Qualys IaC Security Integration with GitLab

In the current continuous integration and continuous deployment (CICD) environment, the security scans are conducted on cloud resources after deployment. As a result, you secure your cloud resources post deployment to respective Cloud accounts.

With an introduction of Infrastructure as Code (IaC) security feature by Qualys CloudView, you can now secure your IaC templates before the cloud resources are deployed in your cloud environments. The IaC Security feature will help you shifting cloud security and compliance posture to the left, allowing evaluation of cloud resource for misconfigurations much early during development phase.

CloudView offers an integration with GitLab to secure GitLab repositories using a pipeline template, that can be used to scan your IaC templates from GitLab repositories. It continuously verifies security misconfigurations against CloudView security controls and displays the failed checks for each run. You have a continuous visibility of security posture of your IaC Templates at GitLab Pipeline and plan for remediation. Follow this guide for more details.

For supported templates, other integrations, and features of Cloud IaC Security, refer to CloudView User Guide and CloudView API User Guide.

Scanning IaC Templates at GitLab

The GitLab integration allows you to perform IaC scans at the GitLab repositories on the push and merge requests. It checks the security issues and displays the failed checks in a vulnerability report. We provide you with a pipeline template and options that can be configured to run based on various triggers.

You can perform IaC scan on either of the following:

- the entire repository for the branch where the manual/scheduled event was performed.

- the templates that were changed or newly added to the branch.

The results are generated within GitLab pipeline output that provide you with proactive visibility into the security of your IaC templates residing in GitLab repositories.

Let us see the quick workflow:

Pre-requisite

Configure Environment Variables

Configure Pipeline

Trigger Scan

Understanding Scan Output

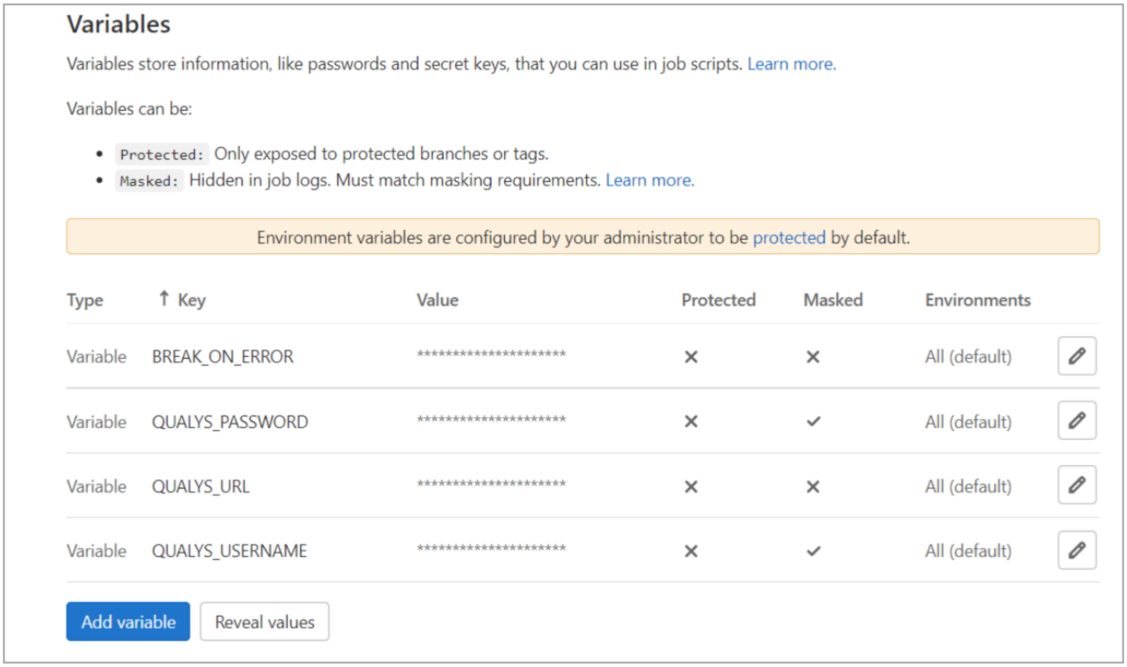
Pre-requisite

Ensure that you have valid subscription of Qualys CloudView (Cloud Security Assessment) app.

