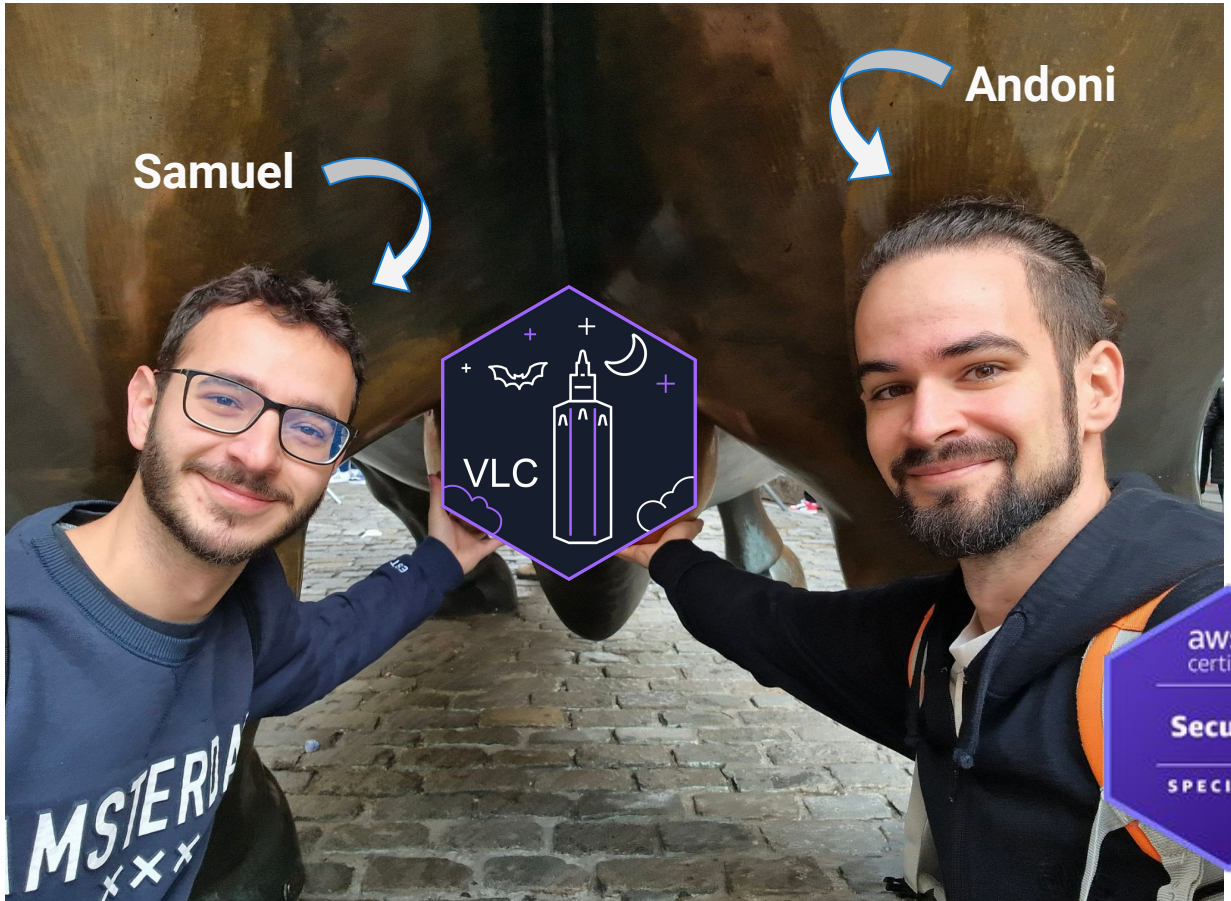
Crea tu propio CSPM con Steampipe, SecurityHub y AWS Organizations

$ ₦ £ € R ₹ ¥ $ ₦ £ € ƒ

$ aws sts get-caller-identity --profile unicrons_cloud



flywire

unicrons.cloud

Agenda

- What's a CSPM
- Our path
- Steampipe (and Powerpipe)
  - Default mods
  - Add custom controls
- Integrate Steampipe with Organizations
- Integrate Powerpipe with SecurityHub
- Recap and Demo!

$ ₦ £ € R ₹ ¥ $ ₦ £ € ƒ

What is a CSPM?

What is CSPM?

- Cloud Security Posture Management
- Continuously monitoring cloud environments for security risks and misconfigurations.

Why do I need CSPM?

- Proactive Risk Management
- Continuous Compliance
- Scalability
- Incident Response
- Unified Security View

Makes your cloud looks like this...

flywire

What is CSPM?

- Cloud Security Posture Management
- Continuously monitoring cloud environments for security risks and misconfigurations.

Why do I need CSPM?

- Proactive Risk Management
- Continuous Compliance
- Scalability
- Incident Response
- Unified Security View

Makes your cloud looks like this...

And not this...

flywire

Our path

Our path

1st attempt: 3rd party tool

- Price per resource $$$
- Custom rules complexity
  - Pseudo-SQL
- No support for custom findings
- Terraform provider missing features

flywire

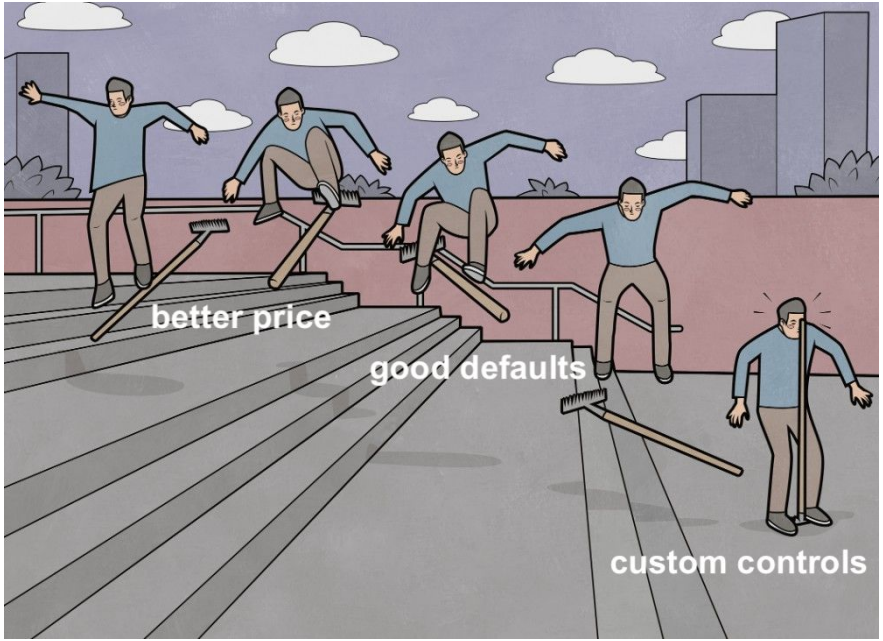
Our path

1st attempt: 3rd party tool

- Price per resource $$$
- Custom rules complexity
  - Pseudo-SQL
- No support for custom findings
- Terraform provider missing features

2nd attempt: AWS Config + SecurityHub

- Better price per resource
- Good default controls
- Custom rules:
  - Lambda
  - AWS CloudFormation Guard



flywire

Our path

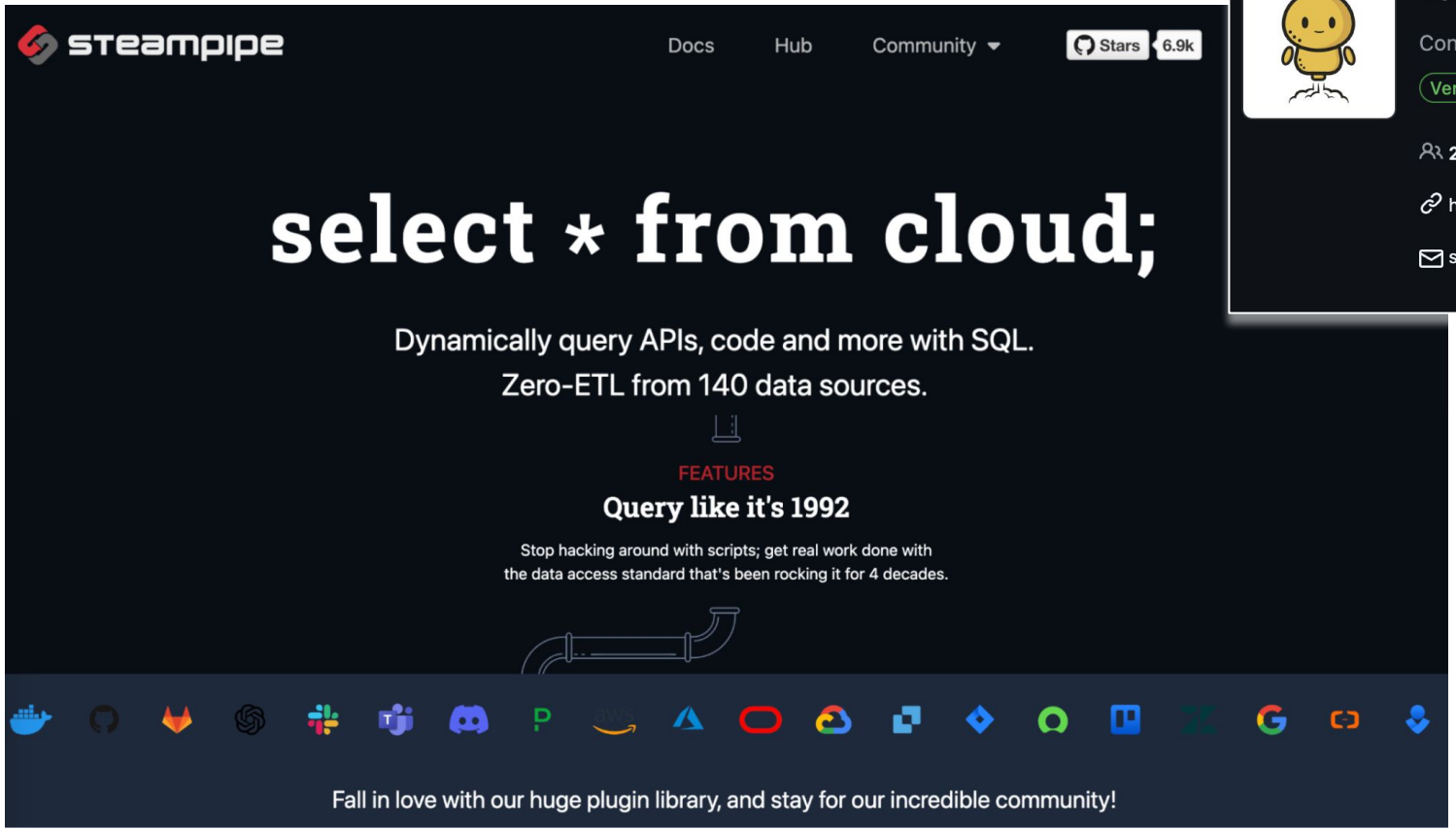
Current approach: Steampipe + SecurityHub

