GCC 2.0 Tech Talks

- AWS GA is coming on **4th May 2022**.
- If and when we talk about Native Services, we will probably cite **AWS only** as these are gearing towards AWS GA preparation.
- Information on Azure will be shared in coming months (to recap, Azure GA will be by Q3 2022).
- All slides will be shared and most of the documentation will also be translated to either Developers Portal (accessible by everyone) or Docs Portal (only accessible by for TechPass account holders).
- All the slides can be shared with existing contractors who are required to manage Projects on GCC as deemed fit by Agencies.
- The series of “Brown Bag” lunch time tech talk is arranged so as to ensure more people can join us in view that some will clash with your meetings. Please feel free to have your lunch while you join us.

For Your Info

- You will be put on mute by default.
- Video should be turned off.

Q&A Segment

- Type in message box when you want to ask a question.
- Wait to be acknowledged by the presenter before speaking.
- Unmute your microphone and state your name and agency clearly.

Session Recording

- Please note that the series of GCC 2.0 Tech Talks will be recorded.
- The video recordings will be made available (in SharePoint).

Let Us Know Your Feedback!

https://form.gov.sg/625cb8b4ef648600142b2cd2

- Let us know what went well and how we can improve.
- We want to ensure that we are bringing the right contents to you so as to help Agencies.
- If you have any questions, please reach out to us at Ask_CODEX@tech.gov.sg

Continuous Compliance in GCC 2.0

Chua Kai Ming
GDS / ENP – Cloud

Date: 19th April 2022

TABLE OF CONTENTS

1. Light Touch Approach in GCC 2.0
2. Challenges of compliance
3. Why use cloud native security products
4. Intro to Cloud Native security products used in continuous compliance coverage
5. What are benefits with GCC 2.0 continuous compliance
6. Cost of GCC 2.0 continuous compliance to tenants
7. Q&A

The Light Touch Approach in GCC 2.0

- In GCC 1.0, Agencies face challenges with development due to the tight restrictions imposed by AWS Organizations Service Control Policies (SCPs) and IAM Permissions Boundary policies. For GCC 2.0, agencies will have more liberty with platform usage by replacing some SCPs and permissions boundaries with Policy-as-Code (PaC).

- In addition, GCC2.0 will implement the use of cloud native security compliance services to enable continuous compliance coverage on cloud workloads.

- When it comes to managing and monitoring security and compliance of workloads in GCC 2.0, agencies can have easier access to the compliance states of their cloud resources.

Before Continuous Compliance

The security governance team is asking for statistics. Without central visibility, I need to poll Agencies on cloud infrastructure compliance status.

☹

How can agency adopt a security compliance solution that is updated with latest industry security standards and internal security policies?

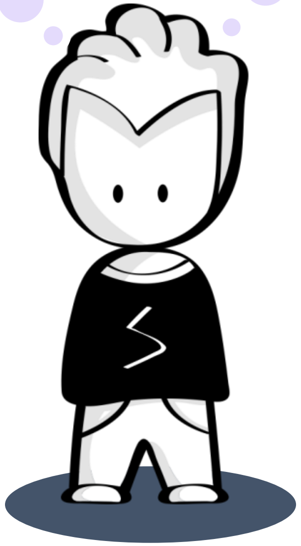
☹

How do I get alerted to cloud infrastructure changes that fail security standards so that I can react pro-actively?

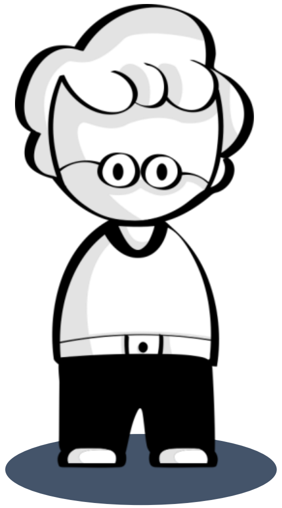
☹

My DevOps teams are constantly rolling out changes.
Our security audits are not frequent enough to catch errors early?

☹



GCC



Agency

Why Use Cloud Native Security Products

Speed

Faster Response
Event triggered configuration changes enable just in compliance detection and remediation is made possible with various notification capabilities.

