GitHub actions at Flutter

Action workflows can be enabled by writing a yaml file inside .github/workflows folder of a given repository. These workflows run arbitrary code from GitHub repositories and with read/write permissions in the repository assets. This can be dangerous as anyone with write permissions to the repository can enable workflows using malicious code. To mitigate this only workflows with pinned commits within an allowed list can be executed.

Flutter repositories have workflows enabled with readonly ACLs by default. The ACLs can be overwritten providing specific permissions in the configuration file.

Determining whether a given workflow is secure or not goes well beyond flutter's capacity and it is the responsibility of the person enabling the workflow to diligently check the workflow for any potential security issues.

Adding a new GitHub Actions workflow

To add a new workflow please open a new bug using the ticket queue process. The following data points are required:

- Description/reason to enable this workflow
- workflow repository
- pinned commit

Updating a GitHub Actions workflow

To update an existing workflow please open a new bug using the ticket queue process. The following data points are required:

- Description/reason to update the pinned version
- workflow/old_pinned_version
- workflow/new_pinned_version

flutter/engine and flutter/flutter

flutter/engine please do not add any action workflows to this repository. The preferred way of building and testing is to use LUCI. This allows to plan for scalability, security and maintainability.

flutter/flutter the main use of workflows in this repo is to process bugs, projects, etc. Please do not use action workflows to build, run tests or release artifacts.

Checklist

New workflow:

- Does it have an associated bug?

- Was the workflow/commit added to the allow list? Is the workflow pinned to a given commit?
- If the workflow require write access, is it overriding the ACLs explicitly?
- If the target repository has branch protection, is the configuration using ***secrets.FLUTTERGITHUBBOT_TOKEN*** instead of the default one?
- Is the workflow configured to not run on forks?

Update workflow:

- Does it have an associated bug?
- Was the workflow with old and new commits added to the allowed list?