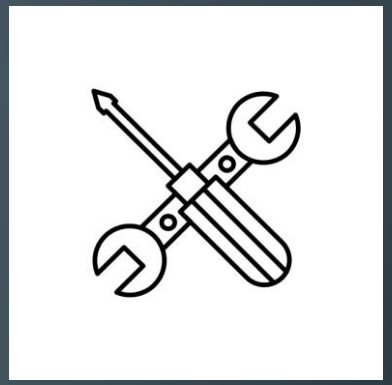
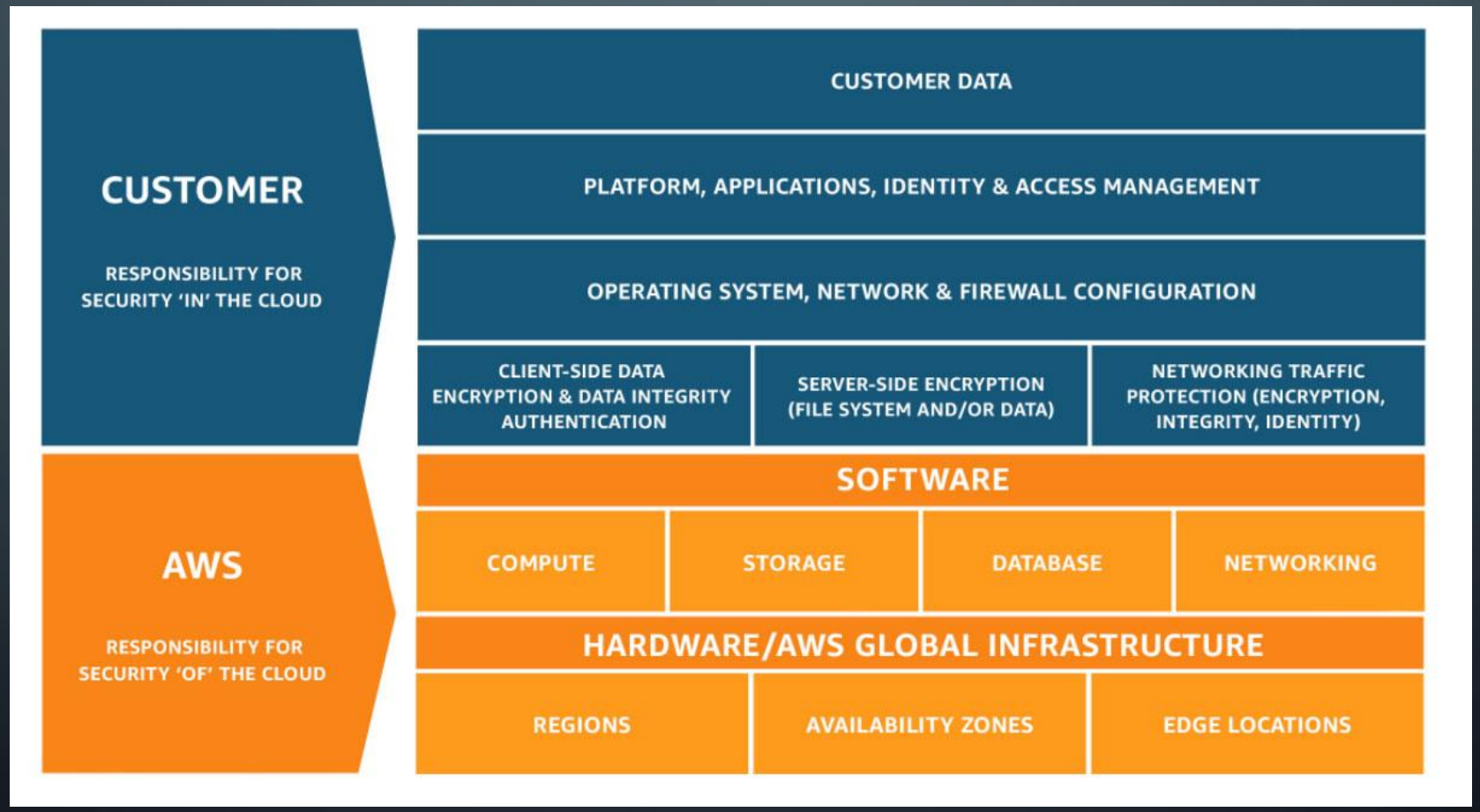
AUTOMATED REMEDIATION METHODS

WHAT IS REMEDIATION?



- Remediation is the process of mitigating a vulnerability or threat.
- Remediation can happen WITHOUT an incident, but incident response requires remediation.
- Incident remediation is the final stages of an incident response process

SHARED RESPONSIBILITY MODEL



WHEN TO RESPOND OR REMEDIATE?

- When a deviation from the baseline occurs, such as by a misconfiguration or changing external factors, you will need to respond and investigate.
- Also need to prepare, educate and train cloud teams before security issues occur.

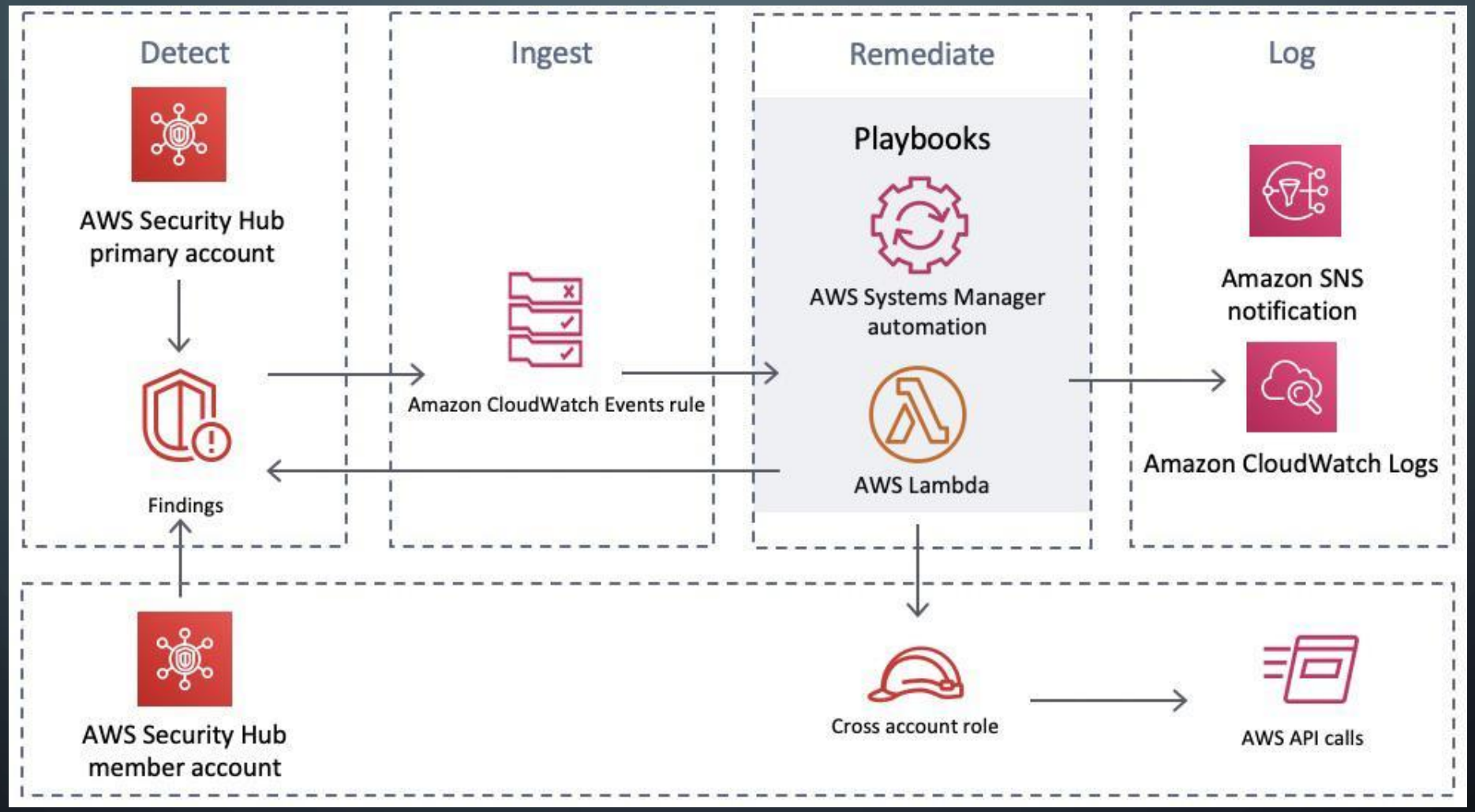
STEPS TO PREPARE FOR INCIDENT RESPONSE

- **Prepare** for incident response with response plans to make your incidents less reactive
- **Automate** response to work on your behalf while your resolvers get involved
- **Detect** and evaluate your security compliance posture with AWS Config conformance packs or Security tooling
- **Learn** from each finding and incident to improve your preparation
- **Identify** remediation methods that use automation to improve response speed and consistency
- Iterate and update playbooks and runbooks regularly
- Simulate security events in environment – game days

KEY BENEFITS OF REMEDIATION WITH AUTOMATION

Benefit	Description
Efficiency	Quickly, consistently apply security controls across an environment.
Accuracy	Less prone to human error, created with code instead of knowledge.
Scalability	Scales up with infrastructure without needing to hire anyone extra.
Response time	Automation can help you quickly detect and respond to security threats and incidents, minimizing impact of potential breaches.
Consistent Compliance	Reliably audit Infrastructure as Code for compliance and use integrations to achieve compliance easily.
External integrations	AWS allows you to integrate more sophisticated, external CSPM (Cloud Security Posture Management) frameworks like Paladin Cloud.