- Cheaper, much cheaper
- Good default controls
- SQL rules, real SQL rules

flywire

Steampipe

Steampipe

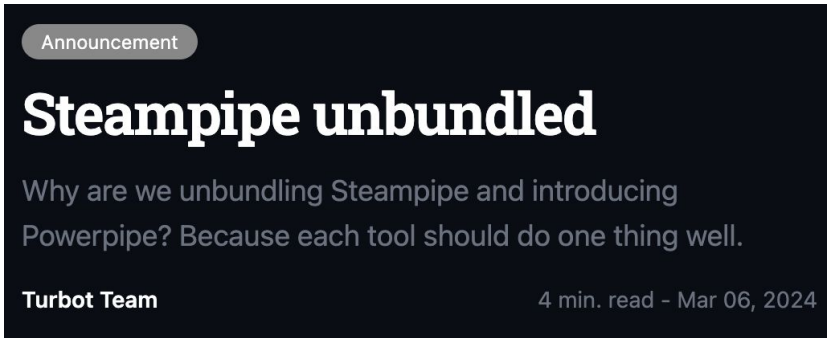


flywire

Steampipe

Component	Does one thing well
Steampipe	select * from cloud;
Powerpipe	Dashboards for DevOps.
Flowpipe	Workflow for DevOps.

https://steampipe.io/blog/steampipe-unbundled



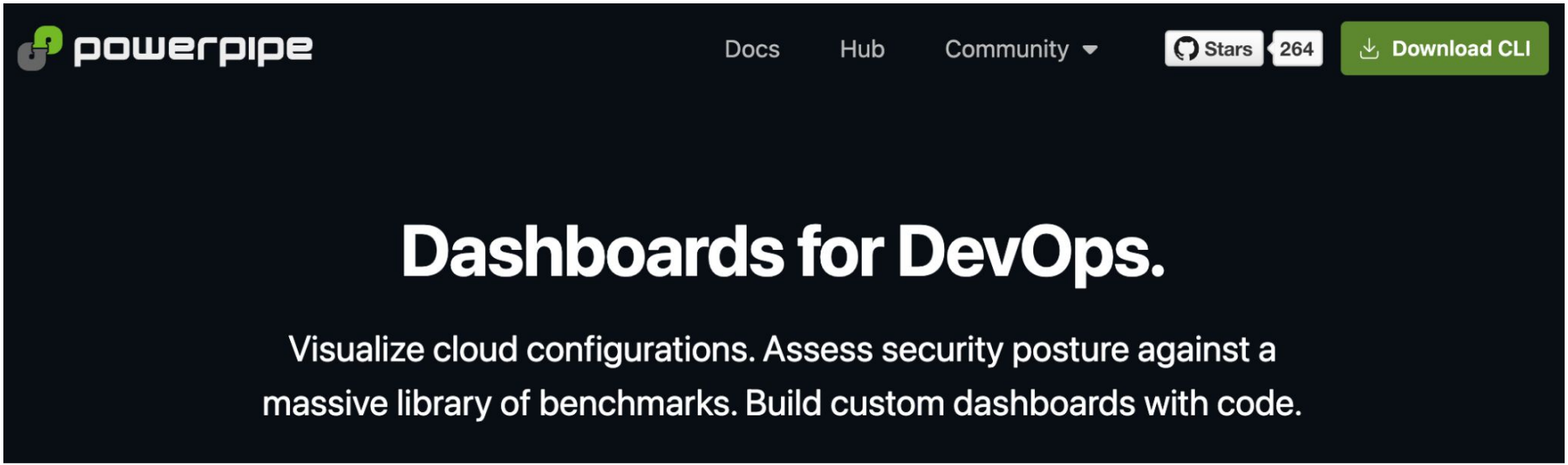
Steampipe

```
> select
  runtime,
  count(*) as functions
from
  aws_lambda_function
group by
  runtime;
+------------+-----------+
|  runtime   | functions |
+------------+-----------+
| nodejs12.x |         1 |
| python3.7  |         1 |
| python3.8  |         2 |
+------------+-----------+
```

```
> select
  aws.name as aws_user_name,
  slack.id as slack_user_id,
  slack.display_name as slack_name
from
  aws_iam_user as aws,
  slack_user as slack
where
  aws.name = slack.email;
+--------------------------+---------------+------------+
|     aws_user_name        | slack_user_id | slack_name |
+--------------------------+---------------+------------+
| dwight@dundermifflin.com | U2EMB8HLP     | dwight     |
| jim@dundermifflin.com    | U02HE4Z7E     | jim        |
+--------------------------+---------------+------------+
```

flywire

Powerpipe



> ***Powerpipe is now the recommended way to run dashboards and benchmarks!*** *Mods still work as normal in Steampipe for now, but they are deprecated and will be removed in a future release:*
>
> - *Steampipe Unbundled →*
> - *Powerpipe for Steampipe users →*

flywire

Powerpipe

```
control "s3_untagged" {
  title = "S3 Untagged"

  sql = <<EOT
    select
      arn as resource,
      case
        when tags is not null then 'ok'
        else 'alarm'
      end as status,
      case
        when tags is not null then name || ' has tags.'
        else name || ' has no tags.'
      end as reason,
      region,
      account_id
    from
      aws_s3_bucket
    EOT
}
```

Required columns:

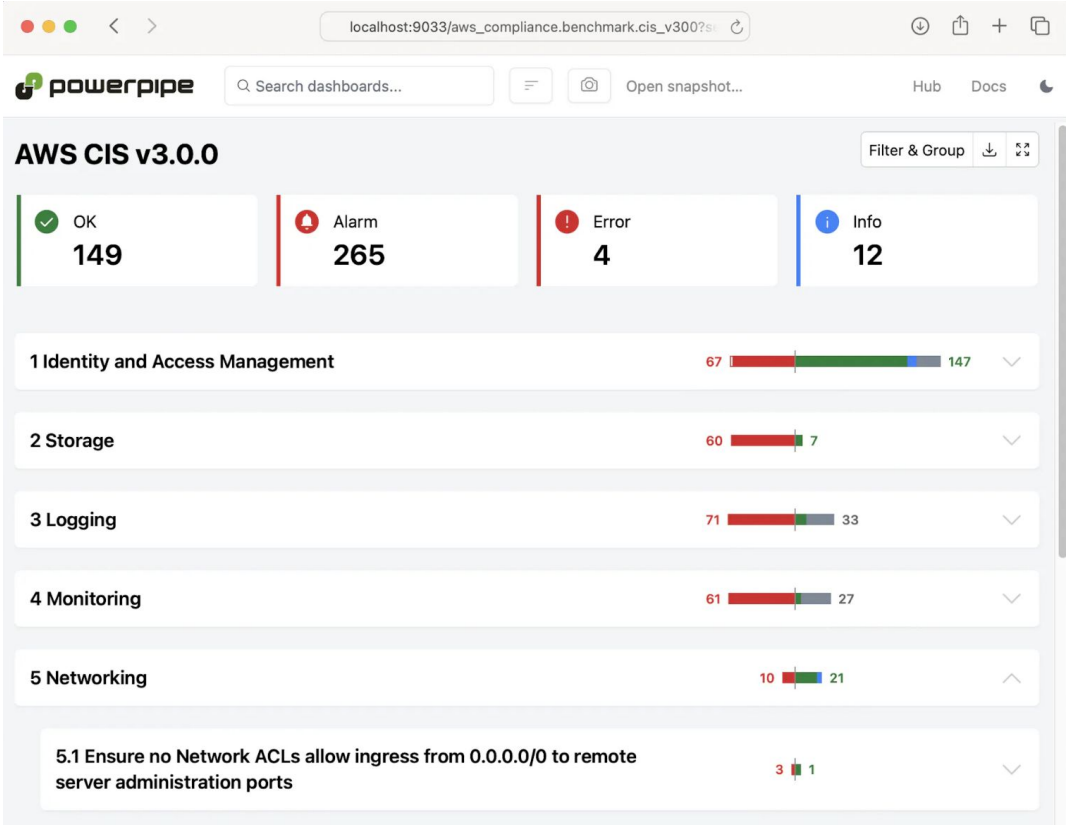
- resource
- status
  - ok
  - alarm
  - skip
  - info
  - error
- reason

Powerpipe

```
benchmark "cisv130" {
  title         = "CIS v1.3.0"
  description   = "The CIS Amazon Web Services Found
  documentation = file("./docs/cis-overview.md")

  children = [
    benchmark.cis_v130_1,
    benchmark.cis_v130_2,
    benchmark.cis_v130_3,
    benchmark.cis_v130_4,
    benchmark.cis_v130_5
  ]

  tags = {
    cloud_provider = "aws"
    framework      = "cis"
    cis_version    = "v1.3.0"
  }
}
```