Before you trigger IaC scans in GitLab, ensure that you configure environment variables that are used in the pipeline.

Configure Environment Variables

On GitLab console, go to Setting > CI/CD > Variables.



Variables

Variables store information, like passwords and secret keys, that you can use in job scripts. Learn more.

Variables can be:

- Protected: Only exposed to protected branches or tags.
- Masked: Hidden in job logs. Must match masking requirements. Learn more.

Environment variables are configured by your administrator to be protected by default.

Type	↑ Key	Value	Protected	Masked	Environments
Variable	BREAK_ON_ERROR	********************	✕	✕	All (default)
Variable	QUALYS_PASSWORD	********************	✕	✓	All (default)
Variable	QUALYS_URL	********************	✕	✕	All (default)
Variable	QUALYS_USERNAME	********************	✕	✓	All (default)

Provide the required details for environment variables.

Variable	Description
QUALYS_URL	Qualys platform URL. To know about your Qualys platform URL, click here.
QUALYS_USERNAME	Qualys username
QUALYS_PASSWORD	Qualys password
BREAK_ON_ERROR	Set this variable as false if you do not want the pipeline to fail on any failed checks in IaC scan. Else, set this as true or do not add this variable.

Configure Pipeline

We provide you with a pipeline template that you can use to scan the repository.

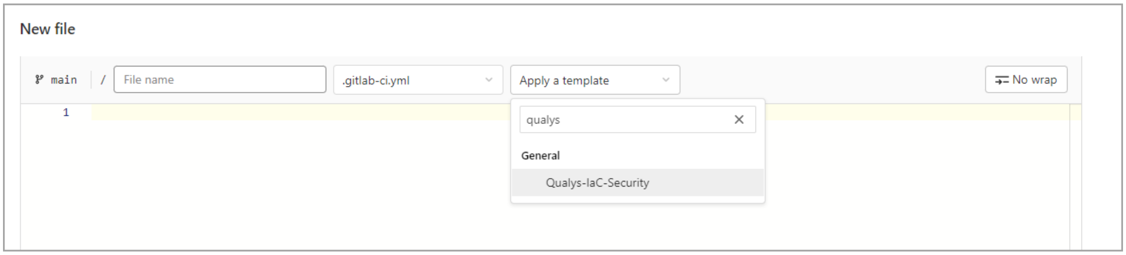
To use the template:

1. In GitLab, navigate to your repository.

2. Click + ˅ > New file.

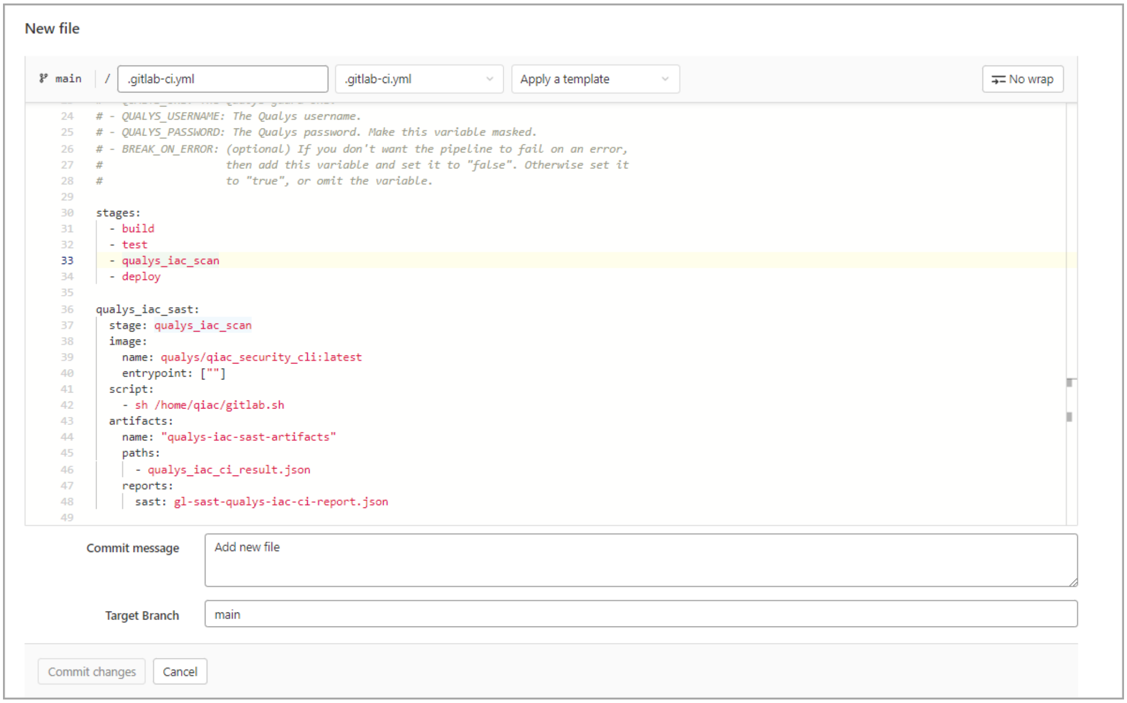
3. Select the .gitlab-ci.yml from the Select a template type drop-down.