REMEDIATION AUTOMATION USING AWS TOOLING



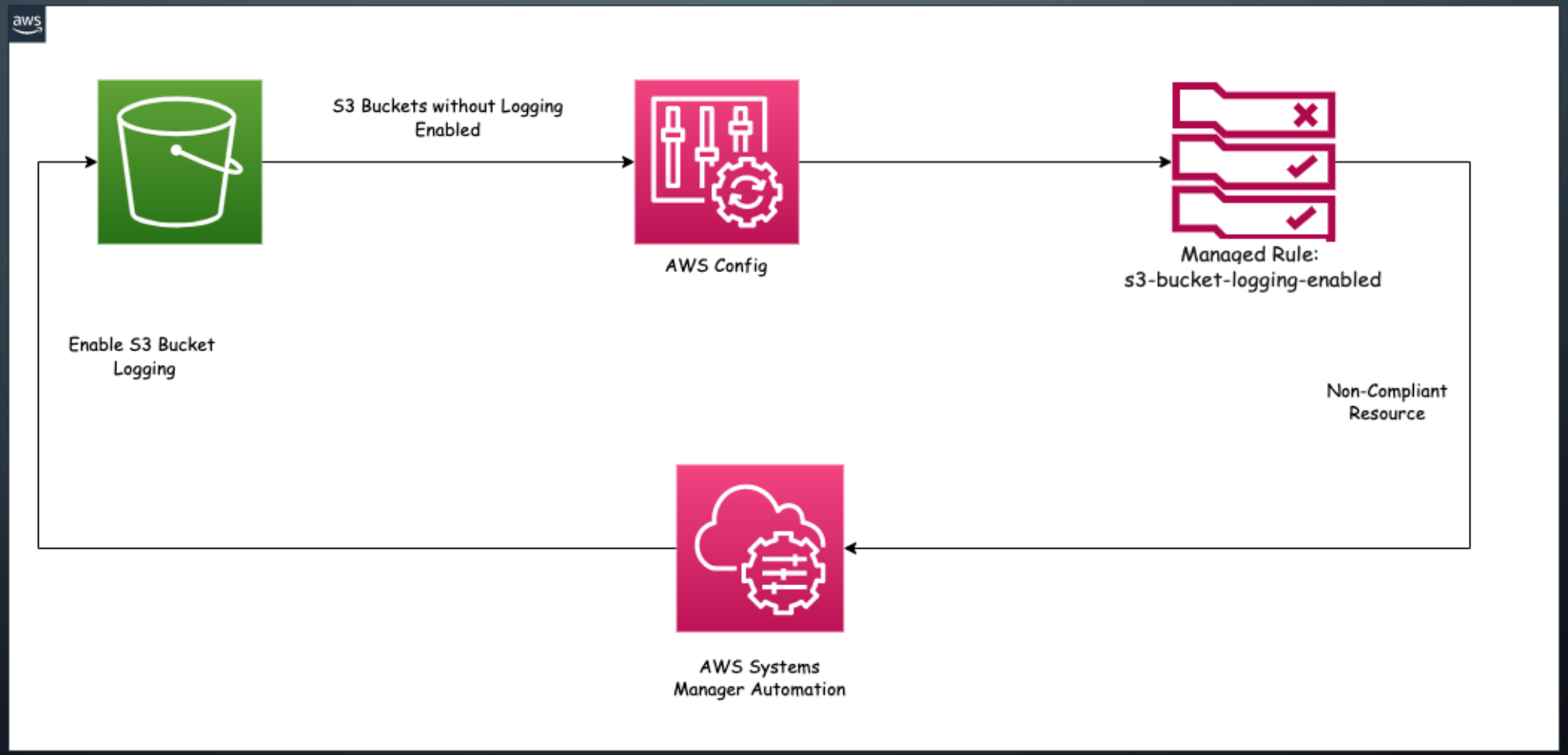
Example architecture

COMMON REMEDIATION AUTOMATION TECHNIQUES

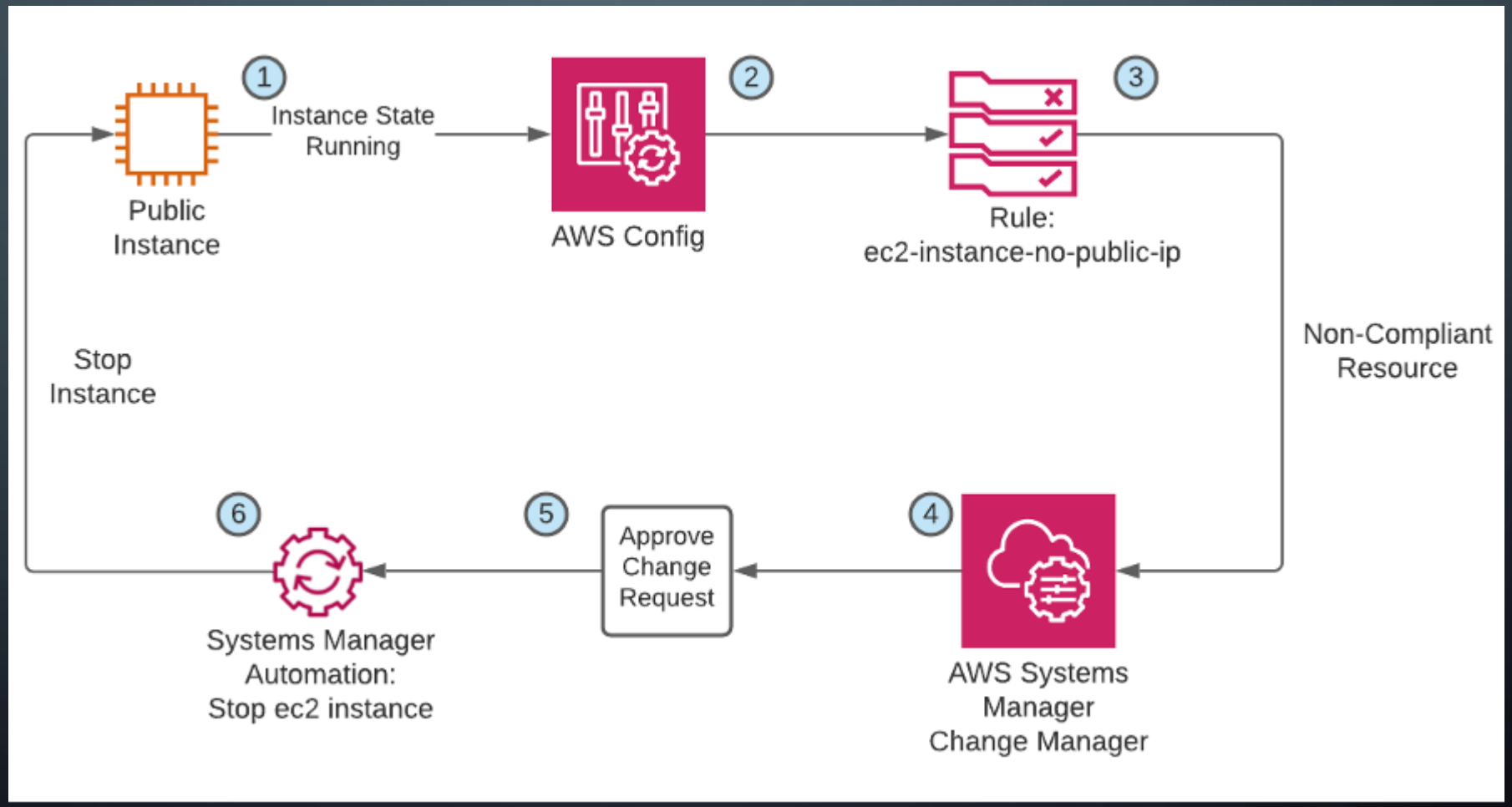
AWS CONFIG + AWS SYSTEMS MANAGER

- **AWS Config rules** can be used in conjunction with **AWS Systems Manager** to effectively **remediate noncompliant resources**.
- Use AWS Systems Manager Explorer to gather the compliance status of AWS Config rules in your AWS accounts across AWS Regions
- Use Systems Manager **Automation documents** (runbooks) to resolve your noncompliant AWS Config rules.

REMEDIATE NON-COMPLIANT S3 CONFIG RULE



REMEDIATE NON-COMPLIANT EC2 CONFIG RULE



AWS Config > Rules > ec2-instance-managed-by-systems-manager

ec2-instance-managed-by-systems-manager

Actions

Rule details

Edit

Description

Checks whether the Amazon EC2 instances in your account are managed by AWS Systems Manager.

Config rule ARN

arn:aws:config:us-east-1:[redacted]:config-rule/config-rule-xc3lxu

Trigger type

- Oversized configuration changes
- Configuration changes

Scope of changes

Resources

Resource types

- EC2 Instance
- SSM ManagedInstanceInventory

Last successful evaluation

January 15, 2021 2:20 PM

Resources in scope

View details | Remediate

Noncompliant

1

	ID	Type	Status	Annotation	Compliance
○	i-[redacted]	EC2 Instance	-	-	Noncompliant

Edit: Remediation action

Select remediation method

- ○ **Automatic remediation**
  The remediation action gets triggered automatically when the resources in scope become noncompliant.
- ◉ **Manual remediation**
  You have to manually choose to remediate the noncompliant resources.

Remediation action details

The execution of remediation actions is achieved using AWS Systems Manager Automation

Choose remediation action

AWS-AttachIAMToInstance

Attach IAM to Instance

Resources in scope

View details | Remediate

Noncompliant

ID	Type	Status	Annotation	Compliance
i-	EC2 Instance	-	-	Noncompliant

aws | Services | N. Virginia | Support

AWS Systems Manager

- Quick Setup
- Operations Management
  - Explorer New
  - OpsCenter
  - CloudWatch Dashboard
  - PHD
- Application Management
  - Resource Groups
  - AppConfig New
  - Parameter Store
- Actions & Change
  - Automation
  - Change Calendar New
  - Maintenance Windows
- Instances & Nodes
  - Compliance
  - Inventory
  - Managed Instances
  - Hybrid Activations
  - Session Manager
  - Run Command
  - State Manager

