I tried the GitHub App Installation via the Sumo Logic App Catalog for Improved Dashboarding and Search Capabilities to Unlock Data Analysis

dev.classmethod.jp/articles/i-tried-the-github-app-installation-via-the-sumo-logic-app-catalog-for-improved-dashboarding-and-search-capabilities-to-unlock-data-analysis

HemanthKumar R

August 24, 2023

目次

Introduction

Hemanth from the Department of Alliance. I'll demonstrate how to install Github app via the Sumo Logic App Catalog for Improved Dashboarding and Search Capabilities to Unlock Data Analysis.

Sumo Logic

Before going further let's understand what sumo logic is. A cloud-based log management and analytics software called Sumo Logic enables businesses to exploit their machine data for useful insights. Sumo Logic's flexible capabilities make log data analysis simple and offer real-time visibility into operational and security insights.

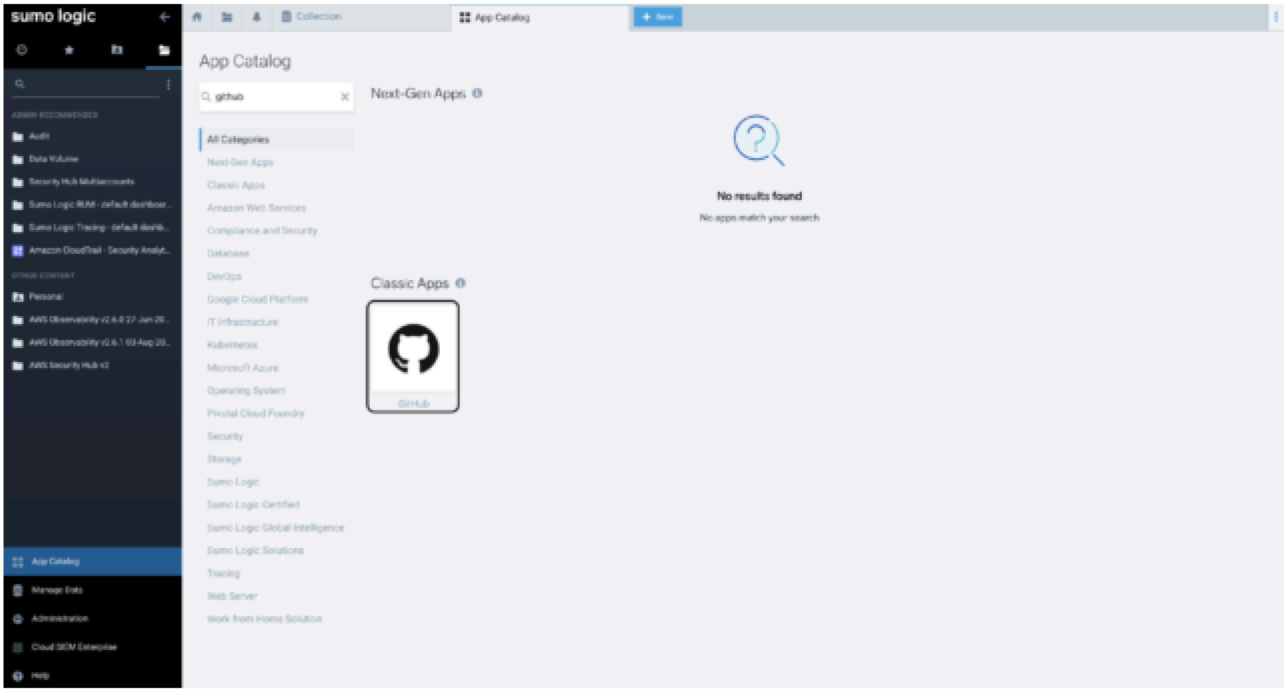
Github

Developers can work together on software projects, manage their code, and participate in open source communities using the GitHub platform. Over 100 million developers utilize GitHub worldwide, and it is the home to many well-known open source projects. This platform promotes creativity and collaboration, allowing people from all over the world to create anything they can imagine.

