



GitLab CI / CD / DevOps / Auto DevOps / ...

Kamil Trzciński, Staff Developer

@ayufanpl

CERN

GitLab CI? or CD?? or Auto
DevOps???

PIPELINES

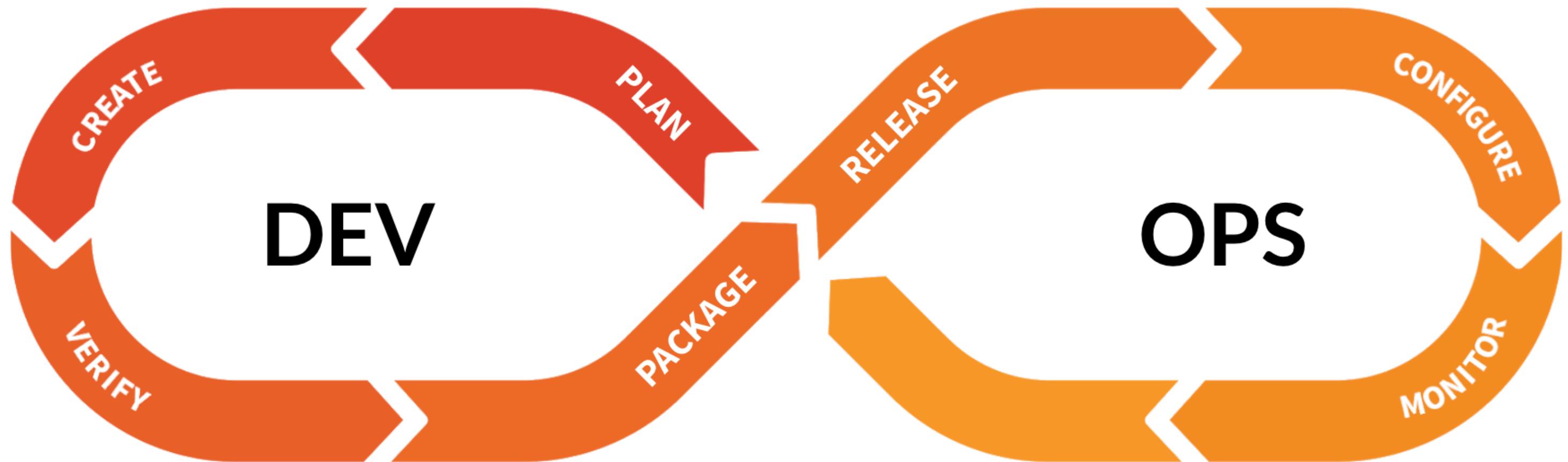


PIPELINES EVERYWHERE

memegenerator.net

<http://es.memegenerator.net/instance/61228673>





								
Manage	Plan	Create	Verify	Package	Release	Configure	Monitor	Secure
Cycle Analytics	Issue Trackers	Source Code Management	Continuous Integration (CI)	Container Registry	Continuous Delivery (CD)	Auto DevOps	Metrics	SAST
DevOps Score	Issue Boards	Code Review	Unit Testing	Maven Packages Repository	Pages	Kubernetes Configuration	Logging	DAST
Audit Management	Service Desk	Wiki	Integration Testing		Review apps	ChatOps	Cluster Monitoring	Dependency Scanning
Authentication and Authorization	Portfolio Management	Snippets	Code Quality		Incremental Rollout			Container Scanning
		Web IDE	Performance Testing					License Management

* New *



Verify



Package



Release



Configure



Monitor



Secure

Continuous
Integration (CI)

Unit Testing
Integration
Testing

Code Quality

Performance
Testing

Container
Registry

Maven Packages
Repository

Continuous
Delivery (CD)

