Confronting Ransomware:
Six Habits of Highly Effective Threat Detection/Incident Response Teams

Merritt Baer
Principal, Office of the CISO
merrbaer@amazon.com
@merrittbaer (twitter)

Megan O'Neil
Senior Security Specialist SA
megoneil@amazon.com

Best Practices for Ransomware (and everything else…)

1. Governance, guardrails, and democratization
2. Have a strategy for logging
3. Operationalize your insights
4. Runbooks, playbooks, and tabletop exercises
5. Canaries, validation, and sandboxes
6. Automation throughout your TDIR* lifecycle

*Threat Detection and Incident Response

How did we get here?

PANAMA 1989

Habit 1: Governance, guardrails, and democratization

> **Make the secure thing to do, the easy thing to do—and that is hard.**

AWS Security

Governance, guardrails, and democratization: a non-exhaustive guide!

Governance

How your organization knows assets, enacts policies, and controls change management over time.

Metrics and accountability

Guardrails

Proscribing access and actions to least privilege and “paved roads”

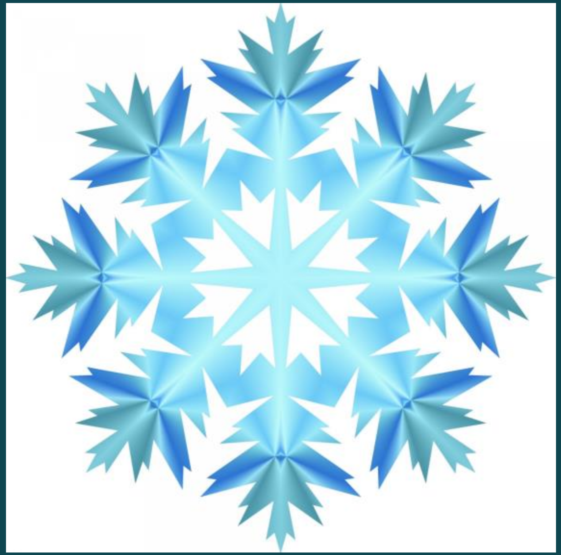
Democratization

Ability to delegate ownership down to developers and other stakeholders

Integration of business and security goals

Governance

- How do you know what you have? (Asset awareness and management)
- How do you enforce governance?
  - Human-level and technical-level tools
  - AWS Organizations
- Change Management and Visibility
  - Tools: Config, Config Rules
  - Versioning, backups, vaults and locks
- Allow for prioritization and force executive buy-in for risk tolerance



Guardrails (and Alarming): Bowling with bumpers

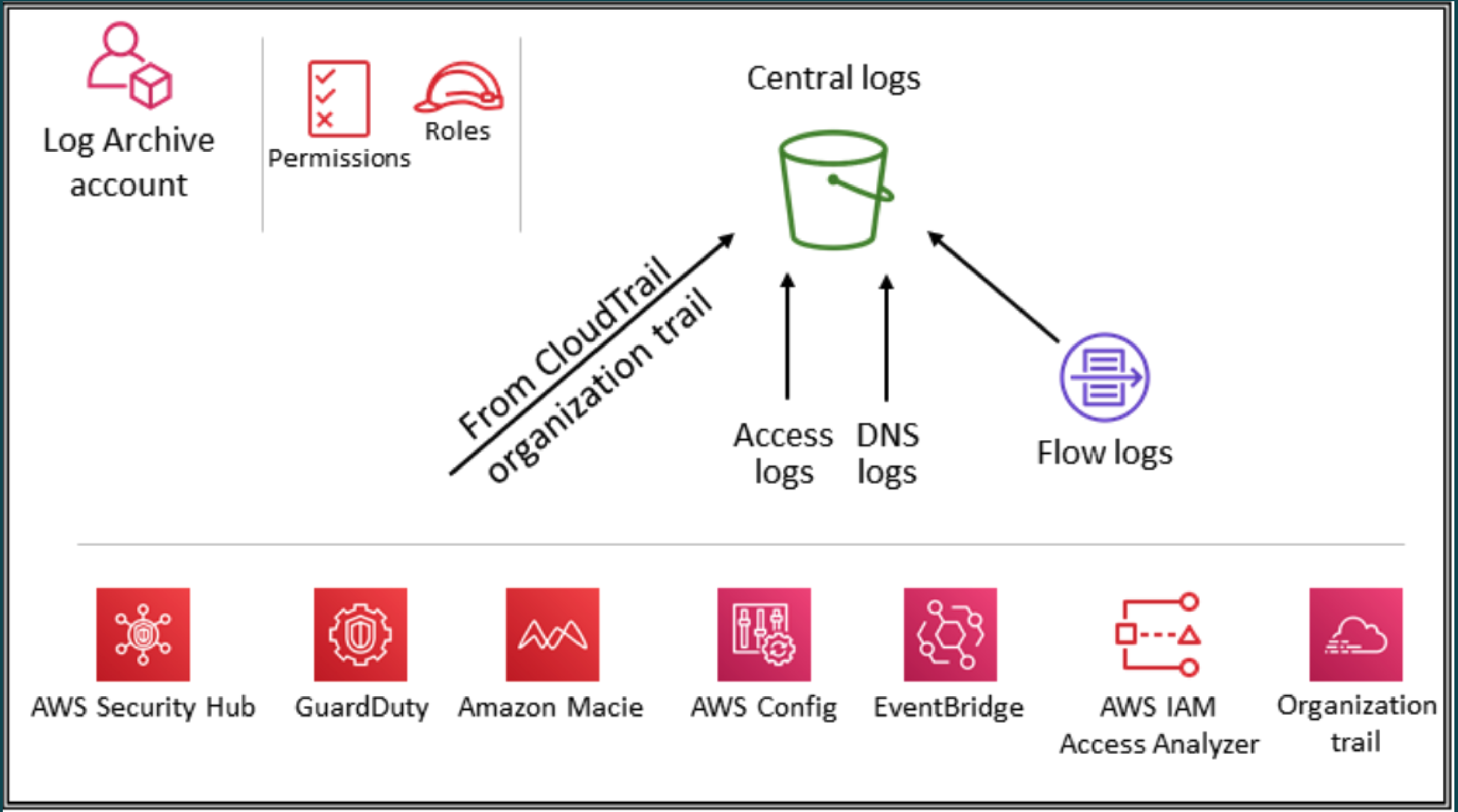
- CloudTrail, CloudWatch, Organizational Units
- Embrace ephemerality/ immutability

