Workshop Guide: Automating Threat Hunting with Detection As Code

References used within this guide:
Getting Started with Detection-as-Code and Chronicle Security Operations (Part 1 of 2)
AI Runbooks for Google SecOps: Security Operations with Model Context Protocol
Building an open ecosystem for AI-driven security with MCP

Table of Contents

Prerequisites

- A GitHub account

(if you're using your local VS Code IDE)

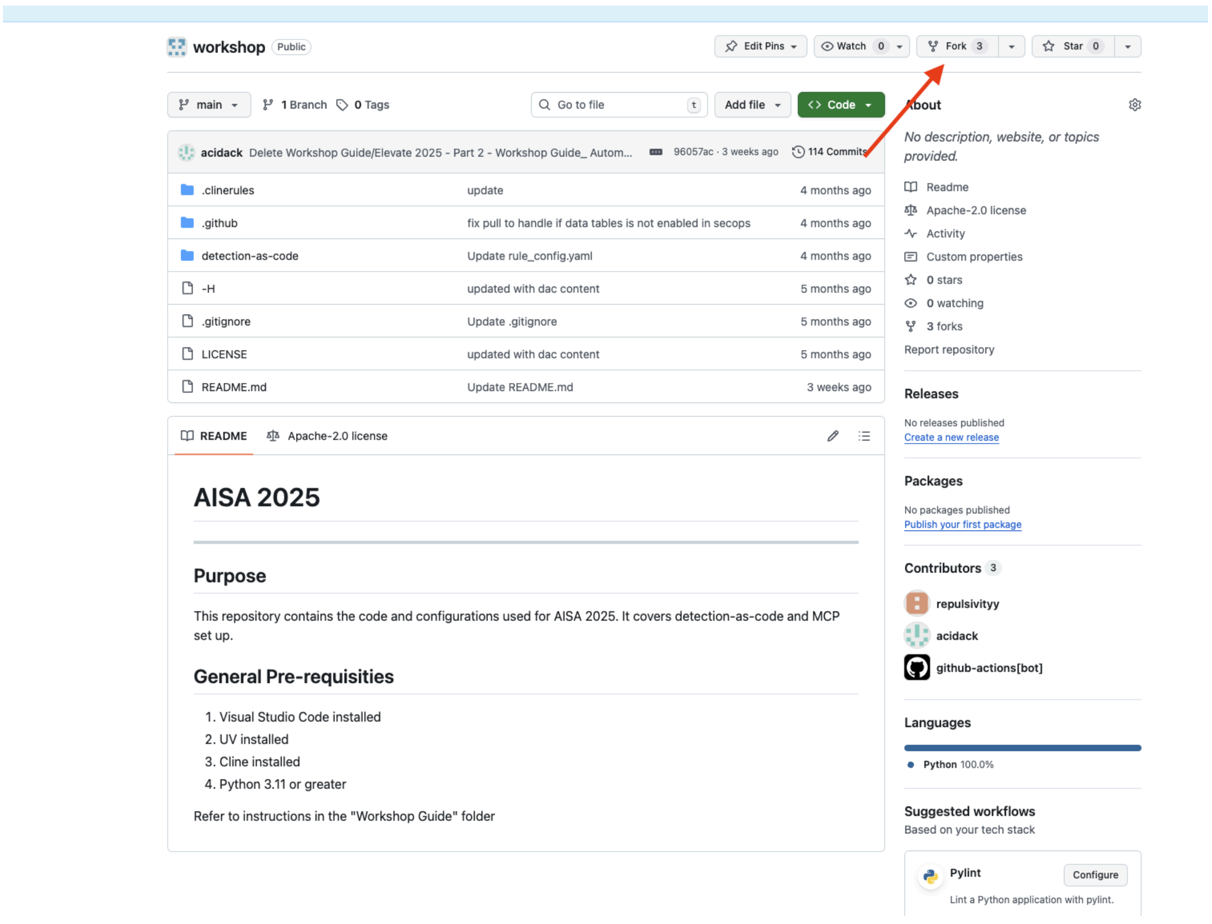
- Visual Studio Code
- If using local VS Code:
    a. Installed in your local terminal:
        i. Python
        ii. uv
        iii. gcloud CLI
        iv. jq
        v. Github cli

Setting up Detection-As-Code on GitHub

Setting up Github

1. Set up (if you don't have one) and log into a Github account

2. Next, back in github start by creating a fork of this repo https://github.com/SumitsWorkshopOrg/workshop into your own repo e.g. *[https://github.com/[YOUR_REPO]/workshop](https://github.com/[YOUR_REPO]/workshop)*



acidack Delete Workshop Guide/Elevate 2025 - Part 2 - Workshop Guide_ Autom... 96057ac · 3 weeks ago 114 Commits

.clinerules	update	4 months ago
.github	fix pull to handle if data tables is not enabled in secops	4 months ago
detection-as-code	Update rule_config.yaml	4 months ago
-H	updated with dac content	5 months ago
.gitignore	Update .gitignore	5 months ago
LICENSE	updated with dac content	5 months ago
README.md	Update README.md	3 weeks ago

README Apache-2.0 license

AISA 2025

Purpose

This repository contains the code and configurations used for AISA 2025. It covers detection-as-code and MCP set up.

General Pre-requisities

1. Visual Studio Code installed
2. UV installed
3. Cline installed
4. Python 3.11 or greater

Refer to instructions in the "Workshop Guide" folder

About

No description, website, or topics provided.

Readme
Apache-2.0 license
Activity
Custom properties
0 stars
0 watching
3 forks
Report repository

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Contributors 3

repulsivityy
acidack
github-actions[bot]

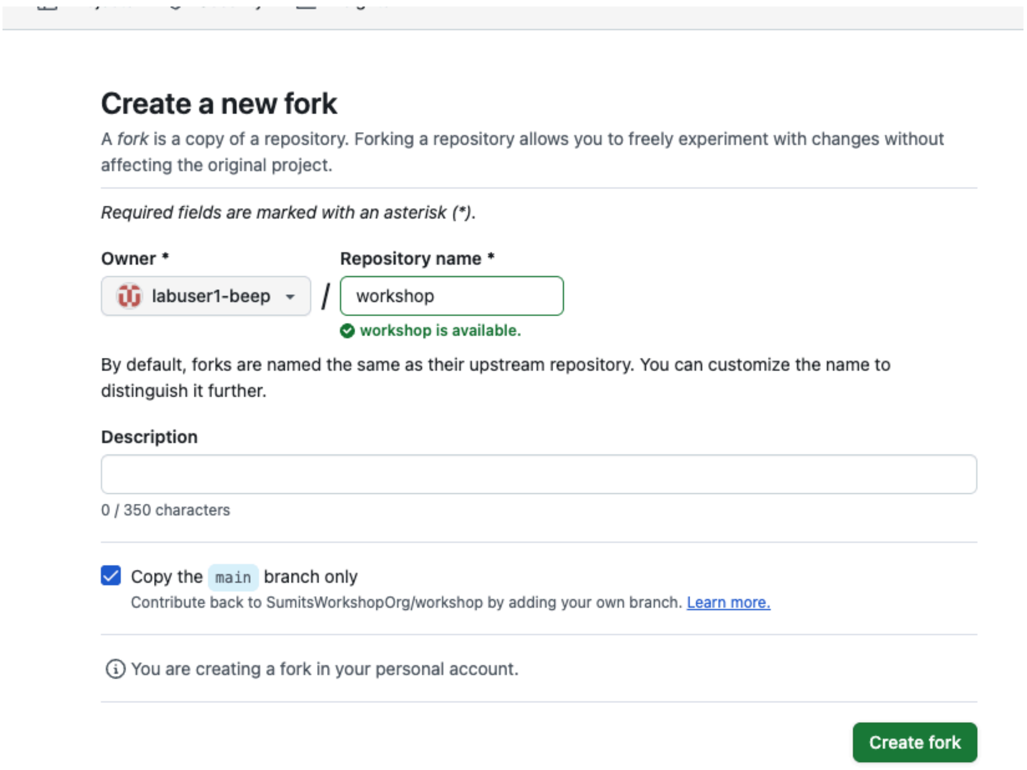
Languages

Python 100.0%

Suggested workflows
Based on your tech stack

Pylint Configure
Lint a Python application with pylint.

TLP:GREEN



Create a new fork

A *fork* is a copy of a repository. Forking a repository allows you to freely experiment with changes without affecting the original project.

Required fields are marked with an asterisk (*).

Owner *: labuser1-beep / Repository name *: workshop

workshop is available.

By default, forks are named the same as their upstream repository. You can customize the name to distinguish it further.

Description

0 / 350 characters

[✓] Copy the `main` branch only

Contribute back to SumitsWorkshopOrg/workshop by adding your own branch. Learn more.

You are creating a fork in your personal account.

3. *At this point, organizers will permit access based on Github user accounts that have forked the repo above (please be patient till this step is completed)*

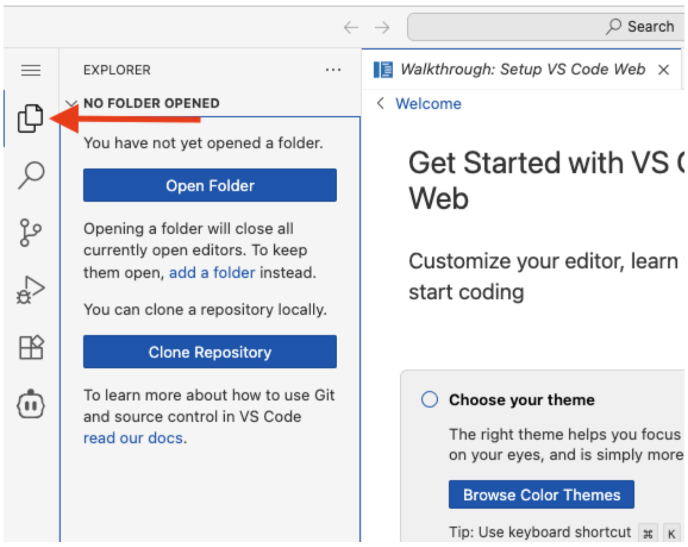
TLP:GREEN

Accessing Web based VS Code

1. Open VS Code via https://code.patesumi.dev/?ew=true

2. *(Organizer to allocate) username / password*

3. Select the **Explorer** icon in the menu



Search

EXPLORER

NO FOLDER OPENED

You have not yet opened a folder.

Open Folder

Opening a folder will close all currently open editors. To keep them open, add a folder instead.

You can clone a repository locally.

Clone Repository

To learn more about how to use Git and source control in VS Code read our docs.

Walkthrough: Setup VS Code Web

Welcome

Get Started with VS C
Web

Customize your editor, learn
start coding

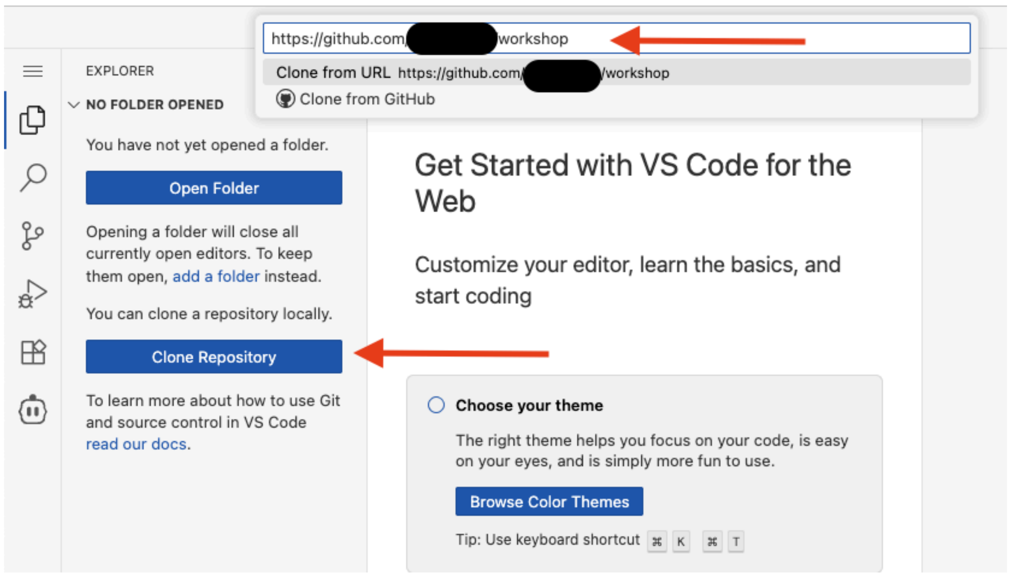
Choose your theme

The right theme helps you focus
on your eyes, and is simply more

Browse Color Themes

Tip: Use keyboard shortcut ⌘ K

4. In VS Code, select "**Clone Repository**" of YOUR repo you just forked



https://github.com/[redacted]workshop

Clone from URL https://github.com/[redacted]/workshop

Clone from GitHub

EXPLORER

NO FOLDER OPENED

You have not yet opened a folder.

Open Folder

Opening a folder will close all currently open editors. To keep them open, add a folder instead.

You can clone a repository locally.

Clone Repository

To learn more about how to use Git and source control in VS Code read our docs.