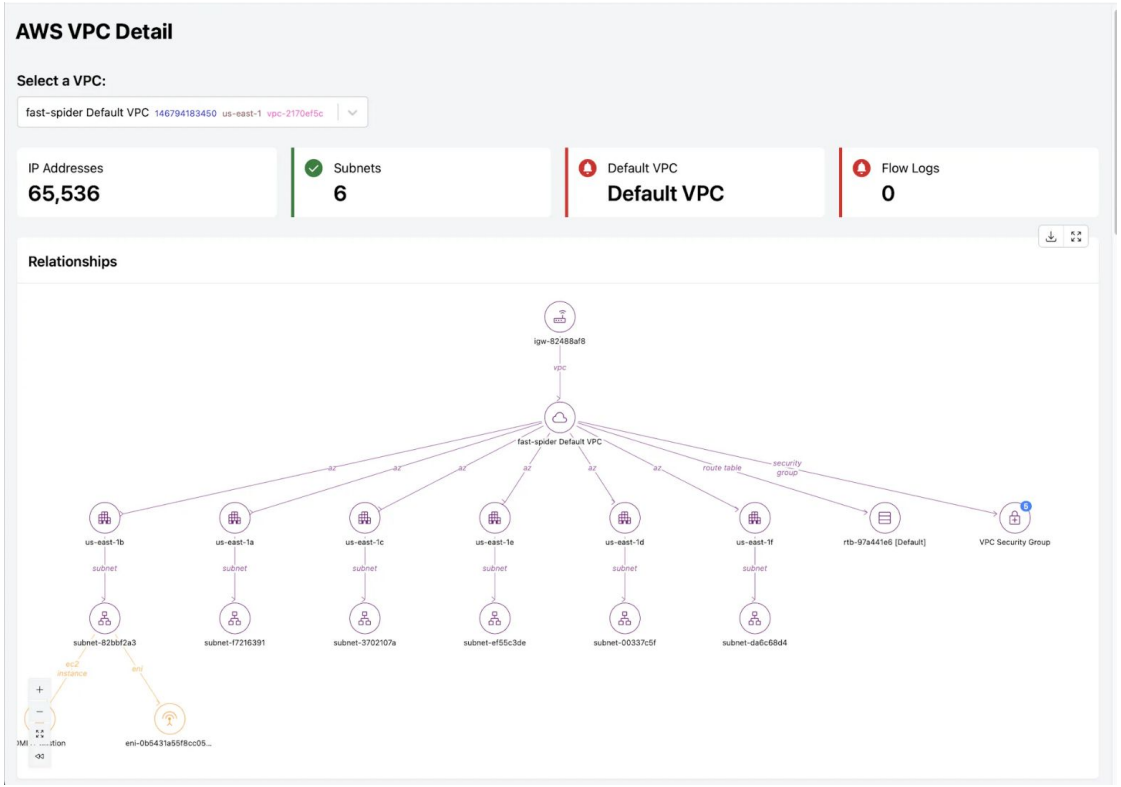
```
benchmark "cisv130_1" {
  title         = "1 Identity and Access Management"
  documentation = file("./docs/cisv130_1.md")

  children = [
    control.cis_v130_1_1,
    control.cis_v130_1_2,
    control.cis_v130_1_3,
    control.cis_v130_1_4,
    control.cis_v130_1_5,
    control.cis_v130_1_6
  ]

  tags = {
    cloud_provider = "aws"
    framework      = "cis"
    cis_version    = "v1.3.0"
  }
}
```

Powerpipe



flywire

Powerpipe



https://github.com/turbot/steampipe-mod-aws-insights/blob/main/dashboards/vpc/vpc_detail.sp

flywire

Powerpipe

```
⊗ → my-mods powerpipe benchmark run aws_compliance.benchmark.cis_v300

CIS v3.0.0 ..................................................... 283 / 538 [==========]
|
+ 1 Identity and Access Management ..................................  81 / 248 [=====     ]
| |
| + 1.1 Maintain current contact details ..............................   0 /   2 [=         ]
| | |
| | INFO : Manual verification required. ..................................... 146794183450
| | INFO : Manual verification required. ..................................... 480721418648
| |
| + 1.2 Ensure security contact information is registered ..............   1 /   2 [==        ]
| | |
| | ALARM: 146794183450 security contact not registered. ..................... 146794183450
| | OK   : 480721418648 has security contact Example registered. ............. 480721418648
| |
| + 1.3 Ensure security questions are registered in the AWS account .....   0 /   2 [=         ]
| | |
| | INFO : Manual verification required. ..................................... 146794183450
| | INFO : Manual verification required. ..................................... 480721418648
| |
| + 1.4 Ensure no 'root' user account access key exists ..................   0 /   2 [=         ]
| | |
| | OK   : No root user access keys exist. ................................... 146794183450
| | OK   : No root user access keys exist. ................................... 480721418648
| |
| + 1.5 Ensure MFA is enabled for the 'root' user account ...............   2 /   2 [=         ]
| | |
```

flywire

Default mods

Default mods

Featured Use Cases

Security & Compliance

Identify and monitor security metrics, alerts and compliance status. Track progress on resolving vulnerabilities over-time.

Cost Management

Track cloud utilization and costs. Reduce operational costs by analyzing trends and identifying underutilized resources.

Shift-left Scanning

Run security benchmarks across your Terraform stacks (or include in your pipelines) to stop cloud misconfiguration before it starts.

Asset Inventory & Insights

Use dashboards to explore the relationships, configuration and status of servers, containers, cloud services and networking.

flywire

Default mods

AWS Compliance

Steampipe

`turbot/aws_compliance` v0.98

Run individual configuration, compliance and security controls or full compliance benchmarks for CIS, FFIEC, PCI, NIST, HIPAA, RBI CSF, GDPR, SOC 2, Audit Manager Control Tower, FedRAMP, GxP and AWS Foundational Security Best Practices controls across all your AWS accounts using Powerpipe and Steampipe.

AWS Well-Architected

Steampipe

`turbot/aws_well_architected` v0.11

Run controls across all of your AWS accounts to check if they are following AWS Well-Architected best practices using Powerpipe and Steampipe.

Formula 1

SQLite

`turbot/formula1` v1.0.0

Zoom into the high-speed world of Formula 1 with the Formula 1 Dashboard, offering a detailed overview of races, drivers, constructors, and seasons, alongside in-depth performance analysis, driver statistics, race highlights, and insights into the global distribution of drivers and circuits, using SQLite with Powerpipe.

Default mods

```
powerpipe mod init
```

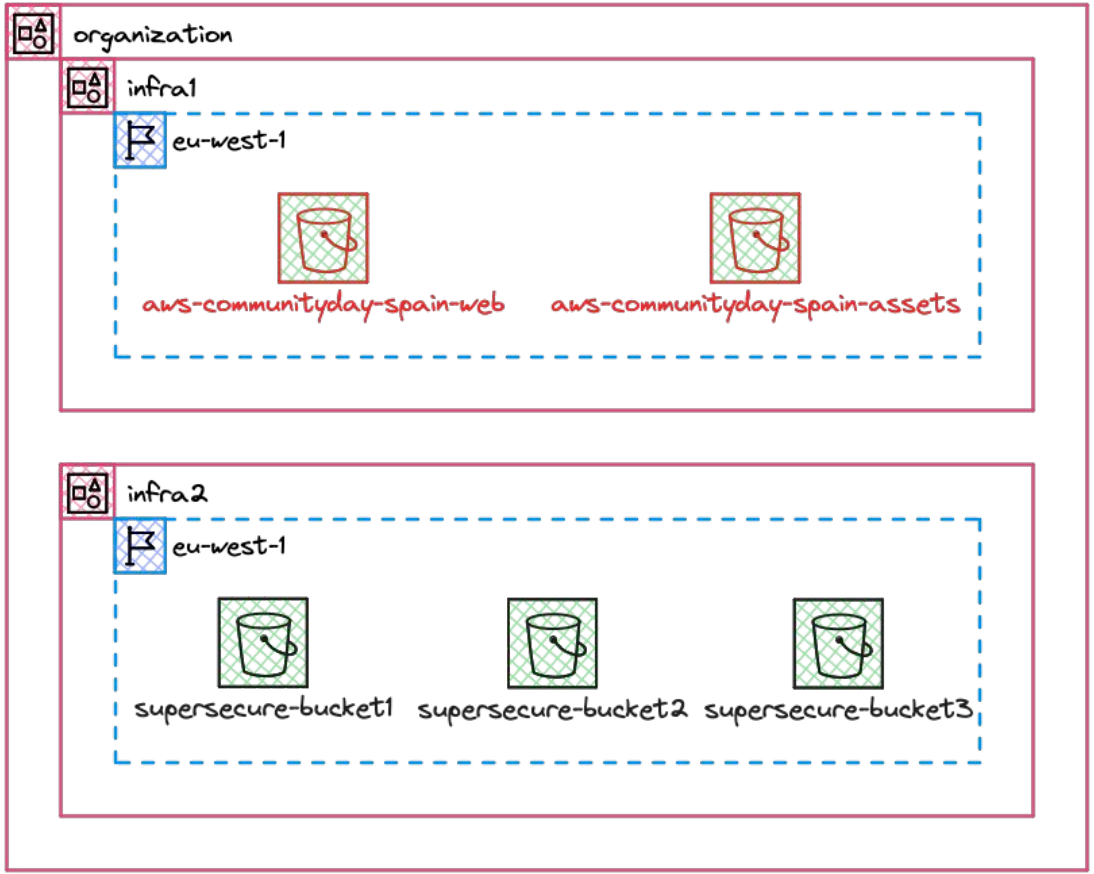
```
powerpipe mod install github.com/turbot/steampipe-mod-aws-insights
```

```
powerpipe server
```

