RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **DSO-F01**

Solving for DevOps Auditors with Automated Compliance

Michelle Nikulshin

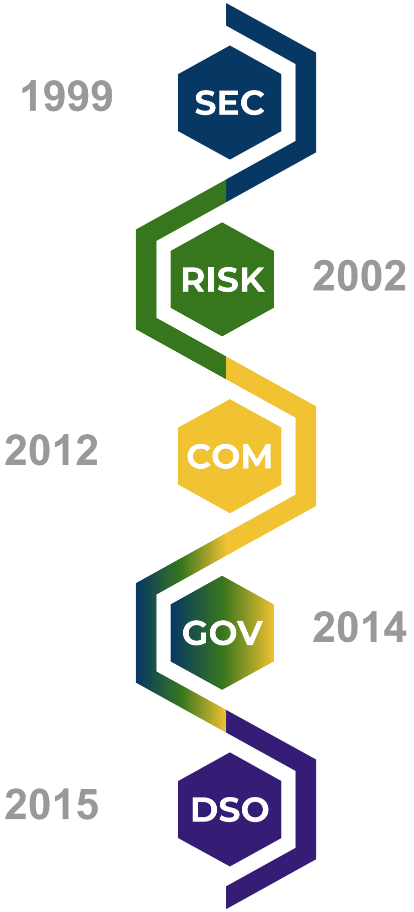
Director, Security Governance
Intuit

Shannon Lietz

Director, Adversary Management
Intuit

<michelle />

MY pseudo JOURNEY LINE...



1999 SEC

2002 RISK

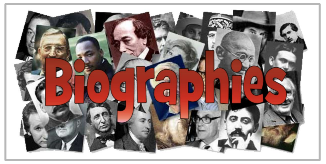
2012 COM

2014 GOV

2015 DSO

WHAT MAKES ME HUMAN...

FAMILY AND FRIENDS



HOW I SPEND MY DAYS...

intuit

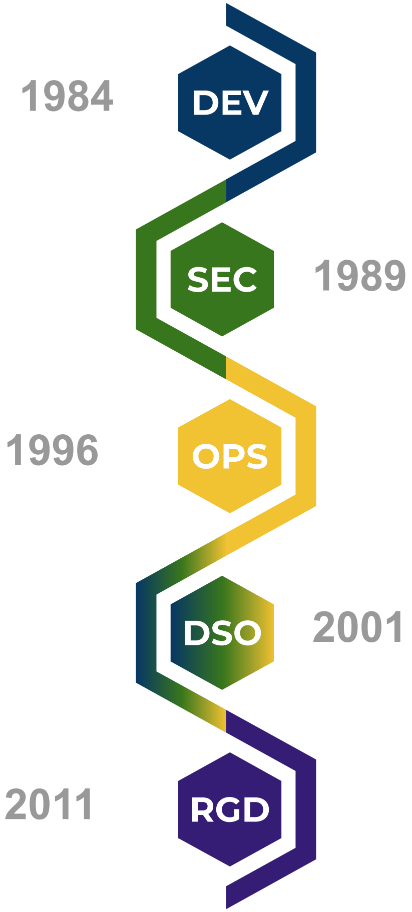
turbotax quickbooks mint

REGULATORY COMPLIANCE

amazon web services

<shannon />

MY pseudo JOURNEY LINE...



1984 DEV

1989 SEC

1996 OPS

2001 DSO

2011 RGD

WHAT MAKES ME HUMAN...

STEM

Science · Technology · Engineering · Math

Sugar plum fairies

COMICS

I **<heart>** Kickboxing

HOW I SPEND MY DAYS...

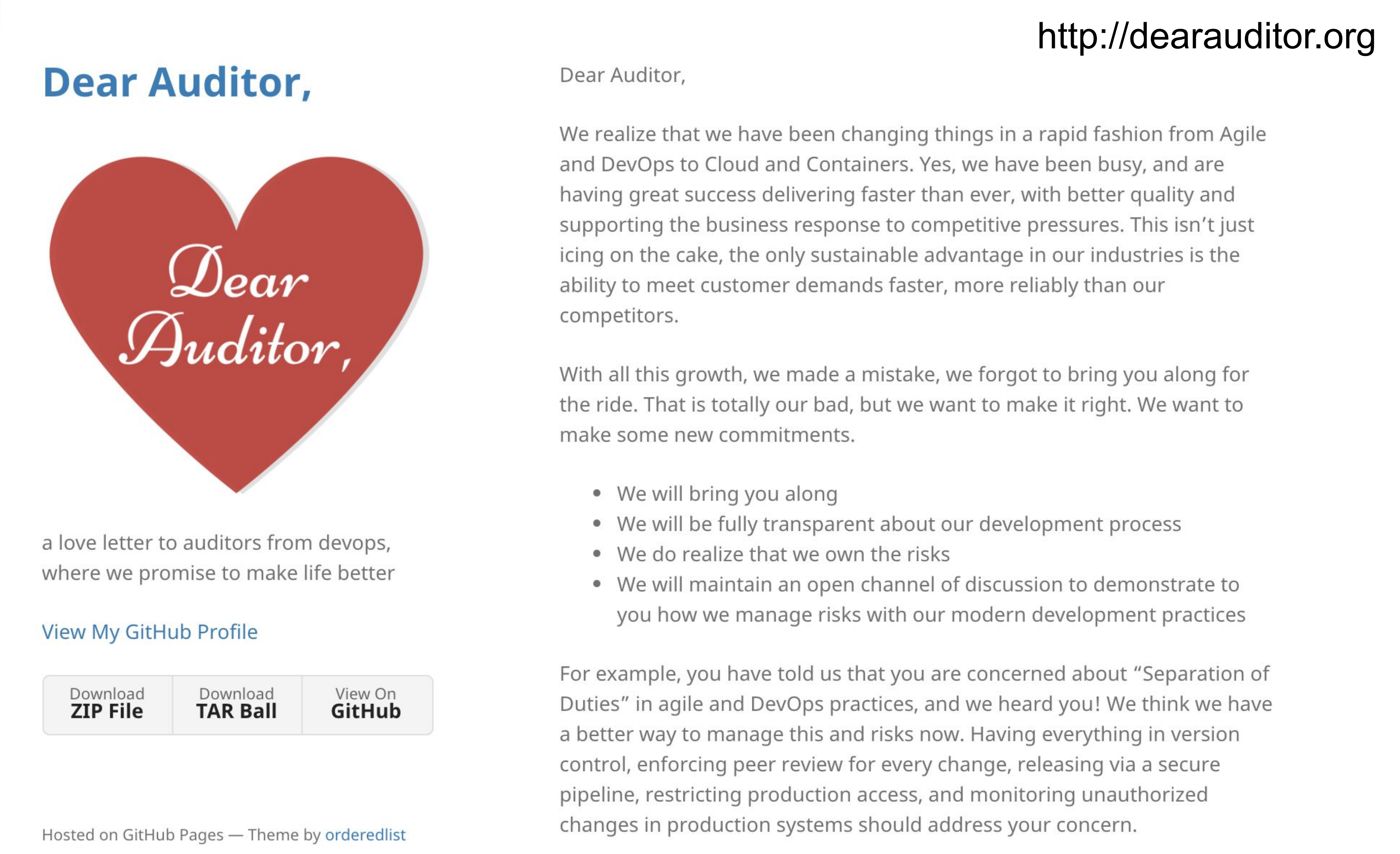
DEV	SOFTWARE
SEC	SAFER
OPS	SOONER

intuit®

IANS

HACKERGIRL

http://dearauditor.org



Dear Auditor,

a love letter to auditors from devops, where we promise to make life better

View My GitHub Profile

Hosted on GitHub Pages — Theme by orderedlist

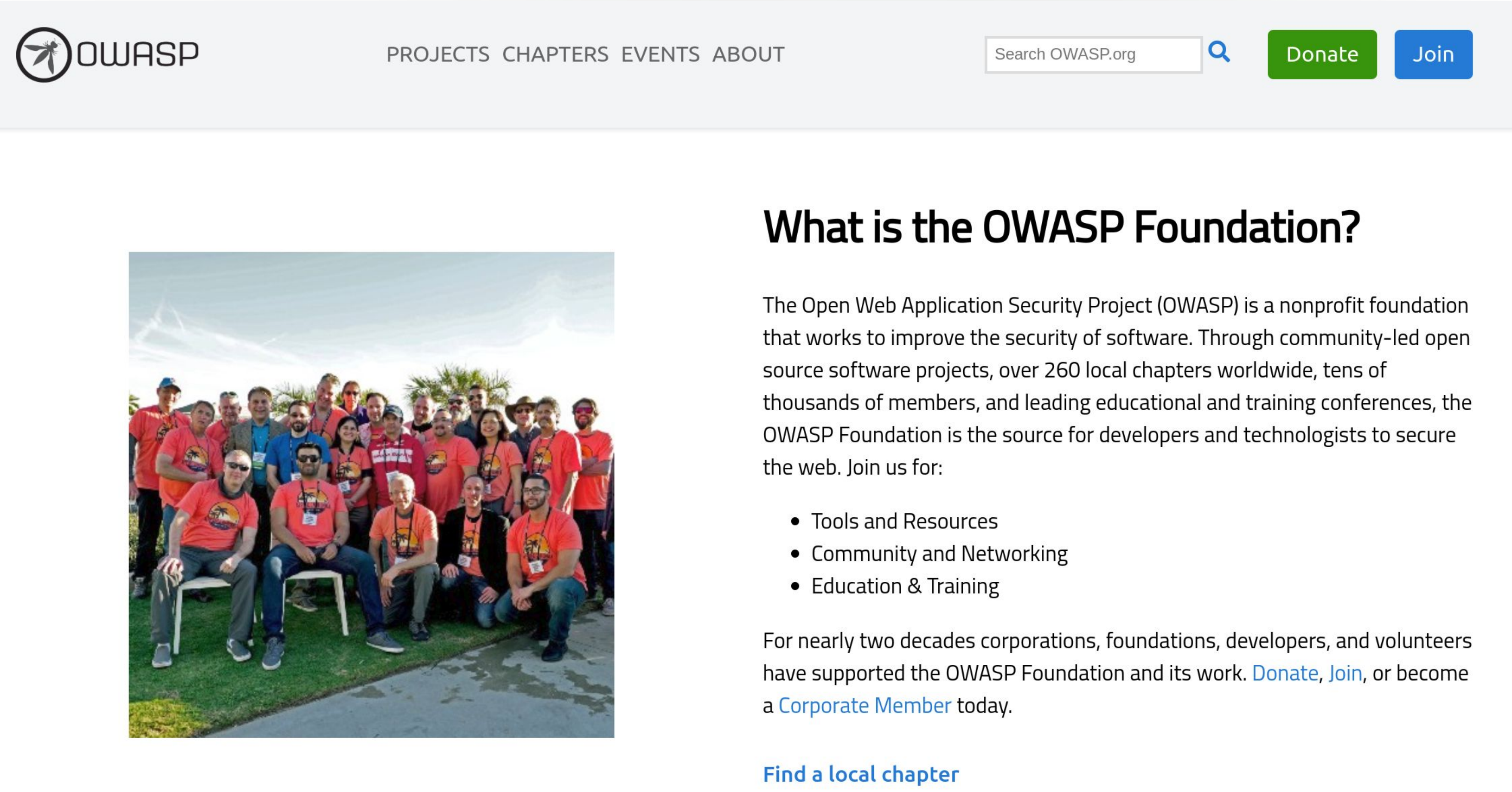
Dear Auditor,

We realize that we have been changing things in a rapid fashion from Agile and DevOps to Cloud and Containers. Yes, we have been busy, and are having great success delivering faster than ever, with better quality and supporting the business response to competitive pressures. This isn't just icing on the cake, the only sustainable advantage in our industries is the ability to meet customer demands faster, more reliably than our competitors.

With all this growth, we made a mistake, we forgot to bring you along for the ride. That is totally our bad, but we want to make it right. We want to make some new commitments.

- We will bring you along
- We will be fully transparent about our development process
- We do realize that we own the risks
- We will maintain an open channel of discussion to demonstrate to you how we manage risks with our modern development practices

For example, you have told us that you are concerned about "Separation of Duties" in agile and DevOps practices, and we heard you! We think we have a better way to manage this and risks now. Having everything in version control, enforcing peer review for every change, releasing via a secure pipeline, restricting production access, and monitoring unauthorized changes in production systems should address your concern.



What is the OWASP Foundation?

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, over 260 local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web. Join us for:

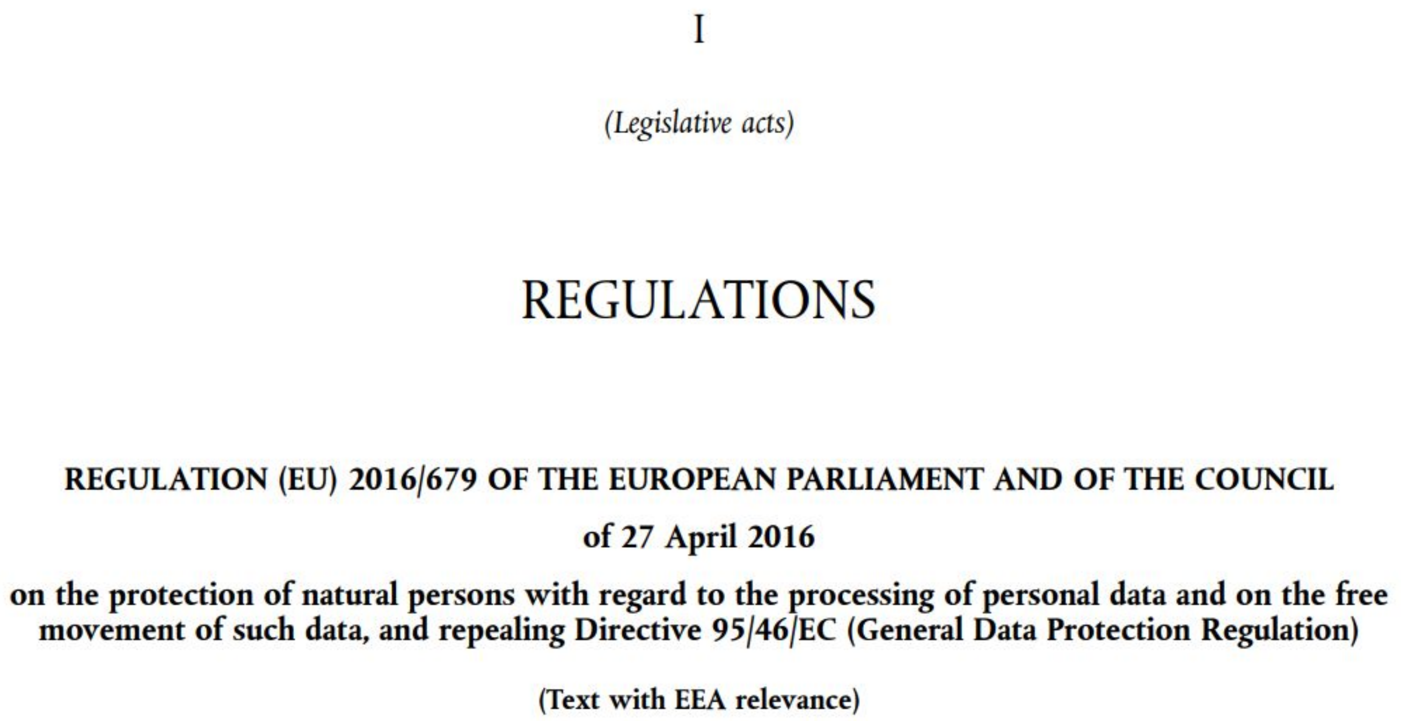
- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. Donate, Join, or become a Corporate Member today.

Find a local chapter

New API Security Project:
https://www.owasp.org/images/e/ea/OWASP_APIs_Security_Project_Kick_Off.pdf

CALIFORNIANS FOR
CONSUMER PRIVACY



I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

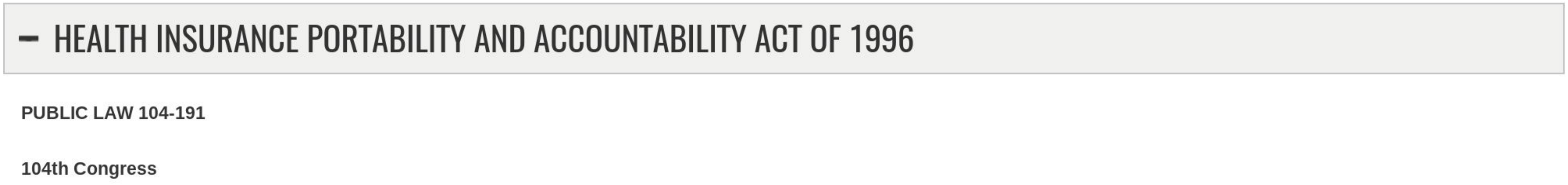
of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

NIST

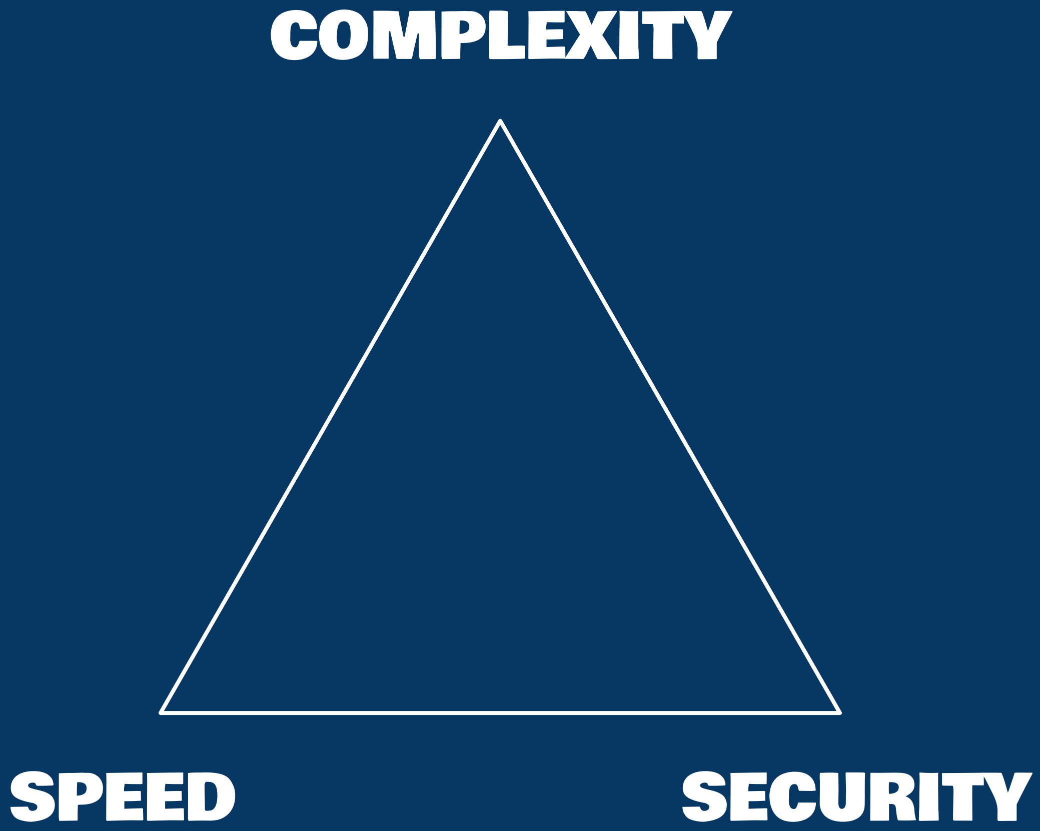
pci
Security
Standards Council
®



− HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

PUBLIC LAW 104-191

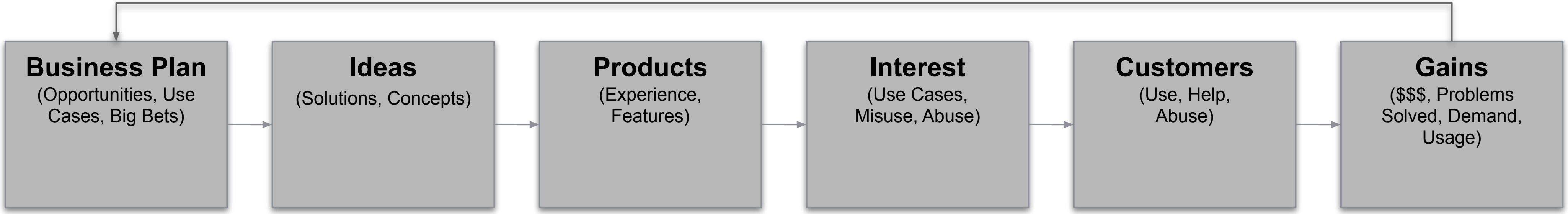
104th Congress



COMPLEXITY

SPEED

SECURITY



Business Plan
(Opportunities, Use Cases, Big Bets)

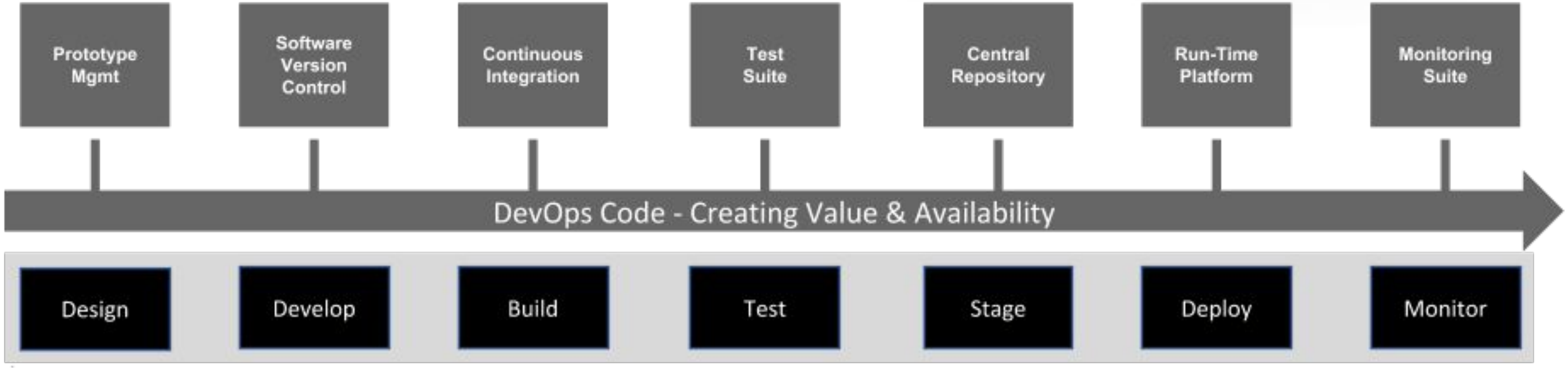
Ideas
(Solutions, Concepts)