Democratization

- Every service team owns the security of their service
- AppSec and ArchSec
- Codepipeline, Codeguru, and other pipelines to production
- CI/CD at scale

Habit 2: (Have a) Strategy for Logging

Centralized logging



- ✓ CloudTrail
- ✓ S3
- ✓ VPC Flow Logs
- ✓ DNS Logs
- ✓ Config

https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/log-archive.html

AWS resource logging guidance

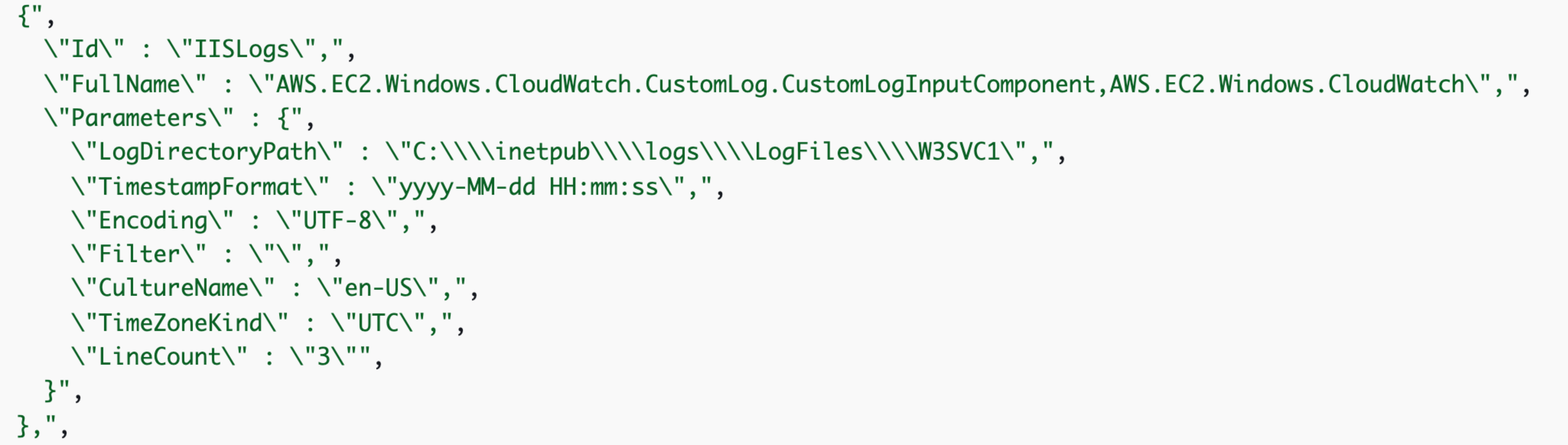
- ✓ EC2 - Linux
- ✓ EC2 – Windows
- ✓ CloudFront
- ✓ LoadBalancers
- ✓ Route53
- ✓ Etc.

