

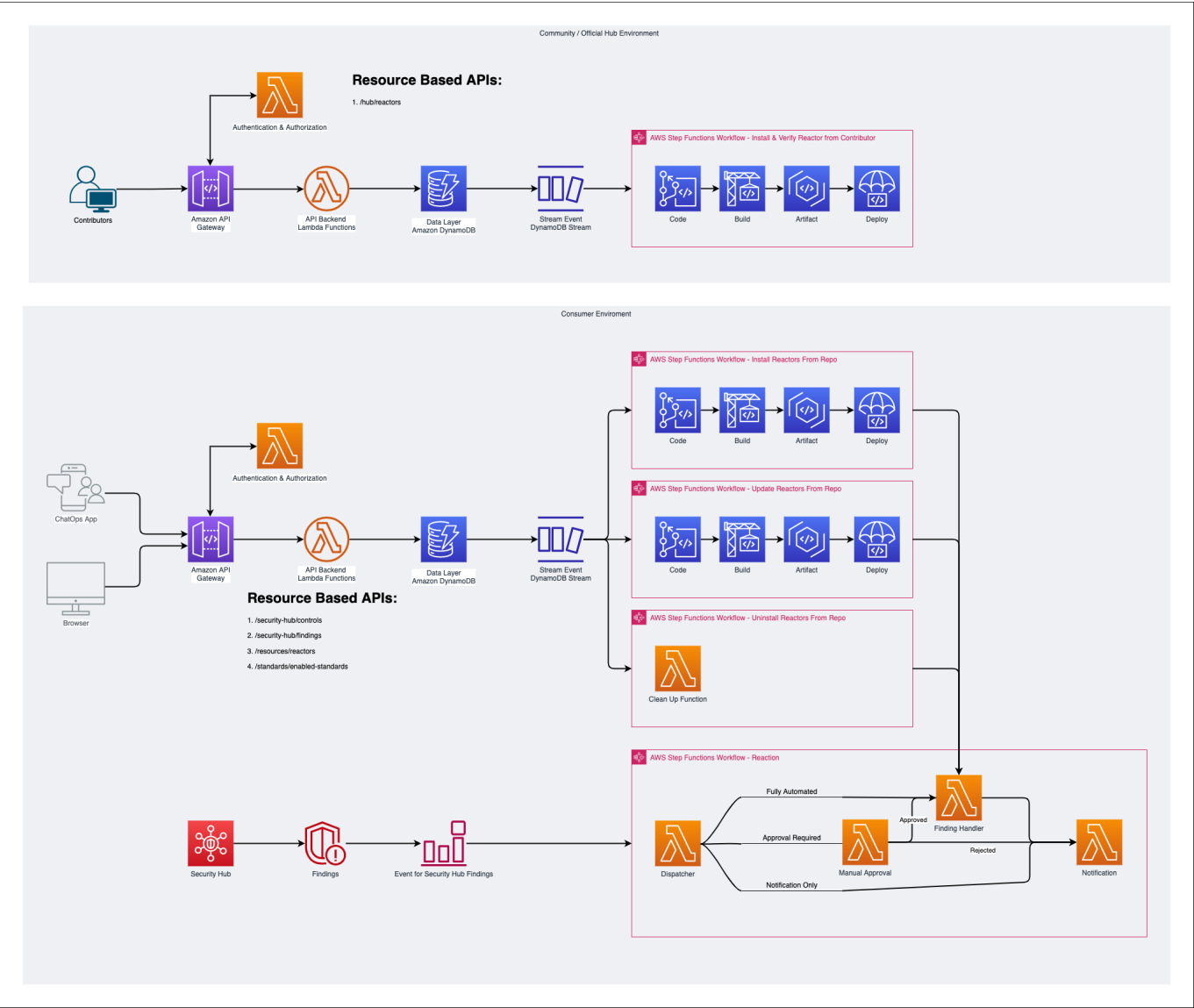
Overview / 项目概述

项目采用无服务器架构实现基于Security Hub的安全事件响应框架

Online Demo

[Ouroboros Reactor](#)

Architecture / 架构图



Components

Frontend

Ouroboros Frontend is built with VUE3 + Nuxt3 + Element-Plus and deployed with Amazon S3 Static Web Hosting.