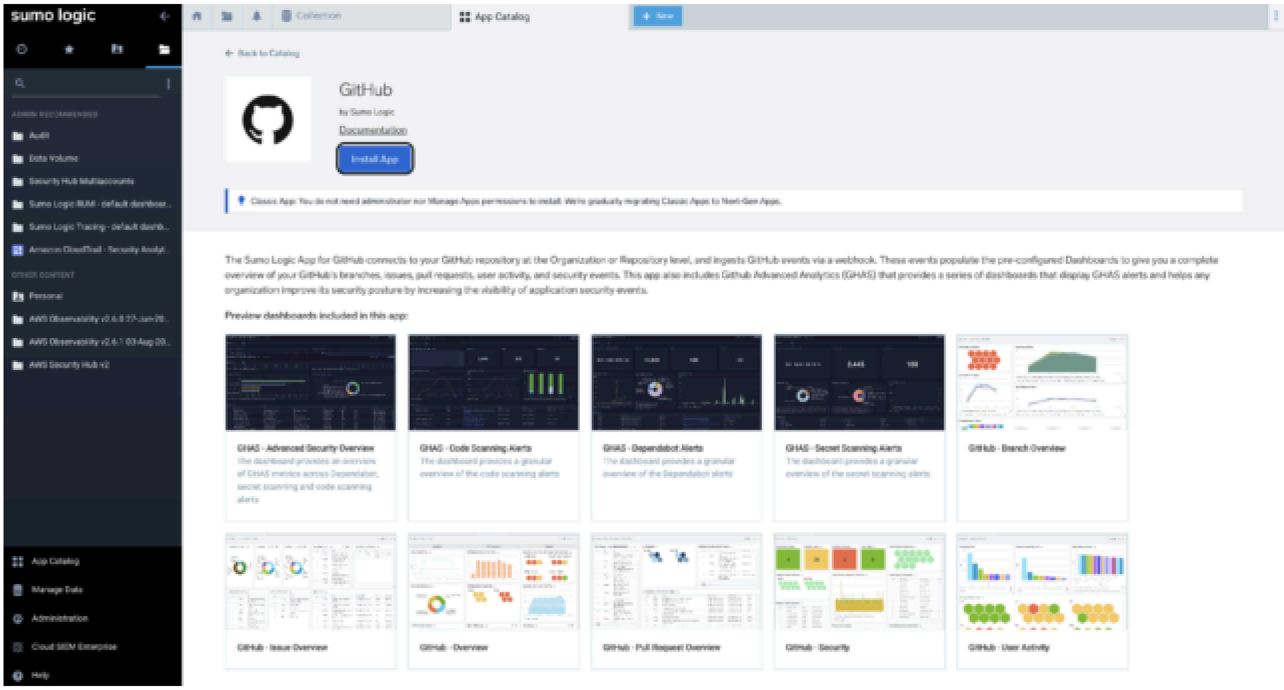
Follow the below if you still haven't set your collector and source for your github in Sumo logic

Demo

Navigating to app catalog within sumo logic, search for github app and click to select it.



click on install app and installation process starts


sumo logic
Collection
App Catalog
+ New
← Back to Catalog
Install App
Audit
Data Volume
Security Hub Multiaccounts
Sumo Logic RUM - default dashboar...
Sumo Logic Tracing - default dashb...
Amazon CloudTrail - Security Analyt...
Personal
AWS Observability v2.6.0 27-Jan-20...
AWS Observability v2.6.1 03-Aug-20...
AWS Security Hub v2
App Catalog
Manage Data
Administration
Cloud SIEM Enterprise
Help

GitHub

by Sumo Logic

Documentation

Classic App: You do not need administrator nor Manage Apps permissions to install. We're gradually migrating Classic Apps to Next-Gen Apps.

The Sumo Logic App for GitHub connects to your GitHub repository at the Organization or Repository level, and ingests GitHub events via a webhook. These events populate the pre-configured Dashboards to give you a complete overview of your GitHub's branches, issues, pull requests, user activity, and security events. This app also includes Github Advanced Analytics (GHAS) that provides a series of dashboards that display GHAS alerts and helps any organization improve its security posture by increasing the visibility of application security events.

Preview dashboards included in this app:

GHAS - Advanced Security Overview
The dashboard provides an overview of GHAS metrics across Dependabot, secret scanning and code scanning alerts

GHAS - Code Scanning Alerts
The dashboard provides a granular overview of the code scanning alerts

GHAS - Dependabot Alerts
The dashboard provides a granular overview of the Dependabot alerts

GHAS - Secret Scanning Alerts
The dashboard provides a granular overview of the secret scanning alerts