Products
(Experience, Features)

Interest
(Use Cases, Misuse, Abuse)

Customers
(Use, Help, Abuse)

Gains
($$$, Problems Solved, Demand, Usage)



Prototype Mgmt

Software Version Control

Continuous Integration

Test Suite

Central Repository

Run-Time Platform

Monitoring Suite

DevOps Code - Creating Value & Availability

Design

Develop

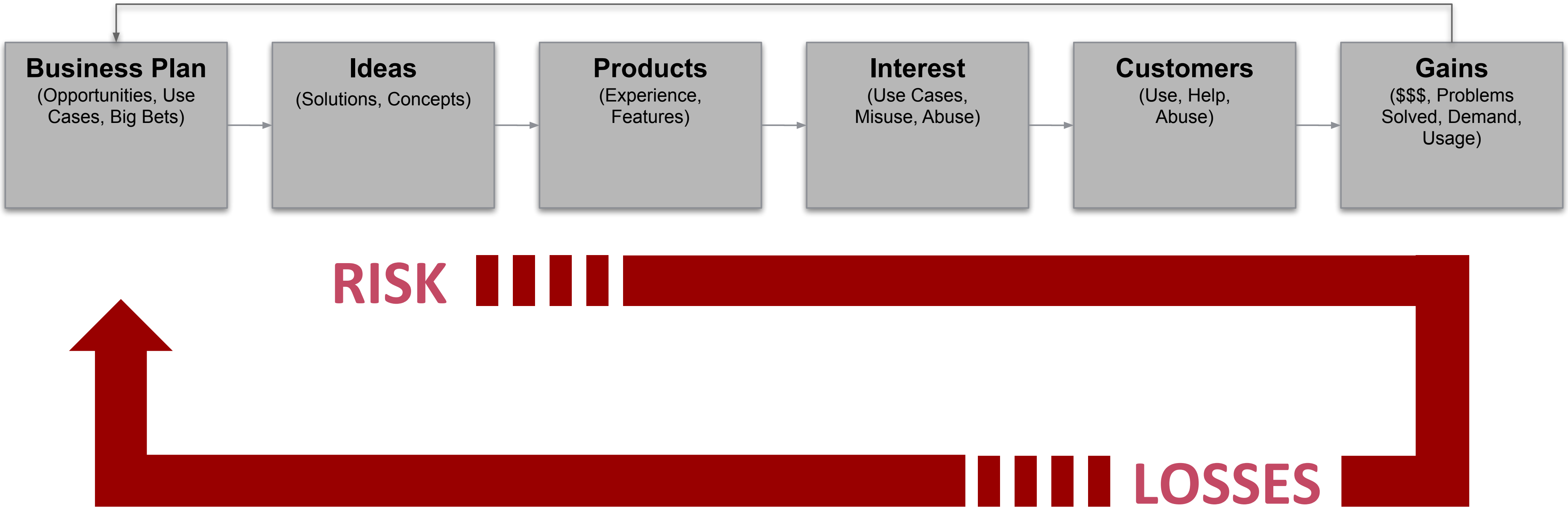
Build

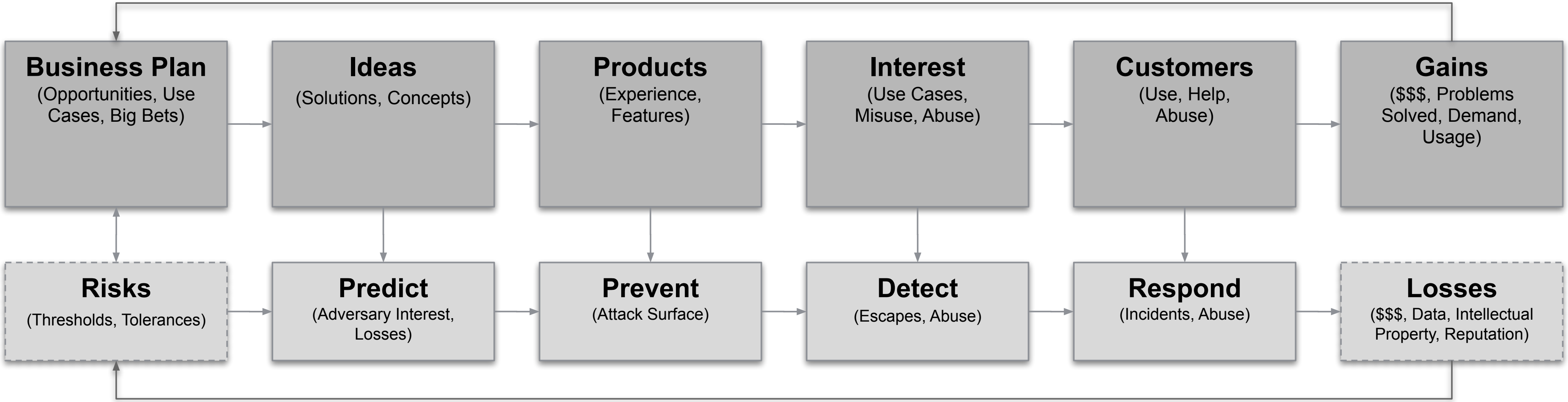
Test

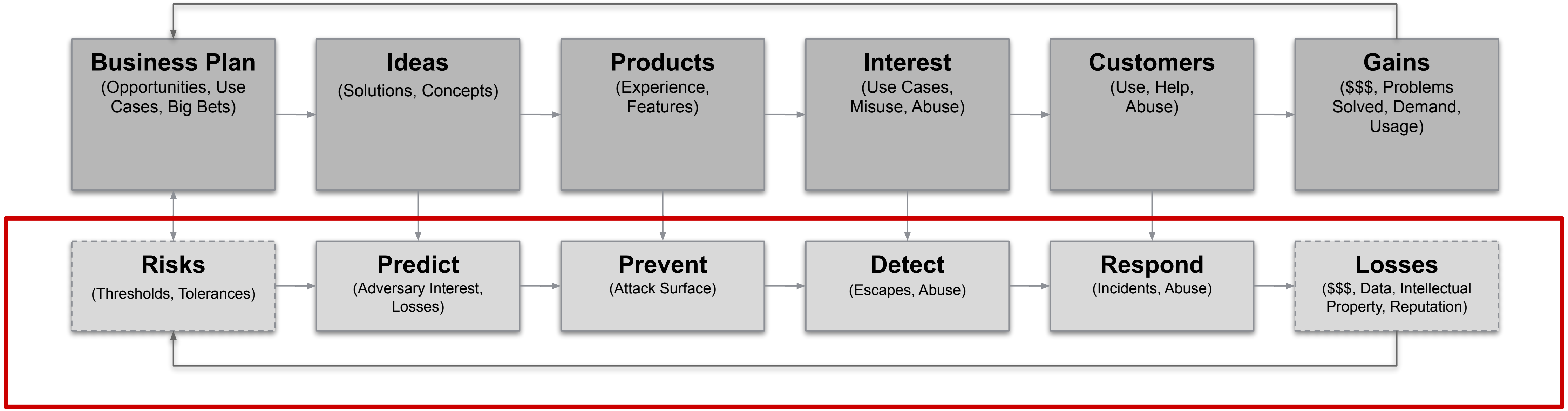
Stage

Deploy

Monitor


Business Plan
(Opportunities, Use Cases, Big Bets)
Ideas
(Solutions, Concepts)
Products
(Experience, Features)
Interest
(Use Cases, Misuse, Abuse)
Customers
(Use, Help, Abuse)
Gains
($$$, Problems Solved, Demand, Usage)
RISK
LOSSES


Business Plan
(Opportunities, Use Cases, Big Bets)
Ideas
(Solutions, Concepts)
Products
(Experience, Features)
Interest
(Use Cases, Misuse, Abuse)
Customers
(Use, Help, Abuse)
Gains
($$$, Problems Solved, Demand, Usage)
Risks
(Thresholds, Tolerances)
Predict
(Adversary Interest, Losses)
Prevent
(Attack Surface)
Detect
(Escapes, Abuse)
Respond
(Incidents, Abuse)
Losses
($$$, Data, Intellectual Property, Reputation)



Business Plan
(Opportunities, Use Cases, Big Bets)

Ideas
(Solutions, Concepts)

Products
(Experience, Features)

Interest
(Use Cases, Misuse, Abuse)

Customers
(Use, Help, Abuse)

Gains
($$$, Problems Solved, Demand, Usage)

Risks
(Thresholds, Tolerances)

Predict
(Adversary Interest, Losses)

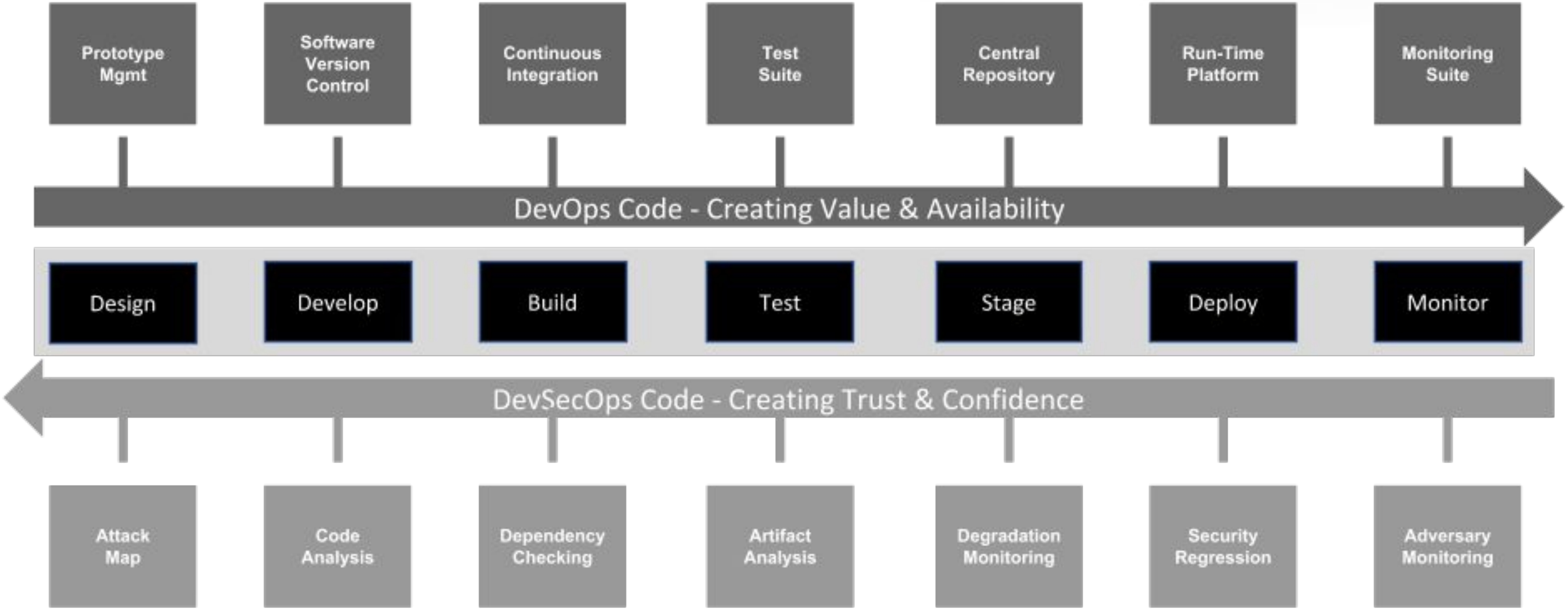
Prevent
(Attack Surface)

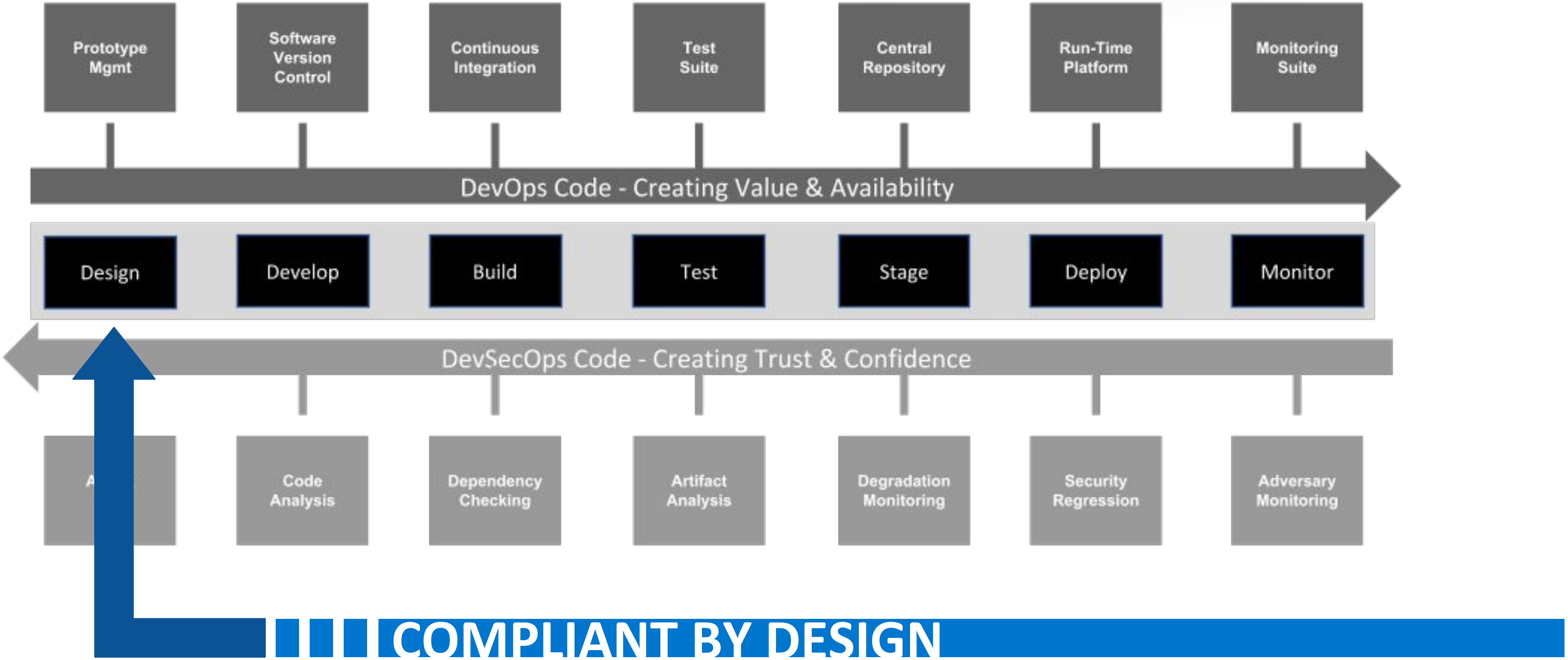
Detect
(Escapes, Abuse)

Respond
(Incidents, Abuse)

Losses
($$$, Data, Intellectual Property, Reputation)

CONTROL ENVIRONMENT


Prototype Mgmt
Software Version Control
Continuous Integration
Test Suite
Central Repository
Run-Time Platform
Monitoring Suite
DevOps Code - Creating Value & Availability
Design
Develop
Build
Test
Stage
Deploy
Monitor
DevSecOps Code - Creating Trust & Confidence
Attack Map
Code Analysis
Dependency Checking
Artifact Analysis
Degradation Monitoring
Security Regression
Adversary Monitoring