Fast to Deploy
Cloud Native security products are SaaS that can be subscribed on demand and fast to deploy.

Simplicity

Increase Visibility
GCC and Agencies has access to a central system that automatically aggregate compliance findings from both AWS native and third-party products and reduces customer's effort to integrate different products.

Easy Onboarding
Auto-enable feature in Organisation AWS SecurityHub makes linked member account onboarding fast, simple and easy.

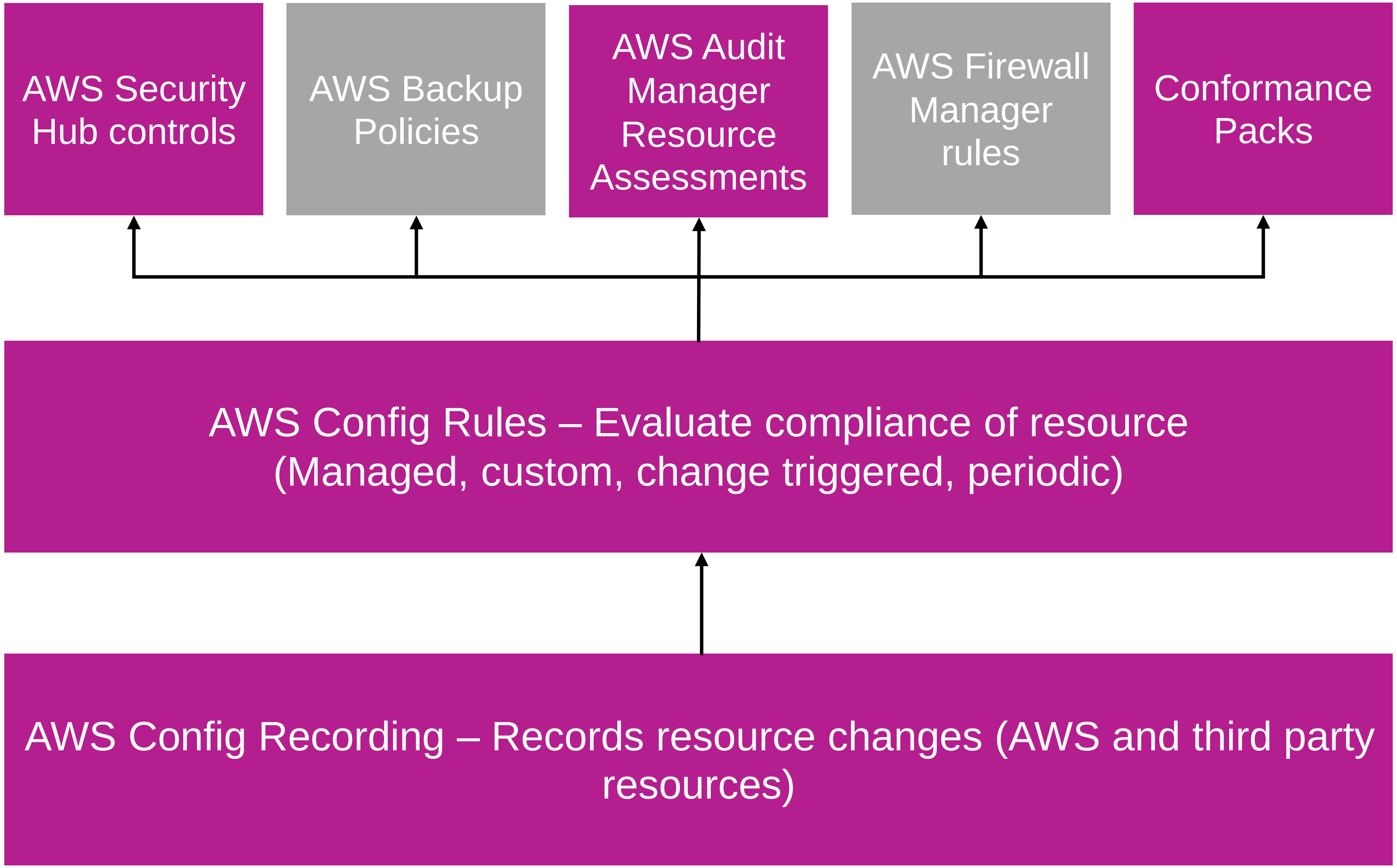
Sustainability

Reuseability
To fulfil an Organization on-going governance needs, conformance pack is a YAML listing referencing existing AWS Config managed and/or custom rules and remediation actions that can be easily customised.