AWS Systems Manager > Automation

Executions | Preferences

Automation executions

View details | Cancel execution | Actions | Execute automation

Show child automations

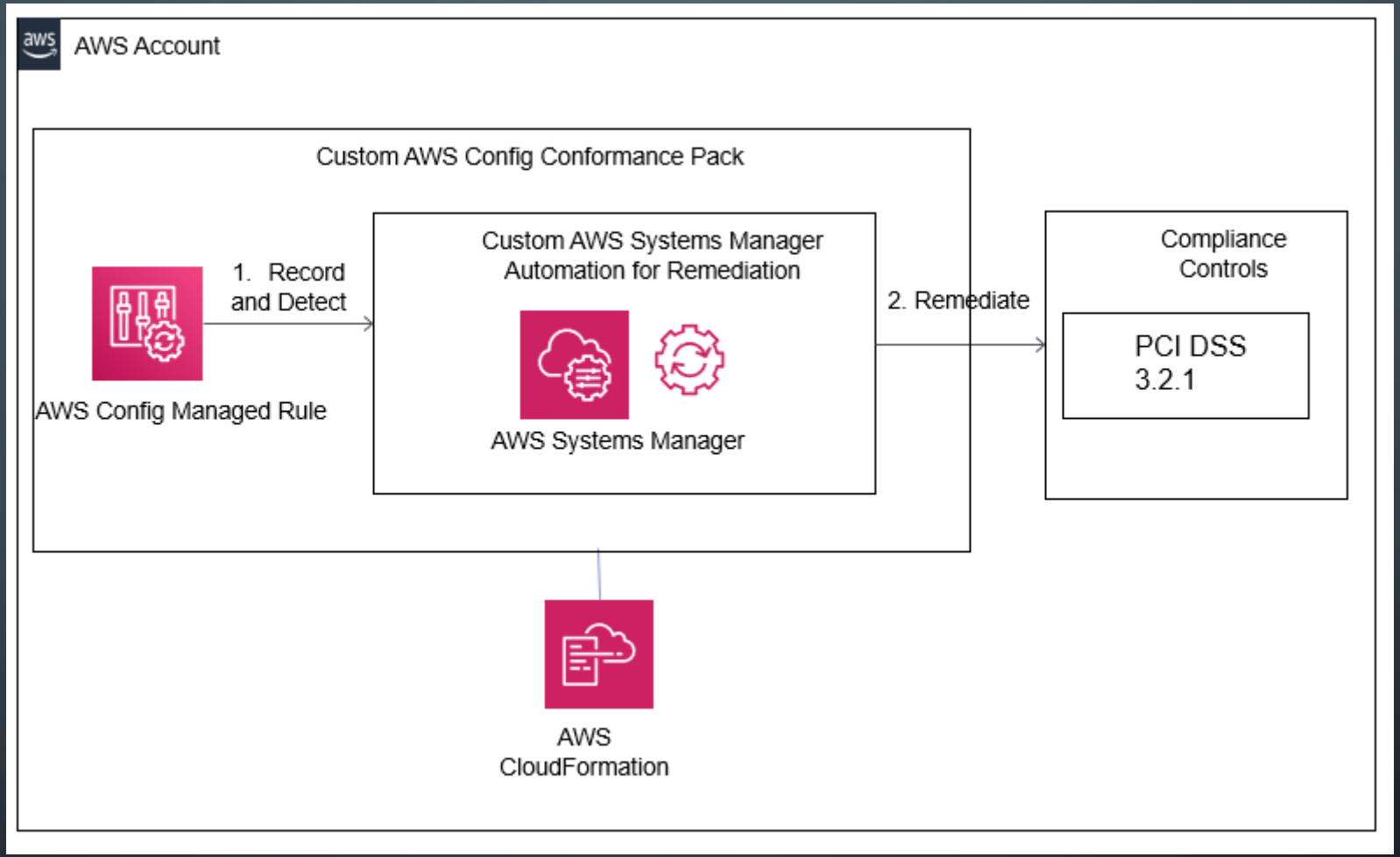
Execution ID	Document name	Status	Start time	End time	Executed by
d25ebdea-7fda-4705-8e79-b2897a263169	AWS-AttachIAMToInstance	Success	Thu, 26 Nov 2020 14:38:59 GMT	Thu, 26 Nov 2020 14:39:02 GMT	

Feedback | English (US)

Privacy Policy | Terms of Use

CONFORMANCE PACK + AWS SYSTEMS MANAGER

- A **conformance pack** is a **collection of AWS Config rules and remediation actions** that can be deployed as a single entity in an account and Region, or across an organization in AWS Organizations.
- Conformance packs are created by authoring a **YAML** template that contains the list of **AWS Config managed or custom rules and remediation actions.**
- Use the **Conformance Pack Dashboard** to understand the level of compliance of your conformance packs and use the **compliance score to track remediation progress**



A custom Config Conformance pack with Managed config rule and custom SSM remediation runbook

aws Services ▼ N. Virginia ▼ Support ▼

AWS Config

- Dashboard
- Conformance packs
- Rules
- Resources
- Aggregators
  - Rules
  - Resources
  - Authorizations
- Advanced queries
- Settings

- What's new
- Documentation
- Partners
- FAQs

AWS Config > Conformance packs

Conformance packs

A conformance pack is a collection of AWS Config rules and remediation actions that can be deployed and monitored as a single entity in your AWS account. Learn more

Conformance packs

Actions ▼ | Deploy conformance pack

Filter rules by name or compliance status

1

Name	Deployment	Compliance

You have no conformance packs deployed in your account.

Deploy a new conformance pack using sample conformance pack templates or using your own template.

Deploy conformance pack

aws Services ▼ N. Virginia ▼ Support ▼

AWS Config > Conformance packs > Deploy conformance pack

Step 1
Specify template

Step 2
Specify conformance pack details

Step 3
Review and deploy

Specify conformance pack details

Conformance pack details

Region
US East (N. Virginia)

Conformance pack name
Give the deployment of this template a name.

s3conformancepackwithremediation

Conformance pack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-) but cannot include spaces.

Parameters - optional

Parameters are defined in your template and allow you to input custom values when you create or update a conformance pack.

Key	Value	
S3TargetBucketNameForEnableLogging		Remove

Add parameter

Cancel Previous Next

Feedback English (US) ▼

Privacy Policy Terms of Use

aws Services ▼ N. Virginia ▼ Support ▼

AWS Config

- Dashboard
- Conformance packs
- Rules
- Resources
- Aggregators
  - Rules
  - Resources
  - Authorizations
- Advanced queries
- Settings

- What's new
- Documentation
- Partners
- FAQs
- Pricing

AWS Config > Conformance packs > s3conformancepackwithremediation

s3conformancepackwithremediation

Deployment:
Completed

Rules | Settings

Rules (6)

Filter rules by name or compliance status

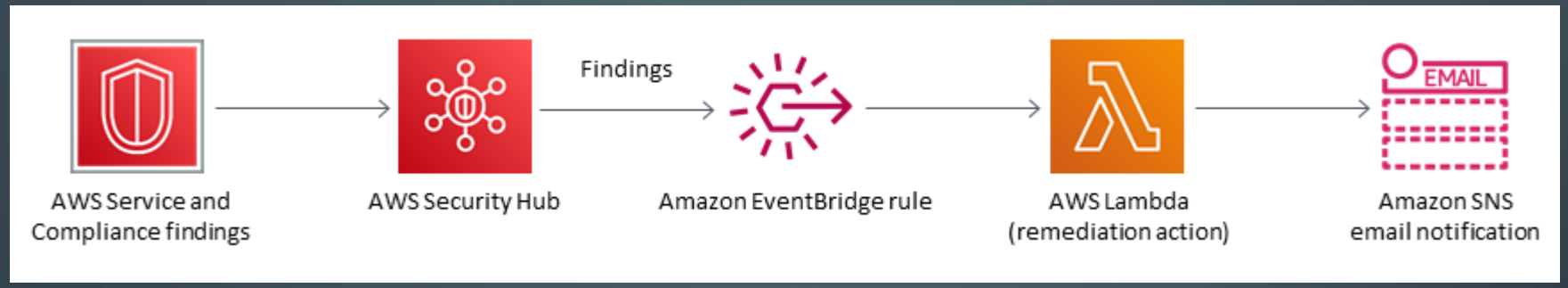
1

Name	Remediation action	Compliance
S3BucketPublicWriteProhibited-conformance-pack-tlhqzzk4p	AWS-DisableS3BucketPublicReadWrite	Compliant
S3BucketReplicationEnabled-conformance-pack-tlhqzzk4p	Not set	Noncompliant
S3BucketLoggingEnabled-conformance-pack-tlhqzzk4p	AWS-ConfigureS3BucketLogging	Noncompliant
S3BucketPublicReadProhibited-conformance-pack-tlhqzzk4p	AWS-DisableS3BucketPublicReadWrite	Compliant
S3BucketSSLRequestsOnly-conformance-pack-tlhqzzk4p	Not set	Noncompliant
S3BucketServerSideEncryptionEnabled-conformance-pack-tlhqzzk4p	AWS-EnableS3BucketEncryption	Noncompliant

Feedback English (US) ▼

Privacy Policy Terms of Use

AUTOMATE REMEDIATION FOR AWS SECURITY HUB FINDINGS - CUSTOM ACTIONS



- AWS Security Hub sends all findings to Amazon EventBridge by default.
- This pattern provides a security control that deploys an EventBridge rule to identify AWS Foundational Security Best Practices standard findings.

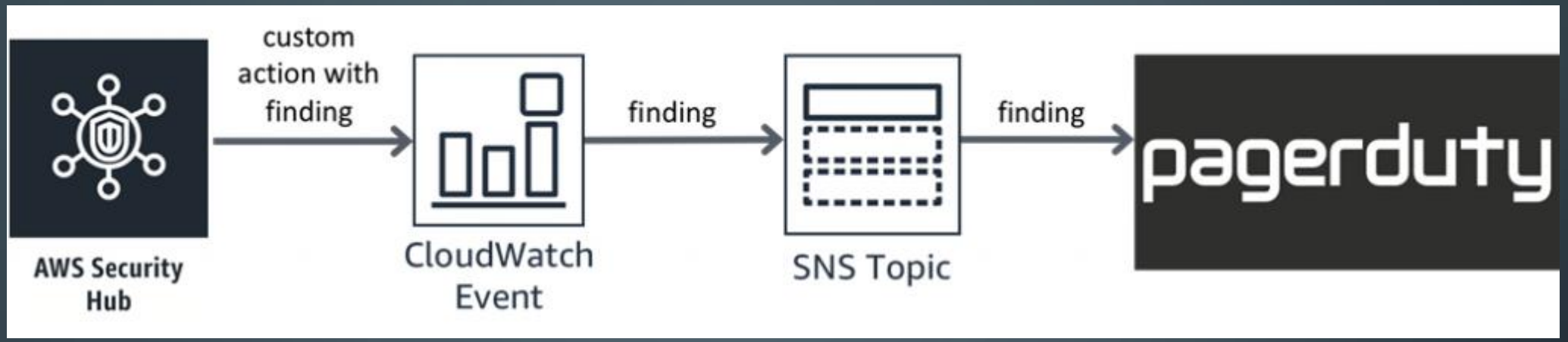
- The rule identifies the findings for automatic scaling, virtual private clouds (VPCs), Amazon Elastic Block Store (Amazon EBS), and Amazon Relational Database Service (Amazon RDS) from the AWS Foundational Security Best Practices standard.

- The EventBridge rule forwards these findings to an AWS Lambda function, which remediates the finding.

- The Lambda function then sends a notification with remediation information to an Amazon Simple Notification Service (Amazon SNS) topic.

Example Figure Data flow supporting remediation of Security Hub findings using custom actions

- Security Hub will send CIS check finding to CloudWatch Events
- CloudWatch Events will send the findings to a Lambda function
- The Lambda function will identify the affected CloudTrail trail and configure it with CloudWatch Logs to monitor the trail logs.
- You need necessary AWS IAM permissions to work with Security Hub, CloudWatch Events, Lambda and AWS CloudTrail.



Security Hub custom action integration with PagerDuty an Advanced Technology Partner.