Get Started with VS Code for the Web

Customize your editor, learn the basics, and start coding

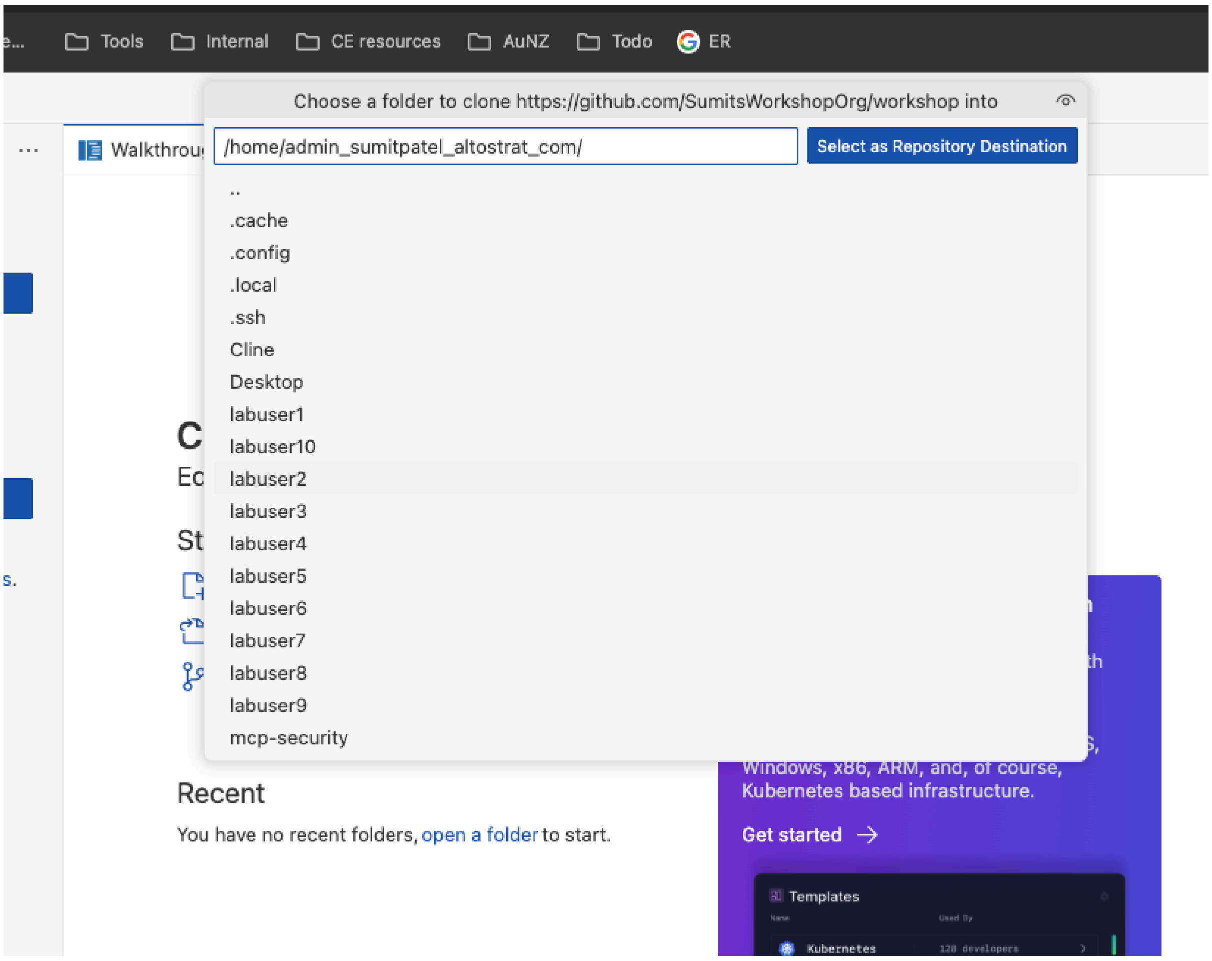
Choose your theme

The right theme helps you focus on your code, is easy on your eyes, and is simply more fun to use.

Browse Color Themes

Tip: Use keyboard shortcut ⌘ K ⌘ T

5. Choose a folder to clone to (use your allocated username folder name)



Choose a folder to clone https://github.com/SumitsWorkshopOrg/workshop into

/home/admin_sumitpatel_altostrat_com/ Select as Repository Destination

..
.cache
.config
.local
.ssh
Cline
Desktop
labuser1
labuser10
labuser2
labuser3
labuser4
labuser5
labuser6
labuser7
labuser8
labuser9
mcp-security

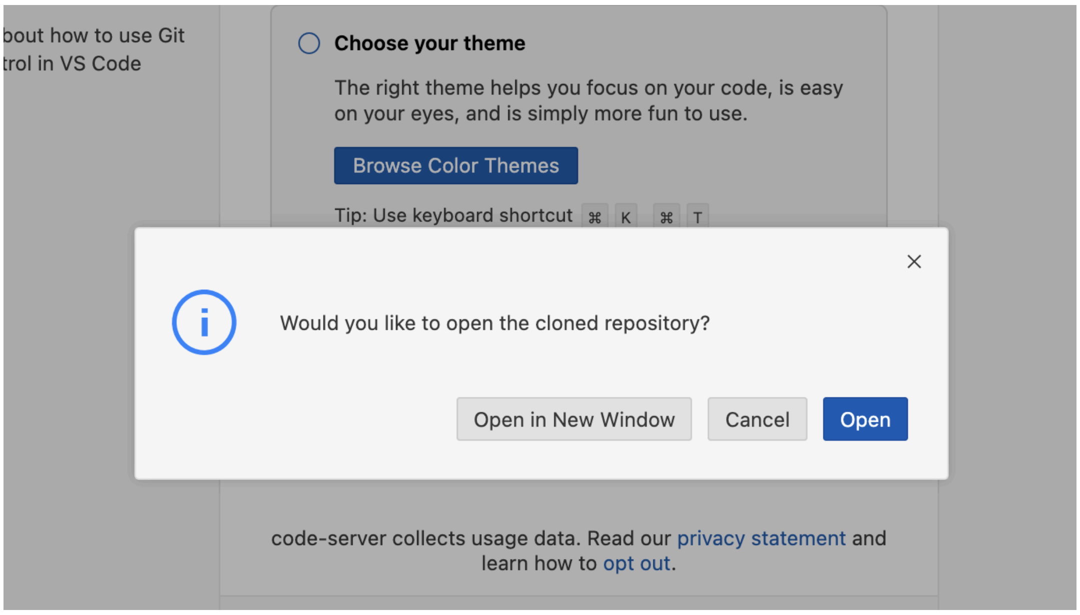
Recent

You have no recent folders, open a folder to start.

Windows, x86, ARM, and, of course, Kubernetes based infrastructure.

Get started

6. Choose “Open”



Choose your theme

The right theme helps you focus on your code, is easy on your eyes, and is simply more fun to use.

Browse Color Themes

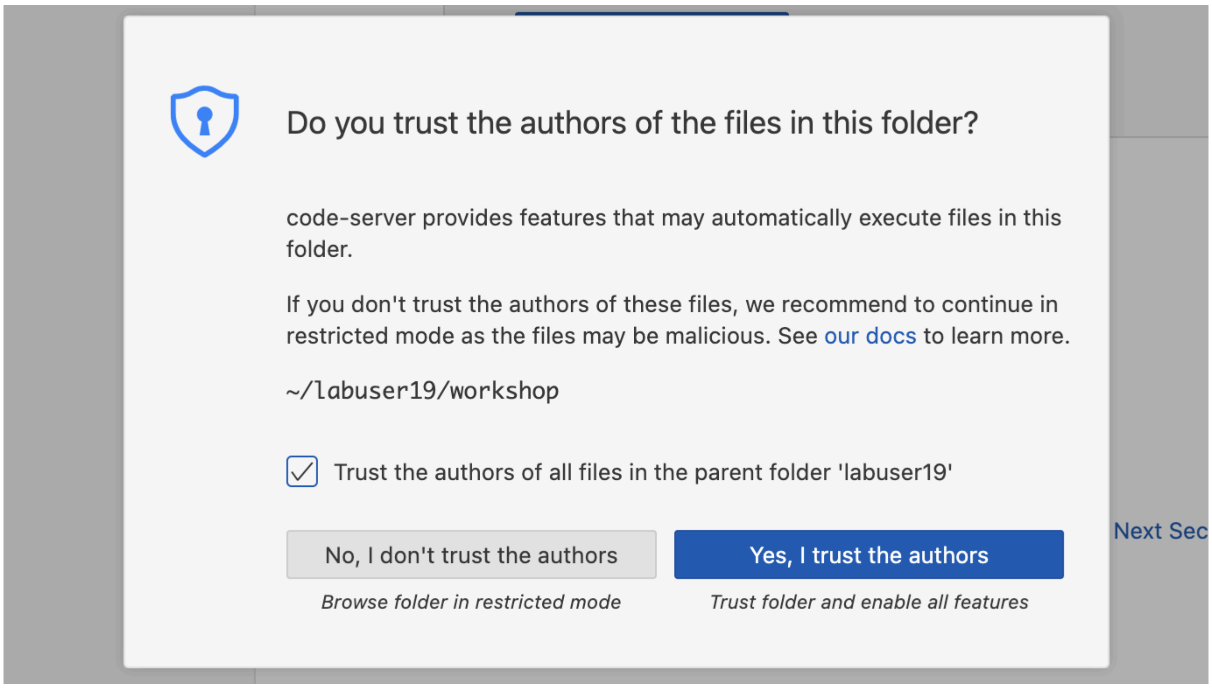
Tip: Use keyboard shortcut ⌘ K ⌘ T

Would you like to open the cloned repository?

Open in New Window Cancel Open

code-server collects usage data. Read our privacy statement and learn how to opt out.

7. Choose **Yes, I trust the authors**



Do you trust the authors of the files in this folder?

code-server provides features that may automatically execute files in this folder.

If you don't trust the authors of these files, we recommend to continue in restricted mode as the files may be malicious. See our docs to learn more.

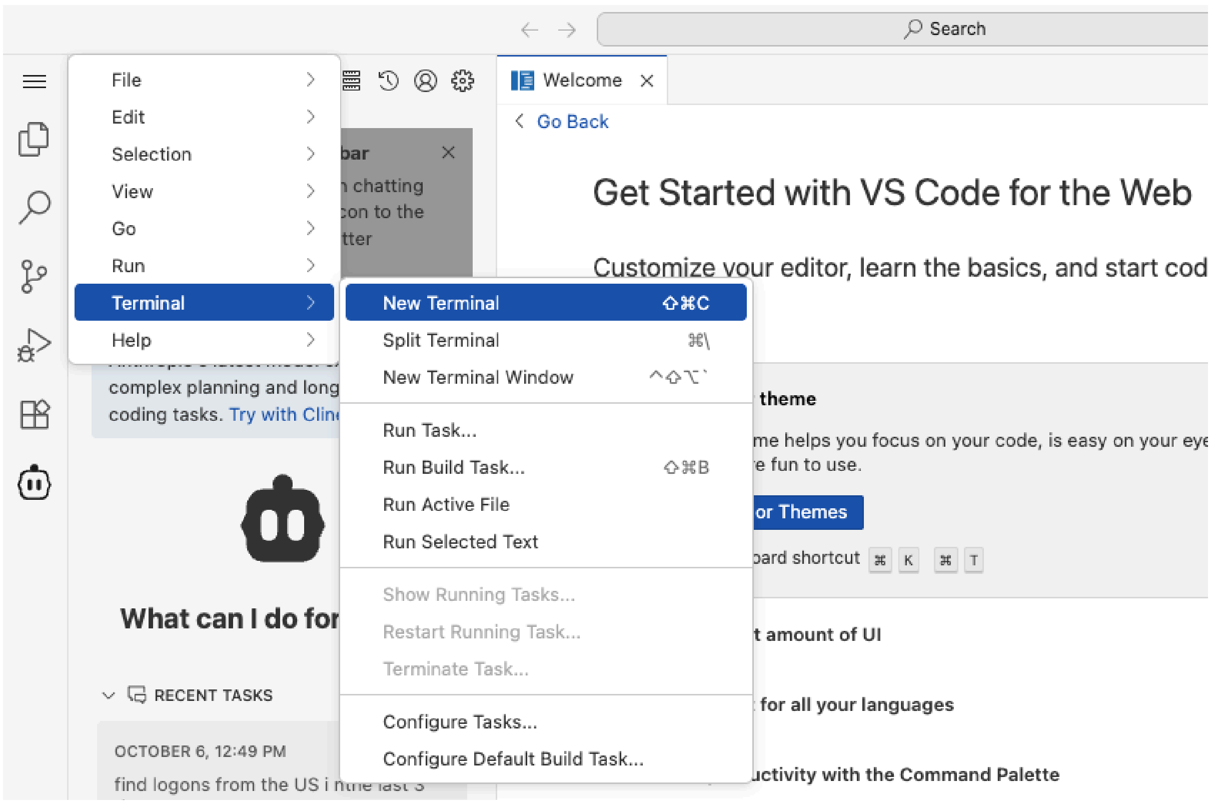
~/labuser19/workshop

☑ Trust the authors of all files in the parent folder 'labuser19'

No, I don't trust the authors
Browse folder in restricted mode
Yes, I trust the authors
Trust folder and enable all features
Next Sec

8. Enter your GitHub details so you can commit and push changes

a) Open New terminal - menu, **Terminal - New Terminal**

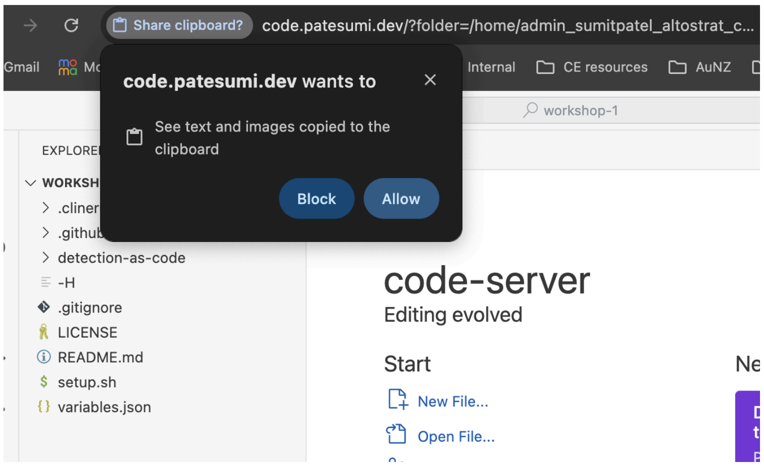


b) Use your name & email you used for GitHub.

