The journey to customized security

From first steps to full automation

AWS Enterprise Support Day Iberia | Barcelona

AWS community builders

aws User Group Leader

unicrons.cloud

aws certified Security SPECIALTY

```
> aws sts get-caller-identity

{
 "name": "Samuel Burgos López",
 "job position": "Cloud Security Engineer",
 "company": "Flywire",
 "rrss": {
   "bluesky": "@sbldevnet.com",
   "twitter": "@sbldevnet",
   "linkedin": "sbldevnet",
   "blog": "unicrons.cloud"
 }
}
```

flywire

Agenda

- What’s a CSPM?
- Our Journey
- Auto Remediation
- Next Steps
- Key Takeaways

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
- Cost Efficiency

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
- Cost Efficiency

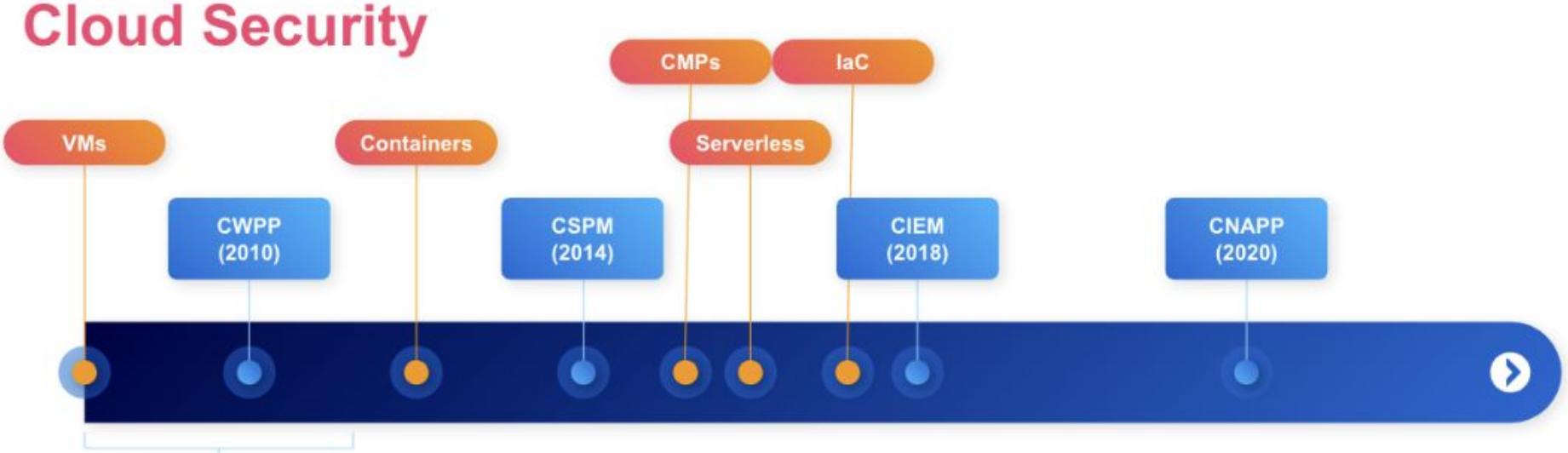
Makes your cloud looks like this...

And not this...

flywire

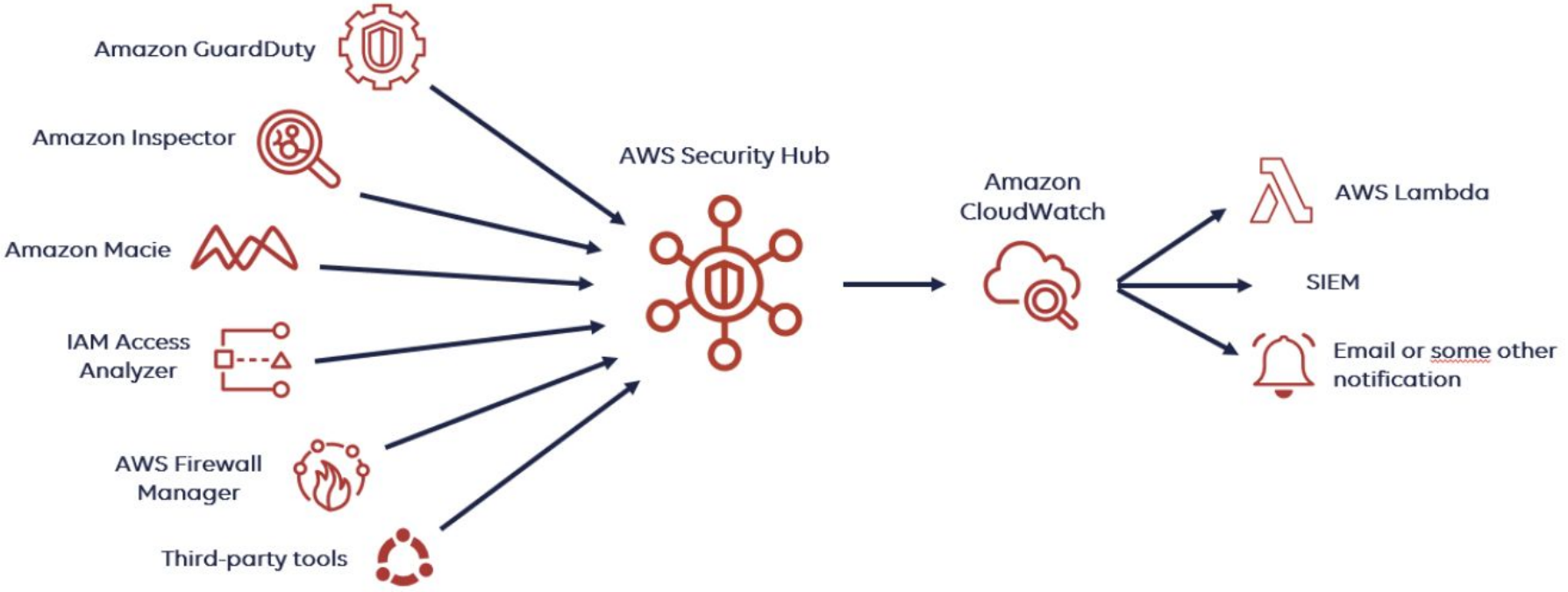
What is CSPM?

And what about CWPP, CIEM, CNAPP and CTEM?



flywire

What is CSPM?



flywire

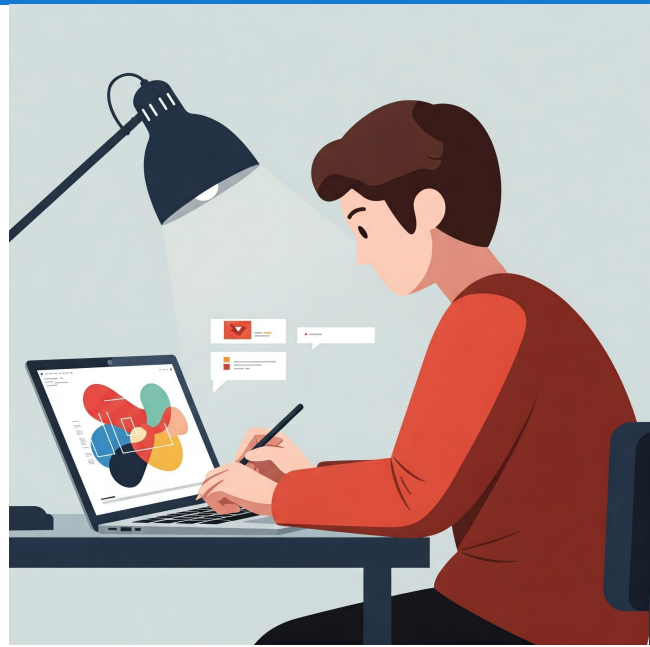
Our Journey

Our journey: the beginning

The beginning

- Small team.
- Local execution.
- What do I have?
- What's the status of my environment?