Pages
Review apps
Incremental
Rollout

Auto DevOps

Kubernetes
Configuration
ChatOps

Metrics

Logging
Cluster
Monitoring

SAST

DAST

Dependency
Scanning

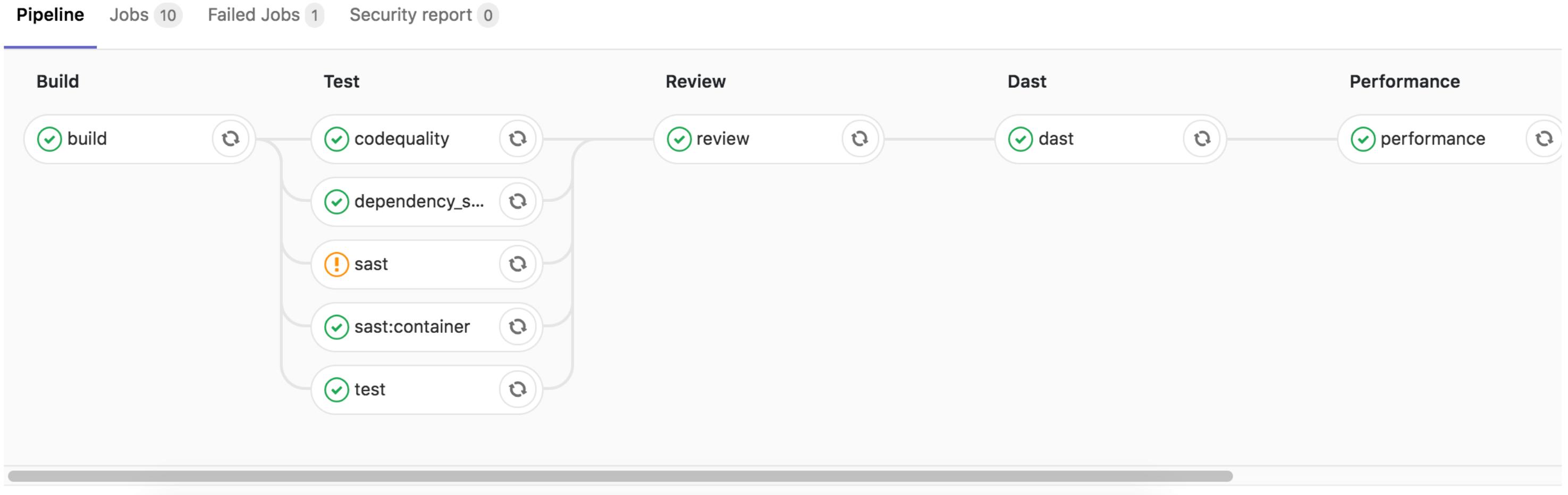
Container
Scanning

License
Management



Recent features

Auto DevOps (11.0)



<https://docs.gitlab.com/ee/topics/autodevops/>

Security Dashboard (11.1)

The screenshot shows the GitLab Security Dashboard for the 'Awesome project'. The pipeline was triggered 1 hour ago by John Doe (represented by a green hexagonal icon) on the master branch (commit hash: 8fc350a9). The dashboard displays the following findings:

- SAST detected 3 vulnerabilities**
 - High: Insecure variable usage in subdir/src/main/java/com/gitlab/security_products/tests/App.java:19
 - Medium: Cipher with no integrity in subdir/src/main/java/com/gitlab/security_products/tests/App.java:29
 - Medium: ECB mode is insecure in subdir/src/main/java/com/gitlab/security_products/tests/App.java:29
- Dependency scanning detected 3 vulnerabilities**
 - Unknown: CSRF protection bypass for org.apache.struts/struts2-core in pom.xml
 - Unknown: Long parameter name DoS for org.apache.struts/struts2-core in pom.xml
 - Unknown: Remote command execution due to flaw in the includeParams attribute of URL and Anchor tags for org.apache.struts/struts2-core in pom.xml
- Container scanning detected no vulnerabilities**
- DAST detected no vulnerabilities**

Security Reports (11.1)

- ! Dependency scanning detected [4 vulnerabilities](#)
- ! Container scanning detected [1 vulnerability](#)
- ! DAST detected [1 vulnerability](#)

Pipeline Jobs 5 **Security report 67**

- ! SAST detected [61 vulnerabilities](#) [?](#) [Expand](#)
- ! Dependency scanning detected [4 vulnerabilities](#) [?](#) [Expand](#)
- ! Container scanning detected [1 vulnerability](#) [?](#) [Collapse](#)

Unapproved vulnerabilities (red) can be marked as approved. [Learn more about whitelisting](#)