Enter the following:

```
git config --global user.name "Your Name"
git config --global user.email "youremail@example.com"
```

Note: you may be asked to allow clipboard - choose Allow.



code.patesumi.dev wants to

See text and images copied to the clipboard

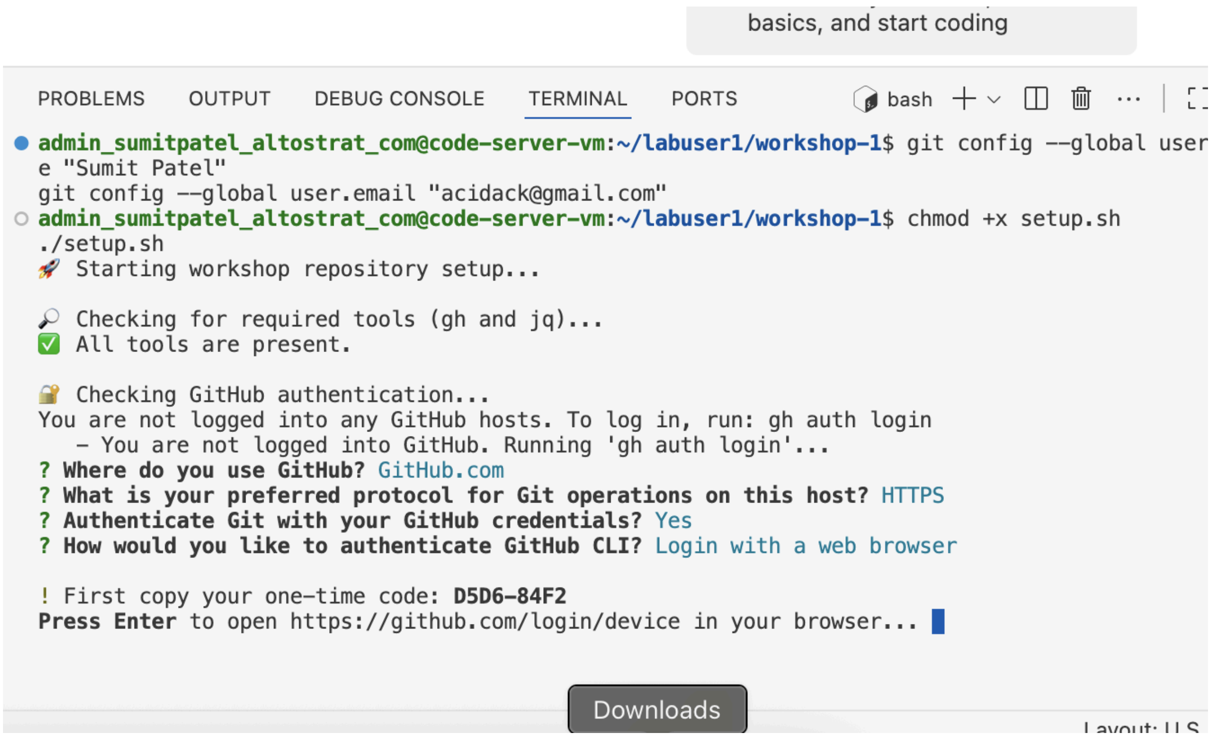
Block Allow

8. **Run the Setup Script:** This script will check for required tools and automatically set up all the necessary GitHub Actions variables in your forked repository.

a) In terminal enter:

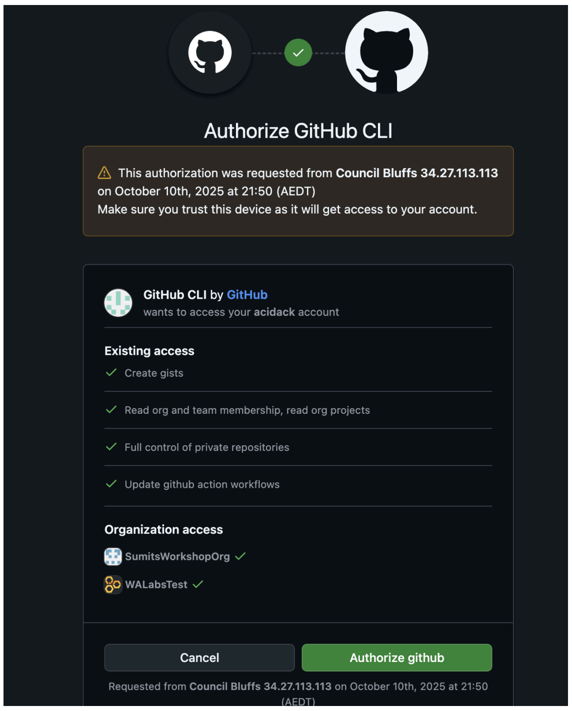
```
chmod +x setup.sh
./setup.sh
```

b) Authenticate when asked (***Github.com**, HTTPS, Yes, Login with a browser*) :



```
admin_sumitpatel_altostrat_com@code-server-vm:~/labuser1/workshop-1$ git config --global user
e "Sumit Patel"
git config --global user.email "acidack@gmail.com"
admin_sumitpatel_altostrat_com@code-server-vm:~/labuser1/workshop-1$ chmod +x setup.sh
./setup.sh
🚀 Starting workshop repository setup...

🔎 Checking for required tools (gh and jq)...
✅ All tools are present.

🔐 Checking GitHub authentication...
You are not logged into any GitHub hosts. To log in, run: gh auth login
   - You are not logged into GitHub. Running 'gh auth login'...
? Where do you use GitHub? GitHub.com
? What is your preferred protocol for Git operations on this host? HTTPS
? Authenticate Git with your GitHub credentials? Yes
? How would you like to authenticate GitHub CLI? Login with a web browser

! First copy your one-time code: D5D6-84F2
Press Enter to open https://github.com/login/device in your browser...
```

c) **Authorize github** with the one-time code



Authorize GitHub CLI

⚠ This authorization was requested from **Council Bluffs 34.27.113.113** on October 10th, 2025 at 21:50 (AEDT)
Make sure you trust this device as it will get access to your account.

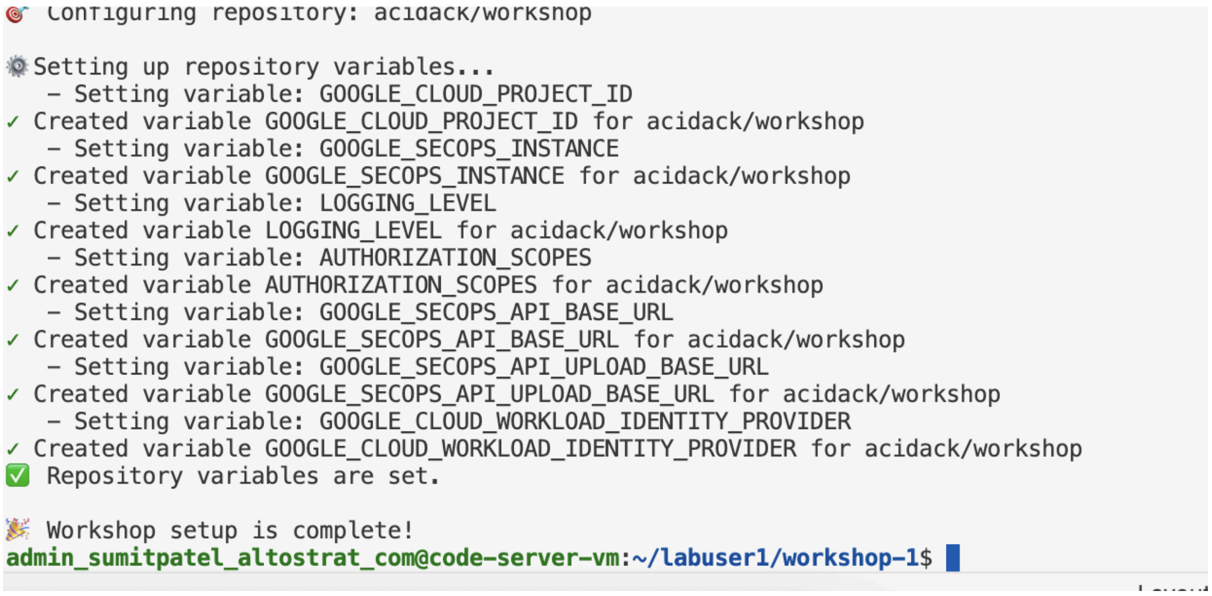
GitHub CLI by GitHub
wants to access your **acidack** account

Existing access
✓ Create gists
✓ Read org and team membership, read org projects
✓ Full control of private repositories
✓ Update github action workflows

Organization access
SumitsWorkshopOrg ✓
WALabsTest ✓

Requested from **Council Bluffs 34.27.113.113** on October 10th, 2025 at 21:50 (AEDT)

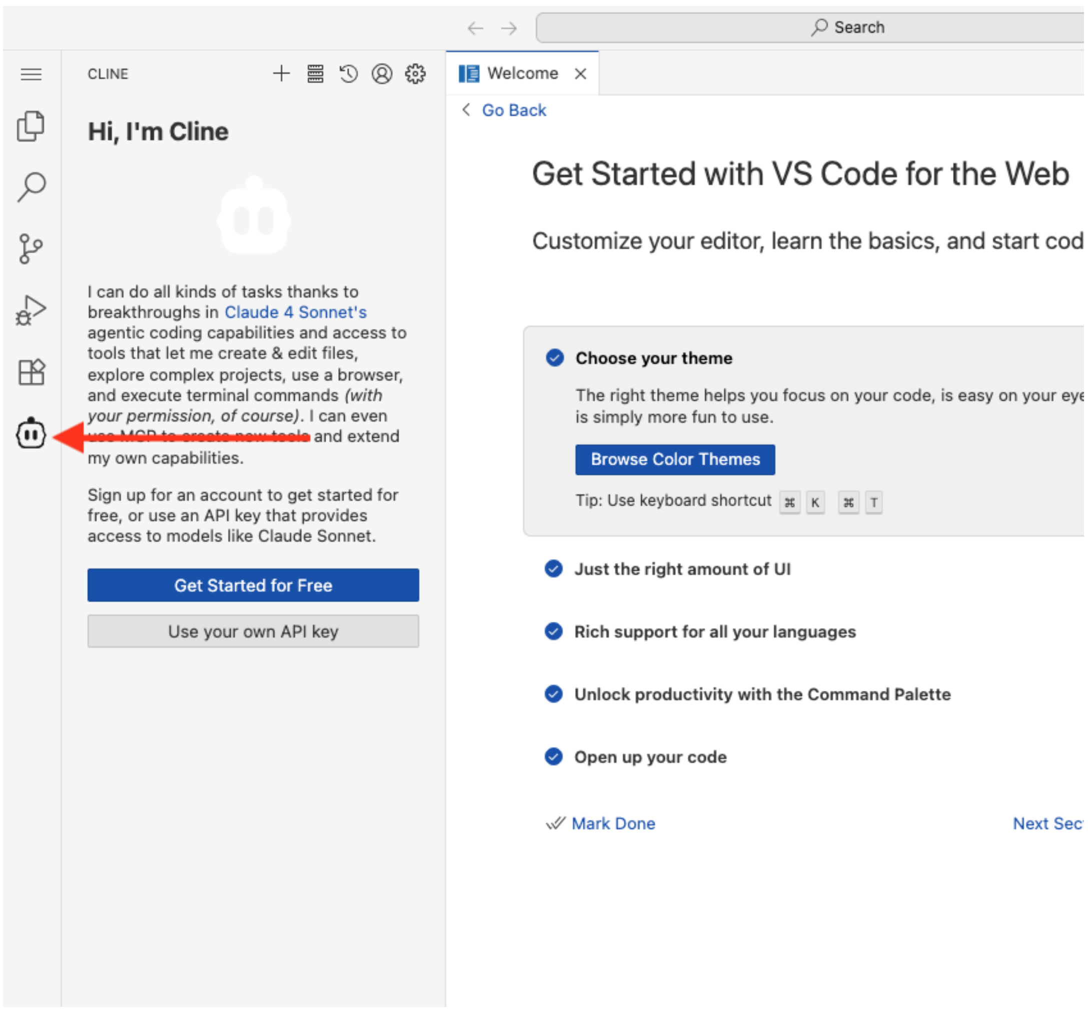
d) If successful it should have created the variables in your github repo



```
🎯 Configuring repository: acidack/workshop

⚙️Setting up repository variables...
   - Setting variable: GOOGLE_CLOUD_PROJECT_ID
✓ Created variable GOOGLE_CLOUD_PROJECT_ID for acidack/workshop
   - Setting variable: GOOGLE_SECOPS_INSTANCE
✓ Created variable GOOGLE_SECOPS_INSTANCE for acidack/workshop
   - Setting variable: LOGGING_LEVEL
✓ Created variable LOGGING_LEVEL for acidack/workshop
   - Setting variable: AUTHORIZATION_SCOPES
✓ Created variable AUTHORIZATION_SCOPES for acidack/workshop
   - Setting variable: GOOGLE_SECOPS_API_BASE_URL
✓ Created variable GOOGLE_SECOPS_API_BASE_URL for acidack/workshop
   - Setting variable: GOOGLE_SECOPS_API_UPLOAD_BASE_URL
✓ Created variable GOOGLE_SECOPS_API_UPLOAD_BASE_URL for acidack/workshop
   - Setting variable: GOOGLE_CLOUD_WORKLOAD_IDENTITY_PROVIDER
✓ Created variable GOOGLE_CLOUD_WORKLOAD_IDENTITY_PROVIDER for acidack/workshop
✅ Repository variables are set.

🎉 Workshop setup is complete!
admin_sumitpatel_altostrat_com@code-server-vm:~/labuser1/workshop-1$
```

Setting up AI on VS Code

1. Select Cline extension from menu on left



CLINE

Hi, I'm Cline

I can do all kinds of tasks thanks to breakthroughs in Claude 4 Sonnet's agentic coding capabilities and access to tools that let me create & edit files, explore complex projects, use a browser, and execute terminal commands *(with your permission, of course)*. I can even ~~use MCP to create new tools~~ and extend my own capabilities.