Prototype Mgmt

Software Version Control

Continuous Integration

Test Suite

Central Repository

Run-Time Platform

Monitoring Suite

DevOps Code - Creating Value & Availability

Design

Develop

Build

Test

Stage

Deploy

Monitor

DevSecOps Code - Creating Trust & Confidence

A

Code Analysis

Dependency Checking

Artifact Analysis

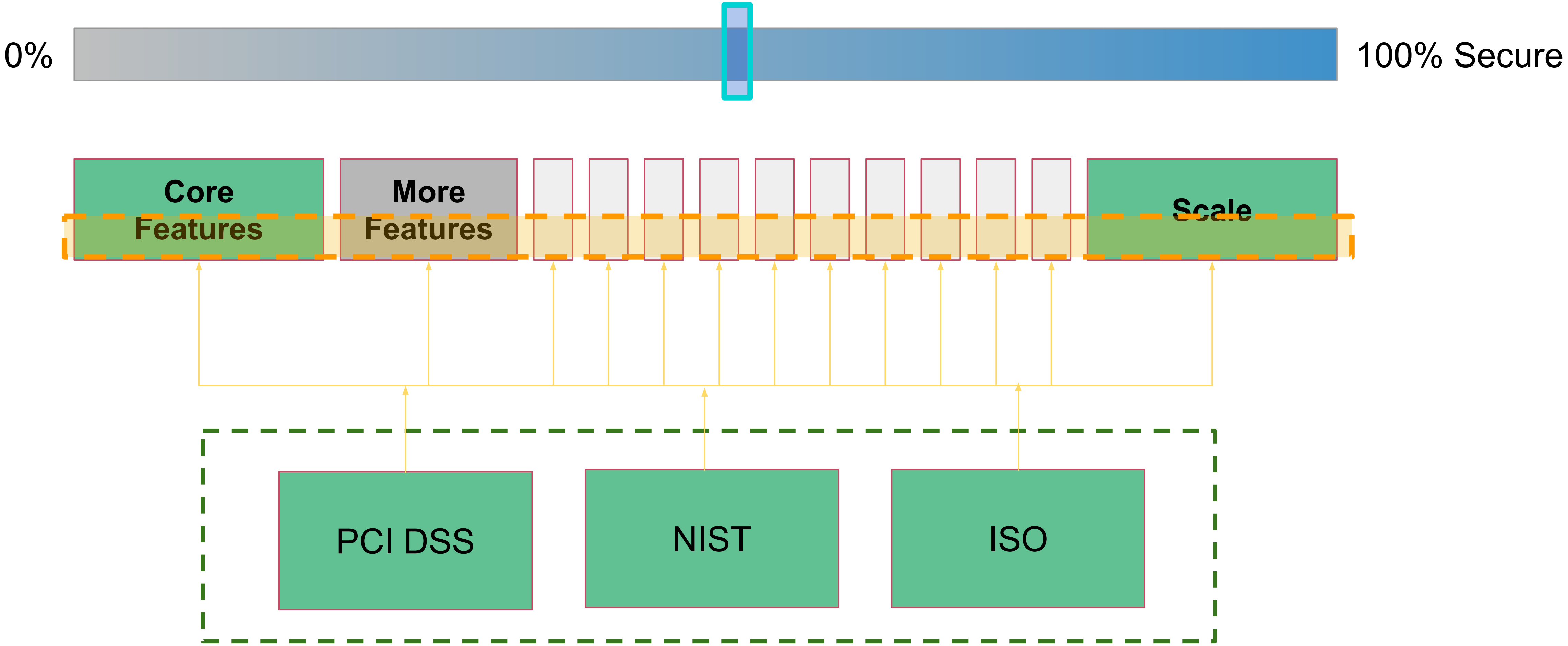
Degradation Monitoring

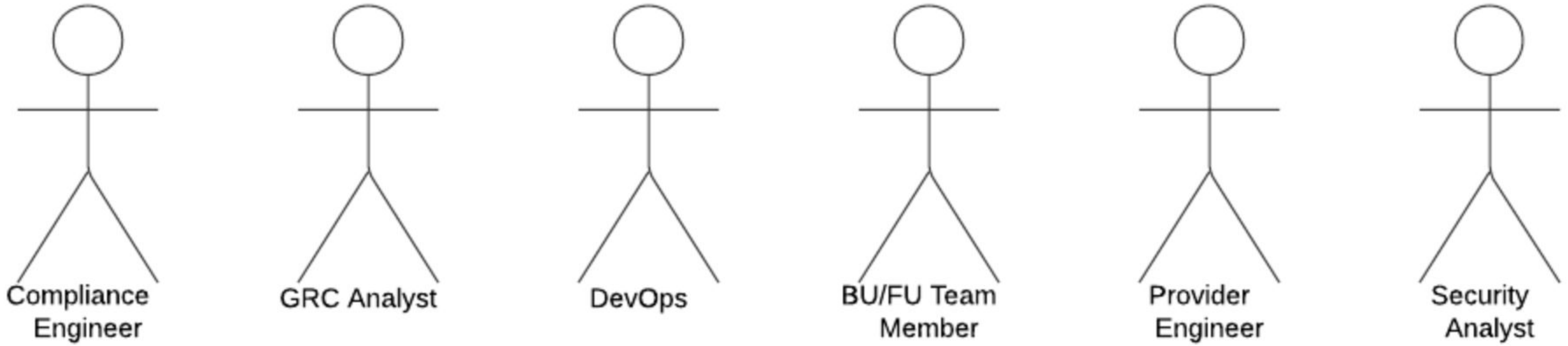
Security Regression

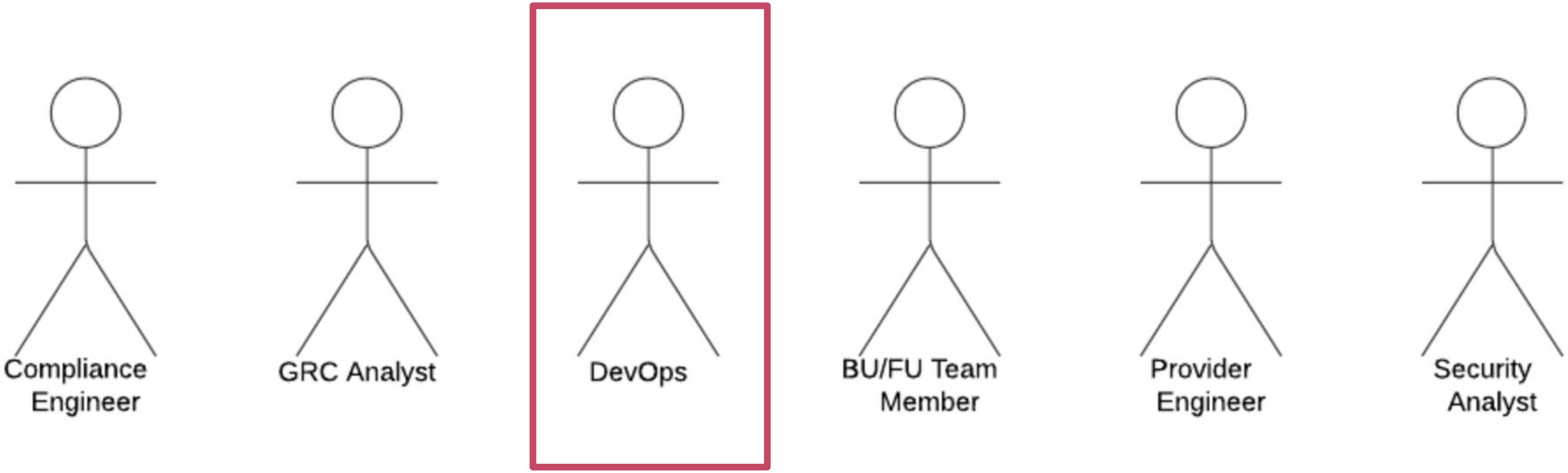
Adversary Monitoring

COMPLIANT BY DESIGN

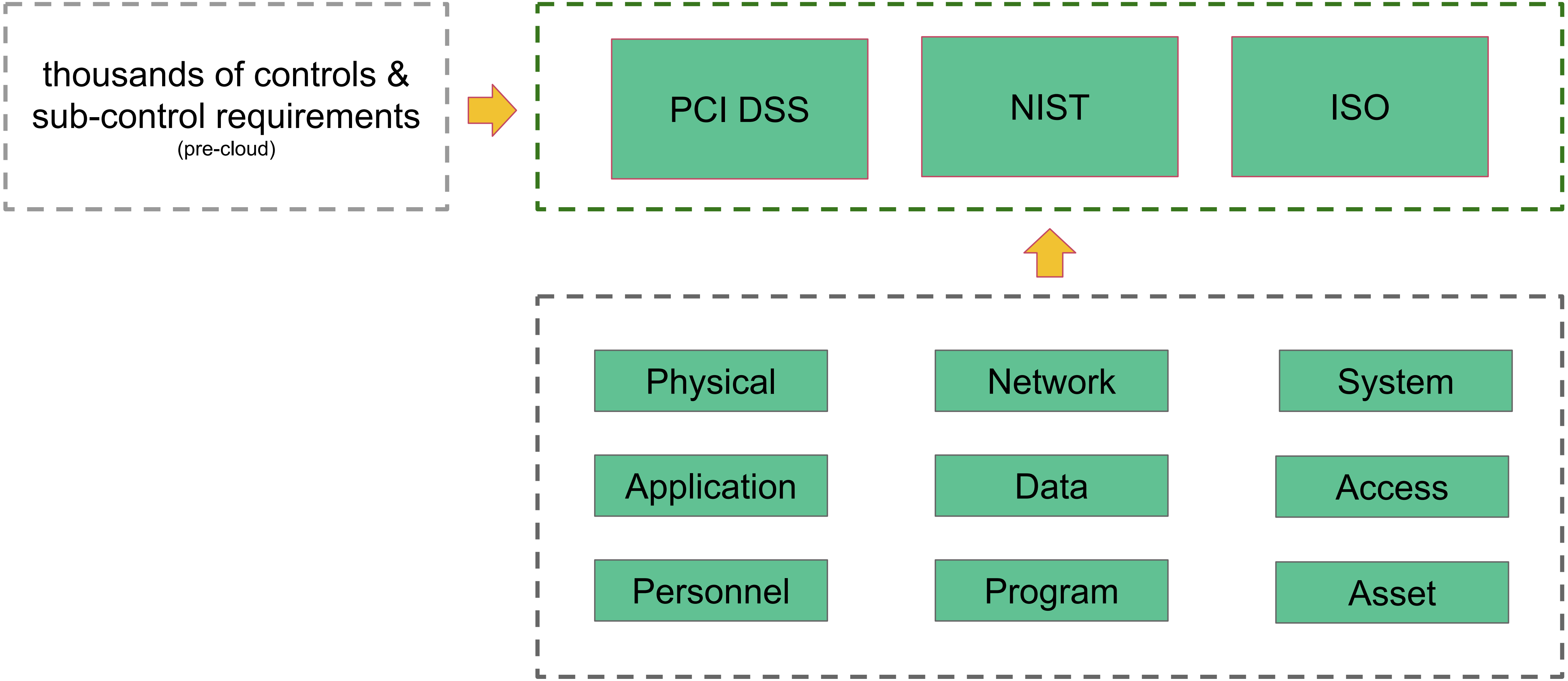
The Checklist Approach




Compliance Engineer
GRC Analyst
DevOps
BU/FU Team Member
Provider Engineer
Security Analyst


Compliance Engineer
GRC Analyst
DevOps
BU/FU Team Member
Provider Engineer
Security Analyst

An Opportunity - The Controls Approach



thousands of controls & sub-control requirements
(pre-cloud)

PCI DSS

NIST

ISO

Physical

Network

System

Application

Data

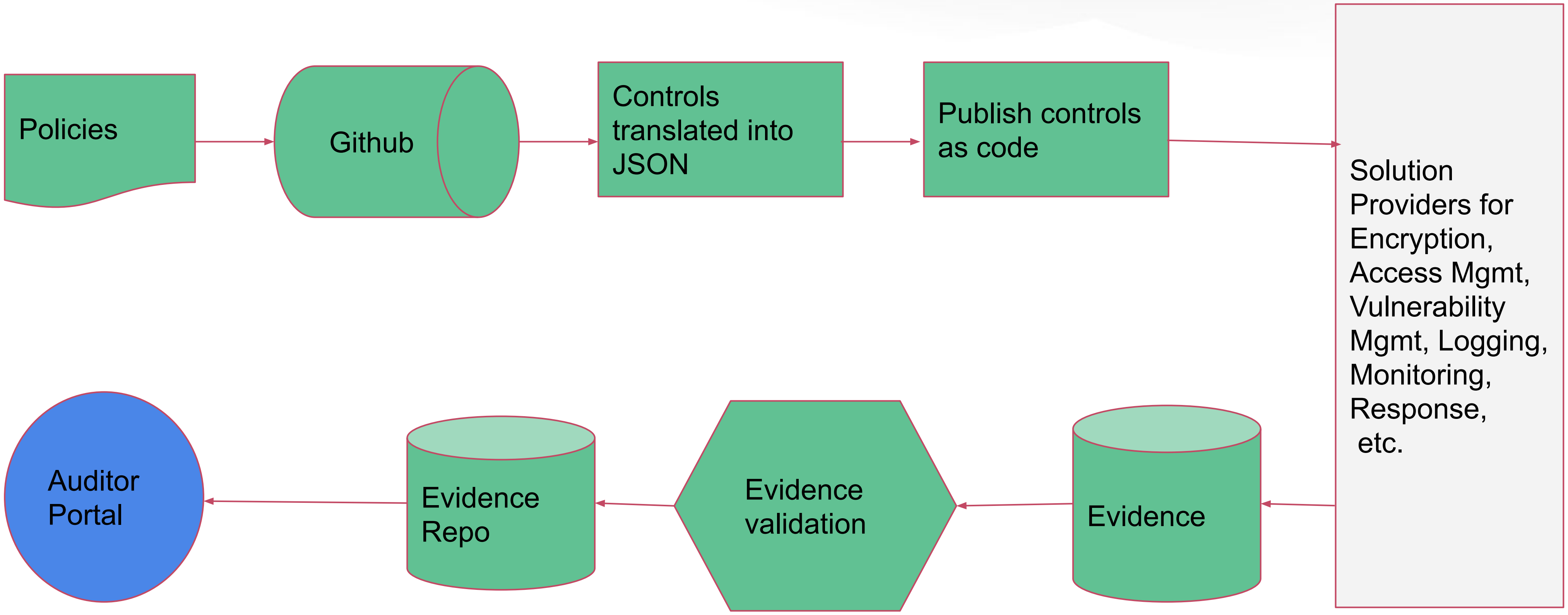
Access

Personnel

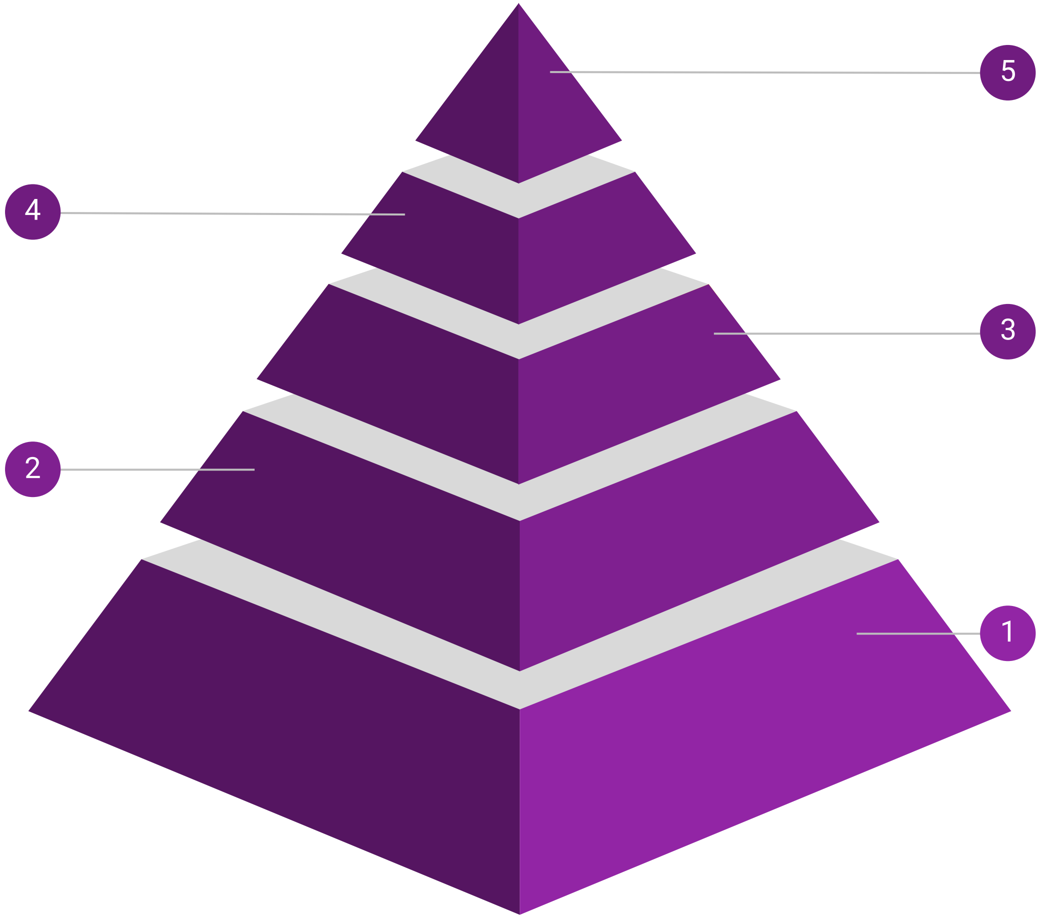
Program

Asset

Controls as Code


Policies
Github
Controls translated into JSON
Publish controls as code
Solution Providers for Encryption, Access Mgmt, Vulnerability Mgmt, Logging, Monitoring, Response, etc.
Evidence
Evidence validation
Evidence Repo
Auditor Portal

Security Hierarchy of Needs



Encryption

Prevent data loss by leveraging the benefits of encryption for selectively eliminating injection attacks and transparently protecting access to data

Authentication

Focus on securing access through identity verification and two-factor authentication mechanisms to establish trusted usage

Logging

Implement event logging and audit trails to ensure visibility, detection and response for abuse cases

Asset Management

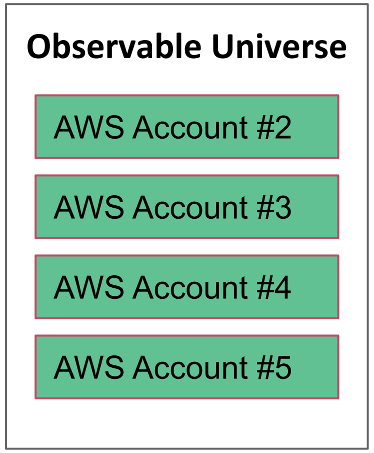
Maintain a manifest of all components, configurations and attribution data to ensure proper asset handling, lifecycle management and to speed up response events

Zoning & Containment

Establish trust boundaries and control blast radius to ensure workload safety, viability and resiliency