Kaniko support (11.2)

```
build:  
  stage: build  
  image:  
    name: gcr.io/kaniko-project/executor:debug  
    entrypoint: []  
  script:  
    - 'mkdir -p /root/.docker'  
    - echo ... > /root/.docker/config.json  
    - /kaniko/executor \  
      --context "$CI_PROJECT_DIR" \  
      --dockerfile "$CI_PROJECT_DIR/Dockerfile" \  
      --destination "$CI_REGISTRY_IMAGE:$CI_COMMIT_TAG"
```

https://docs.gitlab.com/ee/ci/docker/using_kaniko.html

JUnit (11.2)

Request to merge 4335-branch...ll-be-merged  into master (3 commits behind) Check out branch  ▾

 Pipeline #515678902 running for 98ed20bb9 

 Test summary found 2 failed tests and 1 resolved test out of 34 total Collapse

 Rspec failed 2 test and fixed 1 tests out of 34 total

 New testOne failed in SampleTest.java
 testTwo failed in SampleTest.java
 testThree passed in SampleTest.java

 Merge Remove source branch Modify commit message

<https://docs.gitlab.com/ee/ci/junittestreports.html>

JUnit (11.2)

```
rspec:  
  script:  
    - rspec spec/lib/ --format RspecJunitFormatter --out rspec.xml  
artifacts:  
  reports:  
    junit: rspec.xml
```

<https://docs.gitlab.com/ee/ci/junittestreports.html>

Maven Packages (11.3)

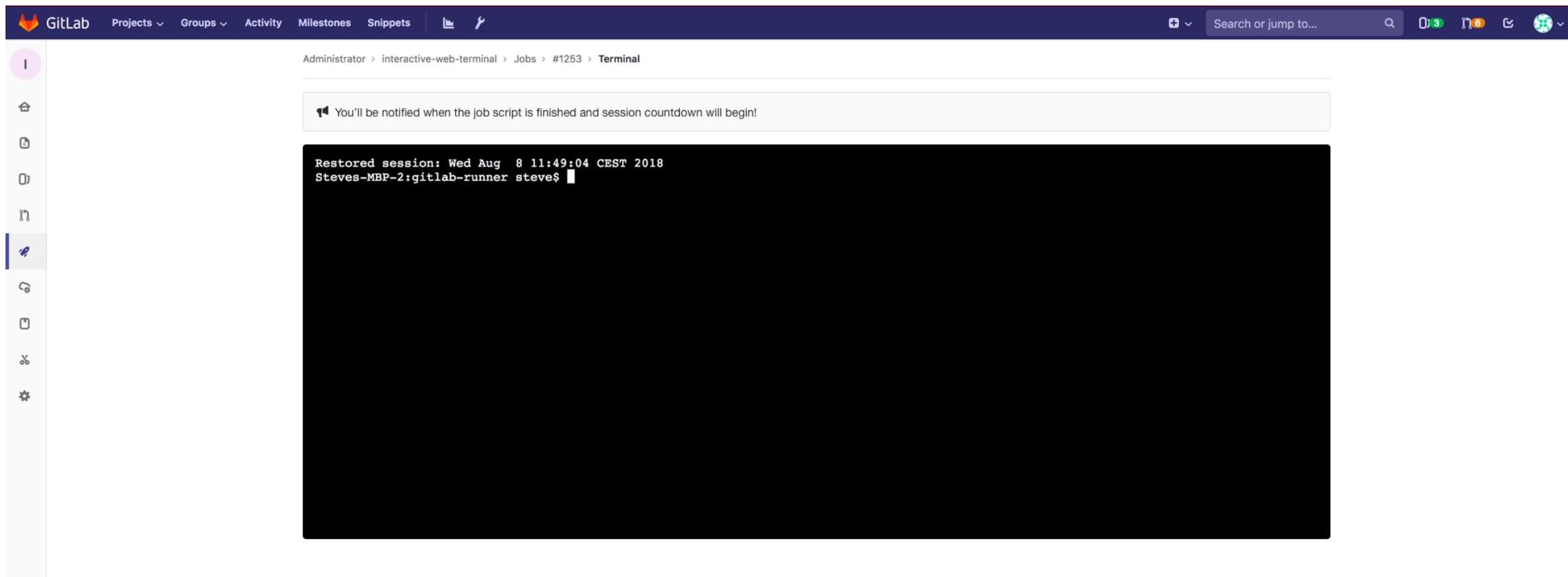
 GitLab.org > Examples > mvn-example > Packages > com/mycompany/app/my-app > **1.5-SNAPSHOT**