flywire

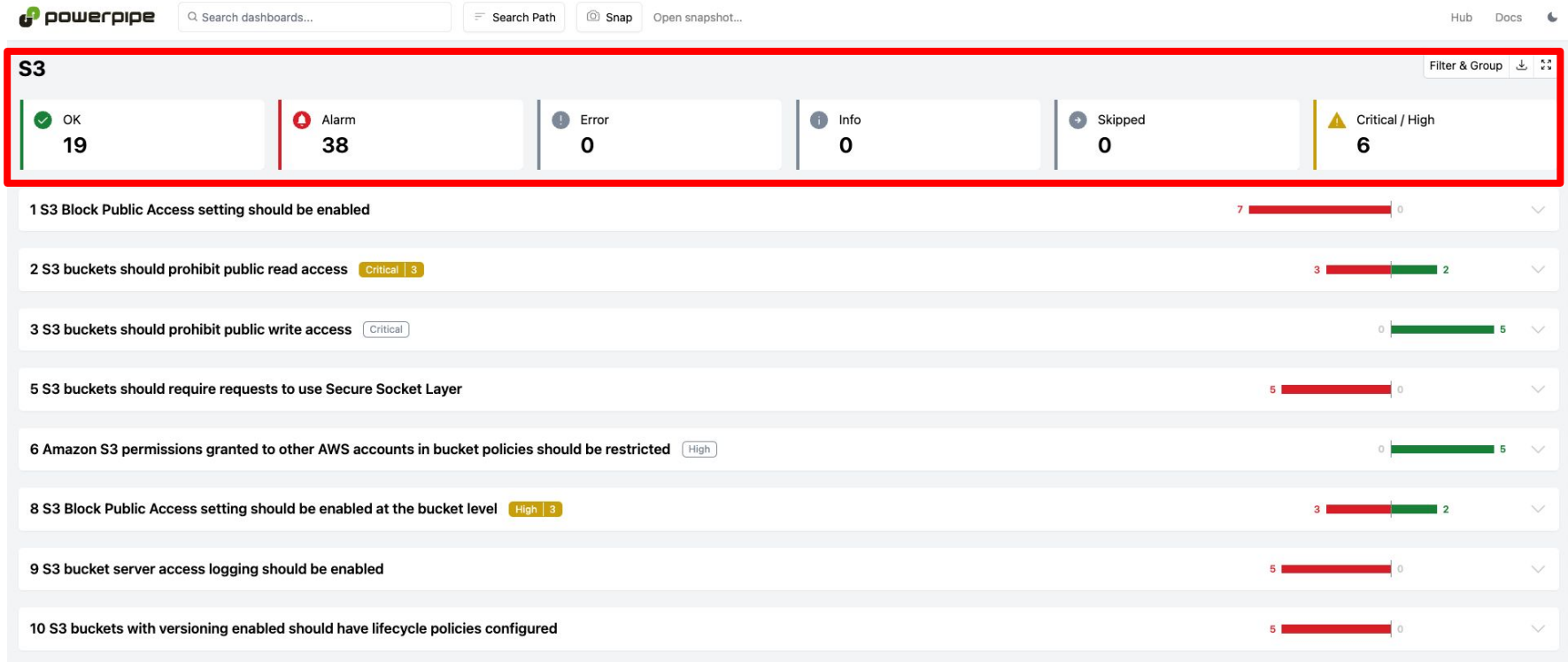
Add custom controls

Add custom controls



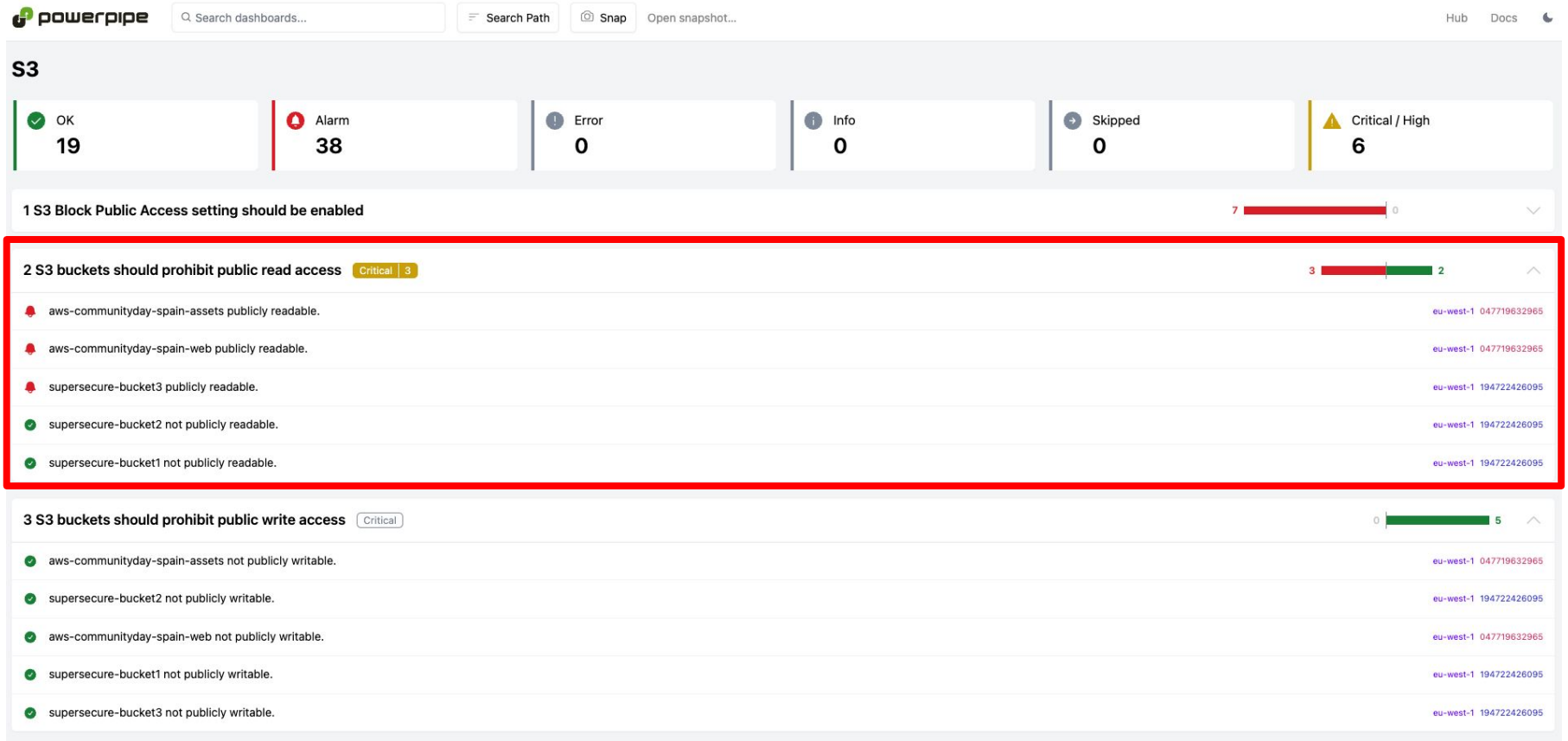
flywire

Add custom controls



flywire

Add custom controls



Add custom controls

```
control "s3_bucket_restrict_public_read_access" {
  title       = "S3 buckets should prohibit public read access"
  description = "Not allowed S3 buckets should prohibit public read access."
  query       = query.s3_bucket_restrict_public_read_access

  tags = {
    plugin = "aws"
  }
}

query "s3_bucket_restrict_public_read_access" {
  sql = <<-EOQ
    select
      arn as resource,
      case
        when bucket_policy_is_public and restrict_public_buckets then 'skip'
        when bucket_policy_is_public then 'alarm'
        else 'ok'
      end as status,
      case
        when bucket_policy_is_public then title || ' has a public bucket policy.'
        else title || ' does not have a public bucket policy.'
      end as reason,
      region,
      account_id
    from
      aws_s3_bucket;
  EOQ
}

```

flywire

Add custom controls

```
control "s3_bucket_restrict_public_read_access" {
  title       = "S3 buckets should prohibit public read access"
  description = "Not allowed S3 buckets should prohibit public read access."
  query       = query.s3_bucket_restrict_public_read_access

  tags = {
    plugin = "aws"
  }
}

query "s3_bucket_restrict_public_read_access" {
  sql = <<-EOQ
    select
      arn as resource,
      case
        when bucket_policy_is_public and restrict_public_buckets then 'skip'
        when bucket_policy_is public and tags ->> 'public' = 'true' then 'info'
        when bucket_policy_is_public then 'alarm'
        else 'ok'
      end as status,
      case
        when bucket_policy_is_public then title || ' has a public bucket policy.'
        else title || ' does not have a public bucket policy.'
      end as reason,
      region,
      account_id
    from
      aws_s3_bucket;
  EOQ
}
```

flywire

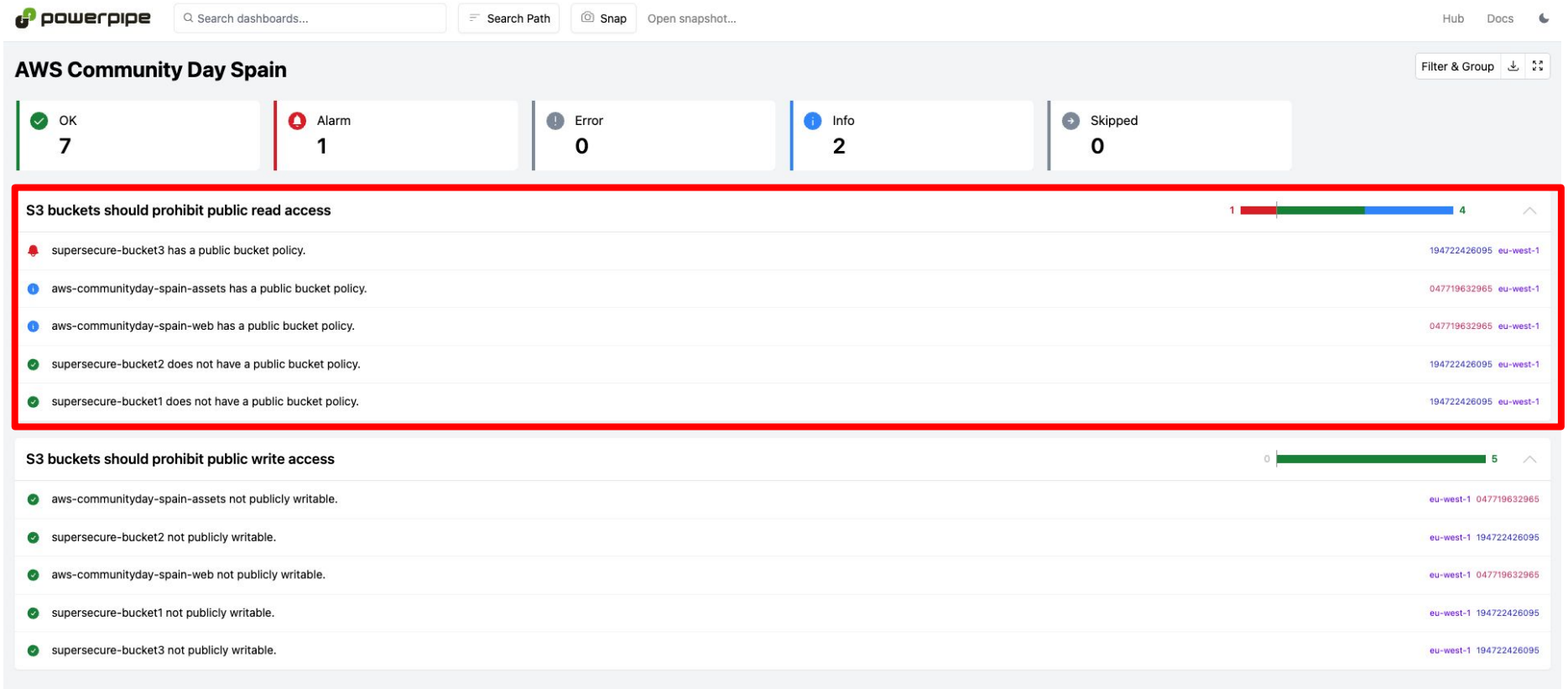
Add custom controls

benchmark.pp

```
benchmark "aws_communityday" {
  title         = "AWS Community Day Spain"
  description   = "Demo benchmark."

  children = [
    control.s3_bucket_restrict_public_read_access,
    aws_compliance.control.s3_bucket_restrict_public_write_access
  ]

  tags = {
    cloud_provider = "aws"
  }
}

