RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **HT-R06**

Goodbye Credential Leaks: Securing Code Together

Mariam Sulakian, CIPP/US

Product Manager
GitHub

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Agenda

background

detection

remediation

prevention

take aways

RSAConference2022

Credential leaks are a human error

Background: How & why secrets leak

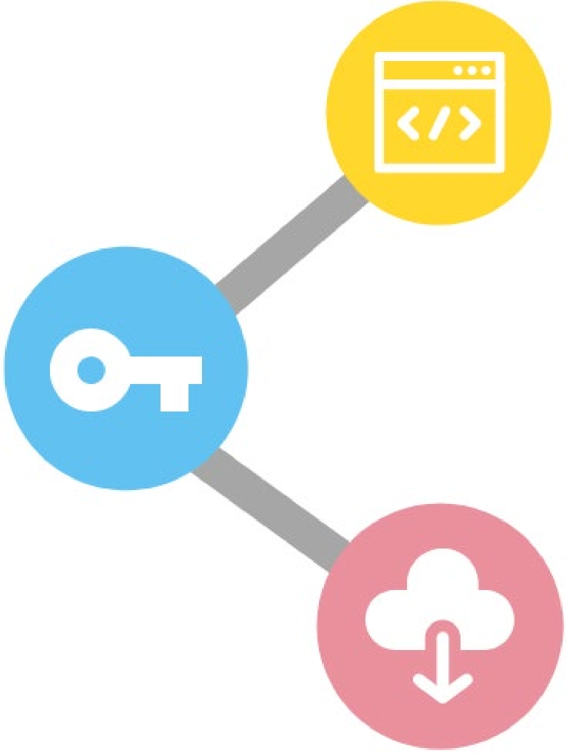
How do secrets get leaked?

Leaked secrets allow malicious actors to impersonate others & fraudulently use services

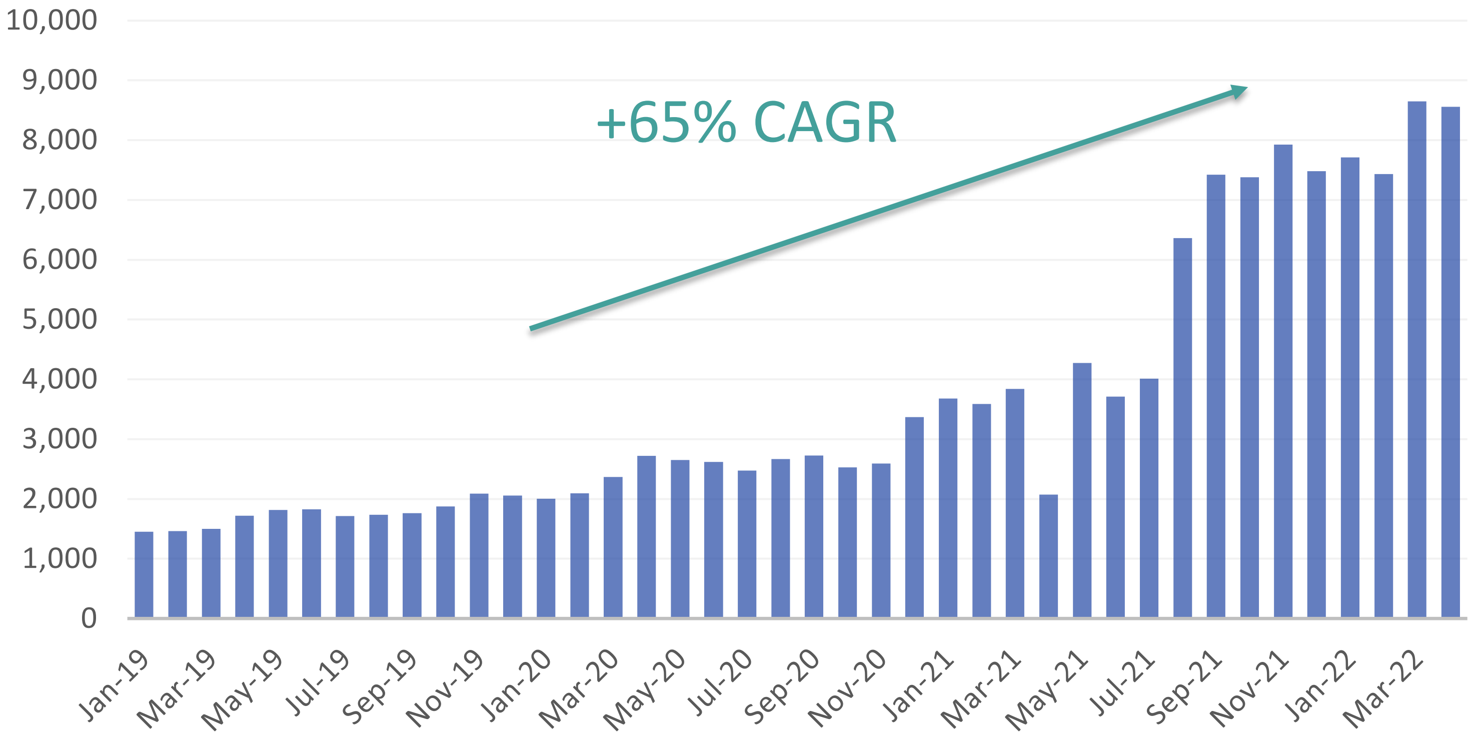
On accident

Left in git commit history

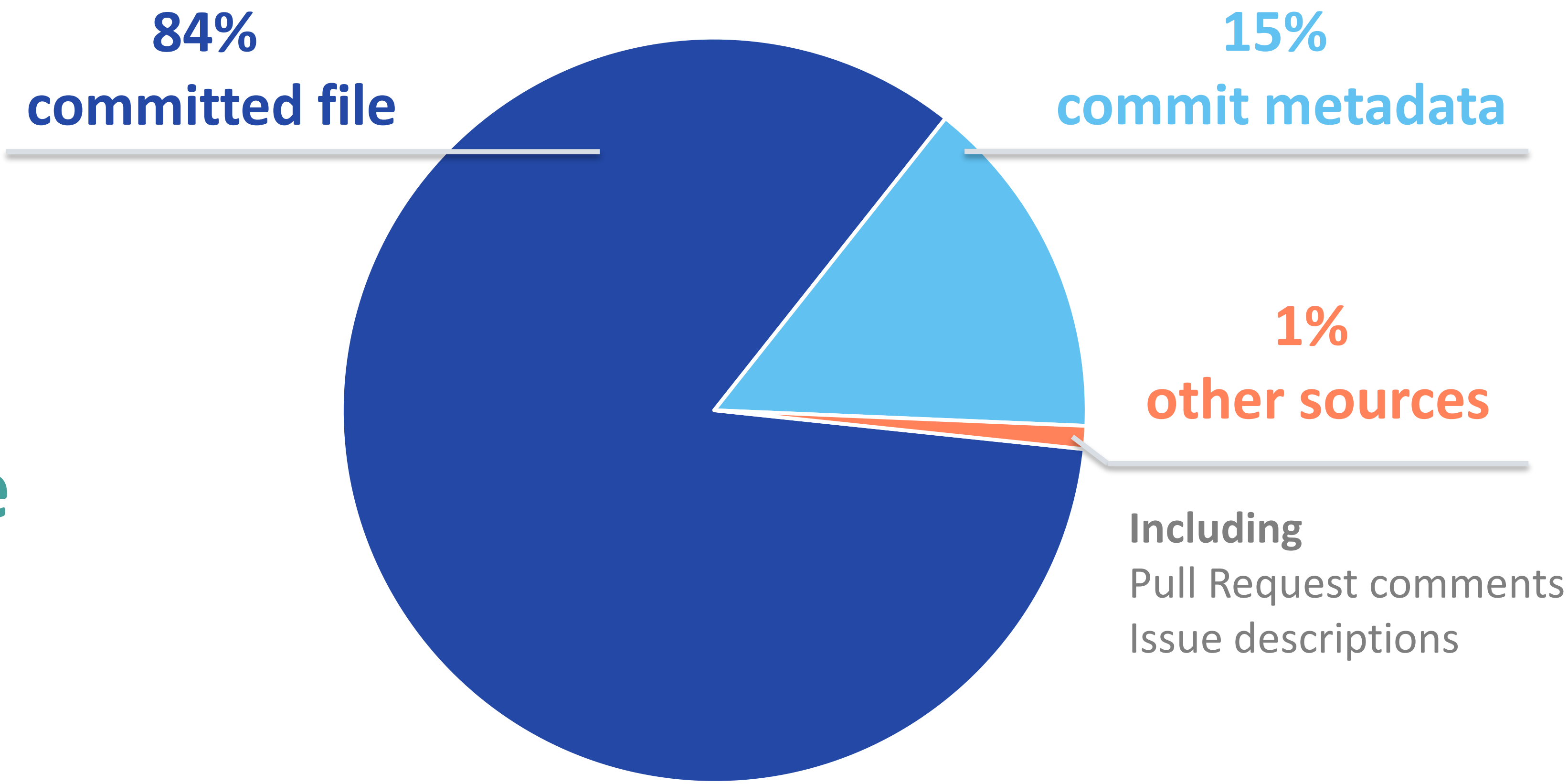
Intentionally



Contributors leak over 100 GitHub tokens a DAY!



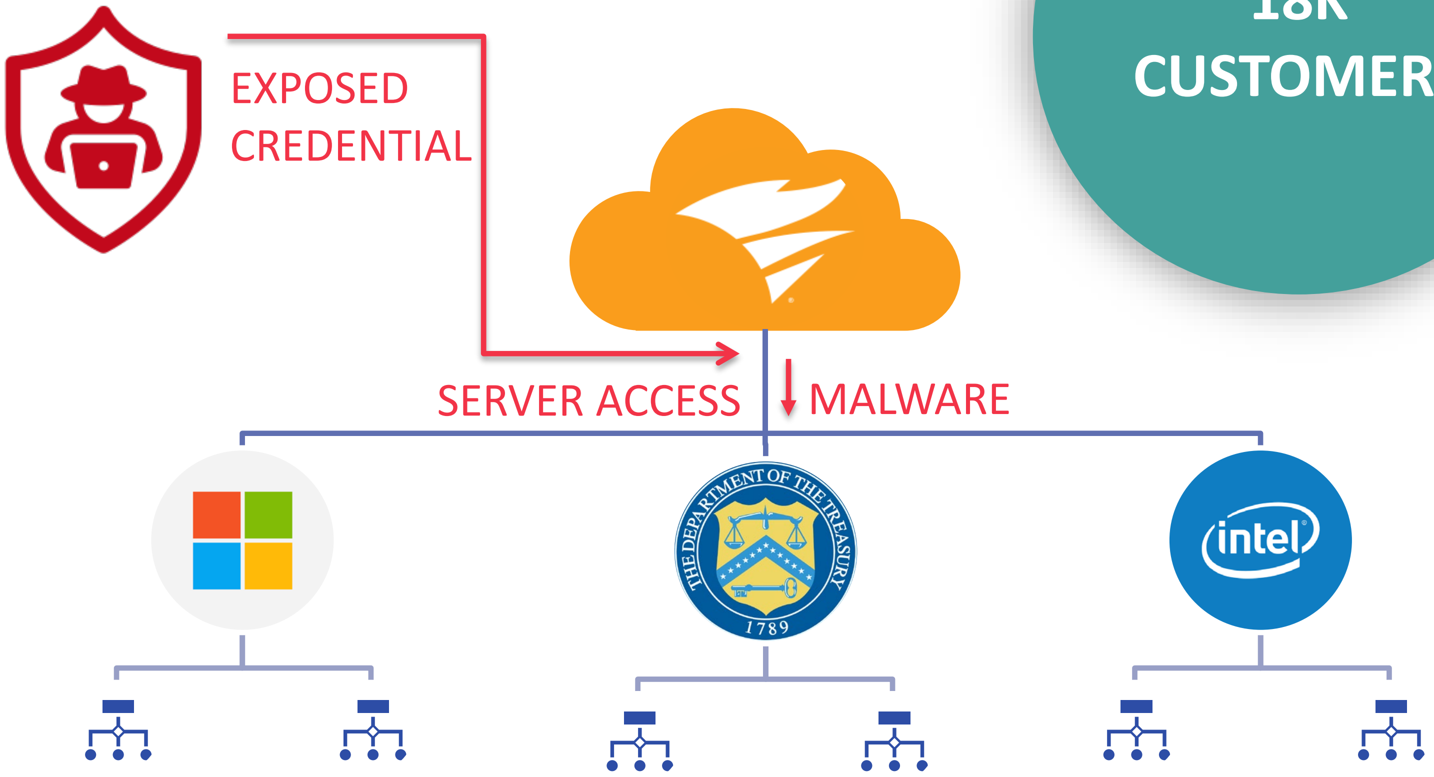
Secrets can leak anywhere you're building software



Including
Pull Request comments
Issue descriptions

18K CUSTOMERS

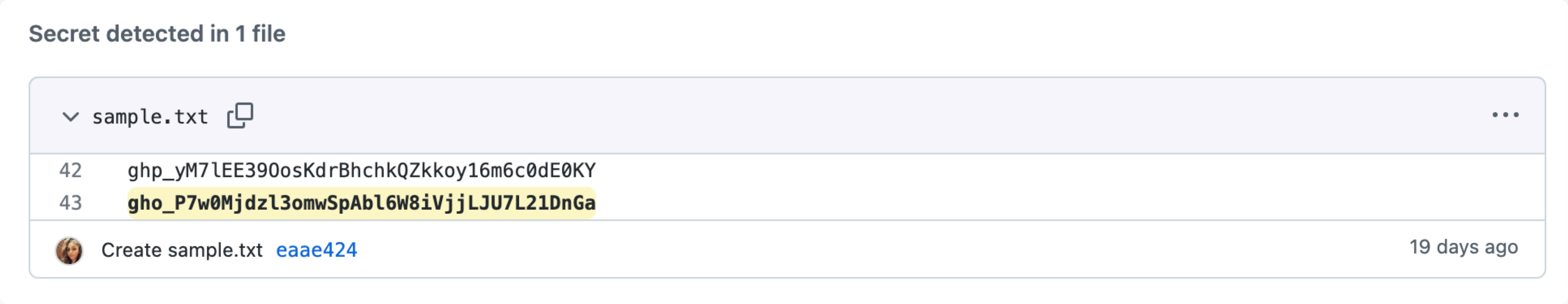
One secret is all it takes



RSAConference2022

Detecting your leaks

Reactively finding & remediating exposed secrets



Secret detected in 1 file

sample.txt

```
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
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
```

Create sample.txt eaae424

19 days ago

You leaked a secret…now what?