1.5-SNAPSHOT

Package information		Maven Metadata	
Name	com/mycompany/app/my-app	Group ID	com.mycompany.app
Version	1.5-SNAPSHOT	Artifact ID	my-app
Created on	Sep 14, 2018 7:43am	Version	1.5-SNAPSHOT
Name		Size	Created
 maven-metadata.xml		767 Bytes	20 hours ago
 my-app-1.5-20180914.074901-1.pom		1.4 KB	20 hours ago
 my-app-1.5-20180914.074901-1.jar		2.4 KB	20 hours ago

https://docs.gitlab.com/ee/user/project/packages/maven_repository.html

Interactive Web Terminal (11.3)



Limited to Kubernetes and Shell
<https://docs.gitlab.com/ee/administration/integration/terminal.html>

Protected Environments (11.3)

Protected environments

Protect environments in order to restrict who can execute deployments.

[Collapse](#)

Protect an environment

Environment
Select an environment

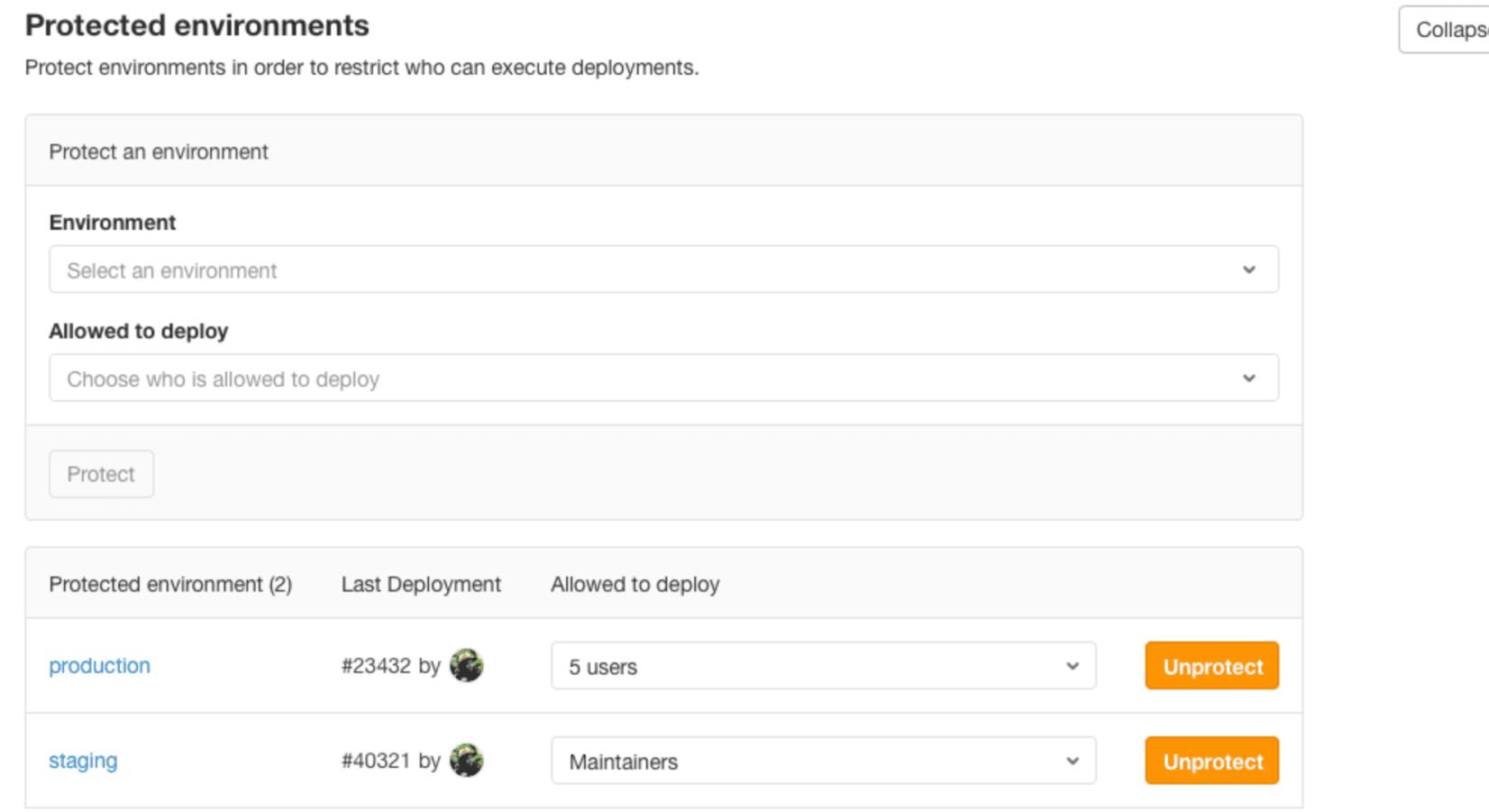
Allowed to deploy
Choose who is allowed to deploy

