
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC206-R

Security operations metrics that matter

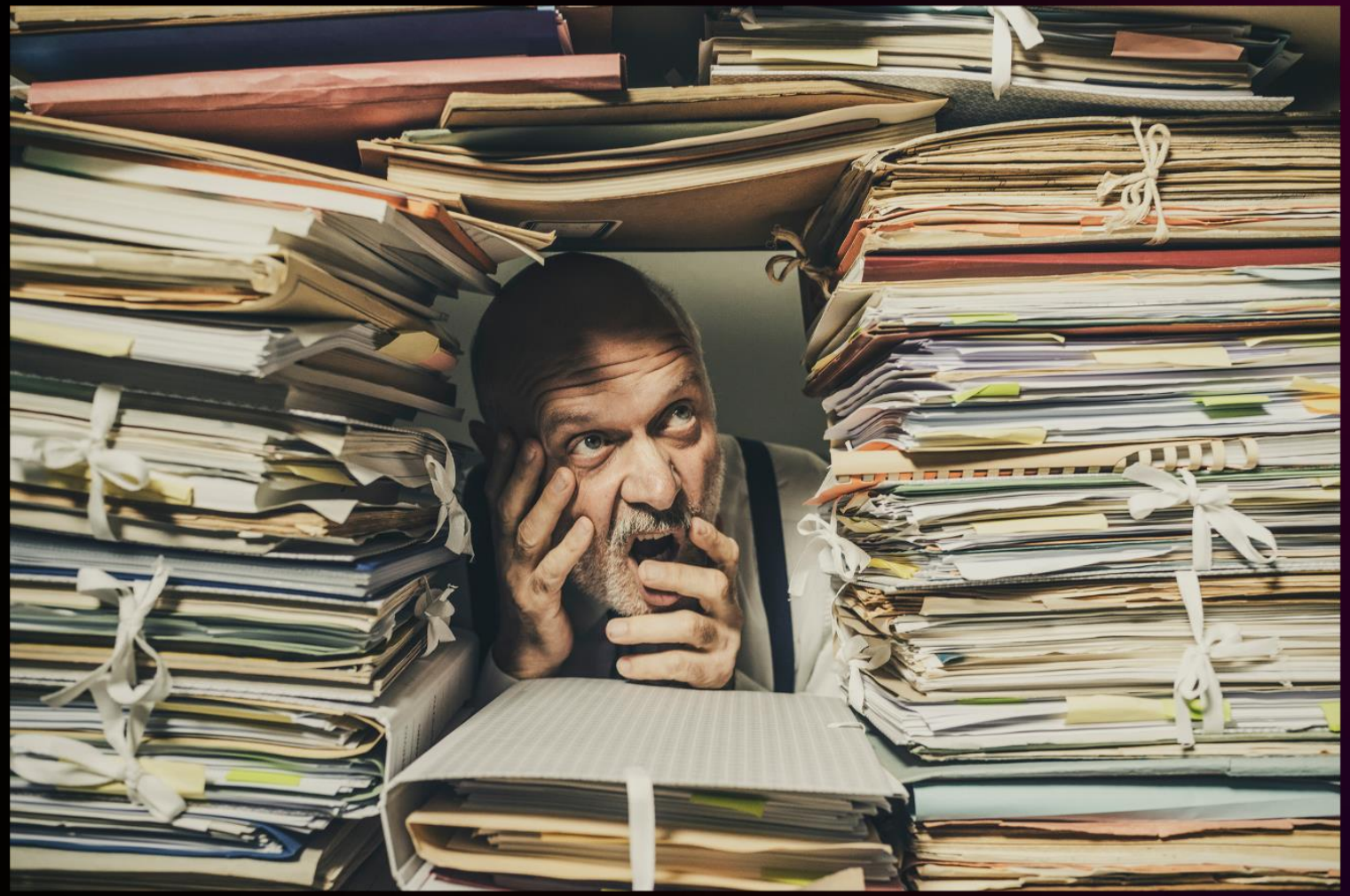
Anna McAbee