Detecting tokens with GitHub secret scanning

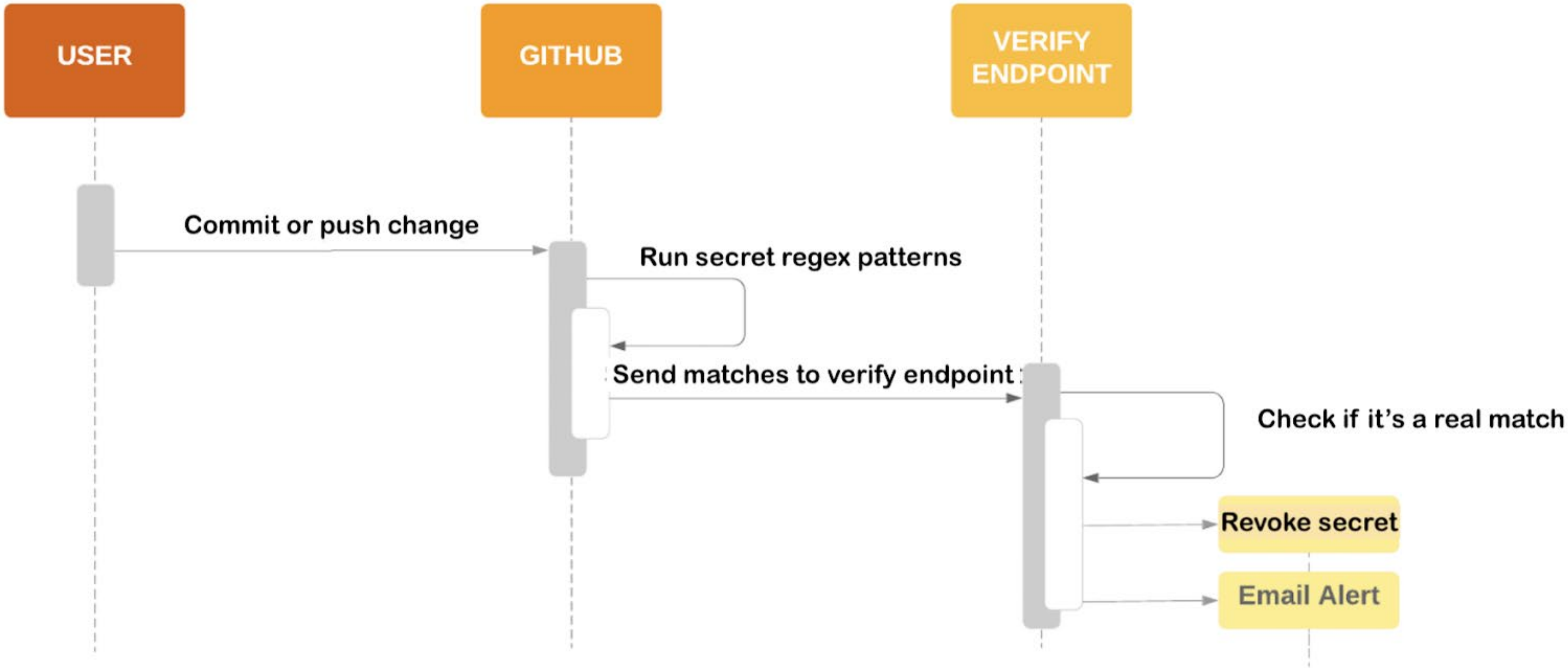
Service enabled by default on GitHub.com

Scans public contributions for secrets

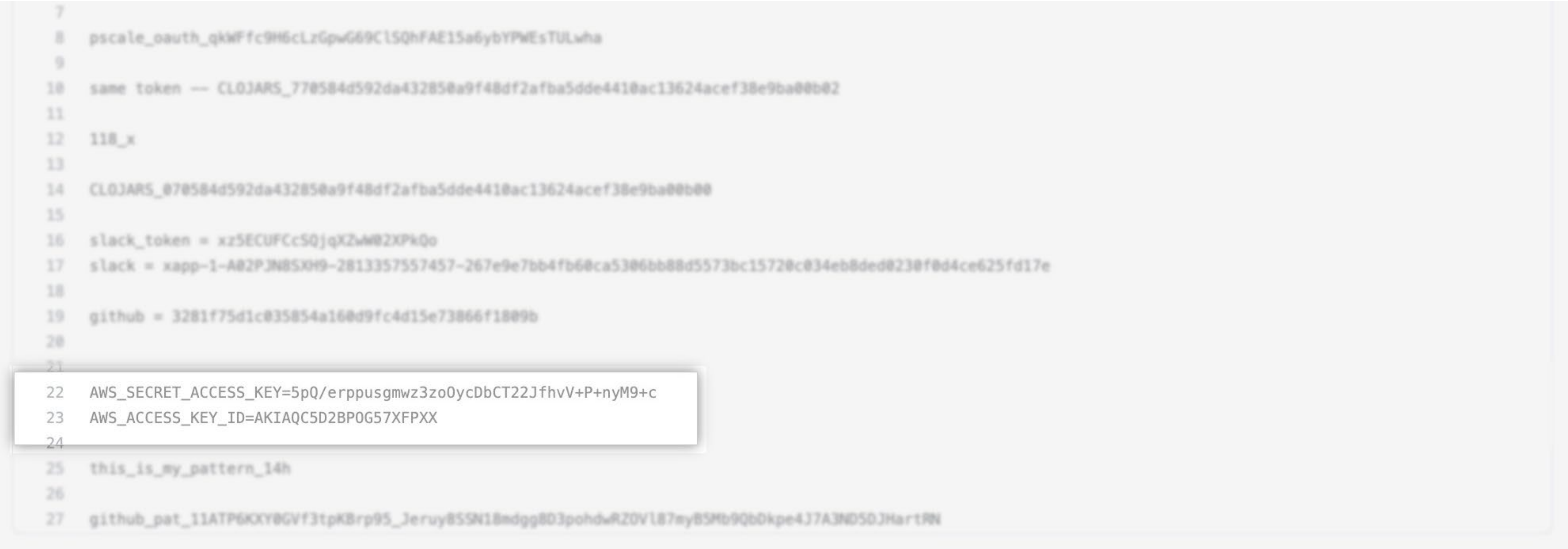
Notifies provider for leaked secrets

Available through GitHub Advanced Security for private repositories

Secret scanning

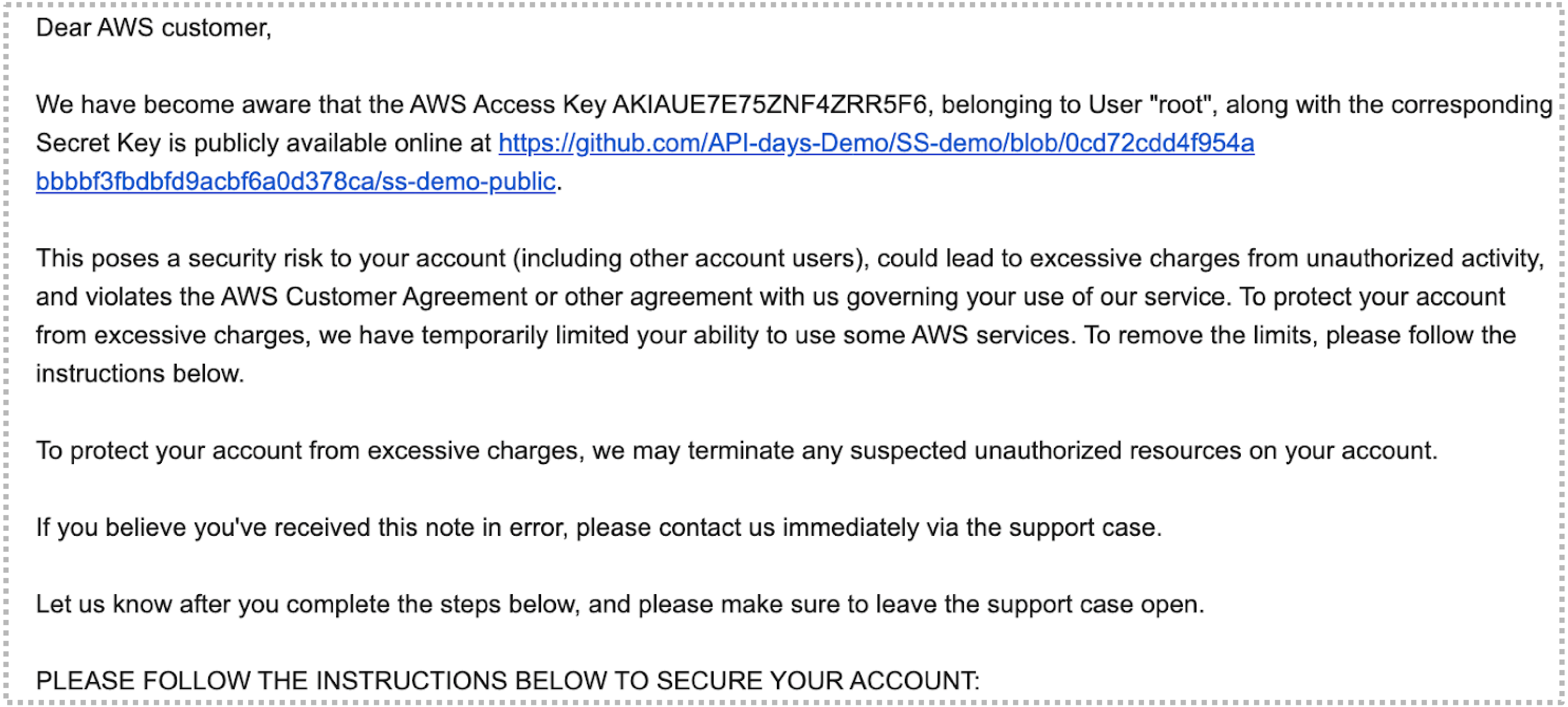

USER
GITHUB
VERIFY ENDPOINT
Commit or push change
Run secret regex patterns
Send matches to verify endpoint
Check if it’s a real match
Revoke secret
Email Alert

A case study: leaking AWS credentials



```

pscale_oauth_qkWFfc9H6cLzGpwG69ClSQhFAE15a6ybYPWEsTULwha

same token -- CLOJARS_770584d592da432850a9f48df2afba5dde4410ac13624acef38e9ba00b02

118_x

CLOJARS_070584d592da432850a9f48df2afba5dde4410ac13624acef38e9ba00b00

slack_token = xz5ECUFCcSQjqXZwW02XPkQo
slack = xapp-1-A02PJN8SXH9-2813357557457-267e9e7bb4fb60ca5306bb88d5573bc15720c034eb8ded0230f0d4ce625fd17e

github = 3281f75d1c035854a160d9fc4d15e73866f1809b


AWS_SECRET_ACCESS_KEY=5pQ/erppusgmwz3zoOycDbCT22JfhvV+P+nyM9+c
AWS_ACCESS_KEY_ID=AKIAQC5D2BPOG57XFPXX

this_is_my_pattern_14h

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
```

A case study: leaking AWS credentials



Dear AWS customer,

We have become aware that the AWS Access Key AKIAUE7E75ZNF4ZRR5F6, belonging to User "root", along with the corresponding Secret Key is publicly available online at https://github.com/API-days-Demo/SS-demo/blob/0cd72cdd4f954abbbbf3fbdbfd9acbf6a0d378ca/ss-demo-public.

This poses a security risk to your account (including other account users), could lead to excessive charges from unauthorized activity, and violates the AWS Customer Agreement or other agreement with us governing your use of our service. To protect your account from excessive charges, we have temporarily limited your ability to use some AWS services. To remove the limits, please follow the instructions below.