When you select the template type, the Apply a template drop-down is available.



4. Select the Qualys-IaC-Security from the Apply a template drop-down.

Once you select the template, the contents of the file are automatically loaded.



```
# - QUALYS_USERNAME: The Qualys username.
# - QUALYS_PASSWORD: The Qualys password. Make this variable masked.
# - BREAK_ON_ERROR: (optional) If you don't want the pipeline to fail on an error,
#                   then add this variable and set it to "false". Otherwise set it
#                   to "true", or omit the variable.

stages:
  - build
  - test
  - qualys_iac_scan
  - deploy

qualys_iac_sast:
  stage: qualys_iac_scan
  image:
    name: qualys/qiac_security_cli:latest
    entrypoint: [""]
  script:
    - sh /home/qiac/gitlab.sh
  artifacts:
    name: "qualys-iac-sast-artifacts"
    paths:
      - qualys_iac_ci_result.json
    reports:
      sast: gl-sast-qualys-iac-ci-report.json

```

Commit message: Add new file

Target Branch: main

Alternatively, you can also create the .gitlab-ci.yml file in the root directory of your repository, with the content provided.

Contents of Pipeline Script (.gitlab-ci.yml)

```
stages:
  - build
  - test
  - qualys_iac_scan
  - deploy
qualys_iac_sast:
  stage: qualys_iac_scan
  image:
    name: qualys/qiac_security_cli:latest
    entrypoint: [""]
  script:
    - sh /home/qiac/gitlab.sh
  artifacts:
    name: "qualys-iac-sast-artifacts"
    paths:
      - qualys_iac_ci_result.json
    reports:
      sast: gl-sast-qualys-iac-ci-report.json
```

Trigger Scan

Once you have configured the pipeline, you can trigger a scan in the following ways:

Trigger Scan (Automatically)

Trigger Scan (Manually)

Trigger Scan (Scheduled)

Trigger Scan (Automatically)

The IaC scan is automatically triggered on every push request and merge request. Once the pipeline is configured, it is automatically executed, and the scan is triggered with every push request and merge request. With every such action, the committed or merged files that were added to the branch are scanned.