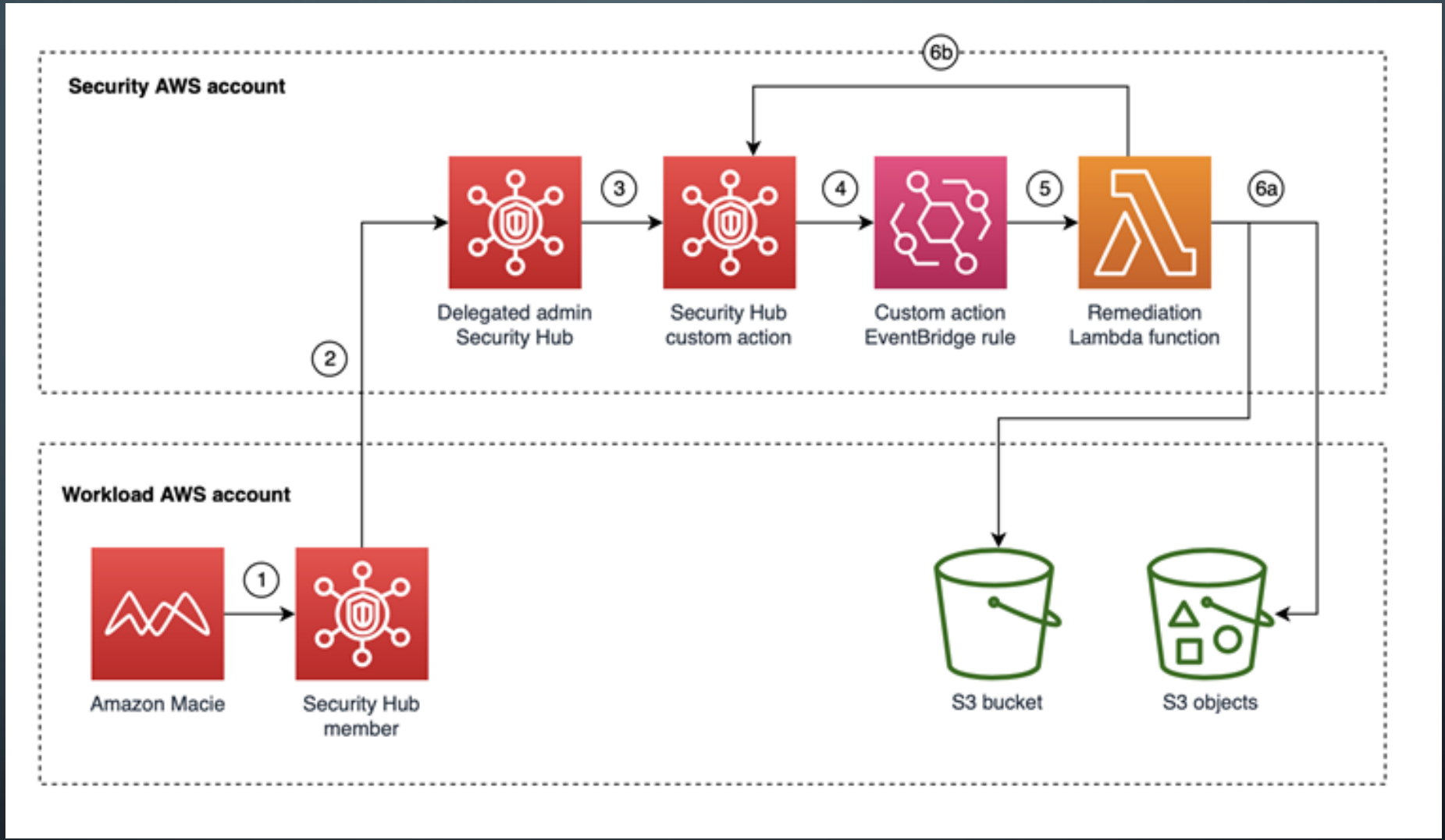
- This integration allows you to send Security Hub findings to PagerDuty
- PagerDuty platform manages, organizes, and responds to Security Hub events

AMAZON MACIE FINDING REMEDIATION

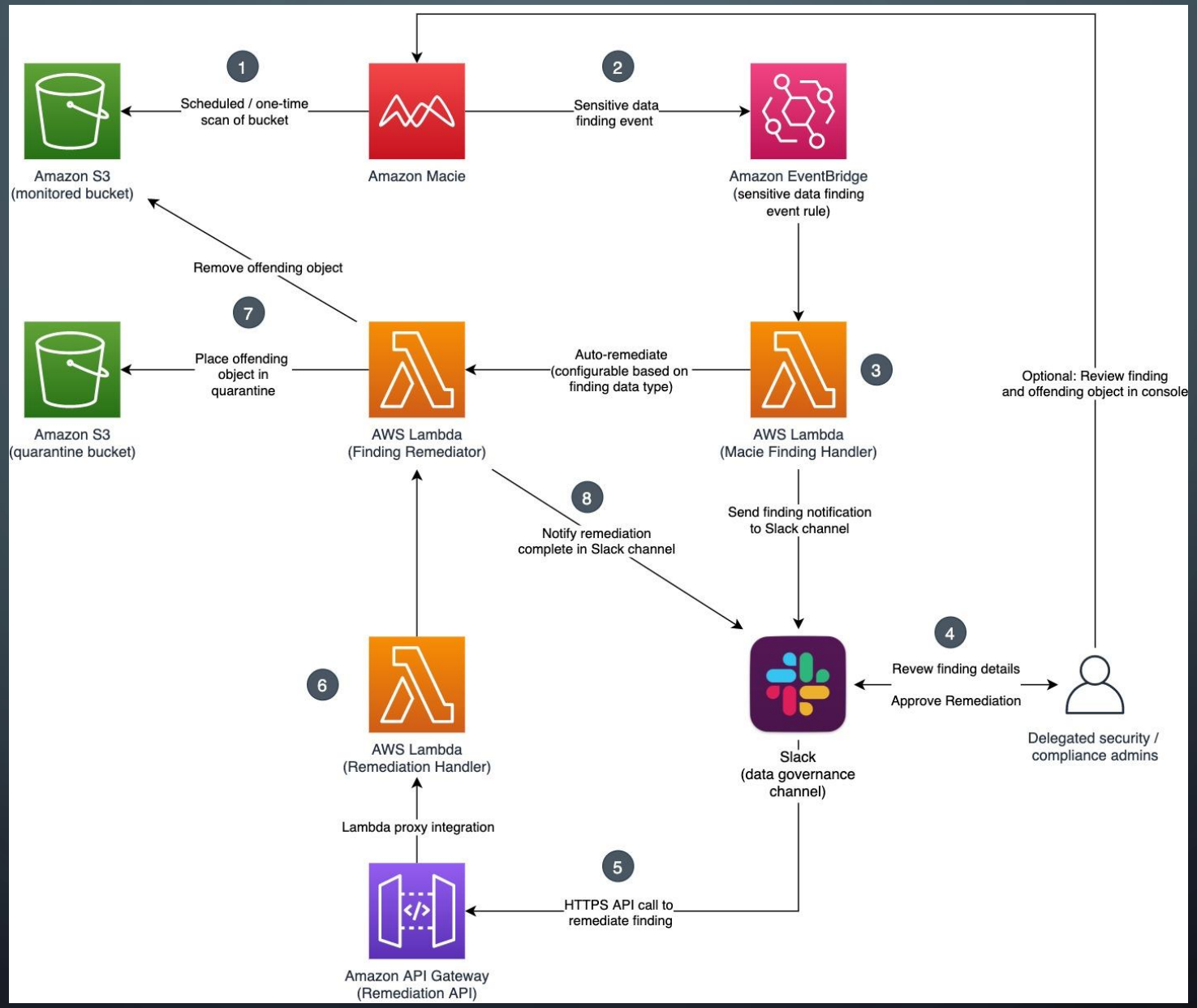
- Macie findings flow to AWS Security Hub for review and analysis.
- Macie also integrates with Amazon Event Bridge to facilitate automated responses to findings such as alerts, feeds to security information and event management (SIEM) systems, and automated remediation.
- After you conduct your Macie scans either manually or with automation, you can implement semi- or fully automated response and remediation actions based on the sensitive data findings.

The following are **examples** of automated response and remediation actions that you can take:

- You can deploy the solution to automatically send notifications to Slack if sensitive data is found for buckets with specific sensitivity scores.
- You can use AWS Security Hub custom actions to develop pre-determined response and remediation actions on Macie sensitive data findings.

