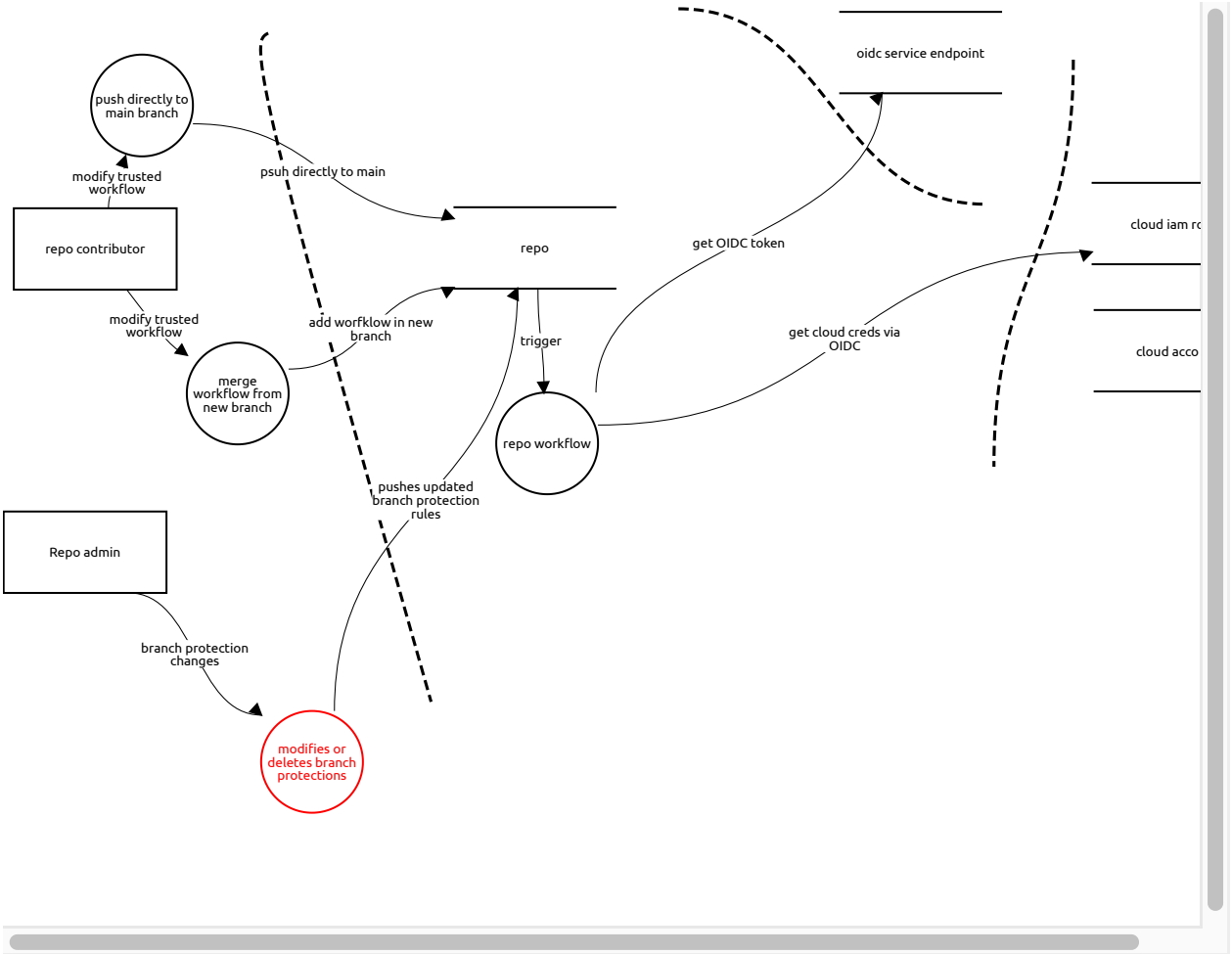
# Threat model report for GitHub Repo Actions/OIDC Threat Model