GitHub - Branch Overview

GitHub - Issue Overview

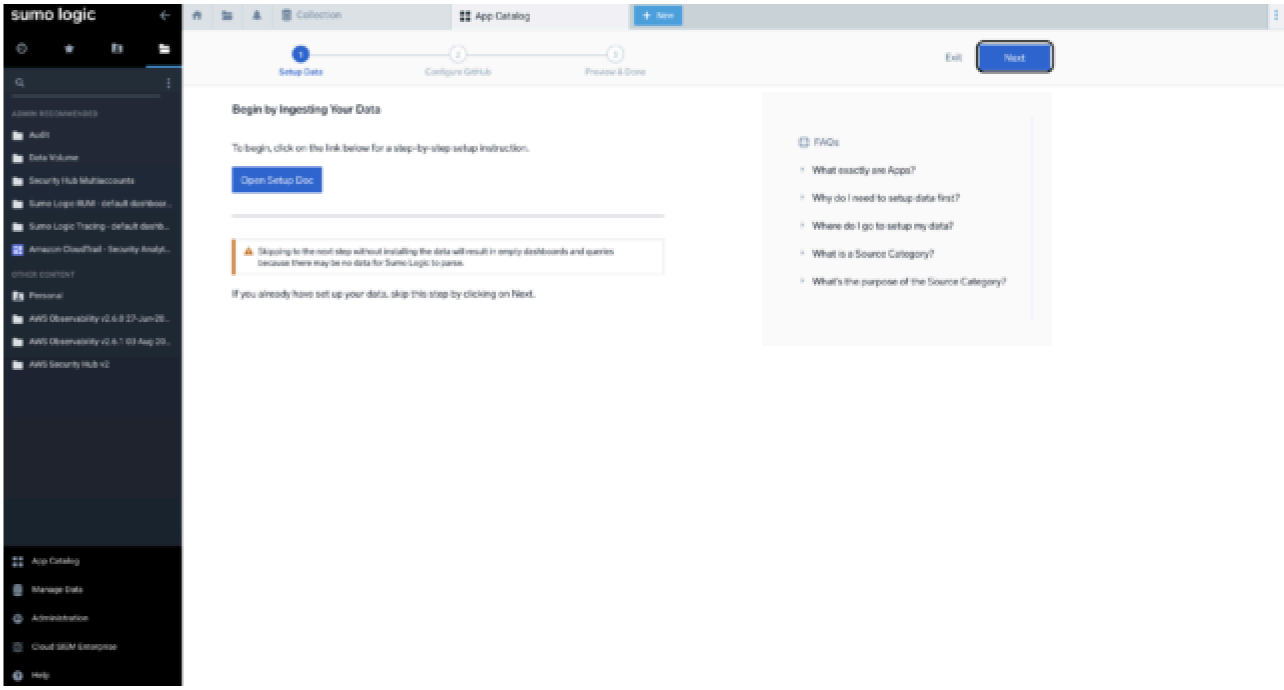
GitHub - Overview

GitHub - Pull Request Overview

GitHub - Security

GitHub - User Activity

Click on option of open setup doc or follow the above blog and finish the initial setup procedure. Once completed click "Next".


sumo logic
Collection
App Catalog
+ New
1
Setup Data
2
Configure GitHub
3
Preview & Done
Exit
Next
Open Setup Doc
Audit
Data Volume
Security Hub Multiaccounts
Sumo Logic RUM - default dashboar...
Sumo Logic Tracing - default dashb...
Amazon CloudTrail - Security Analyt...
Personal
AWS Observability v2.6.0 27-Jan-20...
AWS Observability v2.6.1 03-Aug-20...
AWS Security Hub v2
App Catalog
Manage Data
Administration
Cloud SIEM Enterprise
Help

Begin by Ingesting Your Data

To begin, click on the link below for a step-by-step setup instruction.

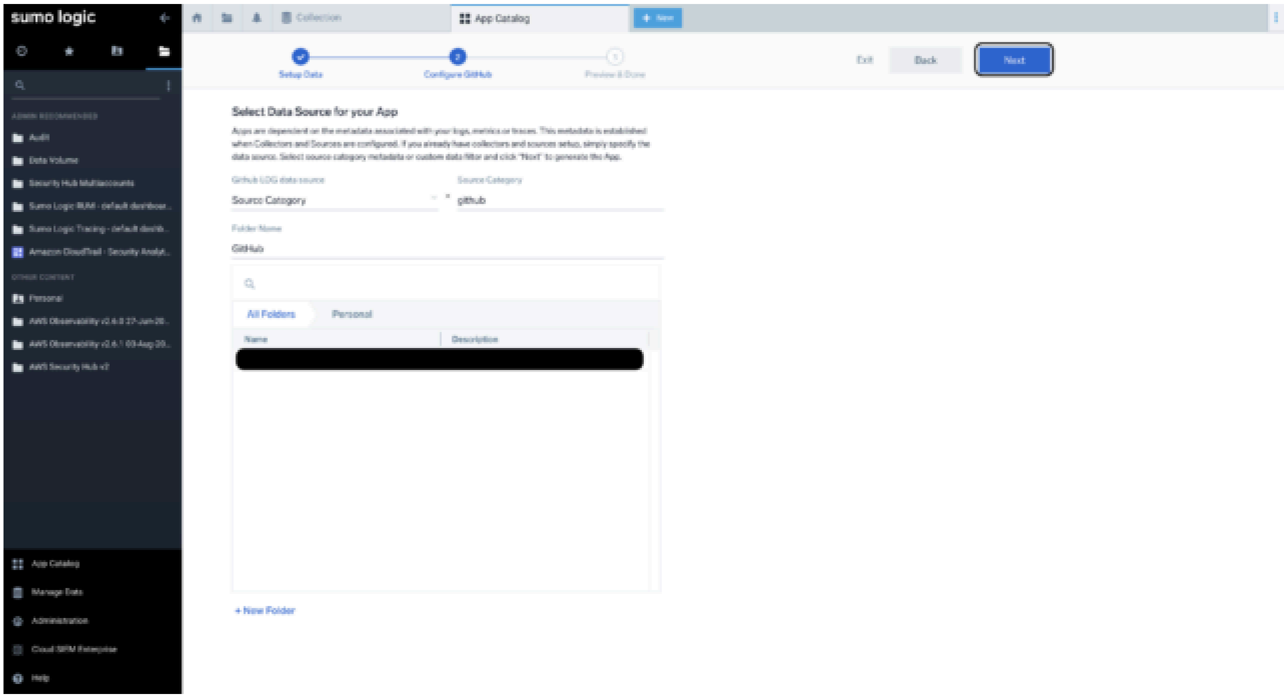
Skipping to the next step without installing the data will result in empty dashboards and queries because there may be no data for Sumo Logic to parse.

If you already have set up your data, skip this step by clicking on Next.

FAQs

- What exactly are Apps?
- Why do I need to setup data first?
- Where do I go to setup my data?
- What is a Source Category?
- What's the purpose of the Source Category?