Security Specialist SA (TD/IR)
AWS

Megan O'Neil

Principal Security Specialist SA (TD/IR)
AWS

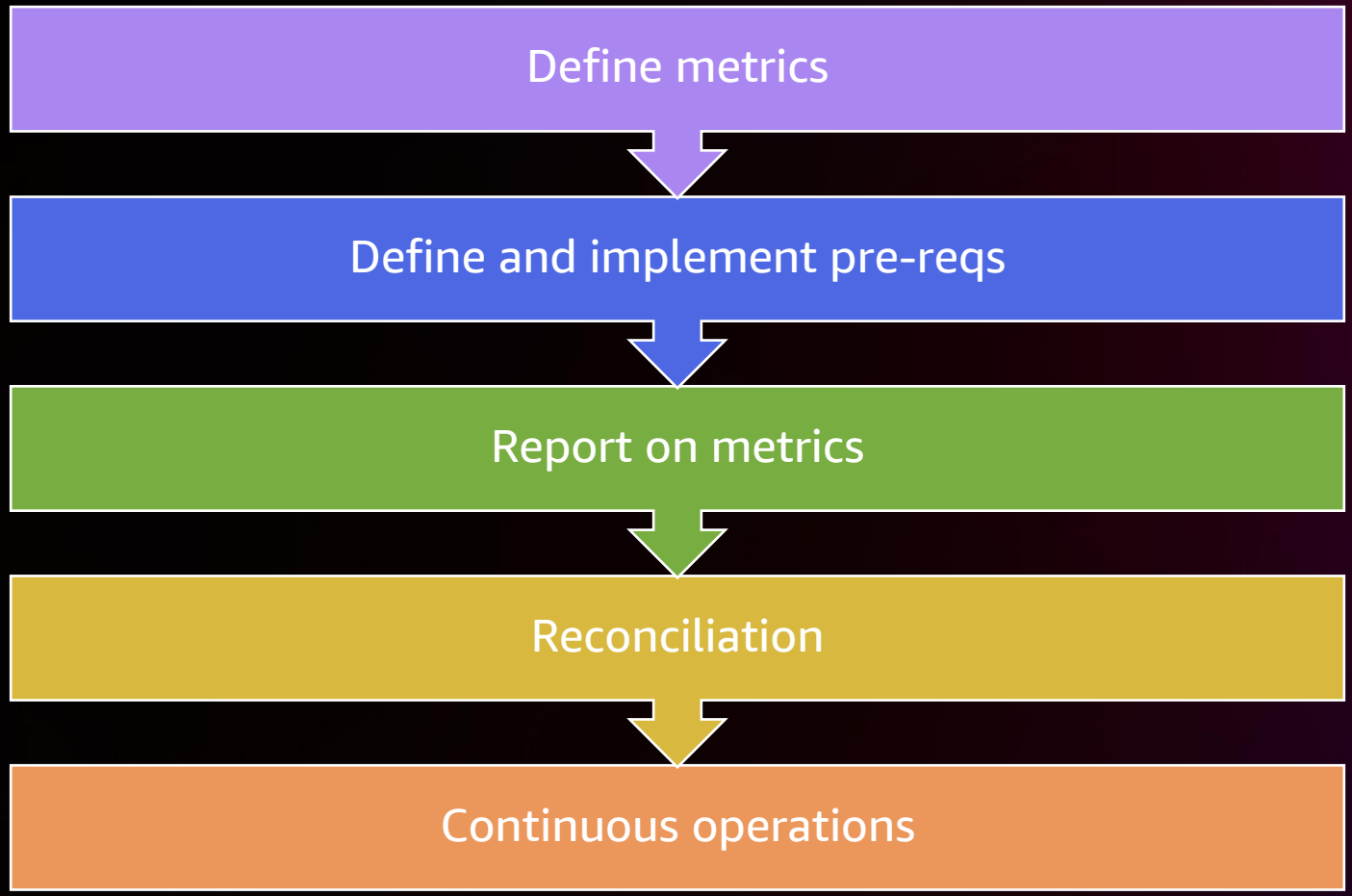
The challenge with cloud security metrics