```

flywire

Add custom controls



Add custom controls

```
❯ powerpipe control run local.control.s3_bucket_restrict_public_read_access

+ S3 buckets should prohibit public read access ..... 1 / 5 [════════]
  |
  ALARM: supersecure-bucket3 has a public bucket policy. ..... eu-west-1 194722426095
  INFO : aws-communityday-spain-web has a public bucket policy. ..... eu-west-1 047719632965
  INFO : aws-communityday-spain-assets has a public bucket policy. ..... eu-west-1 047719632965
  OK   : supersecure-bucket2 does not have a public bucket policy. ..... eu-west-1 194722426095
  OK   : supersecure-bucket1 does not have a public bucket policy. ..... eu-west-1 194722426095

Summary

OK ..... 2 [═══       ]
SKIP ..... 0 [          ]
INFO ..... 2 [═══       ]
ALARM ..... 1 [═          ]
ERROR ..... 0 [          ]

TOTAL ..... 1 / 5 [═══════]
```

Integrate Steampipe with AWS Organizations

flywire

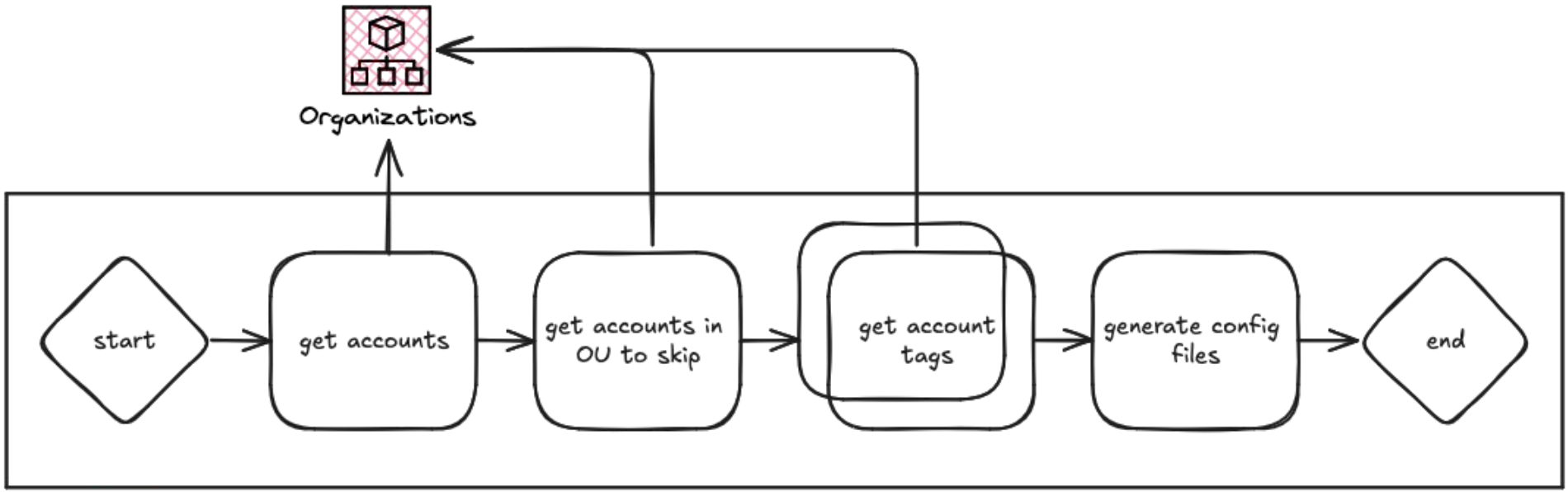
Integrate Steampipe with AWS Organizations

```
connection "aws_infra1" {
  plugin         = "aws"
  profile        = "infra1"
  regions        = ["*",]
  default_region = "eu-west-1"
  import_schema  = "enabled"
}

connection "aws_infra2" {
  plugin         = "aws"
  profile        = "infra2"
  regions        = ["*",]
  default_region = "eu-west-1"
  import_schema  = "enabled"
}

connection "aws_infra3" {
  plugin         = "aws"
  profile        = "infra3"
  regions        = ["*",]
  default_region = "eu-west-1"
  import_schema  = "enabled"
}

connection "aws_infra4" {
  plugin         = "aws"
  profile        = "infra4"
  regions        = ["*",]
  default_region = "eu-west-1"
  import_schema  = "enabled"
}

connection "aws_infra5" {
  plugin         = "aws"
  profile        = "infra5"
  regions        = ["*",]
```

```
[infra1]
role_arn = arn:aws:iam::047719632965:role/security/cspm-scanner
credential_source = EcsContainer
role_session_name = steampipe

[infra2]
role_arn = arn:aws:iam::194722426095:role/security/cspm-scanner
credential_source = EcsContainer
role_session_name = steampipe

[infra3]
role_arn = arn:aws:iam::522814726532:role/security/cspm-scanner
credential_source = EcsContainer
role_session_name = steampipe

[infra4]
role_arn = arn:aws:iam::340752821193:role/security/cspm-scanner
credential_source = EcsContainer
role_session_name = steampipe

[infra5]
role_arn = arn:aws:iam::440744219876:role/security/cspm-scanner
credential_source = EcsContainer
role_session_name = steampipe

[infra6]
role_arn = arn:aws:iam::890742587187:role/security/cspm-scanner
credential_source = EcsContainer
role_session_name = steampipe

[infra7]
role_arn = arn:aws:iam::491085404728:role/security/cspm-scanner
credential_source = EcsContainer
role_session_name = steampipe

[infra8]
role_arn = arn:aws:iam::892223657599:role/security/cspm-scanner
```

flywire

Integrate Steampipe with AWS Organizations



steampipe-config-generator

flywire

Integrate Steampipe with AWS Organizations

```
❯ ./steampipe_config_generator -role security/cspm-scanner -template custom_template.tmpl
```

```
❯ ./steampipe_config_generator
Usage of ./steampipe_config_generator:
  -assume string
        AWS Role to assume for getting Organization accounts
  -connections string
        Steampipe AWS connections file path
  -credential string
        AWS Credential source. Valid values are: Ec2InstanceMetadata, Environment, EcsContainer (default "Environment")
  -path string
        AWS Credentials file path
  -region string
        AWS Connection default region
  -regions string
        AWS Connection target regions (default "all")
  -role string
        AWS Role to use in AWS config credentials
  -schema string
        AWS Connection import schema. Valid values are: enabled, disabled (default "enabled")
  -skipOUs string
        AWS OU IDs to skip from account connections
  -template string
        Custom connections template path
```

flywire

Integrate Steampipe with AWS Organizations

steampipe-config-generator Public

Features

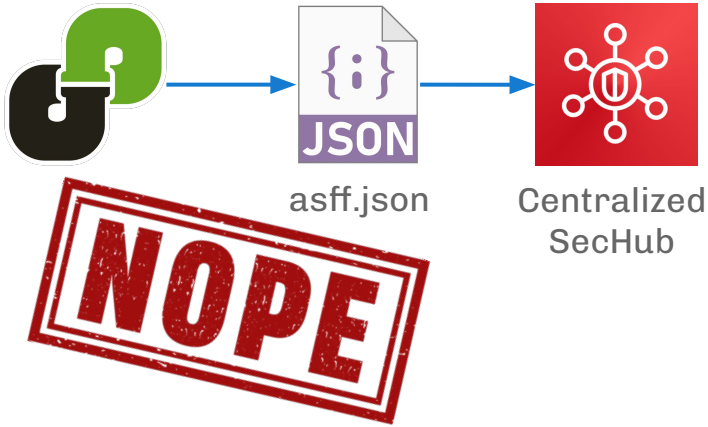
- Automate the Steampipe AWS config files.
- Skip accounts based on their OU.
- Create aggregators based on account tags.
- AssumeRole to avoid deploying it in a privileged account.
- Compatible with IMDSv2 inside EC2 and ECS.
- Open Source!