Trigger Scan (Manually)

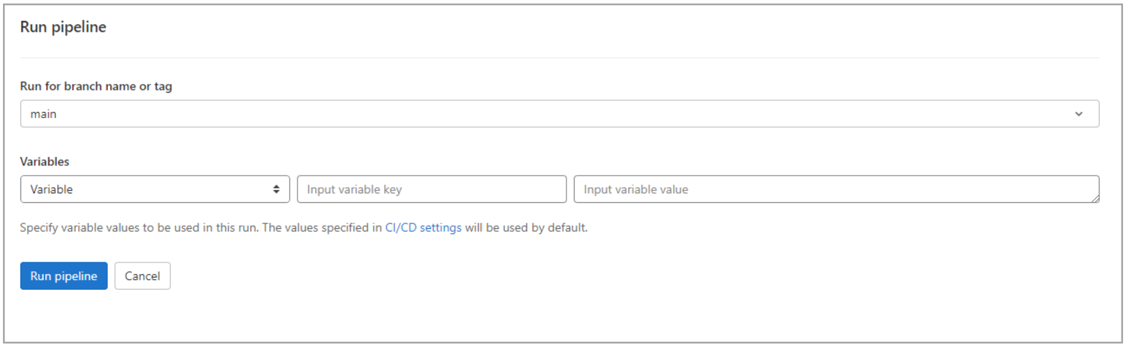
You could manually trigger a scan for the entire repository.

1. In GitLab, navigate to your project.

2. Click CI/CD > Pipelines.

3. Click Run pipeline.

The Run pipeline screen is displayed.



Run pipeline

Run for branch name or tag: main

Variables: Variable | Input variable key | Input variable value

Specify variable values to be used in this run. The values specified in CI/CD settings will be used by default.

4. In the **Run for branch name or tag** field, select the branch or tag for which you want to trigger the scan.

5. Click Run pipeline.

The scan is initiated on all the files in the selected branch of your repository.

Trigger Scan (Scheduled)

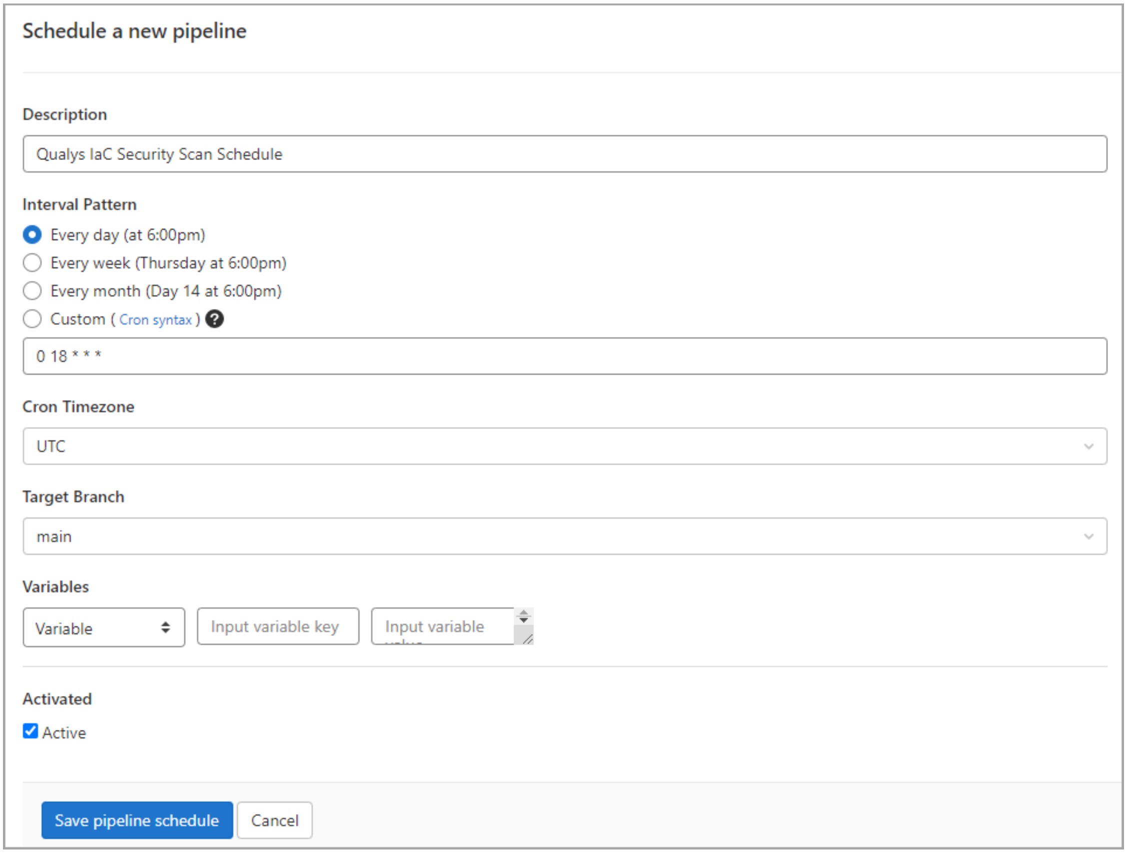
You could schedule the IaC scans to be executed at a scheduled time at specific intervals.