Reduce Toil
AWS maintains industry security standards up to date and reduces effort to customer.

AWS Config

AWS Config



AWS Security Hub controls

AWS Backup Policies

AWS Audit Manager Resource Assessments

AWS Firewall Manager rules

Conformance Packs

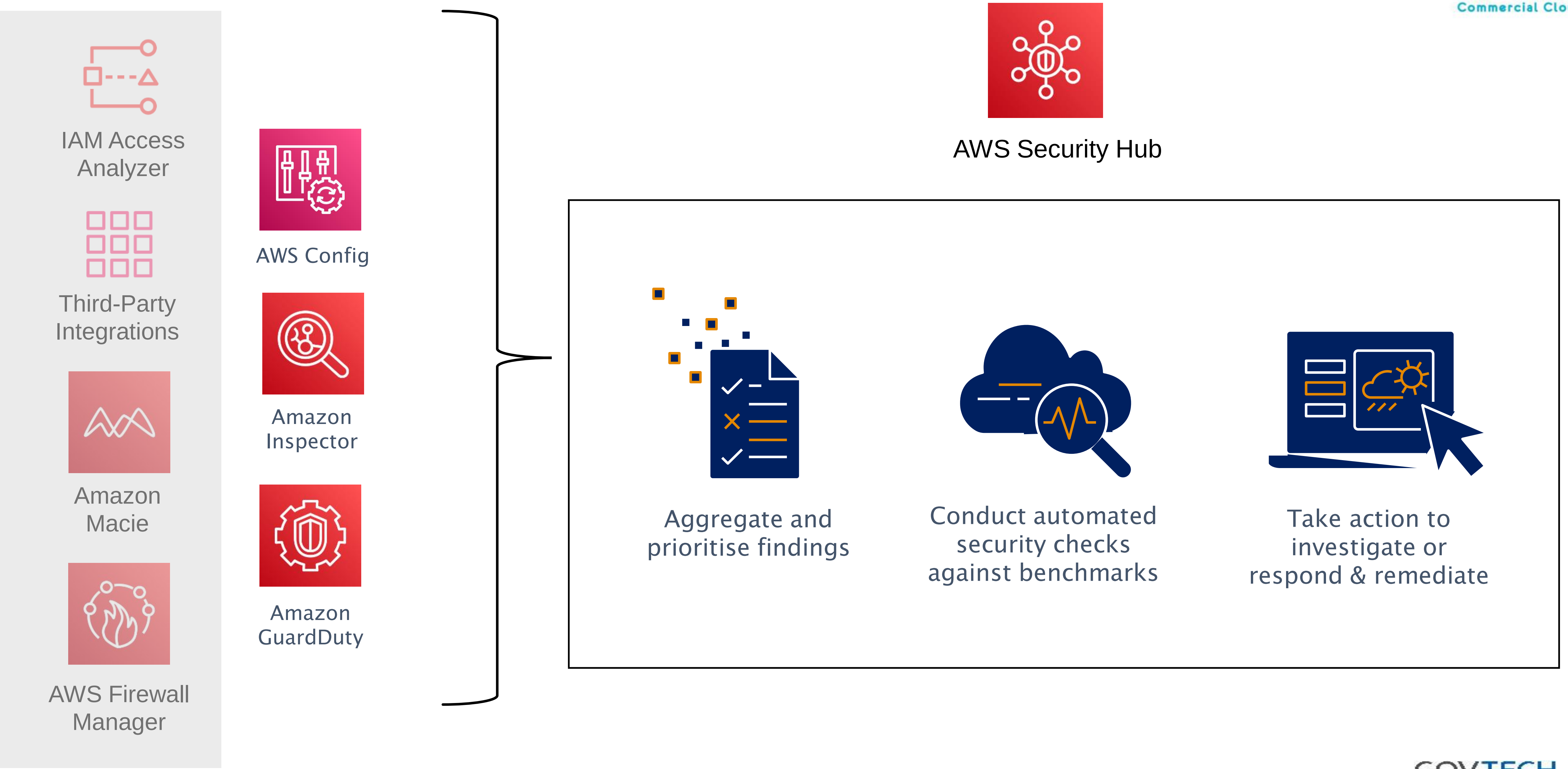
AWS Config Rules – Evaluate compliance of resource (Managed, custom, change triggered, periodic)