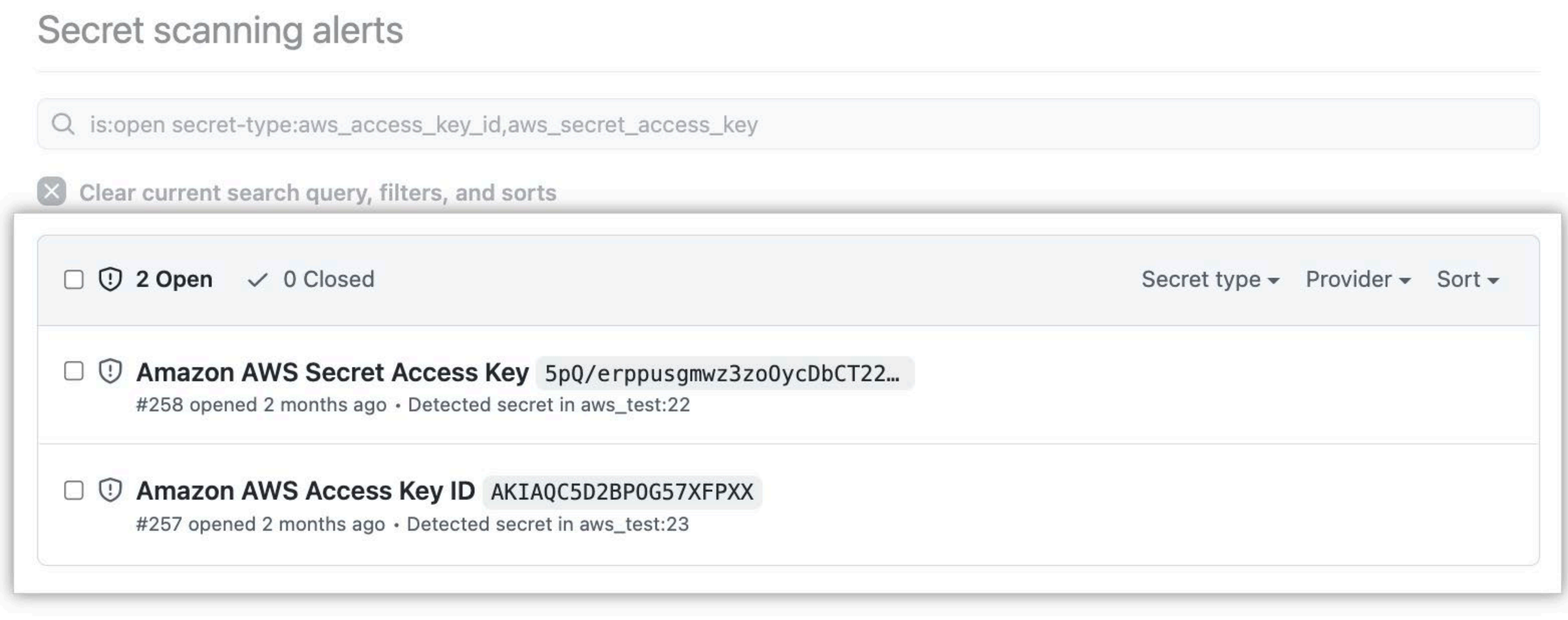
To protect your account from excessive charges, we may terminate any suspected unauthorized resources on your account.

If you believe you've received this note in error, please contact us immediately via the support case.

Let us know after you complete the steps below, and please make sure to leave the support case open.

PLEASE FOLLOW THE INSTRUCTIONS BELOW TO SECURE YOUR ACCOUNT:

A case study: leaking AWS credentials



Secret scanning alerts

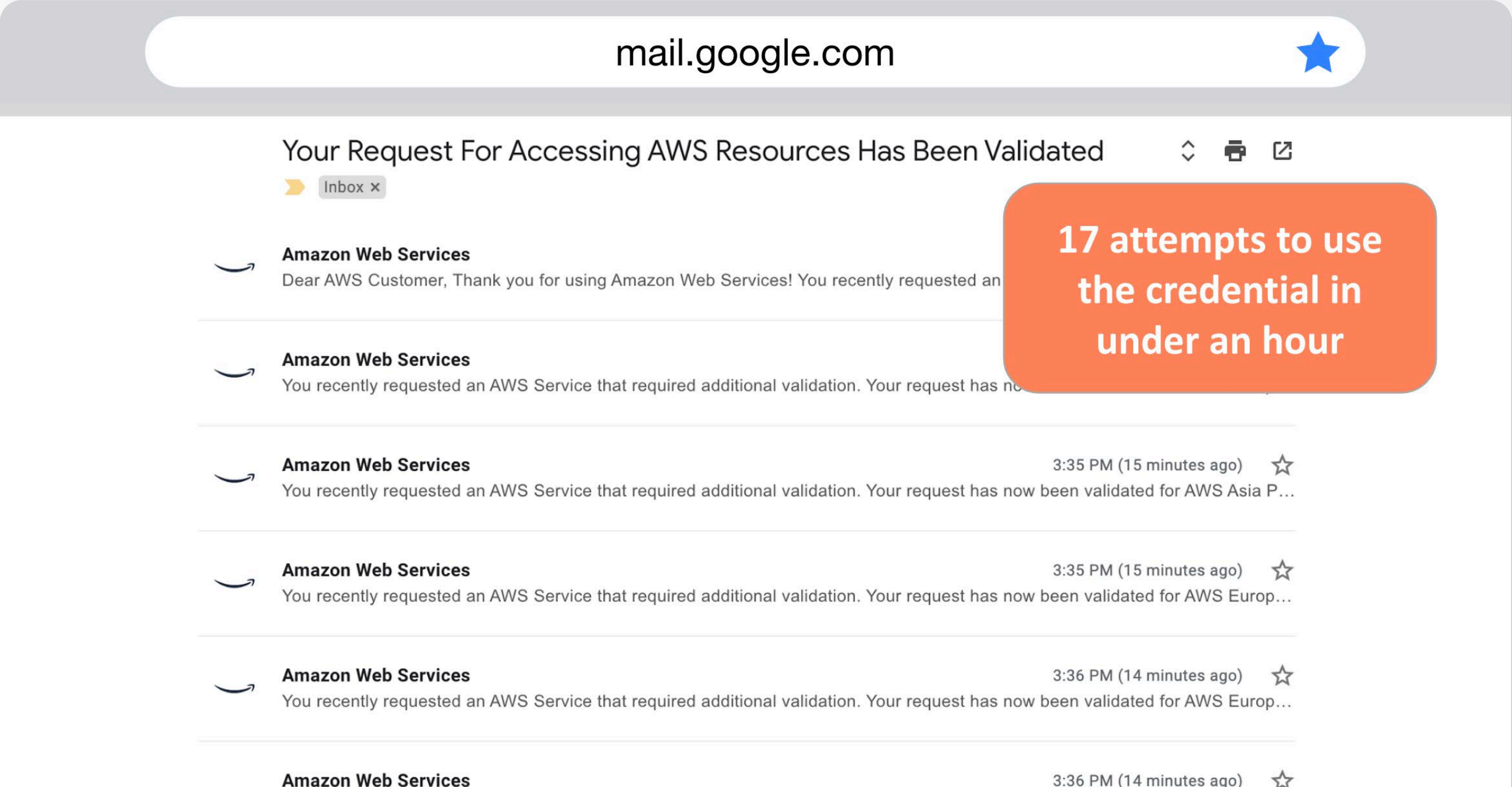
is:open secret-type:aws_access_key_id,aws_secret_access_key

☒ Clear current search query, filters, and sorts

□ **Amazon AWS Secret Access Key** `5pQ/erppusgmwz3zo0ycDbCT22…`
#258 opened 2 months ago • Detected secret in aws_test:22

□ **Amazon AWS Access Key ID** `AKIAQC5D2BP0G57XFPXX`
#257 opened 2 months ago • Detected secret in aws_test:23

A case study: leaking AWS credentials



mail.google.com

Your Request For Accessing AWS Resources Has Been Validated

Inbox ×

Amazon Web Services
Dear AWS Customer, Thank you for using Amazon Web Services! You recently requested an

Amazon Web Services
You recently requested an AWS Service that required additional validation. Your request has no

Amazon Web Services 3:35 PM (15 minutes ago)
You recently requested an AWS Service that required additional validation. Your request has now been validated for AWS Asia P…

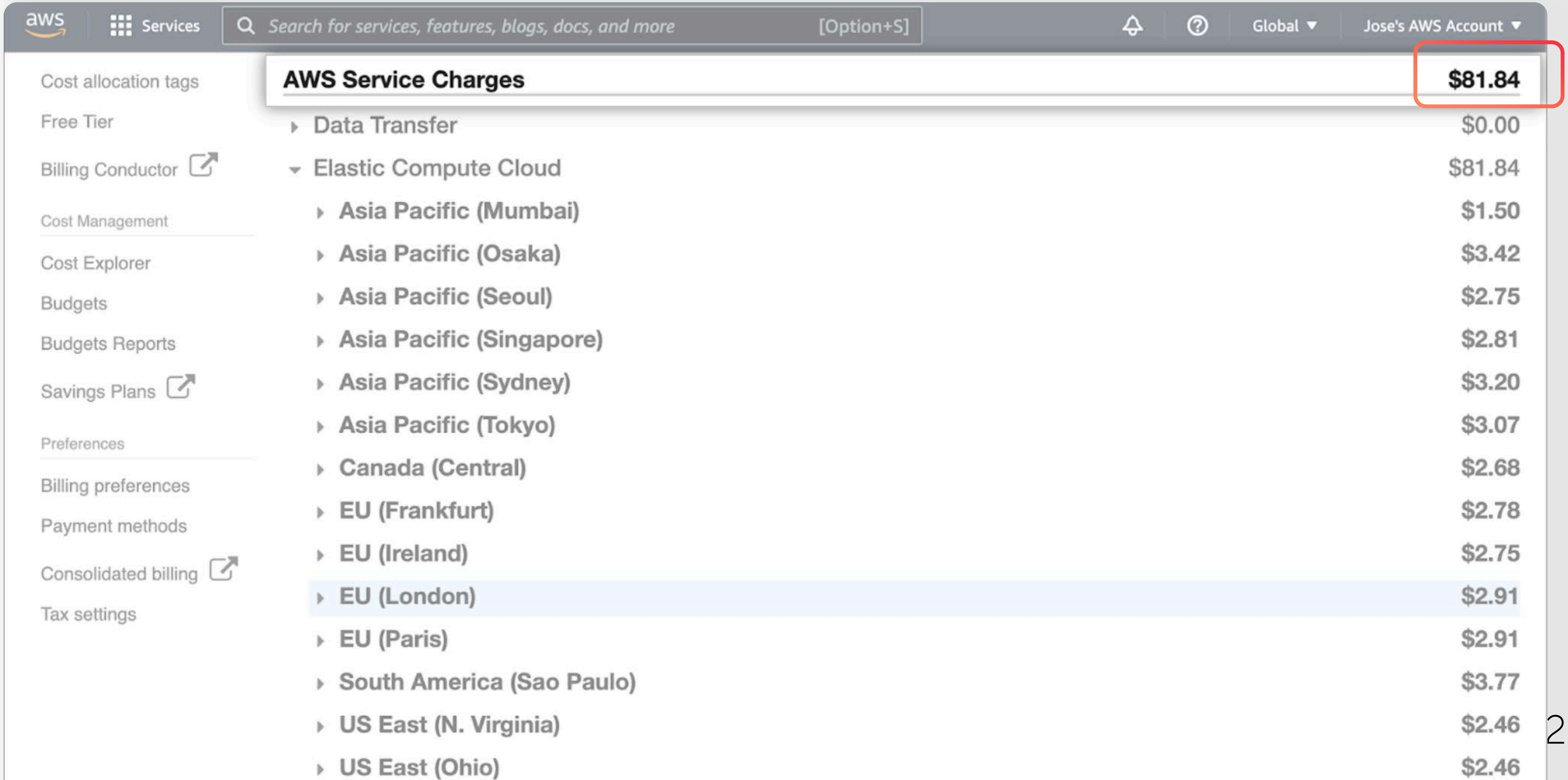
Amazon Web Services 3:35 PM (15 minutes ago)
You recently requested an AWS Service that required additional validation. Your request has now been validated for AWS Europ…

Amazon Web Services 3:36 PM (14 minutes ago)
You recently requested an AWS Service that required additional validation. Your request has now been validated for AWS Europ…

Amazon Web Services 3:36 PM (14 minutes ago)

17 attempts to use the credential in under an hour

A case study: leaking AWS credentials

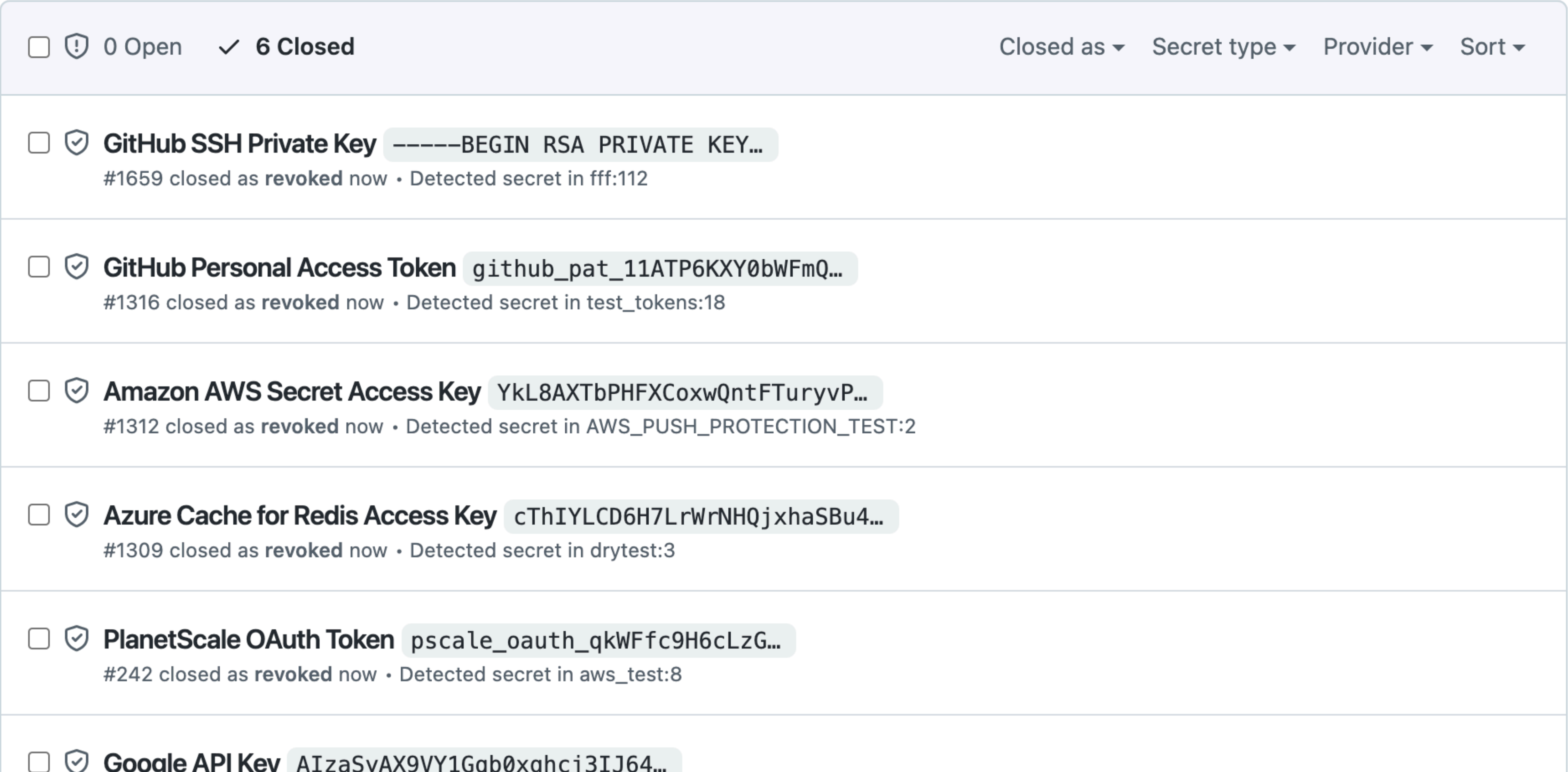


Cost allocation tags
Free Tier
Billing Conductor
Cost Management
Cost Explorer
Budgets
Budgets Reports
Savings Plans
Preferences
Billing preferences
Payment methods
Consolidated billing
Tax settings