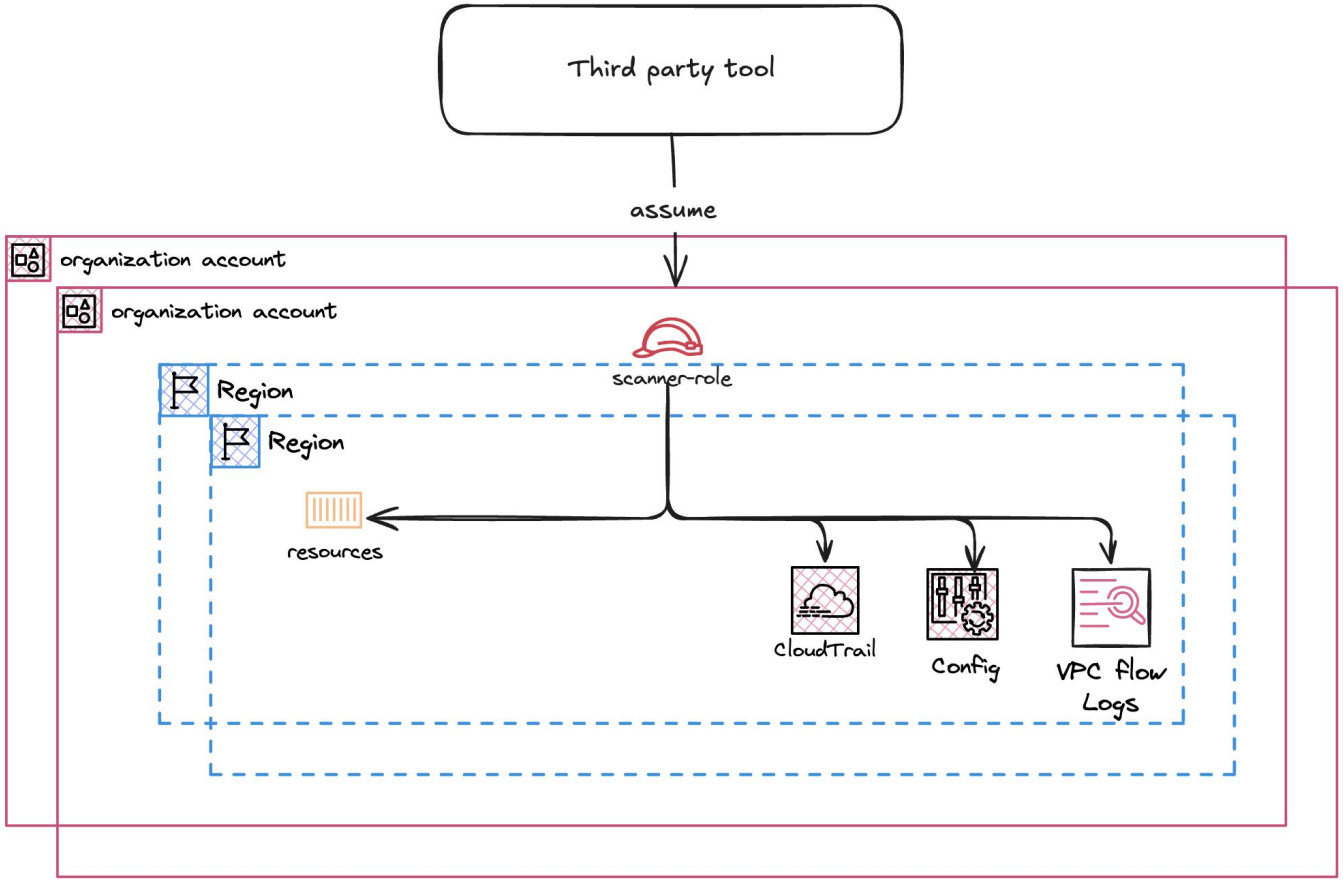
Let's start to automate it 🚀



prowler

flywire

Our journey: 1st attempt



flywire

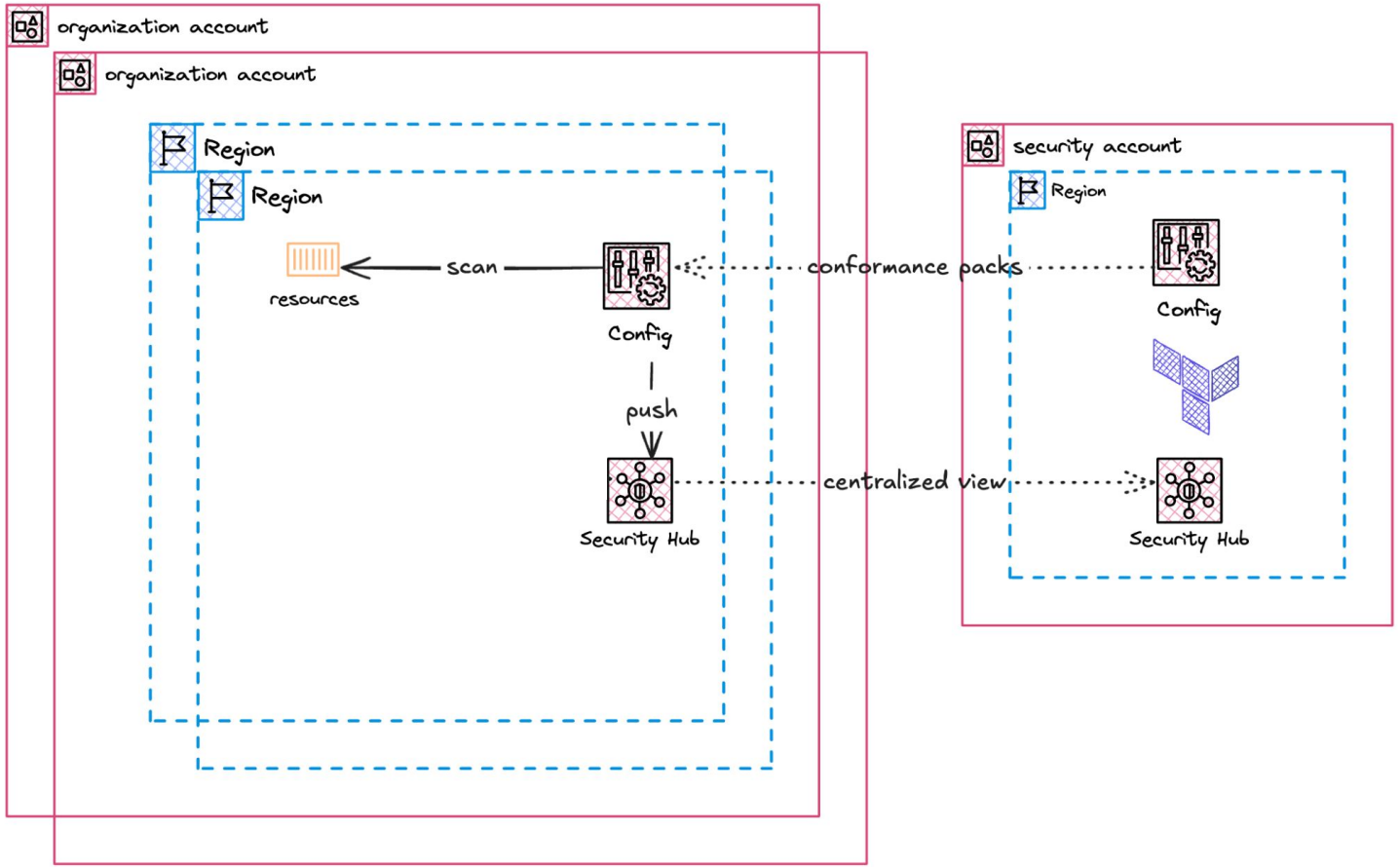
Our journey: 1st attempt

1st attempt: 3rd party tool

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

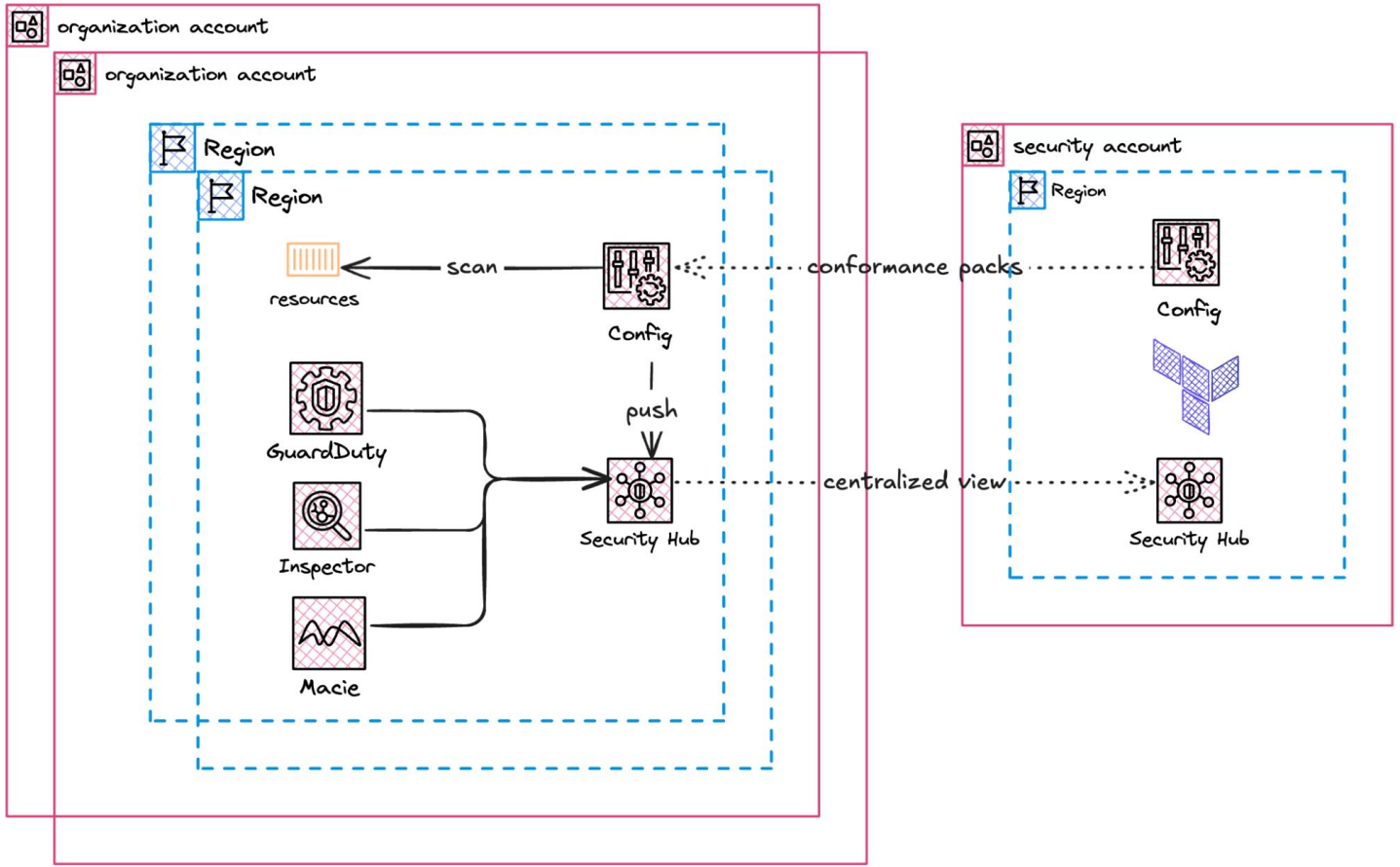
flywire

Our journey: 2nd attempt

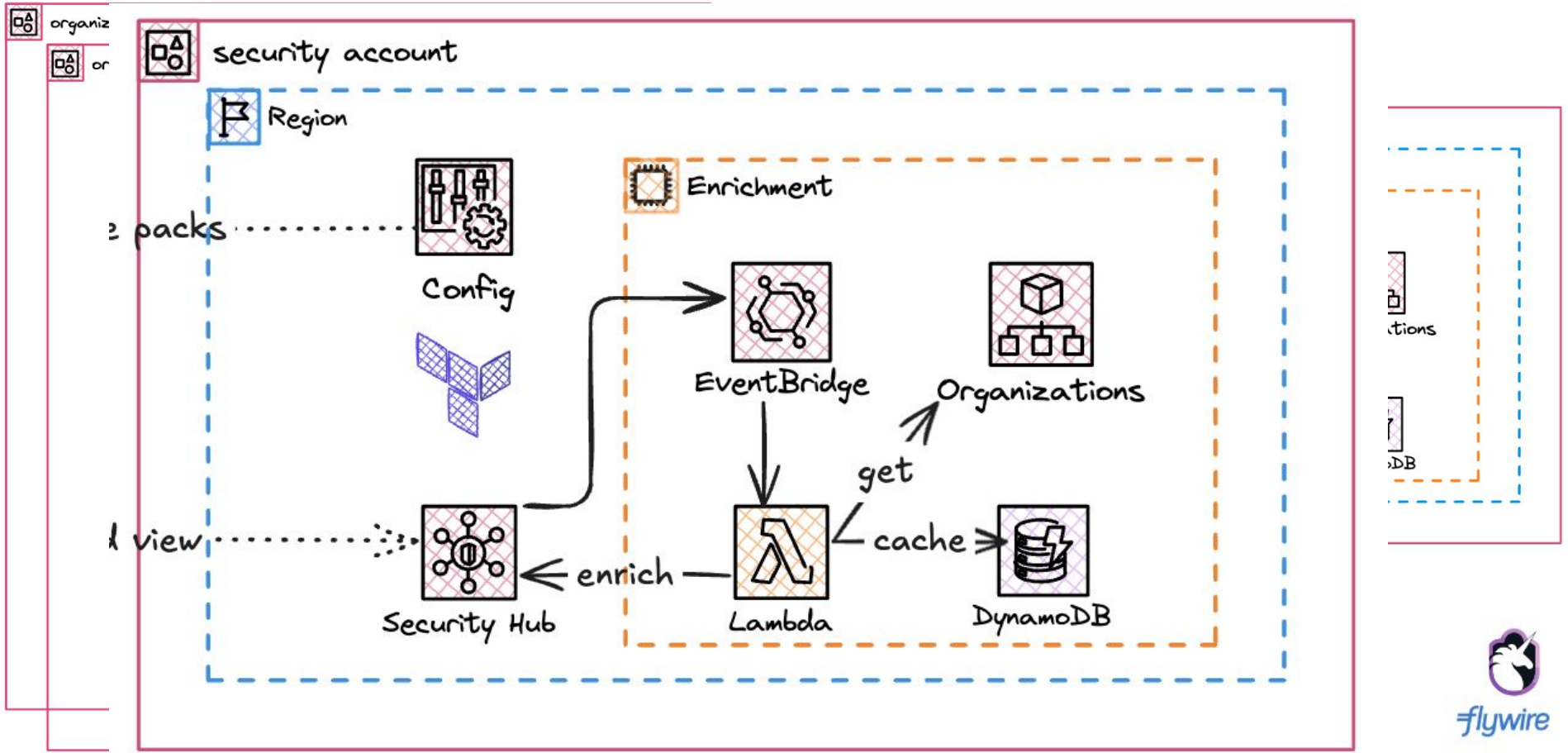


flywire