Sign up for an account to get started for free, or use an API key that provides access to models like Claude Sonnet.

Get Started with VS Code for the Web

Customize your editor, learn the basics, and start cod

Choose your theme

The right theme helps you focus on your code, is easy on your eye is simply more fun to use.

Tip: Use keyboard shortcut ⌘ K ⌘ T

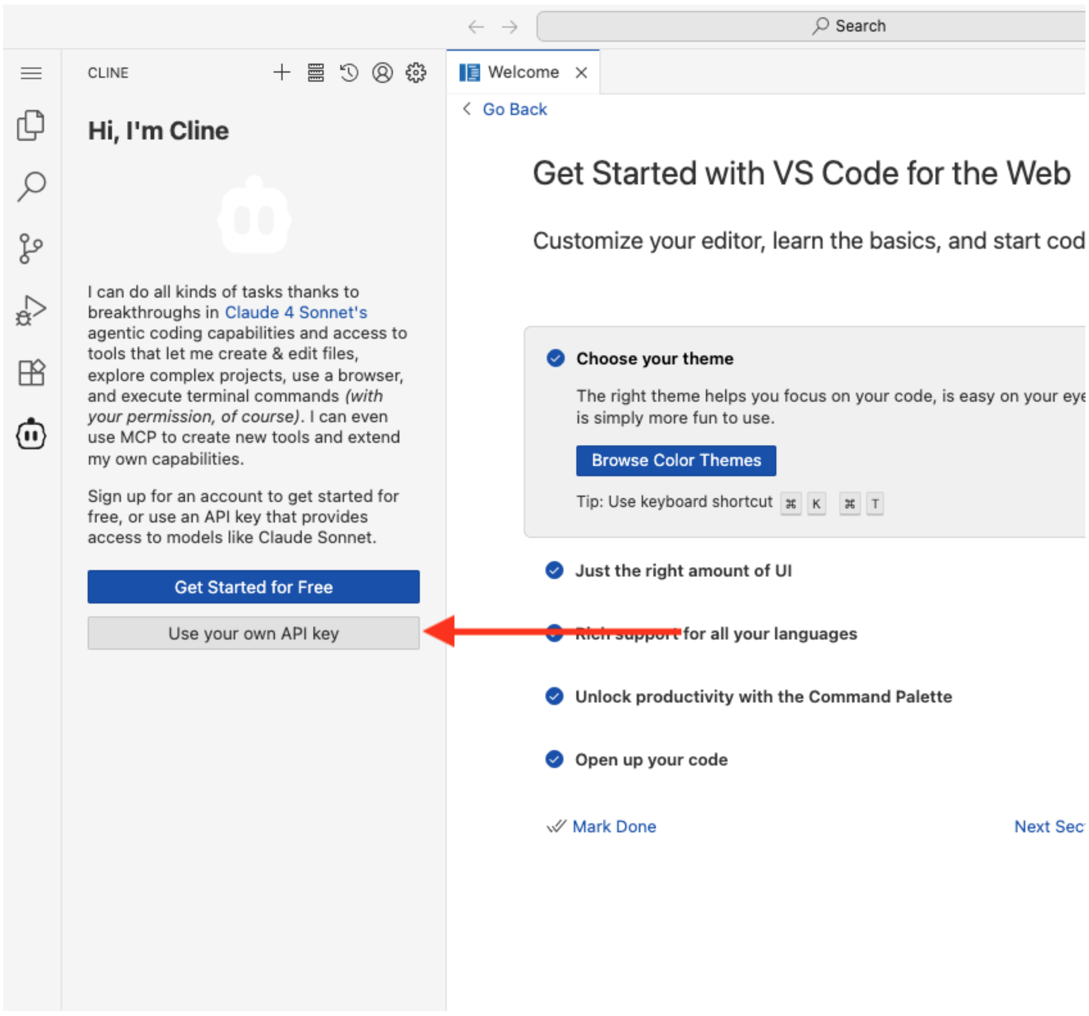
Just the right amount of UI

Rich support for all your languages

Unlock productivity with the Command Palette

Open up your code

2. Select “**Use your own API key**”



Hi, I'm Cline

I can do all kinds of tasks thanks to breakthroughs in Claude 4 Sonnet's agentic coding capabilities and access to tools that let me create & edit files, explore complex projects, use a browser, and execute terminal commands *(with your permission, of course)*. I can even use MCP to create new tools and extend my own capabilities.

Sign up for an account to get started for free, or use an API key that provides access to models like Claude Sonnet.

Get Started with VS Code for the Web

Customize your editor, learn the basics, and start cod

Choose your theme

The right theme helps you focus on your code, is easy on your eye is simply more fun to use.

Tip: Use keyboard shortcut ⌘ K ⌘ T

Just the right amount of UI

Rich support for all your languages

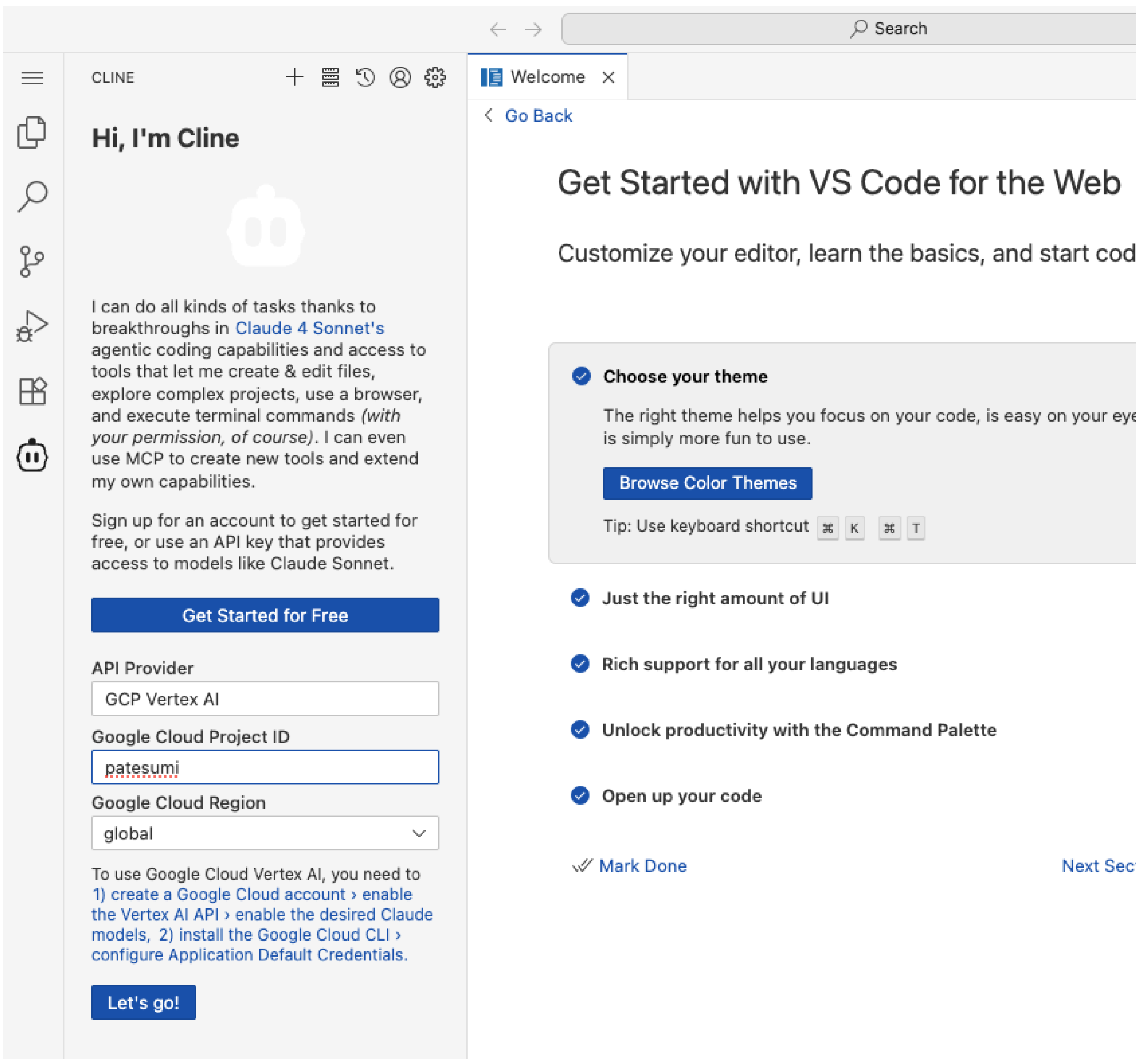
Unlock productivity with the Command Palette

Open up your code

a) Select “**GCP Vertex AI**”, project ID: **patesumi**, region: **global**

b) Choose **“Lets go!”**

TLP:GREEN



CLINE

Hi, I'm Cline

I can do all kinds of tasks thanks to breakthroughs in Claude 4 Sonnet's agentic coding capabilities and access to tools that let me create & edit files, explore complex projects, use a browser, and execute terminal commands *(with your permission, of course)*. I can even use MCP to create new tools and extend my own capabilities.

Sign up for an account to get started for free, or use an API key that provides access to models like Claude Sonnet.

Get Started for Free

API Provider: GCP Vertex AI

Google Cloud Project ID: patesumi

Google Cloud Region: global

To use Google Cloud Vertex AI, you need to 1) create a Google Cloud account › enable the Vertex AI API › enable the desired Claude models, 2) install the Google Cloud CLI › configure Application Default Credentials.

Let's go!

Welcome

Go Back

Get Started with VS Code for the Web

Customize your editor, learn the basics, and start cod

Choose your theme

The right theme helps you focus on your code, is easy on your eye is simply more fun to use.

Browse Color Themes

Tip: Use keyboard shortcut ⌘ K ⌘ T

Just the right amount of UI

Rich support for all your languages

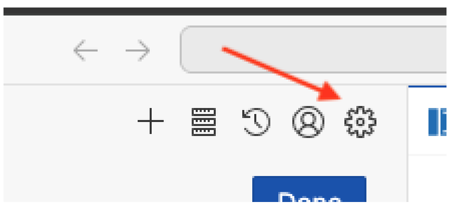
Unlock productivity with the Command Palette

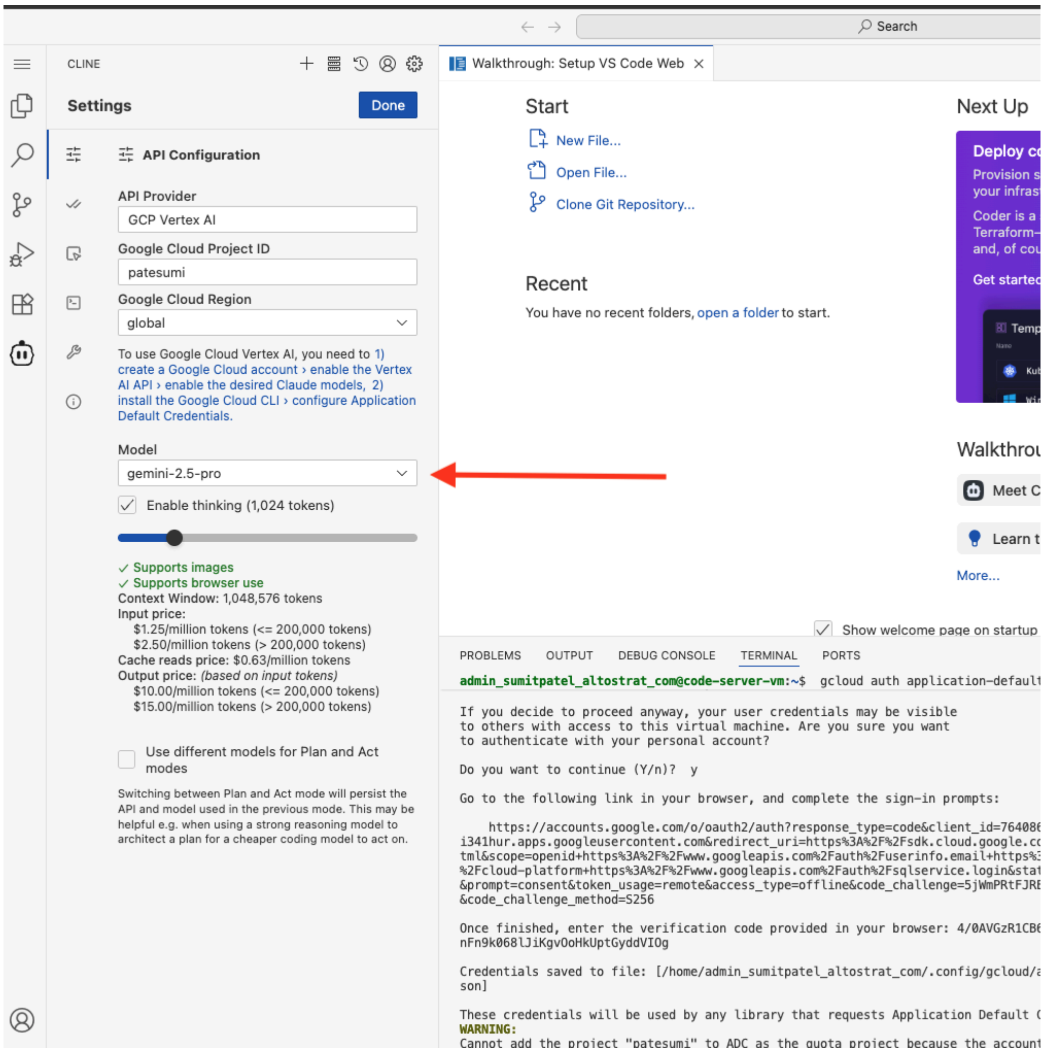
Open up your code

Mark Done

Next Sec

3. Next, select the Settings icon and select **gemini-2.5-pro** as the Model





Settings

Done

API Configuration

API Provider

GCP Vertex AI

Google Cloud Project ID

patesumi

Google Cloud Region

global

To use Google Cloud Vertex AI, you need to 1) create a Google Cloud account › enable the Vertex AI API › enable the desired Claude models, 2) install the Google Cloud CLI › configure Application Default Credentials.