AWS Service Charges	$81.84
Data Transfer	$0.00
Elastic Compute Cloud	$81.84
Asia Pacific (Mumbai)	$1.50
Asia Pacific (Osaka)	$3.42
Asia Pacific (Seoul)	$2.75
Asia Pacific (Singapore)	$2.81
Asia Pacific (Sydney)	$3.20
Asia Pacific (Tokyo)	$3.07
Canada (Central)	$2.68
EU (Frankfurt)	$2.78
EU (Ireland)	$2.75
EU (London)	$2.91
EU (Paris)	$2.91
South America (Sao Paulo)	$3.77
US East (N. Virginia)	$2.46
US East (Ohio)	$2.46

Increasing signal, reducing noise

Keeping false positives low



□ 0 Open ✓ 6 Closed

□ **GitHub SSH Private Key** `-----BEGIN RSA PRIVATE KEY…`
#1659 closed as **revoked** now • Detected secret in fff:112

□ **GitHub Personal Access Token** `github_pat_11ATP6KXY0bWFmQ…`
#1316 closed as **revoked** now • Detected secret in test_tokens:18

□ **Amazon AWS Secret Access Key** `YkL8AXTbPHFXCoxwQntFTuryvP…`
#1312 closed as **revoked** now • Detected secret in AWS_PUSH_PROTECTION_TEST:2

□ **Azure Cache for Redis Access Key** `cThIYLCD6H7LrWrNHQjxhaSBu4…`
#1309 closed as **revoked** now • Detected secret in drytest:3

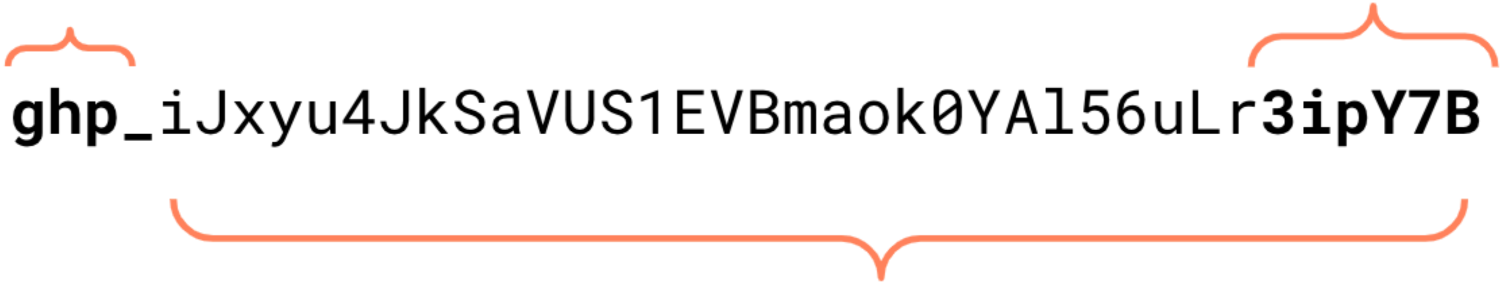
□ **PlanetScale OAuth Token** `pscale_oauth_qkWFfc9H6cLzG…`
#242 closed as **revoked** now • Detected secret in aws_test:8

□ **Google API Key** `AIzaSyAX9VY1Gqb0xqhci3IJ64…`

Identifiable tokens = better tokens

Defined prefixes with “_” for highlighting

32 bit checksum:
validate token without hitting a database



ghp_iJxyu4JkSaVUS1EVBmaok0YAl56uLr**3ipY7B**

High entropy random strings

Identifiable tokens: the false positive remedy

Before

je5WGi23lgk84GEPQglwafj3slgk2lgiwhio8rgk

842b9e8fb032869e88b653fc4df0786240ae6174209b8505c2f9e228a2144e8c

After

prefix

32-bit checksum

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

dop_v1_ae5067bb5c1d3bcb1f9e580f7a8dd56186f27791101ccc32bd942c8eb9247901

prefix

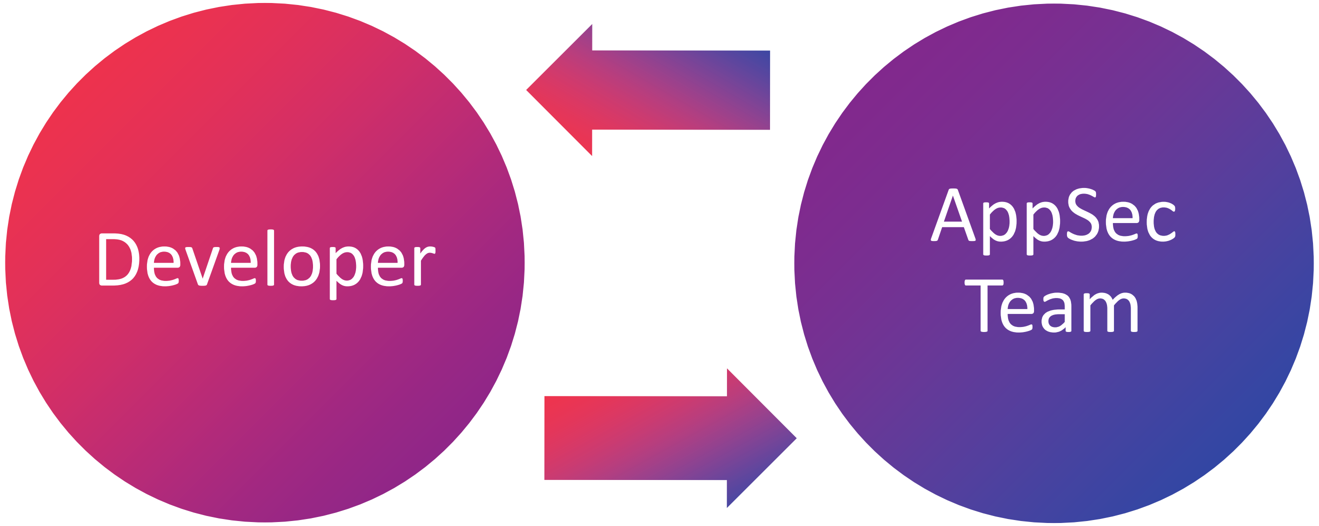
High entropy (randomness)

Remediating leaks

When a secret does leak…

How do I remediate a leaked secret?

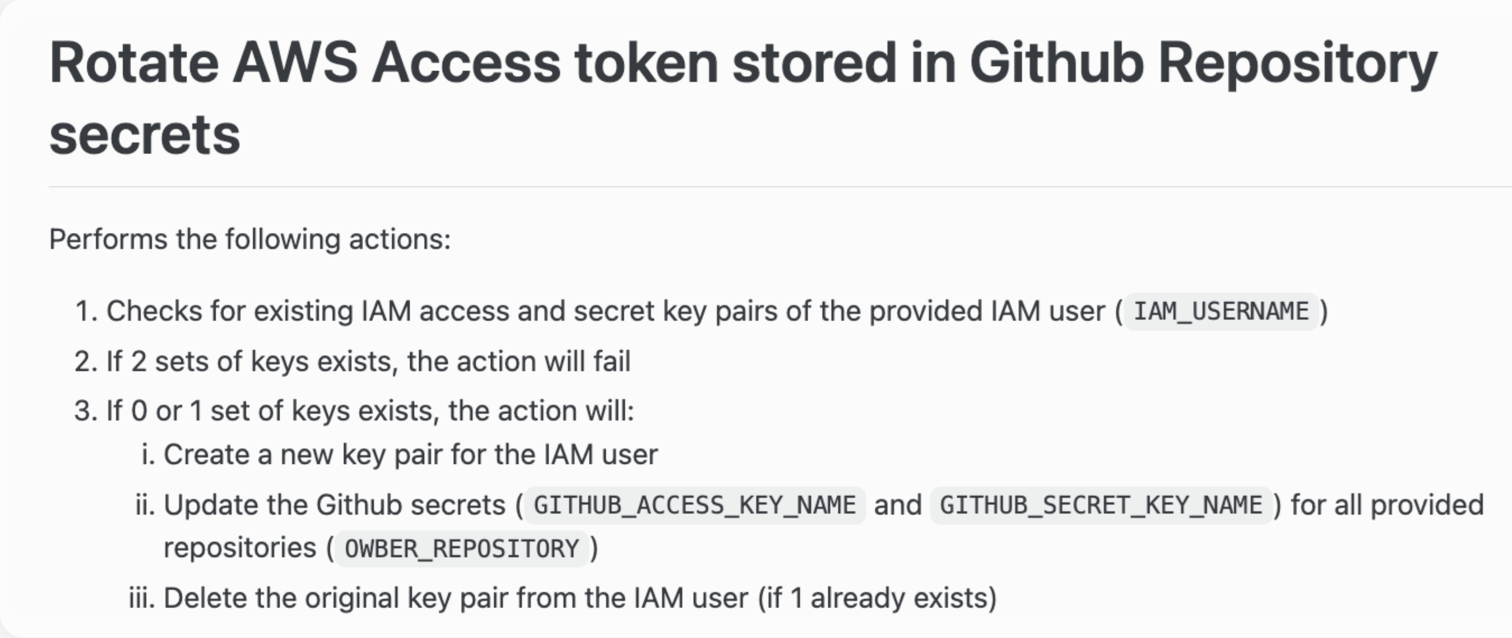
Assess impact to revoke



How do I remediate a leaked secret?

Assess impact to revoke

Rotate the secret



Rotate AWS Access token stored in Github Repository secrets

Performs the following actions:

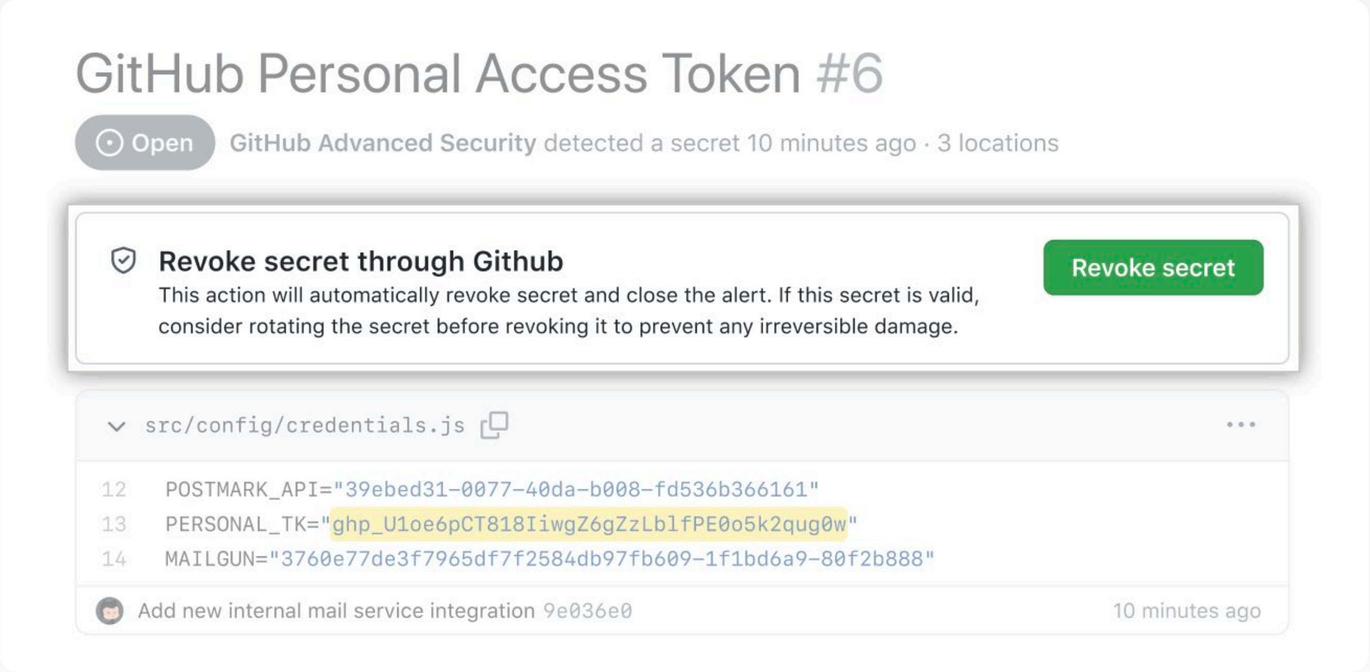
1. Checks for existing IAM access and secret key pairs of the provided IAM user (`IAM_USERNAME`)
2. If 2 sets of keys exists, the action will fail
3. If 0 or 1 set of keys exists, the action will:
    1. Create a new key pair for the IAM user
    2. Update the Github secrets (`GITHUB_ACCESS_KEY_NAME` and `GITHUB_SECRET_KEY_NAME`) for all provided repositories (`OWBER_REPOSITORY`)
    3. Delete the original key pair from the IAM user (if 1 already exists)

How do I remediate a leaked secret?