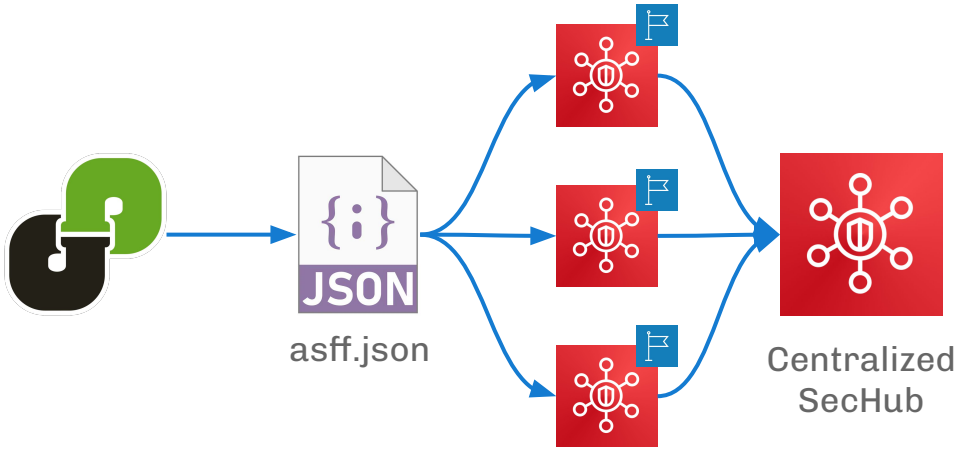
flywire

Integrate Powerpipe with AWS SecurityHub

Integrate Powerpipe with AWS SecurityHub

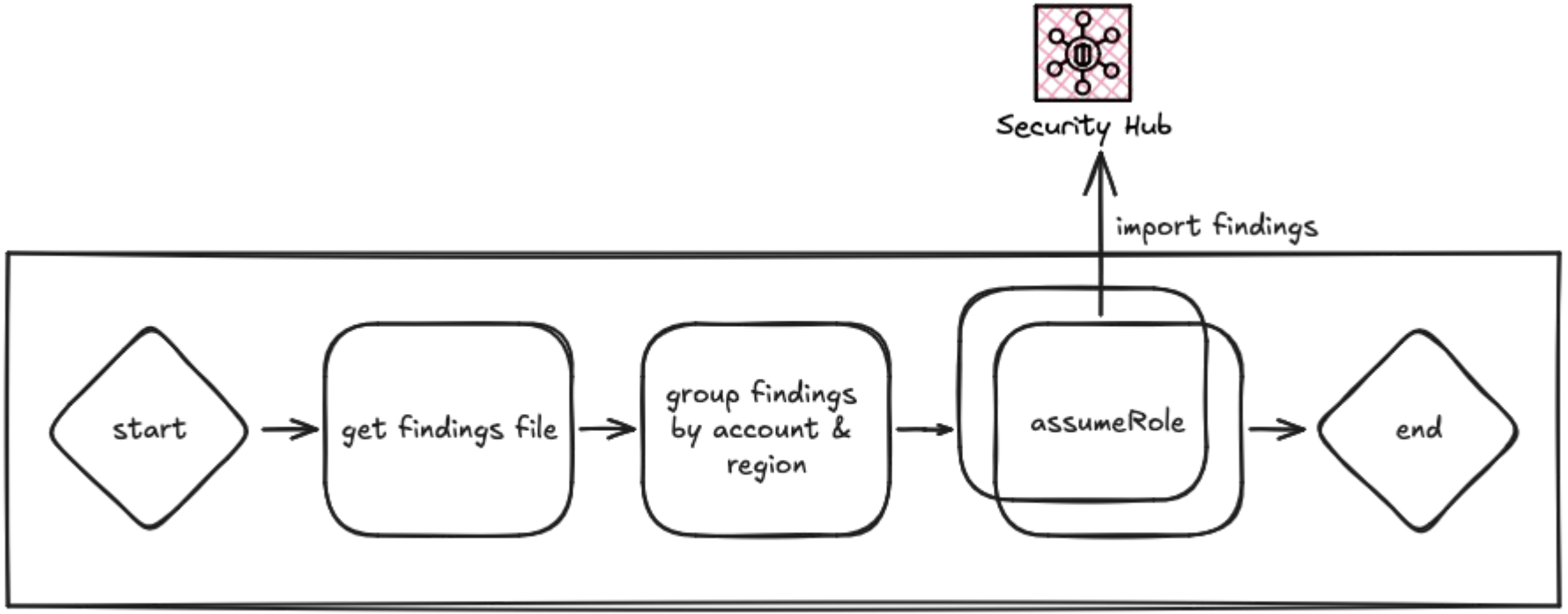
```
❯ powerpipe benchmark run aws_communityday --export asff.json
```





flywire

Integrate Powerpipe with AWS SecurityHub



powerpipe-securityhub-importer

flywire

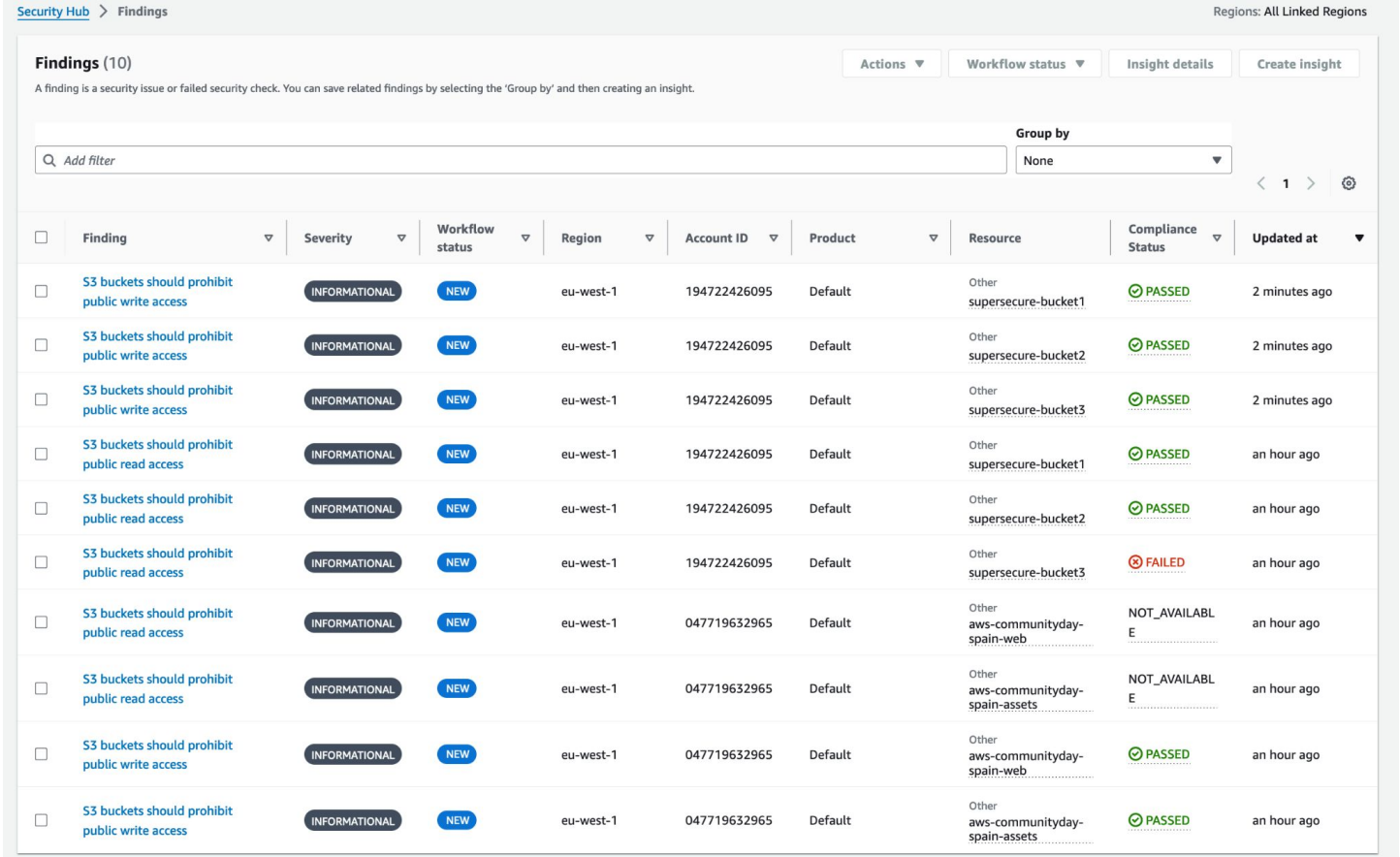
Integrate Powerpipe with AWS SecurityHub

```
❯ ./powerpipe-securityhub-importer -role security/cspm-scanner -findings findings.asff.json
```

```
❯ ./powerpipe-securityhub-importer
Usage of ./powerpipe-securityhub-importer:
  -failed
        Skip Importing PASSED & NOT_AVAILABLE findings
  -findings string
        SecurityHub asff json file path
  -log string
        Log format: default, json (default "default")
  -role string
        AWS assume role name
  -session string
        AWS assume role session name (default "powerpipe-securityhub-importer")
```

flywire

Integrate Powerpipe with AWS SecurityHub



Security Hub > Findings

Regions: All Linked Regions

Findings (10)

Actions | Workflow status | Insight details | Create insight

A finding is a security issue or failed security check. You can save related findings by selecting the 'Group by' and then creating an insight.

Add filter

Group by: None

1

Finding	Severity	Workflow status	Region	Account ID	Product	Resource	Compliance Status	Updated at
S3 buckets should prohibit public write access	INFORMATIONAL	NEW	eu-west-1	194722426095	Default	Other supersecure-bucket1	PASSED	2 minutes ago
S3 buckets should prohibit public write access	INFORMATIONAL	NEW	eu-west-1	194722426095	Default	Other supersecure-bucket2	PASSED	2 minutes ago
S3 buckets should prohibit public write access	INFORMATIONAL	NEW	eu-west-1	194722426095	Default	Other supersecure-bucket3	PASSED	2 minutes ago
S3 buckets should prohibit public read access	INFORMATIONAL	NEW	eu-west-1	194722426095	Default	Other supersecure-bucket1	PASSED	an hour ago
S3 buckets should prohibit public read access	INFORMATIONAL	NEW	eu-west-1	194722426095	Default	Other supersecure-bucket2	PASSED	an hour ago
S3 buckets should prohibit public read access	INFORMATIONAL	NEW	eu-west-1	194722426095	Default	Other supersecure-bucket3	FAILED	an hour ago
S3 buckets should prohibit public read access	INFORMATIONAL	NEW	eu-west-1	047719632965	Default	Other aws-communityday-spain-web	NOT_AVAILABLE	an hour ago
S3 buckets should prohibit public read access	INFORMATIONAL	NEW	eu-west-1	047719632965	Default	Other aws-communityday-spain-assets	NOT_AVAILABLE	an hour ago
S3 buckets should prohibit public write access	INFORMATIONAL	NEW	eu-west-1	047719632965	Default	Other aws-communityday-spain-web	PASSED	an hour ago
S3 buckets should prohibit public write access	INFORMATIONAL	NEW	eu-west-1	047719632965	Default	Other aws-communityday-spain-assets	PASSED	an hour ago