Resource	Retention (Days)	Mechanism (Tool)	Logging Configuration Details
EC2-Windows	90	CloudWatchLogs Agent	Application Security System

“Lower the friction of security…”
-Steve Schmidt from AWS Re:Invent 2021

Example: AWS CloudFormation templates

- Windows IIS Logs



```
{",
  \"Id\" : \"IISLogs\",",
  \"FullName\" : \"AWS.EC2.Windows.CloudWatch.CustomLog.CustomLogInputComponent,AWS.EC2.Windows.CloudWatch\",",
  \"Parameters\" : {",
    \"LogDirectoryPath\" : \"C:\\\\inetpub\\\\logs\\\\LogFiles\\\\W3SVC1\",",
    \"TimestampFormat\" : \"yyyy-MM-dd HH:mm:ss\",",
    \"Encoding\" : \"UTF-8\",",
    \"Filter\" : \"\",",
    \"CultureName\" : \"en-US\",",
    \"TimeZoneKind\" : \"UTC\",",
    \"LineCount\" : \"3\"",
  }",
},",
```

Leveraging a SIEM: Build or Bring Your Own

- SIEM Operations
  - Can be hosted in the cloud or on-premises
  - Not uncommon during migration to continue shipping all cloud logs to on-premises SIEM
  - Ideally, SIEM is implemented in the cloud (most effective/efficient solution) but we often see a “hybrid” approach
- It’s common to need an additional cloud-native log search/analysis capability

Habit 3: Operationalize your Insights

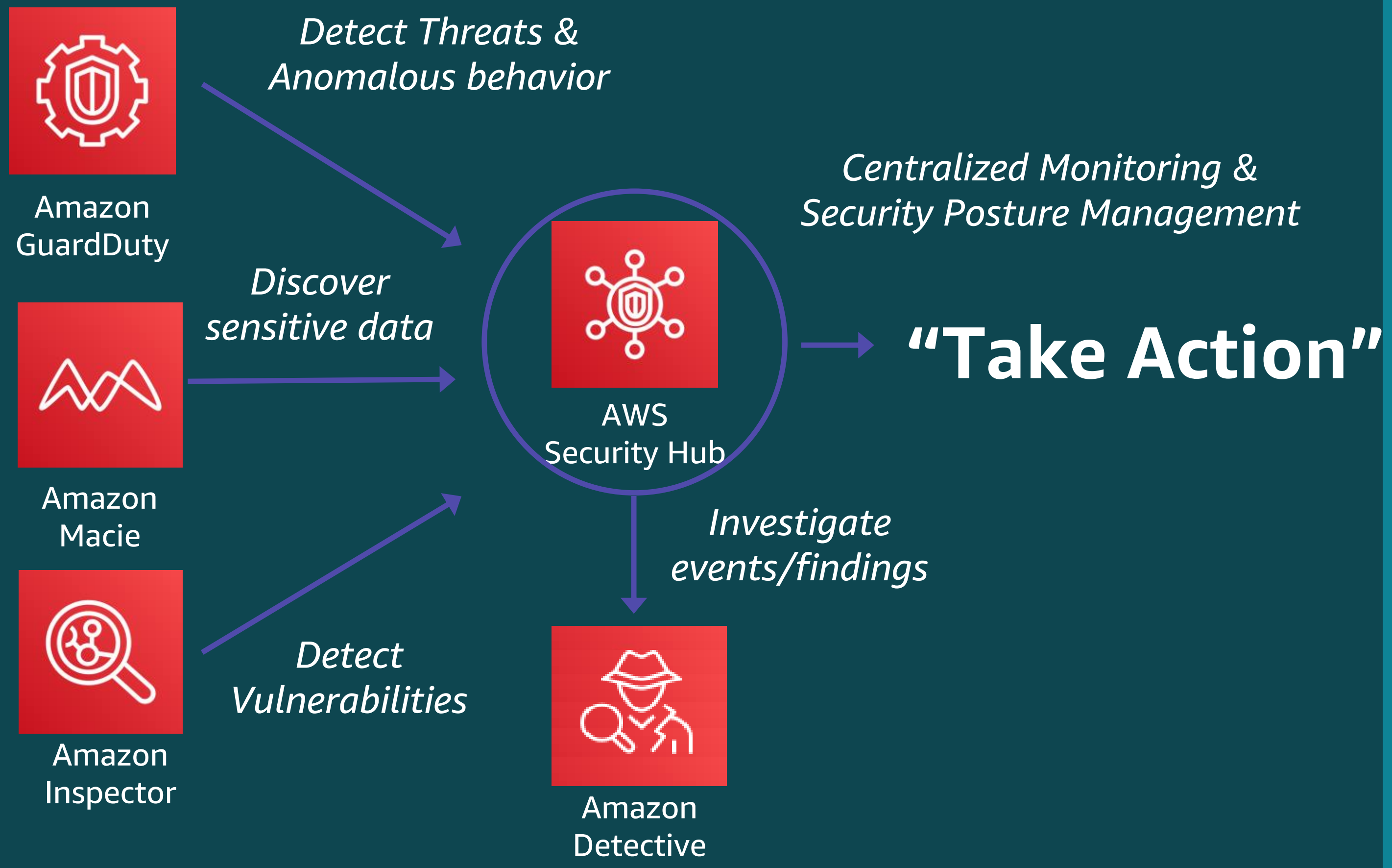
Threat detection, monitoring, and response