Opportunity #1 - Separation of Duties

Opportunity #1 - Separation of Duties



Observable Universe

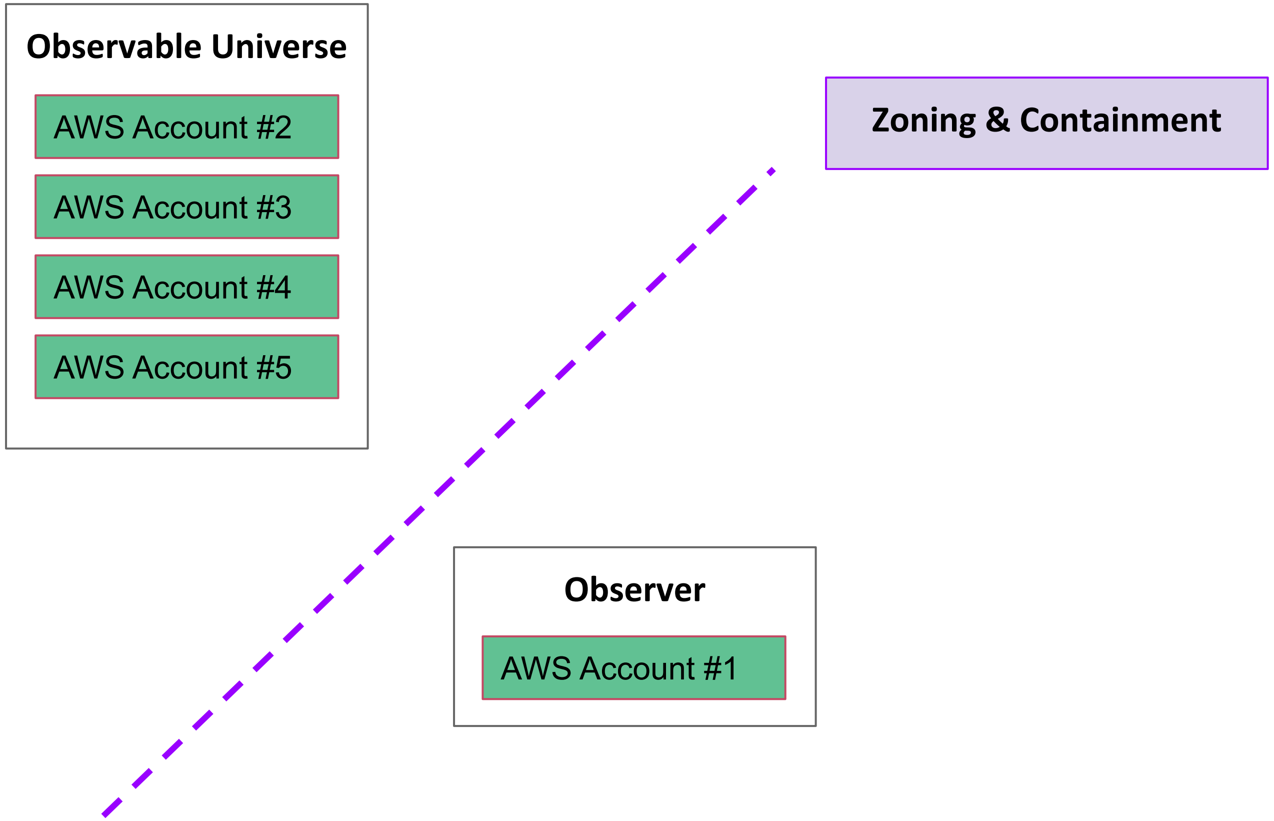
AWS Account #2

AWS Account #3

AWS Account #4

AWS Account #5

Opportunity #1 - Separation of Duties



Observable Universe

AWS Account #2

AWS Account #3

AWS Account #4

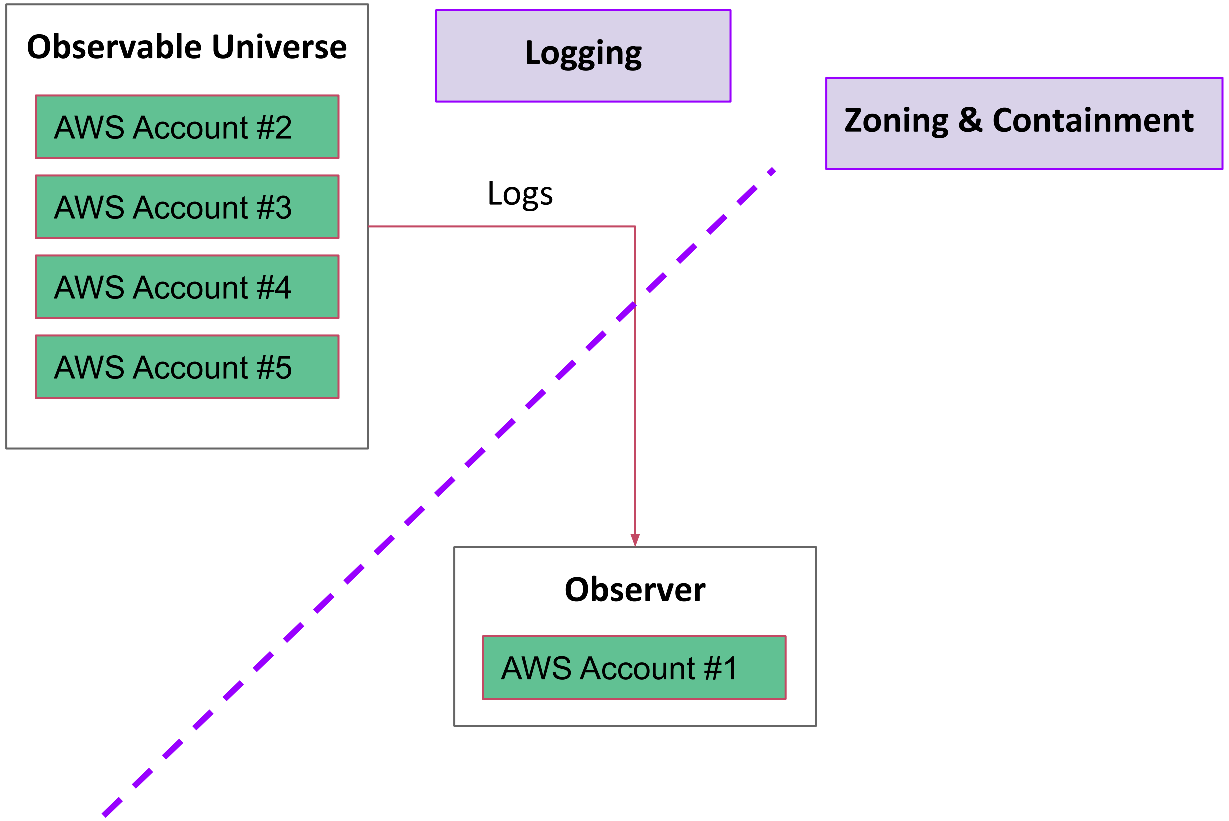
AWS Account #5

Zoning & Containment

Observer

AWS Account #1

Opportunity #1 - Separation of Duties



Observable Universe

AWS Account #2

AWS Account #3

AWS Account #4

AWS Account #5

Logging

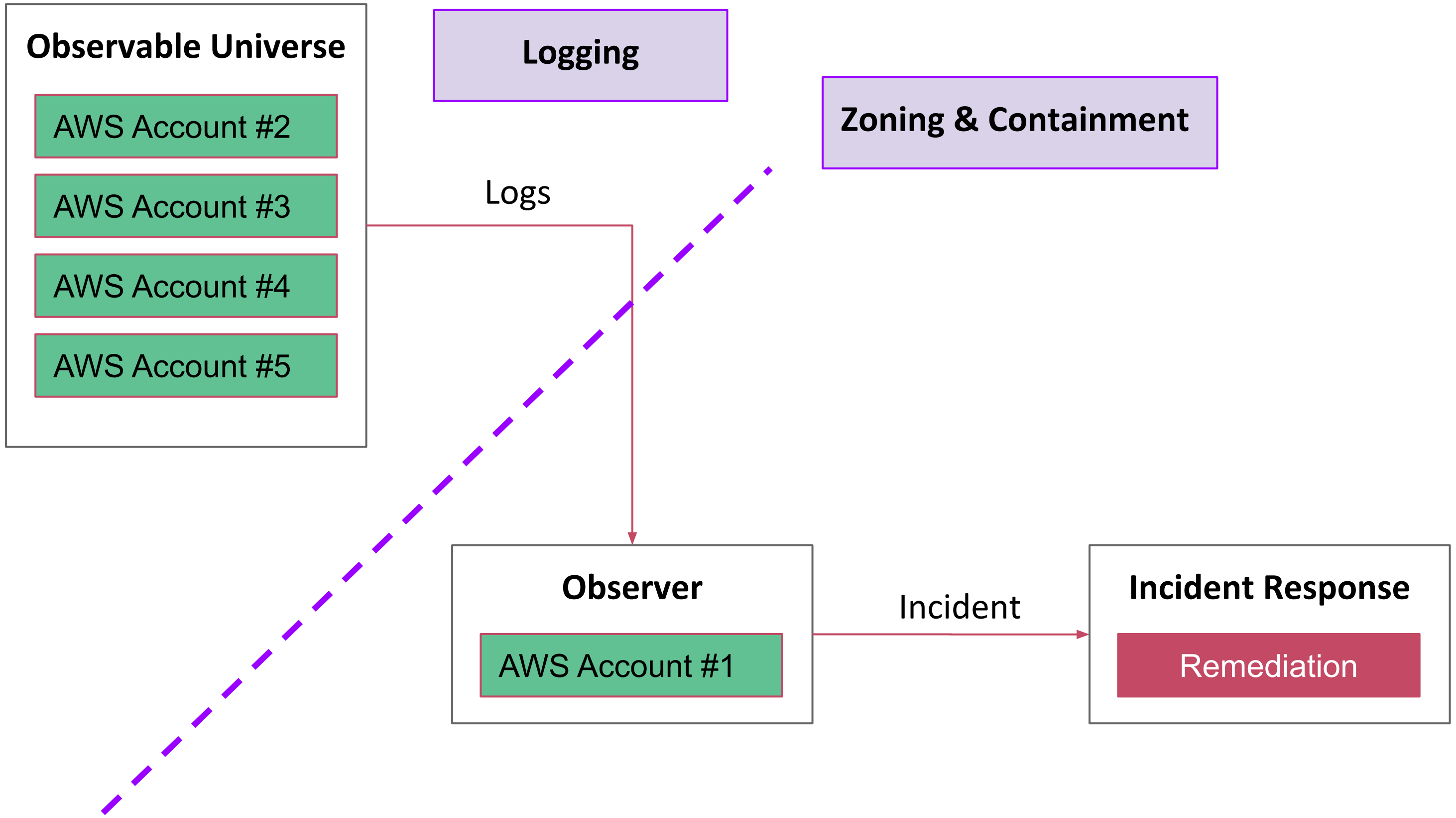
Zoning & Containment

Logs

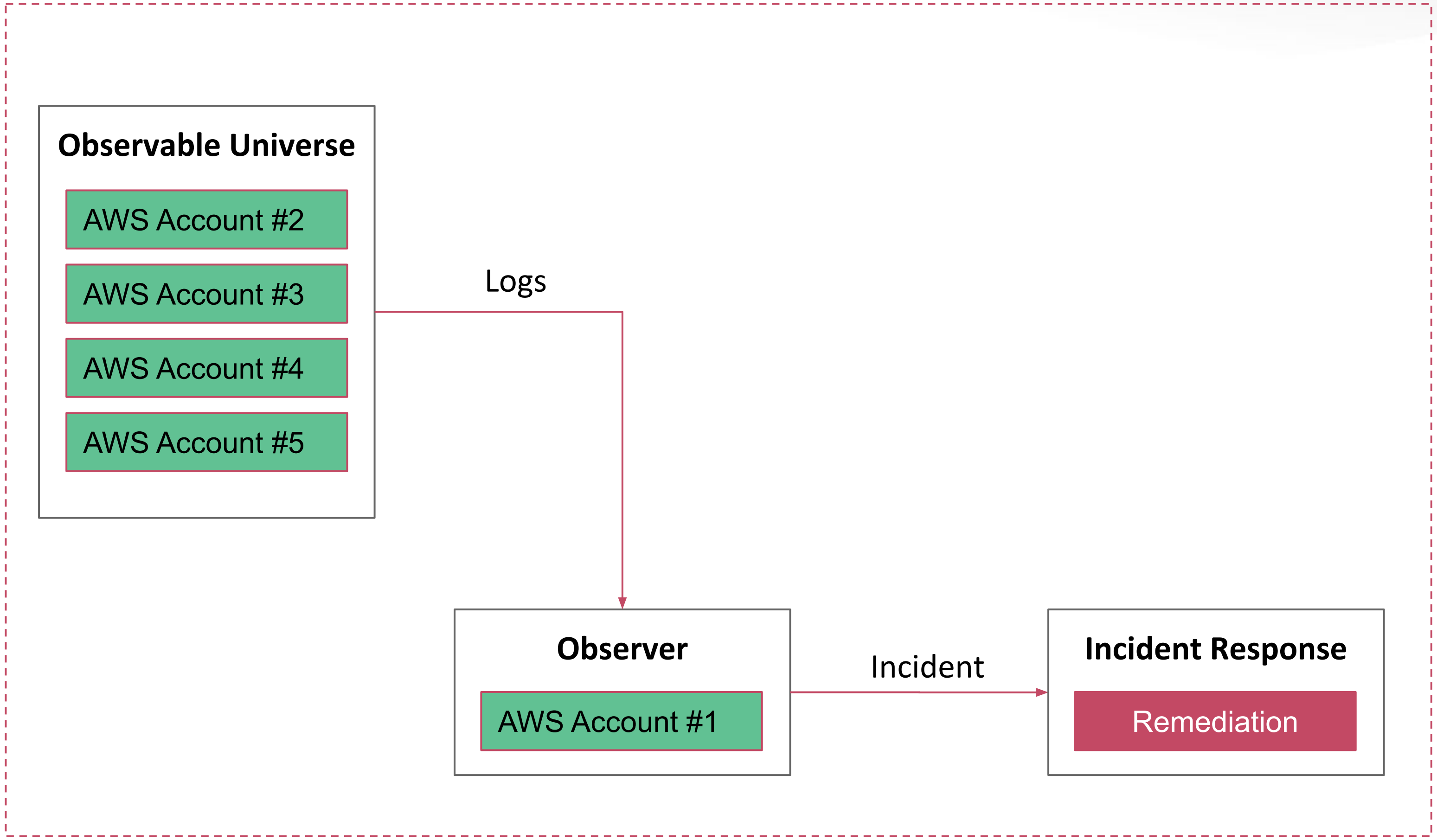
Observer

AWS Account #1

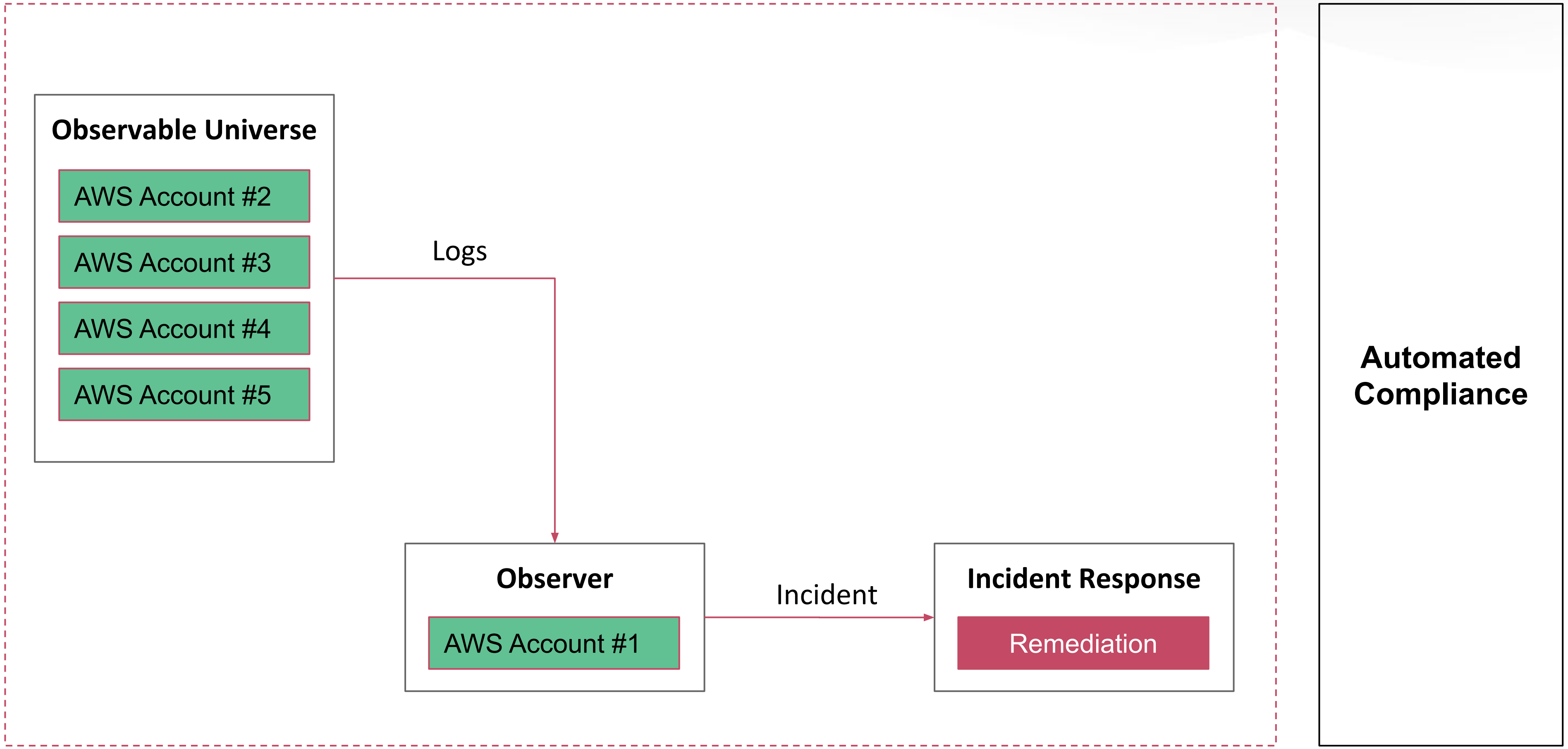
Opportunity #1 - Separation of Duties



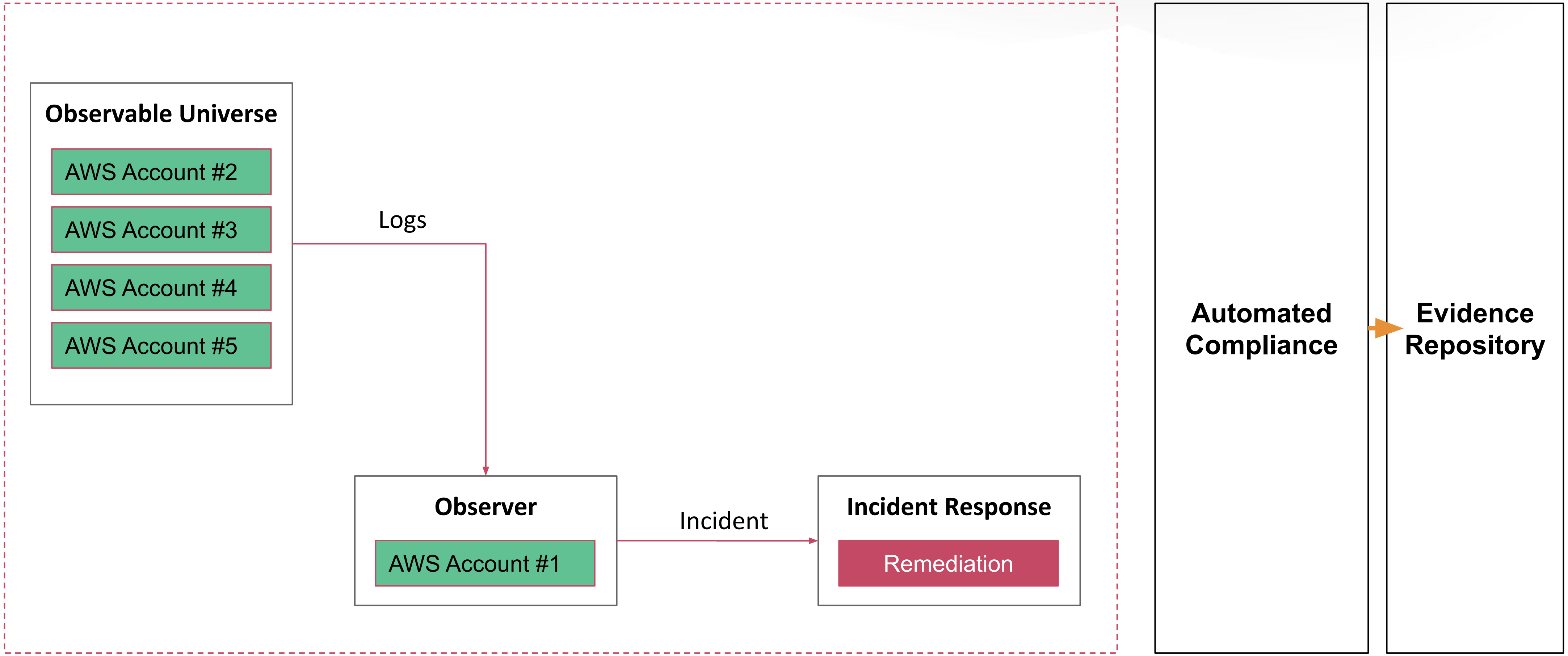
Opportunity #1 - Separation of Duties



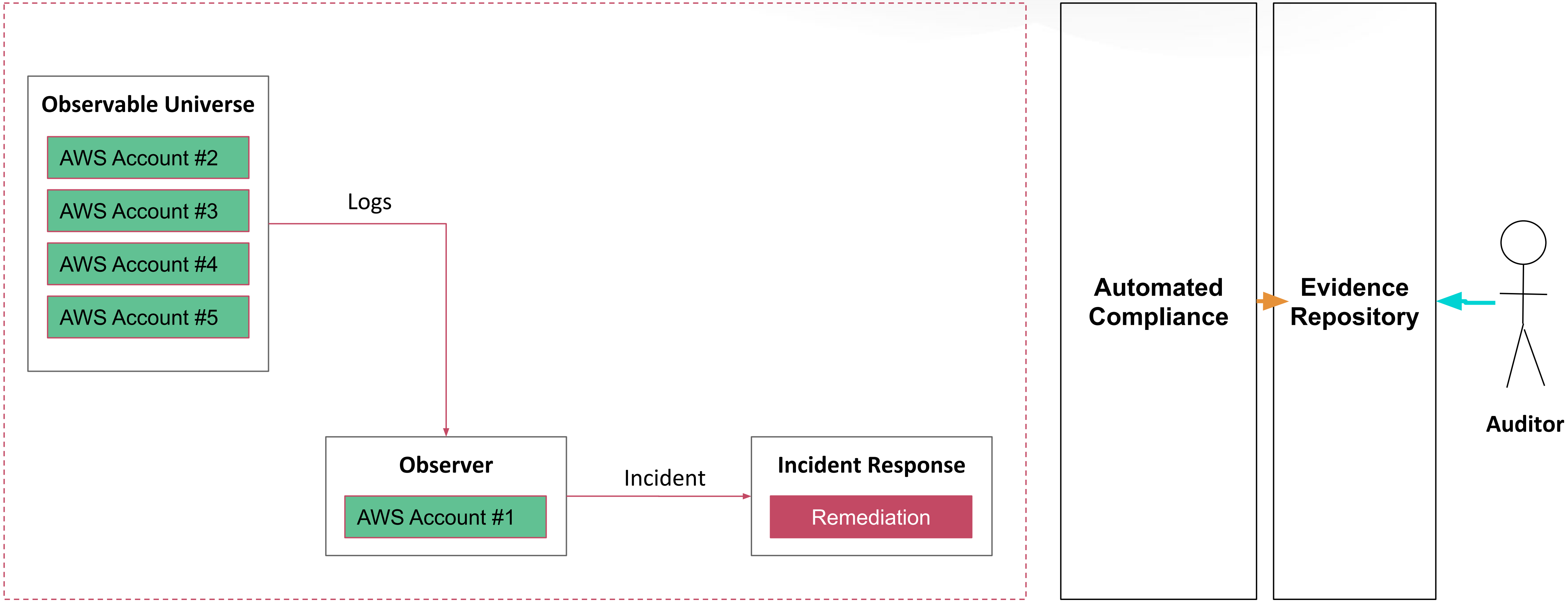
Opportunity #1 - Separation of Duties



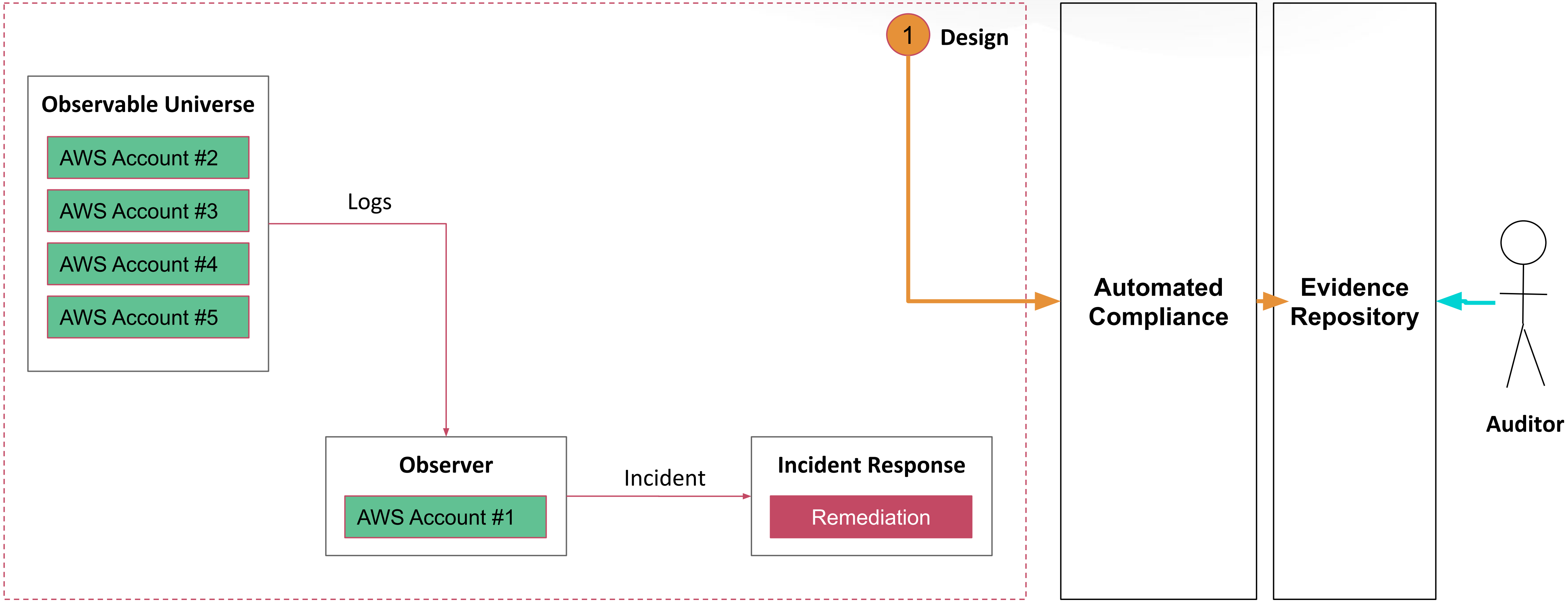
Opportunity #1 - Separation of Duties



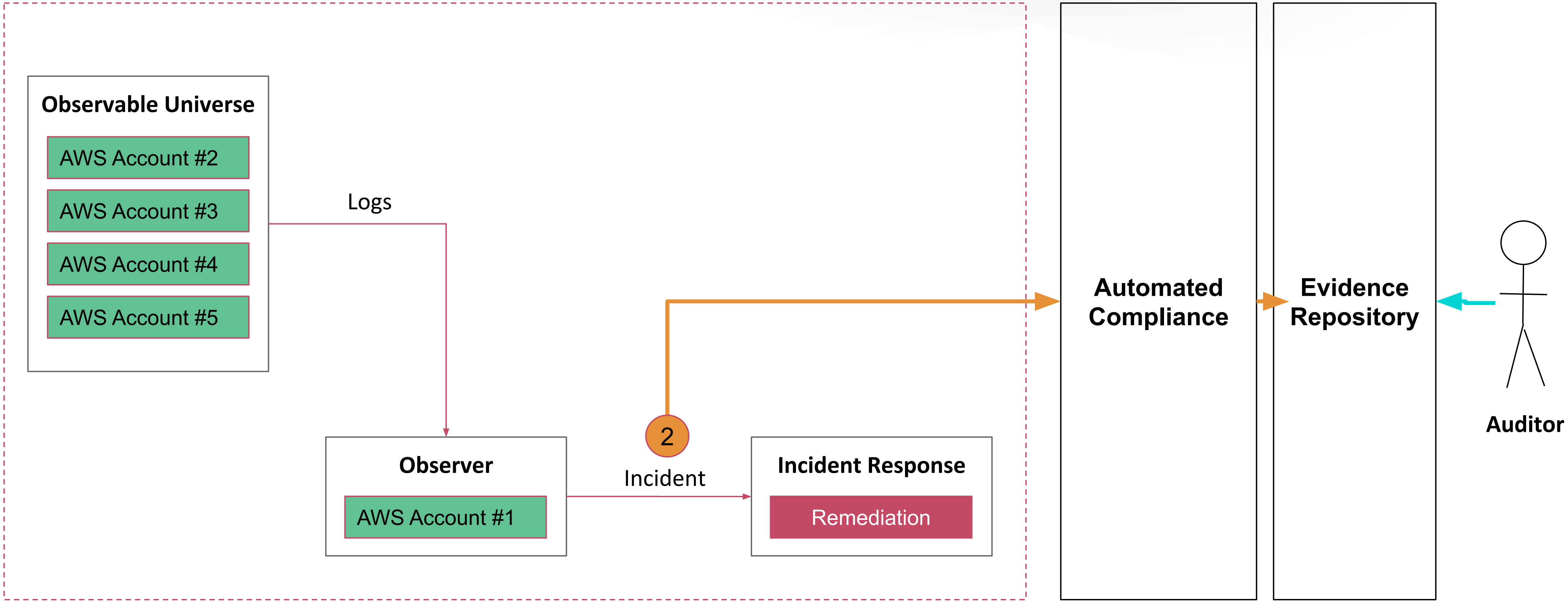
Opportunity #1 - Separation of Duties



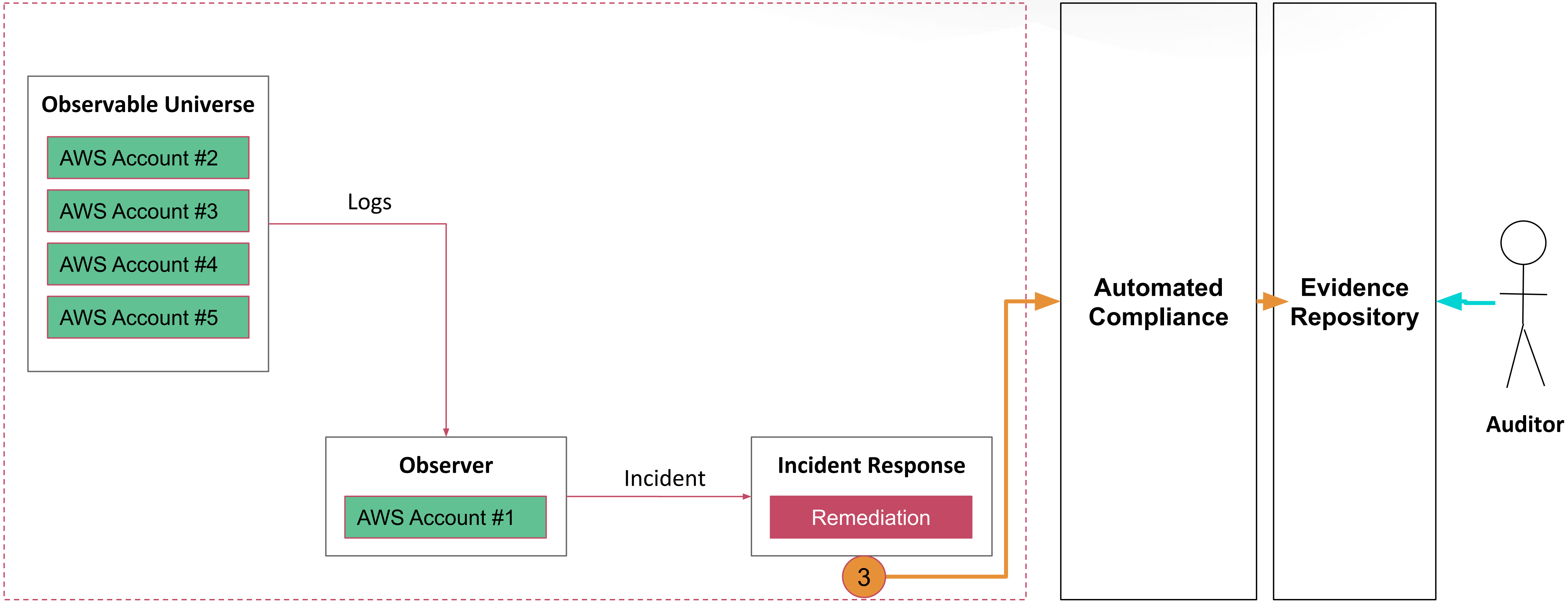