Our journey: More services

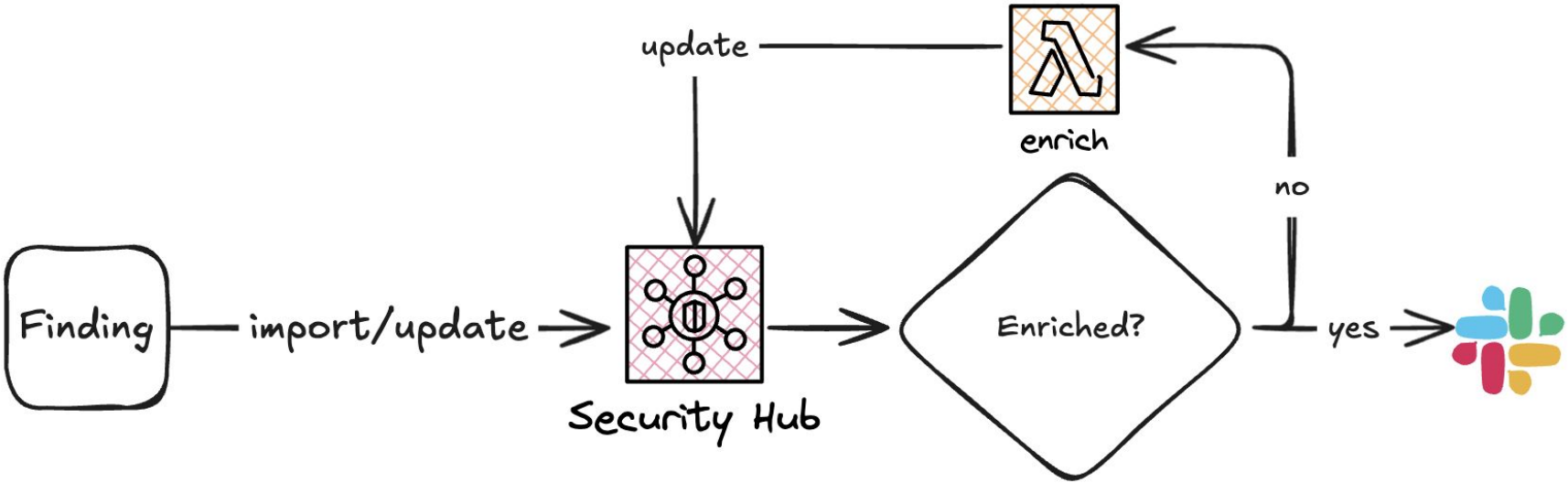


Our journey: Enrichment



flywire

Our journey: Enrichment

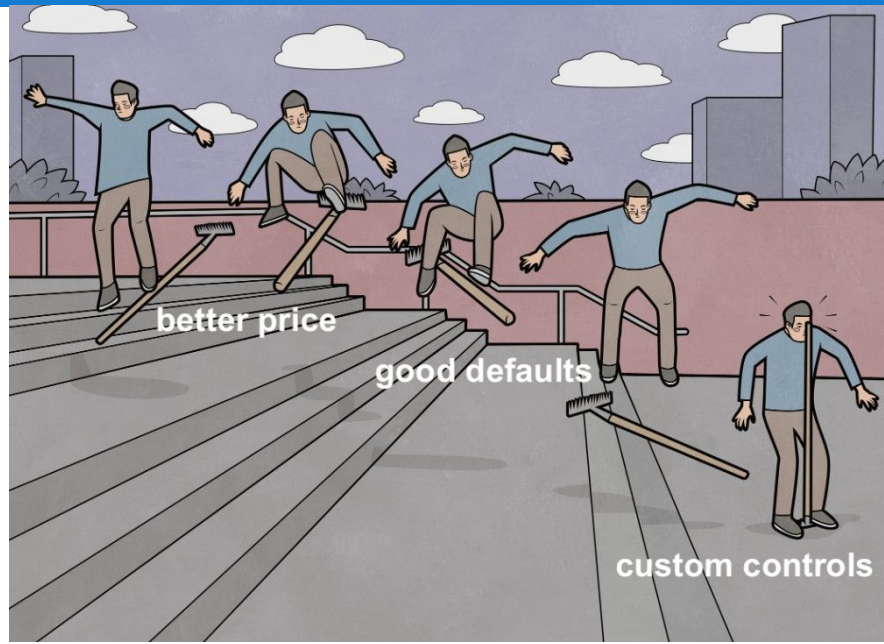


flywire

Our journey: 2nd attempt

2nd attempt: AWS Config + SecurityHub

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

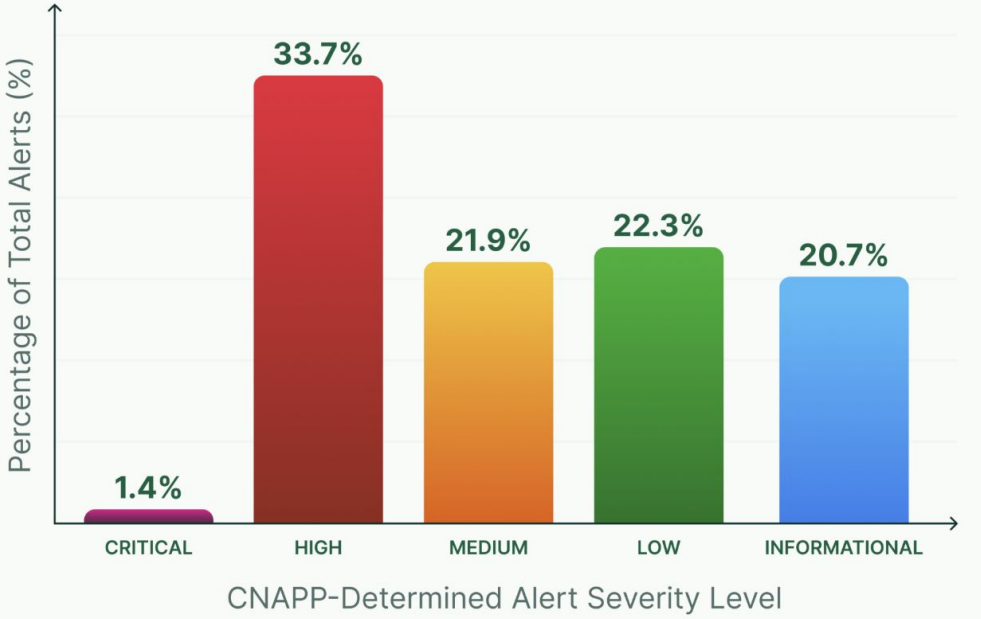


Default controls are standard. Your company is not.