Assess impact to revoke

Rotate the secret

Revoke the secret



GitHub Personal Access Token #6

GitHub Advanced Security detected a secret 10 minutes ago · 3 locations

Revoke secret through Github

This action will automatically revoke secret and close the alert. If this secret is valid, consider rotating the secret before revoking it to prevent any irreversible damage.

src/config/credentials.js

```
POSTMARK_API="39ebed31-0077-40da-b008-fd536b366161"
PERSONAL_TK="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"
MAILGUN="3760e77de3f7965df7f2584db97fb609-1f1bd6a9-80f2b888"
```

Add new internal mail service integration 9e036e0 10 minutes ago

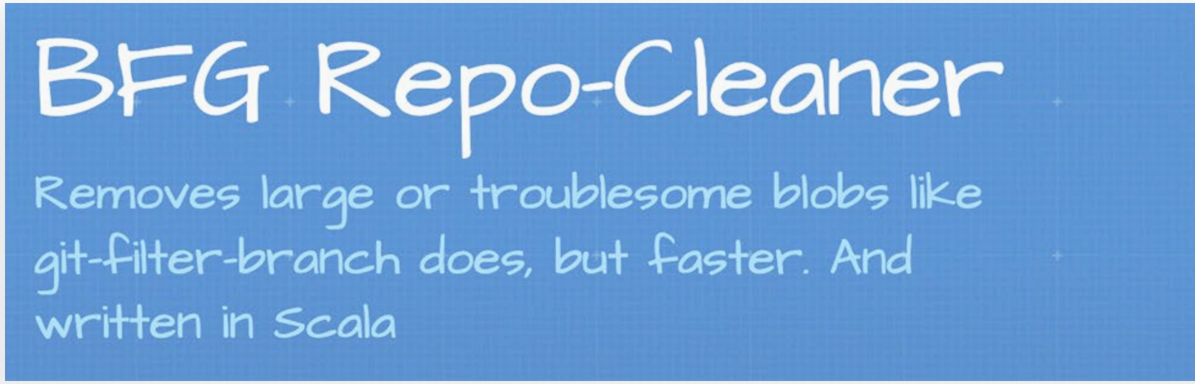
How do I remediate a leaked secret?

Assess impact to revoke

Rotate the secret

Revoke the secret

Rewrite your git history



BFG Repo-Cleaner

Removes large or troublesome blobs like git-filter-branch does, but faster. And written in Scala