Opportunity #1 - Separation of Duties



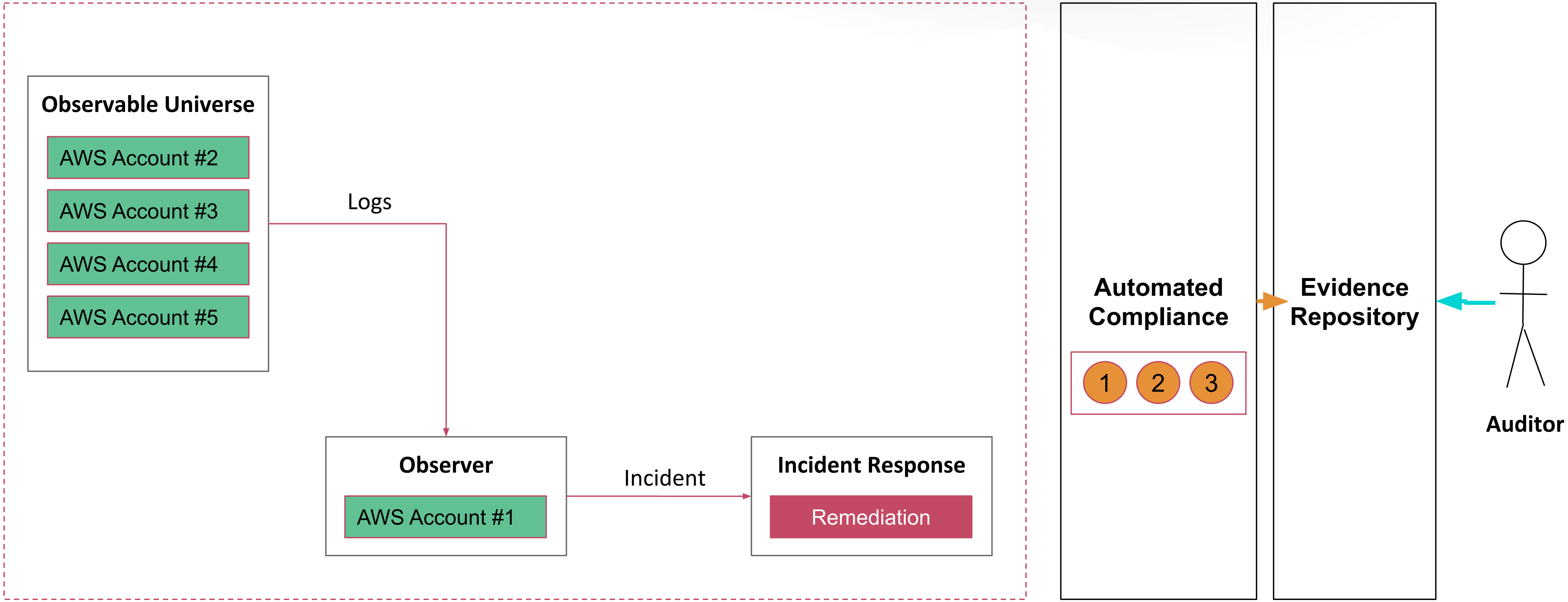
Opportunity #1 - Separation of Duties



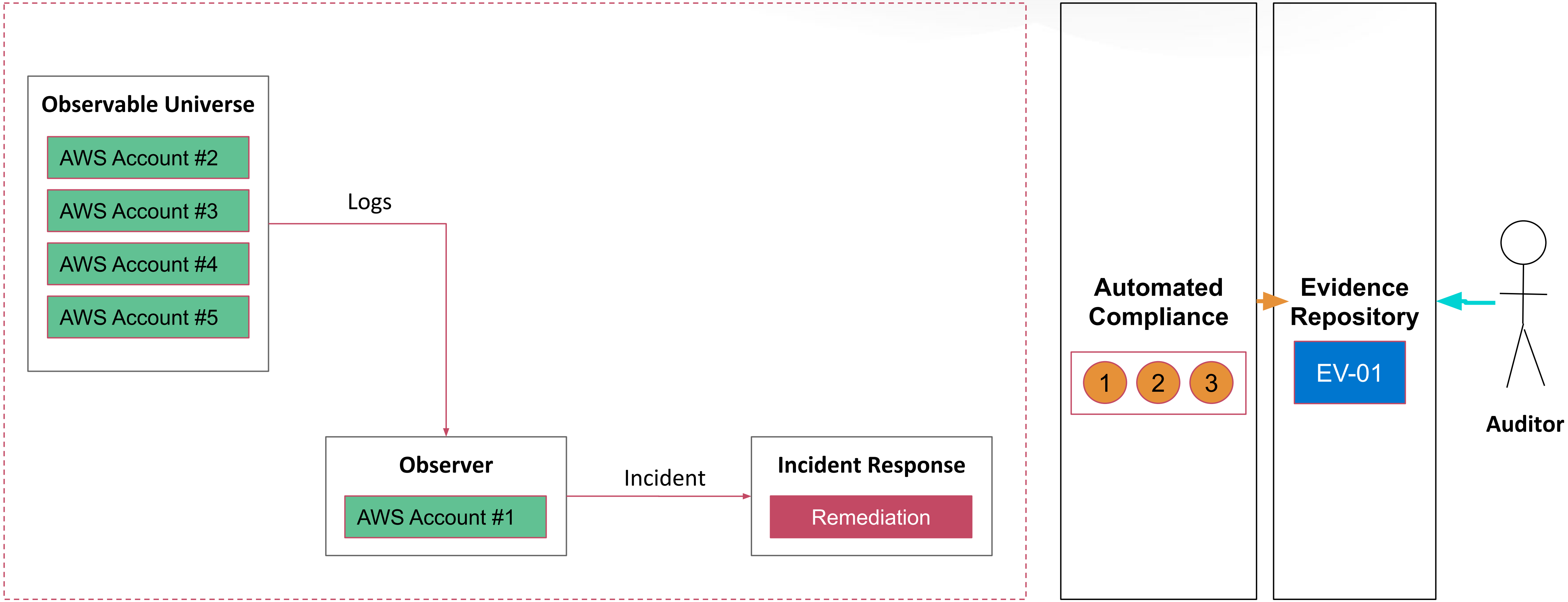
Opportunity #1 - Separation of Duties



Opportunity #1 - Separation of Duties



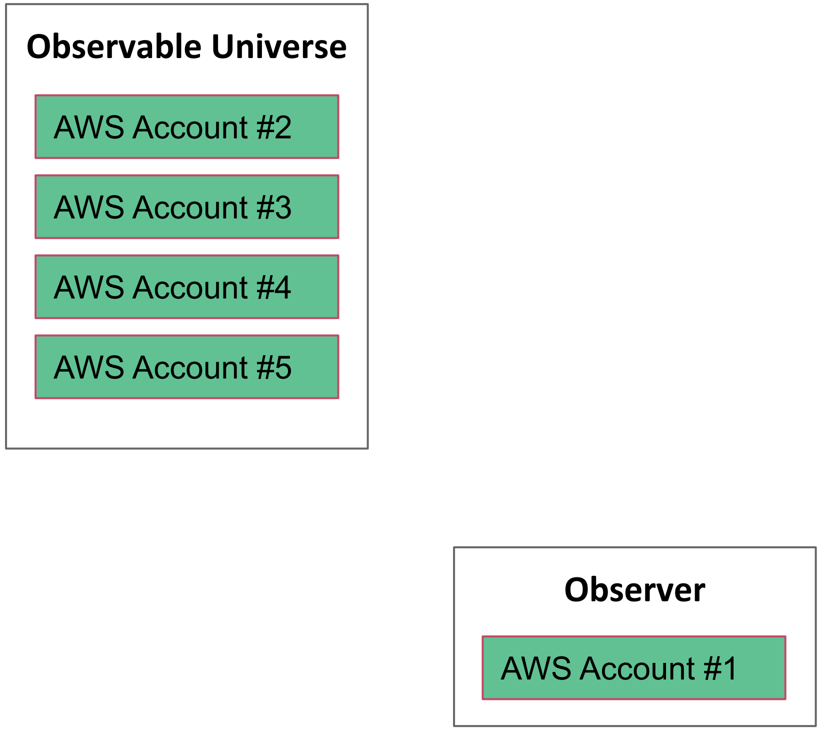
Opportunity #1 - Separation of Duties



RSAConference2020

Opportunity #2 - Change Management

Opportunity #2 - Change Management



Observable Universe

AWS Account #2

AWS Account #3

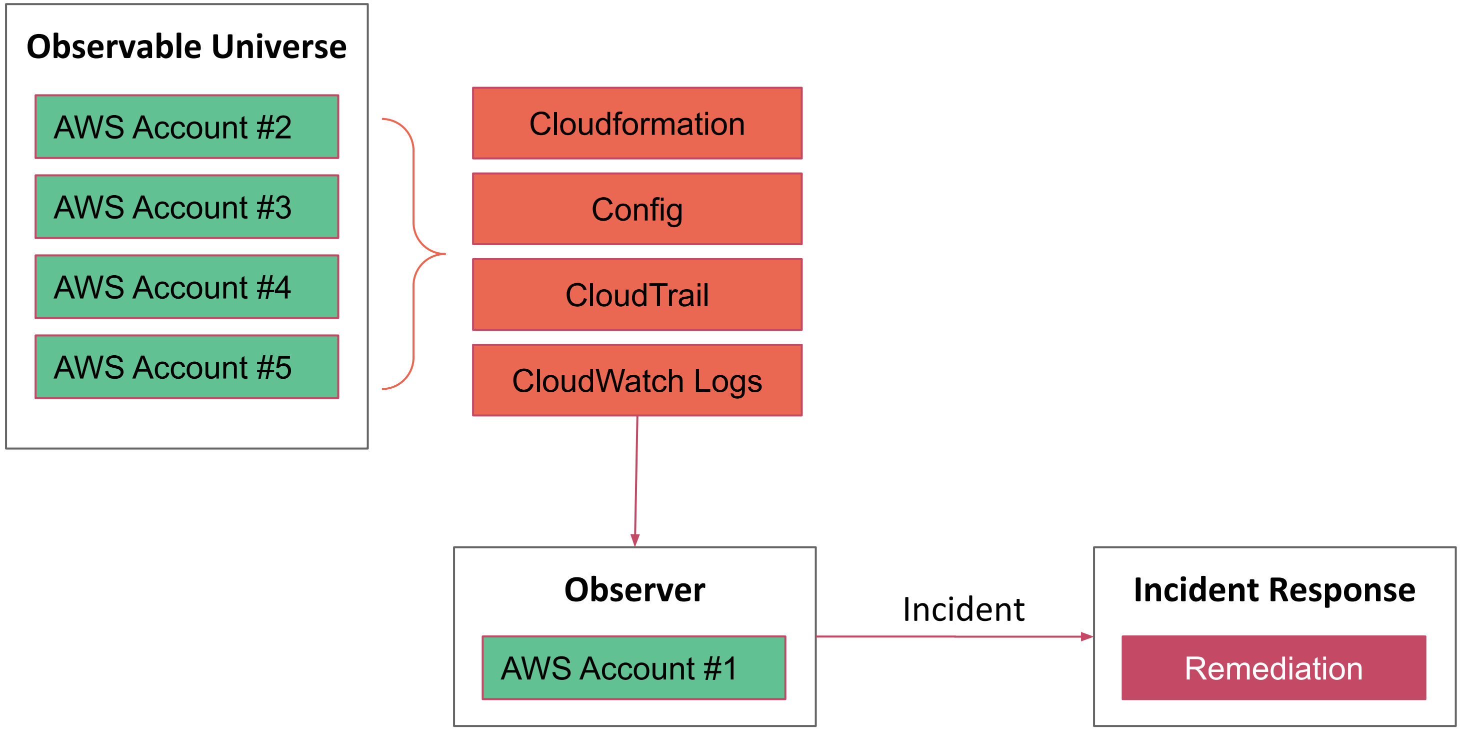
AWS Account #4

AWS Account #5

Observer

AWS Account #1

Opportunity #2 - Change Management



Observable Universe

AWS Account #2

AWS Account #3

AWS Account #4

AWS Account #5

Cloudformation

Config

CloudTrail

CloudWatch Logs

Observer

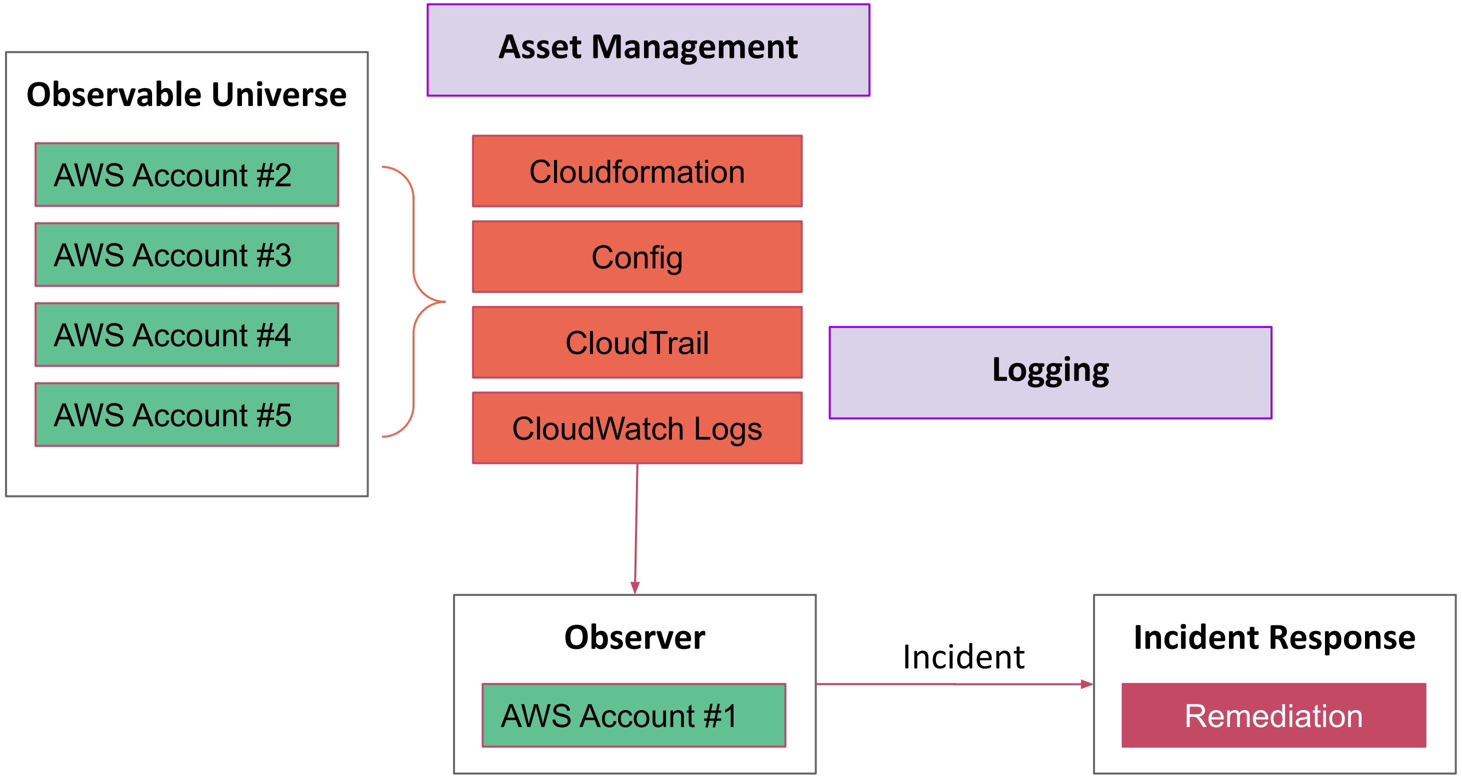
AWS Account #1

Incident

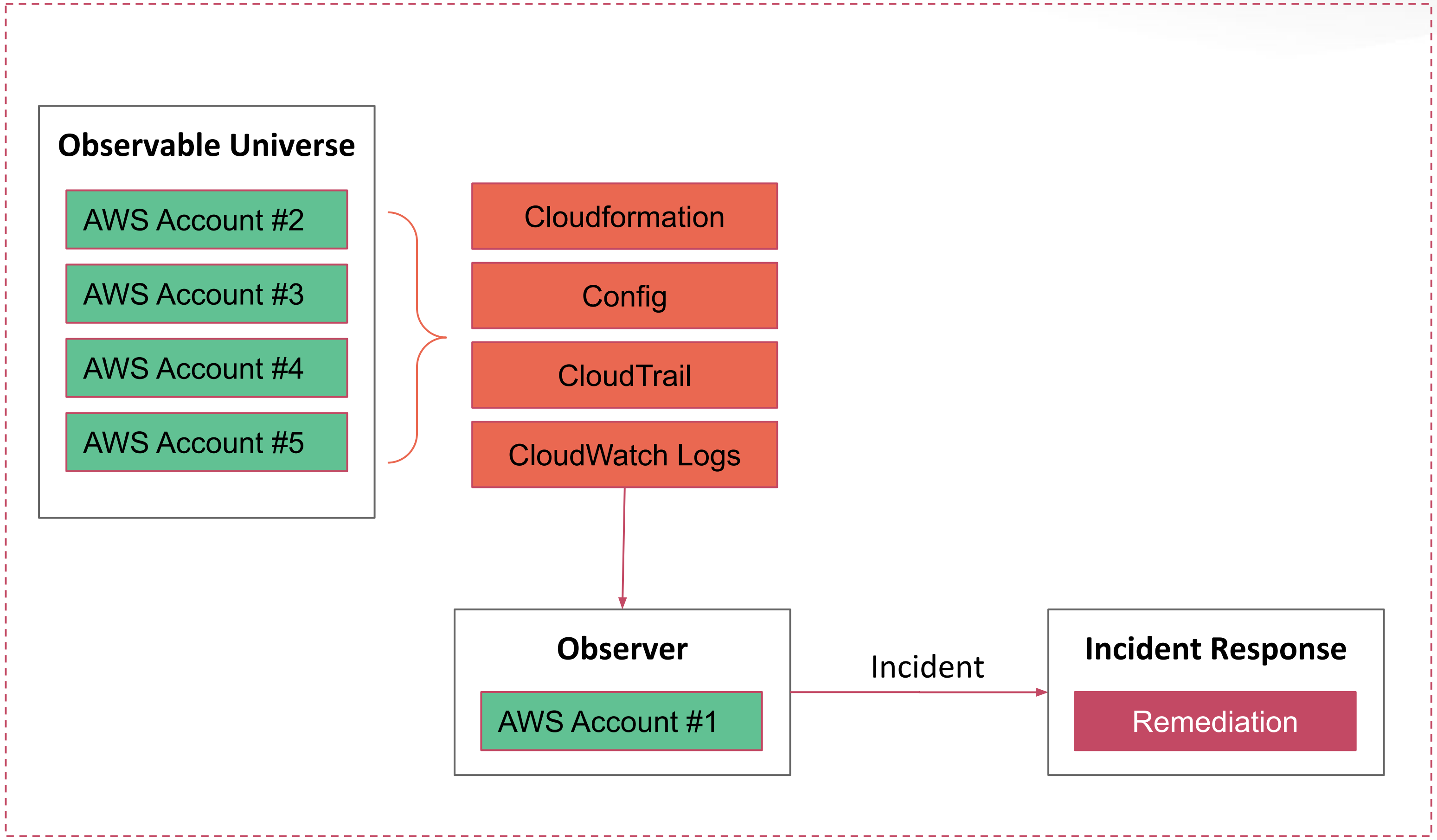
Incident Response

Remediation

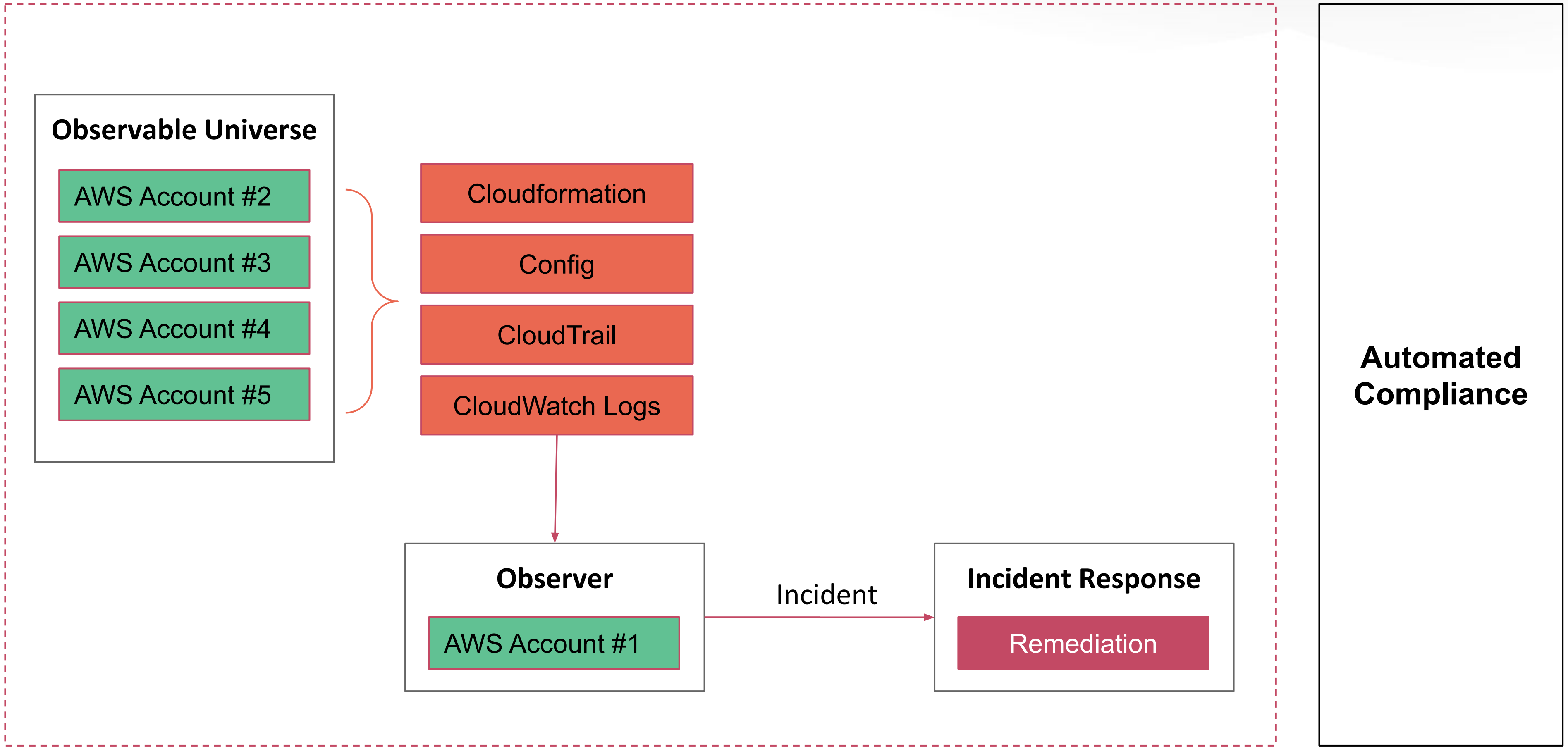
Opportunity #2 - Change Management



Opportunity #2 - Change Management



Opportunity #2 - Change Management



Observable Universe

AWS Account #2

AWS Account #3

AWS Account #4