Model

gemini-2.5-pro

✓ Enable thinking (1,024 tokens)

✓ Supports images
✓ Supports browser use
Context Window: 1,048,576 tokens
Input price:
$1.25/million tokens (<= 200,000 tokens)
$2.50/million tokens (> 200,000 tokens)
Cache reads price: $0.63/million tokens
Output price: *(based on input tokens)*
$10.00/million tokens (<= 200,000 tokens)
$15.00/million tokens (> 200,000 tokens)

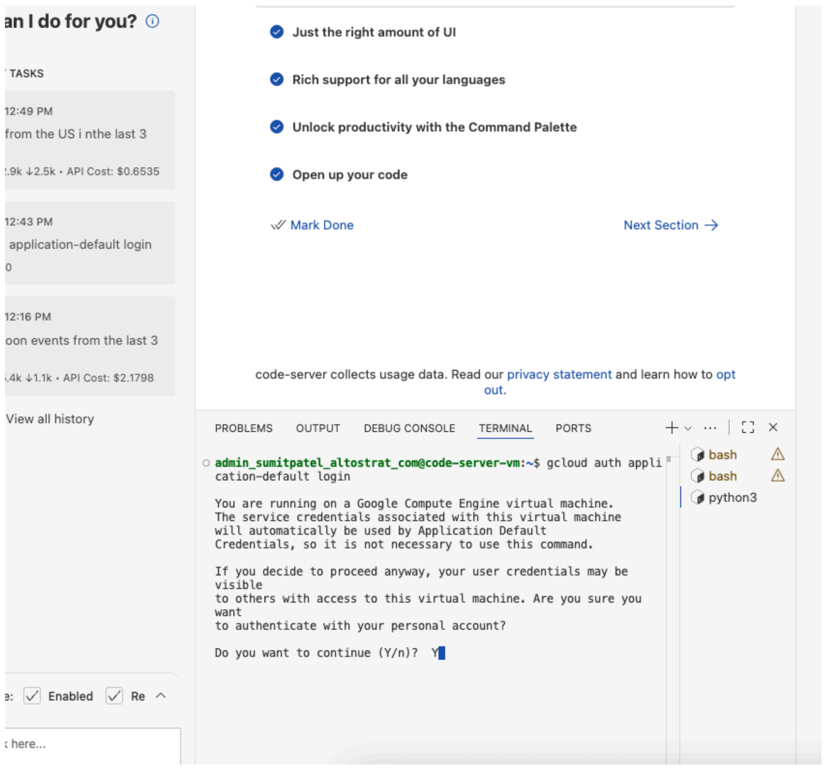
☐ Use different models for Plan and Act modes

Switching between Plan and Act mode will persist the API and model used in the previous mode. This may be helpful e.g. when using a strong reasoning model to architect a plan for a cheaper coding model to act on.

```
admin_sumitpatel_altostrat_com@code-server-vm:~$  gcloud auth application-default

If you decide to proceed anyway, your user credentials may be visible
to others with access to this virtual machine. Are you sure you want
to authenticate with your personal account?

Do you want to continue (Y/n)?  y

Go to the following link in your browser, and complete the sign-in prompts:

    https://accounts.google.com/o/oauth2/auth?response_type=code&client_id=76408
i341hur.apps.googleusercontent.com&redirect_uri=https%3A%2F%2Fsdk.cloud.google.c
tml&scope=openid+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%
%2Fcloud-platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fsqlservice.login&sta
&prompt=consent&token_usage=remote&access_type=offline&code_challenge=5jWmPRtFJR
&code_challenge_method=S256

Once finished, enter the verification code provided in your browser: 4/0AVGzR1CB
nFn9k068lJiKgvOoHkUptGyddVIOg

Credentials saved to file: [/home/admin_sumitpatel_altostrat_com/.config/gcloud/
son]

These credentials will be used by any library that requests Application Default
WARNING:
Cannot add the project "patesumi" to ADC as the quota project because the account
```

4. Go back to your Terminal. Type `gcloud auth login`

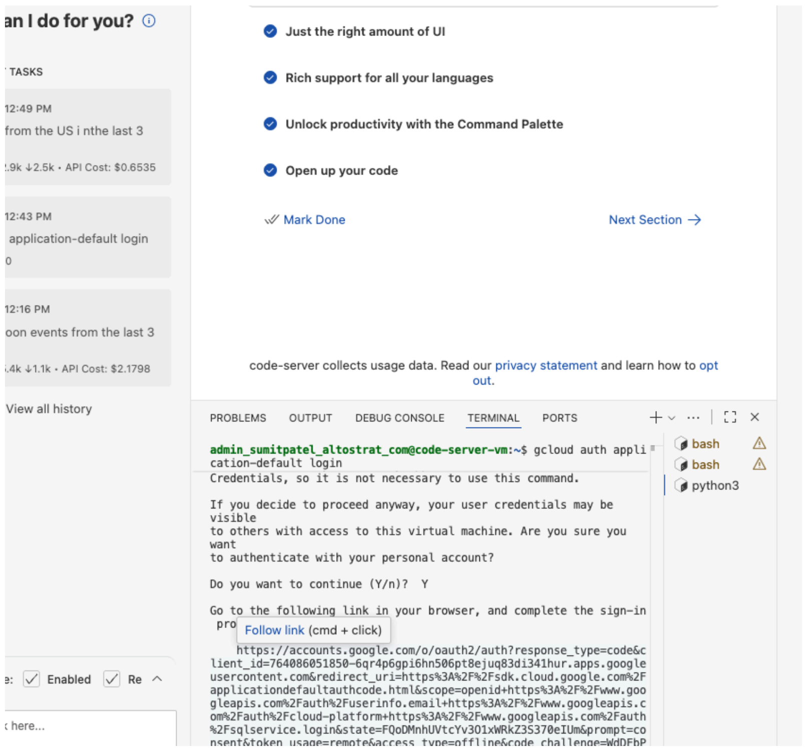
   Hit enter, then type Y


an I do for you?
TASKS
12:49 PM
from the US i nthe last 3
.9k ↓2.5k • API Cost: $0.6535
12:43 PM
application-default login
0
12:16 PM
oon events from the last 3
.4k ↓1.1k • API Cost: $2.1798
View all history
e: Enabled Re
here...
Just the right amount of UI
Rich support for all your languages
Unlock productivity with the Command Palette
Open up your code
Mark Done
Next Section →
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
bash
bash
python3

code-server collects usage data. Read our privacy statement and learn how to opt out.

```
admin_sumitpatel_altostrat_com@code-server-vm:~$ gcloud auth appli
cation-default login

You are running on a Google Compute Engine virtual machine.
The service credentials associated with this virtual machine
will automatically be used by Application Default
Credentials, so it is not necessary to use this command.

If you decide to proceed anyway, your user credentials may be
visible
to others with access to this virtual machine. Are you sure you
want
to authenticate with your personal account?

Do you want to continue (Y/n)?  Y
```

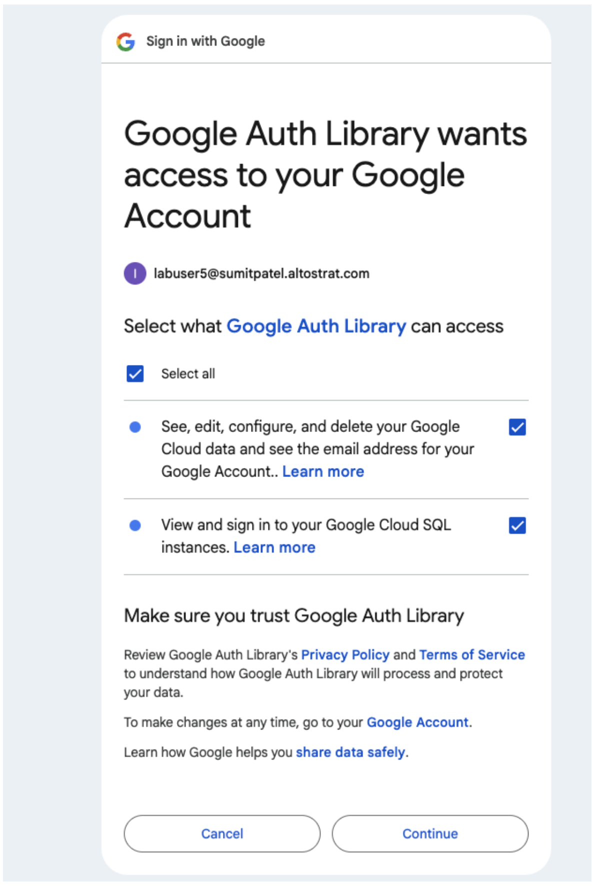
5. Open the web link


an I do for you?
TASKS
12:49 PM
from the US i nthe last 3
.9k ↓2.5k • API Cost: $0.6535
12:43 PM
application-default login
0
12:16 PM
oon events from the last 3
.4k ↓1.1k • API Cost: $2.1798
View all history
e: Enabled Re
here...
Just the right amount of UI
Rich support for all your languages
Unlock productivity with the Command Palette
Open up your code
Mark Done
Next Section →
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
bash
bash
python3
Follow link (cmd + click)

code-server collects usage data. Read our privacy statement and learn how to opt out.

```
admin_sumitpatel_altostrat_com@code-server-vm:~$ gcloud auth appli
cation-default login
Credentials, so it is not necessary to use this command.

If you decide to proceed anyway, your user credentials may be
visible
to others with access to this virtual machine. Are you sure you
want
to authenticate with your personal account?

Do you want to continue (Y/n)?  Y

Go to the following link in your browser, and complete the sign-in
 pro

    https://accounts.google.com/o/oauth2/auth?response_type=code&c
lient_id=764086051850-6qr4p6gpi6hn506pt8ejuq83di341hur.apps.google
usercontent.com&redirect_uri=https%3A%2F%2Fsdk.cloud.google.com%2F
applicationdefaultauthcode.html&scope=openid+https%3A%2F%2Fwww.goo
gleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.c
om%2Fauth%2Fcloud-platform+https%3A%2F%2Fwww.googleapis.com%2Fauth
%2Fsqlservice.login&state=FQoDMnhUVtcYv3O1xWRkZ3S370eIUm&prompt=co
nsent&token_usage=remote&access_type=offline&code_challenge=WdDFbP
```

6. Sign in with your credentials from step 1, tick **Select all** and continue



Google Auth Library wants access to your Google Account

labuser5@sumitpatel.altostrat.com

Select what Google Auth Library can access

[✓] Select all

- See, edit, configure, and delete your Google Cloud data and see the email address for your Google Account.. Learn more [✓]
- View and sign in to your Google Cloud SQL instances. Learn more [✓]

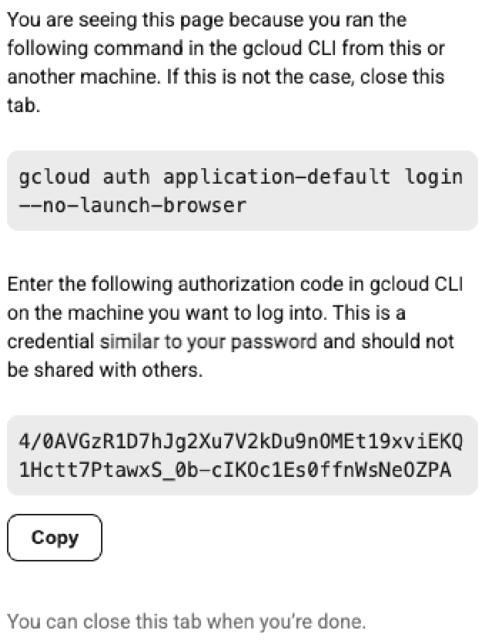
Make sure you trust Google Auth Library

Review Google Auth Library's Privacy Policy and Terms of Service to understand how Google Auth Library will process and protect your data.

To make changes at any time, go to your Google Account.

Learn how Google helps you share data safely.

7. Copy the unique code


You are seeing this page because you ran the following command in the gcloud CLI from this or another machine. If this is not the case, close this tab.