项目前端使用了VUE3 + Nuxt3 + Element-Plus 开发, 使用AWS S3静态网站发布功能进行部署

API - Lambda Function

- **ouroboros_ims_service_security_hub**
- **ouroboros_ims_service_security_hub_controls**
- **ouroboros_ims_service_security_hub_findings**

Handle requests from API gateway, query schedule rules and logs in dynamodb and response

应用后端使用API Gateway + Lambda 开发, 负责处理来自前端的REST API请求, 查询DynamoDB中的数据并返回响应结果, 对于非只读类的接口采用API KEY 进行认证

Time-based Backend Jobs - Lambda Function

- **ouroboros_ims_collector_security_hub**

Triggered with time-based event, collect enabled standards, controls of standards in to dynamodb

由event bridge定时事件触发, 用于收集Master账号中启用的安全标准和对应的控制项

- **ouroboros_ims_collector_security_hub_findings**

Triggered with time-based event, collect findings in managed accounts to dynamodb

由event bridge定时事件触发, 用于收集所有账号中产生后集中到管理账号的findings

Database - DynamoDB (Consumer)

- **cmdb_dev_security_controls**
- **cmdb_dev_security_findings**
- **cmdb_dev_security_local_reactors**

Tables to store standards, controls, findings, reactors(installed).

DynamoDB表, 用于存储启用的标准, 控制项, 检查结果以及已经安装的安全事件响应程序

- **cmdb_dev_sfn_statemachines**

Table to store reactor execution history.

Database - DynamoDB (Hub)

- **cmdb_dev_security_controls**
- **cmdb_dev_security_reactors**

Tables to store standards, controls, reactors(repository).

DynamoDB表, 用于存储启用的标准, 控制项, 以及供Consumer安装的安全事件响应程序

Streaming Service - DynamoDB Stream (Consumer)

cmdb_dev_security_local_reactors/stream

Event stream capture both INSERT and REMOVE operations in *cmdb_dev_security_local_reactors* and trigger installation/uninstallation pipelines

使用了DynamoDB的Stream功能, 自动捕获数据库中Reactor对象的变化, 触发Reactor Lambda函数的部署或清理流水线

Streaming Service - DynamoDB Stream (Hub)

cmdb_dev_security_reactors/stream

Event stream capture both INSERT and REMOVE operations in *cmdb_dev_security_local_reactors* and trigger installation/verification pipelines