AWS Config Recording – Records resource changes (AWS and third party resources)

What are Conformance Packs

- Collection of managed or custom AWS Config rules as a single Amazon resource name
- Deploy across AWS Organisation from the delegated admin account
- Immutable
- Process checks rules
- Simplify reporting

AWS Security Hub



IAM Access Analyzer

Third-Party Integrations

Amazon Macie

AWS Firewall Manager

AWS Config

Amazon Inspector

Amazon GuardDuty

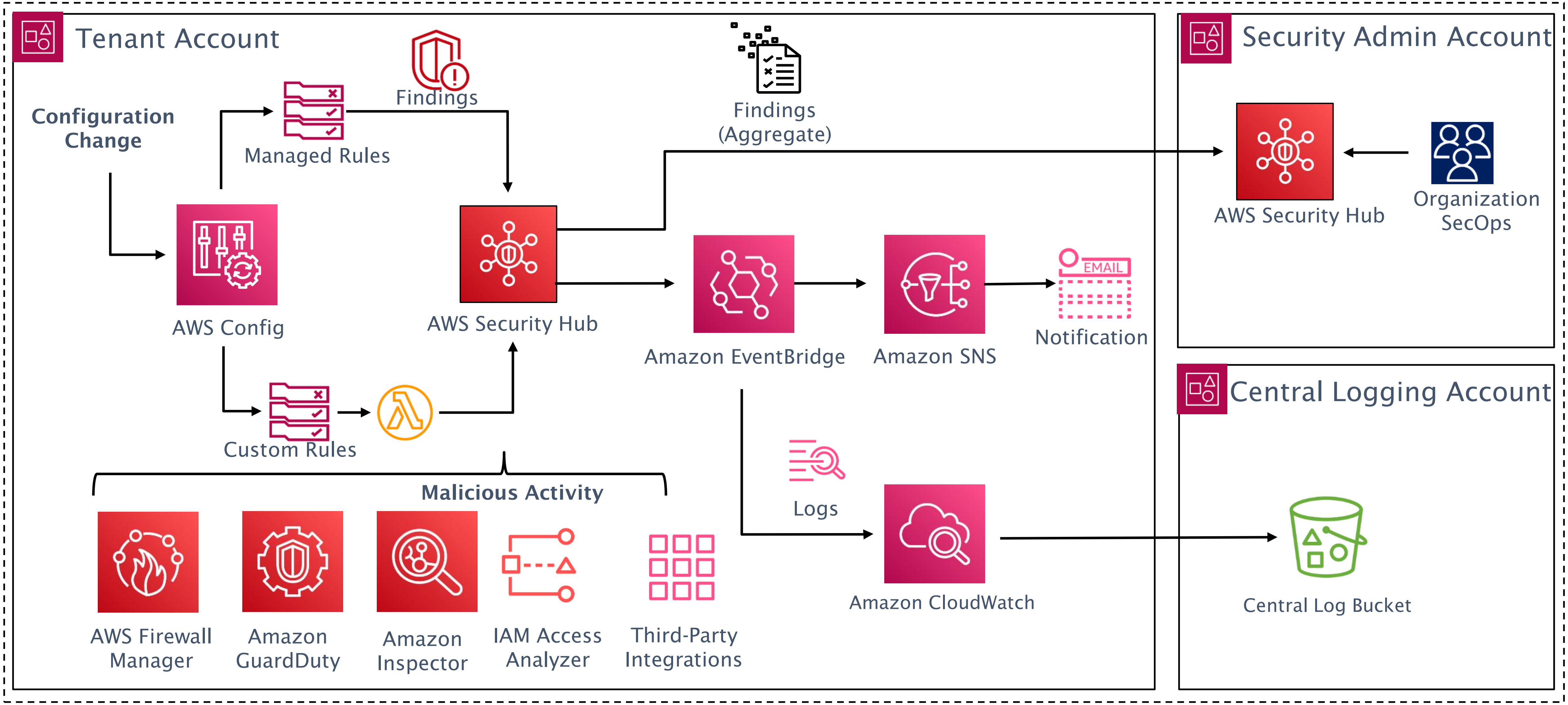
AWS Security Hub

Aggregate and prioritise findings

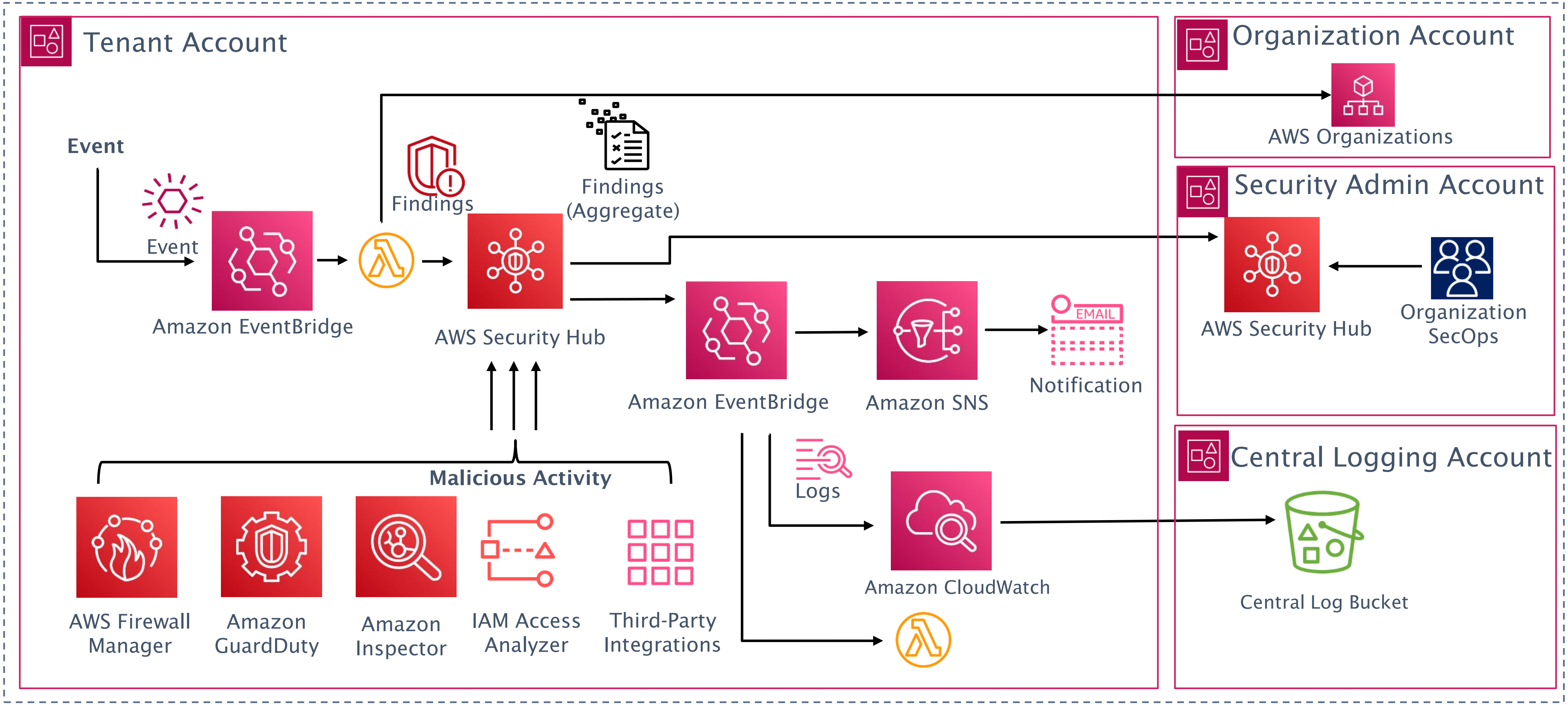
Conduct automated security checks against benchmarks