Foundations

Framework

FOUNDATIONS



AWS security services

FOUNDATIONS

Detective controls

Gain the visibility you need to spot issues before they impact your business, improve your security posture, and reduce the risk profile of your environment

AWS Config

Record and evaluate configurations of your AWS resources to enable compliance auditing, resource change tracking, and security analysis

Amazon GuardDuty

Intelligent threat detection and continuous monitoring to protect your AWS accounts and workloads

Amazon Inspector

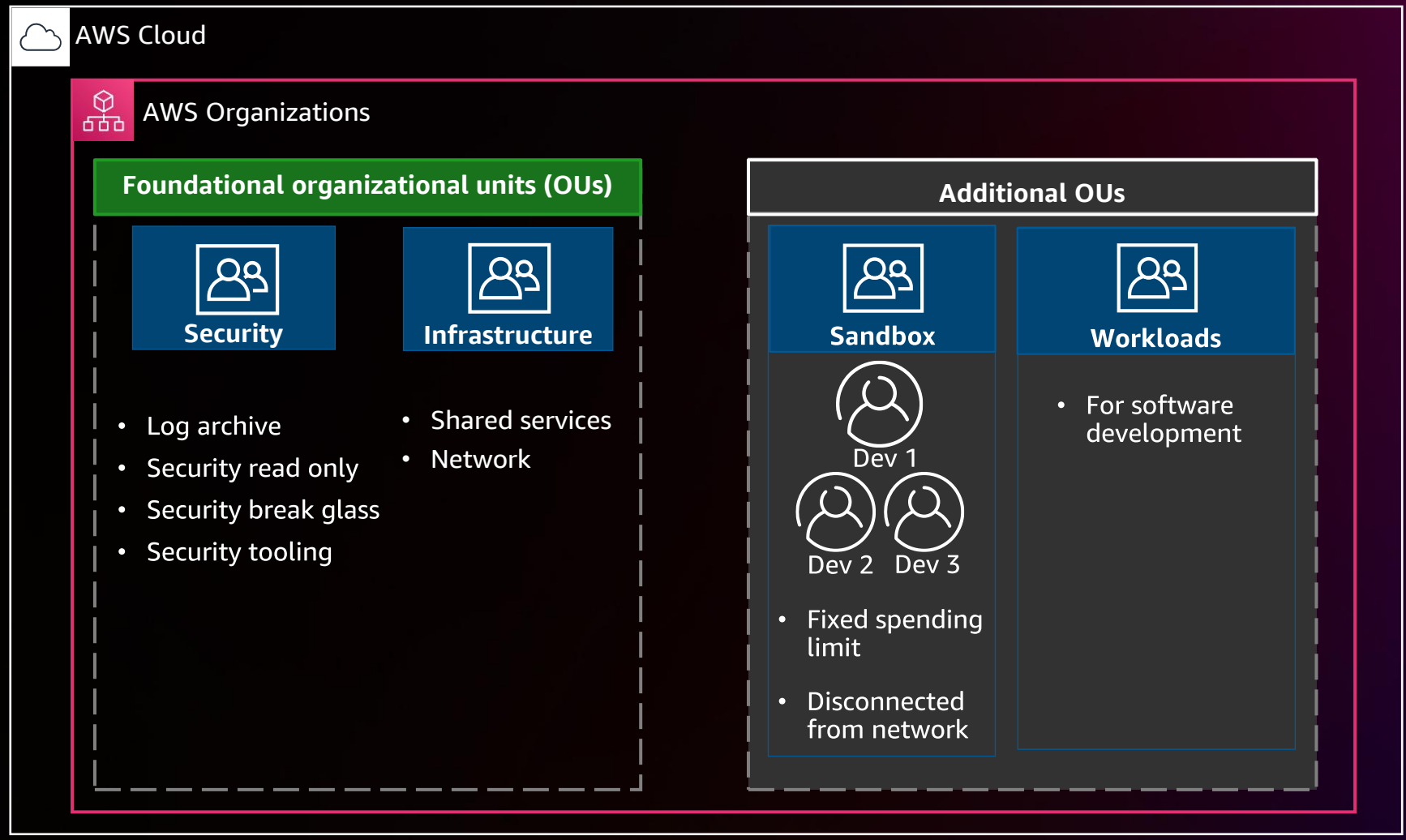
Automates security assessments to help improve the security and compliance of applications deployed on AWS