Security Monitoring and Threat Detection

Amazon EC2

AWS Identity and Access Management (IAM)

Amazon Simple Storage Service (S3)



Amazon GuardDuty

Detect Threats & Anomalous behavior

Amazon Macie

Discover sensitive data

Amazon Inspector

Detect Vulnerabilities

AWS Security Hub

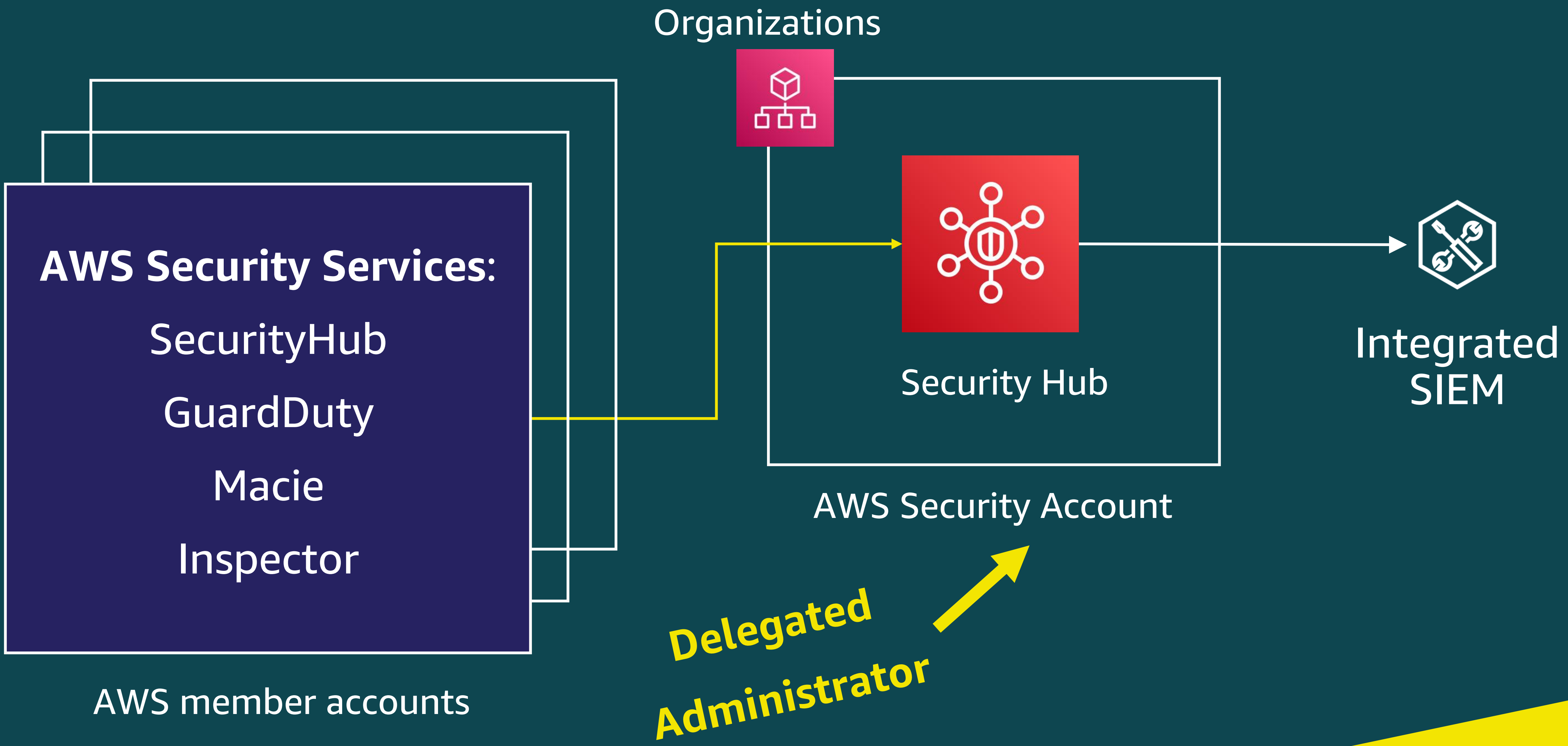
Centralized Monitoring & Security Posture Management

“Take Action”

