEM

- Comes with security monitoring features built in as well.
- Configurable by tenants according to the usecase.

Support cross CSP ingestion and correlation

- Support cross CSP ingestion and correlation

Why choose StackOps?

1 To improve observability across your application and improve DevSecOps maturity model using a **solution built for the Government**

2 To have a central monitoring solution **across the division/agency** and to reduce silos

3 To **leverage pre-built templates** for different personas like L1 Ops, CIO, TechOps, System Owners etc

4 To have an **inner sourced collection of SIEM rules** to monitor various Cloud services you use.

StackOps Value-Added Features

Observability	• Single tool for monitoring (Infra, Application, Network etc.) • Pre defined templates for different personas(*) • Central IT Ops functionality for Central IT teams
Security / Compliance	• Built-in SIEM • Community of WOG users (inner sourced model) • Log sharing between various existing Monitoring tools (*)
Add-Ons	• Unified product experience as other SGTS products (Onboarding via Techbiz) • Overhead of Procurement is taken away from tenants • Monitoring of monitoring clusters handled by product team

(*) Features are not readily available. WIP

Cloud Native vs StackOps

	Cloud Native Tools (AWS)	StackOps
Logging lifecycle management	Limited	Multi-phase self-define
SIEM	-	Fleet
Service Journey Metrics/UX Metrics	-	Built-in
Data locality in CSP	AWS Only	Yes
Built in dashboards	Limited	Very extensive
Central visibility	No	Yes
Consumer service integration	PromQuery + AWS API per account	KQL+API centralized
Golden Signal SLI/SLO creation	Manual CW API	Built-in
Abnormally detection	-	Built-in
Agent Management	Multiple node exporters	Single fleet agent
Log transformation	-	Logstash
Agent Lifecycle	Manual	Centralized automation

StackOps Product Roadmap

Goal: re-defined and customizable dashboards for early observation and anomaly detection of application performance, to support SRE

Component	FY' 23 - Q1	FY' 23 -Q2	FY' 23 -Q3	FY' 23 -Q4
Security / Compliance	Using built-in SIEM for compliance.	SIEM inner sourcing Framework	Logs sharing between platforms GDS – Security Dashboard	
Observability	SGTS Dashboard POC with Monthly report	Visualization framework	Prebuilt Dashboards – L1 Ops	Prebuilt Dashboards – Security, L1 Support team setup
Integration	Techbiz Integration	Techbiz Integration	Configuration management interface	
Platform Ops	Elastic Cloud GA	Baseline configuration	Ops/Support team with new Service desk (JIRA)	
Continuous Activities	Customer onboarding/enablement/support Internal product improvement (Data definition, SHIP 2.0 migration, Log forwarding etc)			

Pilot Use Cases

LifeSG

- Logs from DB & App is ingested to StackOps.
- Alerting via Kibana
- On Prod & Dev environment

Government on Commercial Cloud

- Monitoring team extracts and aggregates from various data sources and monitor alerts
- Dev team access the data for next level investigation or troubleshooting

HOUSING & DEVELOPMENT BOARD

- Renovation system on Trial phase
- Will be onboarding all the apps once GCC2.0 migration is complete