flywire

Our journey: Current approach

High Alerts Make Up the Majority of Your Alerts

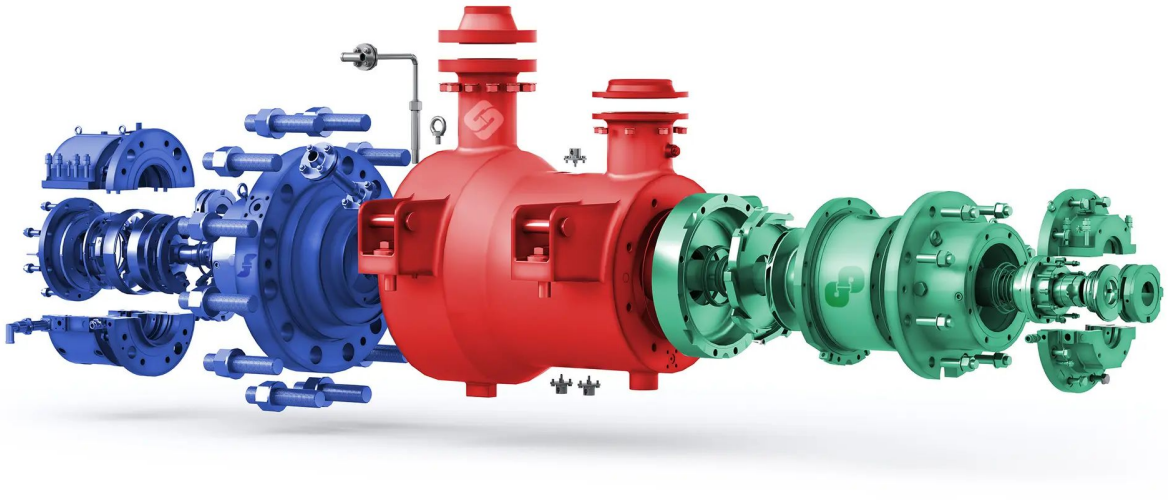


flywire

Our journey: Current approach

Current approach: Steampipe + SecurityHub

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



flywire

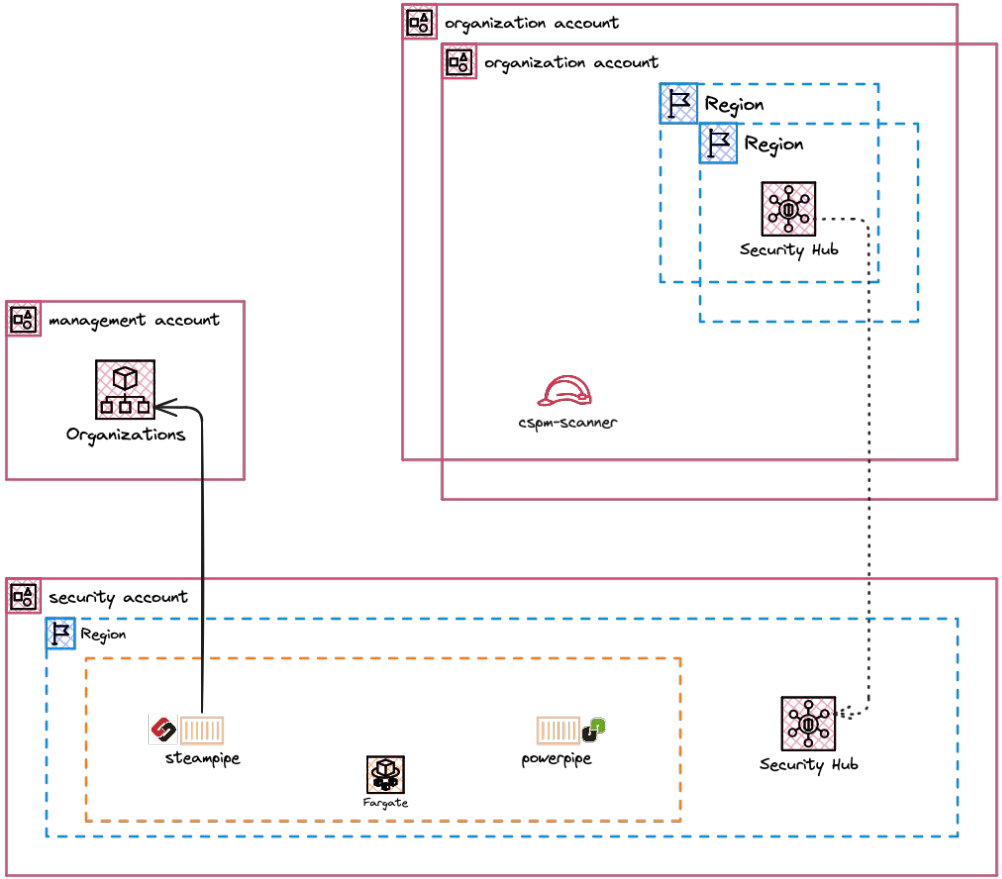
Our journey: Current approach

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

```
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

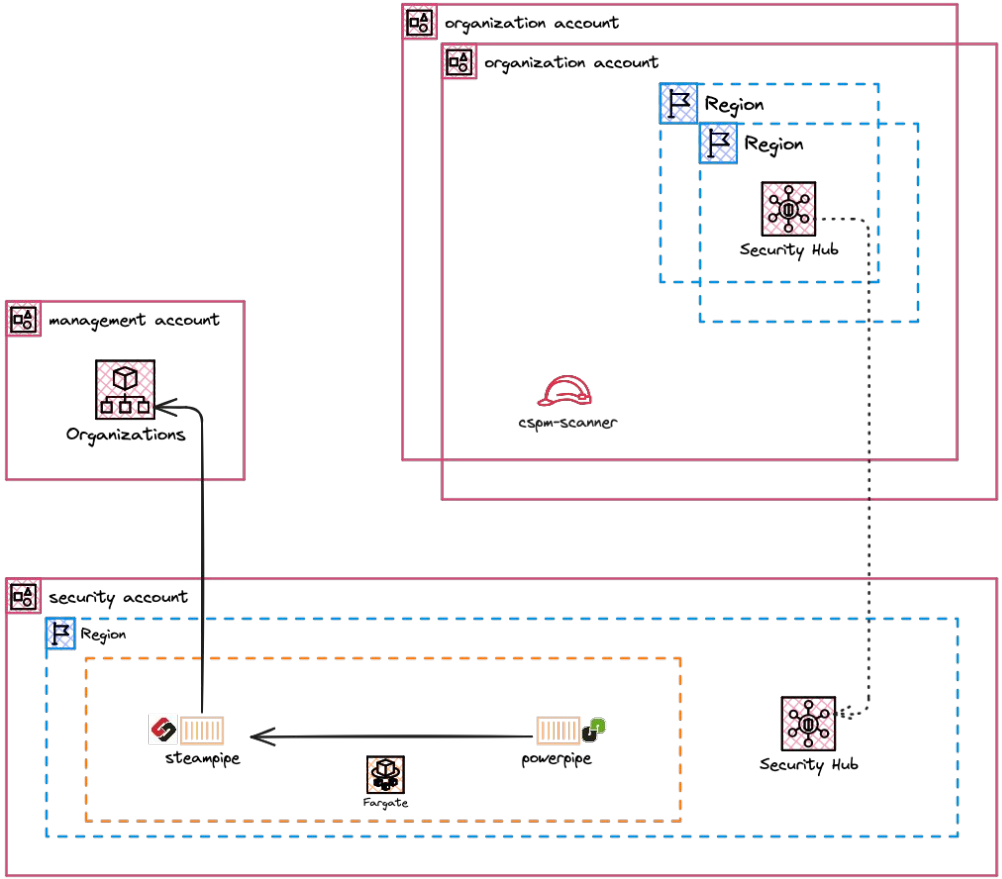
Our journey: Current approach



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

flywire

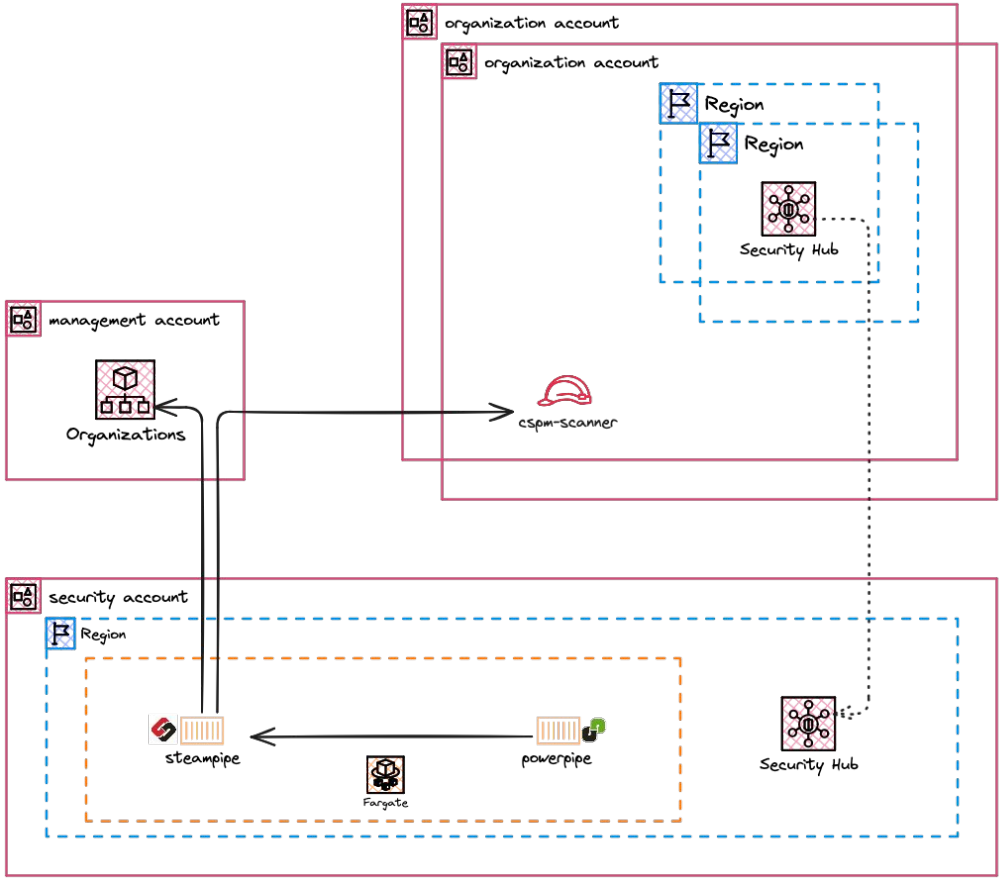
Our journey: Current approach