AWS Security Hub

Centrally view and manage security alerts and automate compliance checks

Starter AWS multi-account framework

FOUNDATIONS



Define metrics

Top cloud security operations metrics

DEFINE METRICS

Reactive

- High severity Amazon GuardDuty findings
- AWS Health Dashboard: discovered access keys and security notifications
- Unintended public resources

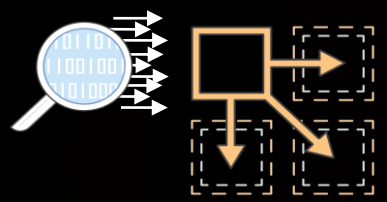
Proactive

- AWS Identity and Access Management (IAM) users with access keys
- Unpatched Amazon EC2 instances and containers
- Critical and high Security Hub: foundational security best practices findings

Reactive 1: High severity Amazon GuardDuty findings

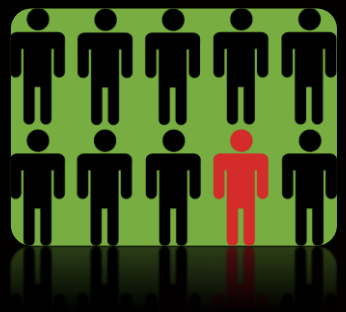
DEFINE METRICS TO CAPTURE

What does GuardDuty detect?



Detect known threats using threat intelligence

- Sites hosting malware & hacker tools
- Cryptocurrency mining pools



Unknown threats using machine learning

- Profiling normal and looking at deviations
- Machine learning classifiers

Reactive 1: High severity Amazon GuardDuty findings

DEFINE METRICS TO CAPTURE

What is a high severity GuardDuty finding?

- Indicates that the resource in question (an EC2 instance or a set of IAM user credentials) is compromised
- Resource is actively being used for unauthorized purposes

Immediate action is recommended for high severity findings

Reactive 2: Health dashboard

DEFINE METRICS TO CAPTURE

Example notifications from AWS Health:

Security

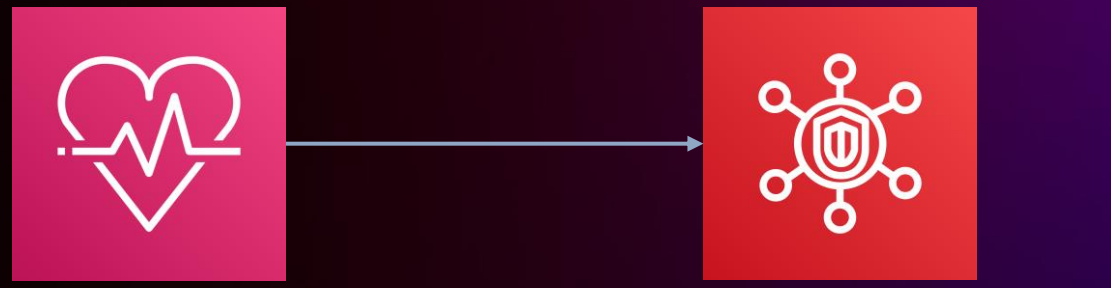
- AWS_SECURITY_NOTIFICATION

Risk

- AWS_RISK_CREDENTIALS_COMPROMISED
- AWS_RISK_CREDENTIALS_EXPOSED
- AWS_RISK_IAM_QUARANTINE

Abuse

- AWS_ABUSE_DOS_REPORT
- AWS_ABUSE_PORT_SCANNING_REPORT



Reactive 3: Unintended public resources

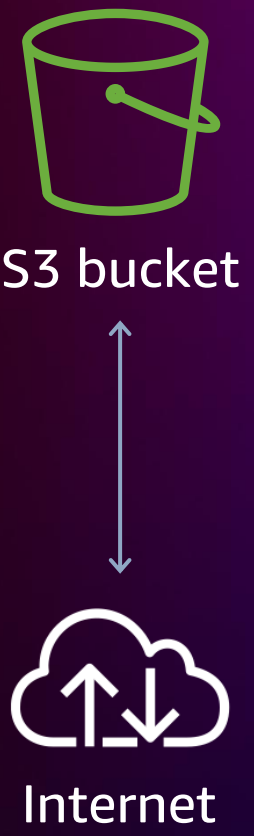
DEFINE METRICS TO CAPTURE

AWS resources that can be public

- S3 buckets
- Amazon EBS snapshots
- Amazon RDS snapshots
- Amazon OpenSearch Service clusters
- Additional resources

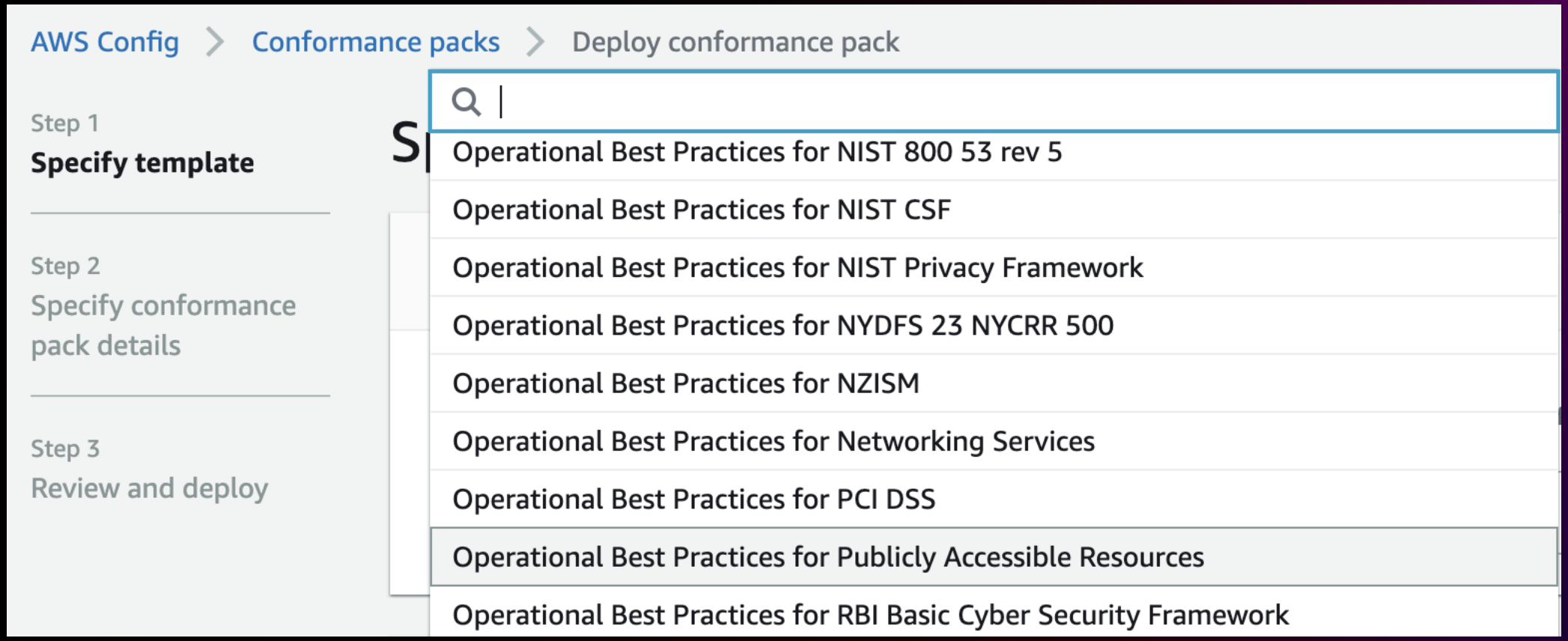
The risk

- An unauthorized user can access the resource without any credentials and from any network



