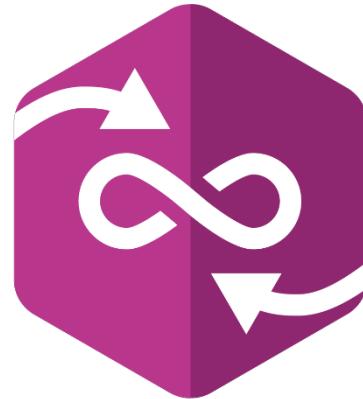


GOVTECH
SINGAPORE

SGTS Product Overview



shiphats

A Product of GDS, GovTech

Agenda

- SAY HELLO TO THE SINGAPORE GOVERNMENT TECH STACK (SGTS)
- INTRODUCING **SHIP-HATS: AN SGTS PRODUCT**
 - UNDER-THE-HOOD
 - BENEFITS
 - TECHNICAL OVERVIEW
- HOW TO GET STARTED
 - SELF LEARN WITH TECH DOCS
 - WORKSHOPS & WEBINARS
 - SUBSCRIPTION MODEL
- WHAT'S NEXT?

Singapore Government Tech Stack (SGTS)



Say Hello to

SGTS

A set of **central platform tools** that streamlines and **simplifies the development and monitoring process** and enables code reuse across WOG to build and monitor secure, high quality applications.

#platformengineering

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

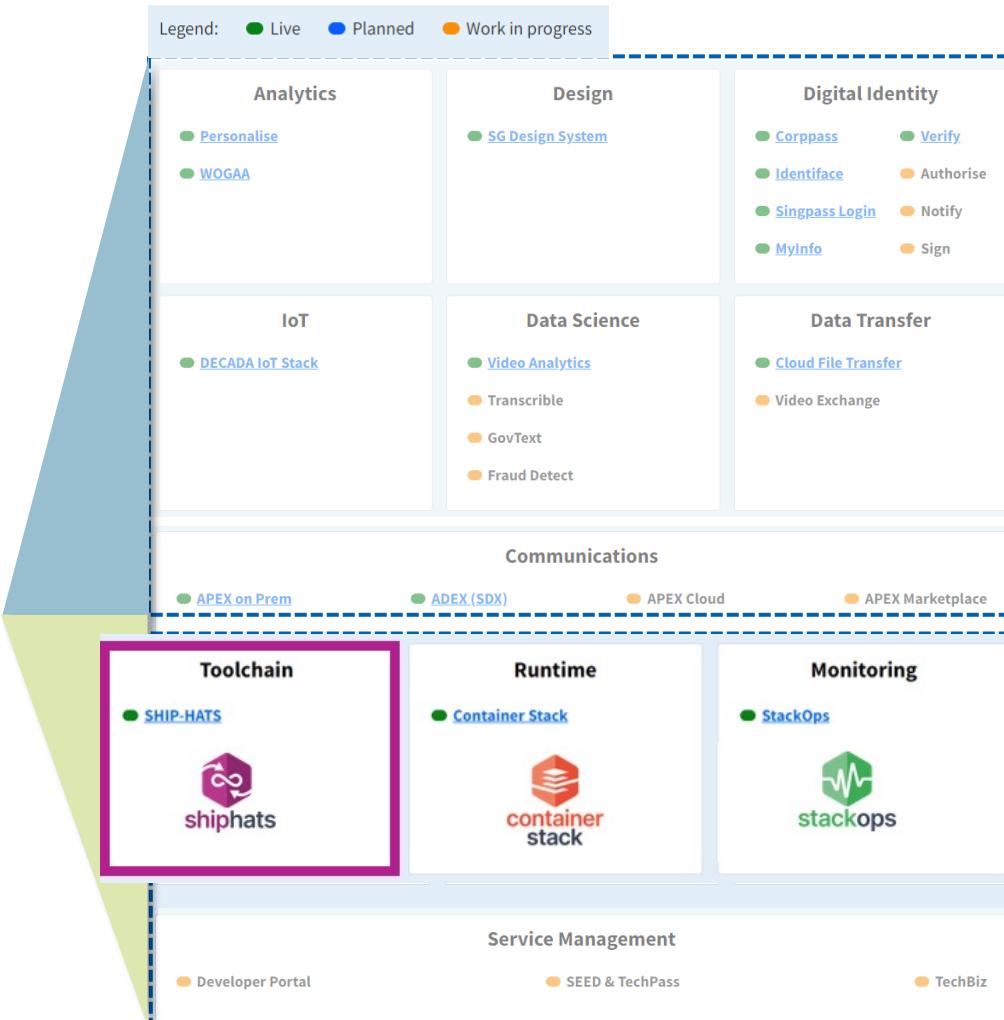
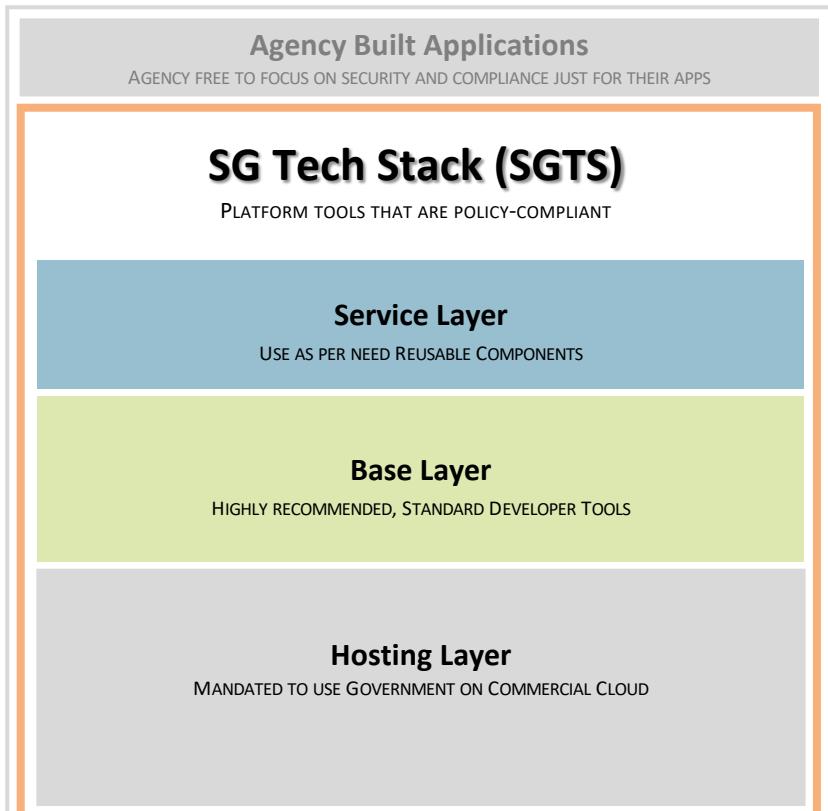
Base Layer

HIGHLY RECOMMENDED, STANDARD DEVELOPER TOOLS

Hosting Layer

MANDATED TO USE GOVERNMENT ON COMMERCIAL CLOUD

SGTS - Unpacked



Benefits of SGTS



Engineers

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



PMs/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 to deliver apps using SGTS

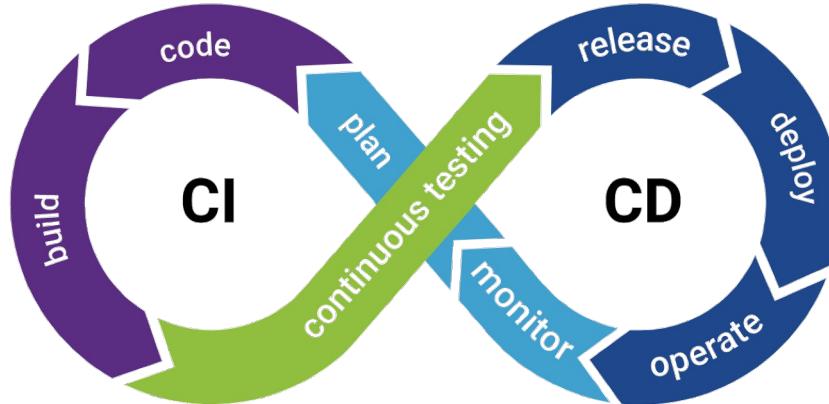
SHIP-HATS

An SGTS Product



What is SHIP-HATS

An **end-to-end Source Code Management and Continuous Integration/Continuous Delivery (CI/CD)** toolchain with security and governance guardrails for developers to build, test, and deploy code to production.