2. Execute desired controls.

flywire

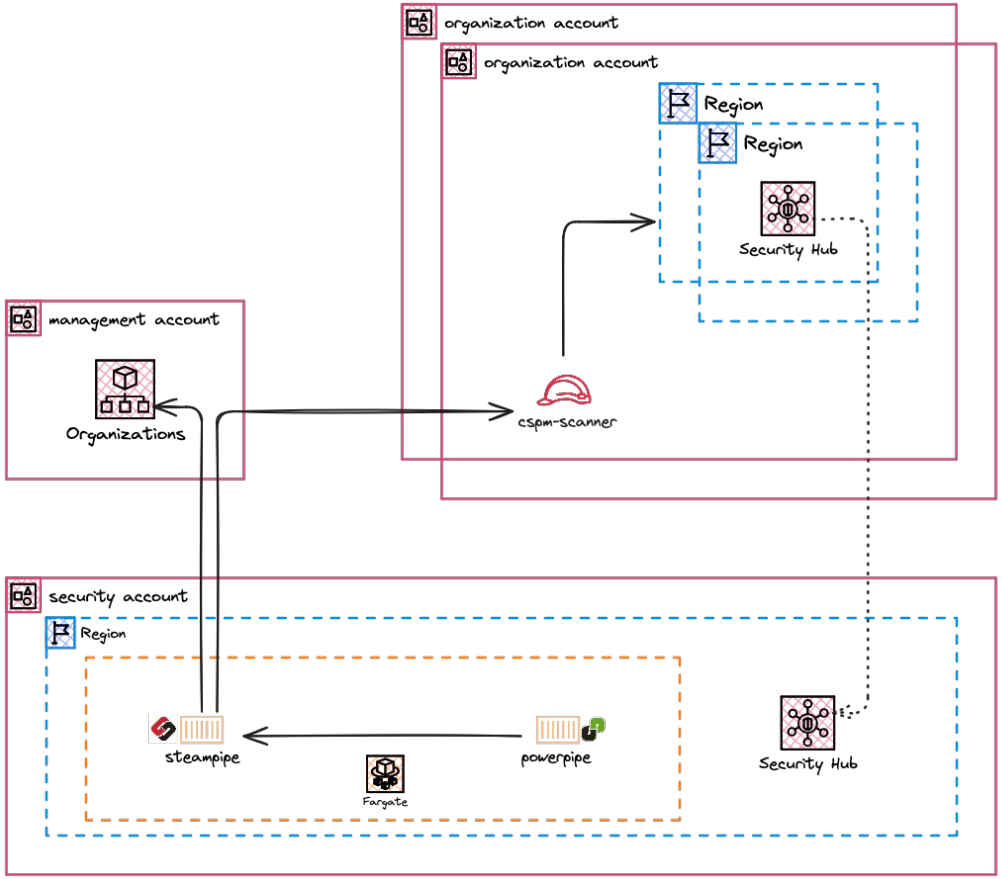
Our journey: Current approach



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

flywire

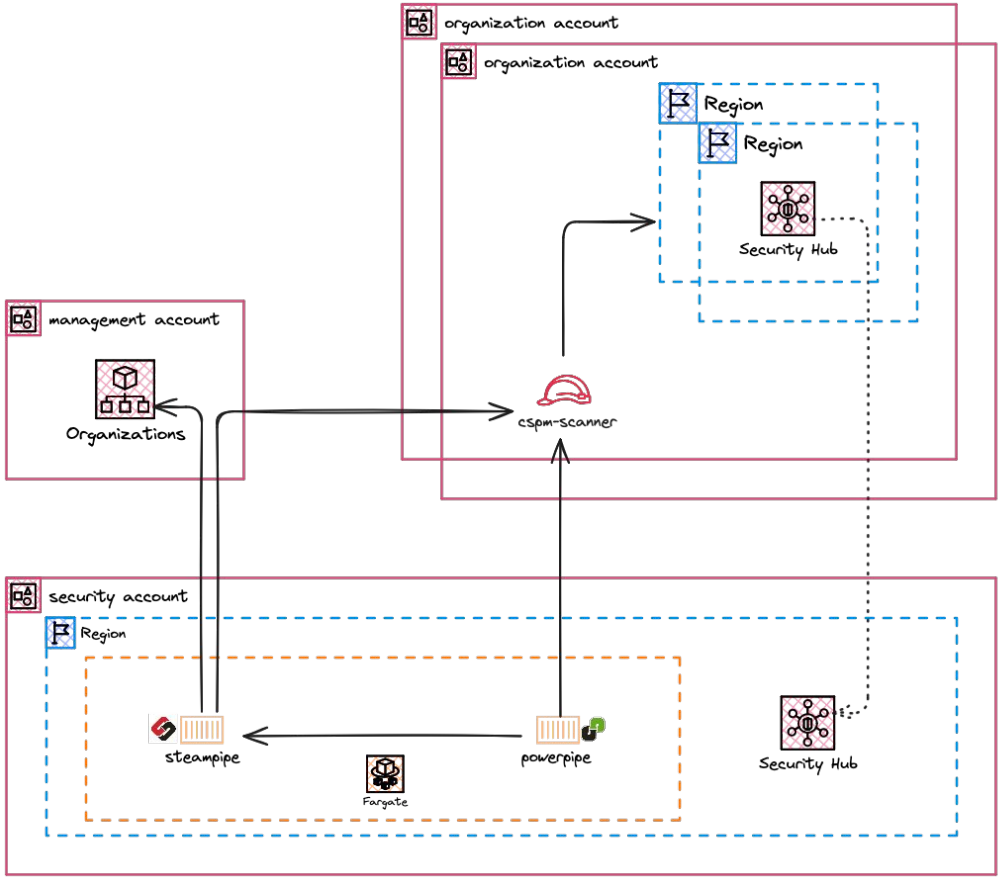
Our journey: Current approach



4. Scan account resources based on controls.

flywire

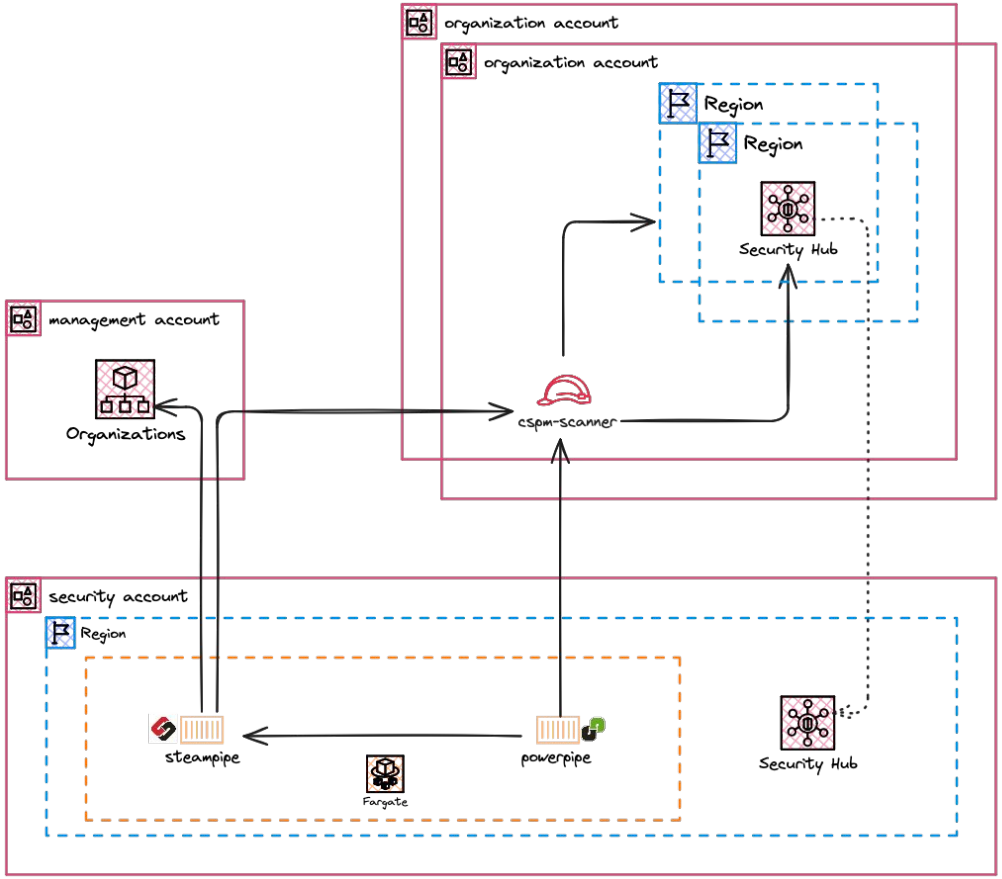
Our journey: Current approach



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

flywire

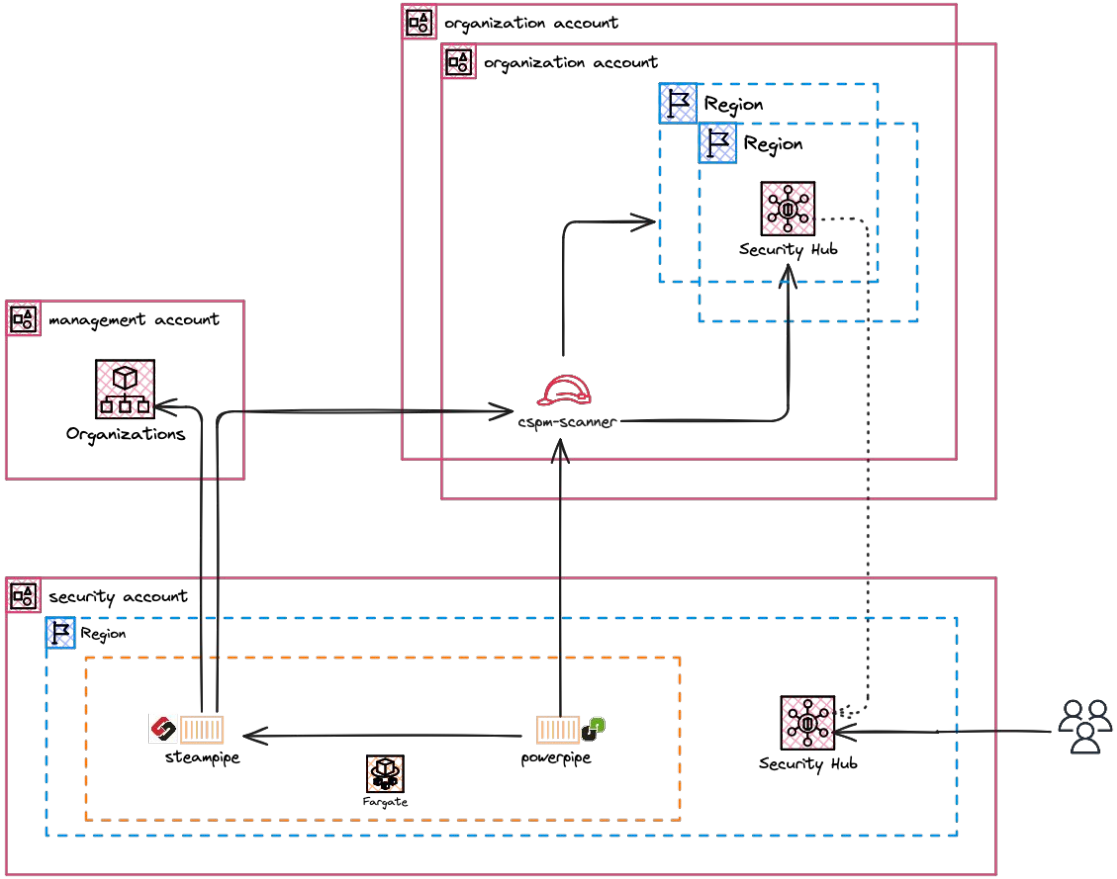
Our journey: Current approach



6. Import findings into AWS SecurityHub.

flywire

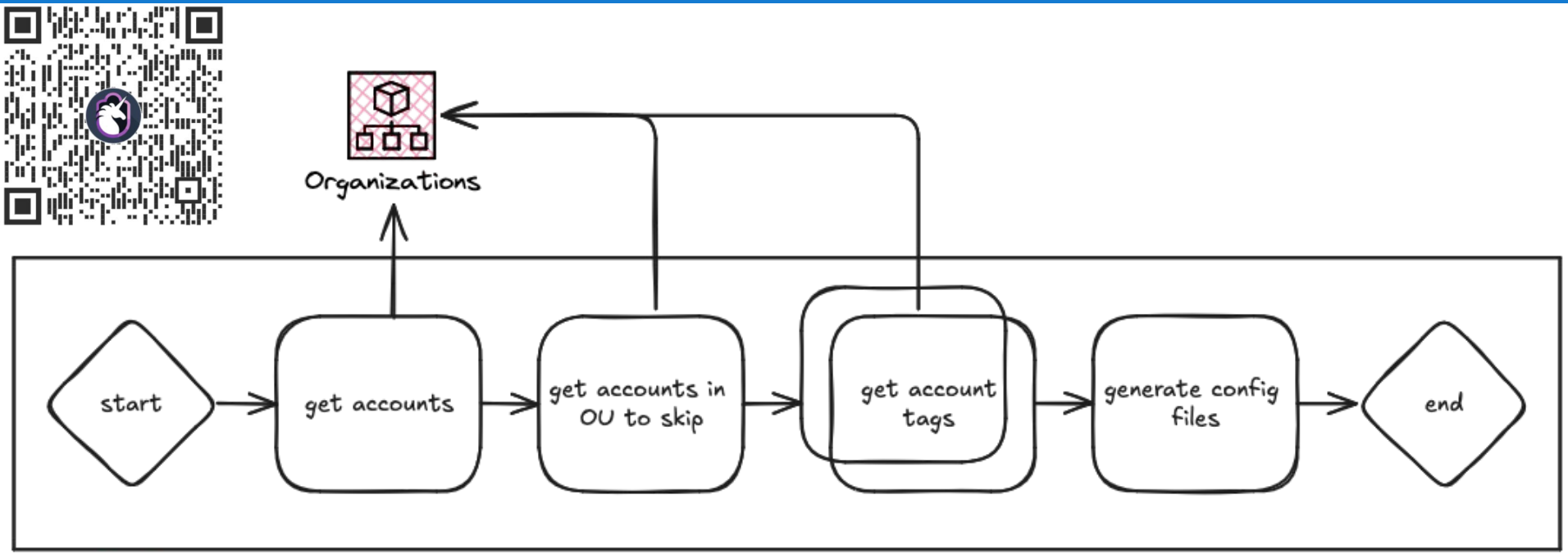
Our journey: Current approach