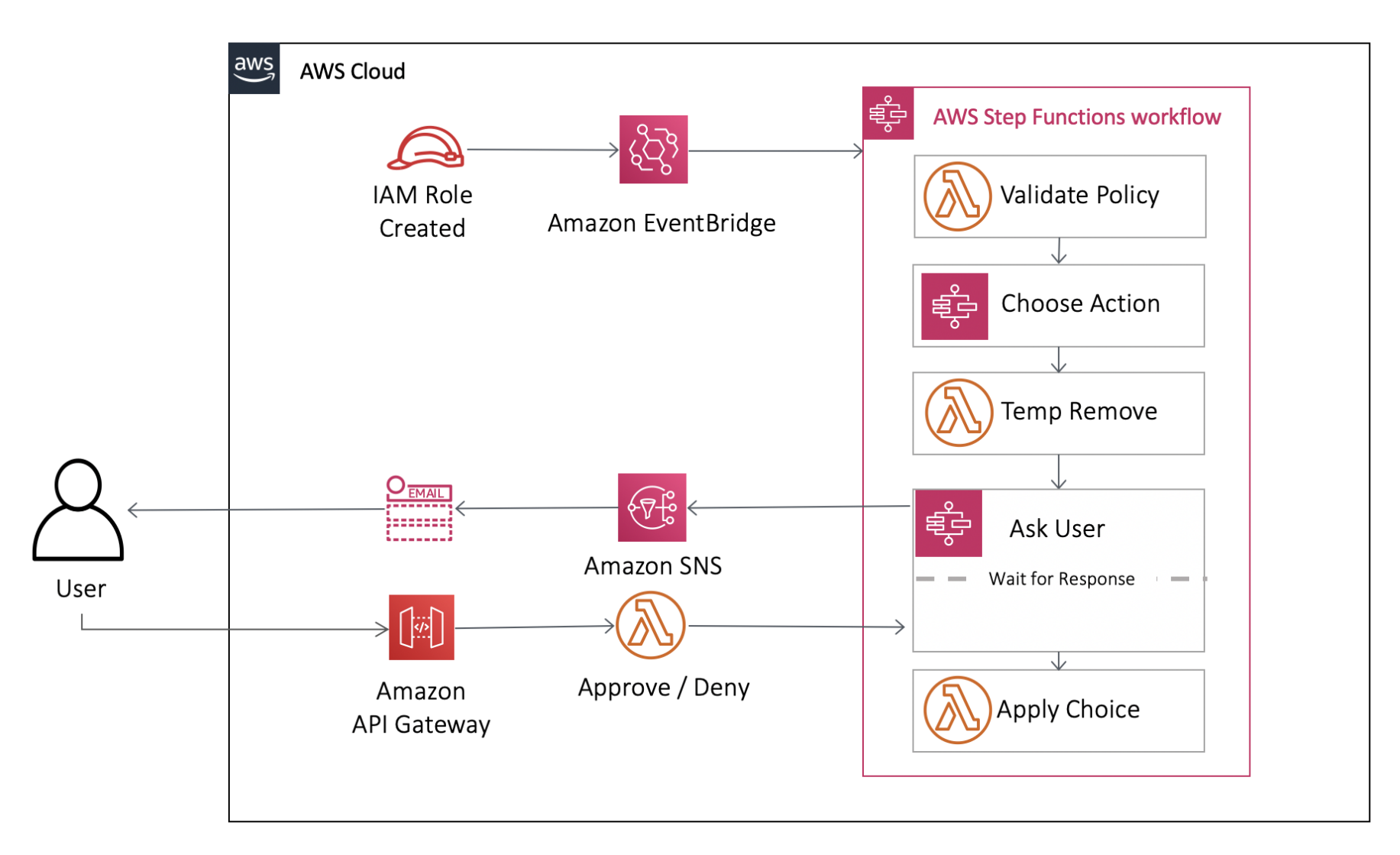


Resources deployed in the Security AWS account taking action on resources identified in the Workload AWS account

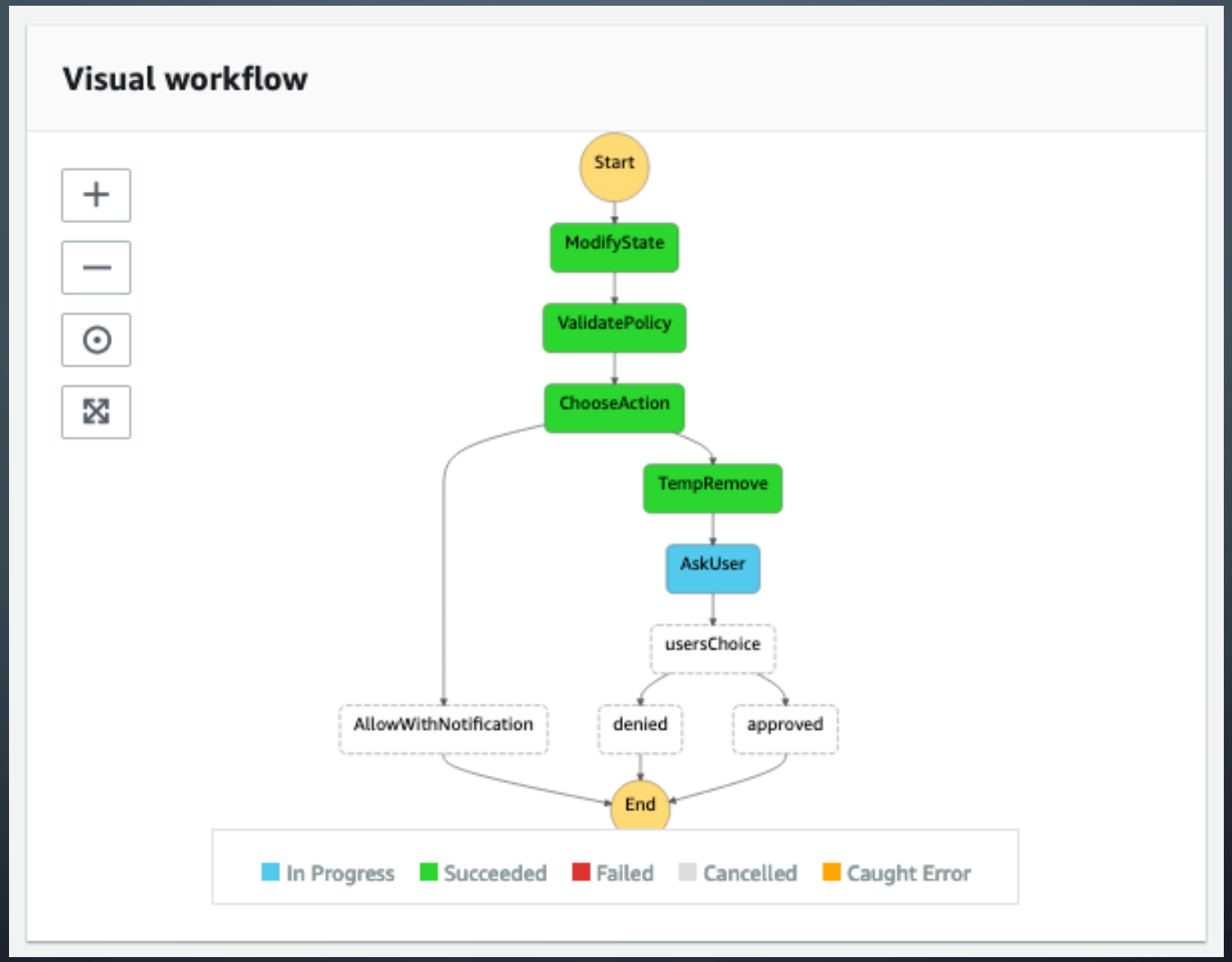

1
Scheduled / one-time scan of bucket
Amazon S3 (monitored bucket)
Amazon Macie
2
Sensitive data finding event
Amazon EventBridge (sensitive data finding event rule)
Remove offending object
7
Place offending object in quarantine
Amazon S3 (quarantine bucket)
AWS Lambda (Finding Remediator)
Auto-remediate (configurable based on finding data type)
AWS Lambda (Macie Finding Handler)
3
Optional: Review finding and offending object in console
8
Notify remediation complete in Slack channel
Send finding notification to Slack channel
4
Revew finding details
Approve Remediation
Delegated security / compliance admins
6
AWS Lambda (Remediation Handler)
Slack (data governance channel)
Lambda proxy integration
5
HTTPS API call to remediate finding
Amazon API Gateway (Remediation API)

ORCHESTRATING A SECURITY INCIDENT RESPONSE WITH AWS STEP FUNCTIONS

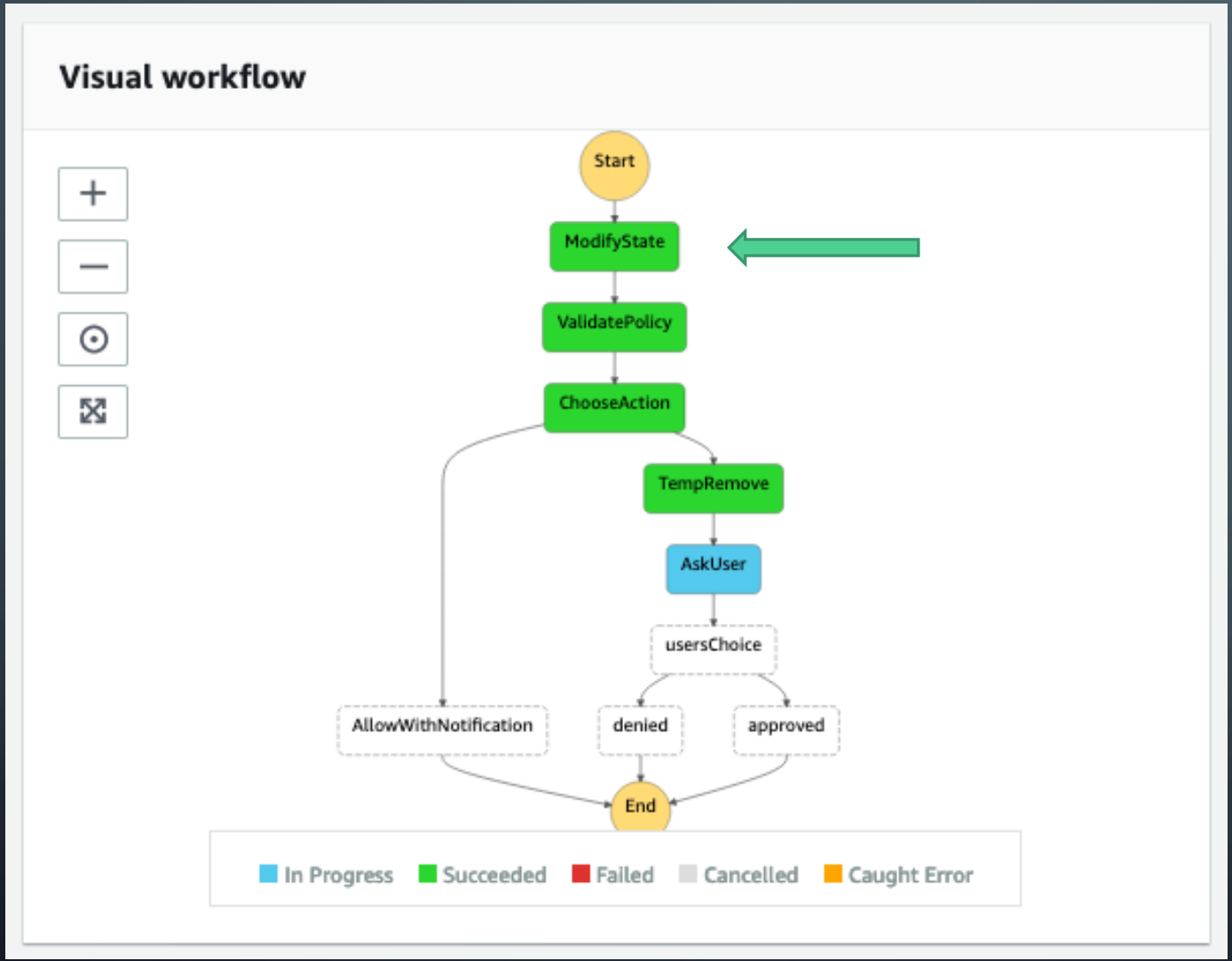
- Implement the callback pattern of an AWS Step Functions Standard Workflow.
- Use a manual approval step into an automated security incident response framework.
- The framework could be extended to remediate automatically. For example, applying alternative actions, or restricting actions to specific ARNs.