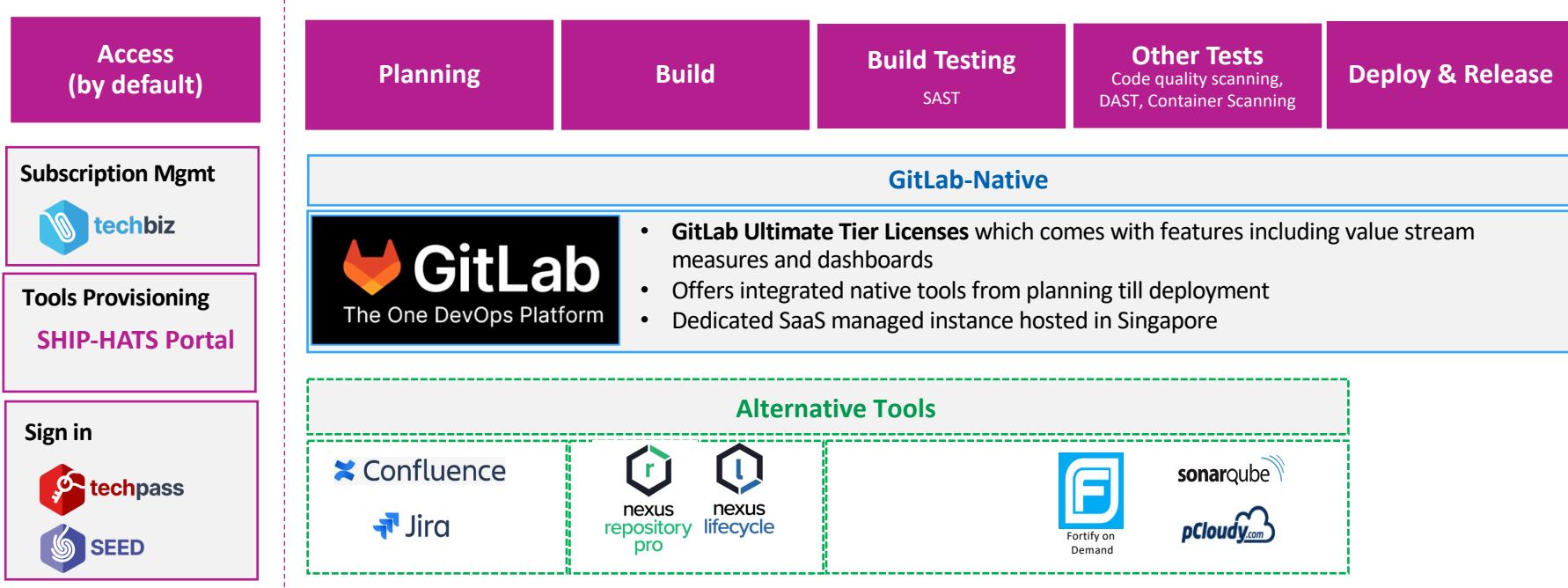
CI/CD pipelines automate incremental code changes to be delivered quickly and reliably to production

Who should use
SHIP-HATS

- For all **Agency Systems that are Cloud Confidential (Eligible) and below**
- **Mandatory for GovTech-owned systems**
- Users can be **Public officers or Vendors**
- Subscription **by Agencies**

SHIP-HATS 2.0. Product Offering

Tools under-the-hood



TOOL SELECTION

Agencies must assess whether Gitlab native is sufficient (e.g. whether the gitlab-native tool supports the language/framework used etc).

1

GitLab Native only

- ✓ Lean teams
- ✓ Simple use cases
- ✓ New Projects
- ✓ Value for \$\$

2

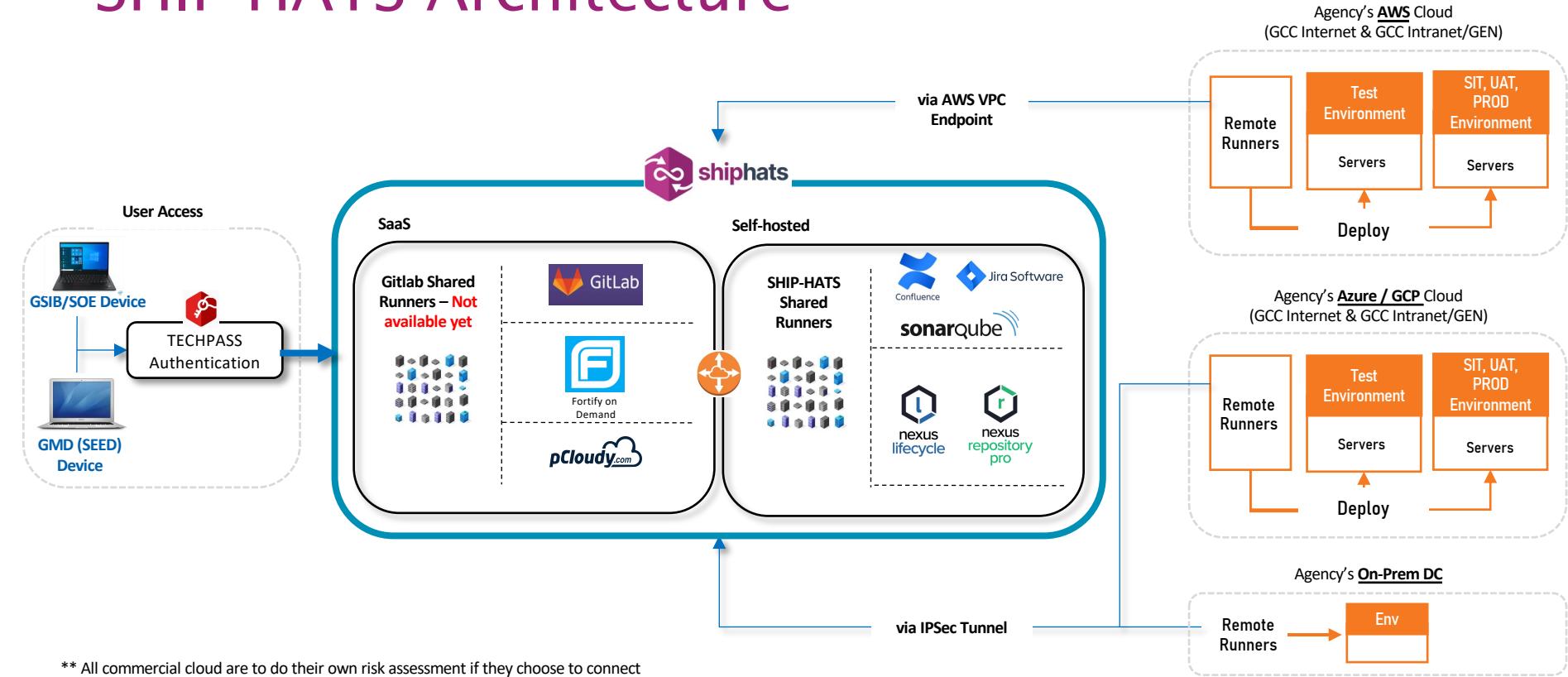
GitLab & Alternative tools

- ✓ Already on alternative tools
- ✓ Complex use cases

- ❖ Both options meet **Security** Policy needs
- ❖ Alternative tools are available as add-on anytime

[Tool comparison available on DevPortal](#)

SHIP-HATS Architecture



13 Copyright of GovTech © Not to be reproduced unless with explicit consent by GovTech.

Benefits of SHIP-HATS



#SHIPHATSforAgencies

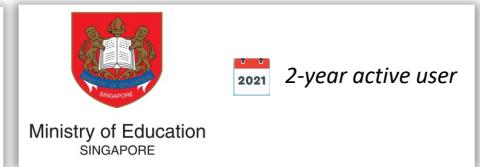


50 Agencies use SHIP-HATS

300+ Agency Systems

Over 3K Active User

50+ Pipeline Templates offered



Why choose SHIP-HATS?