Now choose the source_category of app as below, freely select the folder of your choice or create your own folder. After selection click on next.


sumo logic
Collection
App Catalog
+ New
Setup Data
Configure GitHub
Preview & Done
Exit
Back
Next
Audit
Data Volume
Security Hub Multiaccounts
Sumo Logic RUM - default dashboar...
Sumo Logic Tracing - default dashb...
Amazon CloudTrail - Security Analyt...
Personal
AWS Observability v2.6.0 27-Jan-20...
AWS Observability v2.6.1 03-Aug-20...
AWS Security Hub v2
App Catalog
Manage Data
Administration
Cloud SIEM Enterprise
Help

Select Data Source for your App

Apps are dependent on the metadata associated with your logs, metrics or traces. This metadata is established when Collectors and Sources are configured. If you already have collectors and sources setup, simply specify the data source. Select source category metadata or custom data filter and click "Next" to generate the App.

Github LOG data source: Source Category

Source Category: github

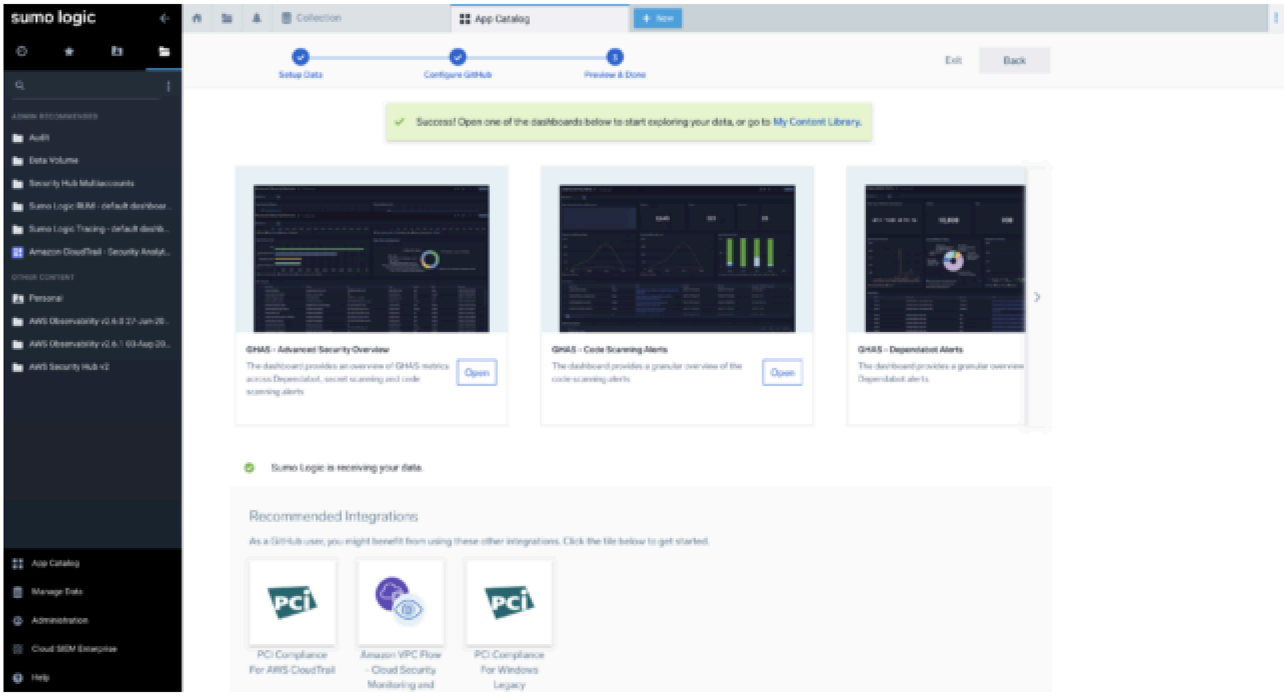
Folder Name: GitHub

All Folders | Personal

Name	Description
[redacted]	

+ New Folder

Successfully completed installation


sumo logic
Collection
App Catalog
+ New
Setup Data
Configure GitHub
Preview & Done
Exit
Back
Audit
Data Volume
Security Hub Multiaccounts
Sumo Logic RUM - default dashboar...
Sumo Logic Tracing - default dashb...
Amazon CloudTrail - Security Analyt...
Personal
AWS Observability v2.6.0 27-Jan-20...
AWS Observability v2.6.1 03-Aug-20...
AWS Security Hub v2
App Catalog
Manage Data
Administration
Cloud SIEM Enterprise
Help
Open
Open

✓ Success! Open one of the dashboards below to start exploring your data, or go to My Content Library.

GHAS - Advanced Security Overview
The dashboard provides an overview of GHAS metrics across Dependabot, secret scanning and code scanning alerts

GHAS - Code Scanning Alerts
The dashboard provides a granular overview of the code scanning alerts

GHAS - Dependabot Alerts
The dashboard provides a granular overview Dependabot alerts

Sumo Logic is receiving your data.

Recommended Integrations

As a GitHub user, you might benefit from using these other integrations. Click the tile below to get started.