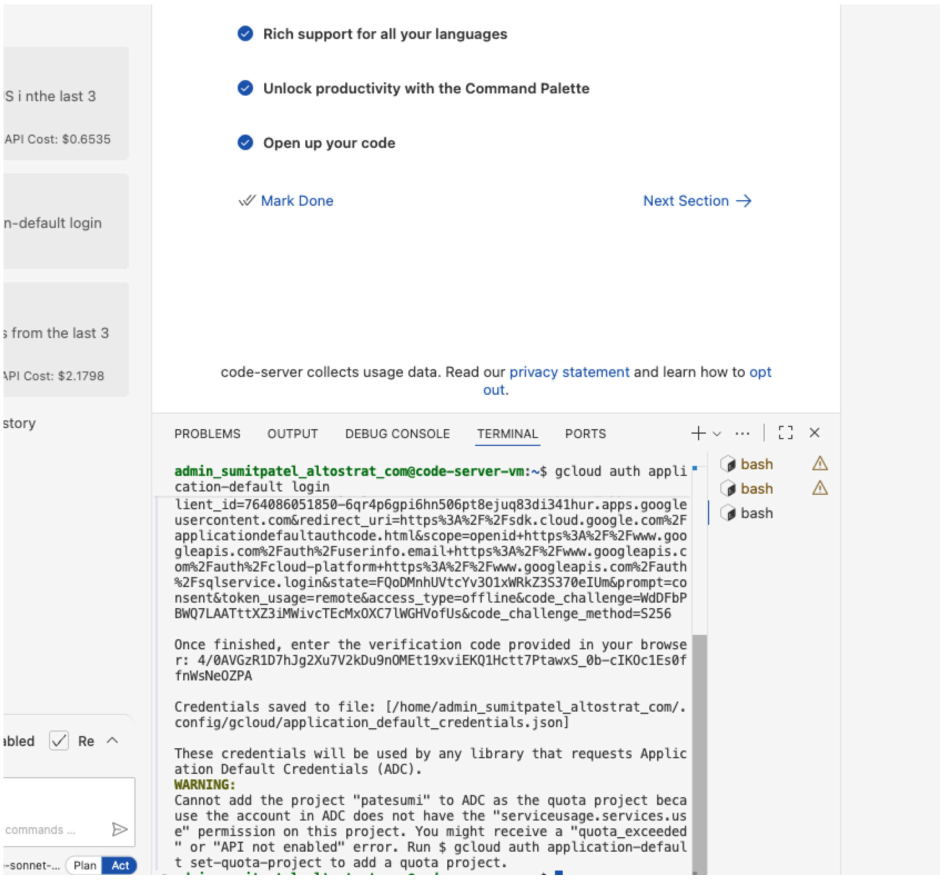
```
gcloud auth application-default login
--no-launch-browser
```

Enter the following authorization code in gcloud CLI on the machine you want to log into. This is a credential similar to your password and should not be shared with others.

```
4/0AVGzR1D7hJg2Xu7V2kDu9nOMEt19xviEKQ
1Hctt7PtawxS_0b-cIKOc1Es0ffnWsNeOZPA
```

You can close this tab when you're done.

8. Copy & paste it back in terminal



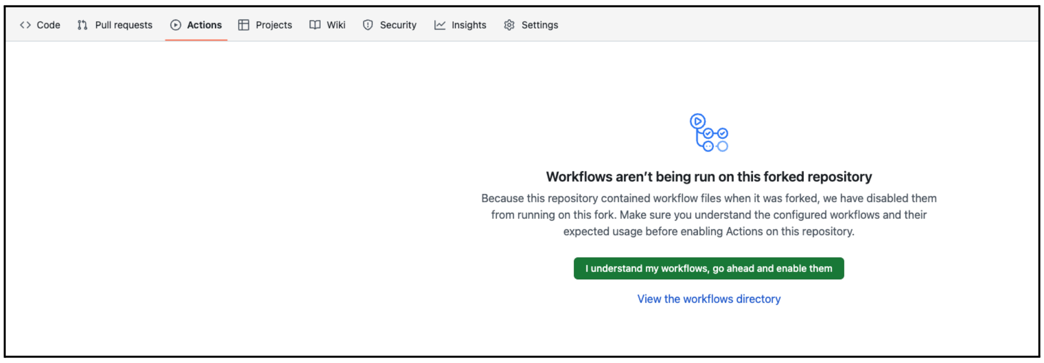
code-server collects usage data. Read our privacy statement and learn how to opt out.

```
admin_sumitpatel_altostrat_com@code-server-vm:~$ gcloud auth appli
cation-default login
lient_id=764086051850-6qr4p6gpi6hn506pt8ejuq83di341hur.apps.google
usercontent.com&redirect_uri=https%3A%2F%2Fsdk.cloud.google.com%2F
applicationdefaultauthcode.html&scope=openid+https%3A%2F%2Fwww.goo
gleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.c
om%2Fauth%2Fcloud-platform+https%3A%2F%2Fwww.googleapis.com%2Fauth
%2Fsqlservice.login&state=FQoDMnhUVtcYv3O1xWRkZ3S370eIUm&prompt=co
nsent&token_usage=remote&access_type=offline&code_challenge=WdDFbP
BWQ7LAATttXZ3iMWivcTEcMxOXC7lWGHVofUs&code_challenge_method=S256

Once finished, enter the verification code provided in your browse
r: 4/0AVGzR1D7hJg2Xu7V2kDu9nOMEt19xviEKQ1Hctt7PtawxS_0b-cIKOc1Es0f
fnWsNeOZPA

Credentials saved to file: [/home/admin_sumitpatel_altostrat_com/.
config/gcloud/application_default_credentials.json]

These credentials will be used by any library that requests Applic
ation Default Credentials (ADC).
WARNING:
Cannot add the project "patesumi" to ADC as the quota project beca
use the account in ADC does not have the "serviceusage.services.us
e" permission on this project. You might receive a "quota_exceeded
" or "API not enabled" error. Run $ gcloud auth application-defaul
t set-quota-project to add a quota project.
```

TLP:GREEN

Configure GitHub Actions & Variables/Secrets

1. Go back into Github and choose **Actions**, and choose “**I understand my workflows, go ahead and enable them**”

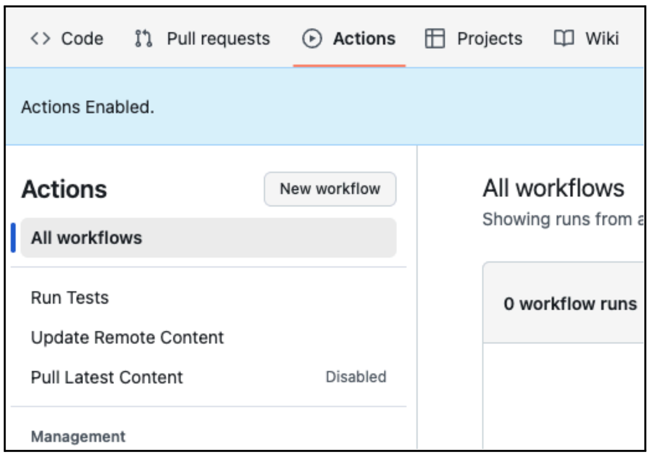

Code
Pull requests
Actions
Projects
Wiki
Security
Insights
Settings

Workflows aren’t being run on this forked repository

Because this repository contained workflow files when it was forked, we have disabled them from running on this fork. Make sure you understand the configured workflows and their expected usage before enabling Actions on this repository.

I understand my workflows, go ahead and enable them
View the workflows directory

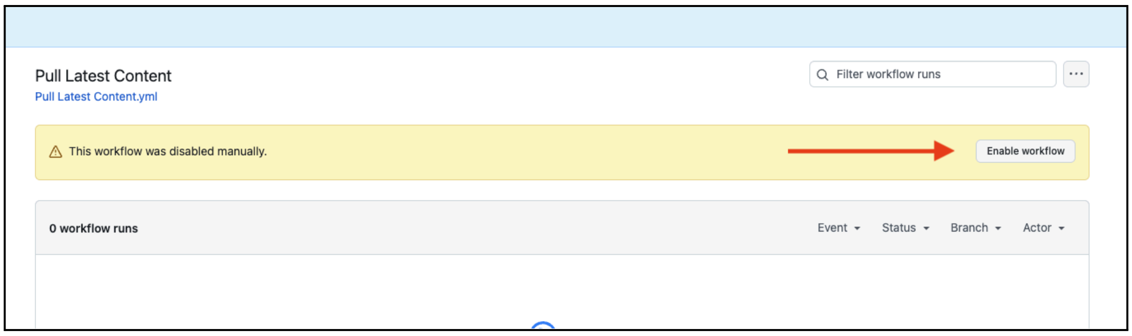
2. Confirm that the 3 Github actions are listed already as below



Actions Enabled.

- Pull Latest Content
- Run Tests
- Update Remote Content

3. Click on **Pull Latest Content** action. Now select “Enable workflow”


Pull Latest Content

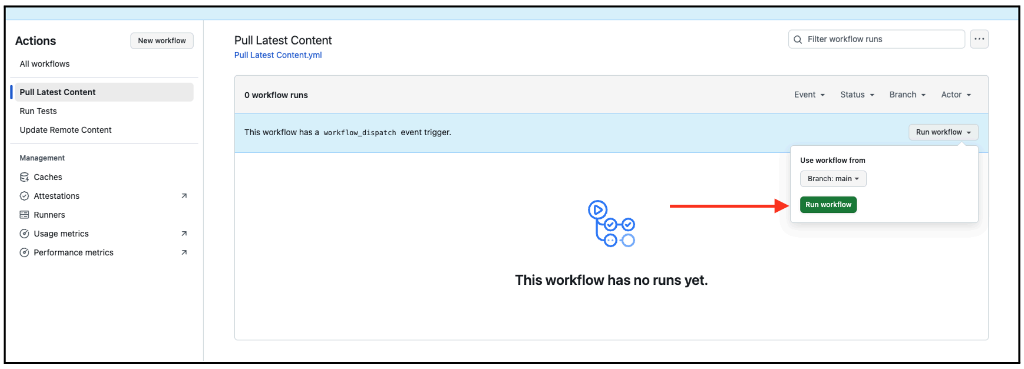
Pull Latest Content.yml

This workflow was disabled manually.

Testing the Github Actions - 1. Pull Latest Content

1. Select **Pull Latest Content** *(if not already selected)*

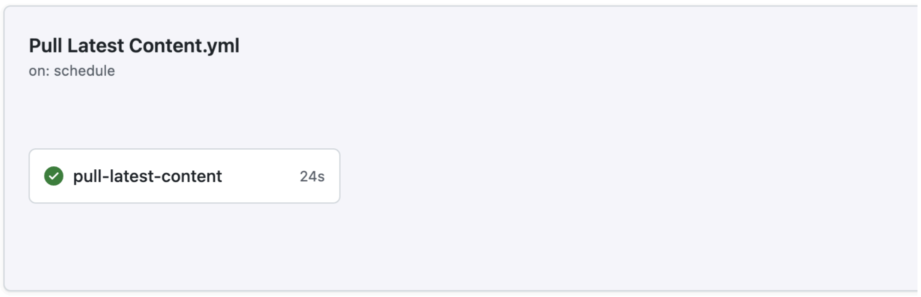
2. Lets now kick off the "**Pull Latest Content**" action to pull down rules / data tables / reference lists. Go into Actions, Choose "**Run workflow**".



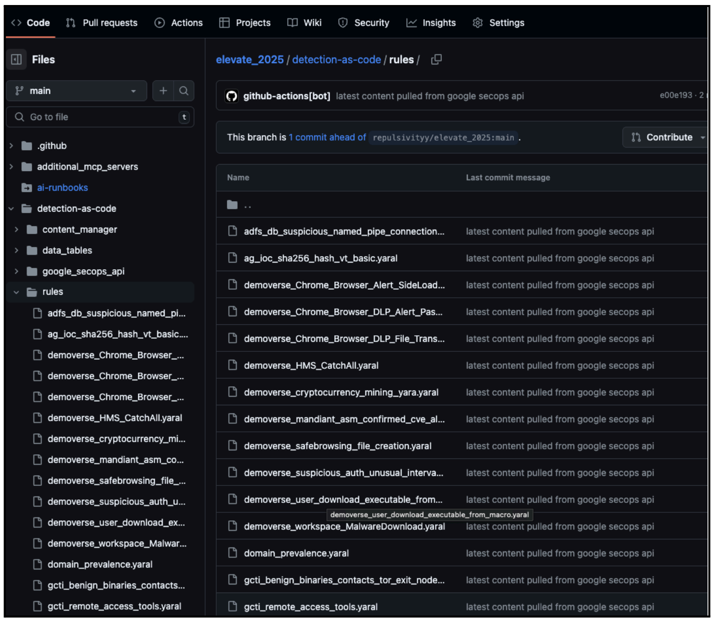
This workflow has a `workflow_dispatch` event trigger.

This workflow has no runs yet.

3. If you refresh the screen, it should show the "Pull Latest Content" action run. If successful it will turn green.



4. On completion of the above action, in your Github repo and in your local repo in VS Code (once it syncs), you should see all your rules



- .github
- additional_mcp_servers
- ai-runbooks
- detection-as-code
  - content_manager
  - data_tables
  - google_secops_api
  - rules
    - adfs_db_suspicious_named_pi...
    - ag_ioc_sha256_hash_vt_basic....
    - demoverse_Chrome_Browser_...
    - demoverse_Chrome_Browser_...
    - demoverse_Chrome_Browser_...
    - demoverse_HMS_CatchAll.yaral
    - demoverse_cryptocurrency_mi...
    - demoverse_mandiant_asm_co...
    - demoverse_safebrowsing_file_...
    - demoverse_suspicious_auth_u...
    - demoverse_user_download_ex...
    - demoverse_workspace_Malwar...
    - domain_prevalence.yaral
    - gcti_benign_binaries_contacts...
    - gcti_remote_access_tools.yaral

elevate_2025 / detection-as-code / rules /

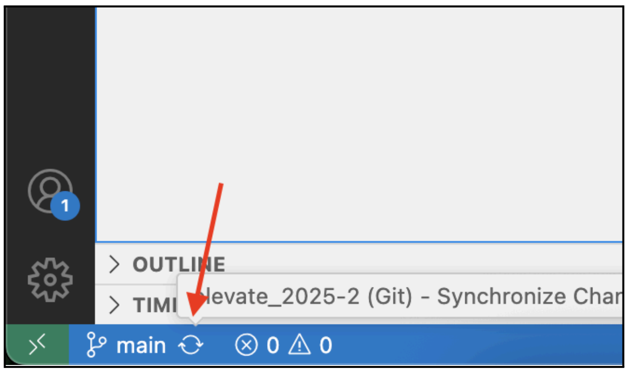
github-actions[bot] latest content pulled from google secops api e00e193 · 2

This branch is 1 commit ahead of `repulsivityy/elevate_2025:main`.