[Protect](#)

Protected environment (2)	Last Deployment	Allowed to deploy
production	#23432 by 	5 users
staging	#40321 by 	Maintainers

[Unprotect](#)

[Unprotect](#)



https://docs.gitlab.com/ee/ci/environments/protected_environments.html

Upcoming features

Feature Flags (11.4)

The screenshot shows the GitLab interface for the 'Gitlab Test' project. The left sidebar includes sections for Project, Repository, Issues (16), Merge Requests (9), CI / CD, Operations (Metrics, Environments, Kubernetes, Feature Flags selected), and Wiki. The main content area displays a landing page for Feature Flags with a heading 'Get started with feature flags', a description about dynamically toggling functionality, and two buttons: 'New Feature Flag' (green) and 'Configure' (blue). A decorative graphic features a user icon, a lightning bolt, and a code editor icon.

Provides Unleash-compatible interface
<https://gitlab.com/gitlab-org/gitlab-ee/issues/779>

Feature Flags (11.4)

```
func init() {
    unleash.Initialize(
        unleash.WithUrl("https://gitlab.com/api/v4/feature_flags/unleash/14"),
        unleash.WithInstanceId("29QmjsW6KngPR5JNPMWx"),
        unleash.WithAppName("production")
    )
}

func helloServer(w http.ResponseWriter, req *http.Request) {
    if unleash.IsEnabled("my_feature_name") {
        io.WriteString(w, "Feature enabled\n")
    } else {
        io.WriteString(w, "hello, world!\n")
    }
}
```

Kubernetes RBAC (11.4)

Create new Cluster on GKE Add existing cluster

Enter the details for your Kubernetes cluster

Please enter access information for your Kubernetes cluster. If you need help, you can read our [documentation](#) on Kubernetes

Kubernetes cluster name

Kubernetes cluster name

API URL

API URL

CA Certificate

Certificate Authority bundle (PEM format)

Token

Service token

Project namespace (optional, unique)

Project namespace

RBAC-enabled cluster (experimental)

Enable this setting if using role-based access control (RBAC). This option will allow you to install applications on RBAC clusters.

Add Kubernetes cluster

Support for Role-based access control

Auto DevOps RBAC (11.4)

RBAC will limit Kubernetes API access only to given namespace.

https://gitlab.com/gitlab-org/gitlab-ce/merge_requests/21867

Web Terminal (11.4)

1. Support for **Docker** executor,
2. **docker exec** run strategy for Runner (stretch).

<https://gitlab.com/gitlab-org/gitlab-runner/issues/3467>

Run jobs on changed files (11.4)

```
docker_build:  
only:  
changes:  
  - Dockerfile  
  - assets/*
```

The new branches workflow not yet supported:
we need Pipeline for Merge Requests

Delayed jobs (11.4)

```
rollout 10%:  
  script: ...  
  when: delayed  
  start_in: 20 minutes
```

Ideal use-case Incremental Rollouts

<https://gitlab.com/gitlab-org/gitlab-ce/issues/51352>

Group Security Dashboards (11.4)