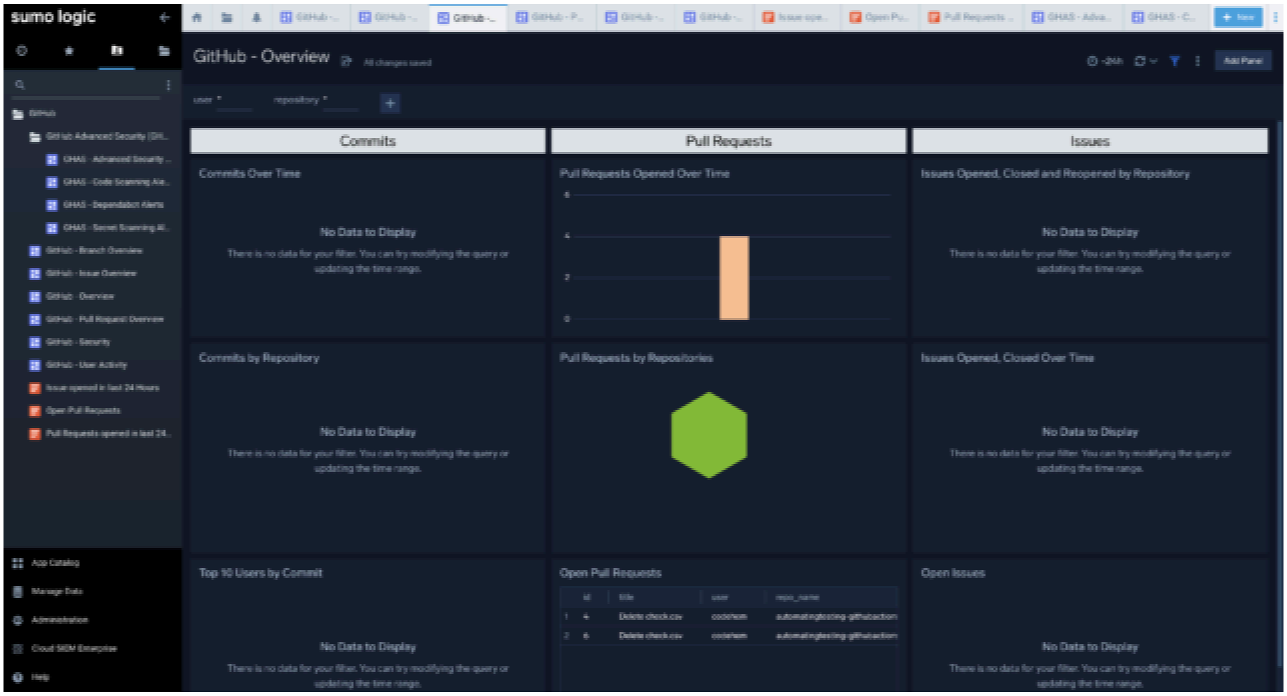
PCI Compliance For AWS CloudTrail

Amazon VPC Flow - Cloud Security Monitoring and

PCI Compliance For Windows Legacy

After the installation is finished, you are prepared to explore a variety of pre-built dashboards and search features:

Some of Dashboards such as Github Overview



GitHub - Overview

All changes saved

Commits

Pull Requests

Issues

Commits Over Time

No Data to Display

There is no data for your filter. You can try modifying the query or updating the time range.

Pull Requests Opened Over Time

Issues Opened, Closed and Reopened by Repository

No Data to Display

There is no data for your filter. You can try modifying the query or updating the time range.

Commits by Repository

No Data to Display

There is no data for your filter. You can try modifying the query or updating the time range.

Pull Requests by Repositories

Issues Opened, Closed Over Time

No Data to Display

There is no data for your filter. You can try modifying the query or updating the time range.

Top 10 Users by Commit

No Data to Display

There is no data for your filter. You can try modifying the query or updating the time range.

Open Pull Requests

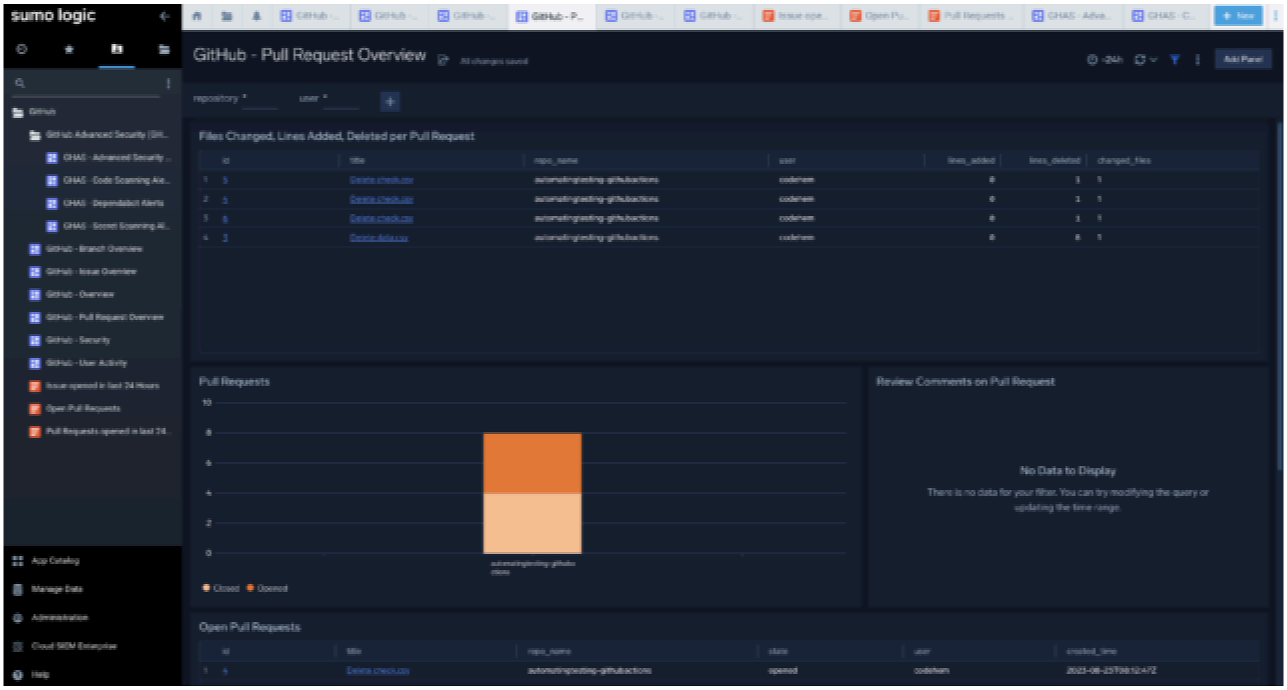
	id	title	user	repo_name
1	4	Delete check.csv	codehem	automatingtesting-githubaction
2	6	Delete check.csv	codehem	automatingtesting-githubaction