AWS Account #5

Cloudformation

Config

CloudTrail

CloudWatch Logs

Observer

AWS Account #1

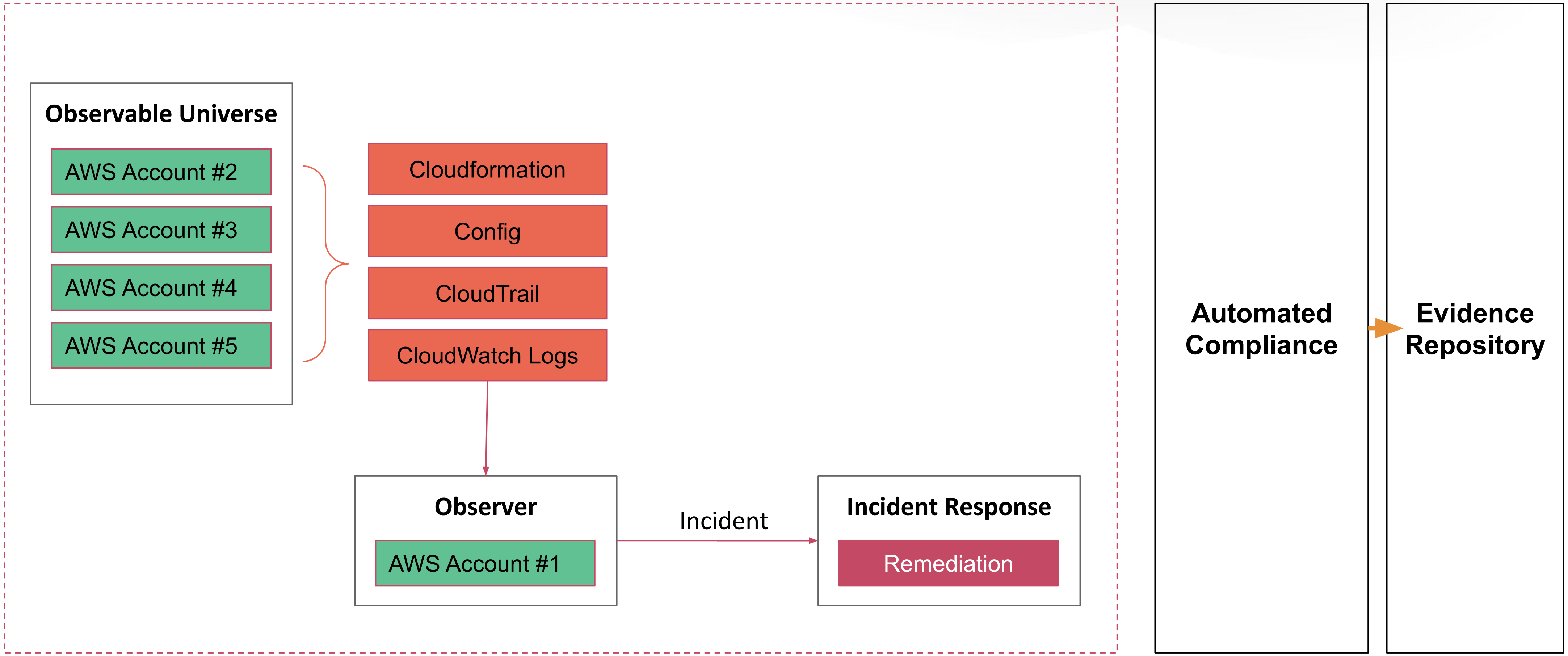
Incident

Incident Response

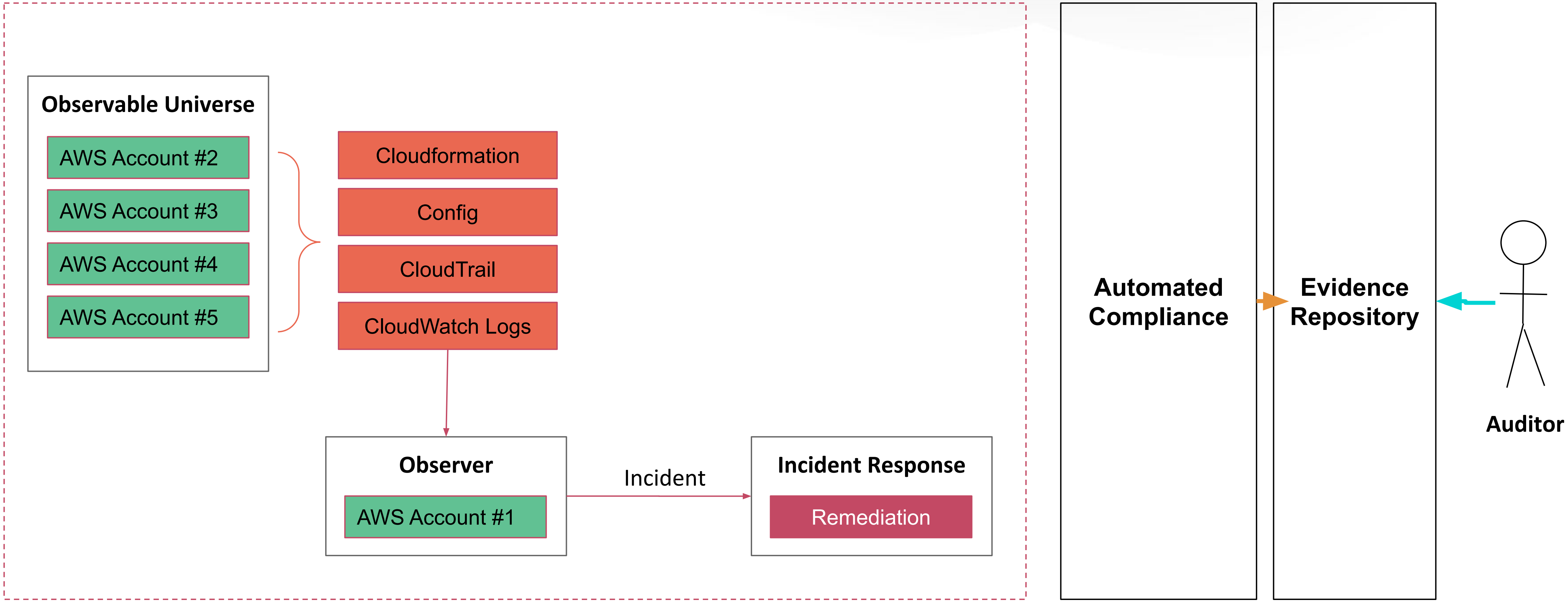
Remediation

Automated Compliance

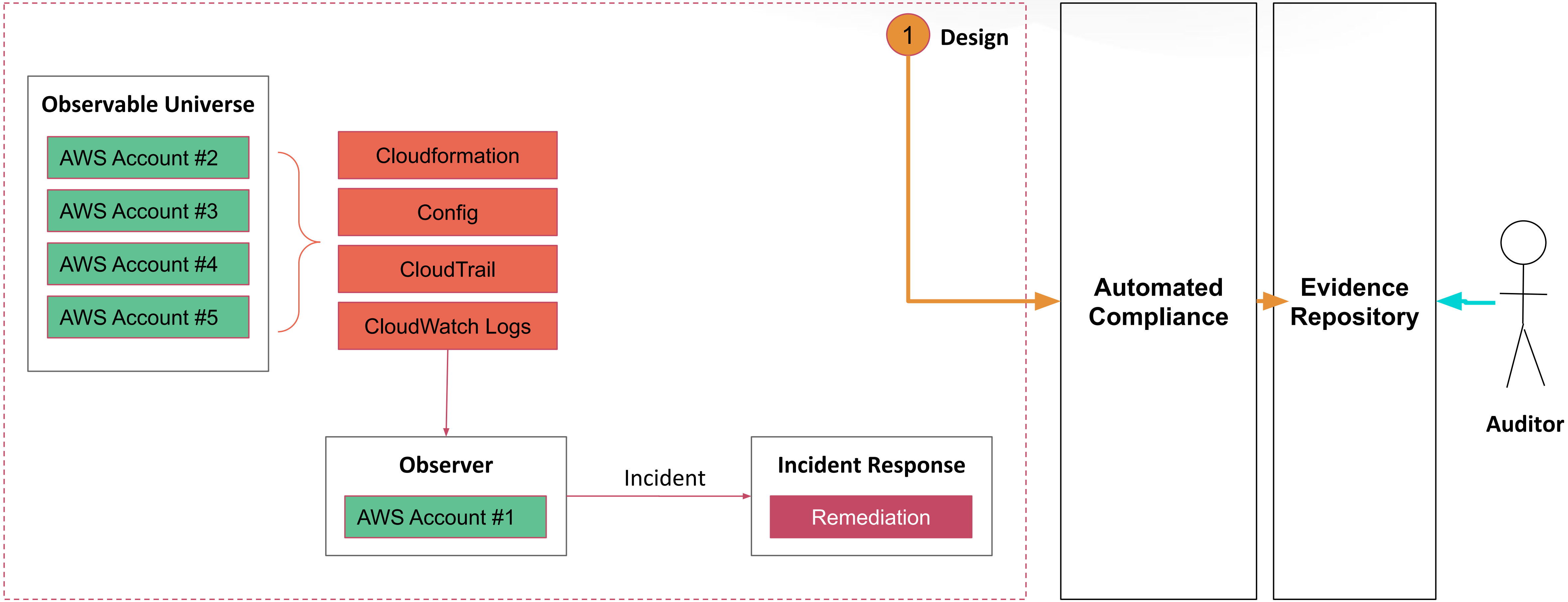
Opportunity #2 - Change Management



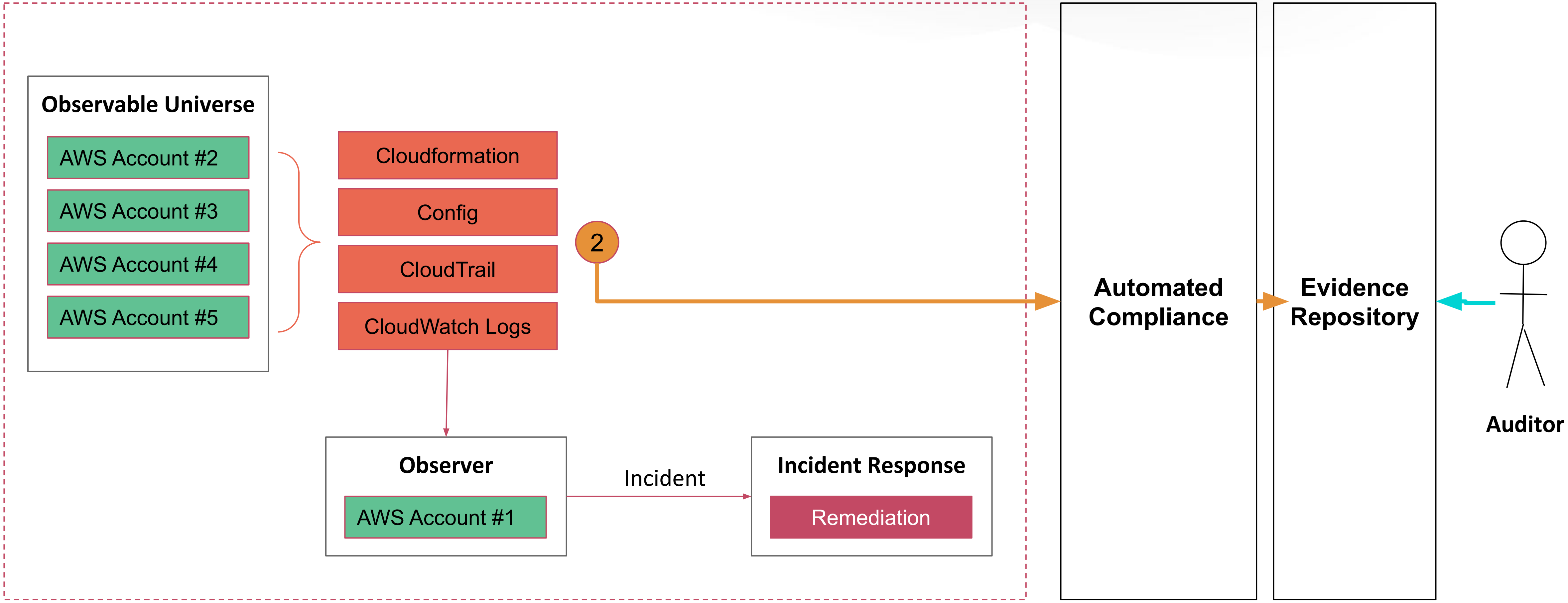
Opportunity #2 - Change Management



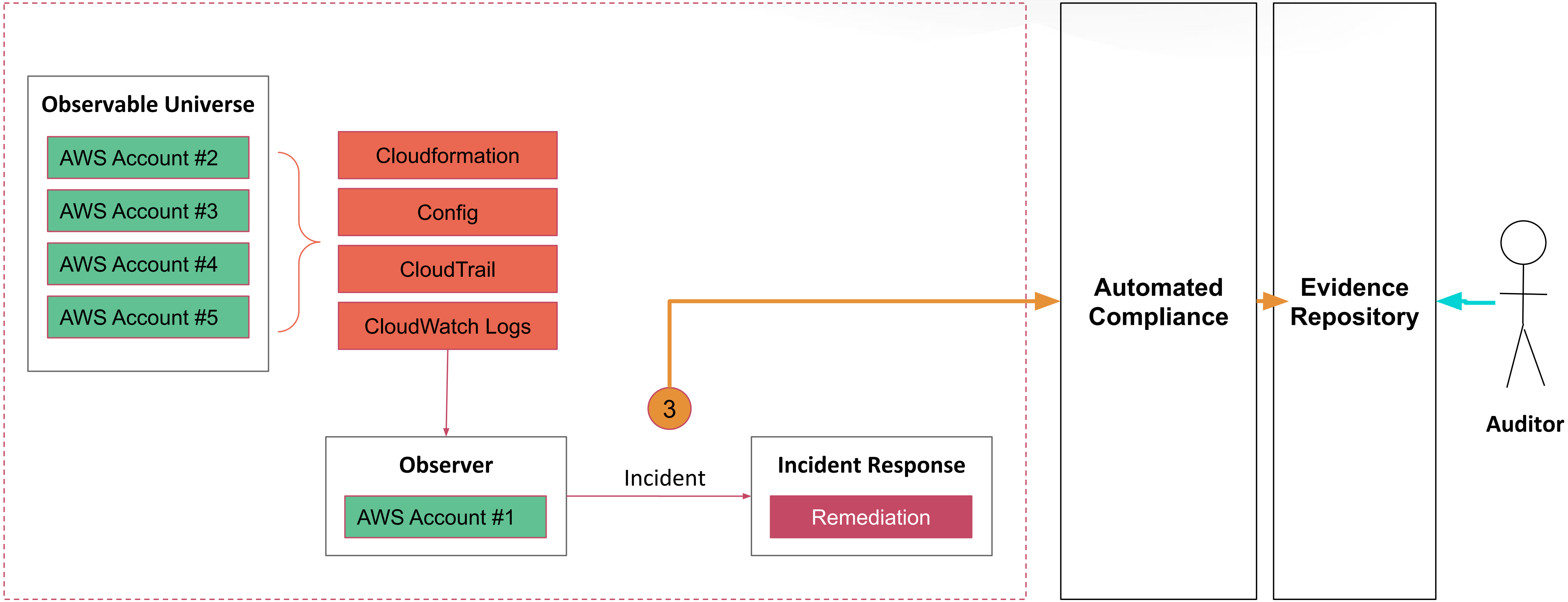
Opportunity #2 - Change Management



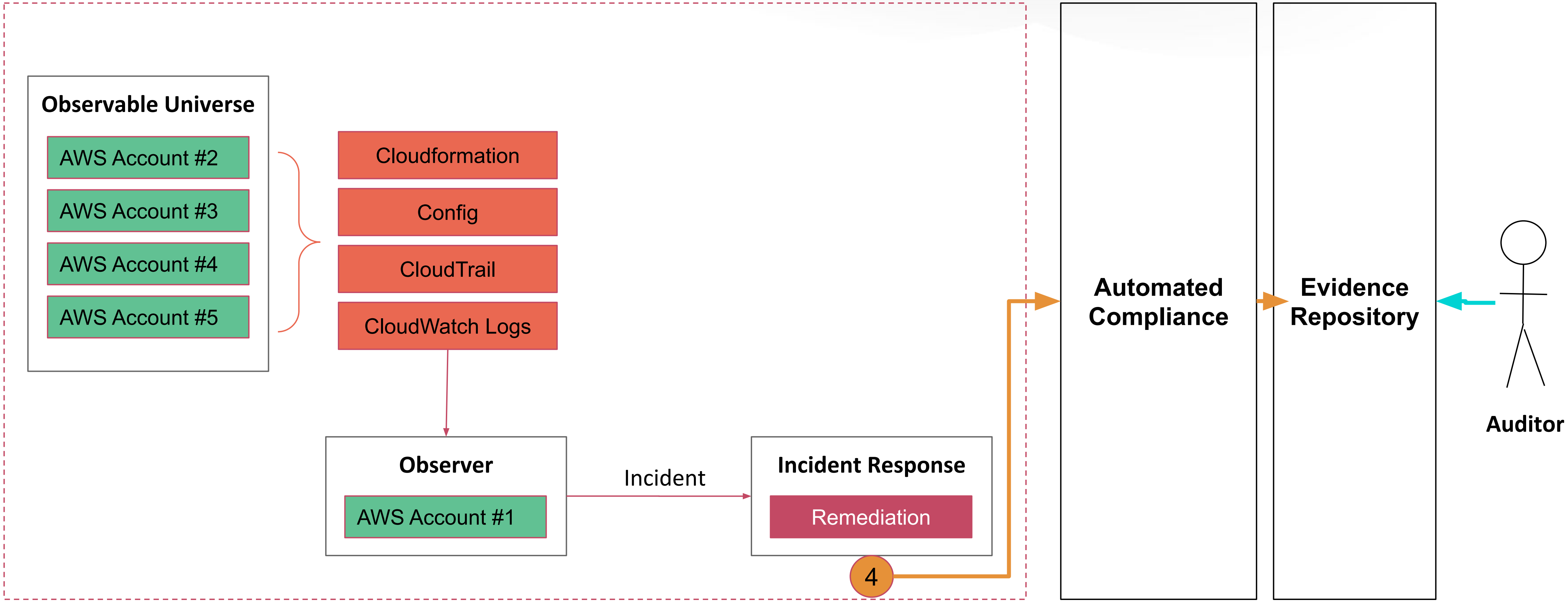
Opportunity #2 - Change Management



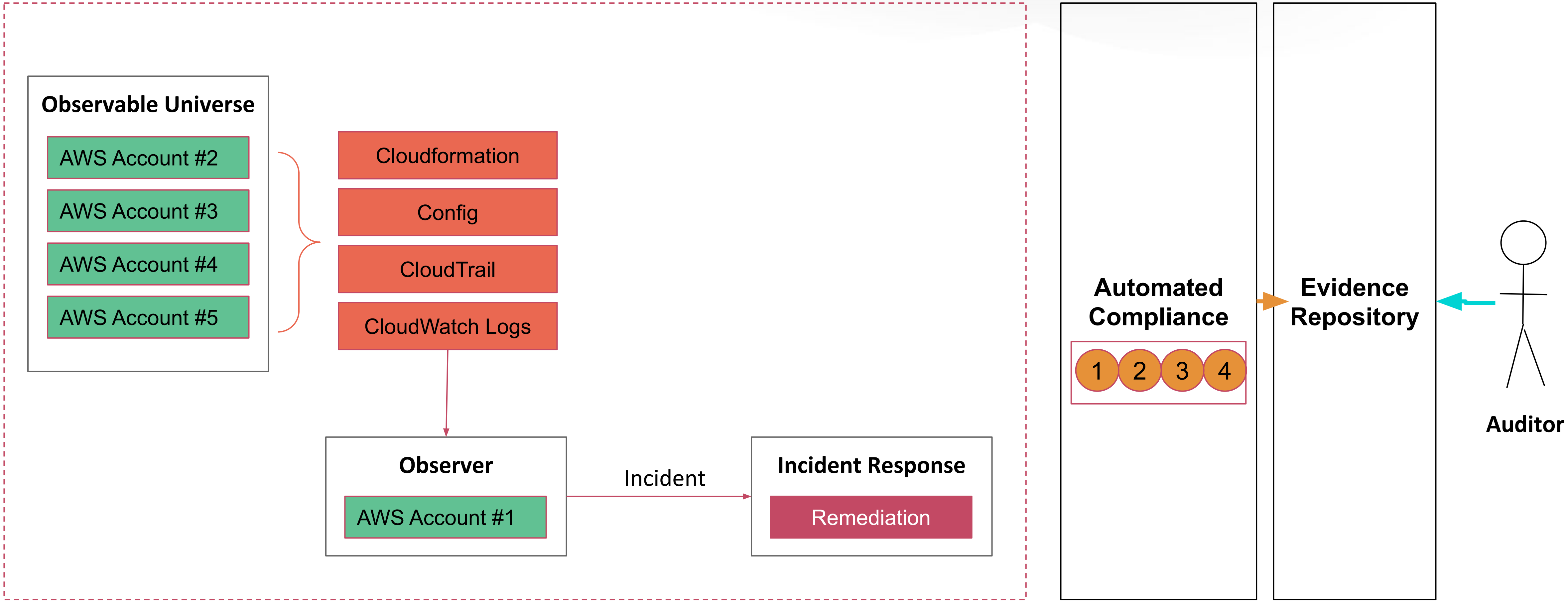
Opportunity #2 - Change Management



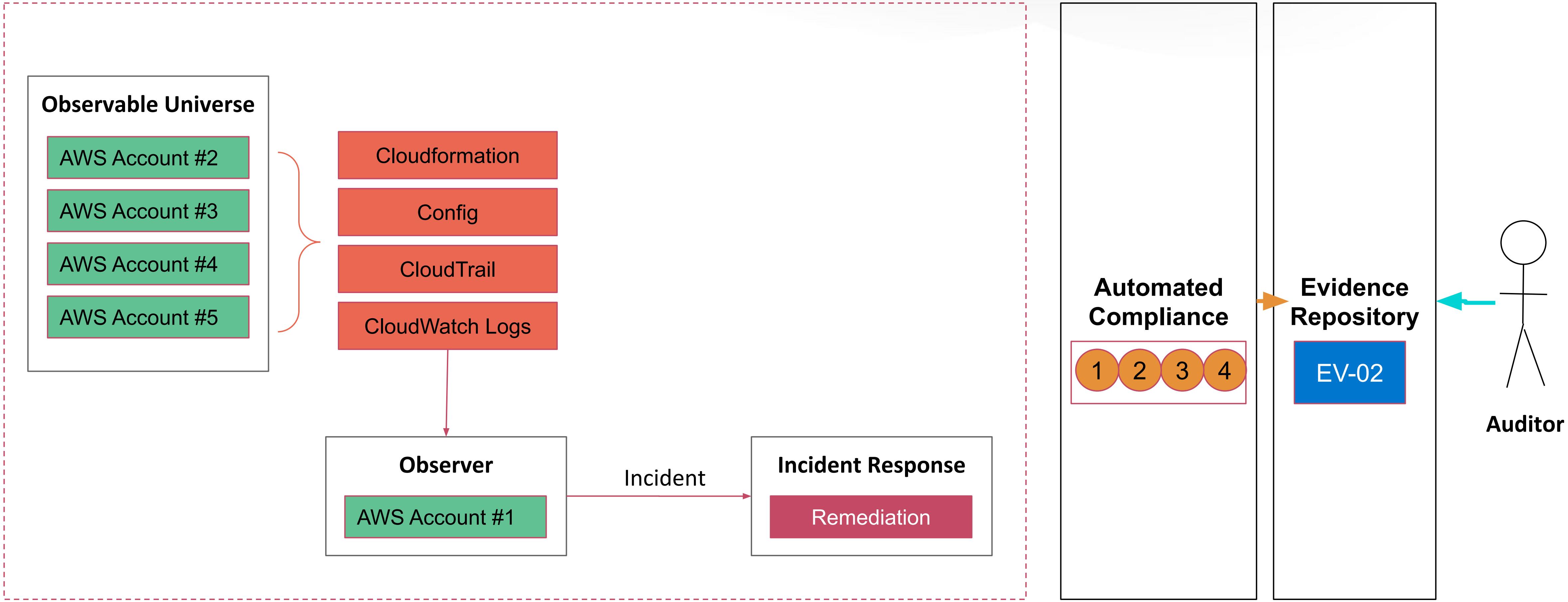
Opportunity #2 - Change Management



Opportunity #2 - Change Management



Opportunity #2 - Change Management



Observable Universe

AWS Account #2

AWS Account #3

AWS Account #4

AWS Account #5

Cloudformation

Config

CloudTrail

CloudWatch Logs

Observer

AWS Account #1

Incident

Incident Response

Remediation

Automated Compliance

1 2 3 4

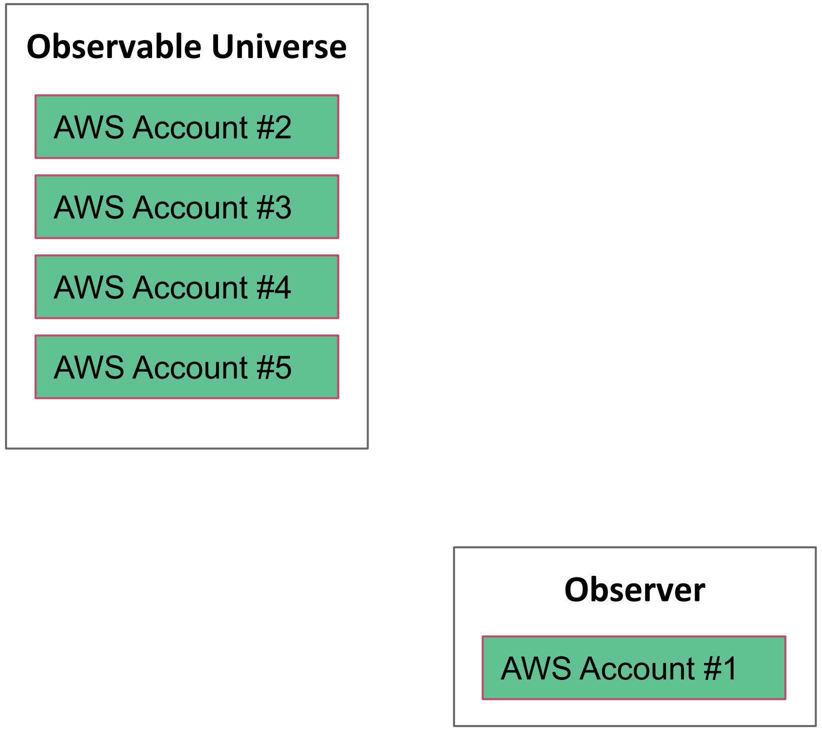
Evidence Repository

EV-02

Auditor

Opportunity #3 - Effectiveness Testing