1. In GitLab, navigate to your project.

2. Click CI/CD > Schedules.

3. Click New schedule.

The Schedule a new pipeline screen is displayed.



Schedule a new pipeline

Description: Qualys IaC Security Scan Schedule

Interval Pattern

● Every day (at 6:00pm)
○ Every week (Thursday at 6:00pm)
○ Every month (Day 14 at 6:00pm)
○ Custom (Cron syntax)

0 18 * * *

Cron Timezone: UTC

Target Branch: main

Variables: Variable | Input variable key | Input variable value

Activated

☑ Active

4. Enter the description for the new schedule.

5. Select the required option from Interval Pattern and add appropriate value in the field.

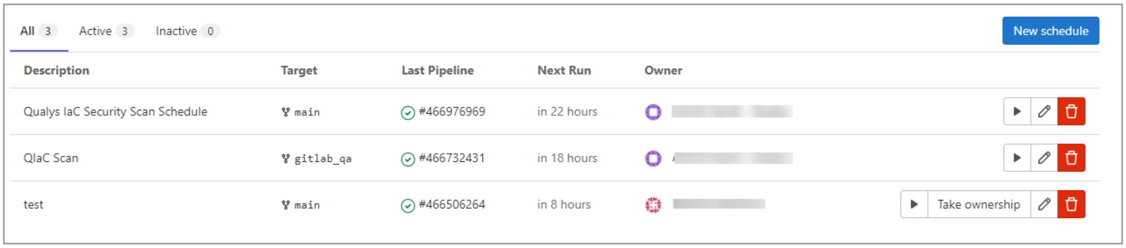
Note: The schedule timing is configured with cron notation.

6. Select the relevant timezone from the Cron Timezone drop-down. For example, UTC.

7. Select the branch on which you want to trigger the scan from the Target Branch drop-down.

8. Click Save pipeline schedule.

In the schedules list page, you can see a list of the pipelines that are scheduled to run. The next run is automatically calculated by the GitLab scheduler.



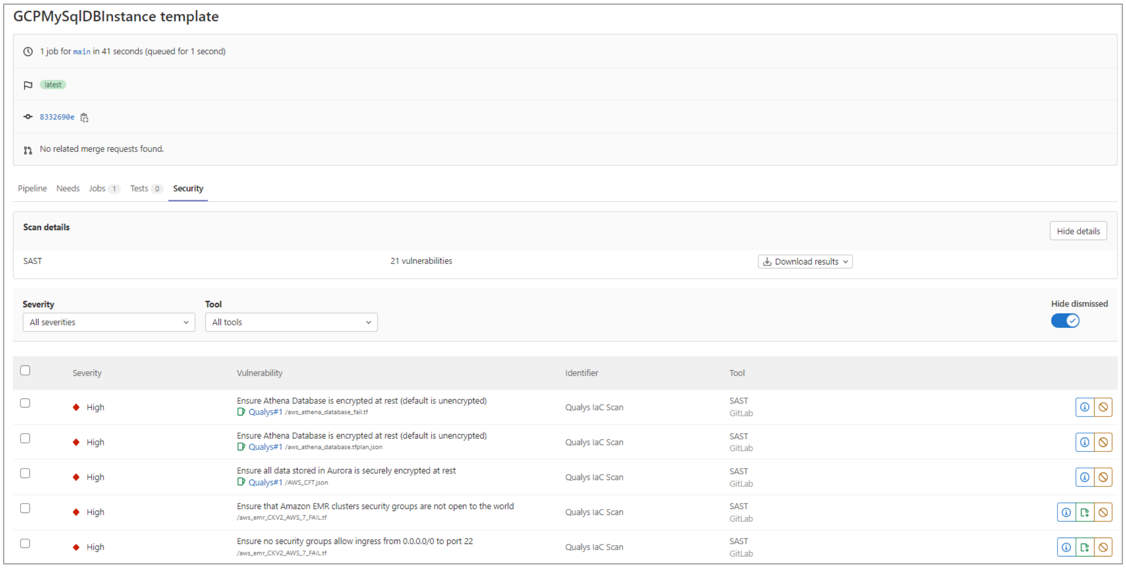
All 3 | Active 3 | Inactive 0 | New schedule