Open Issues

No Data to Display

There is no data for your filter. You can try modifying the query or updating the time range.

Github - Pull Request Overview



GitHub - Pull Request Overview

All changes saved

Files Changed, Lines Added, Deleted per Pull Request

	id	title	repo_name	user	lines_added	lines_deleted	changed_files
1	5	Delete check.csv	automatingtesting-githubactions	codehem	0	1	1
2	5	Delete check.csv	automatingtesting-githubactions	codehem	0	1	1
3	6	Delete check.csv	automatingtesting-githubactions	codehem	0	1	1
4	3	Delete data.csv	automatingtesting-githubactions	codehem	0	0	1

Pull Requests

Review Comments on Pull Request

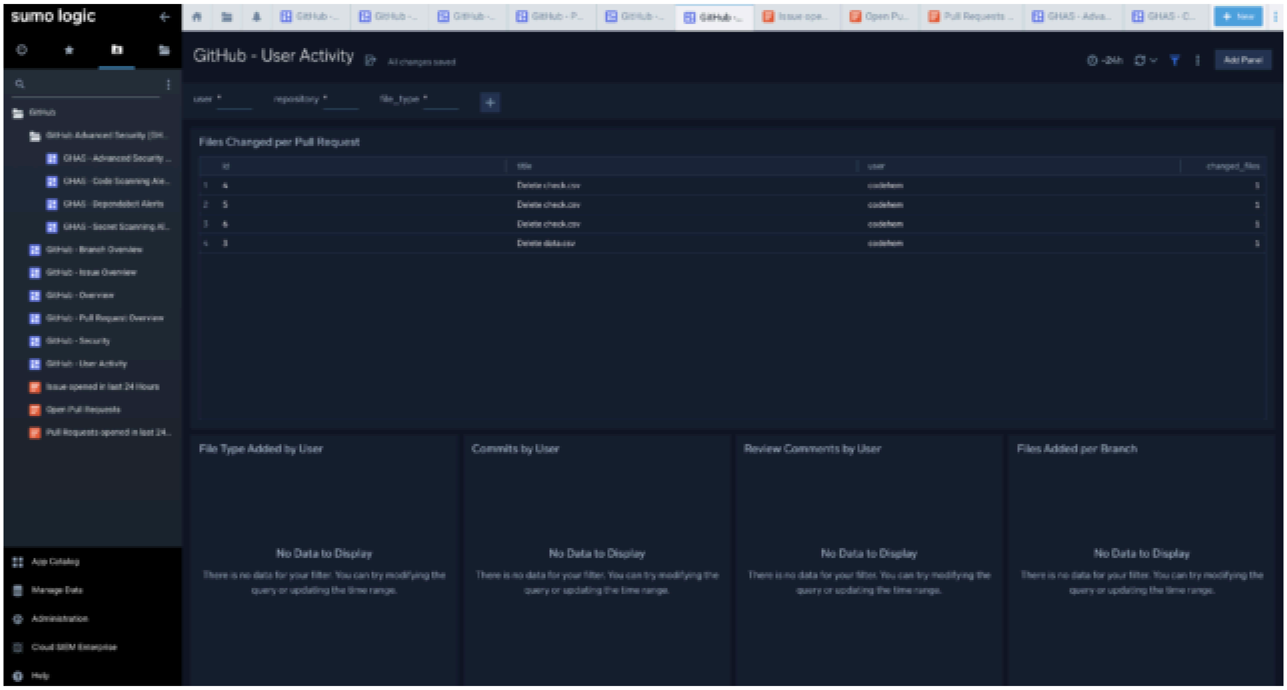
No Data to Display

There is no data for your filter. You can try modifying the query or updating the time range.