Pilot Use Cases - SGTS

stackops

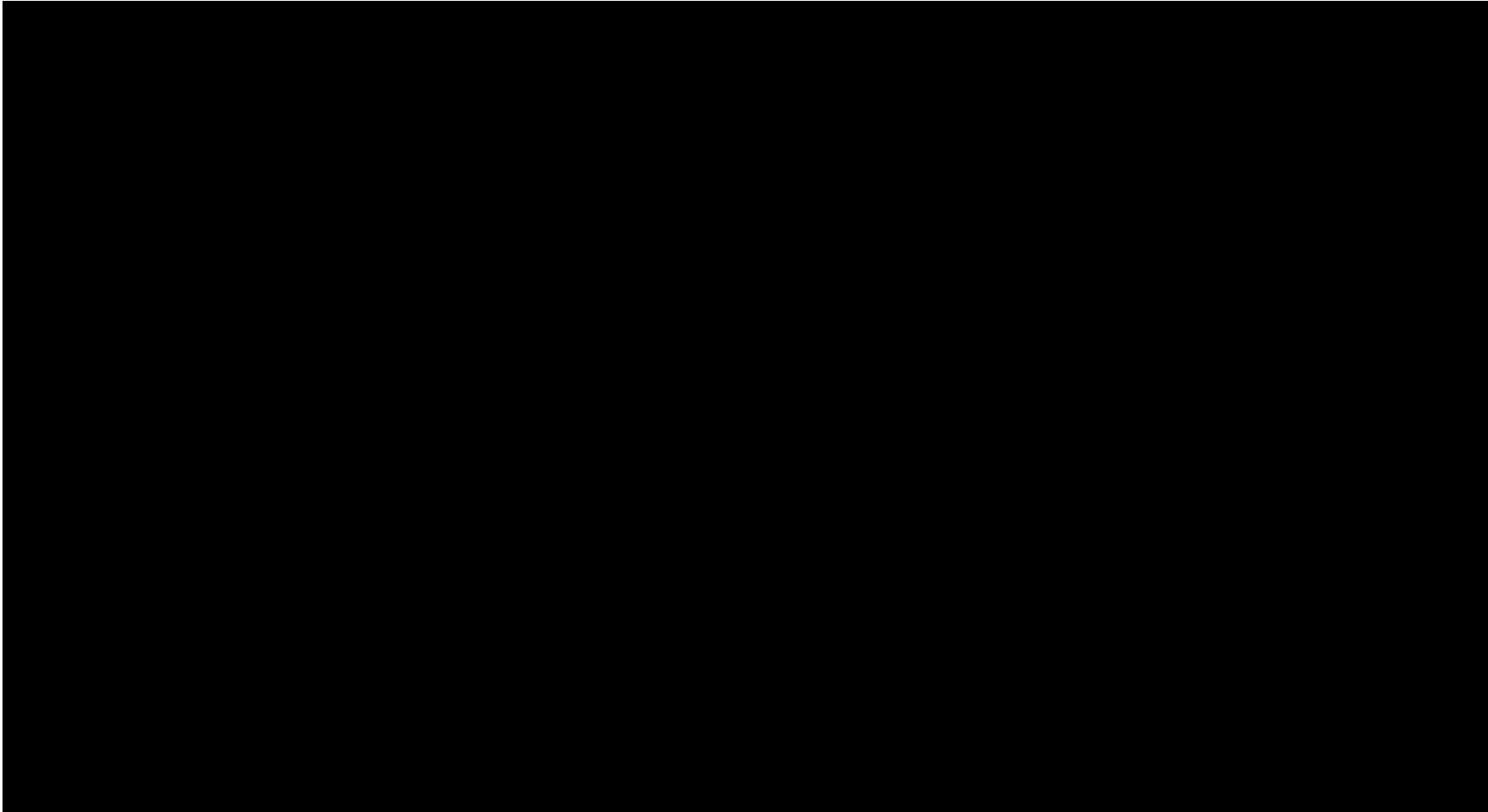containerstack

techpass

techbiz
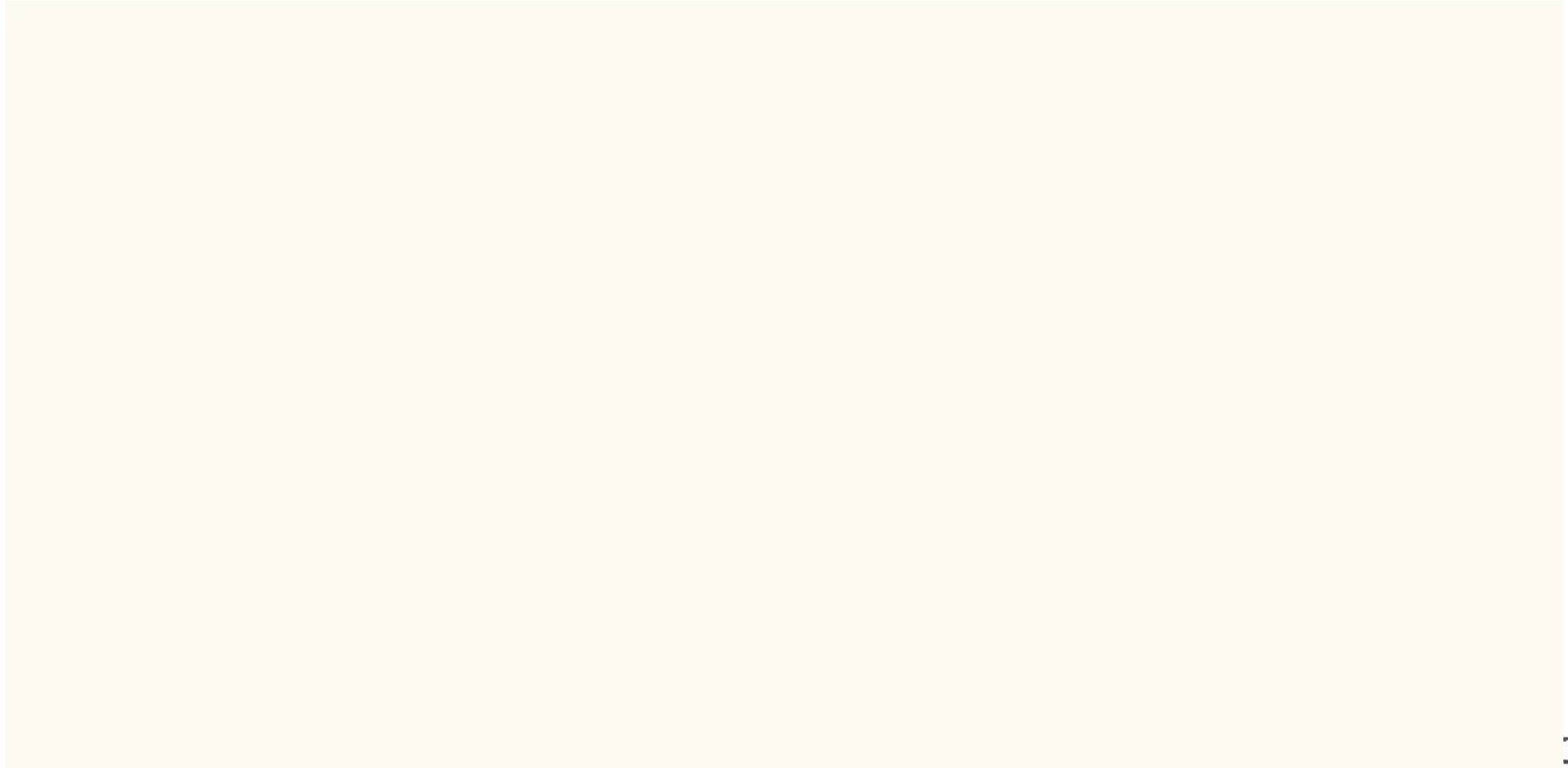
apex

SEED

GOVTECH
SINGAPORE

Central Dashboard POC

- https://gvt-gds-stackops-stackops-prod.kb.ap-southeast-1.aws.found.io/app/dashboards#/view/ec197dc0-75d9-11ed-932b-75d372f4cc72?_g=(filters:!())

Example: Using StackOps to monitor SEED SLA/SLOs and Usage Patterns

Example: Using StackOps to monitor APEX Usage

![stackops logo]

StackOps Community Group

Join your colleagues across WOG who are also using StackOps

SCAN ME

GOVTECH
SINGAPORE