Description	Target	Last Pipeline	Next Run	Owner	
Qualys IaC Security Scan Schedule	main	#466976969	in 22 hours	[redacted]	
QIaC Scan	gitlab_qa	#466732431	in 18 hours	[redacted]	
test	main	#466506264	in 8 hours	[redacted]	Take ownership

Understanding Scan Output

Once the pipeline is executed successfully, you can view the results on the Security tab of completed pipeline job.

To download the report, click Download results.



GCPMySqlDBInstance template

1 job for main in 41 seconds (queued for 1 second)

latest

8332690e

No related merge requests found.

Pipeline | Needs | Jobs 1 | Tests 0 | Security

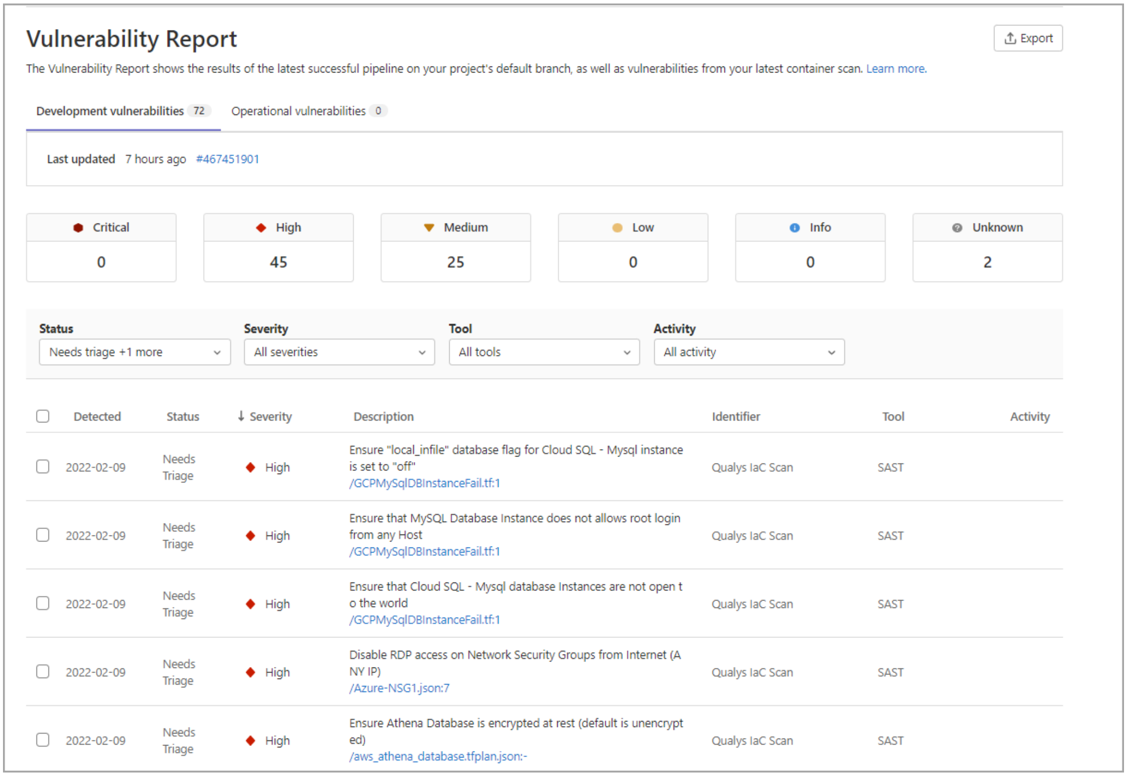
Scan details | Hide details

SAST | 21 vulnerabilities | Download results

Severity: All severities | Tool: All tools | Hide dismissed

□	Severity	Vulnerability	Identifier	Tool
□	◆ High	Ensure Athena Database is encrypted at rest (default is unencrypted) Qualys#1 /aws_athena_database_fail.tf	Qualys IaC Scan	SAST GitLab