1

Faster time to market

- ✓ In-built compliance and best practices through centralized
- ✓ Templates and tools for all users
- ✓ No procurement overheads to get started

2

Security for Public Sector Needs

- ✓ CI/CD platform complies to security needs
- ✓ SaaS benefits for Confi-Cloud (Eligible) Systems as dedicated instance is hosted in Singapore

3

WoG Collaboration

- ✓ Common repo of images for reuse
- ✓ Contribute to templates
- ✓ Learn faster and replicate learnings across WOG

4

Metrics & Data for DevSecOps

- ✓ GitLab Dashboards: Security, DORA metrics, DevOps Adoption, Value Stream Analytics
- ✓ Greater transparency and reduces system reporting overheads

Value-Added Features



SHIP-HATS 2.0. Value-Added Features

As a subscriber, agencies will also have access to the following:

- Platform Enablement Features
- CI/CD Tools and Features
- Security Baseline & Testing Tools
- Metrics and Value Stream Measurements (VSM)

Platform- Enablement e.g. Runners

Option 1: SHIP-HATS Shared Runners

- Hosted by SHIP-HATS team
- Created on-demand
- Available for all SHIP-HATS users at no additional costs
- No overheads for Agencies to maintain runners.
- 4 variants: **CStack, Docker, Windows** and GitLab Shared Runners

Option 2: Self-hosted Remote Runners

- Hosted by the agency
- Agencies to bear the costs of hosting their own runners
- Can be configured for Group or Project level access
- Full-control of the runners

CI/CD Tools & Features

e.g.
Pipeline Templates

- 1 **5 End-to-End Pipeline Templates**
Pipeline skeletons
- 2 **40~Modular Templates**
can be include as per need
- 3 **Reference Pipelines**
fully implemented pipeline samples
- 4 **Pipeline COE**
Reusable container images

5 End-to-End Pipeline Templates

Pipeline skeletons

Your project pipeline plan

End to End Pipeline Template

Your project specific variables



End to End Pipeline Templates from GovTech

Example Use Case:
.NET applications hosted in Azure App Service

**E** E2E Templates

Subgroup information

Epic

0

Issues

7

Merge requests

4

Security & Compliance

Packages & Registries

Analytics

Wiki

WOG > ... > E2E Templates

**E** E2E Templates ⚡

Group ID: 144 Request Access

Templates on
GitLab

Subgroups and projects

Shared projects

Archived projects

Search

> E Examples ⚡

 S SHIP-HATS Docker Image CI Pipeline Templates ⚡
Docker Image CI Pipeline Template 0 S SHIP-HATS Docker Multi Services App E2E Templates ⚡
Docker E2E Template 0 S SHIP-HATS Docker Single Service App E2E Templates ⚡
Dockerapp E2E Template 0

S SHIP-HATS Webapp E2E Templates ⚡ 0

```

1 include:
2   - local: BUILD.gitlab-ci.yml
3   - local: TEST.gitlab-ci.yml
4   - local: DEPLOY.gitlab-ci.yml
5   - project: "WOG/GVT/ship/ship-hats-templates"
6   ref: "main"
7   file:
8     - /templates/vars/.gitlab-ci-sonatype-vars.yml
9     - /templates/.gitlab-ci-publish-to-nexus.yml
10    - /templates/.gitlab-ci-check-app-readiness.yml
11    - /templates/.gitlab-ci-run-test.yml
12    - /templates/.gitlab-ci-create-report.yml
13
14 stages:
15   - build
16   - static-test
17   - deploy-to-testing-env
18   - runtime-test
19   - sign
20   - publish
21   - deploy-to-prod #to PROD
22
23 image: $NEXUSREPO_DOCKER_PROXY_HOSTNAME/alpine:latest
24
25 variables:
26   # app-specific variables
27   WORKING_DIR: "" # app for eg. relative path to application from project
28   OUTPUT_ARTEFACT: "" # "$WORKING_DIR/app.zip" for eg. compiled app to be scanned and uploaded
29   UNIT_TEST_REPORT: "" # "$WORKING_DIR" for eg. relative path to run unit testing
30   WEBAPP_URL: "" # URL to reach project web application
31   WEBAPP_NAME: "" # web application name that can be searched when service is up
32   VERSION: "" # version of web application to release to artefact repository.
33
34 # for e2e integration testing if robot framework is used
35 RF_TESTSCRIPT_FOLDER: "" # "$WORKING_DIR/test-automation/E2eTest/robotframework_testscripts"
36
37 # for dast (pen) testing in compliance framework
38 DAST_WEBSITE: $WEBAPP_URL # target URL to perform dast for web app in testing env
39 DAST_XML_REPORT: "dast-owasp-zap-report.xml" # DAST report that's viewable from your build's
40
41 # for sonarqube scan in compliance framework
42 # check out with SHIP-HATS team for account provisioning
43 # see README.md#provide-sensitive-variables for list of variables required to include ship-sc
44
45 # for nexus iq scan in compliance framework
46 # check out with SHIP-HATS team for account provisioning
47 # see README.md#provide-sensitive-variables for list of variables required to include ship-ne
48 SCAN_TARGETS: $OUTPUT_ARTEFACT # target to perform scan on
49
50 # for fod sast and fod dast in compliance framework
51 # check out with SHIP-HATS team for account provisioning
52 # see README.md#provide-sensitive-variables for list of variables required to include ship-fortify-sast-fod-with-report_and_ship-fortify-dast

```

Yaml for E2E

```

1 include:
2   - project: "WOG/GVT/ship/ship-hats-templates"
3   ref: "main"
4   file:
5     - /templates/vars/.gitlab-ci-sonatype-vars.yml
6
7 image: $NEXUSREPO_DOCKER_PROXY_HOSTNAME/alpine:latest
8
9 .build-webapp:
10   script:
11     - echo "implement building webapp here."
12
13 build-job: # do not change the name of this job, required by compliance
14   extends: .build-webapp
15   # artifacts:
16   #   when: always
17   #   paths:
18   #     - $OUTPUT_ARTEFACT # required by compliance
19

```

40~Modular Templates

can be include as per need

Your project pipeline plan

Your project specific scripts



Modular Testing Template

Modular Repo Template

Your project specific variables



Modular Templates from GovTech

Build & Release Templates

QA & Security Templates

Artifact Repository Templates



Modular Pipeline Templates

The screenshot shows a GitLab project interface. On the left, there's a sidebar with various project management options like Menu, Project information, Repository, Issues, Merge requests, Deployments, Packages & Registries, Monitor, Analytics, Wiki, and Snippets. The main area displays a table of CI templates:

Name	Last commit
vars	Update links from...
.gitlab-ci-aquasec-trivy-scan.yml	Fixes to readme
.gitlab-ci-aws.yml	add entrypoint to...
.gitlab-ci-azure.yml	Update .gitlab-ci-azure.yml
.gitlab-ci-blob-signing.yml	update documentation
.gitlab-ci-check-app-readiness.yml	Include .docker-services job in Readiness-Check-For-Doc...
.gitlab-ci-checksum-verify.yml	Fixes #100 on Container Checksum Template
.gitlab-ci-common.yml	Closes #72 Release management
.gitlab-ci-container-signing.yml	[Change Log] Touch up README
.gitlab-ci-create-fod-report.yml	add nexus proxy
.gitlab-ci-create-report.yml	Reorg readme and add contributing notes.
.gitlab-ci-docker-delete.yml	Add templates for #82 to delete images from GitLab Con...
.gitlab-ci-docker-push.yml	Fixes #101 Nexus Repo Content Selector in examples

Below this, a specific template named `BUILD.gitlab-ci.yml` is shown in its entirety:

```
1 include:
2   - project: "WOG/GVT/ship/ship-hats-templates"
3     ref: "main"
4   file:
5     - /templates/vars/.gitlab-ci-sonatype-vars.yml
6
7 image: $NEXUSREPO_DOCKER_PROXY_HOSTNAME/alpine:latest
8
9 .build-webapp:
10   script:
11     - echo "implement building webapp here."
```

Templates
on GitLab

The screenshot shows a pipeline configuration file named `.gitlab-ci-publish-to-nexus.yml`:

```
1 include:
2   - local: "/templates/vars/.gitlab-ci-sonatype-vars.yml"
3   - local: "/templates/.gitlab-ci-nexus-configure.yml"
4   - local: "/templates/.gitlab-ci-common.yml"
5
6 # Include these variables in your .gitlab-ci.yml
7 # i.e.
8 # variables:
9 #   MAVEN_SETTINGS_SERVER_ID: "test-demo-releases"
10 #   NEXUSREPO_REPO_ID: "test"
11 #   NEXUSREPO_REPO_GROUP_ID: "com.gt.shiphats.demo"
12 #   MVN_SETTINGS_FILE: "./settings.xml"
13 #   ARTEFACT: "./target/demo-0.0.1.jar"
14 #   ARTEFACT_ID: "demo"
15 #   ARTEFACT_VERSION: "0.0.1"
16 #   ARTEFACT_PACKAGE: "jar"
17
18 .publish-maven-artefact:
19   image: $NEXUSREPO_DOCKER_PROXY_HOSTNAME/maven:latest
20   tags:
21     - non_privileged
22     - no_root
23     - cstack
24   script:
25     - export VARIABLE_NAME=MVN_SETTINGS_FILE
26     - !reference [.check-variable-sh, script]
27     - export VARIABLE_NAME=NEXUSREPO_REPO_GROUP_ID
28     - !reference [.check-variable-sh, script]
29     - export VARIABLE_NAME=ARTEFACT_ID
30     - !reference [.check-variable-sh, script]
31     - export VARIABLE_NAME=ARTEFACT_VERSION
32     - !reference [.check-variable-sh, script]
33     - export VARIABLE_NAME=ARTEFACT_PACKAGE
```

Yaml for
modular

Reference Pipelines

fully implemented pipeline samples

Reference pipelines

Following [E2E CI pipeline examples using SHIP-HATS templates](#) are available for use.



If you do not have access to GitLab, you may [access mirror templates in BitBucket](#) for reference only.

Template	Description	Mirror
javaapp	Example end to end CI pipeline for a sample 3-tier application hosted in AWS EC2	Mirror template in BitBucket for reference only if you do not have access to GitLab
javadockerapp	Example end to end CI pipeline for sample containerized Java application hosted in AWS EKS	Mirror template in BitBucket for reference only if you do not have access to GitLab
netapp	Example end to end CI pipeline for sample containerized .NET applications hosted in Azure App Service	Mirror template in BitBucket for reference only if you do not have access to GitLab
netdocker	Example end to end CI pipeline for sample containerized .NET Core application hosted in AWS Fargate	Mirror template in BitBucket for reference only if you do not have access to GitLab
nodetsapp	Example end to end CI pipeline for sample Node.js typescript application hosted in Azure App Service	Mirror template in BitBucket for reference only if you do not have access to GitLab

Developed by CTMO, SVC Group, GovTech

Pipeline COE

aka DevSecOps Governance Framework (DGF) (new branding)

Reusable code & images

- Feature provided by GitLab & maintained by the SHIP-HATS Team with a base set of **reusable code & images**
- Part of inner-sourcing efforts
- The SHIP-HATS team is **continually developing new reusable assets**
- Agencies can raise a Service Ticket to **suggest new assets**

The screenshot shows the GitLab interface for the group **sgts-pipelinecoe**. At the top, it displays recent activity: 6 merge requests created, 15 issues created, and 3 members added over the last 30 days. Below this are tabs for Subgroups and projects, Shared projects, and Archived projects. A search bar and a 'Pipeline COE' watermark are also present.

Subgroup	Count	Description
Containers	10	Ansible Container, Ant Container, AWS-CLI and Kubernetes Container, AWS-CLI and Terraform Container, AWS-CLI Container, Buildah Container, Container Base, Crane Container, ECR Container, Empty Container, ExternalCI Container
Templates	3	IDE Templates, Pipeline Templates

This screenshot shows a detailed view of the 'Containers' subgroup under the **sgts-pipelinecoe** group. It lists various container templates, each with a small icon and a link. A callout on the right side points to the 'Empty Container' template with the text **Container Images for Runners**.

Template	Description
Ansible Container	Ansible Container
Ant Container	Ant Container
AWS-CLI and Kubernetes Container	AWS-CLI and Kubernetes Container
AWS-CLI and Terraform Container	AWS-CLI and Terraform Container
AWS-CLI Container	AWS-CLI Container
Buildah Container	Buildah Container
Container Base	Container Base
Crane Container	Crane Container
ECR Container	ECR Container
Empty Container	Empty Container Project to fork for new images
ExternalCI Container	ExternalCI Container

Security Baseline & Testing Tools

Security Features

Benefits of Automated Security Testing:

- Tests are completed faster
- Consistency of running the same tests across incremental builds
- Repeatability allows the task to be built into a larger automated process
- Auditability of tests through logging and dashboards

To streamline and automate manual testing efforts, the following features were introduced

1	Security with SHIP-HATS Shifting left and codifying security
2	Compliance Framework Automates setting up controls
3	Extended Code Analysis Testing feature from CSG, available by default

Centralising automated security testing via SHIP-HATS

Impetus

- Lack of basic security capabilities across government
- Similar environmental set-up and needs
- Need for speedy remediation

Benefits

- Centralise security experts
- In-built compliance and best practices through centralized tools e.g. SHIP-HATS is preconfigured for OWASP Top 10 (an industry standard)
- Learn faster and replicate learnings across WOG*

What if we don't centralise?