flywire

Integrate Powerpipe with AWS SecurityHub

powerpipe-securityhub-importer Public

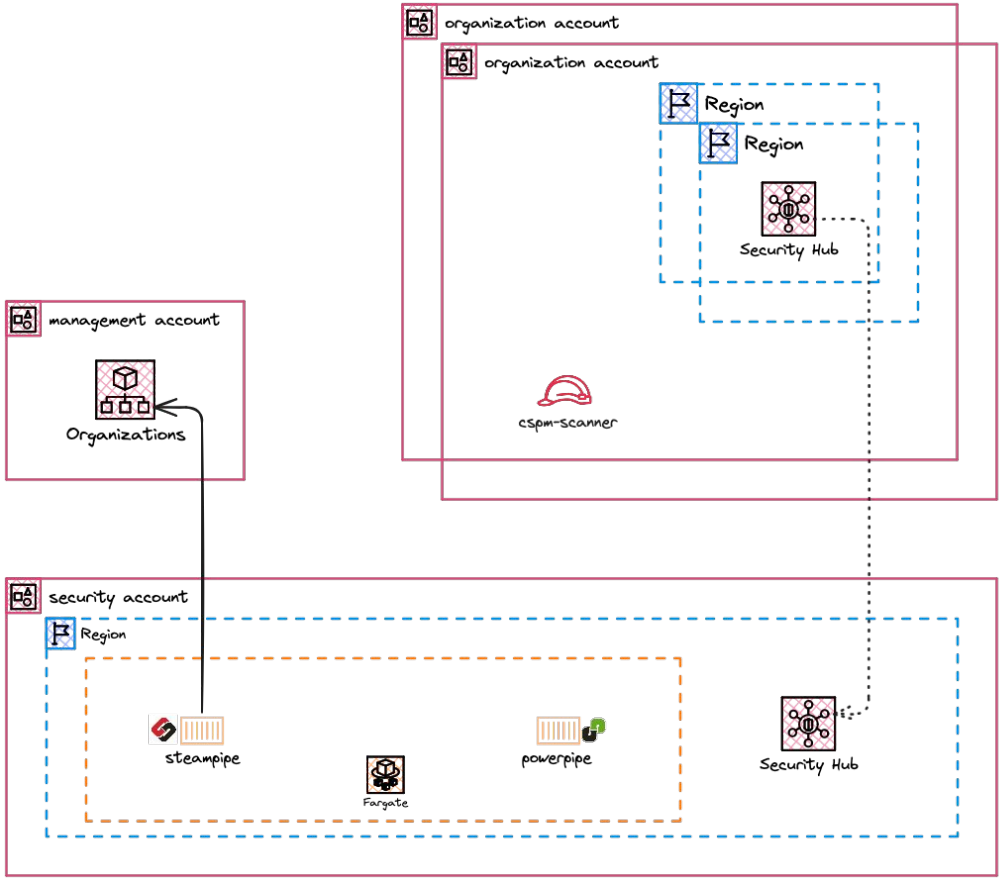
Features

- Import Powerpipe findings in SecurityHub at scale!
- Skip PASSED and NOT_AVAILABLE findings if desired.
- Open Source!