□	◆ High	Ensure Athena Database is encrypted at rest (default is unencrypted) Qualys#1 /aws_athena_database.tfplan.json	Qualys IaC Scan	SAST GitLab
□	◆ High	Ensure all data stored in Aurora is securely encrypted at rest Qualys#1 /AWS_CFT.json	Qualys IaC Scan	SAST GitLab
□	◆ High	Ensure that Amazon EMR clusters security groups are not open to the world /aws_emr_CKV2_AWS_7_FAIL.tf	Qualys IaC Scan	SAST GitLab
□	◆ High	Ensure no security groups allow ingress from 0.0.0.0/0 to port 22 /aws_emr_CKV2_AWS_7_FAIL.tf	Qualys IaC Scan	SAST GitLab

To view the vulnerabilities reported by Qualys IaC Security in all GitLab pipelines, go to Security & Compliance > Vulnerability Report.



Vulnerability Report

The Vulnerability Report shows the results of the latest successful pipeline on your project's default branch, as well as vulnerabilities from your latest container scan. Learn more.

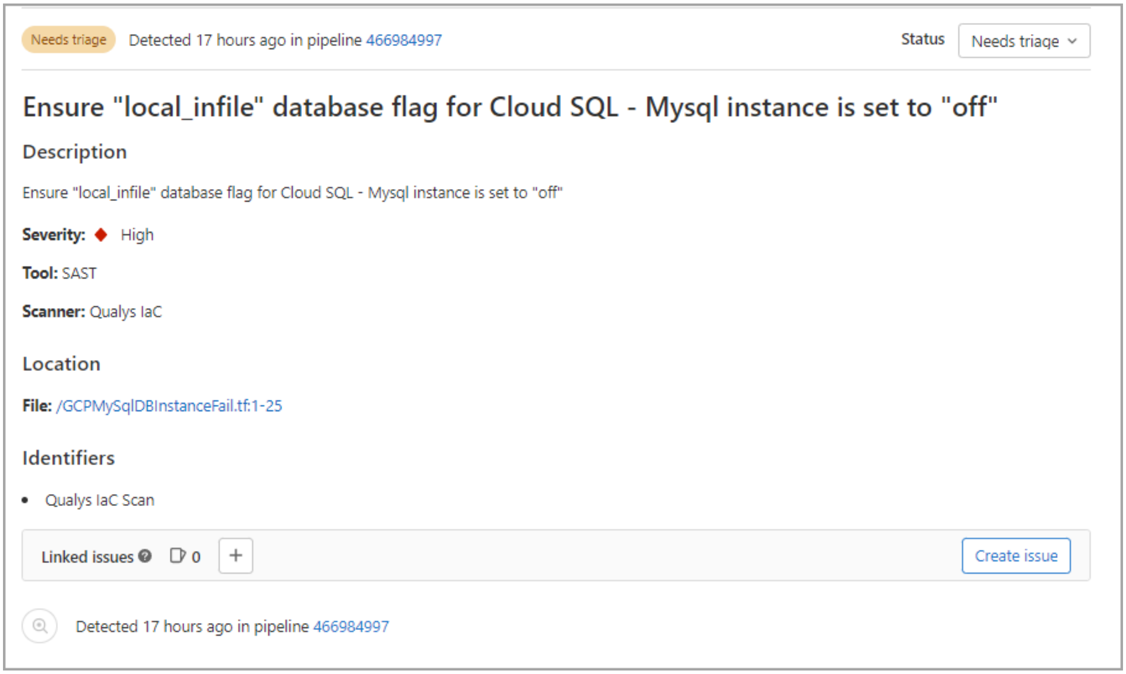
Last updated 7 hours ago #467451901

Critical	High	Medium	Low	Info	Unknown
0	45	25	0	0	2

Status: Needs triage +1 more
Severity: All severities
Tool: All tools
Activity: All activity