Even if your leak was in a private repository…

Check **API activity logs** to ensure you've remediated *in time*

Monitor repository **access permissions**

Ensure proper **secrets management**

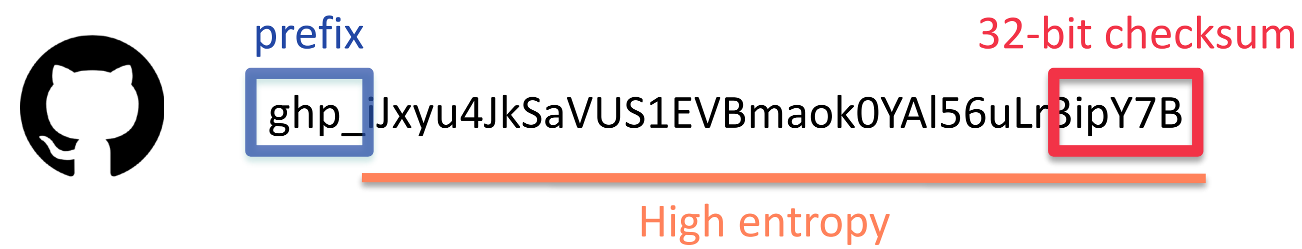
Connect with Ops and AppSec teams

RSA®Conference2022

Preventing leaks

Working proactively

Proactive prevention



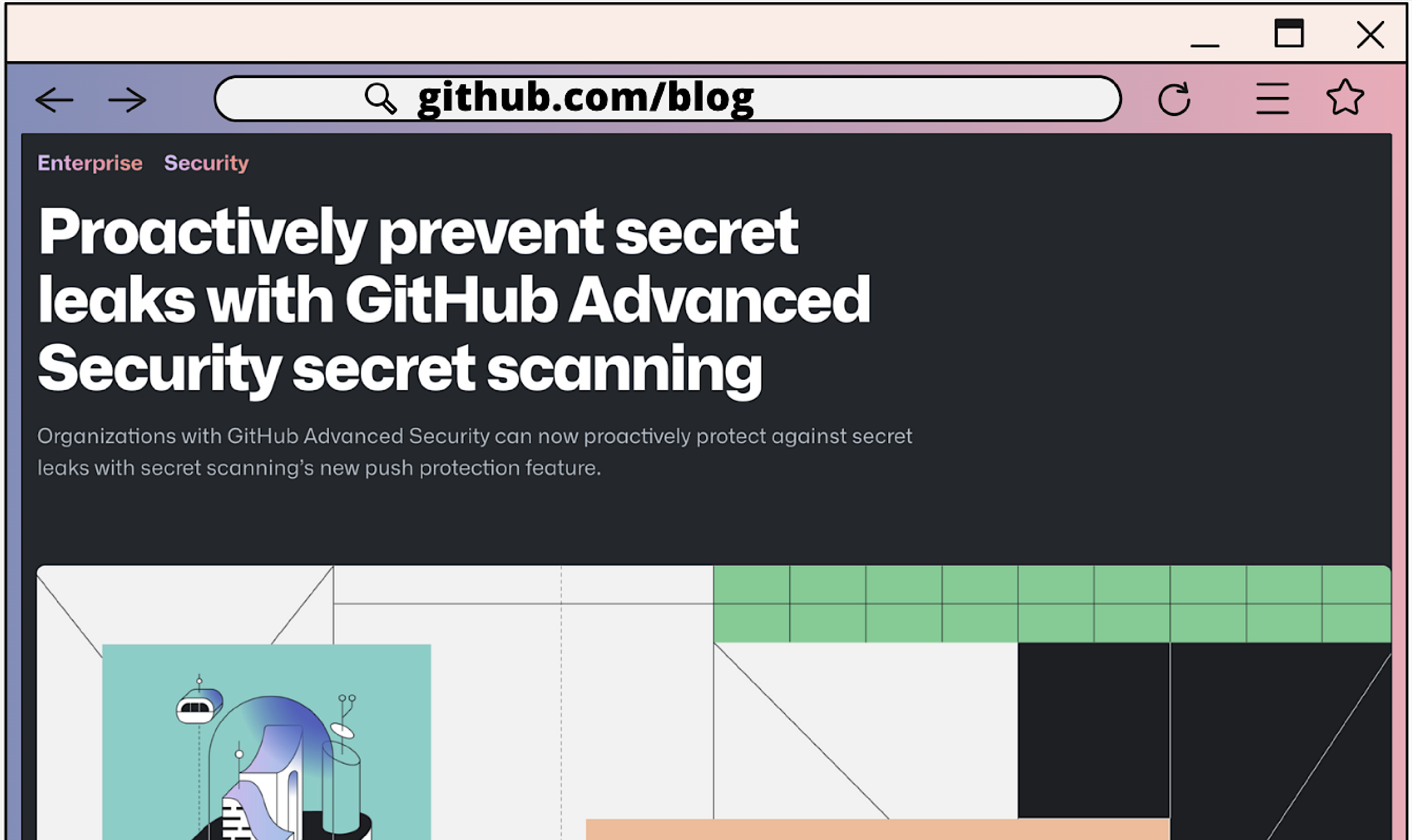
prefix

32-bit checksum

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

High entropy

IDENTIFY token → protect on **PUSH**



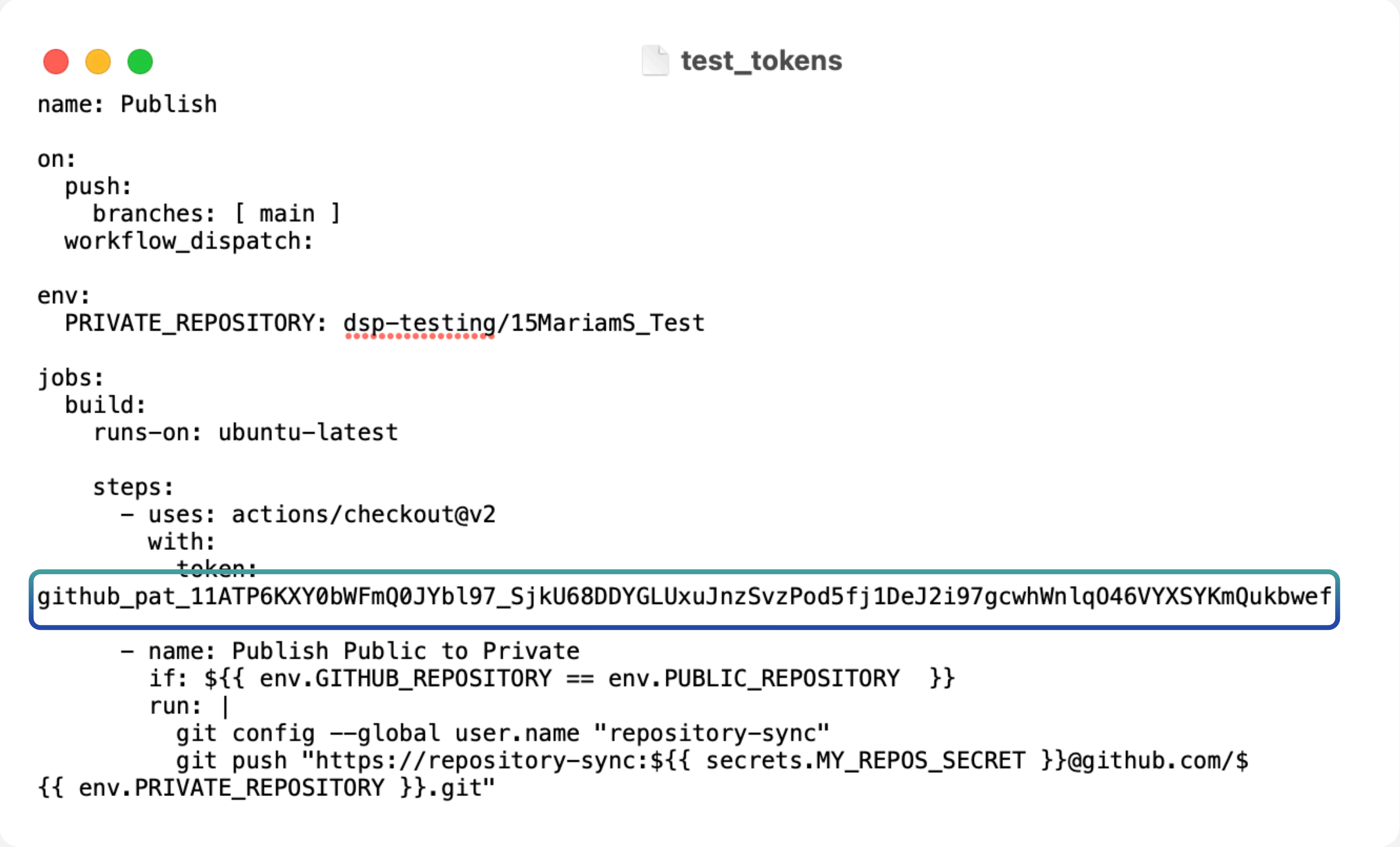
Enterprise Security

Proactively prevent secret leaks with GitHub Advanced Security secret scanning

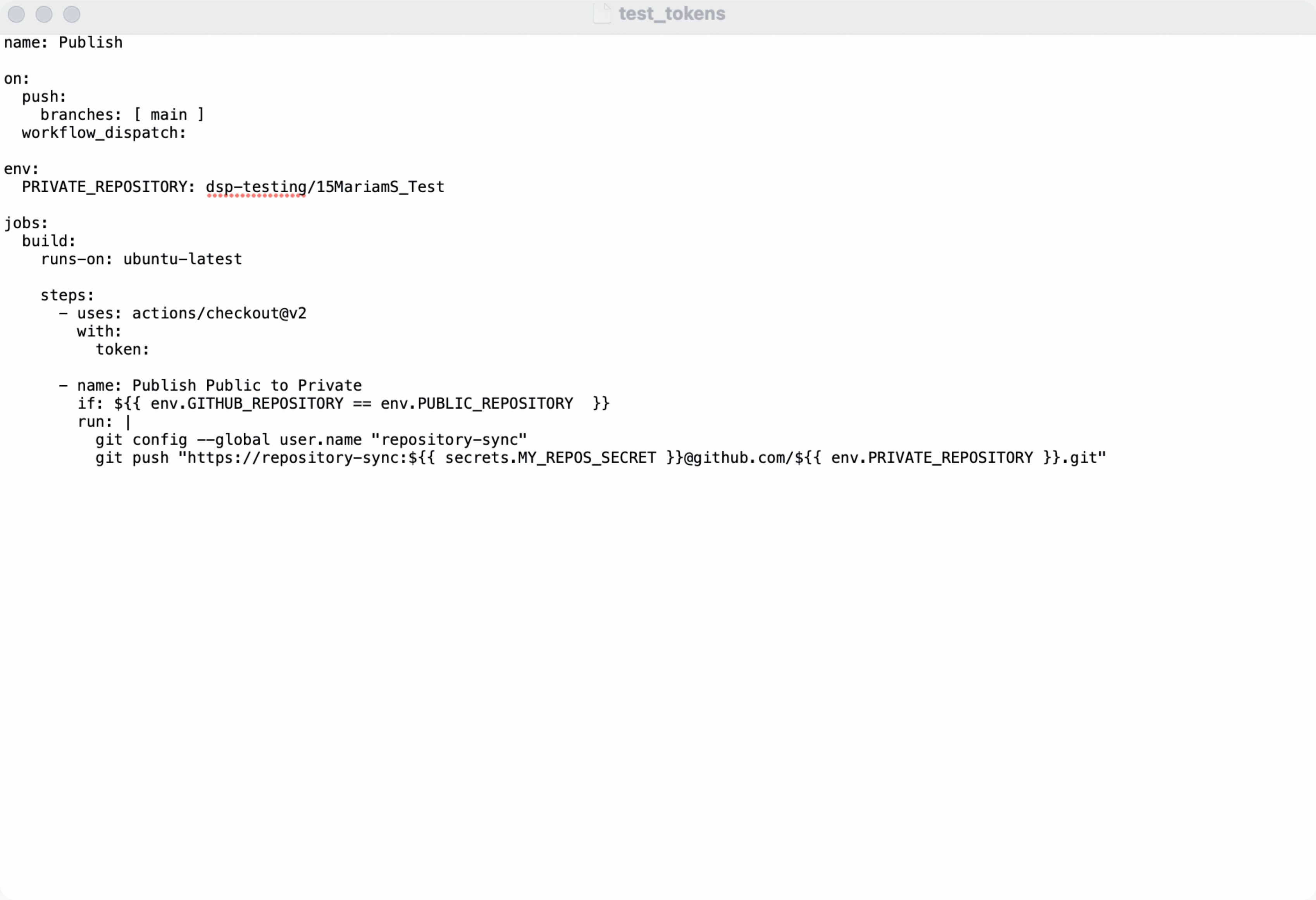
Organizations with GitHub Advanced Security can now proactively protect against secret leaks with secret scanning's new push protection feature.

Demo:

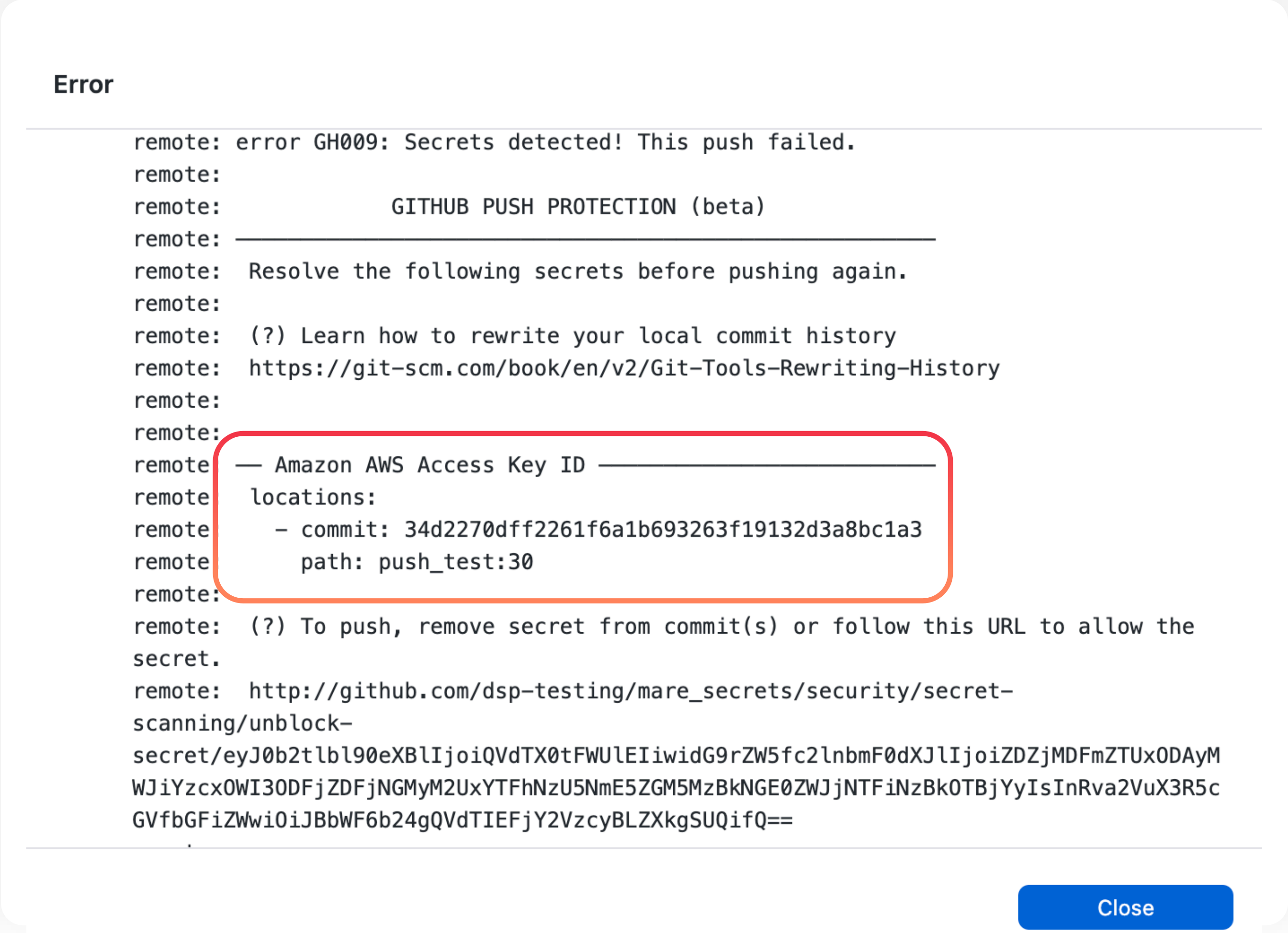
Secret scanning as a push protection



```
name: Publish

on:
  push:
    branches: [ main ]
  workflow_dispatch:

env:
  PRIVATE_REPOSITORY: dsp-testing/15MariamS_Test

jobs:
  build:
    runs-on: ubuntu-latest

    steps:
      - uses: actions/checkout@v2
        with:
          token:
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

      - name: Publish Public to Private
        if: ${{ env.GITHUB_REPOSITORY == env.PUBLIC_REPOSITORY  }}
        run: |
          git config --global user.name "repository-sync"
          git push "https://repository-sync:${{ secrets.MY_REPOS_SECRET }}@github.com/$
{{ env.PRIVATE_REPOSITORY }}.git"
```

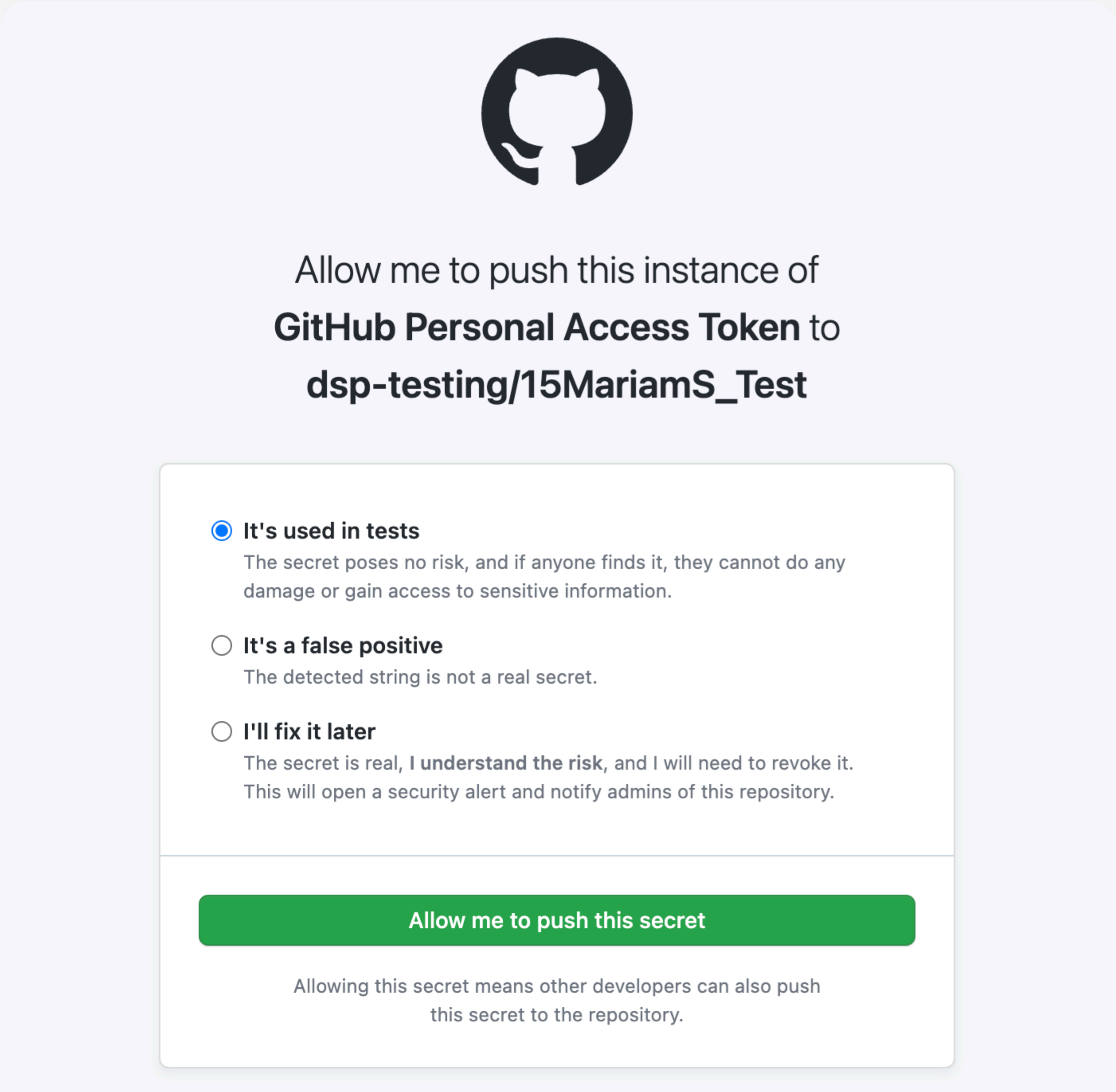


```
name: Publish

on:
  push:
    branches: [ main ]
  workflow_dispatch:

env:
  PRIVATE_REPOSITORY: dsp-testing/15MariamS_Test

jobs:
  build:
    runs-on: ubuntu-latest

    steps:
      - uses: actions/checkout@v2
        with:
          token:

      - name: Publish Public to Private
        if: ${{ env.GITHUB_REPOSITORY == env.PUBLIC_REPOSITORY  }}
        run: |
          git config --global user.name "repository-sync"
          git push "https://repository-sync:${{ secrets.MY_REPOS_SECRET }}@github.com/${{ env.PRIVATE_REPOSITORY }}.git"
```



```
remote: error GH009: Secrets detected! This push failed.
remote:
remote:             GITHUB PUSH PROTECTION (beta)
remote: ———————————————————————————————————————————————————————
remote:  Resolve the following secrets before pushing again.
remote:
remote:  (?) Learn how to rewrite your local commit history
remote:  https://git-scm.com/book/en/v2/Git-Tools-Rewriting-History
remote:
remote:
remote  —— Amazon AWS Access Key ID ——————————————————————————
remote   locations:
remote     - commit: 34d2270dff2261f6a1b693263f19132d3a8bc1a3
remote       path: push_test:30
remote:
remote:  (?) To push, remove secret from commit(s) or follow this URL to allow the
secret.
remote:  http://github.com/dsp-testing/mare_secrets/security/secret-
scanning/unblock-
secret/eyJ0b2tlbl90eXBlIjoiQVdTX0tFWUlEIiwidG9rZW5fc2lnbmF0dXJlIjoiZDZjMDFmZTUxODAyM
WJiYzcxOWI3ODFjZDFjNGMyM2UxYTFhNzU5NmE5ZGM5MzBkNGE0ZWJjNTFiNzBkOTBjYyIsInRva2VuX3R5c
GVfbGFiZWwiOiJBbWF6b24gQVdTIEFjY2VzcyBLZXkgSUQifQ==
```