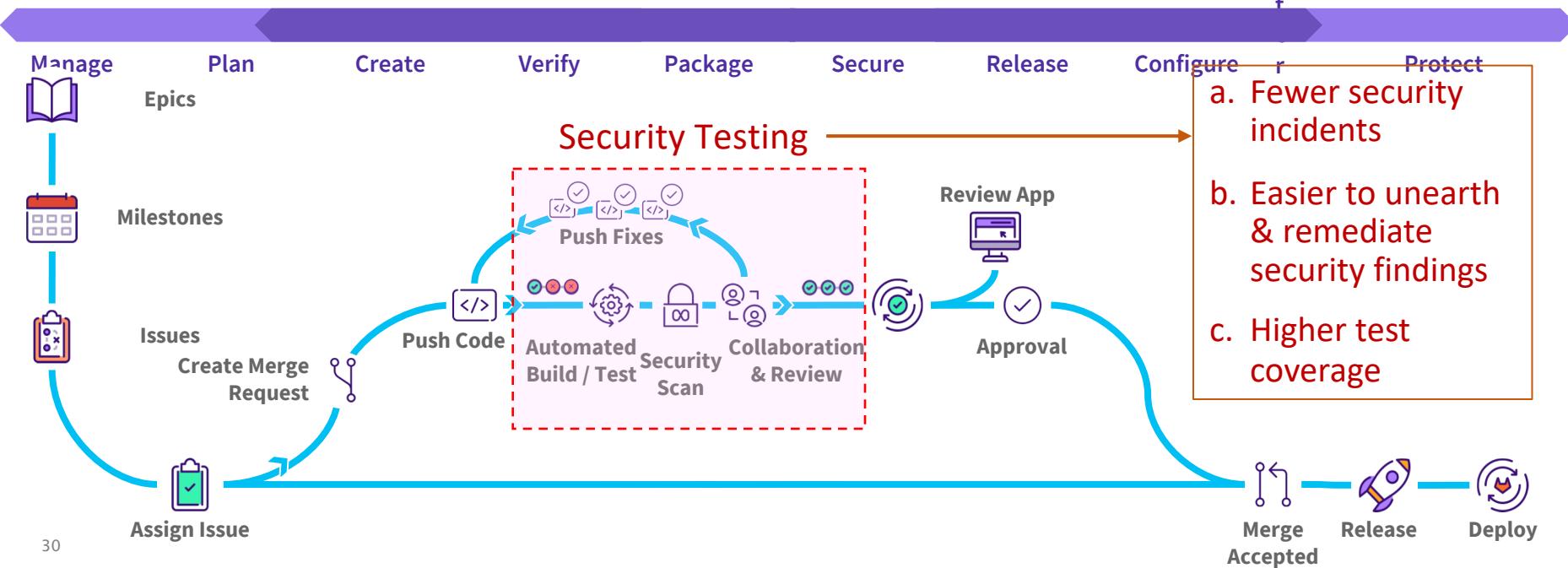
- Agencies will be left to configure tools on their own
- Longer onboarding/adoption times
- Higher manpower costs, esp. for agencies with lower DevSecOps maturity

*Apart from building-in the learnings via tools, best practices are also published in the DevOps Playbook (<https://docs.developer.tech.gov.sg/docs/devsecops-playbook>)

Security with SHIP-HATS

Shifting left and codifying security

Security testing is incorporated in the CI/CD pipeline and is automated (i.e. run every time the app is built)



Design/Plan	Develop	Build	Test	Deploy	Operate & Monitor
Security Architecture (ISC) ² Training via CAPE	Secure Development Secure Code Warrior (SCW)	Secure build management GitLab Build Runners	Performance test & monitoring pCloudy Test Farm	Approval for release to prod. GitLab Continuous Deployment	Continuous monitoring/logging AWS CloudWatch Logs
Threat modelling (ISC) ² Training via CAPE	Code repo security controls GitLab Repo BitBucket (SHIP1.0)	Secrets Detection GitLab Security Analysers Security for Bitbucket (SHIP1.0)	Dynamic App Security Testing (DAST) GitLab DAST Fortify-on-Demand DAST	Artefact repository scanning GitLab Continuous Deployment	Continuous feedback & metrics AWS CloudWatch
Capabilities on SHIP-HATS	Code reviews GitLab Merge Requests	3rd Party component scanning GitLab Dependency Scanning Nexus Intelligence / IQ Server	Manual Pen Test CSAS Bulk Tender	Continuous vuln scan (Host) AWS Systems Patch Manager AWS Inspector	Web Application Firewall AWS Web Application Firewall
	Source code scanning (SAST) GitLab Security Analysers Fortify-on-Demand SAST	Container scanning GitLab Container Scanning Prisma Cloud (SHIP1.0)		Secrets management AWS Secrets Manager	
New Capabilities	Developer endpoint security controls Developers' Environment Endpoint Posture (DEEP)	Mobile app scanning Mobile App Security Hygiene (MASH)	Repeated Security Findings Extended Code Analysis (XCA)		Cloud security controls CloudSCAPE
	Secure-by-Default Designs Secure Infrastructure-as-Code (IaC) Anyhow Code Also Secure ^				^ Denotes Experimental
Threat modelling (+) Integrative Threat Modelling Platform	Supply-chain Security Supply-chain Levels for Software Artifacts (SLSA)				Cloud architecture controls Cloud Architecture Compliance Tooling (CACTi)
					Container Threat Detection Container Anomaly Detection

Compliance Framework

Automates setting up controls

- ✓ Use GitLab feature to automate adopting DevSecOps best practices and security needs

- ✓ Teams can apply the framework from UI and confident that their controls and requirements are set up correctly

The screenshot shows the 'General' settings page for a project named 'Web App Tutorial4'. The 'Compliance framework' section is highlighted with a red box and an arrow pointing to the dropdown menu which contains the option 'ship-hats-webapp-compliance-v1.0.1'. Below this section is a 'Save changes' button. To the right of the main content area are three expandable sections: 'Default description template for issues', 'Service Desk', and 'Advanced', each with its own 'Expand' button.

W Web App Tutorial4

Project information

Repository

Issues 0

Merge requests 0

CI/CD

Security & Compliance

Deployments

Packages and registries

Infrastructure

Monitor

Analytics

Wiki

Snippets

Settings

General

Compliance framework

Select a compliance framework to apply to this project. How are these added?

Compliance framework

ship-hats-webapp-compliance-v1.0.1

Save changes

Default description template for issues

Set a default description template to be used for new issues. [What are description templates?](#)

Service Desk

Enable and disable Service Desk. Some additional configuration might be required. [Learn more.](#)

Advanced

Housekeeping, export, archive, change path, transfer, and delete.

Collapse

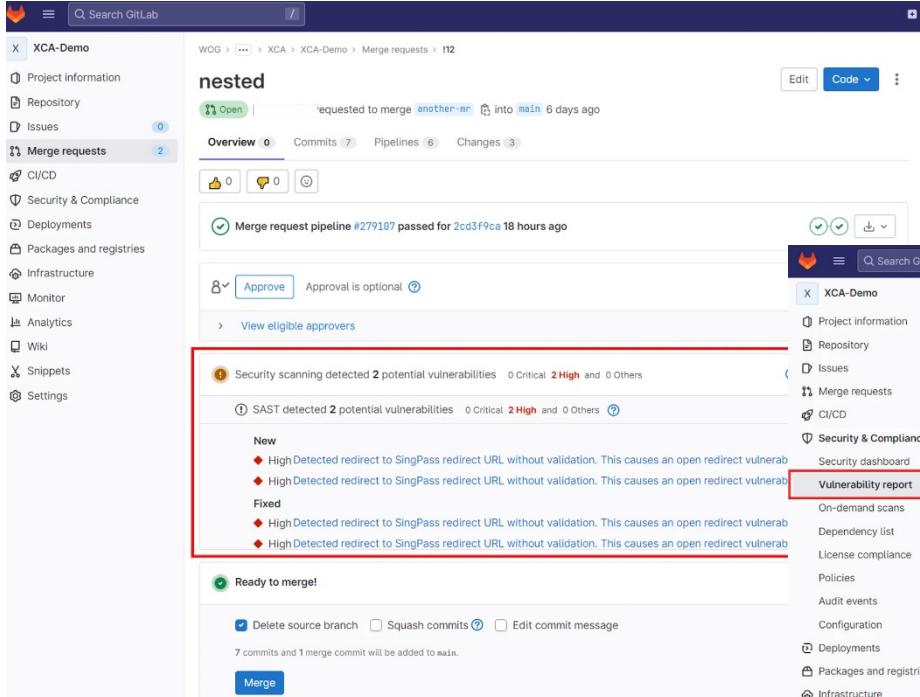
Expand

Expand

Expand

Extended Code Analysis

Testing feature from CSG, available by default



The screenshot shows a GitLab merge request interface for a project named "XCA-Demo". The merge request is titled "nested" and has been requested to merge into the "main" branch. The "Merge requests" tab shows 2 open merge requests. The main panel displays a "Merge request pipeline" status and a "Security scanning" section. A red box highlights the "Vulnerability report" link in the sidebar.