Reactive 3: Unintended public resources

DEFINE METRICS TO CAPTURE



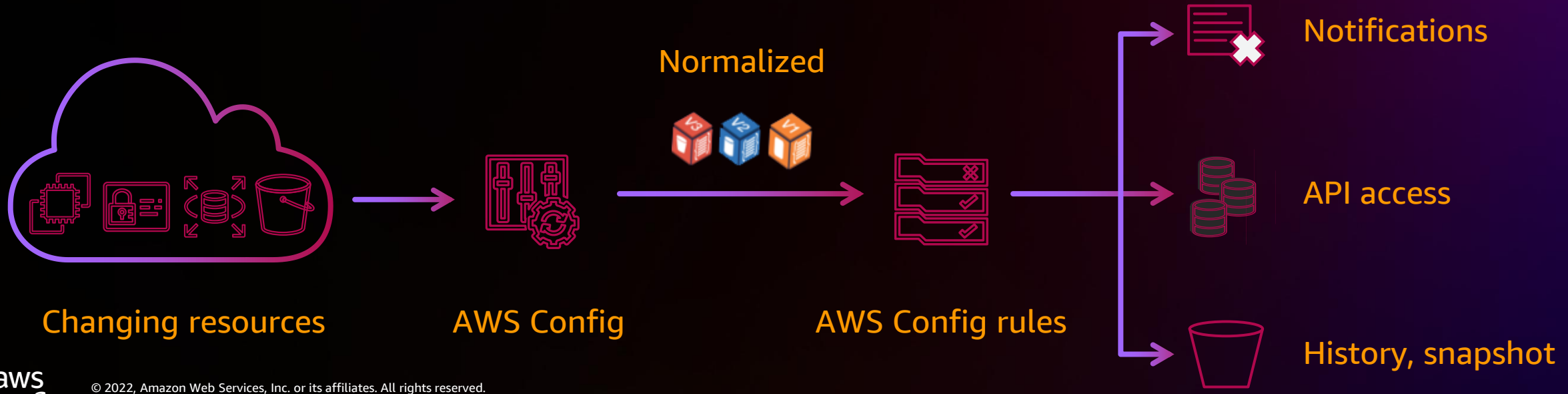
Leverage sample conformance pack, **“Operational Best Practices for Publicly Accessible Resources”**

Proactive 1: IAM users with access keys

DEFINE METRICS TO CAPTURE

AWS Config custom rule: **IAM_USER_NOT_ALLOWED_EXCEPT**

- AWS Config provides continuous configuration auditing
- To ensure IAM users are not present unless from an allowed list
- Trigger: periodic
- Allow list for exceptions



Proactive 2: Public unpatched Amazon EC2 instances

DEFINE METRICS TO CAPTURE

How to track unpatched vulnerabilities

- Amazon Inspector for identification of unpatched EC2 instances and Amazon ECR images
- AWS Config to check for public EC2 instances
- AWS Systems Manager patch manager for automated patch management

AWS Config custom rule:

- **No_EC2_Instances_In_Public_Subnets**
- **EC2_SSM_Patch_Compliance_Status_Check**

Proactive 3: Critical Security Hub FSBP findings

DEFINE METRICS TO CAPTURE

[EC2.19] Security groups should not allow unrestricted access to ports with high risk

[IAM.4] IAM root user access key should not exist

[S3.2] S3 buckets should prohibit public read access

[S3.3] S3 buckets should prohibit public write access

Note: this list is a sampling of critical findings

Proactive 3: High Security Hub FSBP findings

DEFINE METRICS TO CAPTURE

[IAM.1] IAM policies should not allow full “*” administrative privileges

[SSM.2] All EC2 instances managed by systems manager should be compliant with patching requirements

[CloudTrail.1] CloudTrail should be enabled and configured with at least one multi-Region trail that includes read and write management events

[EC2.2] The VPC default security group should not allow inbound and outbound traffic