Take action to investigate or respond & remediate

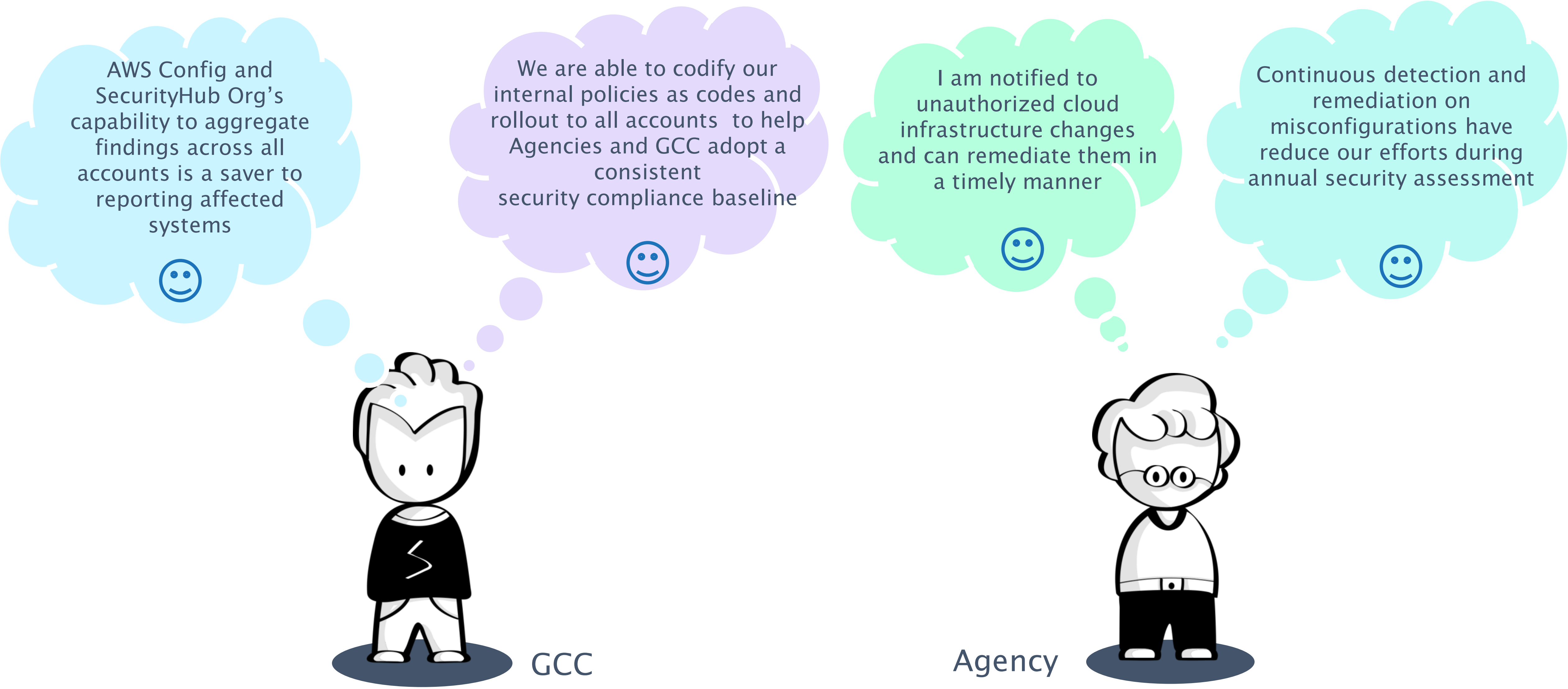
Continuous Compliance with AWS Config



Continuous Compliance with EventBridge



Benefits of Continuous Compliance



AWS Config and SecurityHub Org's capability to aggregate findings across all accounts is a saver to reporting affected systems ☺

We are able to codify our internal policies as codes and rollout to all accounts to help Agencies and GCC adopt a consistent
security compliance baseline ☺