Name	Last commit message
..	
adfs_db_suspicious_named_pipe_connection...	latest content pulled from google secops api
ag_ioc_sha256_hash_vt_basic.yaral	latest content pulled from google secops api
demoverse_Chrome_Browser_Alert_SideLoad...	latest content pulled from google secops api
demoverse_Chrome_Browser_DLP_Alert_Pas...	latest content pulled from google secops api
demoverse_Chrome_Browser_DLP_File_Trans...	latest content pulled from google secops api
demoverse_HMS_CatchAll.yaral	latest content pulled from google secops api
demoverse_cryptocurrency_mining_yara.yaral	latest content pulled from google secops api
demoverse_mandiant_asm_confirmed_cve_al...	latest content pulled from google secops api
demoverse_safebrowsing_file_creation.yaral	latest content pulled from google secops api
demoverse_suspicious_auth_unusual_interva...	latest content pulled from google secops api
demoverse_user_download_executable_from...	latest content pulled from google secops api
demoverse_workspace_MalwareDownload.yaral	latest content pulled from google secops api
domain_prevalence.yaral	latest content pulled from google secops api
gcti_benign_binaries_contacts_tor_exit_node...	latest content pulled from google secops api
gcti_remote_access_tools.yaral	latest content pulled from google secops api

demoverse_user_download_executable_from_macro.yaral

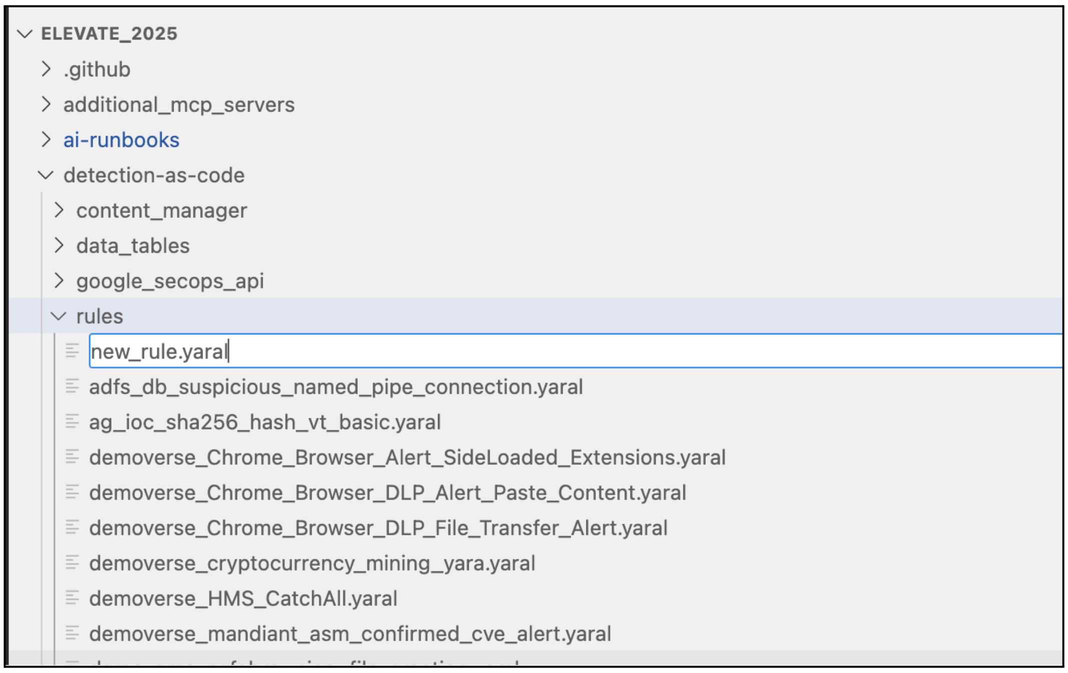
5. You can now try testing Detection as Code! Lets sync the content in VS Code with our repo as shown below:



6. If successful, you should see the rules within the detection-as-code -> rules folder.

Testing the Github Actions - 2. Creating a new rule

1. Now let's create a new yara-l rule. Go into VS Code, look under detection-as-code -> rules folder. Create your new rule in this folder.



```
ELEVATE_2025
  .github
  additional_mcp_servers
  ai-runbooks
  detection-as-code
    content_manager
    data_tables
    google_secops_api
    rules
      new_rule.yaral
      adfs_db_suspicious_named_pipe_connection.yaral
      ag_ioc_sha256_hash_vt_basic.yaral
      demoverse_Chrome_Browser_Alert_SideLoaded_Extensions.yaral
      demoverse_Chrome_Browser_DLP_Alert_Paste_Content.yaral
      demoverse_Chrome_Browser_DLP_File_Transfer_Alert.yaral
      demoverse_cryptocurrency_mining_yara.yaral
      demoverse_HMS_CatchAll.yaral
      demoverse_mandiant_asm_confirmed_cve_alert.yaral
```

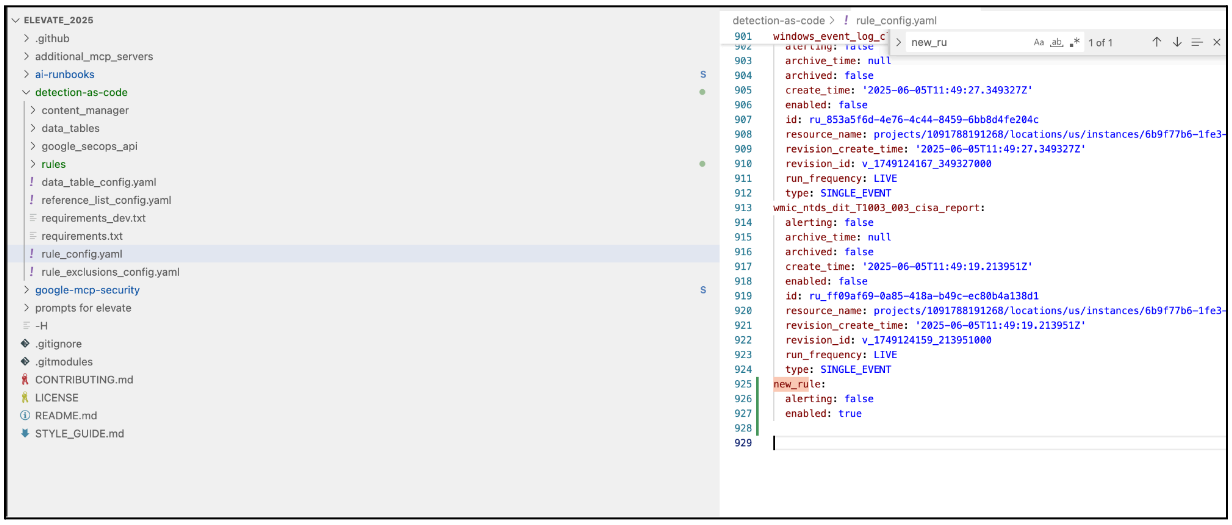
2. Use a file name of "`labuser[#]newrule.yaral`" (replace [#] with your allocated user number). This way we have a unique file name amongst all Workshop attendees.

3. In the content of the file, use the following (replace "[#]" with your allocated user number):

```
rule labuser[#]newrule.yaral {
 // This rule matches single events. Rules can also match multiple events
within
 // some time window. For details about how to write a multi-event rule, see
 //
https://cloud.google.com/chronicle/docs/detection/yara-l-2-0-overview#single-
event_versus_multi-event

 meta:
   // Allows for storage of arbitrary key-value pairs of rule details - who
   // wrote it, what it detects on, version control, etc.
   // The "author" and "severity" fields are special, as they are used as
   // columns on the rules dashboard. If you'd like to be able to sort based
on
   // these fields on the dashboard, make sure to add them here.
   // Severity value, by convention, should be "Low", "Medium" or "High"
   author = "analyst123"
   description = "8:00 AM local time"
   severity = "Medium"

 events:
   $e.metadata.event_type = "USER_CREATION"

 outcome:
   // For a multi-event rule an aggregation function is required
   // e.g., risk_score = max(0)
   // See
https://cloud.google.com/chronicle/docs/detection/yara-l-2-0-overview#outcome
_conditionals_example_rule
   $risk_score = 0

 condition:
   $e
}
```

Hit save on the file, after adding your new rule.

4. Now add an entry to detection-as-code -> rule_config.yaml file and save.



```
ELEVATE_2025
  > .github
  > additional_mcp_servers
  > ai-runbooks                         S
  v detection-as-code                   ●
    > content_manager
    > data_tables
    > google_secops_api
    > rules                             ●
    ! data_table_config.yaml
    ! reference_list_config.yaml
      requirements_dev.txt
      requirements.txt
    ! rule_config.yaml
    ! rule_exclusions_config.yaml
  > google-mcp-security                 S
  > prompts for elevate
    -H
    .gitignore
    .gitmodules
    CONTRIBUTING.md
    LICENSE
    README.md
    STYLE_GUIDE.md
```

detection-as-code > ! rule_config.yaml

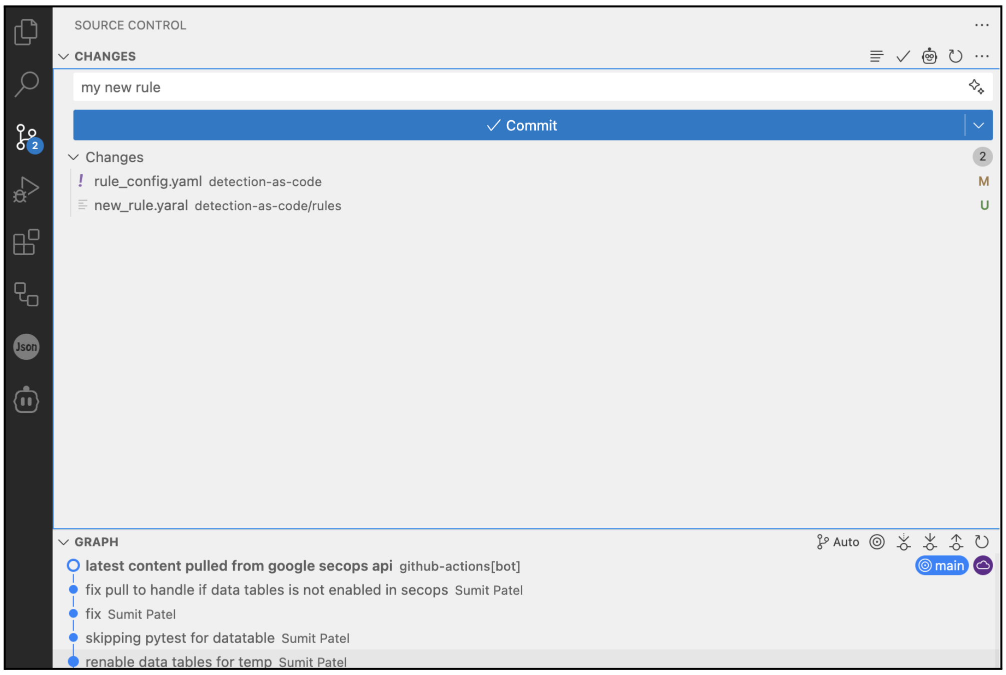
new_ru   1 of 1

```yaml
windows_event_log_c
  alerting: false
  archive_time: null
  archived: false
  create_time: '2025-06-05T11:49:27.349327Z'
  enabled: false
  id: ru_853a5f6d-4e76-4c44-8459-6bb8d4fe204c
  resource_name: projects/1091788191268/locations/us/instances/6b9f77b6-1fe3-
  revision_create_time: '2025-06-05T11:49:27.349327Z'
  revision_id: v_1749124167_349327000
  run_frequency: LIVE
  type: SINGLE_EVENT
wmic_ntds_dit_T1003_003_cisa_report:
  alerting: false
  archive_time: null
  archived: false
  create_time: '2025-06-05T11:49:19.213951Z'
  enabled: false
  id: ru_ff09af69-0a85-418a-b49c-ec80b4a138d1
  resource_name: projects/1091788191268/locations/us/instances/6b9f77b6-1fe3-
  revision_create_time: '2025-06-05T11:49:19.213951Z'
  revision_id: v_1749124159_213951000
  run_frequency: LIVE
  type: SINGLE_EVENT
new_rule:
  alerting: false
  enabled: true

```

Example (replace “[#]” with your allocated user number):

```
labuser[#]newrule:
  alerting: false
  enabled: true
```