使用了DynamoDB的Stream功能, 自动捕获数据库中Reactor对象的变化, 触发Reactor Lambda函数的部署或测试流水线

Security Reactor Workflow - Step Function

- **security_hub_finding_reactor**

Definition

```
{
  "Comment": "A description of my state machine",
  "StartAt": "Parse Security Hub Finding",
  "States": {
    "Parse Security Hub Finding": {
      "Type": "Task",
      "Resource": "arn:aws:states:::lambda:invoke",
      "OutputPath": "$.Payload",
      "Parameters": {
        "Payload": {
          "findings.$": "$.detail.findings"
        },
        "FunctionName": "arn:aws:lambda:ap-southeast-1:592336536196:function:ouroboros_ims_step_parse_finding:$LATEST"
      },
      "Retry": [
        {
          "ErrorEquals": [
            "Lambda.ServiceException",
            "Lambda.AWSLambdaException",
            "Lambda.SdkClientException"
          ],
          "IntervalSeconds": 2,
          "MaxAttempts": 6,
          "BackoffRate": 2
        }
      ],
      "Next": "Process Findings"
    },
    "Process Findings": {
      "Type": "Map",
      "Iterator": {
        "StartAt": "Execute Security Hub Finding Reactor",
```

```

    "States": {
      "Execute Security Hub Finding Reactor": {
        "Type": "Task",
        "Resource": "arn:aws:states:::lambda:invoke",
        "OutputPath": "$.Payload",
        "Parameters": {
          "Payload.$": "$",
          "FunctionName": "arn:aws:lambda:ap-southeast-
1:592336536196:function:ouroboros_ims_step_dispatch_finding:$LATEST"
        },
        "Retry": [
          {
            "ErrorEquals": [
              "Lambda.ServiceException",
              "Lambda.AWSLambdaException",
              "Lambda.SdkClientException"
            ],
            "IntervalSeconds": 2,
            "MaxAttempts": 6,
            "BackoffRate": 2
          }
        ],
        "Next": "Send Notification"
      },
      "Send Notification": {
        "Type": "Task",
        "Resource": "arn:aws:states:::lambda:invoke",
        "OutputPath": "$.Payload",
        "Parameters": {
          "Payload": {
            "messages.$": "$.result.messages"
          },
          "FunctionName": "arn:aws:lambda:ap-southeast-
1:592336536196:function:ouroboros_ims_step_send_notification:$LATEST"
        },
        "Retry": [
          {
            "ErrorEquals": [
              "Lambda.ServiceException",
              "Lambda.AWSLambdaException",
              "Lambda.SdkClientException"
            ],
            "IntervalSeconds": 2,
            "MaxAttempts": 6,
            "BackoffRate": 2
          }
        ],
        "End": true
      }
    }
  },
  "End": true
}

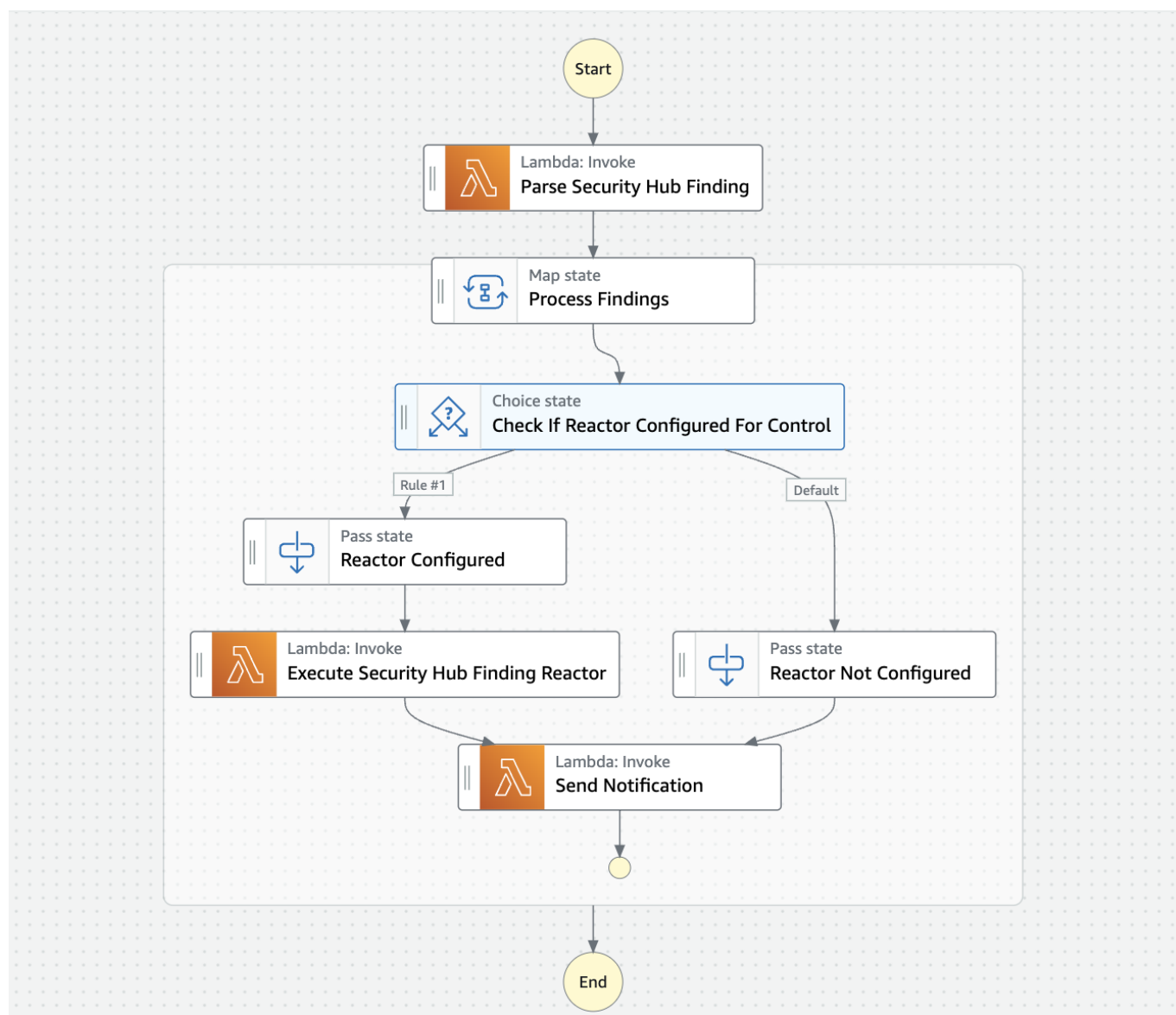
```

```

}
}