**Owner:**
jcetina@
**Reviewer:**
**Contributors:**

## High level system description

## Data Flow Diagram




### cloud iam role (Data Store)

**Description:**

#### Cloud credentials issued to unauthorized workflows

*Elevation of privilege, Mitigated, High Priority*

**Description:**
Only designated Actions workflows should be allowed to acquire third party credentials via OIDC

**Mitigation:**
1. Configure the subject claim at the repo or org level to include job_workflow_ref as part of the subject claim. The job_workflow_ref field includes the repo, file path, and branch of the the workflow that initiated the OIDC request.

2. Configure the relying party (e.g. the cloud provider) to only allow credential issuance to the job_workflow_refs that are authorized to acquire credentials (e.g. "job_workflow_ref:octo-org/octo-automation/.github/workflows/oidc.yml@refs/heads/main")

cloud accoun (Data Store)

**Description:**

*No threats listed.*

repo (Data Store)

**Description:**

*No threats listed.*

repo workflow (Process)

**Description:**

*No threats listed.*

trigger (Data Flow)

**Description:**
pr, issue, merge, pull, etc

*No threats listed.*

oidc service endpoint (Data Store)

**Description:**
where the repo gets an OIDC token from

*No threats listed.*

get OIDC token (Data Flow)

**Description:**

*No threats listed.*

get cloud creds via OIDC (Data Flow)

**Description:**

*No threats listed.*

repo contributor (External Actor)

**Description:**
an authorized repo contributor with write access

*No threats listed.*

merge workflow from new branch (Process)

**Description:**

Update protected workflow without approval
*Tampering, Mitigated, High Priority*

**Description:**
A user could modify an existing workflow that is authorized to acquire cloud credentials in order to exploit the trust that the relying party (cloud provider) has placed in the workflow.

**Mitigation:**
Overall, we need to be extra cautious about protecting workflow files in the repo using multiple branch protection features. The appropriate branch protection mitigations are to:

1. Require a PR with at least one reviewer before merging.
2. Dismiss stale pull request approvals when new commits are pushed
3. If code owners is configured, require a review from code owners
4. Disallow bypass of pull requests
5. Require approval of the most recent push
6. (Unsure given #2) - Ignore approving reviews from pull request contributors
7. Do not allow bypassing the above settings
8. Disallow force pushes

modify trusted workflow (Data Flow)

**Description:**

*No threats listed.*

add worfklow in new branch (Data Flow)

**Description:**

*No threats listed.*

push directly to main branch (Process)

**Description:**

Update protected workflow without approval

*Tampering, Mitigated, High Priority*

**Description:**
A user could modify an existing workflow that is authorized to acquire cloud credentials in order to exploit the trust that the relying party (cloud provider) has placed in the workflow.

**Mitigation:**
Overall, we need to be extra cautious about protecting workflow files in the repo using multiple branch protection features. The appropriate branch protection mitigations are to:

1. Require a PR with at least one reviewer before merging.
2. Dismiss stale pull request approvals when new commits are pushed
3. If code owners is configured, require a review from code owners
4. Disallow bypass of pull requests
5. Require approval of the most recent push
6. (Unsure given #2) - Ignore approving reviews from pull request contributors
7. Do not allow bypassing the above settings
8. Disallow force pushes

modify trusted workflow (Data Flow)

**Description:**

*No threats listed.*

psuh directly to main (Data Flow)

**Description:**

*No threats listed.*

Repo admin (External Actor)

**Description:**

*No threats listed.*

modifies or deletes branch protections (Process)

**Description:**

Rogue admin deletes branch protection rules

*Tampering, Open, High Priority*

**Description:**
A rogue admin could delete branch protection rules, thus removing 2 party review requirements for workflows

**Mitigation:**
None

pushes updated branch protection rules (Data Flow)

**Description:**

*No threats listed.*

branch protection changes (Data Flow)

**Description:**

*No threats listed.*