Investigate events/findings

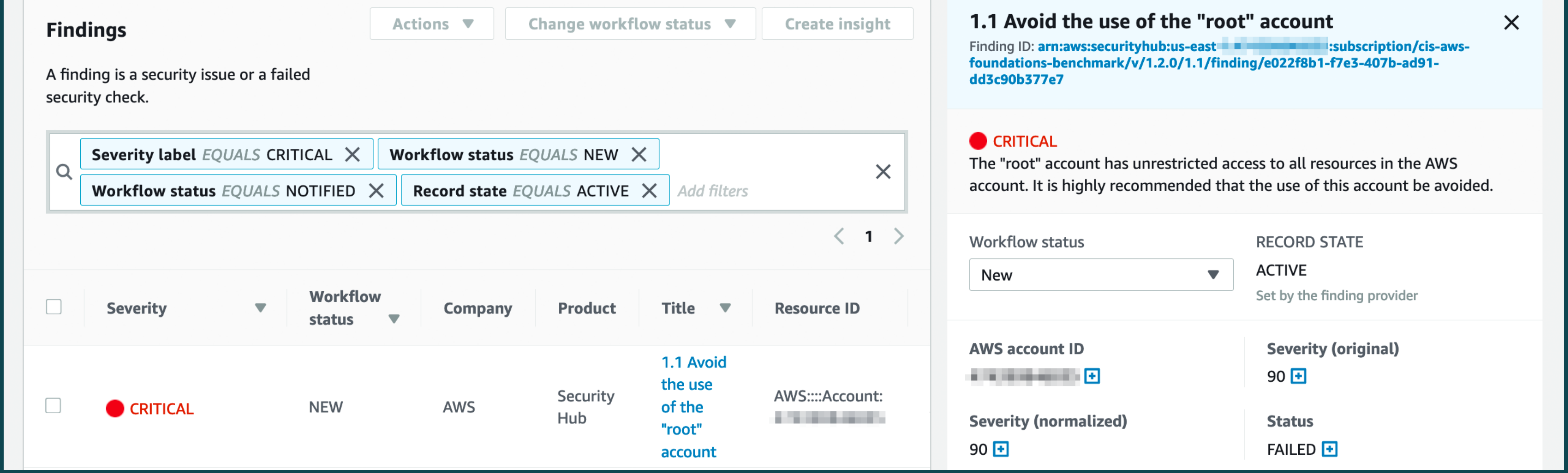
Amazon Detective

Architecture with multi-account strategy



Take action on CRITICAL and HIGH Findings

- Filter Findings on Severity label and Status
- Filters are case sensitive
- Review and Remediate



Findings

A finding is a security issue or a failed security check.

Severity label *EQUALS* CRITICAL ✕ **Workflow status** *EQUALS* NEW ✕ **Workflow status** *EQUALS* NOTIFIED ✕ **Record state** *EQUALS* ACTIVE ✕ *Add filters*

< 1 >

☐	Severity	Workflow status	Company	Product	Title	Resource ID
☐	● CRITICAL	NEW	AWS	Security Hub	1.1 Avoid the use of the "root" account	AWS::::Account: [redacted]

1.1 Avoid the use of the "root" account ✕

Finding ID: arn:aws:securityhub:us-east[redacted]:subscription/cis-aws-foundations-benchmark/v/1.2.0/1.1/finding/e022f8b1-f7e3-407b-ad91-dd3c90b377e7

● CRITICAL
The "root" account has unrestricted access to all resources in the AWS account. It is highly recommended that the use of this account be avoided.

Workflow status: New ▼

RECORD STATE: ACTIVE
Set by the finding provider

AWS account ID: [redacted]