```

Diagram



Receive security hub finding-imported events from event bridge, query dynamodb for reactor configuraton and parse item into individual params for each finding, then execute corresponding reactor lambda function to fix and notify via wechat@work.

Lambda Functions

1. ouroboros_ims_step_parse_finding
2. ouroboros_ims_step_dispatch_finding
3. ouroboros_ims_step_send_notification

主要执行了以下操作:

1. 以Event bridge作为事件源, 捕获所有Findings-Imported 类型的 Security hub事件
2. 查询实践中控制类型所配置的并将事件转化为执行Reactor Lambda, 并将事件转化为执行Reactor Lambda所需要的参数

- 3. 执行Reactor Lambda并记录结果
- 4. 发送通知到企业微信

Notification Service

ouroboros_sns_topic_notification

SNS topic for integration with wechat@work REST API

用于和企业微信或其他即时通信工具的REST API进行集成, 进行事件通知

Sample Reactor

- aws-foundational-security-best-practices-v-1_0_0-S3_2-fix

Fix finding generated for S3.2 of [AWS Foundational Security Best Practices V1.0.0](#)

S3.2 - "S3 buckets should prohibit public read access"

针对AWS Foundational Security Best Practices V1.0.0中 S3.2的修复, 删除允许公网访问所有object的S3 policy statement.

Features / 功能

Security findings view with filter, sort and search

Ouroboros - Security Reactor Framework

Control PanelSecurity HubControlFindingOPAPolicyFindingRepository

Finding Id	Title	Account	Resources	Reactor
arn:aws:securityhub:ap-southeast-1:592336536196:subscription/aws-foundational-security-best-practices/v/1.0.0/S3.13/finding/e25f9c22-3082-4baa-b4e0-f0a83f875daf	S3.13 S3 buckets should have lifecycle policies configured	592336536196	AwsS3Bucket - arn:aws:s3:::ims.knowsnothing.com	not configured
arn:aws:securityhub:ap-southeast-1:592336536196:subscription/aws-foundational-security-best-practices/v/1.0.0/S3.11/finding/a4401a8a-dc37-49da-837e-8f6d7349d0fe	S3.11 S3 buckets should have event notifications enabled	592336536196	AwsS3Bucket - arn:aws:s3:::s3-finding-test	not configured
arn:aws:securityhub:ap-southeast-1:592336536196:subscription/aws-foundational-security-best-practices/v/1.0.0/S3.4/finding/73892812-4374-4849-bf71-69711fdafa64	S3.4 S3 buckets should have server-side encryption enabled	592336536196	AwsS3Bucket - arn:aws:s3:::config-bucket-592336536196	not configured
arn:aws:securityhub:ap-southeast-1:592336536196:subscription/aws-foundational-security-best-practices/v/1.0.0/S3.8/finding/45134e80-4847-4c52-a30b-7a9d156a817c	S3.8 S3 Block Public Access setting should be enabled at the bucket-level	592336536196	AwsS3Bucket - arn:aws:s3:::aws-sam-cli-managed-default-samclisourcebucket-ze4ea4ny4jlm	not configured
arn:aws:securityhub:ap-southeast-				