Security scanning detected 2 potential vulnerabilities

- SAST** detected 2 potential vulnerabilities: 0 Critical, 2 High, and 0 Others.

New

- High Detected redirect to SingPass redirect URL without validation. This causes an open redirect vulnerability.
- High Detected redirect to SingPass redirect URL without validation. This causes an open redirect vulnerability.

Fixed

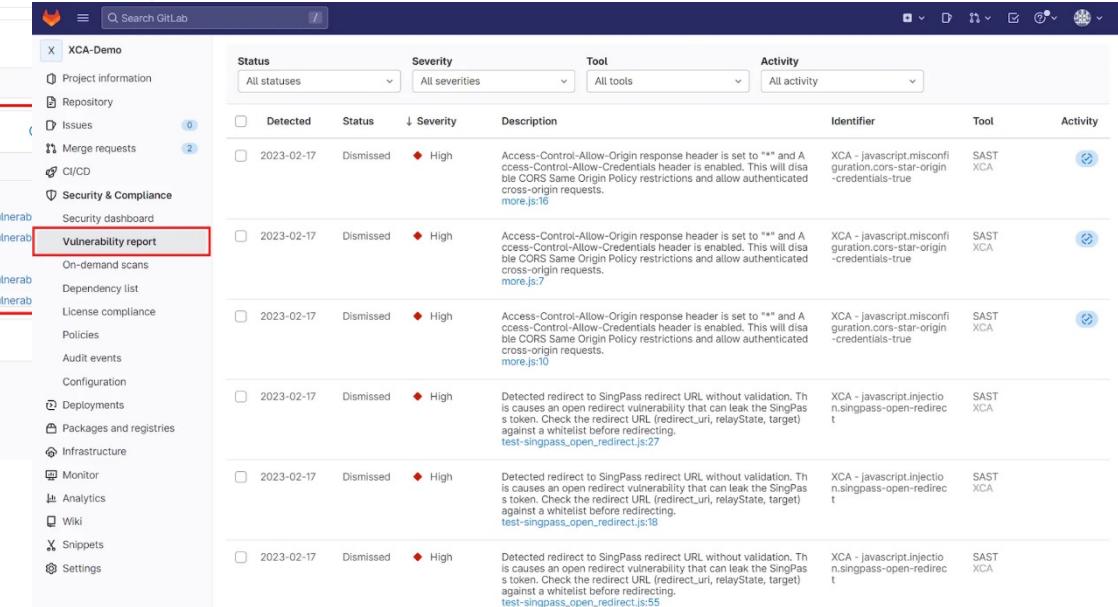
- High Detected redirect to SingPass redirect URL without validation. This causes an open redirect vulnerability.
- High Detected redirect to SingPass redirect URL without validation. This causes an open redirect vulnerability.

Ready to merge!

Delete source branch Squash commits Edit commit message

7 commits and 1 merge commit will be added to main.

Merge

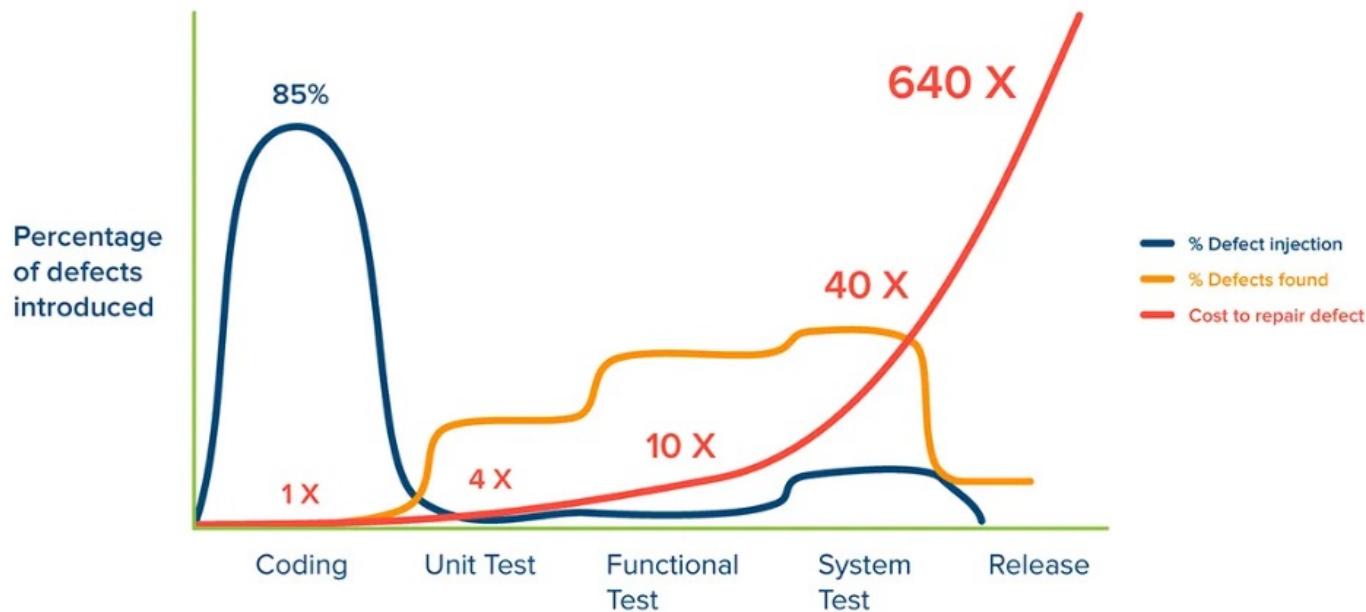


The screenshot shows a GitLab dashboard with a sidebar and a main content area. The sidebar includes links like Project information, Repository, Issues, Merge requests, CI/CD, Security & Compliance, Deployments, Packages and registries, Infrastructure, Monitor, Analytics, Wiki, Snippets, and Settings. The main content area displays a table of vulnerabilities:

Detected	Status	Severity	Description	Identifier	Tool	Activity
2023-02-17	Dismissed	High	Access-Control-Allow-Origin response header is set to "*" and Access-Control-Allow-Credentials header is enabled. This will disable CORS Same Origin Policy restrictions and allow authenticated cross-origin requests. more.js:16	XCA - javascript.misconfiguration.cors-star-origin-credentials=true	SAST XCA	View
2023-02-17	Dismissed	High	Access-Control-Allow-Origin response header is set to "*" and Access-Control-Allow-Credentials header is enabled. This will disable CORS Same Origin Policy restrictions and allow authenticated cross-origin requests. more.js:7	XCA - javascript.misconfiguration.cors-star-origin-credentials=true	SAST XCA	View
2023-02-17	Dismissed	High	Access-Control-Allow-Origin response header is set to "*" and Access-Control-Allow-Credentials header is enabled. This will disable CORS Same Origin Policy restrictions and allow authenticated cross-origin requests. more.js:10	XCA - javascript.misconfiguration.cors-star-origin-credentials=true	SAST XCA	View
2023-02-17	Dismissed	High	Detected redirect to SingPass redirect URL without validation. This causes an open redirect vulnerability that can leak the SingPass token. Check the redirect URL [redirect_uri, relayState, target] against a whitelist before redirecting. test-singpass_open_redirect.js:27	XCA - javascript.injector.singpass-open-redirect	SAST XCA	View
2023-02-17	Dismissed	High	Detected redirect to SingPass redirect URL without validation. This causes an open redirect vulnerability that can leak the SingPass token. Check the redirect URL [redirect_uri, relayState, target] against a whitelist before redirecting. test-singpass_open_redirect.js:18	XCA - javascript.injector.singpass-open-redirect	SAST XCA	View
2023-02-17	Dismissed	High	Detected redirect to SingPass redirect URL without validation. This causes an open redirect vulnerability that can leak the SingPass token. Check the redirect URL [redirect_uri, relayState, target] against a whitelist before redirecting. test-singpass_open_redirect.js:35	XCA - javascript.injector.singpass-open-redirect	SAST XCA	View

Apart from platforms, tools and features, we need to drive security best practices

Regular and more upstream security testing enables 'shift-left', where vulnerabilities are found and remediated earlier in the dev cycle resulting in fewer defects and reduced time/costs for rectification by 10x



Metrics & Value

Stream Metrics (VSM)

For Dev Productivity
and DevSecOps
Maturity

- | | |
|---|---|
| 1 | GitLab-Native Dashboards e.g. Security, Ops etc. |
| 2 | DevSecOps Scoreboard (WIP!) |

1 GitLab-Native Dashboards e.g. Security, Ops etc.

Search GitLab

Switch to

- Projects
- Groups

Explore

- Milestones
- Snippets
- Activity

Your dashboards

- Environments
- Operations
- Security

Operations Dashboard

- GitLab.org / gitaly: 2 hours ago, 0 Alerts, passed
- GitLab.com / GitLab Docs: 2 hours ago, 0 Alerts, running
- GitLab.org / gitlab-runner: 12 hours ago, 0 Alerts, failed
- GitLab.org / GitLab Community Edition: 12 hours ago, 0 Alerts, running

Security Dashboard

Vulnerabilities over time

August 19th to today

Severity

- Critical: 0 vulnerabilities
- High: 3 vulnerabilities
- Medium: 13 vulnerabilities
- Low: 30 vulnerabilities

Project security status

Projects are graded based on the highest severity vulnerability present

- F 0 projects
- D 1 project
- C 0 projects
- B 4 projects
- A 2 projects

Environments Dashboard

GitLab.org > GitLab

- gprd: View app, API, Master -> 77e42d18, Fix the failing specs, 5 hours ago
- gprd-cny: View app, API, Master -> 77e42d18, Fix the failing specs, 7 hours ago

GitLab.com > www-gitlab-com

- staging: View app, deploy_staging #352485..., Master -> c8b4ad21, Merge branch 'brendan-c...', 3 minutes ago
- production: View app, deploy #35248503, Master -> c8b4ad21, Merge branch 'brendan-c...', 3 minutes ago

Lead time charts

These charts display the median time between a merge request being merged and deployed to production, as part of the DORA 4 metrics. Learn more.

Last week Last month Last 90 days

Date range: Mar 8 - Apr 7

Median time to deploy

No merge requests were deployed during this period

Lead time

Date

DevSecOps Scoreboard (WIP!)

A Singapore Government Agency Website [How to identify](#) ▾



shiphats
DevSecOps ScoreBoard

Search for projects DESC 10

Details	Project Name	Project Settings (/6)	Security and Testing (/4)	Pipeline Standardisation (/1)	Score	Rank
Maturity	SHIP-HATS Templates	6	null	null	6	1
Maturity	clglabjavadockerapp	5	null	null	5	2
Maturity	SHIP-HATS Compliance	5	null	null	5	3
Maturity	clglabapp	5	null	null	5	4
Maturity	gitlab-nexus-iq-pipeline	5	null	null	5	5
Maturity	bootstrap-deploy-runner	5	null	null	5	6
Maturity	SHIP-HATS Webapp E2E Templates	5	null	null	5	7

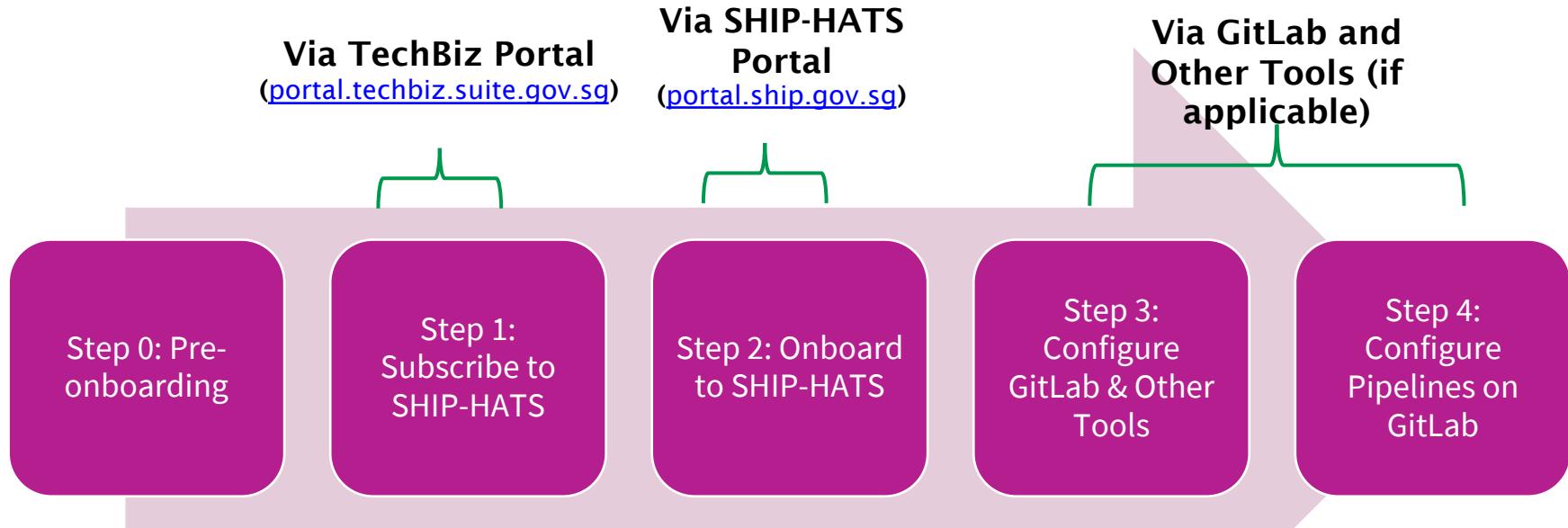
SHIP-HATS 2.0. Product Roadmap

Component	Q1	Q2	Q3	Q4
Platform Enablement	<ul style="list-style-type: none"> Shared runners for Intranet deployment 	<ul style="list-style-type: none"> Runners to support GitLab-Native services Jira/Confluence Cloud Pilot (JSM & Multi-tenancy) 		<ul style="list-style-type: none"> Jira/Confluence Cloud GA (JSM/Multi-tenancy)
CI/CD Tools and Features	<ul style="list-style-type: none"> Low-Cost Flow (GitLab-Native) Pipeline Template GitOps-based Templates 	<ul style="list-style-type: none"> GitLab Guest-Account Enablement with TechPass 	<ul style="list-style-type: none"> Limiting Feature for GitLab Guest Accounts 	<ul style="list-style-type: none"> Support for GCC + BCP
Security Baseline & Testing Tools	<ul style="list-style-type: none"> SemGrep (bg scanning) DevSecOps Security Baseline – identification of baselines and and draft measures 	<ul style="list-style-type: none"> DevSecOps Security Baseline – roll-out to GDS 	<ul style="list-style-type: none"> SLSA DevSecOps Security Baseline – roll-out to GovTech and WOG 	<ul style="list-style-type: none"> DevSecOps Security Baseline – intermediate baselines
Metrics and VSM	<ul style="list-style-type: none"> DevSecOps Scoreboard POC – checking for compliance with IM8, 	<ul style="list-style-type: none"> DevSecOps Scoreboard Beta 	<ul style="list-style-type: none"> DevSecOps Scoreboard GA – Phase 1 	<ul style="list-style-type: none"> DevSecOps Scoreboard GA – Phase 2