□	Detected	Status	↓ Severity	Description	Identifier	Tool	Activity
□	2022-02-09	Needs Triage	◆ High	Ensure "local_infile" database flag for Cloud SQL - Mysql instance is set to "off" /GCPMySqlDBInstanceFail.tf:1	Qualys IaC Scan	SAST	
□	2022-02-09	Needs Triage	◆ High	Ensure that MySQL Database Instance does not allows root login from any Host /GCPMySqlDBInstanceFail.tf:1	Qualys IaC Scan	SAST	
□	2022-02-09	Needs Triage	◆ High	Ensure that Cloud SQL - Mysql database Instances are not open t o the world /GCPMySqlDBInstanceFail.tf:1	Qualys IaC Scan	SAST	
□	2022-02-09	Needs Triage	◆ High	Disable RDP access on Network Security Groups from Internet (A NY IP) /Azure-NSG1.json:7	Qualys IaC Scan	SAST	
□	2022-02-09	Needs Triage	◆ High	Ensure Athena Database is encrypted at rest (default is unencrypt ed) /aws_athena_database.tfplan.json:-	Qualys IaC Scan	SAST	

You can click a vulnerability to view the details of the vulnerability.



Needs triage Detected 17 hours ago in pipeline 466984997

Status: Needs triage

Ensure "local_infile" database flag for Cloud SQL - Mysql instance is set to "off"

Description

Ensure "local_infile" database flag for Cloud SQL - Mysql instance is set to "off"

Severity: ◆ High

Tool: SAST

Scanner: Qualys IaC

Location

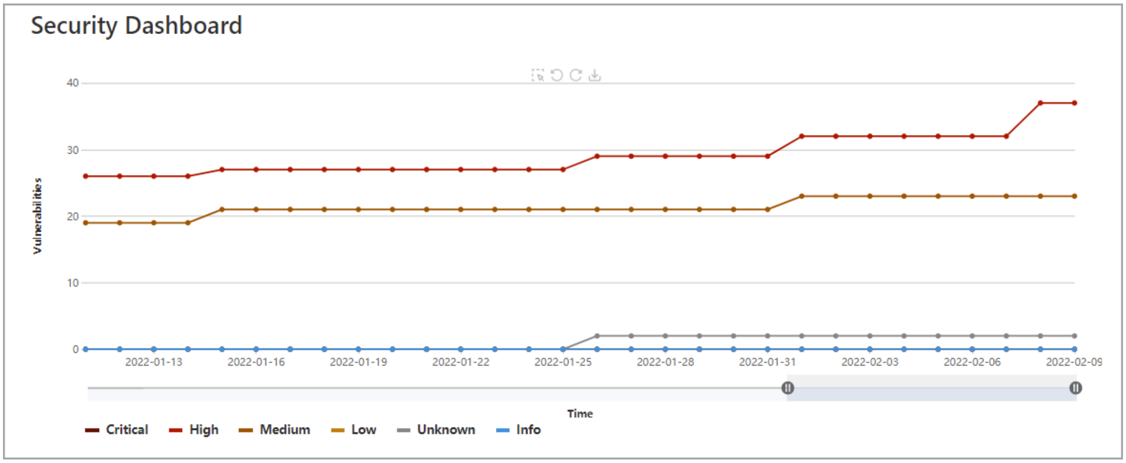
File: /GCPMySqlDBInstanceFail.tf:1-25

Identifiers

- Qualys IaC Scan

Detected 17 hours ago in pipeline 466984997

To view the security dashboard, go to Security & Compliance > Security Dashboard.



For details on elements in the output format, refer to Secure IaC section in CloudView API User Guide.