Security controls view with filter, sort and search

Ouroboros - Security Reactor Framework

Control Panel

Security Hub

Control

Finding

OPA

Policy

Finding

Repository

ControlId	Title	ControlStatus	SeverityRating	ReactorId	
RDS.13	RDS automatic minor version upgrades should be enabled	ENABLED	high	not configured	Configure
AutoScaling.3	Auto Scaling group launch configurations should configure EC2 instances to require Instance Metadata Service Version 2 (IMDSv2)	ENABLED	high	not configured	Configure
IAM.1	IAM policies should not allow full "*" administrative privileges	ENABLED	high	not configured	Configure
ES.2	Elasticsearch domains should be in a VPC	ENABLED	critical	not configured	Configure
EC2.2	The VPC default security group should not allow inbound and outbound traffic	ENABLED	high	not configured	Configure
ECS.5	ECS containers should be limited to read-only access to root filesystems	ENABLED	high	not configured	Configure
ElasticBeanstalk.2	Elastic Beanstalk managed platform updates should be enabled	ENABLED	high	not configured	Configure
IAM.4	IAM root user access key should not exist	ENABLED	critical	not configured	Configure

Search and install reactors from Official Hub

Ouroboros - Security Reactor Framework

Control Panel

Repository

Official

Hub

Community

Community

Local

Local

Reactor	ControlId	Description	Repo	
security-hub-reactor-s3-2	S3.2	Fix S3.2	https://github.com/mars-knowsnothing/security-hub-reactor-s3-2.git	Install

Ouroboros - Security Reactor Framework

Control Panel

Repository

Official

Hub

Community

Community

Local

Local

Reactor	ControlId	Description	Repo	
security-hub-reactor-s3-2	S3.2	Fix S3.2	https://github.com/mars-knowsnothing/security-hub-reactor-s3-2.git	Installing

Reactor Installer

Installation started

Ouroboros - Security Reactor Framework

Control Panel	Reactor	ControlId	Description	Repo	S3.2
Repository	security-hub-reactor-s3-2	S3.2	Fix S3.2	https://github.com/mars-knowsnothing/security-hub-reactor-s3-2.git	Update
Official					
Hub					
Community					
Community					
Local					
Local					

Select installed reactor for specific security control

Control Panel

Security Hub

Control

Finding

OPA

Policy

Finding

Repository

ControlId

S3.2

Title

ControlStatus

SeverityRating

ReactorId

s3.2

Configure

Configure

Reactor

not configured

security-hub-reactor-s3-2

Cancel

Confirm

Event driven automatic finding remediation for configured control

aws Services Search for services, features, blogs, docs, and more [Option+S]

Executions (725)