flywire

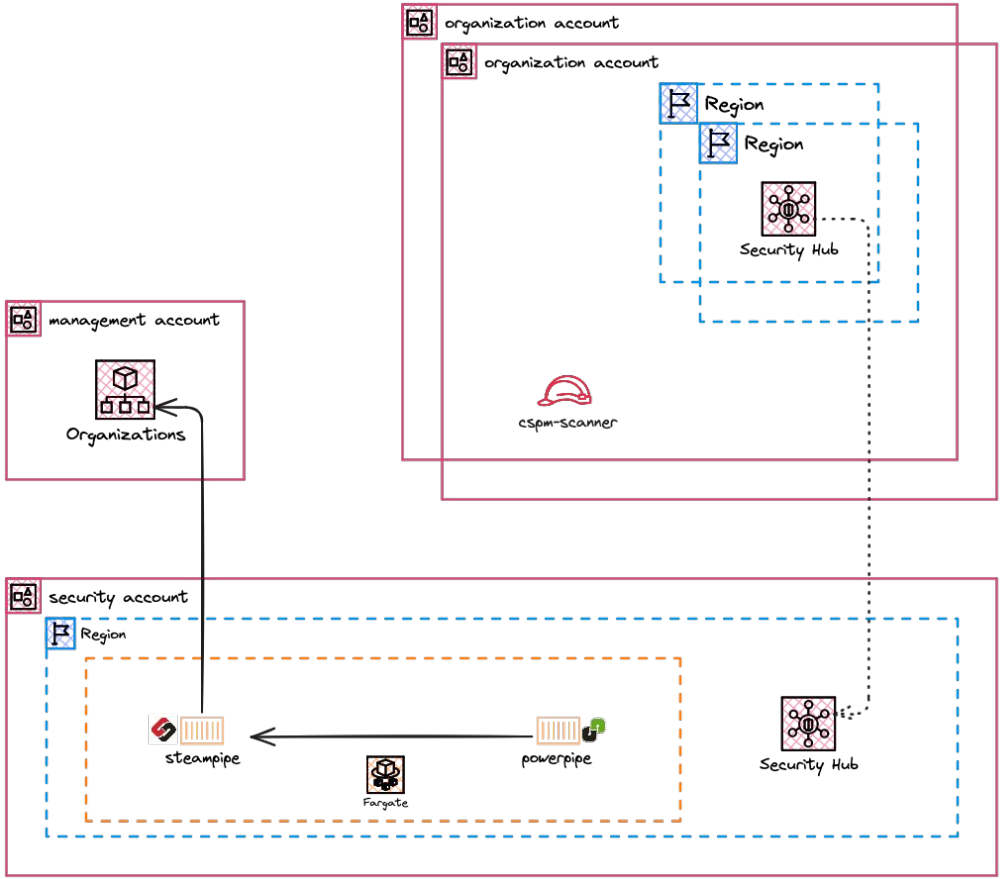
Recap

Recap



1. Generate Steampipe configuration files based on AWS Organization accounts.

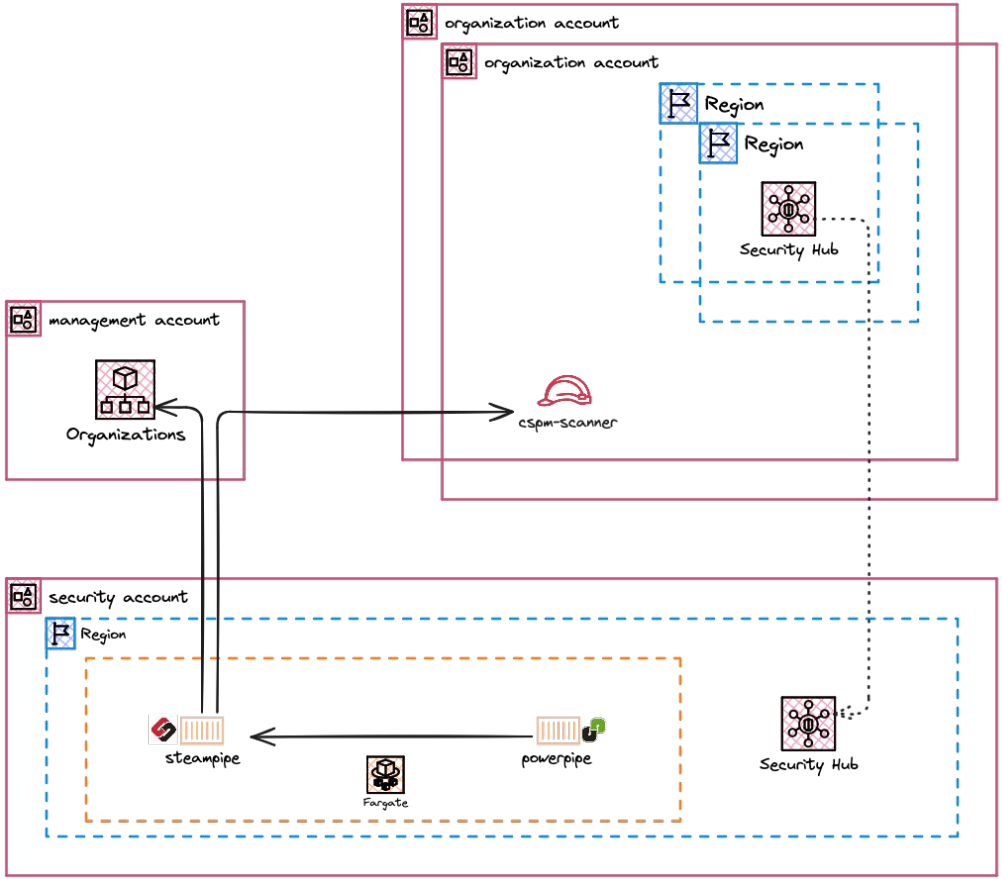
Recap



2. Execute desired controls.

flywire

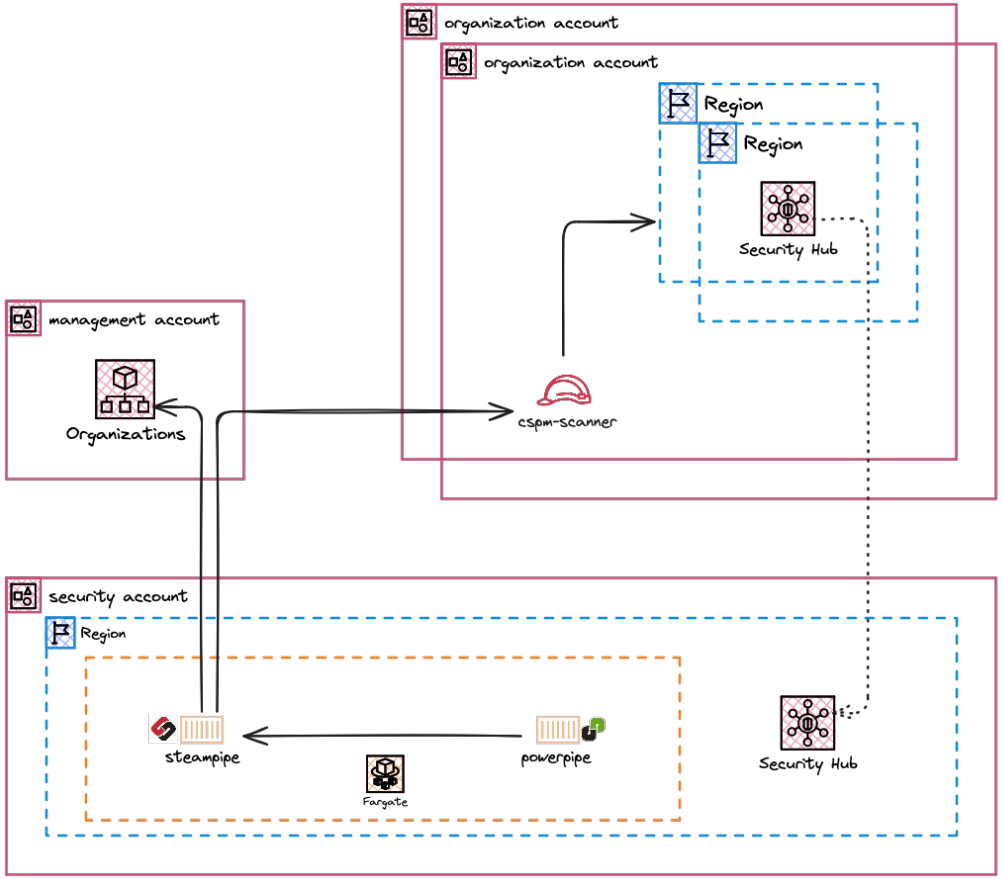
Recap



3. Assume a Role in each AWS Account with the needed permissions.

flywire

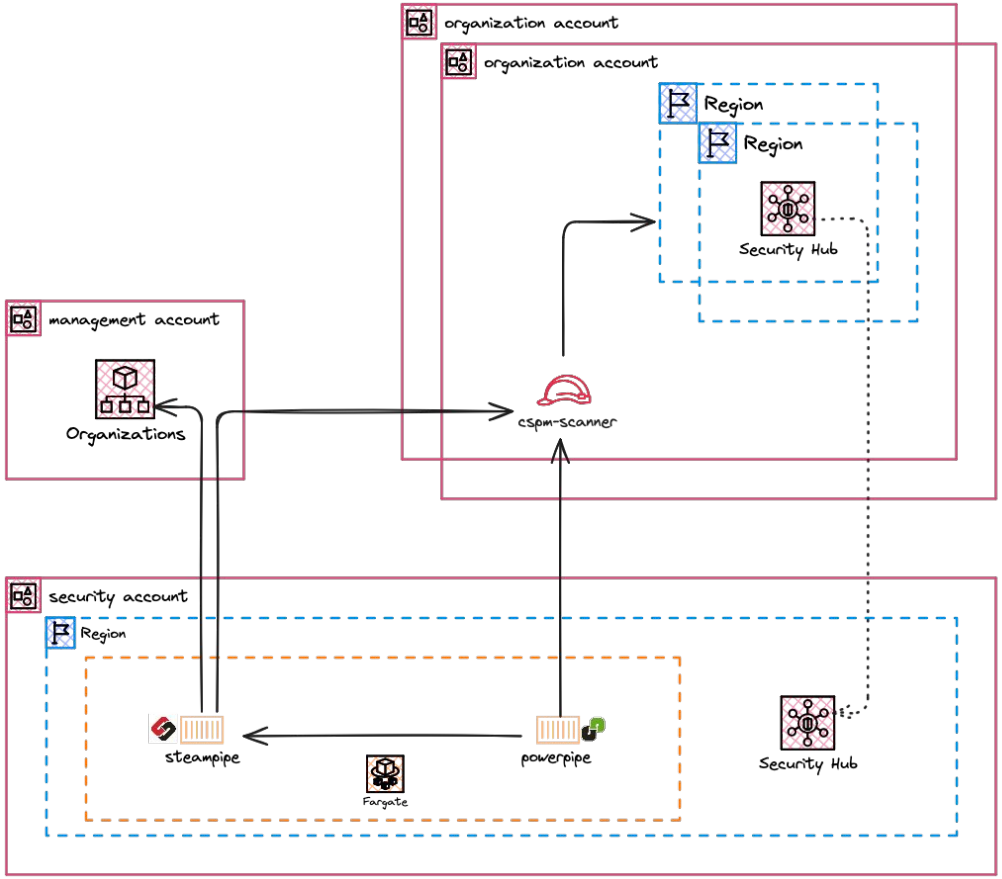
Recap



4. Scan account resources based on controls.

flywire

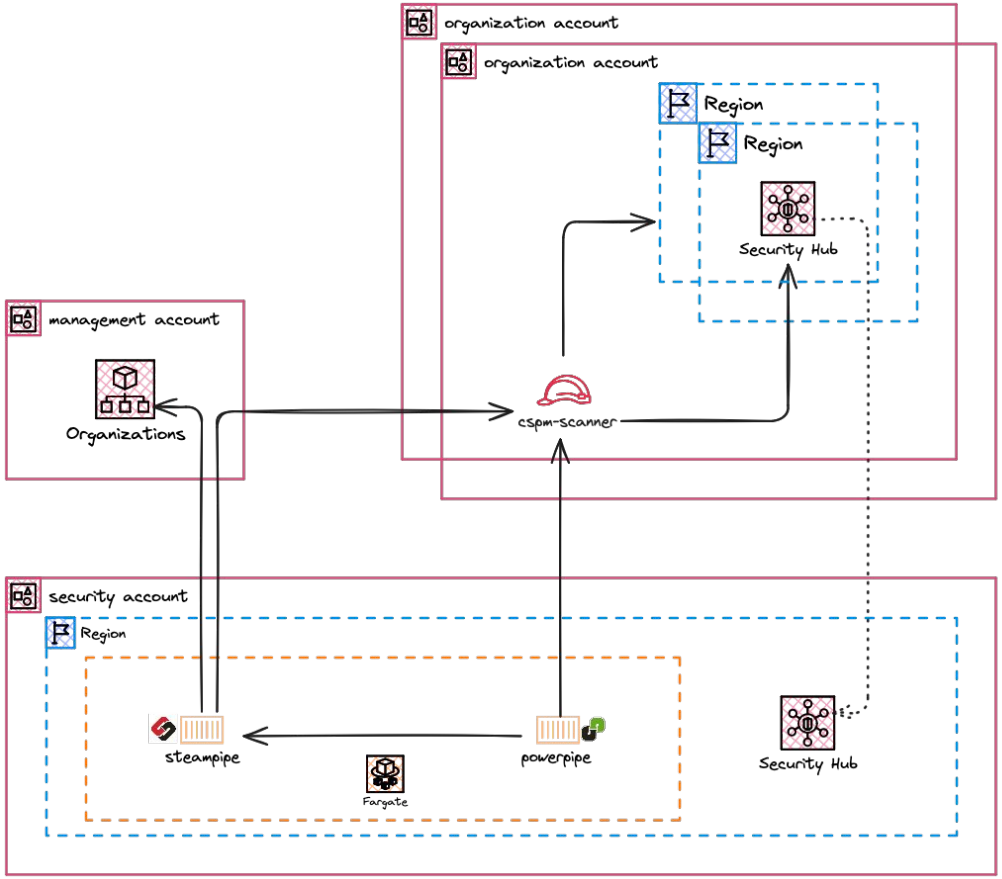
Recap



5. Assume a Role in each AWS Account with the needed permissions.

flywire

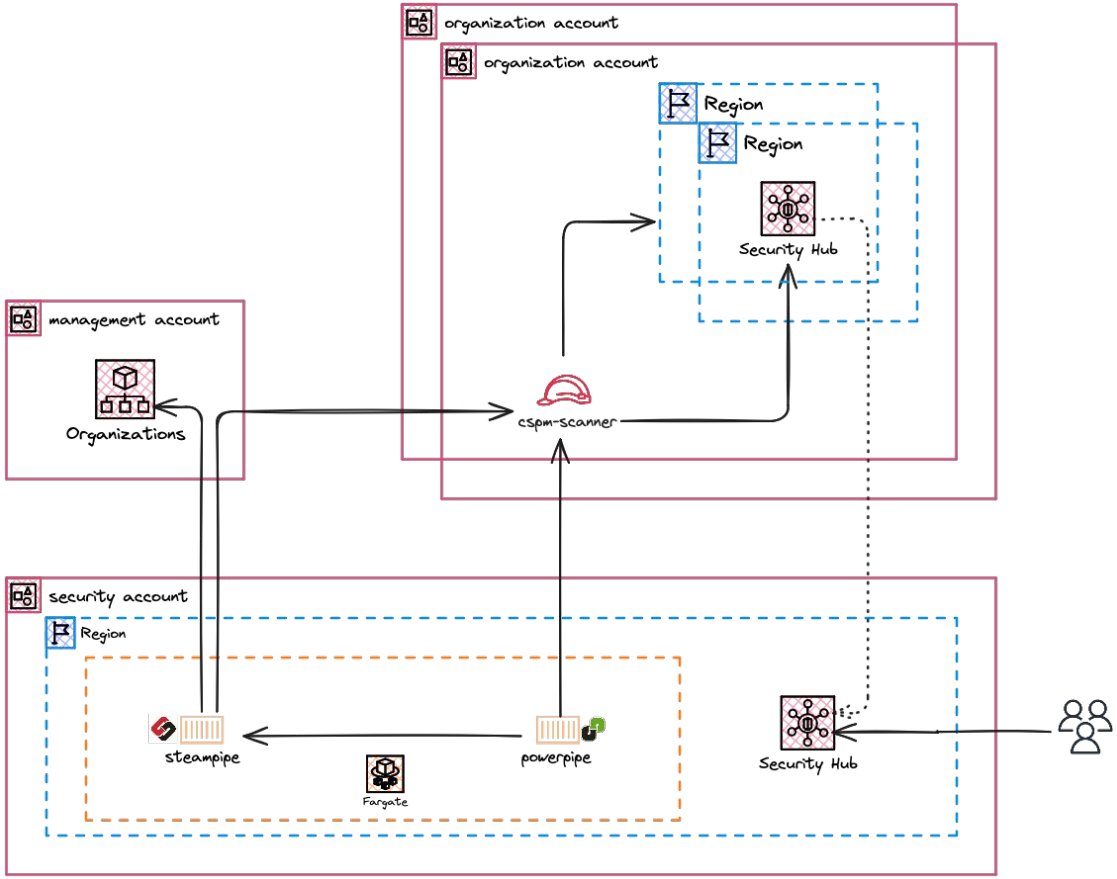
Recap



6. Import findings into AWS SecurityHub.

flywire

Recap



7. Manage centralized findings.

flywire

Demo time!

flywire

flywire

Conclusion

Add a CSPM to your organization...

...or build your own.

There are other opensource alternatives:

Questions?

@sbldevnet

samuelbl

@andoni013

andoniaf

@AWSUG_VLC

@unicrons_cloud