Open Pull Requests

	id	title	repo_name	state	user	created_time
1	6	Delete check.csv	automatingtesting-githubactions	opened	codehem	2023-08-25T08:12:47Z

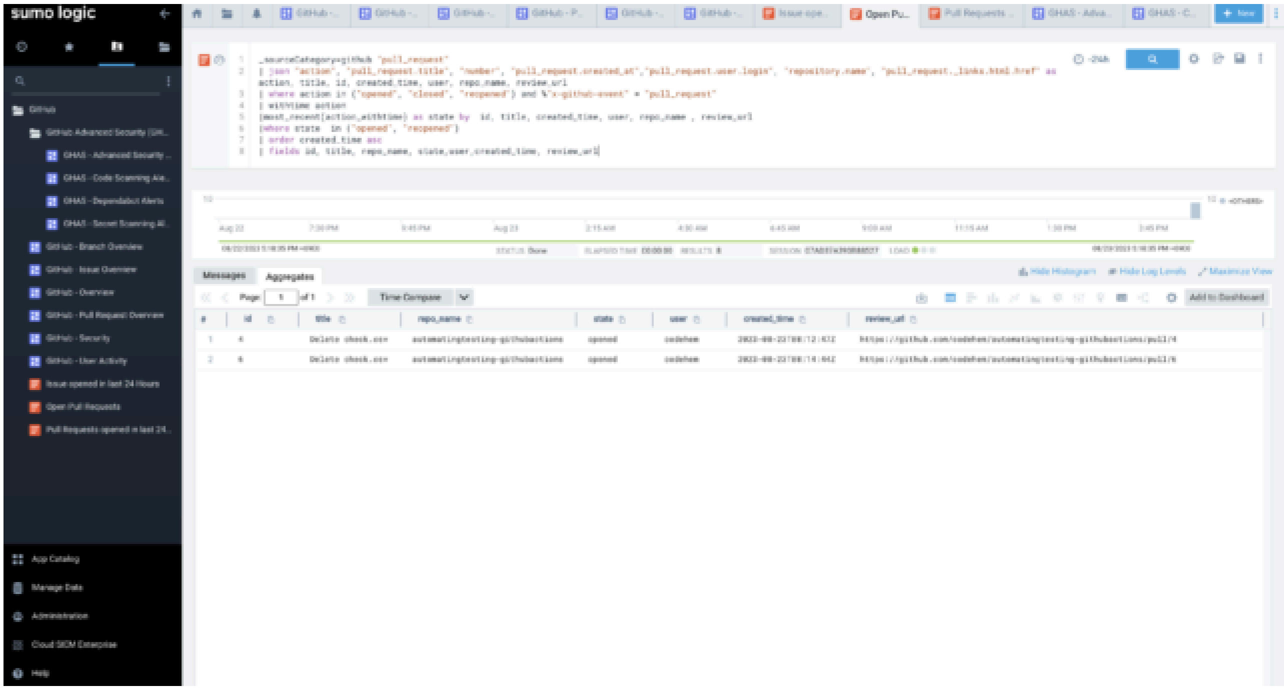
Github User Activity



Files Changed per Pull Request

	id	title	user	changed_files
1	4	Delete check.csv	codehem	1
2	5	Delete check.csv	codehem	1
3	6	Delete check.csv	codehem	1
4	3	Delete data.csv	codehem	1

Navigating Github Logs with Some of specialized log searches: Open Pull Requests

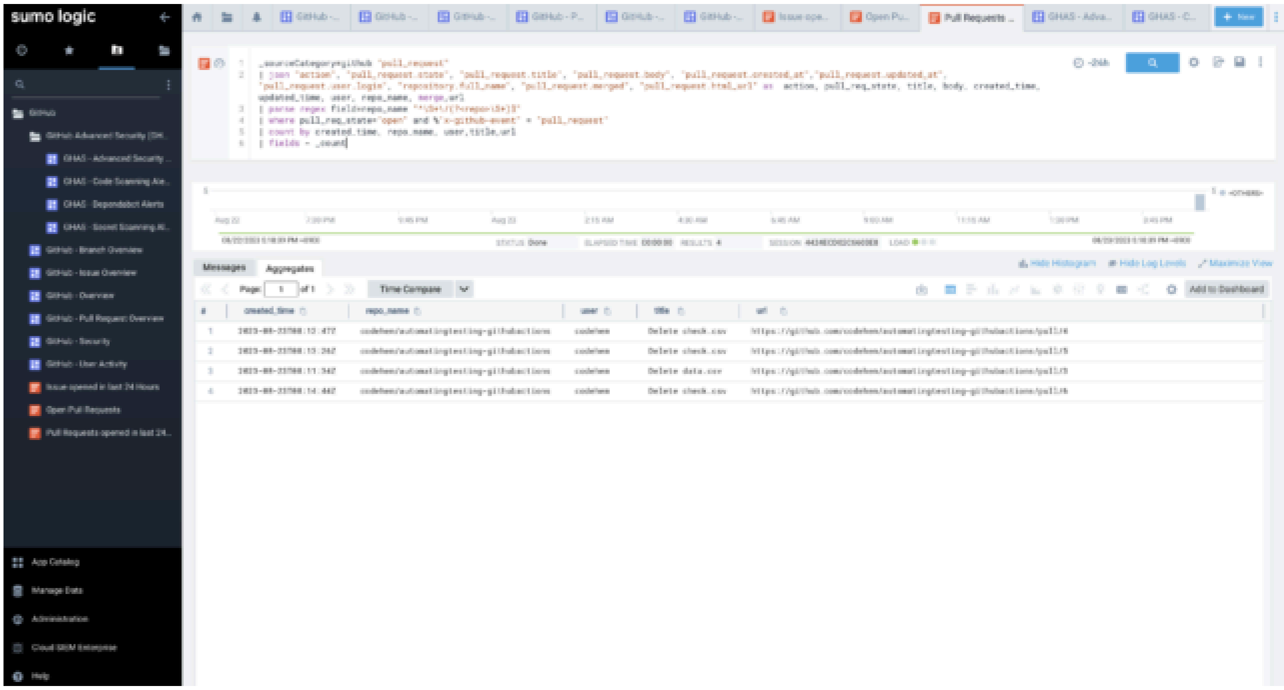


```
_sourceCategory=github "pull_request"
| json "action", "pull_request.title", "number", "pull_request.created_at","pull_request.user.login", "repository.name", "pull_request._links.html.href" as
action, title, id, created_time, user, repo_name, review_url
| where action in ("opened", "closed", "reopened") and %"x-github-event" = "pull_request"
| withtime action
|most_recent(action_withtime) as state by  id, title, created_time, user, repo_name , review_url
|where state  in ("opened", "reopened")
| order created_time asc
| fields id, title, repo_name, state,user,created_time, review_url
```