Opportunity #3 - Effectiveness Testing



Observable Universe

AWS Account #2

AWS Account #3

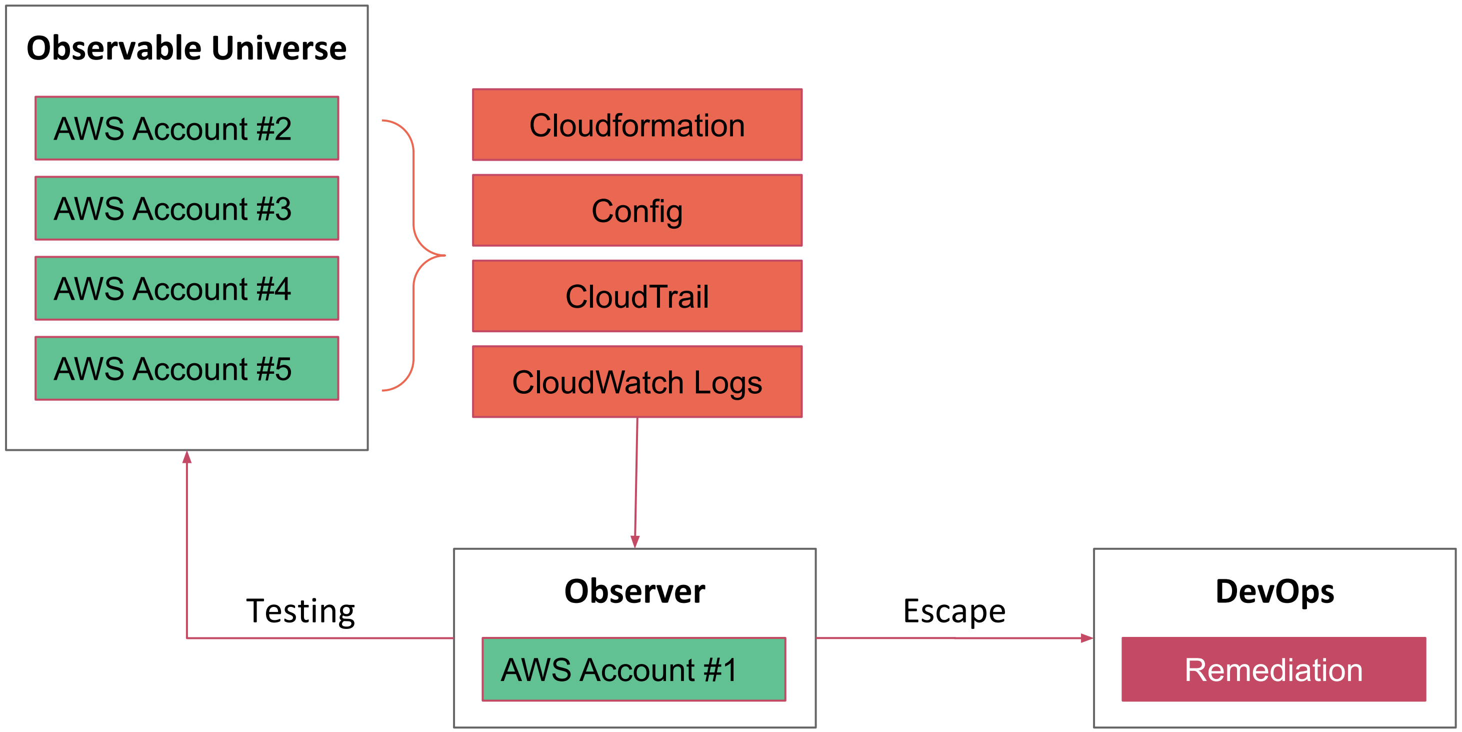
AWS Account #4

AWS Account #5

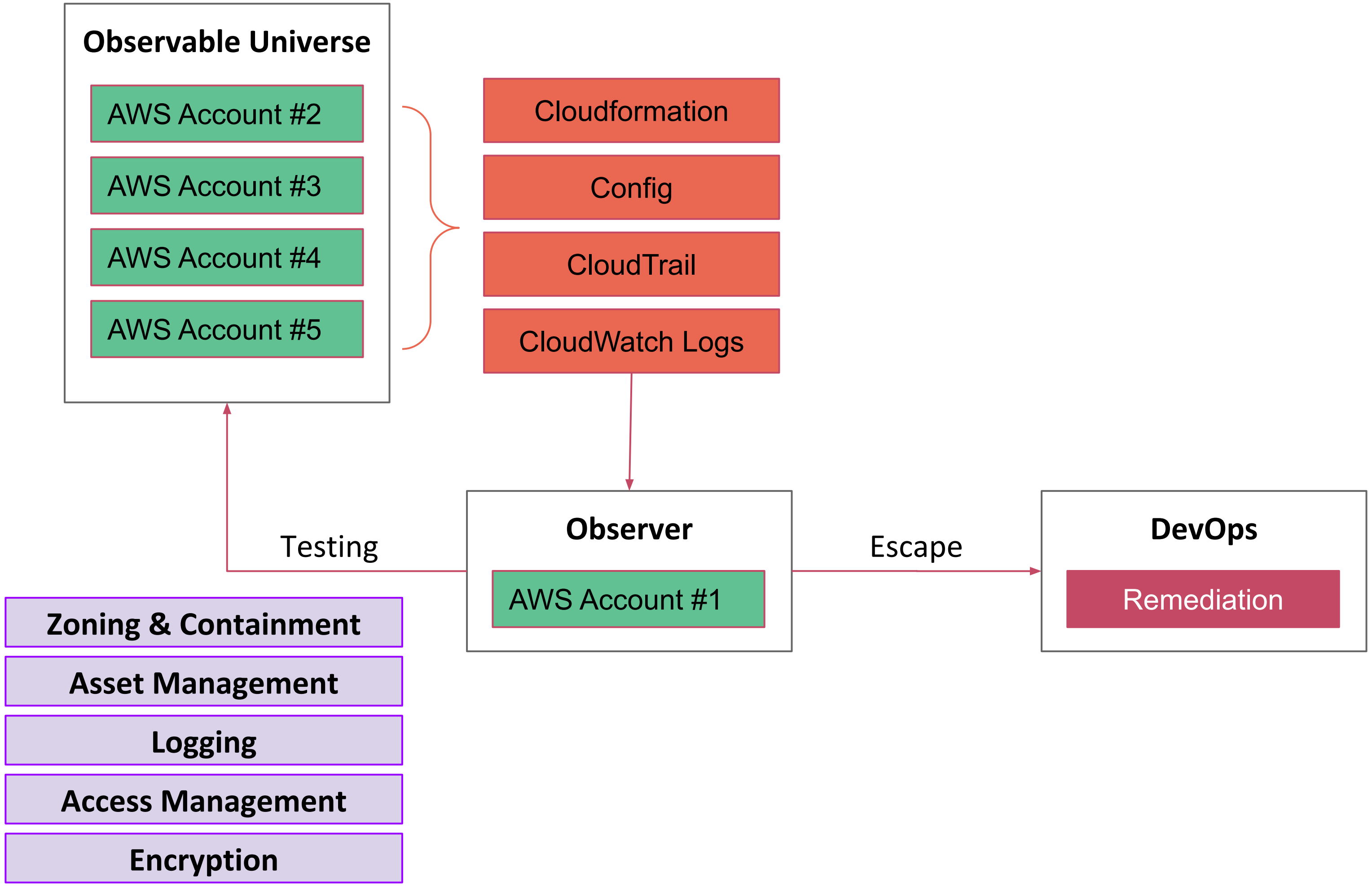
Observer

AWS Account #1

Opportunity #3 - Effectiveness Testing



Opportunity #3 - Effectiveness Testing



Observable Universe

AWS Account #2

AWS Account #3

AWS Account #4

AWS Account #5

Cloudformation

Config

CloudTrail

CloudWatch Logs

Testing

Observer

AWS Account #1

Escape

DevOps

Remediation

Zoning & Containment

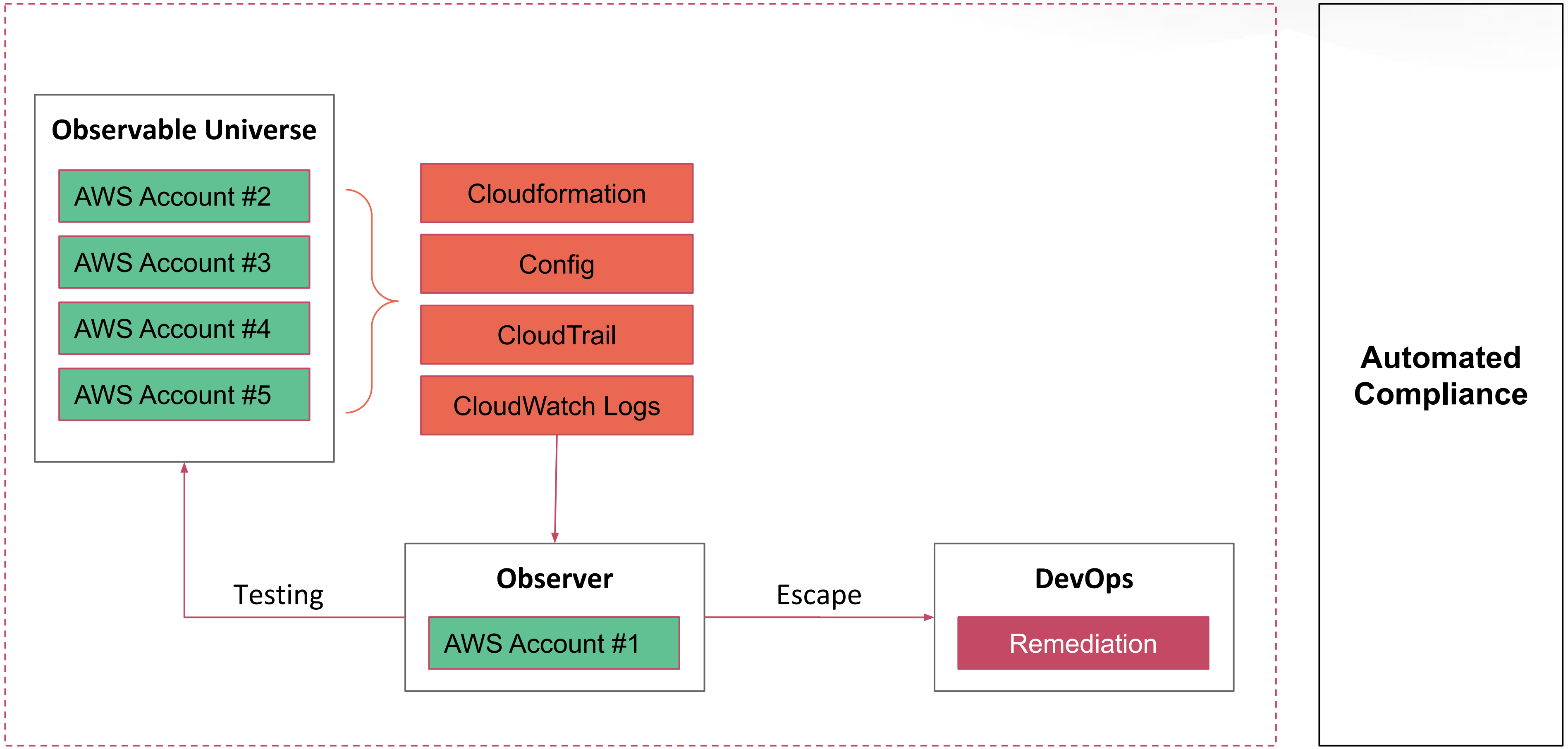
Asset Management

Logging

Access Management

Encryption

Opportunity #3 - Effectiveness Testing



Observable Universe

AWS Account #2

AWS Account #3

AWS Account #4

AWS Account #5

Cloudformation

Config

CloudTrail

CloudWatch Logs

Testing

Observer

AWS Account #1

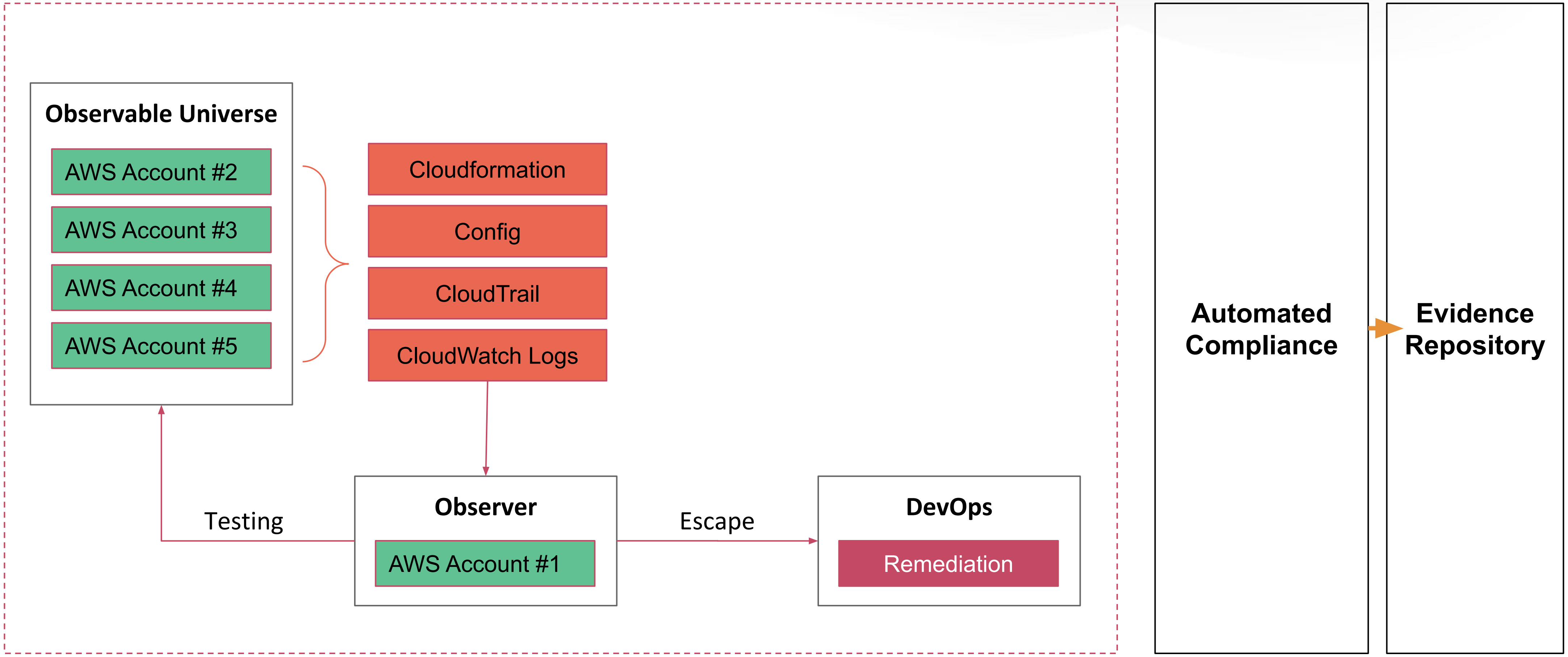
Escape

DevOps

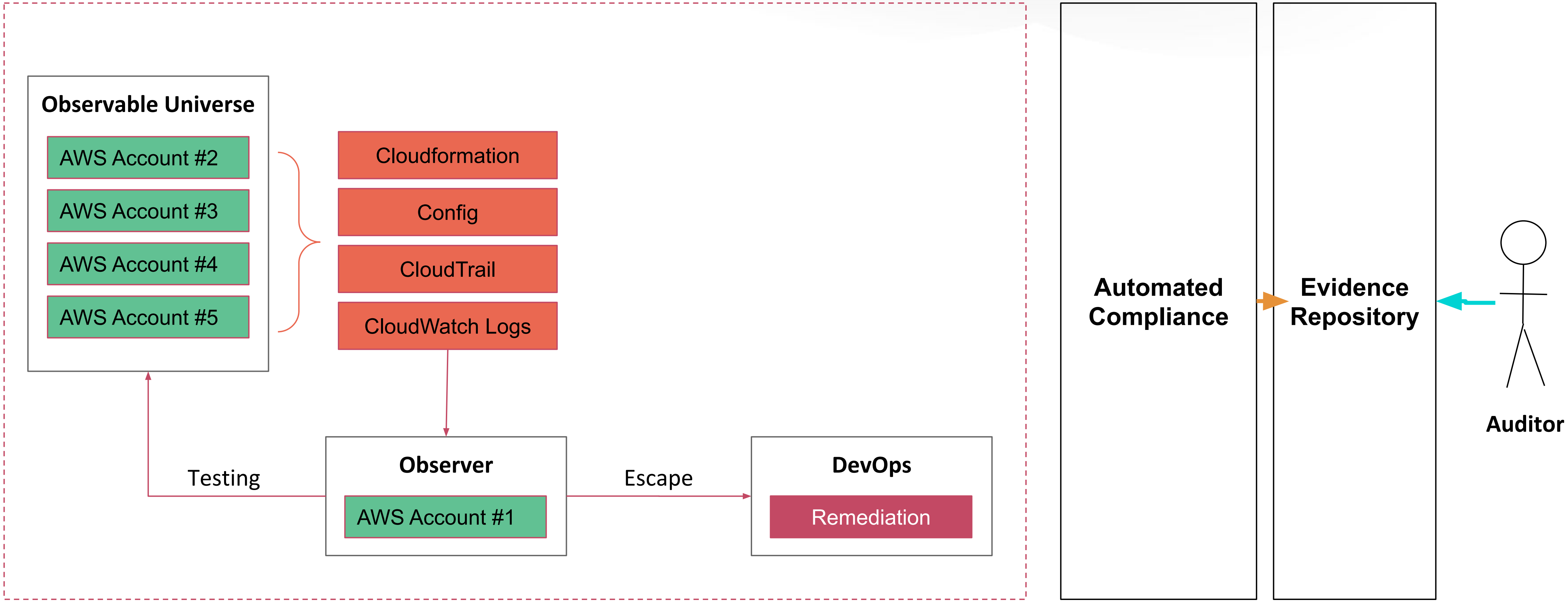
Remediation

Automated Compliance

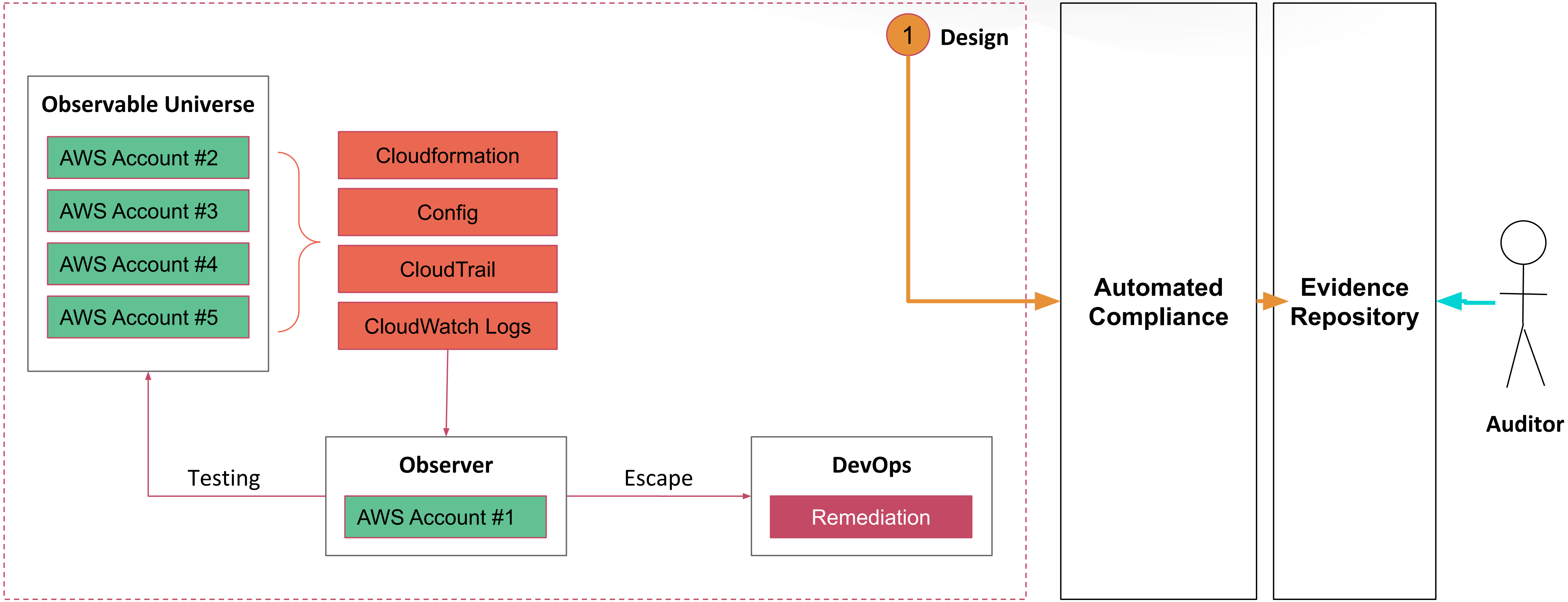
Opportunity #3 - Effectiveness Testing



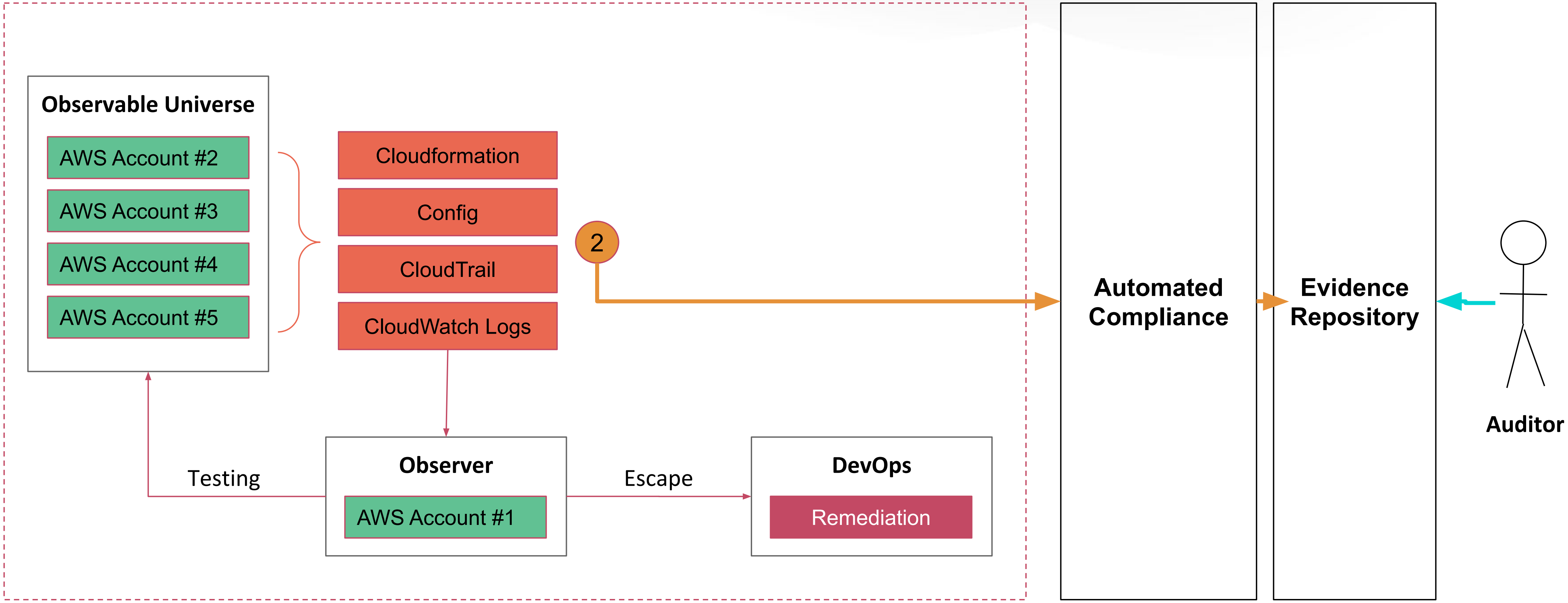