Getting Started



Subscribing and Onboarding to SHIP-HATS



Subscription Options

[Subscription documentation available on Developer Portal](#)

Pricing details on [go.govsg/sh2indicative](#) for Public Officers

BASE PLAN

- ✓ **3 GITLAB ULTIMATE USER LICENSE**
- ✓ **SHARED PCLOUDY**
- ✓ **STANDARD SUPPORT 9.30AM TO 5:30PM**
- ✓ **UP TO 50 GITLAB LICENSES PER BUNDLE**

NOTES

- Start with Base Option
- Add-ons to maximise flexibility

FLEXIBLE ADD-ONS

Component	What's Included	Notes
GitLab Ultimate	1 x GitLab Ultimate User License	Based on the number of users
Jira/Confluence	1 x Jira/Confluence License	Based on the number of users
Sonatype Nexus IQ & Nexus Repo	1 x Nexus IQ 1 x Nexus Repo User License	Based on the number of users
pCloudy Testing Farm	1 x pCloudy iOS Device (dedicated) 1 x pCloudy Android Device (dedicated)	1 device can be used concurrently across multiple GitLab Projects, and tests can be run in parallel
SonarQube	1 x SonarQube Community Edition App 1 x SonarQube Dev Edition App	1 app can be used for 1 subscription (i.e. shared across GitLab projects) 1 app can be used for 1 subscription (i.e. shared across GitLab projects)
Fortify-on-Demand	1 x FOD App	1 app can be shared across multiple GitLab Projects, but tests cannot be run in parallel.
Additional support	Per hour (after 5:30 PM)	Outside office hours

Self-learn with Technical Documentation

Everything on the Internet – Search on Google
Or
Visit <https://go.gov.sg/ship-hats-docs>

The screenshot shows a navigation sidebar on the left with categories like Overview, Key Features, Architecture, and Onboard to SHIP-HATS. The main content area is titled 'Audience' and describes the documentation for users like Subscription Administrators, Project Admins, and New users. It also lists additional resources and a table of related documentation.

SHIP-HATS Getting Started

Home / Docs / SHIP HATS / SHIP HATS Getting Started

Audience

This documentation is intended for the following users:

- Subscription Administrator (SA) and Project Admin (PA) to subscribe and onboard to SHIP-HATS.
- New users to understand how SHIP-HATS helps you set up your CI/CD pipeline and access training resources on using SHIP-HATS.

Following additional documentation resources are available:

Document	Audience	Description
SHIP-HATS Migration	Existing users	Use this documentation to plan migration of your systems from SHIP-HATS 1.0 to SHIP-HATS 2.0.
SHIP-HATS Portal	Subscription Administrator (SA)	Use this documentation to onboard to the SHIP-HATS portal, add projects, set Project Administrators, and manage users.
	Project Administrator (PA)	
SHIP-HATS Tools	Tools Administrators and Developers at Agencies	Use this documentation to learn about tools integrated with SHIP-HATS.
SHIP-HATS Support	All	Use this documentation to understand our Support Offering and learn about Terms & Conditions.

Attend with Workshops & Webinars

<https://go.gov.sg/ship-hats-learning-events>

[Home](#) / [Docs](#) / [SHIP HATS](#) / [SHIP HATS Getting Started](#) / Learning Events

Learning Events

Upcoming events

Date	Topic	Audience	Level	Sign up
Hands on Workshop	SHIP-HATS 2.0 and Introduction to Pipeline Templates	Tech	200	By invitation based on onboarding and migration
Scheduled every month	Classroom session for developers	SHIP-HATS Users & Prospects		
9:00 AM- 5:00 PM				
Webinar	SGTS Learning Events: SHIP-HATS Product Briefing	Non Tech	100	Sign up
20 March 2023	SGTS Overview SHIP-HATS 2.0 Product Offering & Roadmap Subscription packages	SHIP-HATS Users & prospects		
3 PM to 4 PM	Learning Resources & Training			
Webinar	SGTS Learning Events: SHIP-HATS & Application Security with FOD	Tech & Non Tech	100	Sign up
13 April 2023	Learn how modernised tools seamlessly			

SHIP-HATS Subscription

<https://go.gov.sg/sh2indicative>
Accessible via GSIB

- Materials for Subscription
- Indicative Pricing, Pricing Calculator
- Pricing Simulations
- Subscription how-to videos

Next Steps

- Reach out to us at
<https://go.gov.sg/she>
- Technical documentation
<https://go.gov.sg/ship-hats-docs>

SGTS Products

- SGTS Products
[Explore the products](#)
- SGTS Product Documentation
[Read the docs](#)

SGTS Learning Series

--- Online Webinar ---

SHIP-HATS 2.0 Product Briefing [Monday, 20 Mar 2023 3 to 4 PM](#)

Get to know the **CI/CD tool** in Singapore Government Tech Stack including roadmap, features and resources.
Level 100 Tech & Non-Tech

SHIP-HATS & Application Security with FOD [Thursday 13 Apr 2023 4 to 5 PM](#)

Learn how modernised tools seamlessly integrate into SHIP-HATS.
Level 100 Tech & Non-Tech

SHIP-HATS & Sonatype [Wednesday 26 Apr 2023 4 to 5 PM](#)

Learn the best practices of using Sonatype in SHIP-HATS.
Level 100 Tech & Non-Tech

[Learning Events available on Developer Portal](#)

The screenshot shows the Singapore Government Developer Portal's "Learning Events" page. At the top, there are navigation links for "About" and "Documentation", and icons for "Login", "Search", and "Menu". Below the header, there are sections for "Upcoming events" and "Past events". A sidebar on the left contains links for "Training" (with "Upcoming events" highlighted), "Support", and "FAQs". Another sidebar lists "Additional Resources" such as the SHIP-HATS Portal, Tools, Support, and Migration from 1.0 to 2.0. The main content area displays a table of learning events with columns for Date, Topic, Audience, Level, and Sign up.

Date	Topic	Audience	Level	Sign up
Hands on Workshop	SHIP-HATS 2.0 and Introduction to Pipeline Templates	Tech	200	By invitation based on onboarding and migration
Scheduled every month	Classroom session for developers	SHIP-HATS Users & Prospects		
9:00 AM- 5:00 PM				
Webinar	SGTS Learning Events - SHIP-HATS Product Briefing	Non Tech	100	Only by invitation
20 March 2023	SGTS Overview SHIP-HATS 2.0 Product Offering & Roadmap Subscription packages Learning Resources & Training	SHIP-HATS Users & prospects		
3 PM to 4 PM				
Webinar	SHIP-HATS & Sonatype	Tech & Non Tech	100	Sign up
26 April 2023	Covers Benefits of Sonatype Nexus IQ for OSS consumption, Nexus Platform			

Join us and remember to bring your questions for live Q&A.

Thank You