Orchestrating a security incident response with AWS Step Functions



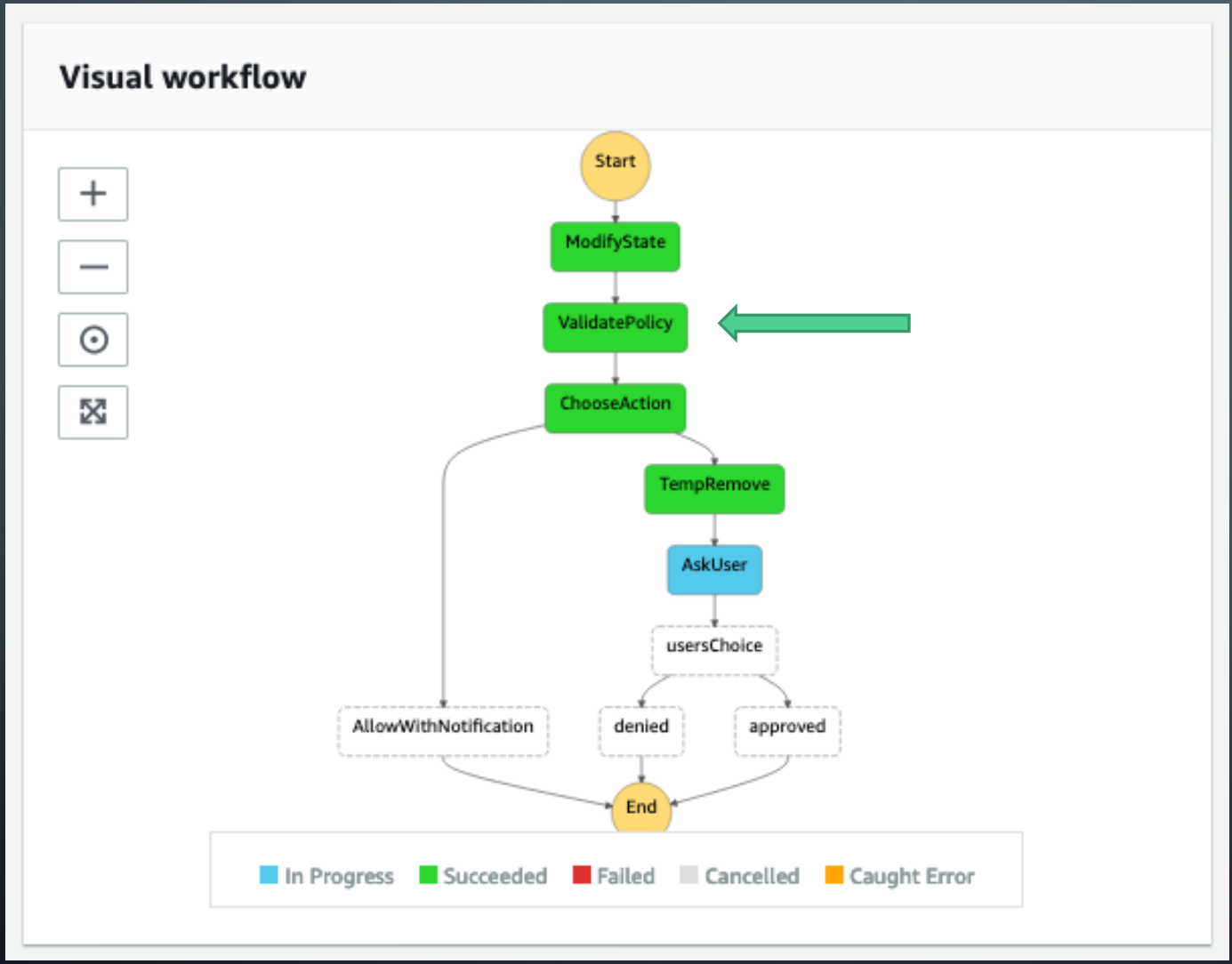
Visual representation of the workflow



ModifyData

State Type: Pass

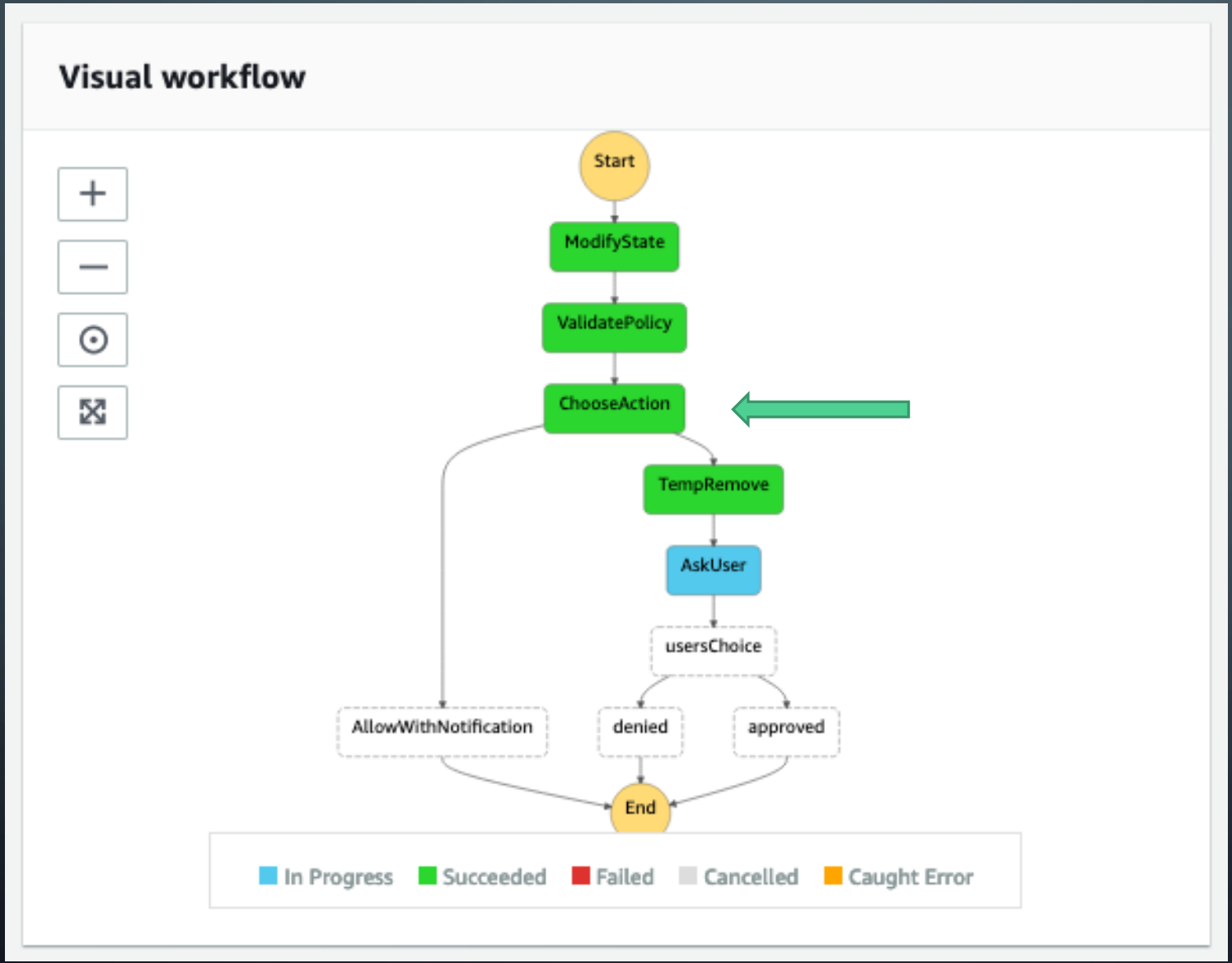
Re-structures the input data into an object that is passed throughout the workflow.



ValidatePolicy

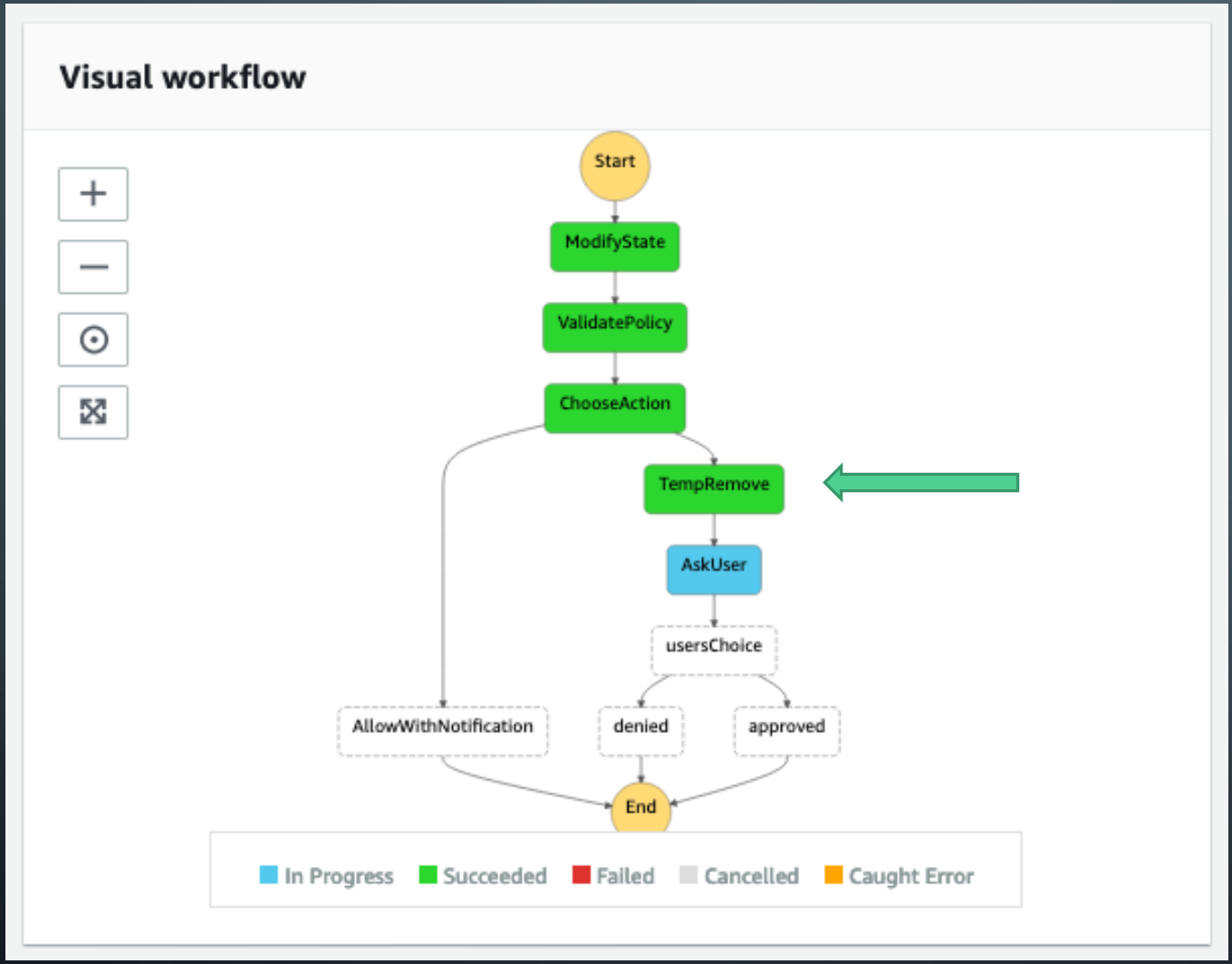
State type: Task. Services: AWS Lambda

Invokes the ValidatePolicy Lambda function that checks the new policy document against the restricted actions.