STATUS Done ELAPSED TIME 00:00:00 RESULTS 8

#	id	title	repo_name	state	user	created_time	review_url
1	4	Delete check.csv	automatingtesting-githubactions	opened	codehem	2023-08-22T08:12:41Z	https://github.com/codehem/automatingtesting-githubactions/pull/4
2	6	Delete check.csv	automatingtesting-githubactions	opened	codehem	2023-08-22T08:14:44Z	https://github.com/codehem/automatingtesting-githubactions/pull/6

Pull Requests opened in last 24 hours



```
_sourceCategory=github "pull_request"
| json "action", "pull_request.state", "pull_request.title", "pull_request.body", "pull_request.created_at","pull_request.updated_at",
"pull_request.user.login", "repository.full_name", "pull_request.merged", "pull_request.html_url" as action, pull_req_state, title, body, created_time,
updated_time, user, repo_name, merge,url
| parse regex field=repo_name "^\S+\/(?<repo>\S+)$"
| where pull_req_state="open" and %"x-github-event" = "pull_request"
| count by created_time, repo_name, user,title,url
| fields - _count
```

STATUS Done ELAPSED TIME 00:00:00 RESULTS 4

#	created_time	repo_name	user	title	url
1	2023-08-23T08:13:47Z	codehen/automatingtesting-githubactions	codehen	Delete check.csv	https://github.com/codehen/automatingtesting-githubactions/pull/4
2	2023-08-23T08:13:26Z	codehen/automatingtesting-githubactions	codehen	Delete check.csv	https://github.com/codehen/automatingtesting-githubactions/pull/5
3	2023-08-23T08:11:34Z	codehen/automatingtesting-githubactions	codehen	Delete data.csv	https://github.com/codehen/automatingtesting-githubactions/pull/3
4	2023-08-23T08:14:44Z	codehen/automatingtesting-githubactions	codehen	Delete check.csv	https://github.com/codehen/automatingtesting-githubactions/pull/6

Conclusion

We have unlocked a world of insights by seamlessly merging sumo logic with github's collaborative capability and extensive log analysis. We have access to improved dashboarding, quick searches, and thorough analysis.

EVENTS

【1/29（木）】クラスメソッドの会社説明会を開催します

開催前

【1/28（水）】クラスメソッドの新卒向け会社説明会を開催します

開催前

クラスメソッド会社説明会
フリーランス
エンジニア編
1.7(水) 12:30-13:00 / 19:00-19:30
【CMグループ/エンド直案件特集】

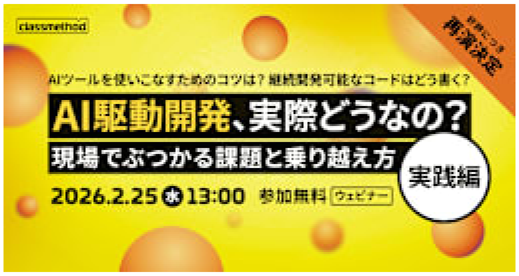
【CMグループ/エンド直案件特集】ITフリーランス向け「CMパートナーズ」説明会 by クラスメソッド

開催前

zendesk
classmethod
オペレーターの生産性を50%アップ!
見て、聞いて、納得できる
AIコールセンター実演セミナー
2026.2.5 木 15:00-18:00
クラスメソッド日比谷オフィス

【2/5（木）東京】オペレーターの生産性を50%アップ！見て、聞いて、納得できるAIコールセンター実演セミナー

開催前


classmethod
好評につき
再演決定
AIツールを使いこなすためのコツは？継続開発可能なコードはどう書く？
AI駆動開発、実際どうなの？
現場でぶつかる課題と乗り越え方
実践編
2026.2.25 水 13:00 参加無料 ウェビナー

【2/25（水）】AI駆動開発、実際どうなの？【実践編】～現場でぶつかる課題と乗り越え方～

開催前

【1/29（木）】今日から始めるAWSセキュリティ対策 3ステップでわかる実践ガイド

開催前

セミナー一覧　会社説明会一覧　勉強会一覧