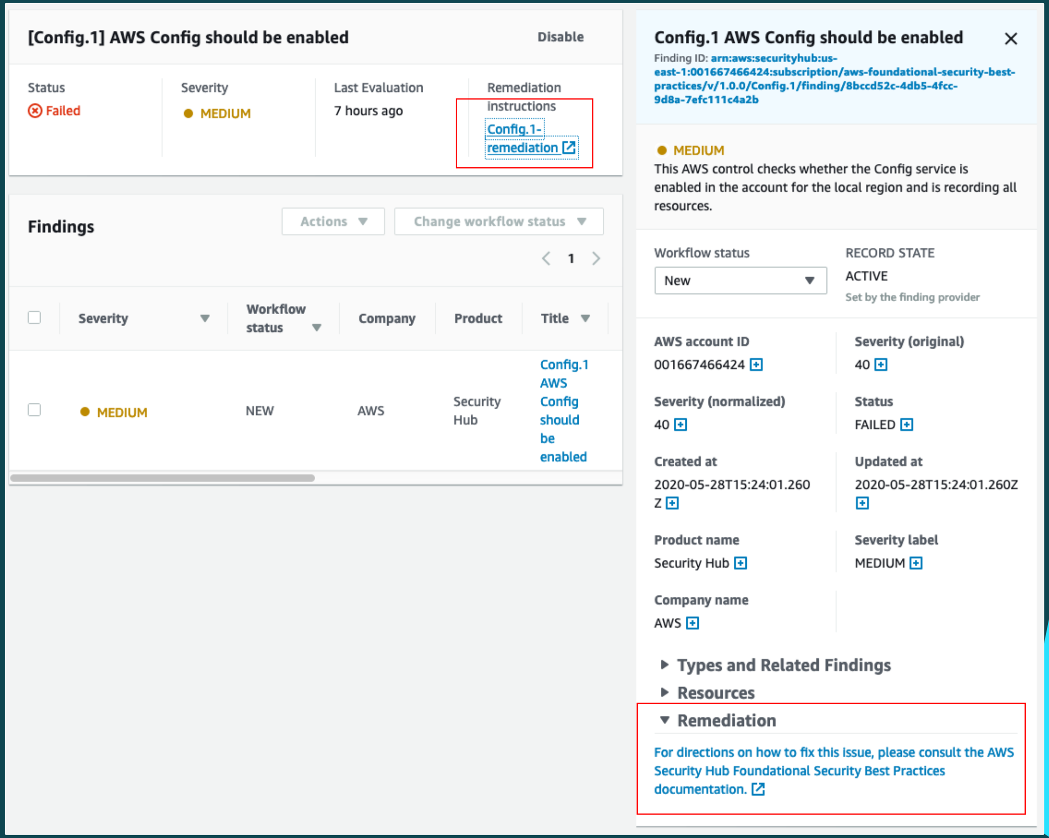
Severity (original): 90

Severity (normalized): 90

Status: FAILED

Leverage available remediation instructions

- Security Hub findings from a Security or Compliance Standard have an associated remediation



[Config.1] AWS Config should be enabled Disable

Status	Severity	Last Evaluation	Remediation instructions
Failed	● MEDIUM	7 hours ago	Config.1-remediation

Findings

□	Severity	Workflow status	Company	Product	Title
□	● MEDIUM	NEW	AWS	Security Hub	Config.1 AWS Config should be enabled

Config.1 AWS Config should be enabled

Finding ID: arn:aws:securityhub:us-east-1:001667466424:subscription/aws-foundational-security-best-practices/v/1.0.0/Config.1/finding/8bccd52c-4db5-4fcc-9d8a-7efc111c4a2b

● MEDIUM

This AWS control checks whether the Config service is enabled in the account for the local region and is recording all resources.