View details Stop execution Start execution

Search for executions Filter by status

Name	Status	Started	End Time
b286feb7-01f4-4ff2-9288-9947c565154b	Succeeded	Sep 24, 2022 09:32:51.148 AM	Sep 24, 2022 09:32:56.095 AM
1f20e3cb-1338-d935-912a-eef959c03af7_c5a9b161-ddea-bfd0-bca0-a0d7258329a9	Succeeded	Sep 24, 2022 09:16:05.498 AM	Sep 24, 2022 09:16:08.686 AM
684027a6-5a1a-c88d-ff5b-cbf370c375a8_2b247db7-0aba-a741-dc63-6f6e9ae8496b	Succeeded	Sep 24, 2022 09:15:44.783 AM	Sep 24, 2022 09:15:47.909 AM
91a3859e-9ca7-77b8-1980-01000683ab2_ff46c14b-f7f6-43fa-792c-28917e0a4480	Succeeded	Sep 24, 2022 09:15:00.710 AM	Sep 24, 2022 09:15:04.201 AM
ed3d3bf1-d593-88c3-06ed-0854ad3cd7d8_950159a3-a42d-1392-7e13-6af86f626736	Succeeded	Sep 24, 2022 09:14:56.062 AM	Sep 24, 2022 09:15:00.537 AM
c360d608-7543-d273-5f18-df8b7a92ca31_6cab2a43-993f-e489-94e8-09bd026a558b	Succeeded	Sep 24, 2022 09:14:55.644 AM	Sep 24, 2022 09:14:59.080 AM
353b796e-1359-7fb1-0a0c-53261a4cd9c1_eeeb3192-3120-68c3-7cf1-93e30f1bbc11	Succeeded	Sep 24, 2022 09:14:54.573 AM	Sep 24, 2022 09:14:57.667 AM
da069304-9457-bbfc-ab90-59734168dc86_2b4009c5-14d7-b961-f4cc-814808798d1a	Succeeded	Sep 24, 2022 09:14:54.545 AM	Sep 24, 2022 09:14:58.814 AM
7da2e360-e402-600c-ced7-980be820fdd9_e8e7216f-28da-d235-e181-836fc4f54bea	Succeeded	Sep 24, 2022 09:14:53.779 AM	Sep 24, 2022 09:14:57.977 AM
86d08bfc-a17a-dce5-25b4-63c8a9723be6_bf5bbe05-d174-4358-aeb6-e2f75af243de	Succeeded	Sep 24, 2022 09:14:53.564 AM	Sep 24, 2022 09:15:01.471 AM
ddc367a1-ba0d-b6cd-f067-8453bce1ba4_0bee15af-294e-7e1c-8f91-4d82e2602602	Succeeded	Sep 24, 2022 09:14:51.891 AM	Sep 24, 2022 09:14:55.736 AM
abfdc08e-9e46-9338-d0d7-26b9f872acd5_39a3686e-49b7-eedd-f1f3-d98ab4929142	Succeeded	Sep 24, 2022 09:14:51.888 AM	Sep 24, 2022 09:14:55.760 AM
a5ec9fbe-9963-2f57-e49d-4670f0939229_c86d12cd-44a5-c0a2-ec94-159b488155f9	Succeeded	Sep 24, 2022 09:14:51.691 AM	Sep 24, 2022 09:14:54.570 AM
6aeb8261-11c9-6e14-26b3-aa9e96c00566_13e96d94-41ab-d34c-5d11-575e88412038	Succeeded	Sep 24, 2022 09:14:51.620 AM	Sep 24, 2022 09:14:54.582 AM

Graph view

Data flow simulator

Export

Layout

Start

Parse Security Hub Finding

Process Findings
Iteration #0

Execute Security Hub Finding Reactor

Send Notification

End

In progress

Failed

Caught error

Canceled

Succeeded

Advanced view

Collapse all

Expand all

Input

```
1 {
2   "detail": {
3     "findings": [
4       {
5         "UpdatedAt": "2022-09-21T13:16:43.776Z",
6         "Region": "ap-southeast-1",
7         "RecordState": "ARCHIVED",
8         "Title": "S3.2 S3 buckets should prohibit public read access",
9         "Compliance": {
10          "Status": "FAILED"
11        },
12        "ProductFields": {
13          "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-
14            security-best-practices/v/1.0.0",
15          "RelatedAWSResources": {
16            "type": "AWS::Config::ConfigRule",
17            "StandardsSubscriptionArn": "arn:aws:securityhub:ap-southeast-
18              1:592336536196:subscription/aws-foundational-security-best-practices/v/1.0.0",
19          }
20        }
21      }
22    ]
23  }
24 }
```

Trigger finding remediation manually

Ouroboros - Security Reactor Framework

Control Panel

Security Hub

Control

Finding

OPA

Policy

Finding

Repository

Finding Id	Title	Account	Resources	Reactor
arn:aws:securityhub:ap-southeast-1:592336536196:subscription/aws-foundational-security-best-practices/v/1.0.0/S3.2/finding/68c770a4-b9cd-440f-9965-7de7db48a59c	S3.2 S3 buckets should prohibit public read access	592336536196	AwsS3Bucket - arn:aws:s3:::serverless-for-good-final	security-hub-reactor-s3-2 Remediate
arn:aws:securityhub:ap-southeast-1:592336536196:subscription/aws-foundational-security-best-practices/v/1.0.0/S3.2/finding/c8532294-d4a5-41f9-8f5c-fdf3b3bf6217	S3.2 S3 buckets should prohibit public read access	592336536196	AwsS3Bucket - arn:aws:s3:::ims.knowsnote.com	security-hub-reactor-s3-2 Processing