Opportunity #3 - Effectiveness Testing



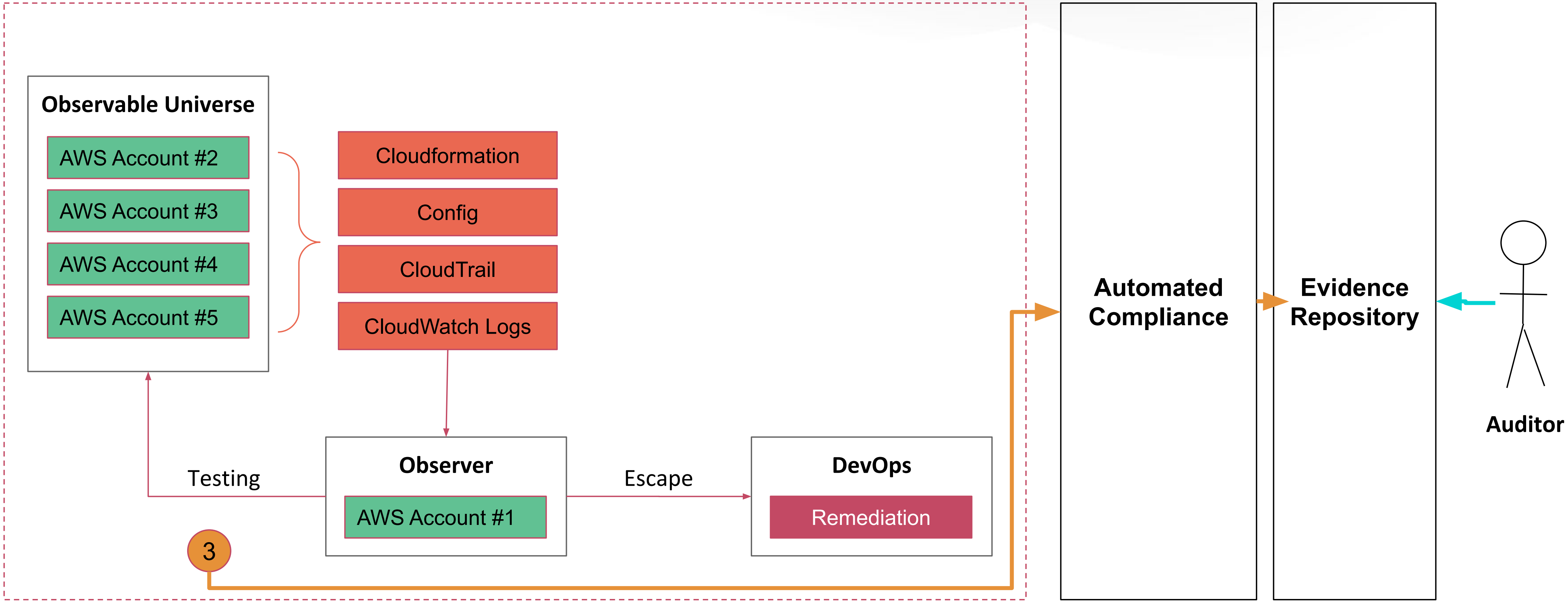
Opportunity #3 - Effectiveness Testing



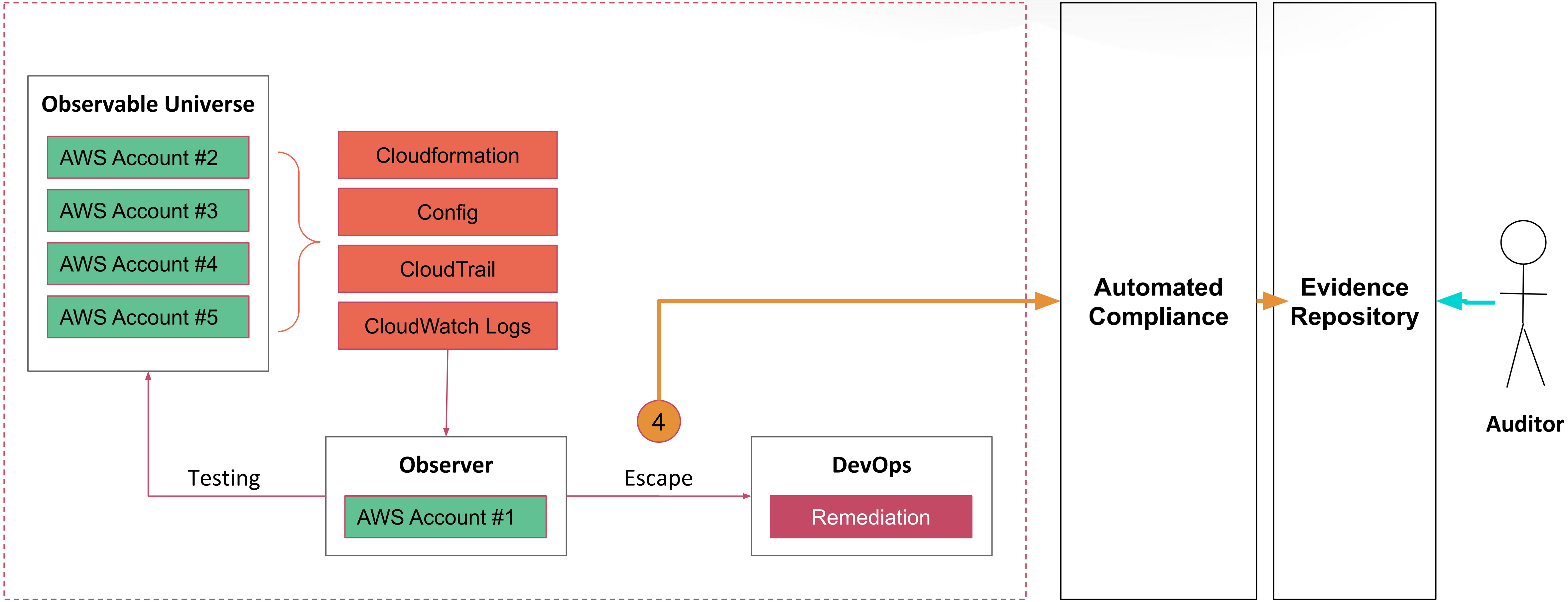
Opportunity #3 - Effectiveness Testing



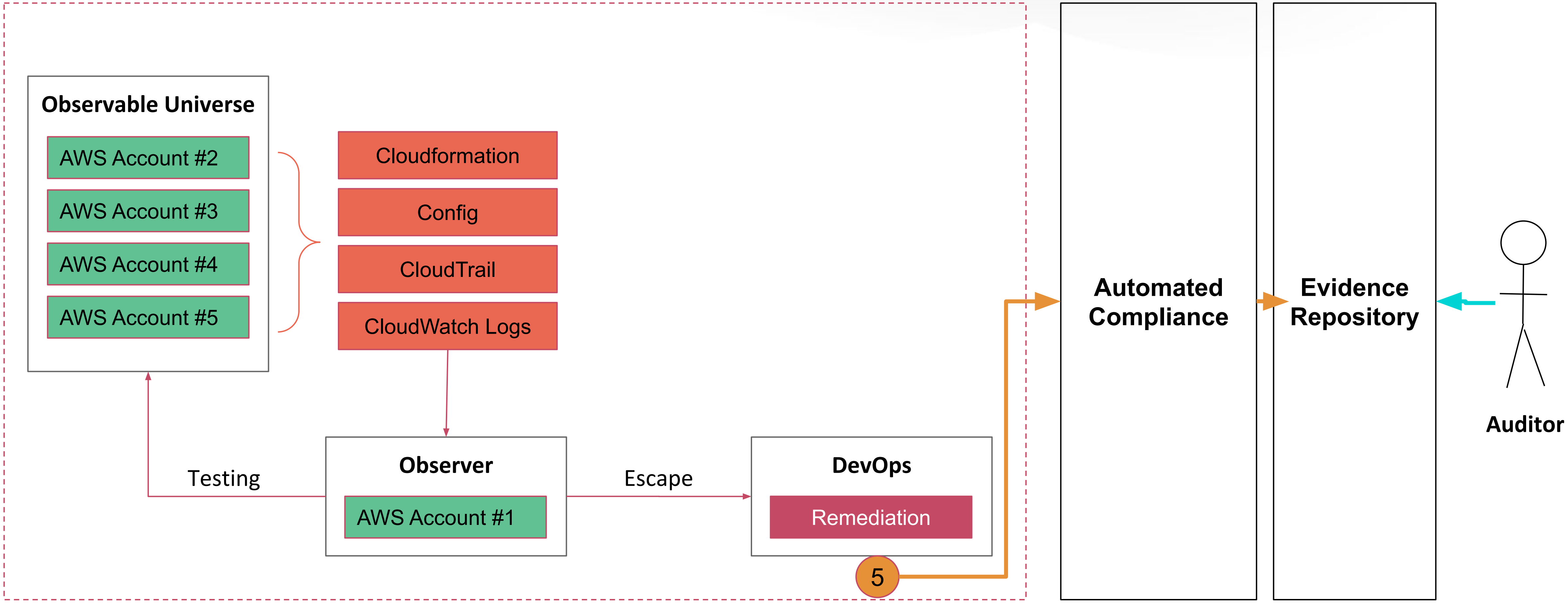
Opportunity #3 - Effectiveness Testing



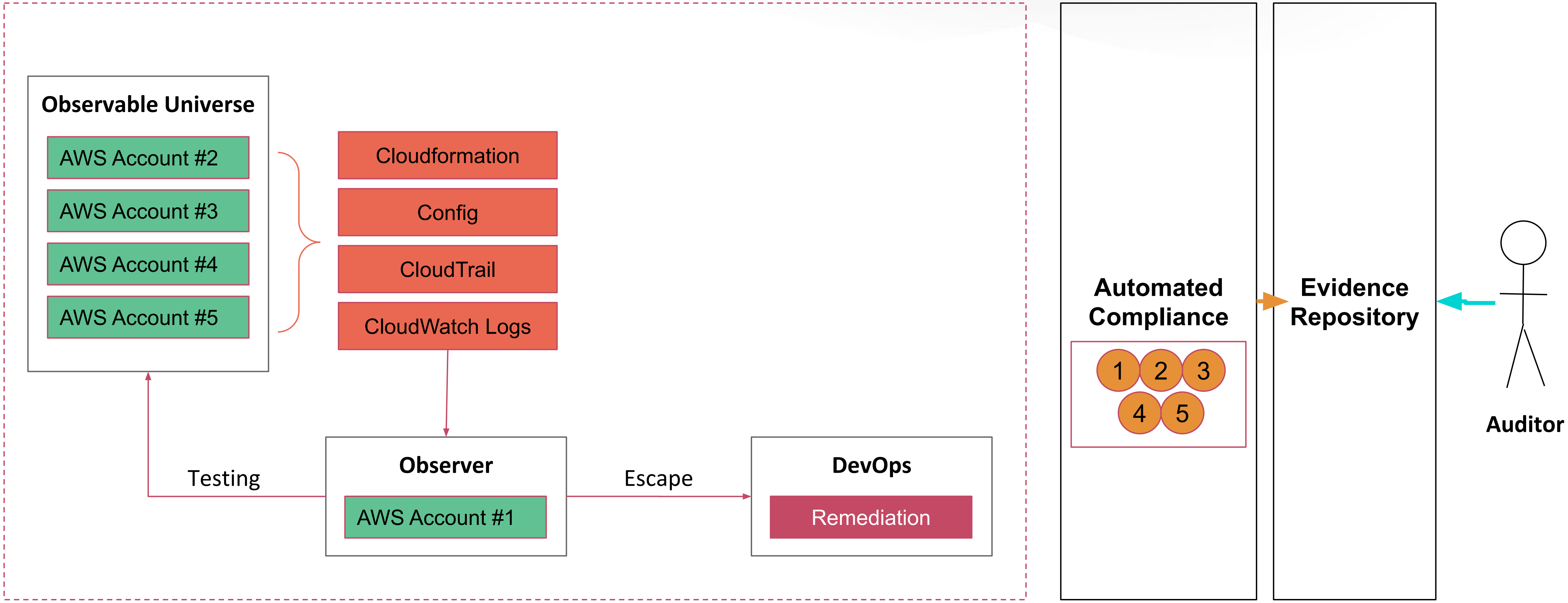
Opportunity #3 - Effectiveness Testing



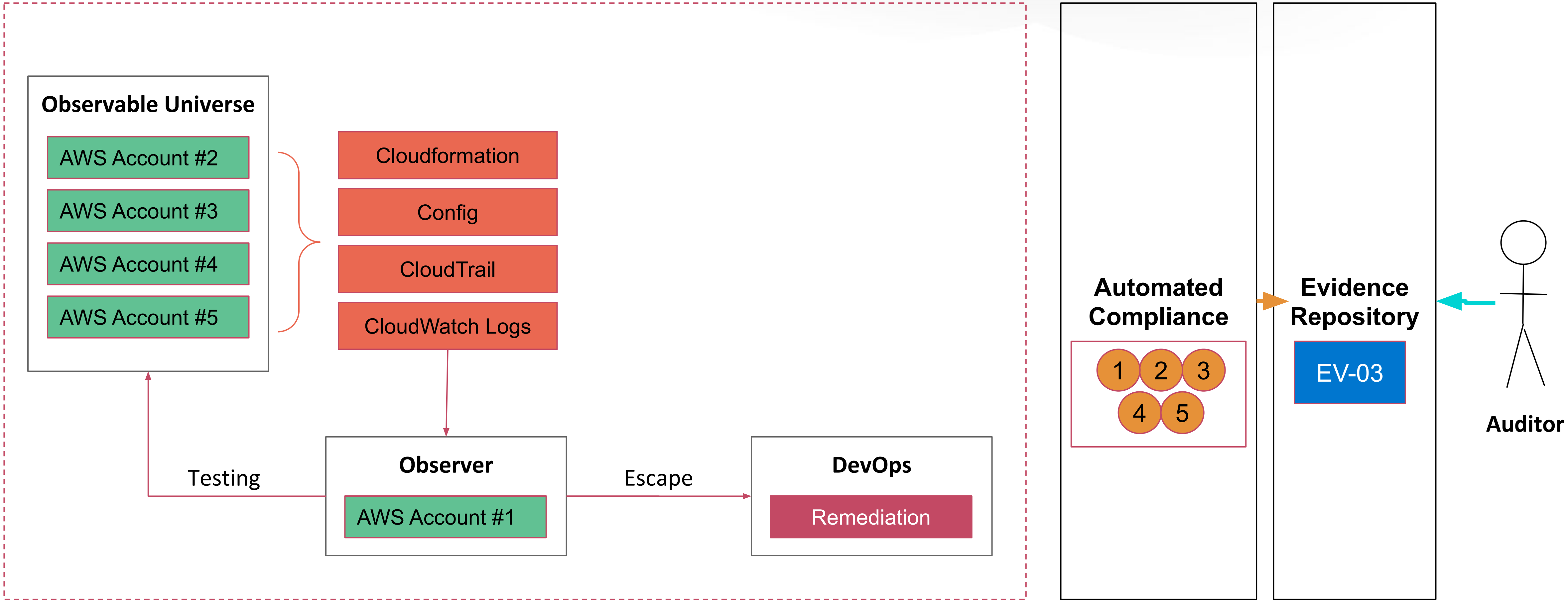
Opportunity #3 - Effectiveness Testing



Opportunity #3 - Effectiveness Testing



Opportunity #3 - Effectiveness Testing



“Apply” Slide

- **Next Week**
  - Evaluate your environment and look for opportunities to automate evidence collection
  - Look for DevOps risks you want to solve for
- **Next 90 Days**
  - Build 1 automated control and store evidence in an online repo
  - Work with your auditor to understand what they want so that patterns can be developed
- **This Year**
  - Inventory your controls and line them up for compliance by design to be consumed
  - Build a control pipeline and automate collection of evidence

RSAConference2020

dso.to/automated-compliance

dso.to/transformed

dso.to/rsa-spar-2020