Workflow status: New

RECORD STATE: ACTIVE

Set by the finding provider

AWS account ID: 001667466424

Severity (original): 40

Severity (normalized): 40

Status: FAILED

Created at: 2020-05-28T15:24:01.260Z

Updated at: 2020-05-28T15:24:01.260Z

Product name: Security Hub

Severity label: MEDIUM

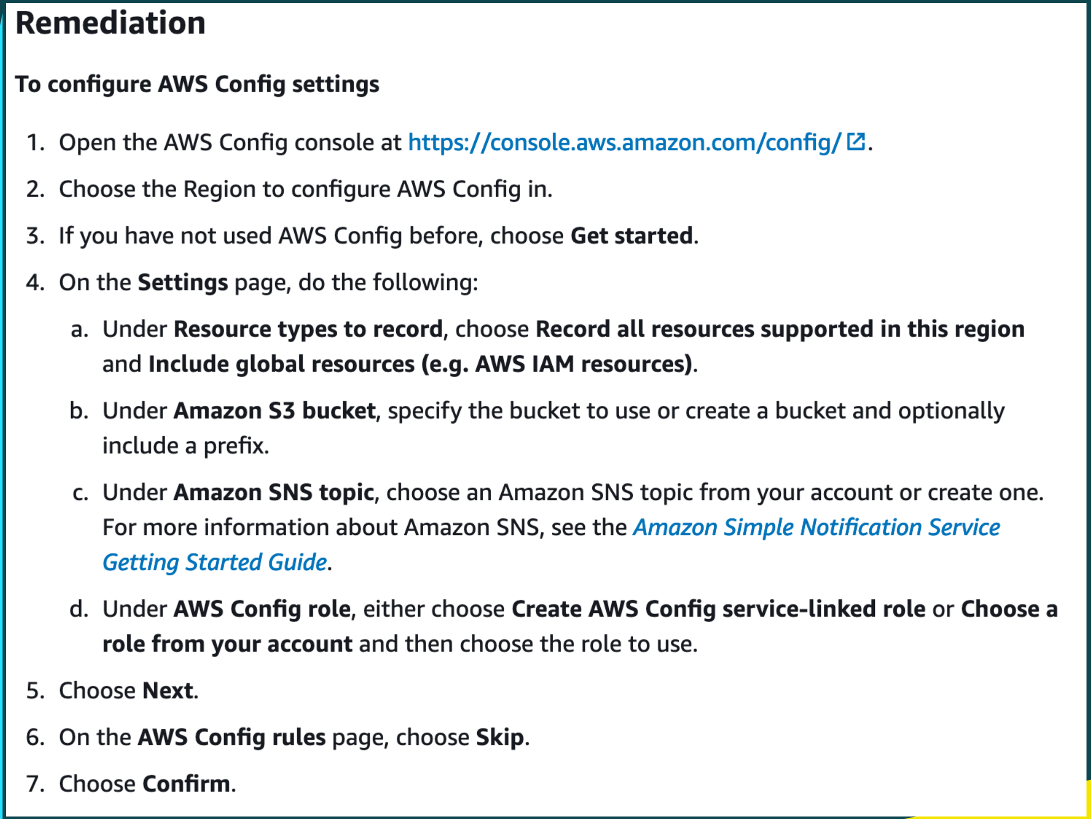
Company name: AWS

▶ Types and Related Findings

▶ Resources

▼ Remediation

For directions on how to fix this issue, please consult the AWS Security Hub Foundational Security Best Practices documentation.



Remediation

To configure AWS Config settings

1. Open the AWS Config console at https://console.aws.amazon.com/config/.
2. Choose the Region to configure AWS Config in.
3. If you have not used AWS Config before, choose **Get started**.
4. On the **Settings** page, do the following:
   a. Under **Resource types to record**, choose **Record all resources supported in this region** and **Include global resources (e.g. AWS IAM resources)**.
   b. Under **Amazon S3 bucket**, specify the bucket to use or create a bucket and optionally include a prefix.
   c. Under **Amazon SNS topic**, choose an Amazon SNS topic from your account or create one. For more information about Amazon SNS, see the *Amazon Simple Notification Service Getting Started Guide*.
   d. Under **AWS Config role**, either choose **Create AWS Config service-linked role** or **Choose a role from your account** and then choose the role to use.
5. Choose **Next**.
6. On the **AWS Config rules** page, choose **Skip**.
7. Choose **Confirm**.

https://pages.awscloud.com/global-traincert-twitch-security.html

Habit 4: Runbooks, playbooks, and tabletop exercises

Runbooks and playbooks

Runbooks

- Tactical review of a situation
- Description of situations that may occur
- Steps to correct or enact a desired outcome
- Contact list for situation

Playbooks

- Strategic review or overview of situational responses
- Strategic planning for future
- Generally non-technical
- C-Level or VP-level information
- Potentially a RACI

Reference: AWS re:Invent 2019: DIY guide to runbooks, incident reports, and incident response (SEC318-R1)

AWS Customer Playbook Framework

100-200 Level

Compromised IAM Credential(s)

Denial of Service/Distributed Denial of Service

Inappropriate Public Resources (S3)

Inappropriate Public Resources (RDS)

Unauthorized Network Changes

300-400 Level

Bitcoin and Crypto jacking

Responding to Ransom in AWS

- EC2 Linux/Unix
- EC2 Windows
- Amazon RDS
- Amazon S3

https://github.com/aws-samples/aws-customer-playbook-framework

Tabletop Exercises and Simulations

Habit 5:
Canaries, validation, and sandboxes

> **There are 2 ways to learn incident response, and one will be chosen for you.**

Beetle@

AWS Security

Canaries

Ability to validate what you know

Always Fail, Always Through

Validation

Better know your environment before you deploy

Validate what you know (ARG)