7. Manage centralized findings.

flywire

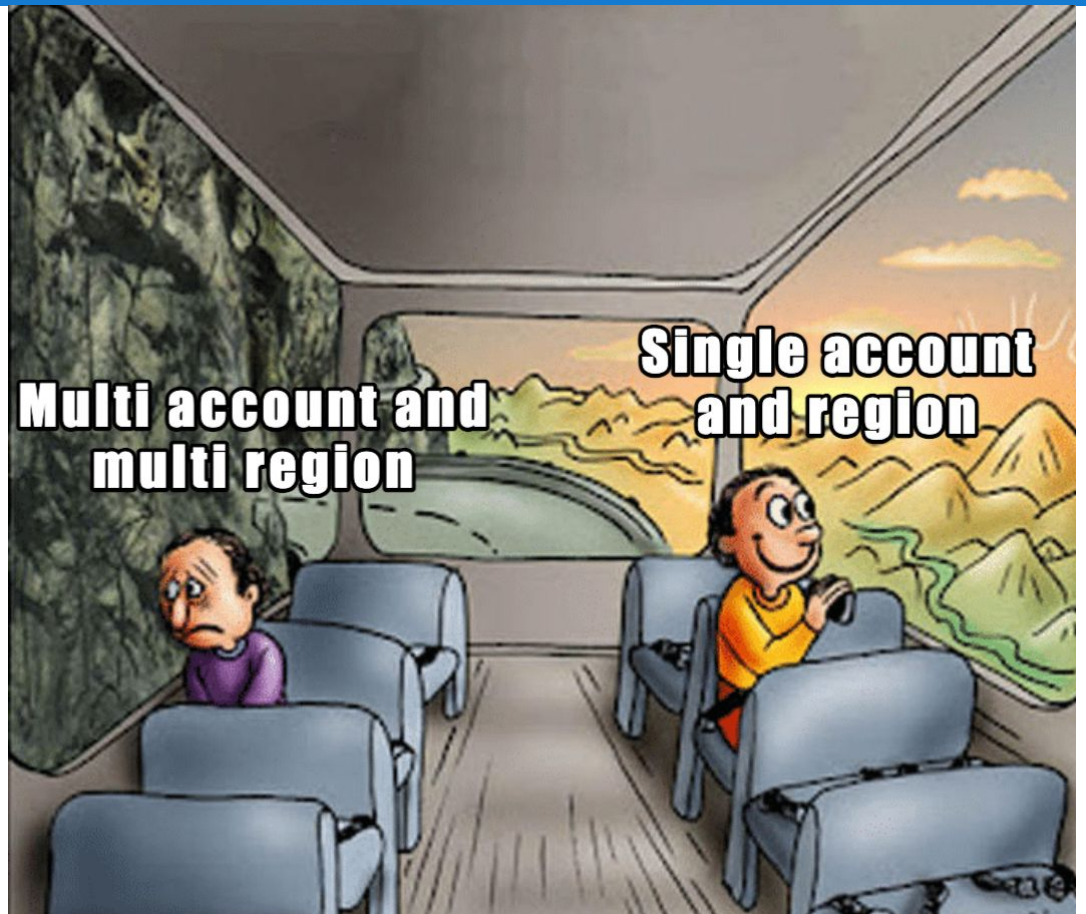
Integrate Steampipe with AWS Organizations



steampipe-config-generator

flywire

Our journey: Current approach



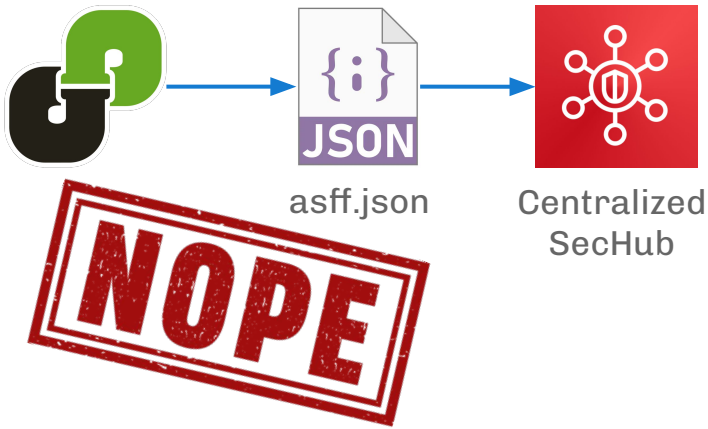
flywire

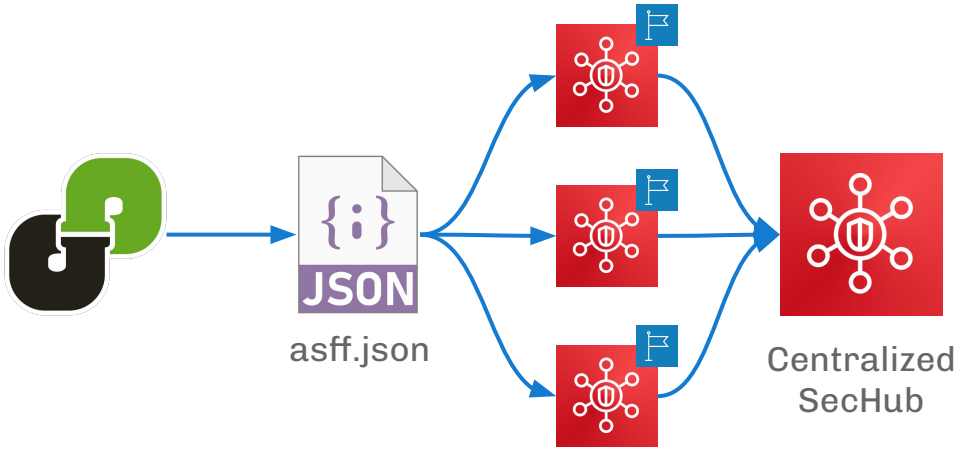
Our journey: Current approach

flywire

Our journey: Current approach

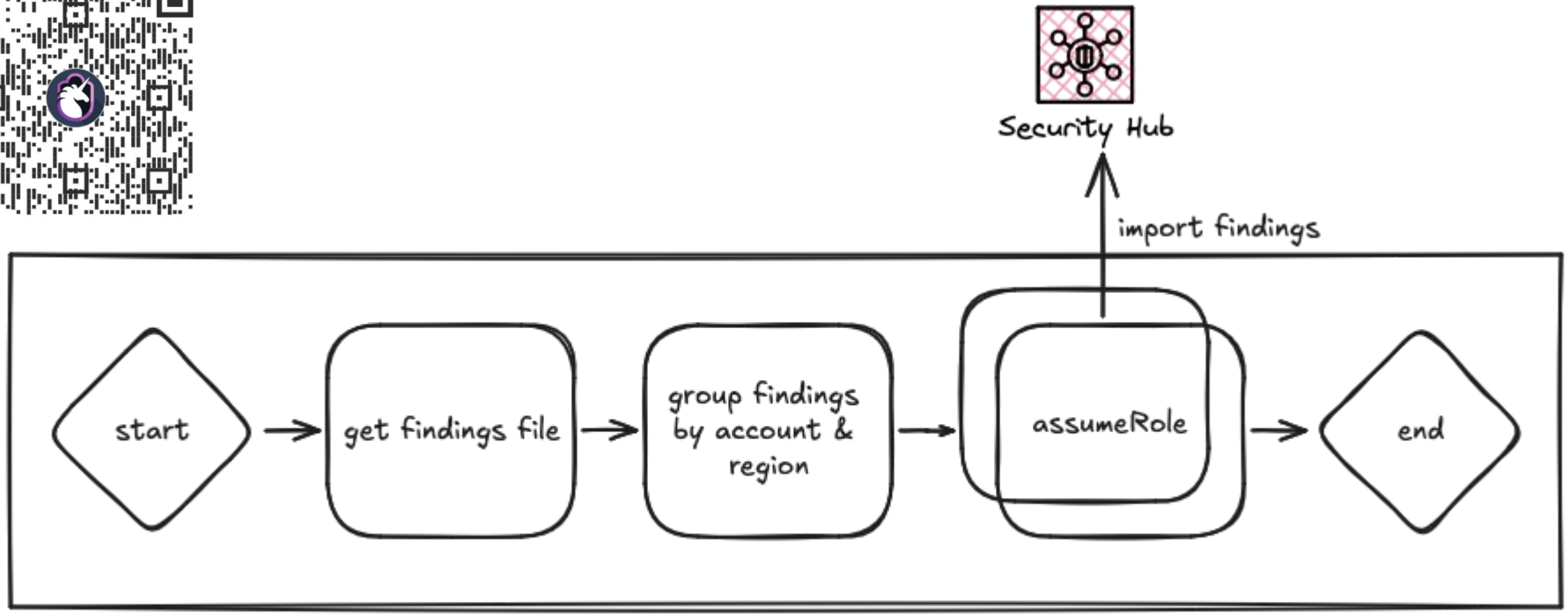
```
❯ powerpipe benchmark run aws_communityday --export asff.json
```





flywire

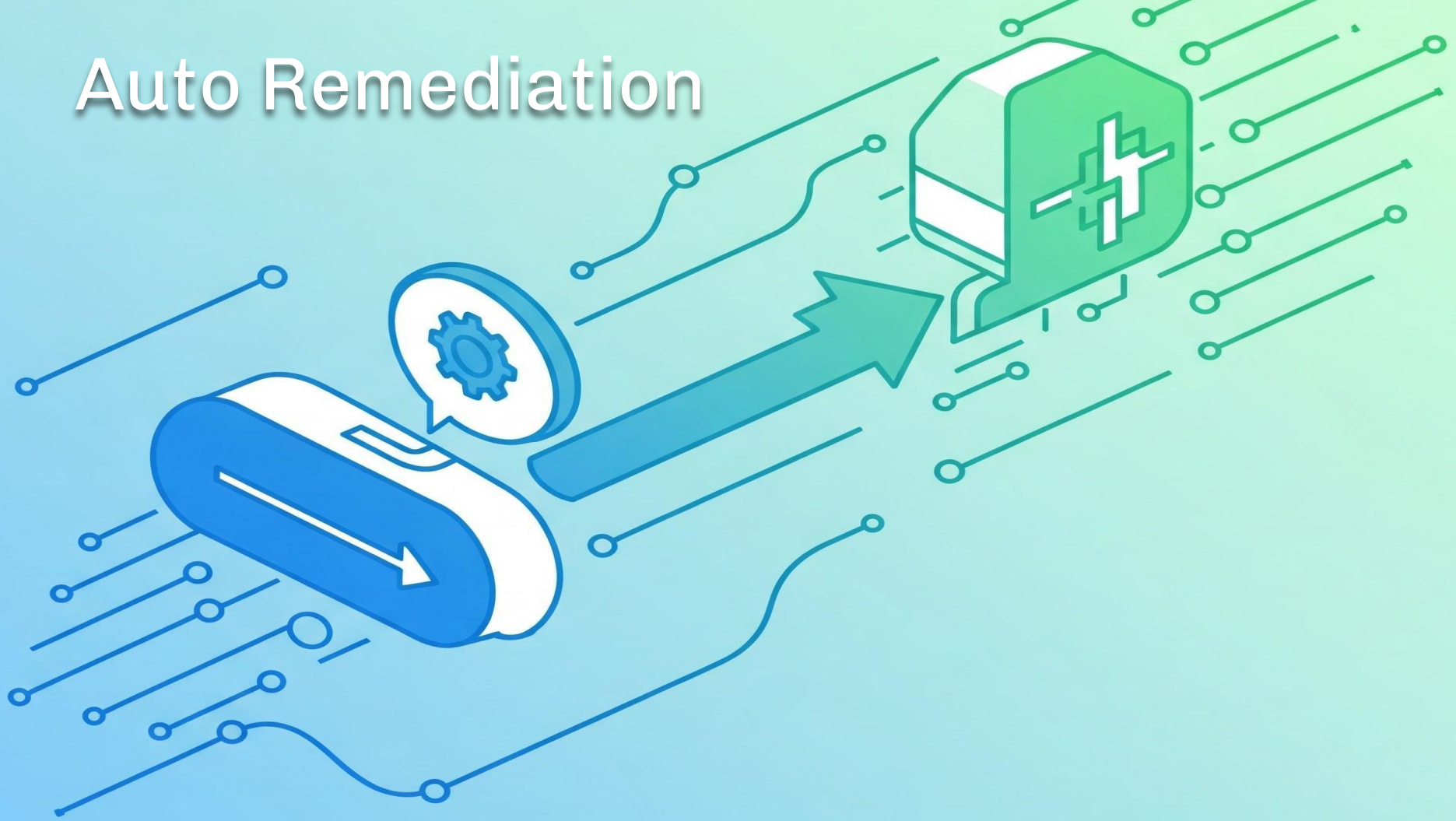
Integrate Powerpipe with AWS SecurityHub



powerpipe-securityhub-importer

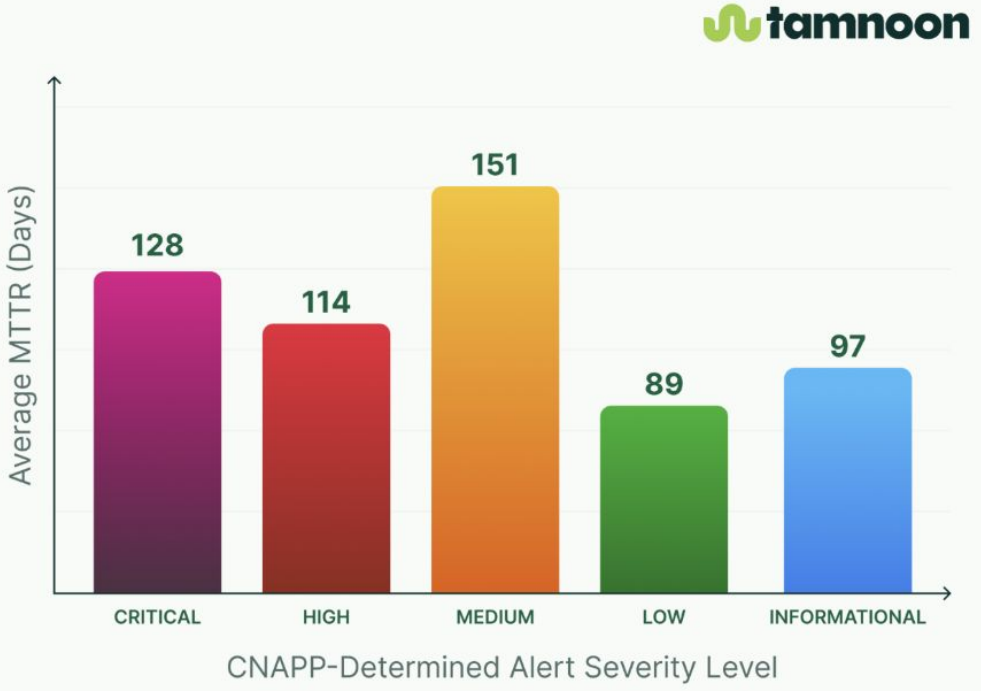
flywire

Auto Remediation