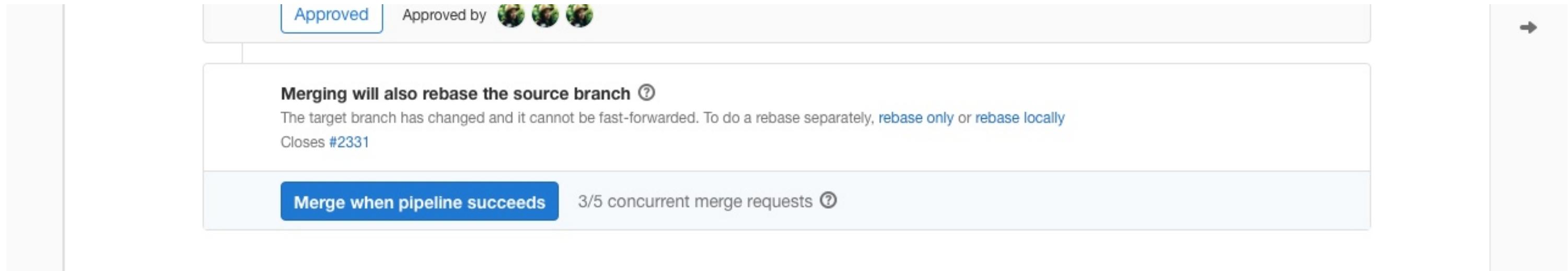
The screenshot shows the GitLab Security Dashboard. At the top, there is a summary of vulnerabilities by severity: Critical (224), High (1025), Medium (2248), Low (45), and Unknown (8). Below this, a table lists vulnerabilities categorized by Severity (CRITICAL, HIGH, MEDIUM, LOW, UNKNOWN), Project, and Confidence. The table includes a header row with filters for Severity, Project, and Confidence, and a 'Reset filters' button.

Severity	Project	Confidence
All	All	All
CRITICAL	Insecure variable usage GitLab.org / security-products / binaries	High
CRITICAL	Insecure variable usage GitLab.org / quality / staging	High
MEDIUM	Insecure variable usage GitLab.org / security-products / license-management	-
HIGH	Insecure variable usage GitLab.org / security-products / codequality	Low
CRITICAL	Insecure variable usage GitLab.org / quality / staging	High
CRITICAL	Insecure variable usage GitLab.org / security-products / license-management	High
HIGH	Selector interpreted as HTML for jquery GitLab.org / security-products / binaries	Medium
MEDIUM	Out-of-bounds Read for stringstream GitLab.org / security-products / binaries	Low
LOW	Remote command execution due to flaw in the includeParams attribute of URL and Anchor tags for org.apache.struts2-core GitLab.org / quality / staging	-
UNKNOWN	Doorkeeper gem does not revoke token for public clients GitLab.org / security-products / codequality	-

At the bottom, there are navigation links: Prev, 1, 2, 3, 4, 5, ..., Next, Last >.

<https://gitlab.com/gitlab-org/gitlab-ee/issues/6709>

Merge Trains (11.5?)



<https://gitlab.com/gitlab-org/gitlab-ee/issues/7380>

Serverless (11.5?)

The screenshot shows the 'Deploy' section of the GitLab settings. On the left is a vertical sidebar with icons for Home, Projects, Runners, Pipelines, CI/CD, Applications, Knative, and Settings. The 'Applications' icon is highlighted.

Application	Description	Status
Placeholder	Deployed applications.	Install
GitLab Runner	GitLab Runner connects to this project's repository and executes CI/CD jobs, pushing results back and deploying applications to production.	Install
JupyterHub	JupyterHub, a multi-user Hub, spawns, manages, and proxies multiple instances of the single-user Jupyter notebook server. JupyterHub can be used to serve notebooks to a class of students, a corporate data science group, or a scientific research group.	Install
Knative	A Knative build extends Kubernetes and utilizes existing Kubernetes primitives to provide you with the ability to run on-cluster container builds from source. For example, you can write a build that uses Kubernetes-native resources to obtain your source code from a repository, build it into a container image, and then run that image.	Installing