Fix Security Hub Finding

Remediation Started

Fix Security Hub Finding

Reactor Execution Completed

Ouroboros - Security Reactor Framework

Control Panel

Security Hub

Control

Finding

OPA

Policy

Finding

Repository

Finding Id	Title	Account	Resources	Reactor
arn:aws:securityhub:ap-southeast-1:592336536196:subscription/aws-foundational-security-best-practices/v/1.0.0/S3.2/finding/68c770a4-b9cd-440f-9965-7de7db48a59c	S3.2 S3 buckets should prohibit public read access	592336536196	AwsS3Bucket - arn:aws:s3:::serverless-for-good-final	security-hub-reactor-s3-2 Remediate
arn:aws:securityhub:ap-southeast-1:592336536196:subscription/aws-foundational-security-best-practices/v/1.0.0/S3.2/finding/c8532294-d4a5-41f9-8f5c-fdf3b3bf6217	S3.2 S3 buckets should prohibit public read access	592336536196	AwsS3Bucket - arn:aws:s3:::ims.knowsnote.com	security-hub-reactor-s3-2 Remediate

Fix Security Hub Finding

Remediation Completed

Manage installed reactors

Ouroboros - Security Reactor Framework

Control Panel

Repository

Official

Hub

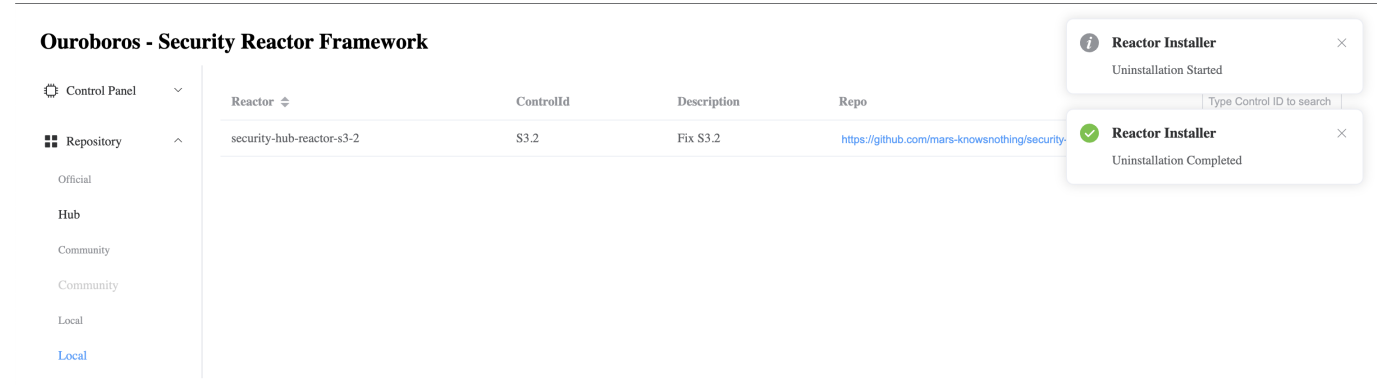
Community

Community

Local

Local

Reactor	ControlId	Description	Repo	
security-hub-reactor-s3-2	S3.2	Fix S3.2	https://github.com/mars-knowsnote/security-hub-reactor-s3-2.git	Uninstall



Cross account remediation support

- Support reactor with sufficient permission can remediate findings in remote accounts via STS.

Business Value

Designed for Enterprise Customers

- Designed for multi-tenant architecture and large-scale cloud infrasture management.
- 为多租户场景和大规模云上基础设施管理而设计，适合企业级用户
- Help enterprise customer to build up continuous security & compliance system in a cost-efficient way.
- 在当前数据安全越来越受重视，规范和监管越来越严格的挑战下，帮助企业用户构建自己的自动化持续安全合规体系

Designed for DevSecOps

- It's a proactive approach to cybersecurity where secure practices are embedded into the entire lifecycle of software development.
- 面向DevSecOps设计，可以方便地通过API与已客户已有的DevOps工具链集成，实现将安全合规内嵌入整个IT生命周期

Designed for builders and leverage the power of builders

- "Builders are people who like to invent, who look at different customer experiences and try to figure out how to reinvent them. We're all builders because companywide, we're all working together to help our customers grow and thrive."
- 面向广大Builders设计，拥抱开源社区文化，共同构建强壮的解决方案