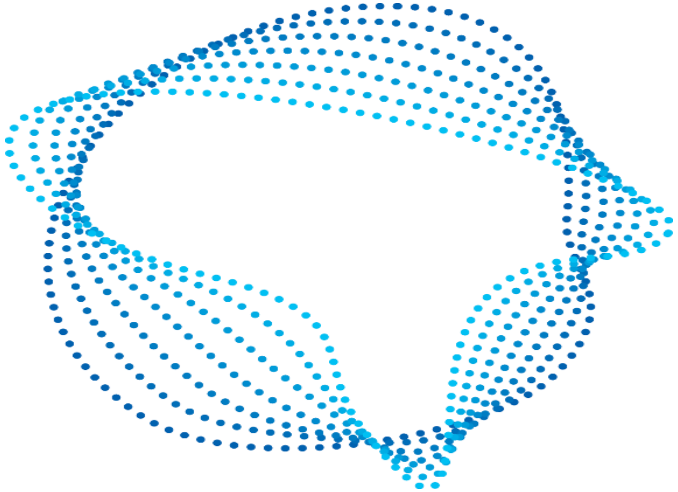
I am notified to unauthorized cloud infrastructure changes and can remediate them in a timely manner ☺

Continuous detection and remediation on misconfigurations have reduce our efforts during annual security assessment ☺

Cost of Continuous Compliance to Tenants

#	AWS Services		Average Monthly Cost (S$)
1	AWS Config	**Rule Evaluations** - 5760 rule evaluations/month **Configuration Items Recorded** - 2000 configuration items/month	$11.76
2	AWS Eventbridge	**Custom Events** - ~ 1000 custom events published	$1.35
3	AWS Lambda	**Executions** - 5760 executions per month	$0.60
4	AWS SNS	**AWS Lambda Endpoint:** - No charge for deliveries to Lambda	$0.00
5	AWS Security Hub	**Security Checks** - 1000 checks (first 100,000 checks/account/region/month): $0.0010/check	$1.00
		Total	**$14.71**

*** Ex Rate : $1USD : $1.35 SGD**



Q&A

Frequently Asked Questions (1/4)

Q1	Are the non-compliant resources automatically remediated?
A1	• No. Findings that comes from managed security standards by AWS, and custom PaC only monitors and reports resource compliance findings. • Tenant account admins shall be responsible to set up their alert notifications and remediate the reported findings accordingly.

Frequently Asked Questions (2/4)

Q2	There are too irrelevant findings reported on AWS Security Hub that are not applicable to our Agency governance policy or are accepted by Agency as exceptions. What can I do to mute such noises in the AWS Security Hub findings?
A2	• In the event of noise resulting from irrelevant controls surfacing on AWS Security Hub, user may choose to disable the control. a) From AWS Security Hub console, navigate to **“Security standards”**. b) Select the security standard that the control falls under. c) Search for the control via the control ID, and disable it.

Frequently Asked Questions (3/4)

Q3	If my Agency is already using AWS Security Hub as a central security account to manage my other AWS accounts in a parent-child relationship, what do I need to do?
A3	• Agency is required to disassociate child link members accounts from your Agency central security account to rejoin to onboard GCC Organisation central security account. • Agency which has their own CASB solution and does not wish to onboard GCC Organisation central security account are to seek exceptions from their respective Agency’s approving authority. • Agency shall raise a service request to GCC with supporting approval from Agency’s approving authority to offboard from GCC Organisation central security accounts.

Frequently Asked Questions (4/4)

Q4	What is the retention period on compliance findings on AWS Security Hub?
A4	• All findings on AWS Security Hub will be available for **<u>90 days.</u>** • For GCC 2.0, compliance findings will be continuously exported to a centralised log storage for up to **<u>12 months</u>** to be compliant with the log retention requirements.

THANK YOU

Questions and Answers

We Want to Hear Your Feedback!

https://form.gov.sg/625cb8b4ef648600142b2cd2

- Let us know what went well and how we can improve.
- We want to ensure that we are bringing the right contents to you so as to help Agencies.
- If you have any questions, please reach out to us at Ask_CODEX@tech.gov.sg