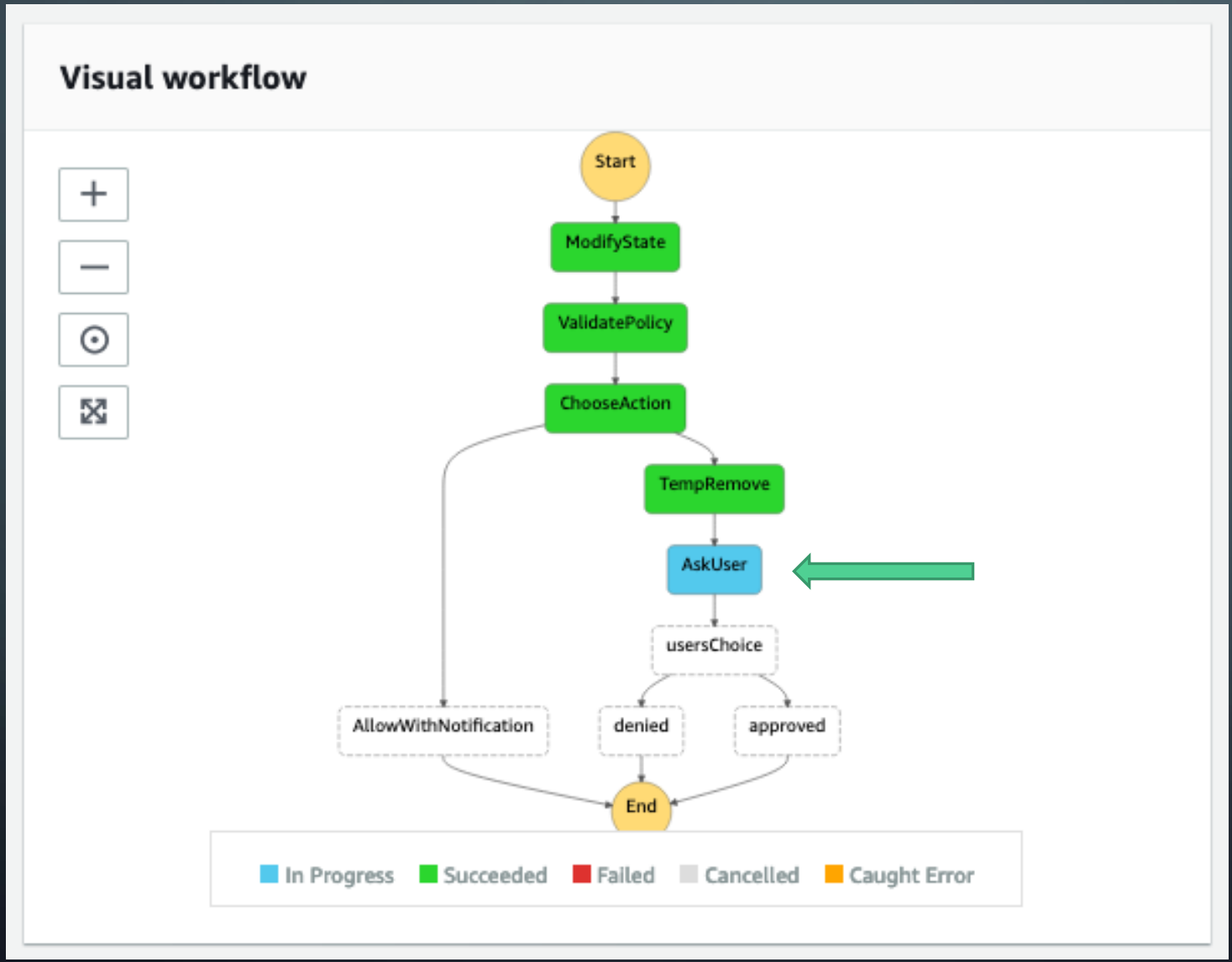


ChooseAction

State type: Choice
Branches depending on input
from ValidatePolicy step.



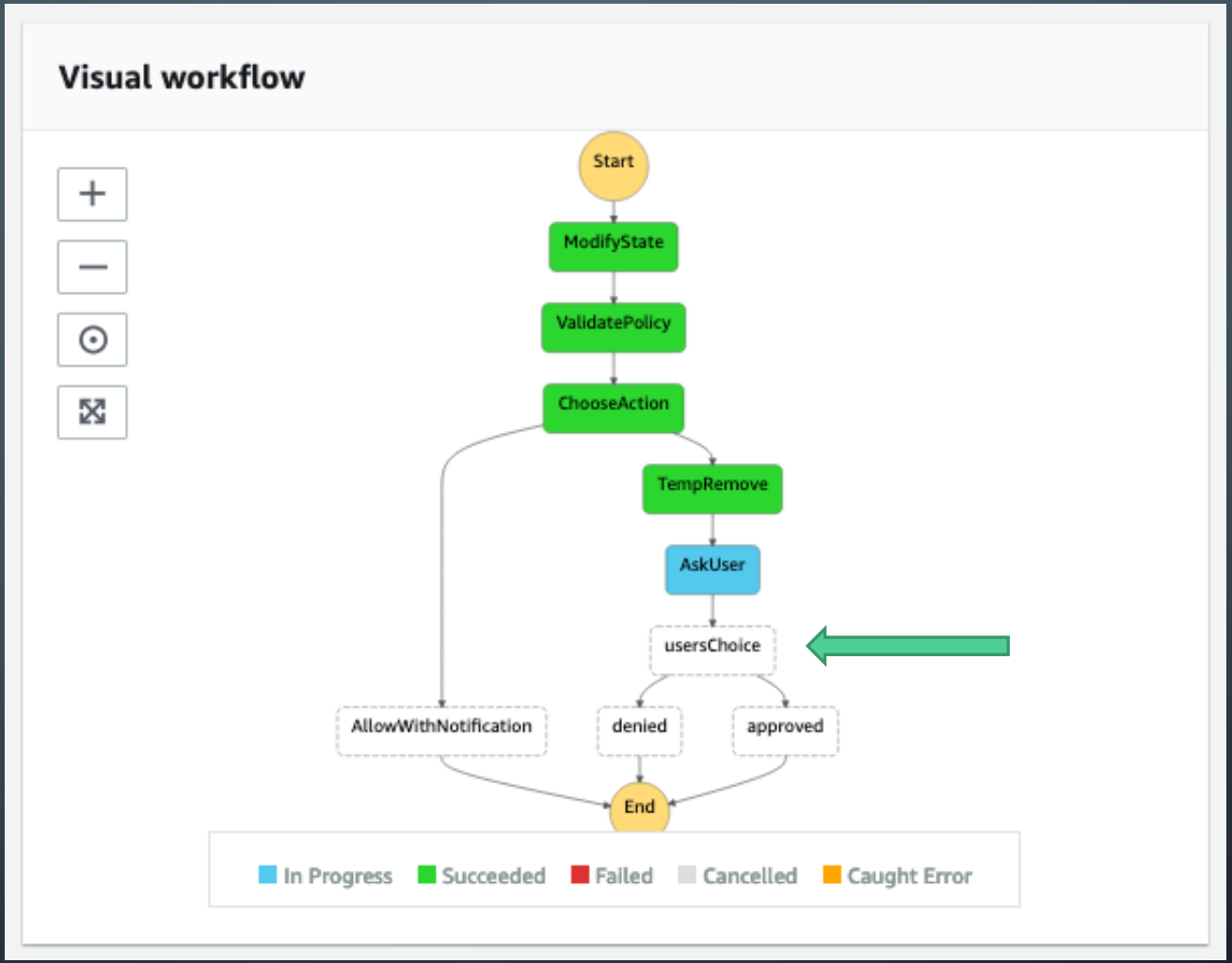
TempRemove
State type: Task.
Service: AWS Lambda
Creates a new default version of the policy with only permissions for Amazon CloudWatch Logs and deletes the previously created policy version.