Auto Remediation

Cloud Alert Resolution Time: Severity Matters

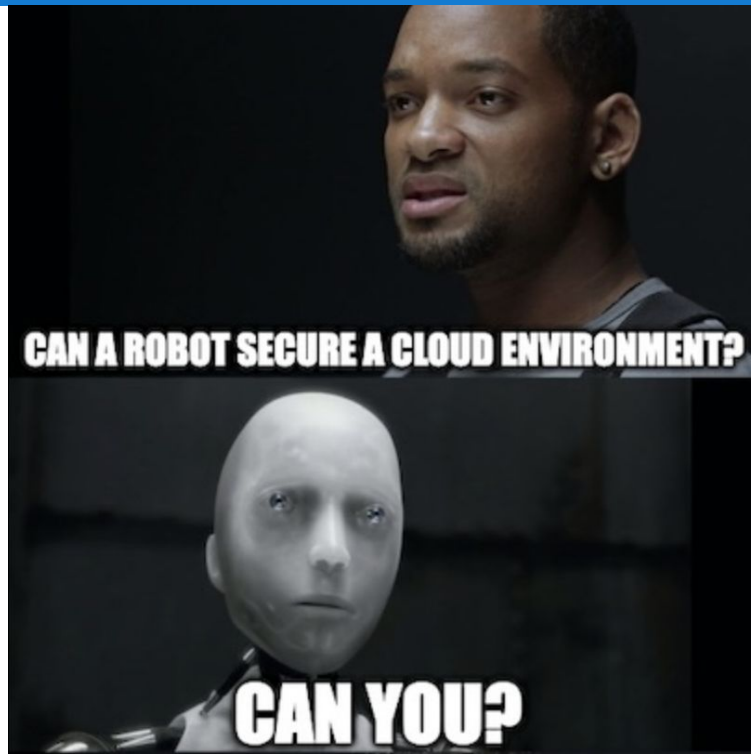


flywire

Auto Remediation

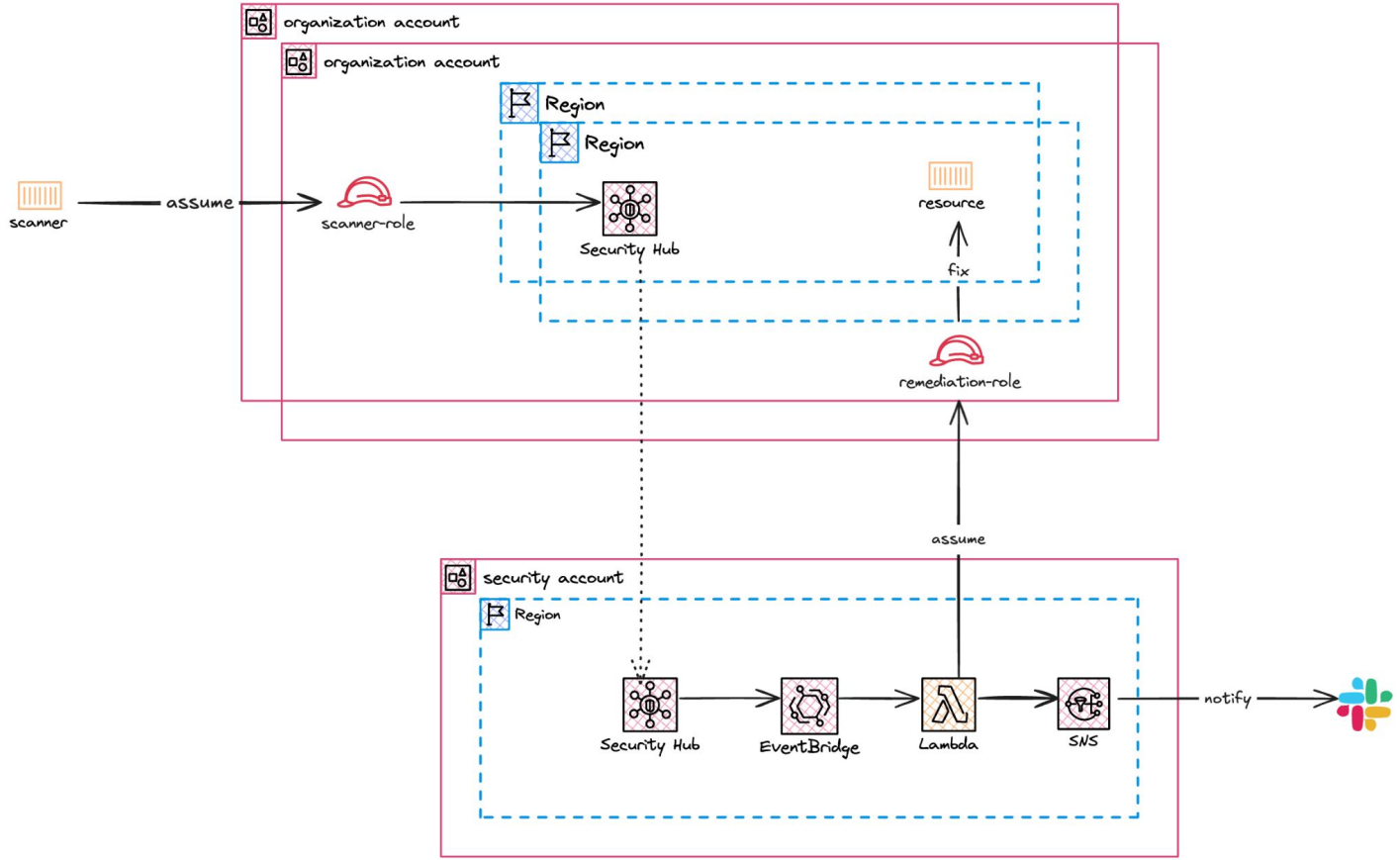
Farris's Three Laws of Cloud Security Auto Remediation:

- A bot must never harm stateful data or allow stateful data to come to harm.
- A bot must act with utmost haste so functionality doesn't become dependent on a misconfiguration.
- A bot must announce its existence and tell a carbon-based life form what it did and why.



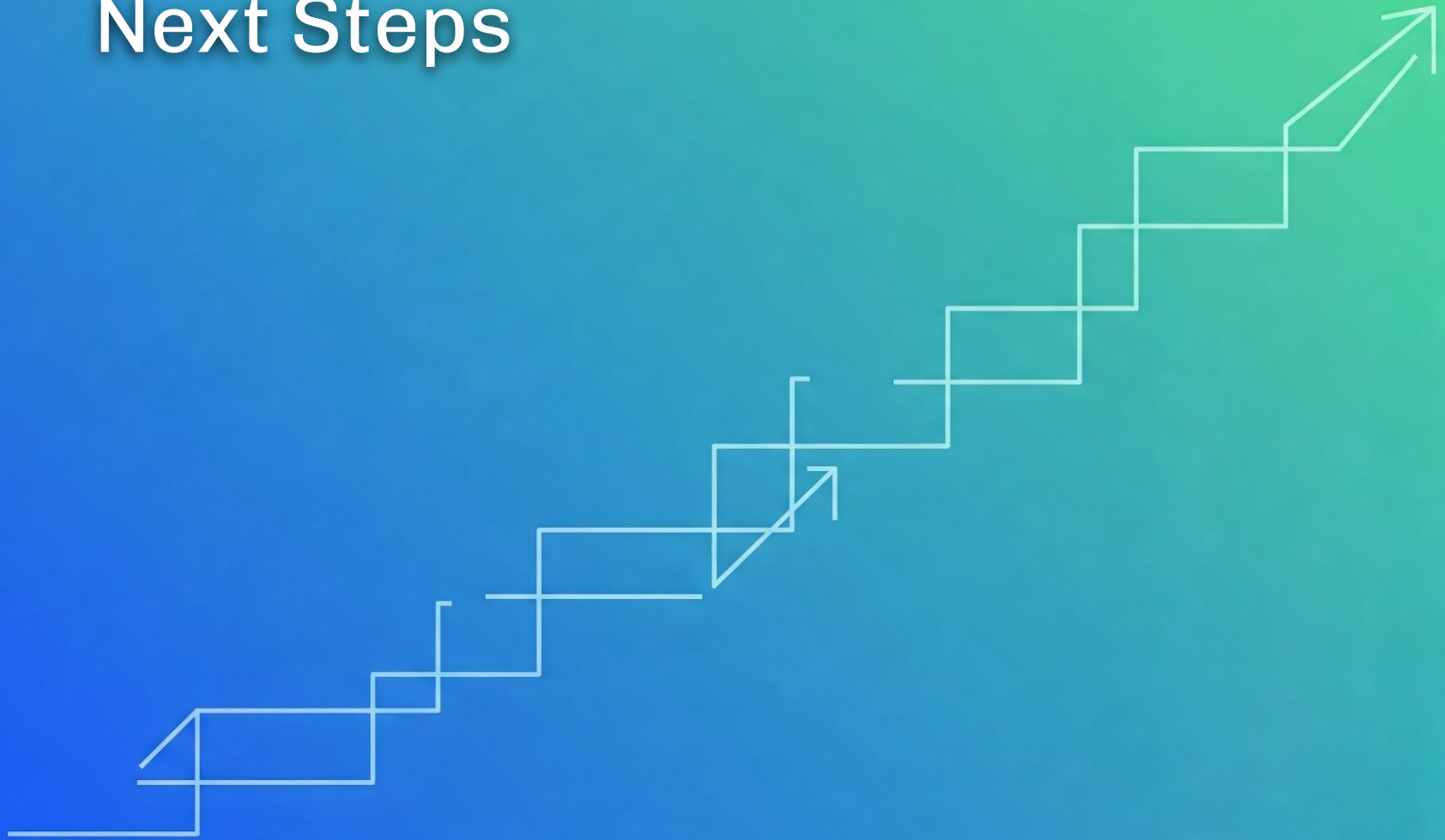
flywire

Auto Remediation



flywire

Next Steps



Next steps

- **RBAC reporting access.**
- **More integrations.**
- **Expand auto remediation coverage.**
- **Auto remediation approvals.**

Key Takeaways

Key Takeaways

- **Use AWS Organizations. Always.**
- **Default controls are standard. Your company is not.**
- **Build your solution is not easy, but it's worth it.**
- **Automate everything as possible.**
- **Expend time building your own reports.**

Questions?

@sbldevnet

sbldevnet

unicrons.cloud

Oct 14, 2024 · in aws, iam, iac, terraform · 6 min read

Deploy IAM Roles across an AWS Organization as code

Oct 18, 2024 · in aws, aws_organizations, go · 3 min read

Import your Powerpipe results into AWS SecurityHub

Automate your Steampipe AWS configuration with AWS Organizations