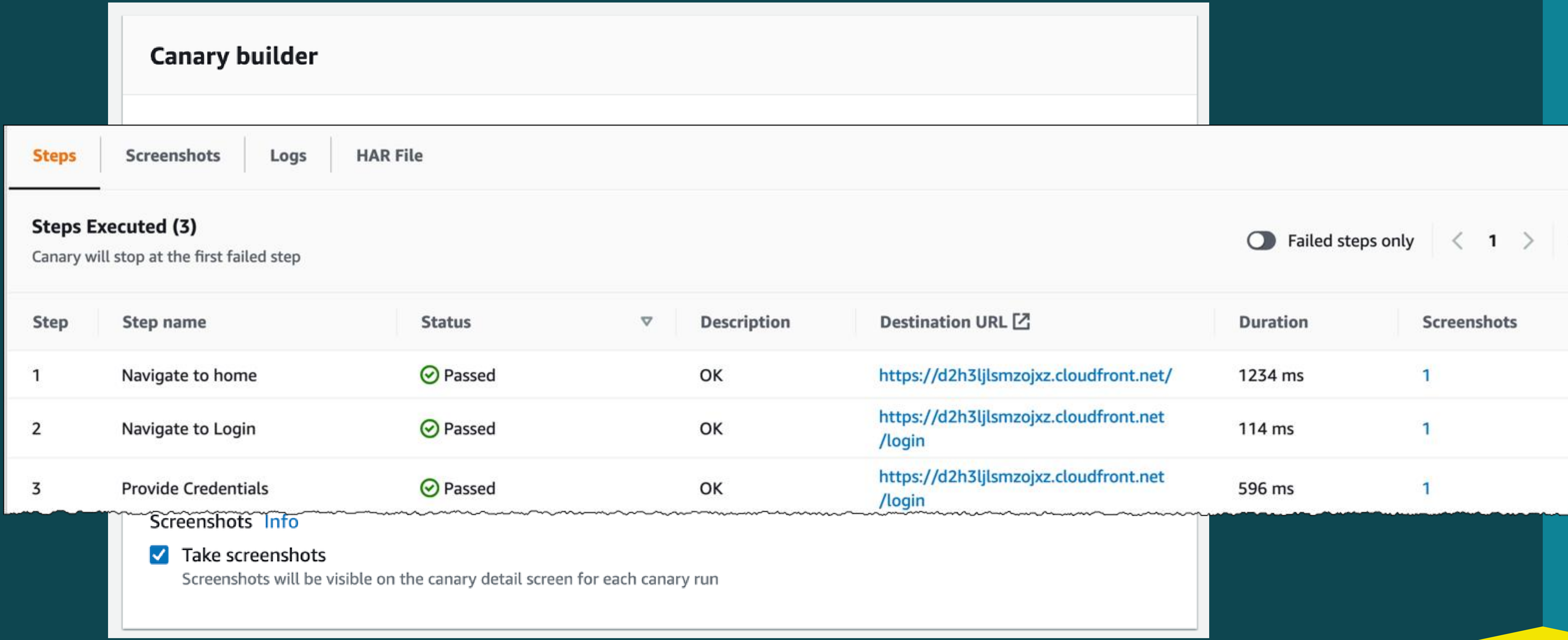
Test your runbooks

Sandboxes

Pipeline to production

Canaries in the Cloud

Example: Canaries using CloudWatch Synthetics



Canary builder

Steps Executed (3)

Canary will stop at the first failed step

Step	Step name	Status	Description	Destination URL	Duration	Screenshots
1	Navigate to home	✓ Passed	OK	https://d2h3ljlsmzojxz.cloudfront.net/	1234 ms	1
2	Navigate to Login	✓ Passed	OK	https://d2h3ljlsmzojxz.cloudfront.net/login	114 ms	1
3	Provide Credentials	✓ Passed	OK	https://d2h3ljlsmzojxz.cloudfront.net/login	596 ms	1

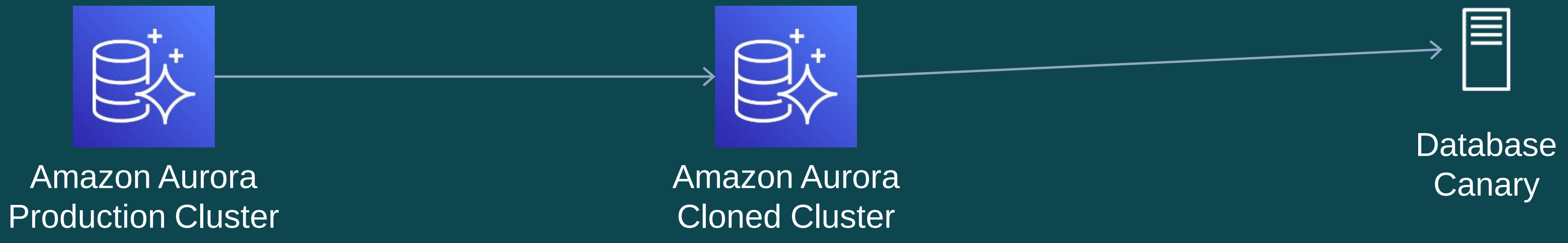
Screenshots Info

☑ Take screenshots

Screenshots will be visible on the canary detail screen for each canary run

https://aws.amazon.com/blogs/mt/create-canaries-in-python-and-selenium-using-amazon-cloudwatch-synthetics/

Example: Database canary using Aurora clones


Amazon Aurora Production Cluster
Amazon Aurora Cloned Cluster
Database Canary

Copy on write = fast and space efficient

Logical corruption
Data consistency
Scan for sensitive data

Habit 6: Automation throughout your TDIR lifecycle

> **We like to hire “lazy” security engineers: they never want to solve the same problem twice**

AWS Security

Pre-IR: Decision-making

Ensure you’re getting the data you need

Reduce the gray area of human decision-making

Backup and redundancy decision-making: including Vaults and locks

During IR: Implementation and Forensics

Your automations run (Lambda, EventBridge, Config Rules, etc.)

Redundancy, backup—come back to known good state.

Post-IR: virtuous cycle

Review what happened—was this a known/accepted risk or unknown?

Address more automations to write

Metrics

> If it’s not someone’s job it’s a hope, and a hope is not a plan.

Eric Brandwine, VP/DE

AWS Security

Thank you!

Merritt Baer

Principal, Office of the CISO

@merrittbaer (twitter)

Megan O’Neil

Senior Security Specialist SA