AskUser

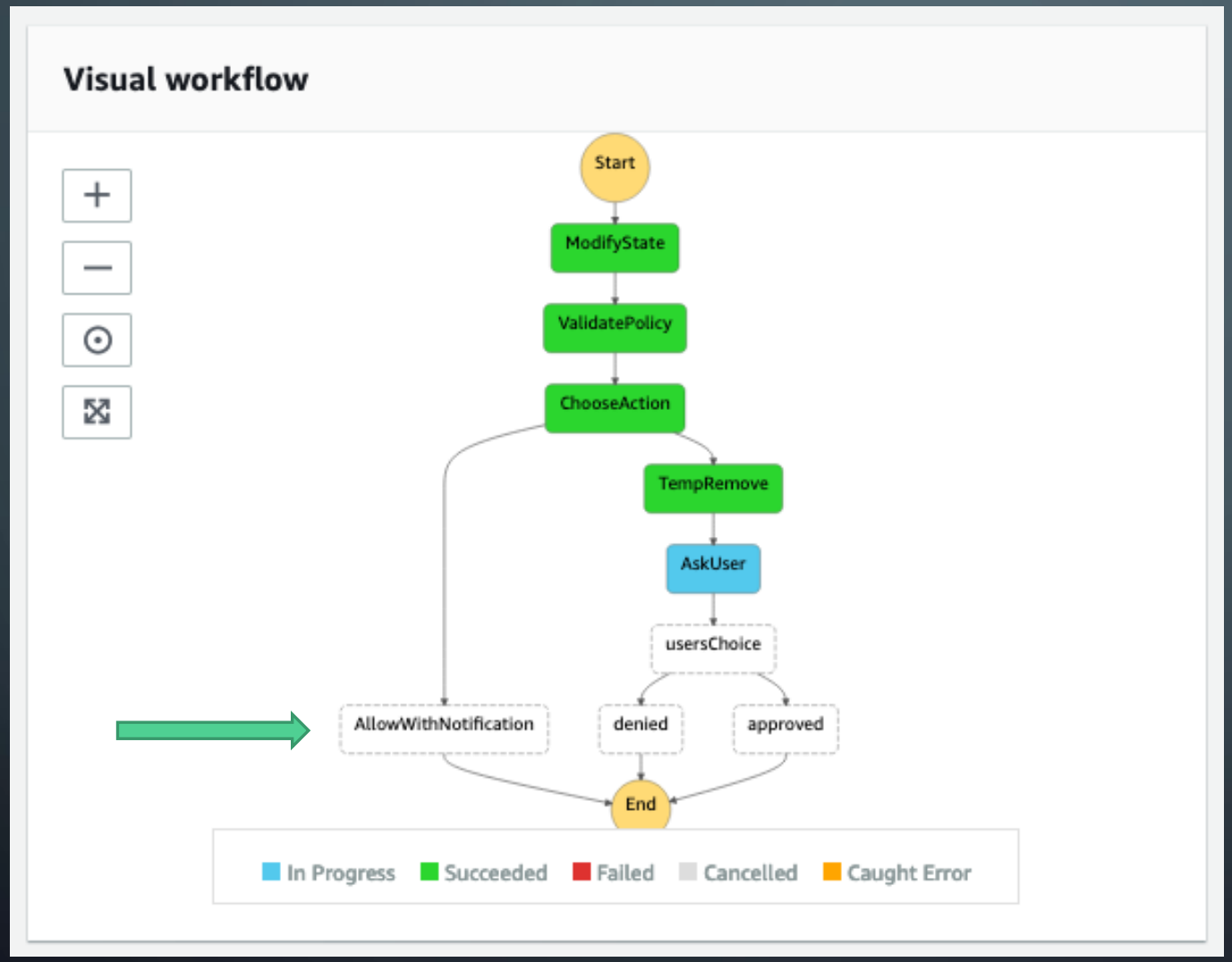
State type: Choice
Sends an approval email to user via SNS, with the task token that initiates the callback pattern.

Denied
State type: Pass
Ends the execution with no further action.



Approved
State type: Task. Service: AWS Lambda
Restores the initial policy document by creating as a new version.

UsersChoice
State type: Choice
Branch based on the user action to approve or deny.



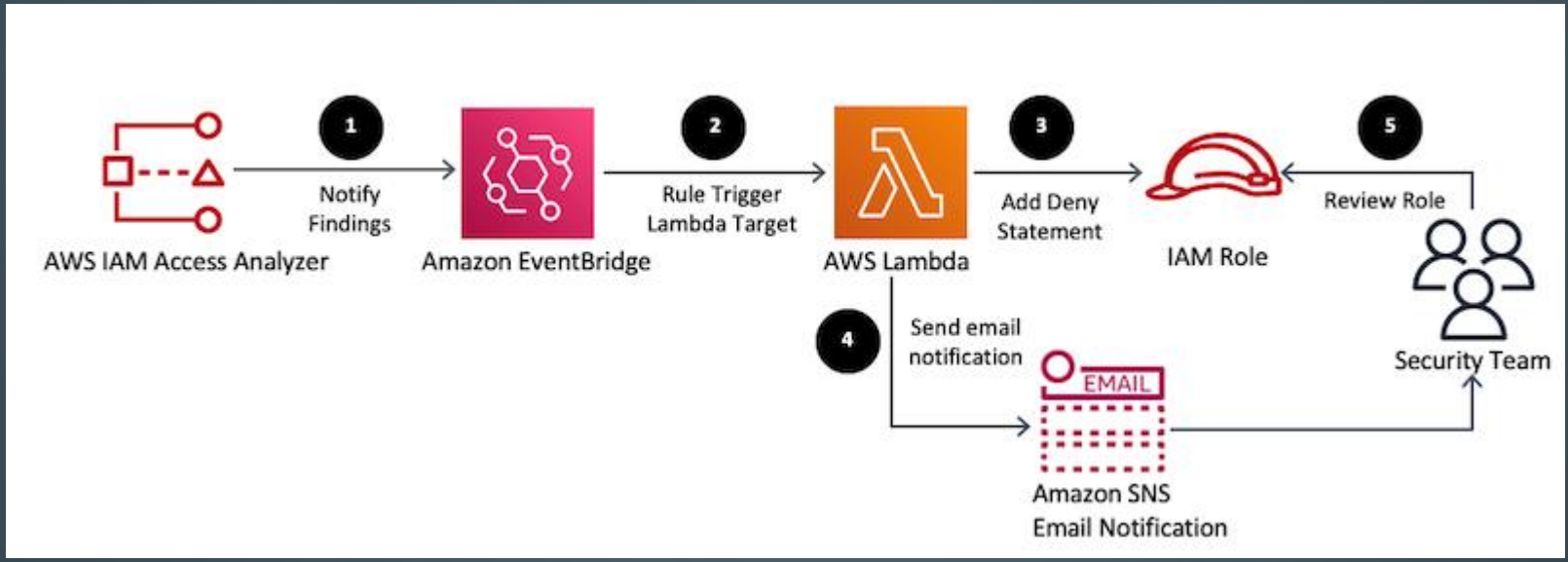
AllowWithNotification

State type: Task. Services: AWS Lambda

With no restricted actions detected, the user is still notified of change (via an email from SNS) before execution ends.

ACCESS ANALYZER FINDING AUTO-REMEDIATION

- When you enable Access Analyzer, you create an analyzer for your entire organization or your account.
- The organization or account you choose is known as the zone of trust for the analyzer.
- The zone of trust determines what type of access is considered trusted by Access Analyzer.
- Access Analyzer continuously monitors all supported resources to identify policies that grant public or cross-account access from outside the zone of trust, and generates findings.



- Resolve AWS Identity and Access Management (IAM) Access Analyzer findings generated in response to unintended cross-account access for IAM roles.

- The solution automates the resolution by responding to the Amazon EventBridge event generated by IAM Access Analyzer for each active finding.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::999988887777:user/Alice"
      },
      "Action": "sts:AssumeRole",
      "Condition": {}
    }
  ]
}
```

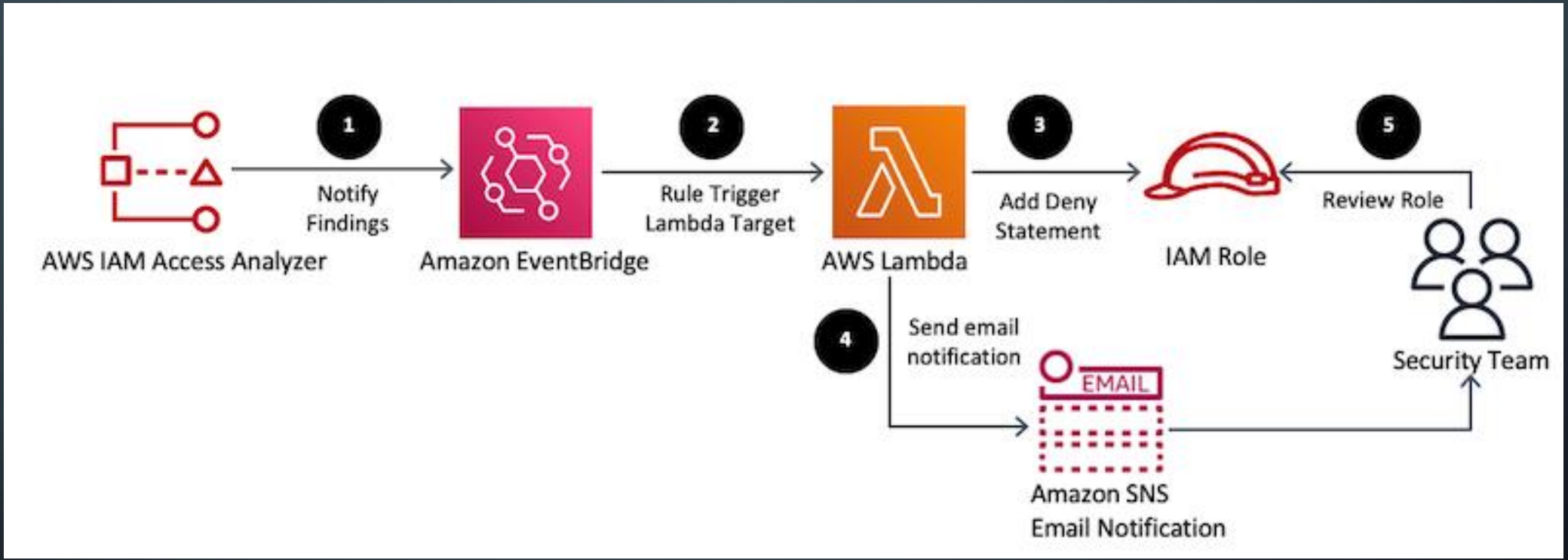
Access Analyzer scans resources and generates findings based on the zone of trust and the archive rules configuration.

```
{
    "version": "0",
    "id": "22222222-dcba-4444-dcba-333333333333",
    "detail-type": "Access Analyzer Finding",
    "source": "aws.access-analyzer",
    "account": "123456789012",
    "time": "2020-05-13T03:14:33Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:access-analyzer:us-east-1: 123456789012:analyzer/AccessAnalyzer"
    ],
    "detail": {
        "version": "1.0",
        "id": "a5018210-97c4-46c4-9456-0295898377b6",
        "status": "ACTIVE",
        "resourceType": "AWS::IAM::Role",
        "resource": "arn:aws:iam::123456789012:role/ Audit_CrossAccountRole",
        "createdAt": "2020-05-13T03:14:32Z",
        "analyzedAt": "2020-05-13T03:14:32Z",
        "analyzedAt": "2020-05-13T03:14:32Z",
        "updatedAt": "2020-05-13T03:14:32Z",
        "accountId": "123456789012",
        "region": "us-east-1",
        "principal": {
            "AWS": "aws:arn:iam::999988887777:user/Alice"
        },
        "action": [
            "sts:AssumeRole"
        ],
        "condition": {},
        "isDeleted": false,
        "isPublic": false
    }
}
```


Access Analyzer scans resources and generates findings based on the zone of trust and the archive rules configuration. The following is an example of an Access Analyzer active finding event sent to Amazon EventBridge

The following is an example of the EventBridge event pattern to match active Access Analyzer findings

```
{
  "source": [
    "aws.access-analyzer"
  ],
  "detail-type": [
    "Access Analyzer Finding"
  ],
  "detail": {
     "status": [ "ACTIVE" ],
    "resourceType": [ "AWS::IAM:Role" ]
    }
}
```



EventBridge receives an event for the Access Analyzer finding, and triggers the AWS Lambda function based on the event rule configuration.

Thank you!