Protect developers from accidentally exposing credentials



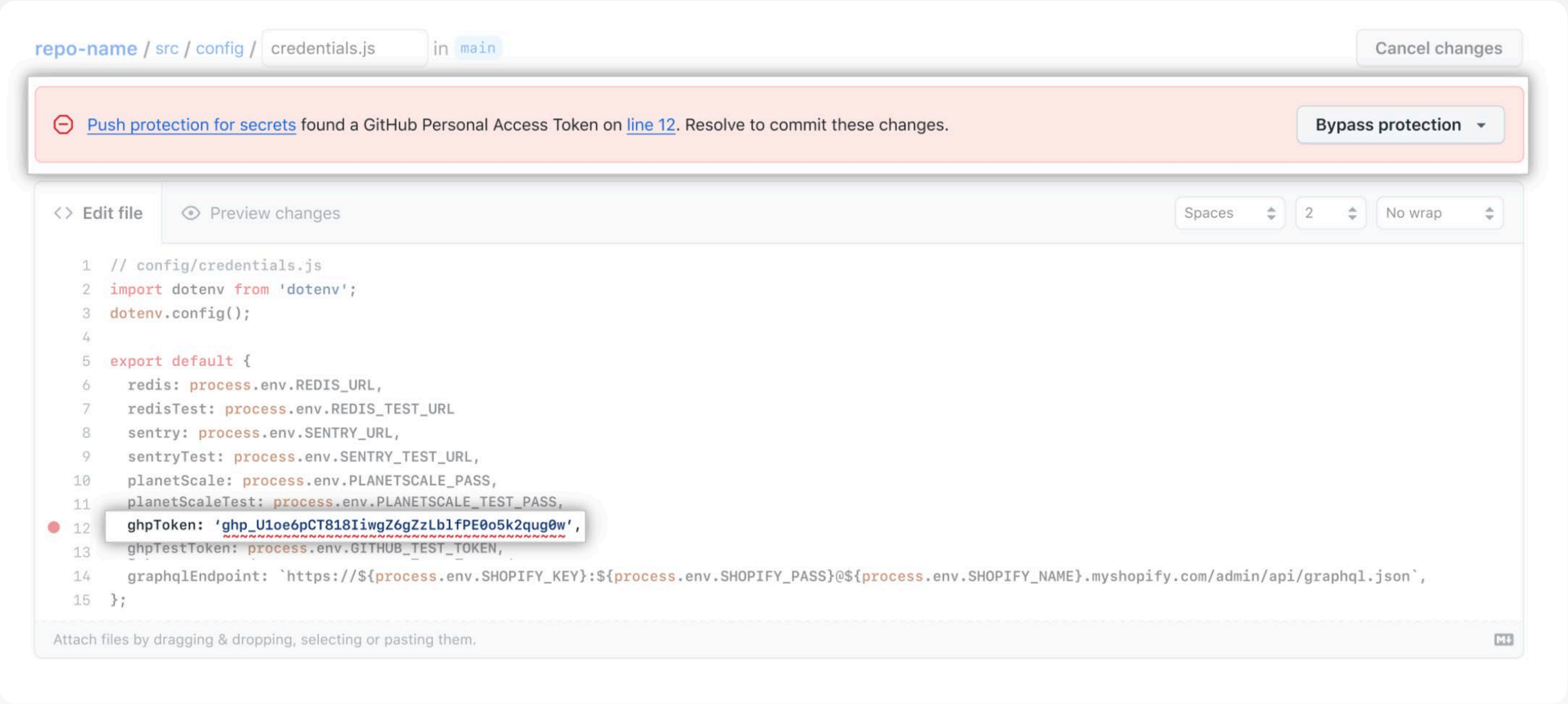
Allow me to push this instance of **GitHub Personal Access Token** to **dsp-testing/15MariamS_Test**

● **It's used in tests**
The secret poses no risk, and if anyone finds it, they cannot do any damage or gain access to sensitive information.

○ **It's a false positive**
The detected string is not a real secret.

○ **I'll fix it later**
The secret is real, **I understand the risk**, and I will need to revoke it. This will open a security alert and notify admins of this repository.

Allowing this secret means other developers can also push this secret to the repository.



repo-name / src / config / credentials.js in main

Push protection for secrets found a GitHub Personal Access Token on line 12. Resolve to commit these changes.

```
1   // config/credentials.js
2   import dotenv from 'dotenv';
3   dotenv.config();
4
5   export default {
6     redis: process.env.REDIS_URL,
7     redisTest: process.env.REDIS_TEST_URL
8     sentry: process.env.SENTRY_URL,
9     sentryTest: process.env.SENTRY_TEST_URL,
10    planetScale: process.env.PLANETSCALE_PASS,
11    planetScaleTest: process.env.PLANETSCALE_TEST_PASS,
12    ghpToken: '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',
13    ghpTestToken: process.env.GITHUB_TEST_TOKEN,
14    graphqlEndpoint: `https://${process.env.SHOPIFY_KEY}:${process.env.SHOPIFY_PASS}@${process.env.SHOPIFY_NAME}.myshopify.com/admin/api/graphql.json`,
15  };
```

Attach files by dragging & dropping, selecting or pasting them.

“Just enable this on everything”

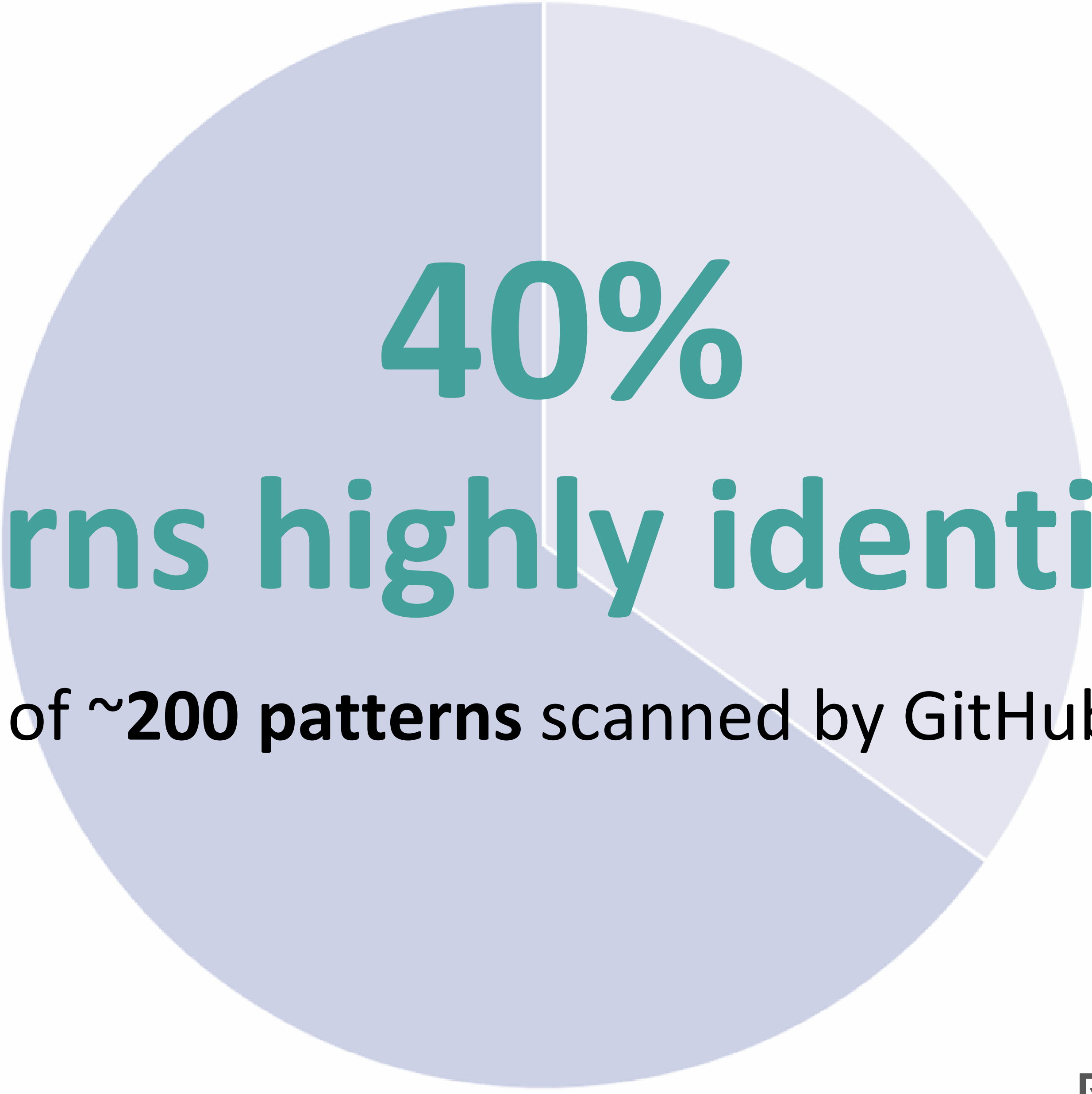
Imagine a token with a 20% false positive rate

↳ Devs constantly blocked

↳ Frustration & loss of trust

↳ More bypasses on protection

↳ Protective step loses purpose

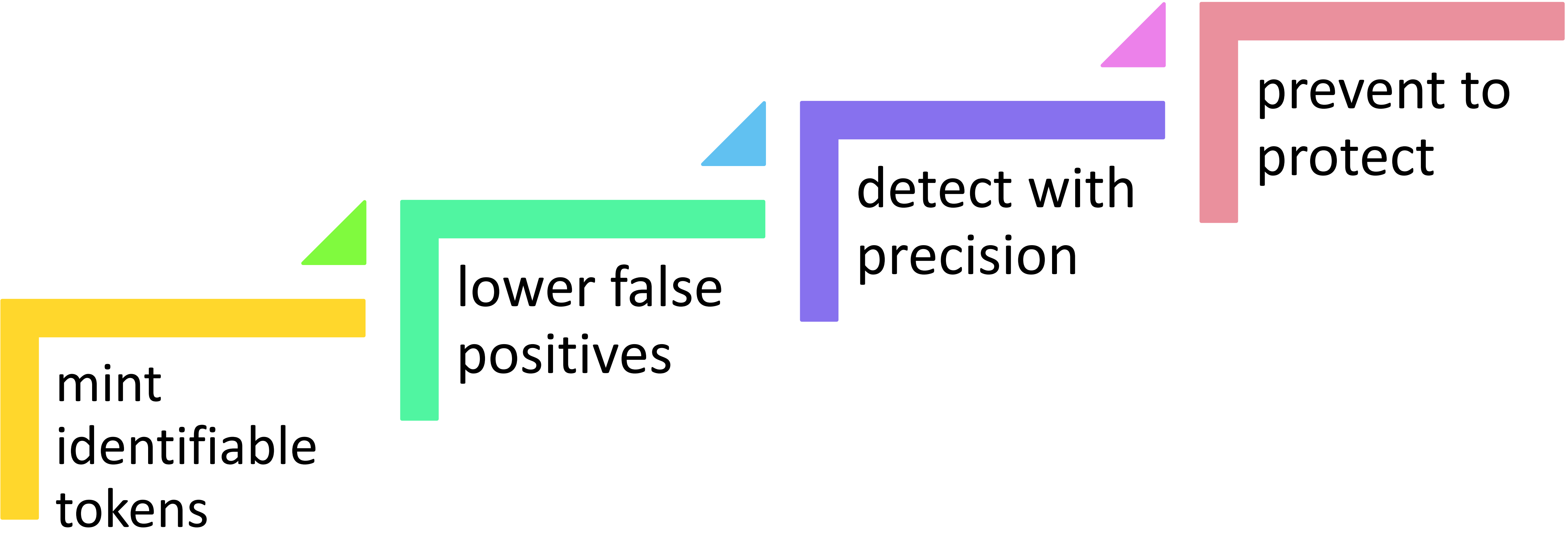


40%

patterns highly identifiable

of ~**200 patterns** scanned by GitHub

Recap: Path to prevention



mint identifiable tokens

lower false positives

detect with precision

prevent to protect

RSA®Conference2022

Takeaways

Apply your learnings and boost security

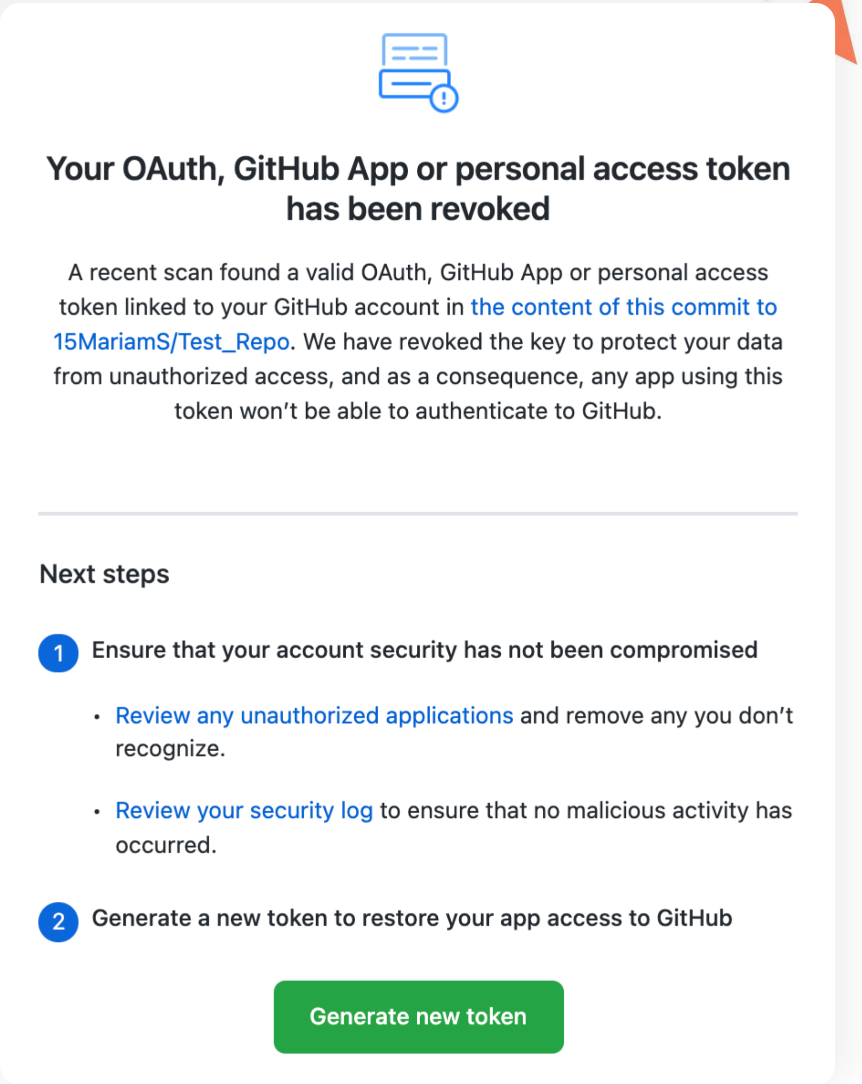
As a developer

Share the security responsibility

Act on alerts

Practice good hygiene

- 2 fac authentication
- Use a vault for secrets
- Scope minimal permissions for secrets



Your OAuth, GitHub App or personal access token has been revoked

A recent scan found a valid OAuth, GitHub App or personal access token linked to your GitHub account in the content of this commit to 15MariamS/Test_Repo. We have revoked the key to protect your data from unauthorized access, and as a consequence, any app using this token won't be able to authenticate to GitHub.