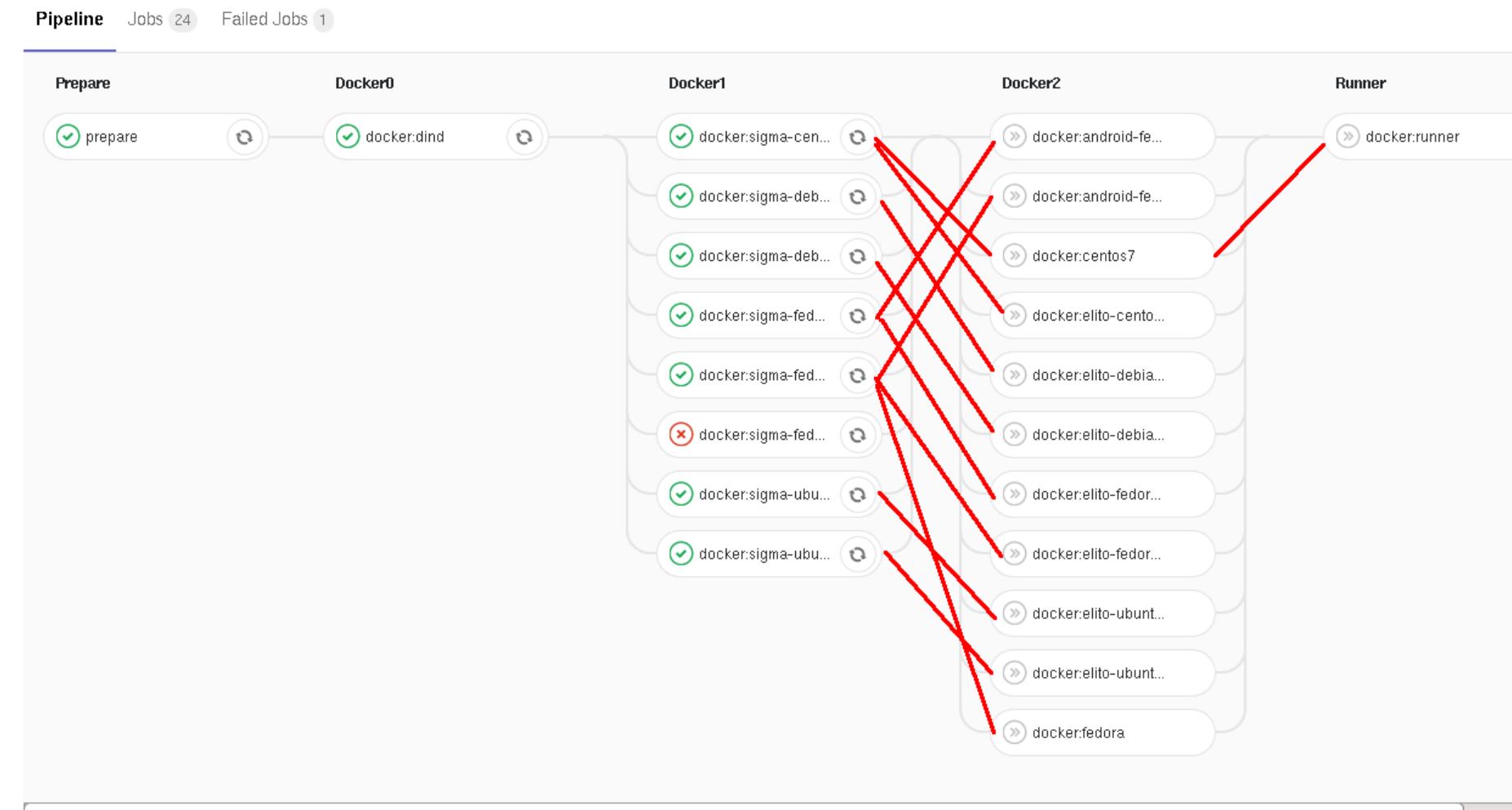
<https://gitlab.com/gitlab-org/gitlab-ce/issues/43959>

Knative (11.5?)

1. **Scale to zero**, request-driven compute model,
2. Cloud-native source to container orchestration (uses **kaniko**),
3. Universal subscription, delivery and management of **events**,
4. GitLab will add abstraction to provide **FaaS** (functions-as-a-service).

Auto DevOps on Knative? or **Auto Serverless**?

Direct acyclic graphs (??)



<https://gitlab.com/gitlab-org/gitlab-ce/issues/47063>

 Manage	 Plan	 Create	 Verify	 Package	 Release	 Configure	 Monitor	 Secure
								
Code analytics	Program Management		System Testing	NPM Registry	Feature flags	Serverless	Tracing	Interactive Application
Workflow Policies	Requirements Management		Acceptance Testing (UAT)	Rubygems Registry	Binary authorization	PaaS	Error Tracking	Security
Product Design Management	Value Stream Management		Usability Testing			Chaos Engineering	Incident Management	Testing (IAST)
			Compatibility Testing			Runbooks	Service Status Page	Web Application Firewall (WAF)
							Production Monitoring	Runtime Application Self-Protection (RASP)

Thanks!

GitLab CI / CD / DevOps / Auto DevOps / ...

Kamil Trzciński, Staff Developer, [@ayufanpl](#)