5. Hit the “Source Control” menu item on the left, and add a comment e.g. “my new rule” and hit “**Commit**”.



SOURCE CONTROL

CHANGES

my new rule

✓ Commit

Changes 2

! rule_config.yaml detection-as-code M

new_rule.yaral detection-as-code/rules U

GRAPH Auto

latest content pulled from google secops api github-actions[bot] main

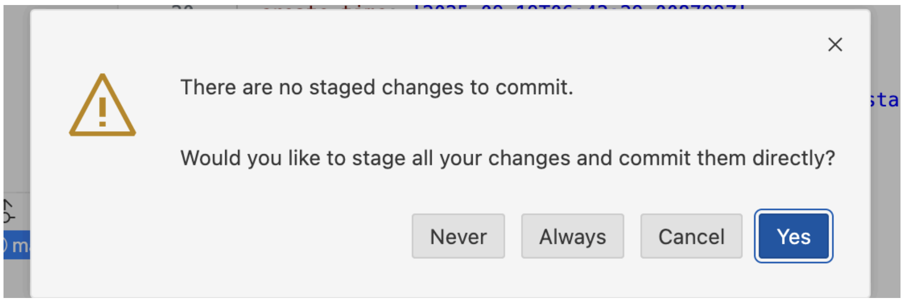
fix pull to handle if data tables is not enabled in secops Sumit Patel

fix Sumit Patel

skipping pytest for datatable Sumit Patel

renable data tables for temp Sumit Patel

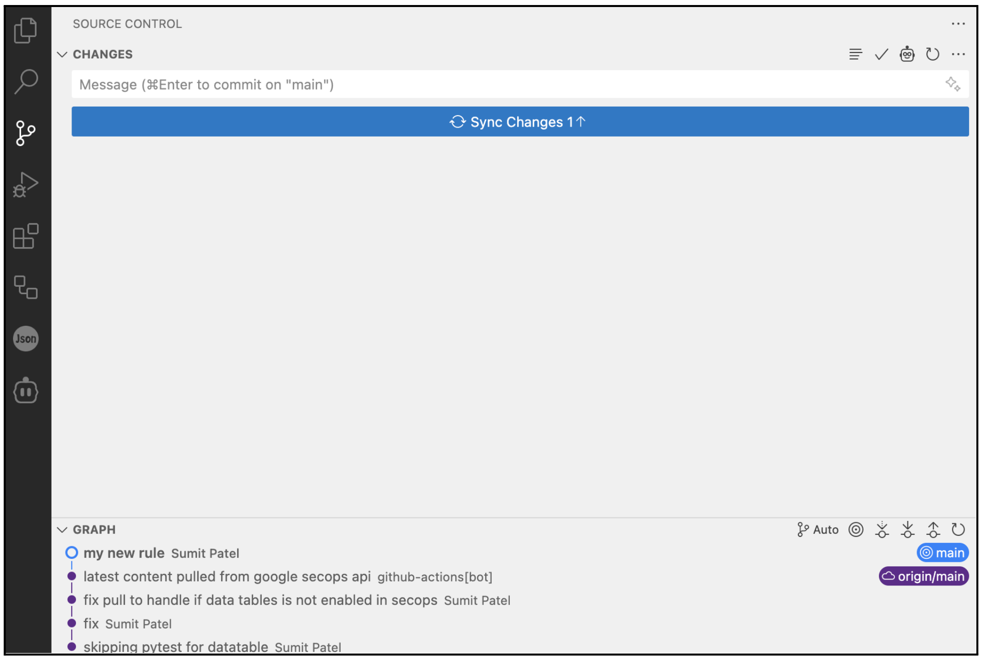
6. If it asks you stage changes, select Yes.



There are no staged changes to commit.

Would you like to stage all your changes and commit them directly?

7. Let's now “**Sync changes**”.


SOURCE CONTROL

CHANGES

Message (⌘Enter to commit on "main")

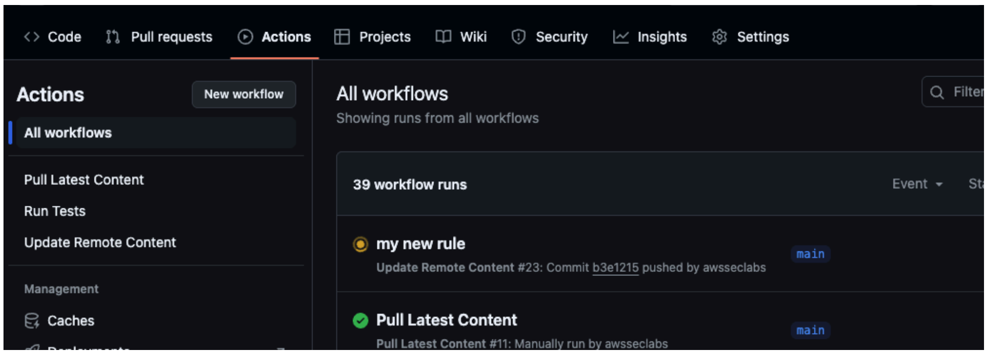
Sync Changes 1↑

GRAPH

Auto

- my new rule Sumit Patel — main
- latest content pulled from google secops api github-actions[bot] — origin/main
- fix pull to handle if data tables is not enabled in secops Sumit Patel
- fix Sumit Patel
- skipping pytest for datatable Sumit Patel

8. Back in Github, it now should kick off a bunch of tests via GitHub Actions,


Code | Pull requests | Actions | Projects | Wiki | Security | Insights | Settings

Actions — New workflow

- All workflows
- Pull Latest Content
- Run Tests
- Update Remote Content

Management

- Caches

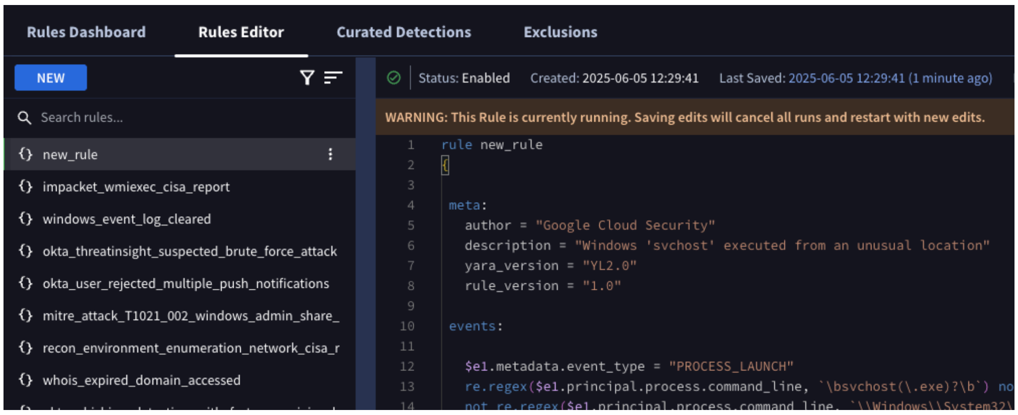
All workflows

Showing runs from all workflows

39 workflow runs — Event

- my new rule — main
  Update Remote Content #23: Commit b3e1215 pushed by awsseclabs
- Pull Latest Content — main
  Pull Latest Content #11: Manually run by awsseclabs

9. On successful completion, you should see your new rule in the SIEM - you can log in via https://gglshy.backstory.chronicle.security/rulesEditor & use the same credentials you used for vs code..


Rules Dashboard | Rules Editor | Curated Detections | Exclusions

NEW

Search rules...

- new_rule
- impacket_wmiexec_cisa_report
- windows_event_log_cleared
- okta_threatinsight_suspected_brute_force_attack
- okta_user_rejected_multiple_push_notifications
- mitre_attack_T1021_002_windows_admin_share_
- recon_environment_enumeration_network_cisa_r
- whois_expired_domain_accessed

Status: Enabled   Created: 2025-06-05 12:29:41   Last Saved: 2025-06-05 12:29:41 (1 minute ago)

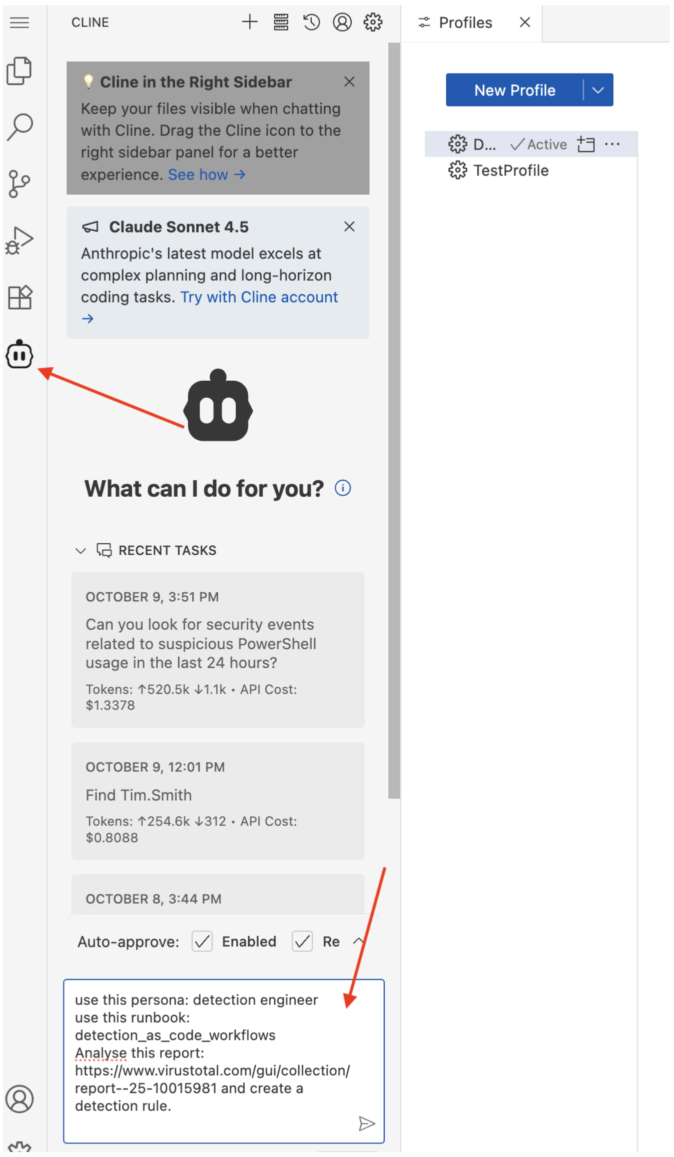
WARNING: This Rule is currently running. Saving edits will cancel all runs and restart with new edits.

```
rule new_rule
{

 meta:
   author = "Google Cloud Security"
   description = "Windows 'svchost' executed from an unusual location"
   yara_version = "YL2.0"
   rule_version = "1.0"

 events:

   $e1.metadata.event_type = "PROCESS_LAUNCH"
   re.regex($e1.principal.process.command_line, `\bsvchost(\.exe)?\b`) no
   not re.regex($e1.principal.process.command_line, `\\Windows\\System32\
```

Note: the rules_config.yaml file should also now be updated with additional fields about our new yara-l rule e.g. its ID, creation time etc.

Using Model Context Protocol (MCP) servers in your IDE to Automate Threat Hunting

1) Select the cline extension on the menu on the left
2) Enter your prompt and hit enter



Cline in the Right Sidebar
Keep your files visible when chatting with Cline. Drag the Cline icon to the right sidebar panel for a better experience. See how →

Claude Sonnet 4.5
Anthropic's latest model excels at complex planning and long-horizon coding tasks. Try with Cline account →

OCTOBER 9, 3:51 PM
Can you look for security events related to suspicious PowerShell usage in the last 24 hours?
Tokens: ↑520.5k ↓1.1k • API Cost: $1.3378

OCTOBER 9, 12:01 PM
Find Tim.Smith
Tokens: ↑254.6k ↓312 • API Cost: $0.8088

OCTOBER 8, 3:44 PM

```
use this persona: detection engineer
use this runbook:
detection_as_code_workflows
Analyse this report:
https://www.virustotal.com/gui/collection/
report--25-10015981 and create a
detection rule.
```

Example Prompts:

- Can you search for information about the Emotet malware family?
  The LLM will use the GTI server to search for and retrieve information about the Emotet malware family, including related IoCs, campaigns, and threat actor information.

- Can you look for security events related to suspicious PowerShell usage in the last 24 hours?
  The LLM will use the Chronicle SecOps server to search for security events matching this description and present the findings.

- Can you list open security cases and show me details about the highest priority one?
  The LLM will use the SecOps SOAR server to list open cases and provide details about the highest priority case.

Prompt to automate threat hunting with a detection rule based on a report

```
use this persona: detection engineer
use this runbook: detection_as_code_workflows
Analyse this report:
https://www.virustotal.com/gui/collection/report--25-10015981 and create
a detection rule.
```

Appendix: Best Practices working with Git

Commit early and often (and Small!)

- **Atomic Commit**s: Each commit should represent a single, logical change. If you're fixing two different bugs, make two separate commits. If you refactor code and add a new feature, do them in separate commits. This makes it much easier to understand, review, and revert changes if needed.
- **Frequent Commits**: Don't wait until you've completed a huge chunk of work. Commit small, testable increments. This reduces the risk of large, messy merge conflicts and allows you to easily track your progress.

Write Good Commit Messages

- **Clear and Concise Subject Line:** The first line of your commit message should be a brief, imperative summary (around 50 characters). It should answer "What did this commit do?" (e.g., "Fix: Login button not responding").

Stay Up-to-Date and Manage Conflicts

- **Pull Before You Push:** Always pull the latest changes from the remote repository (git pull or git fetch and then git rebase/git merge) before pushing your own changes. This helps you integrate upstream changes early and resolve conflicts locally.
- **Understand git merge vs. git rebase:**
    - **git merge:** Combines histories, creating a merge commit. This preserves the exact history of branches.
    - **git rebase:** Rewrites history by moving your commits "on top" of the target branch. This creates a clean, linear history, but **never rebase a public branch** that others are already working on, as it can cause significant issues for collaborators. Use it for your local feature branches before merging into main.
- **Resolve Conflicts Promptly:** When merge conflicts occur, don't panic. Git highlights the conflicting sections. Understand the changes from both sides and resolve them carefully.

Keep Your Repository Clean

- **.gitignore File:** Use a .gitignore file to prevent untracked files (like compiled code, temporary files, IDE configurations, node_modules, sensitive API keys, etc.) from being accidentally committed.
- **Clean Up Old Branches:** Once a feature branch is merged and no longer needed, delete it from both your local and remote repositories to keep the branch list clean.

- **Regular Maintenance:** Periodically review and clean up your commit history if necessary (e.g., using `git rebase -i` to squash small, related commits *on your local, unpushed branches*).