Next steps

1. Ensure that your account security has not been compromised
   - Review any unauthorized applications and remove any you don't recognize.
   - Review your security log to ensure that no malicious activity has occurred.
2. Generate a new token to restore your app access to GitHub

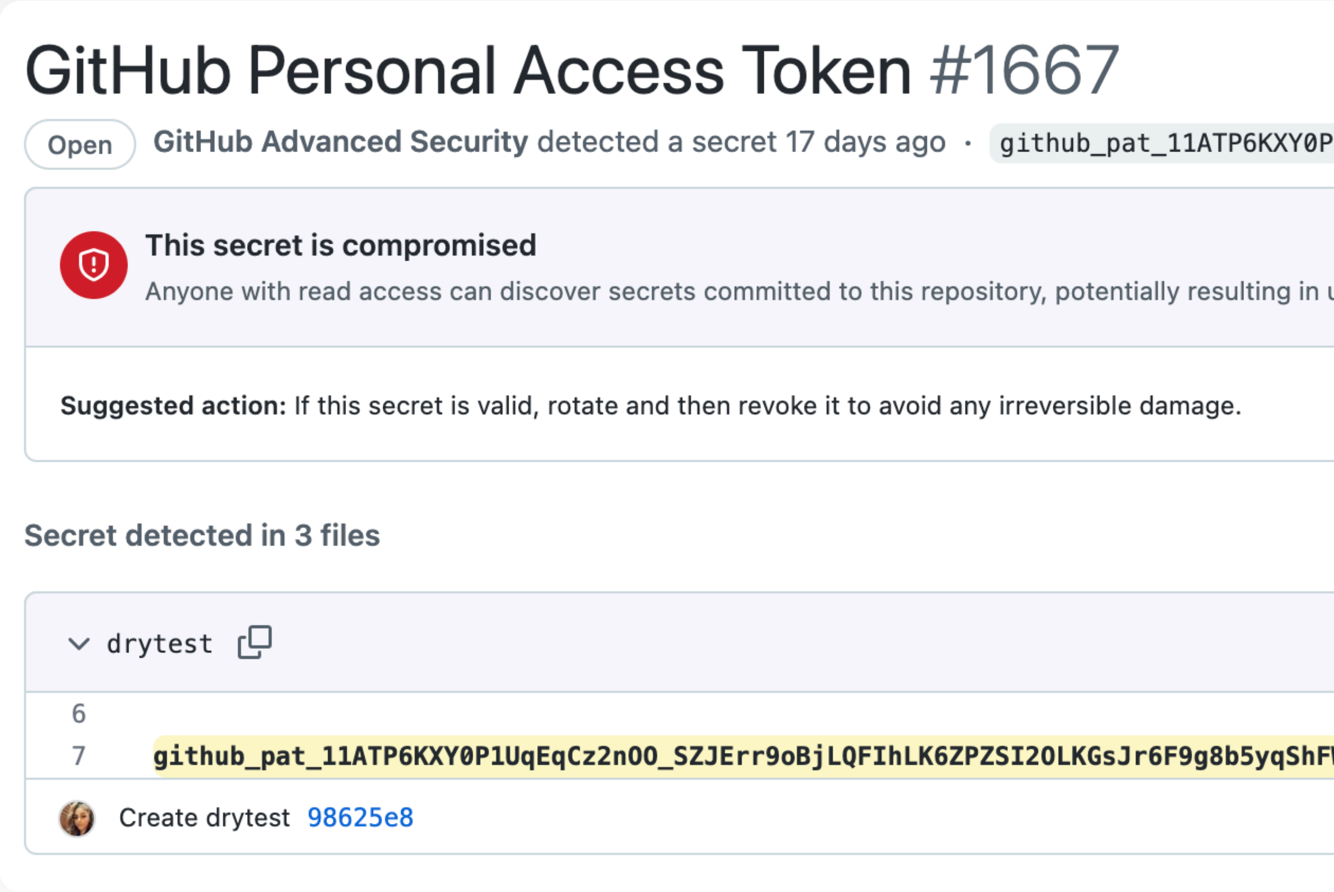
As an organization administrator

Detect

Audit

Remediate

Protect on push



GitHub Personal Access Token #1667

Open **GitHub Advanced Security** detected a secret 17 days ago · `github_pat_11ATP6KXY0P`

This secret is compromised

Anyone with read access can discover secrets committed to this repository, potentially resulting in u

Suggested action: If this secret is valid, rotate and then revoke it to avoid any irreversible damage.

Secret detected in 3 files

drytest

```
6
7   github_pat_11ATP6KXY0P1UqEqCz2nOO_SZJErr9oBjLQFIhLK6ZPZSI2OLKGsJr6F9g8b5yqShF
```

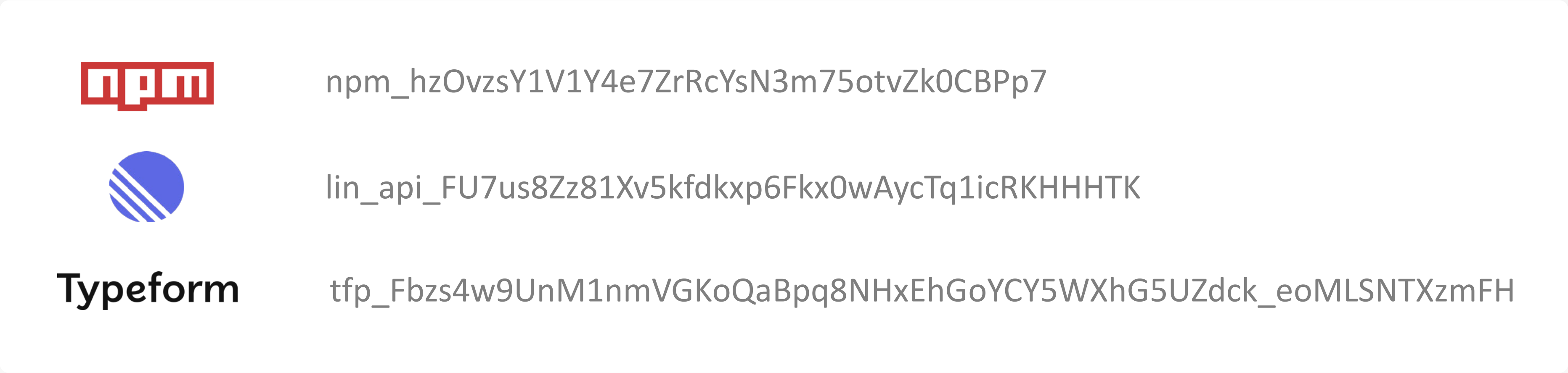
Create drytest 98625e8

As a service provider

Your secrets are already (probably) leaked on GitHub

As a service provider

Make your secrets identifiable

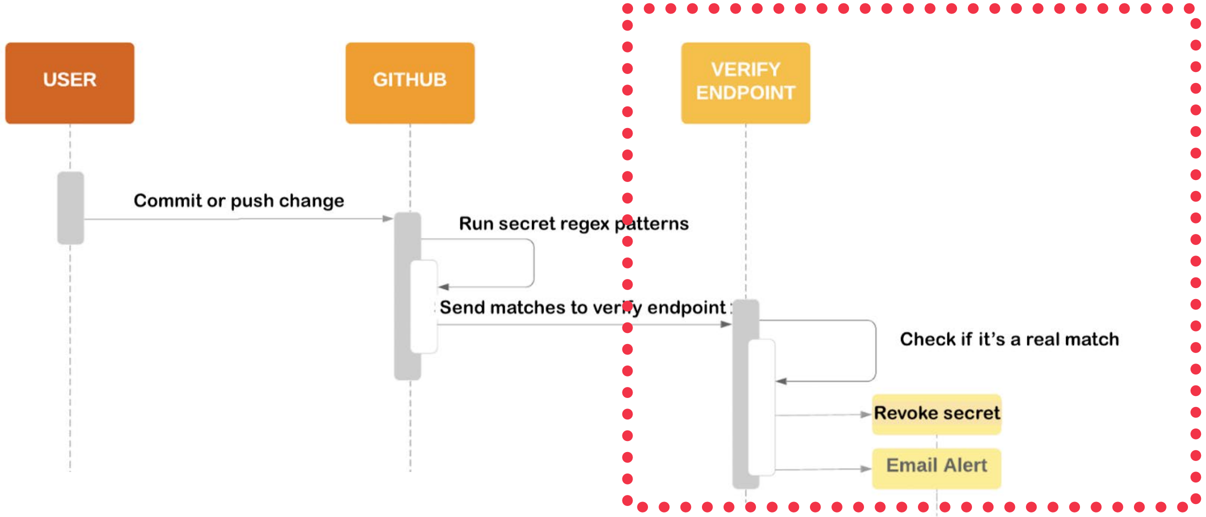


npm	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
	lin_api_FU7us8Zz81Xv5kfdkxp6Fkx0wAycTq1icRKHHHTK
Typeform	tfp_Fbzs4w9UnM1nmVGKoQaBpq8NHxEhGoYCY5WXhG5UZdck_eoMLSNTXzmFH

As a service provider

Make your secrets identifiable

Become a secret scanning partner

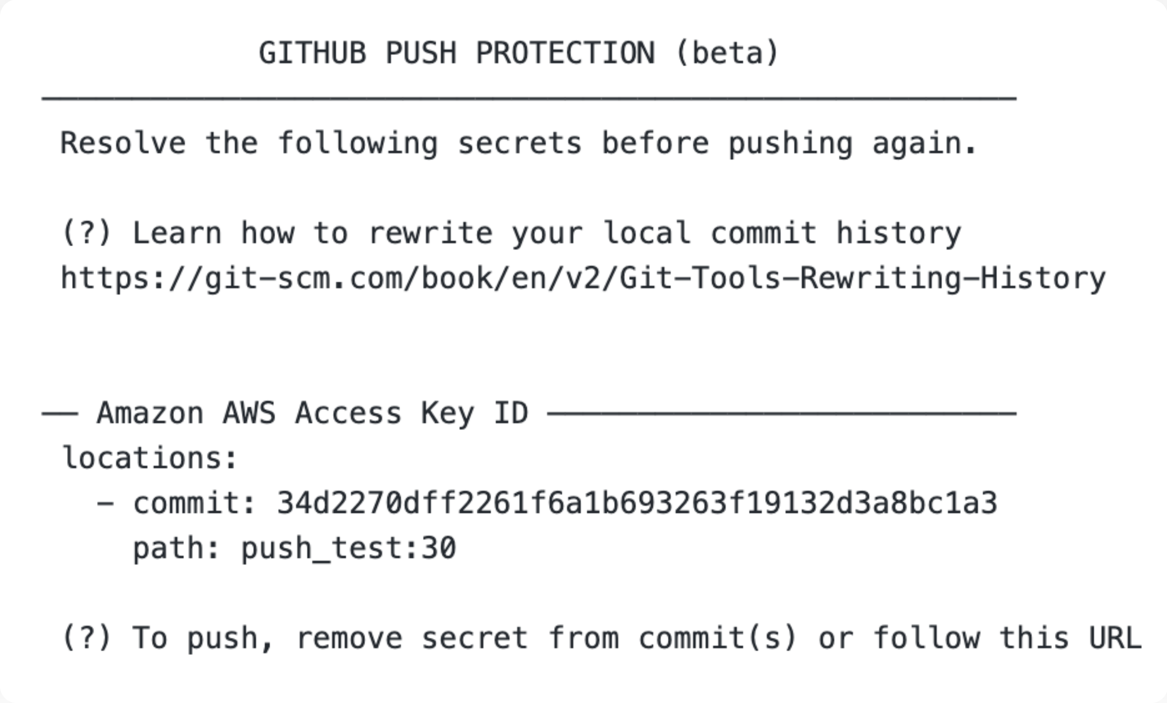

USER
GITHUB
VERIFY ENDPOINT
Commit or push change
Run secret regex patterns
Send matches to verify endpoint
Check if it's a real match
Revoke secret
Email Alert

As a service provider

Make your secrets identifiable

Become a secret scanning partner

Prevent your tokens from accidental leaks



```
              GITHUB PUSH PROTECTION (beta)
 ————————————————————————————————————————————————————————
  Resolve the following secrets before pushing again.

  (?) Learn how to rewrite your local commit history
  https://git-scm.com/book/en/v2/Git-Tools-Rewriting-History


 —— Amazon AWS Access Key ID ——————————————————————————
  locations:
    - commit: 34d2270dff2261f6a1b693263f19132d3a8bc1a3
      path: push_test:30

  (?) To push, remove secret from commit(s) or follow this URL
```

We can solve this problem, together

Questions?

secret-scanning@GitHub.com