[EC2.8] EC2 instances should use IMDSv2

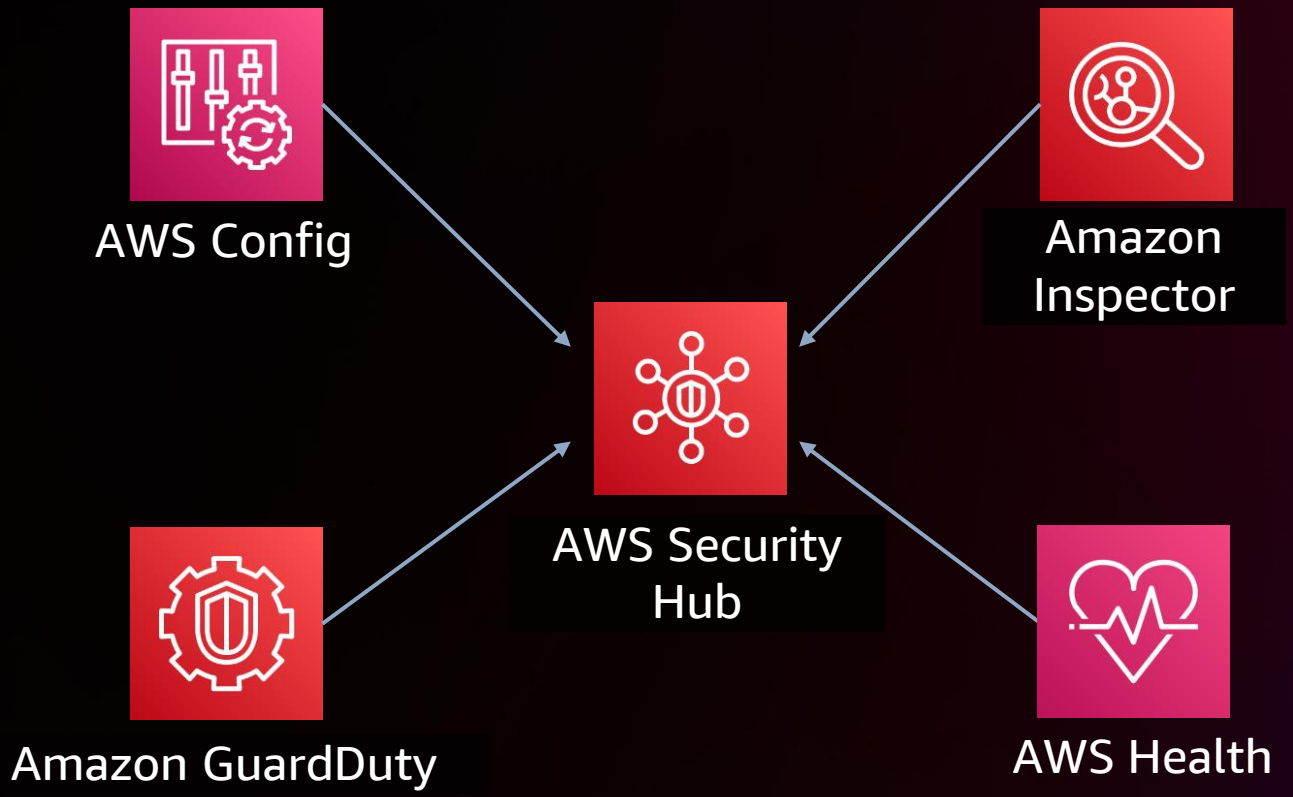
[SageMaker.1] SageMaker notebook instances should not have direct internet access

Note: this list is a sampling of critical findings

Define and implement pre-reqs

Pre-Req Services for Capturing Metrics

DEFINE AND IMPLEMENT PRE-REQS



Tagging

DEFINE AND IMPLEMENT PRE-REQS

Develop a tagging strategy

- Define what you need to know about an AWS resource
- For security metrics, this may include:
  - Critical accounts
  - Business units
  - Data classification
  - Production vs. test
  - Exceptions

Implement the tagging strategy

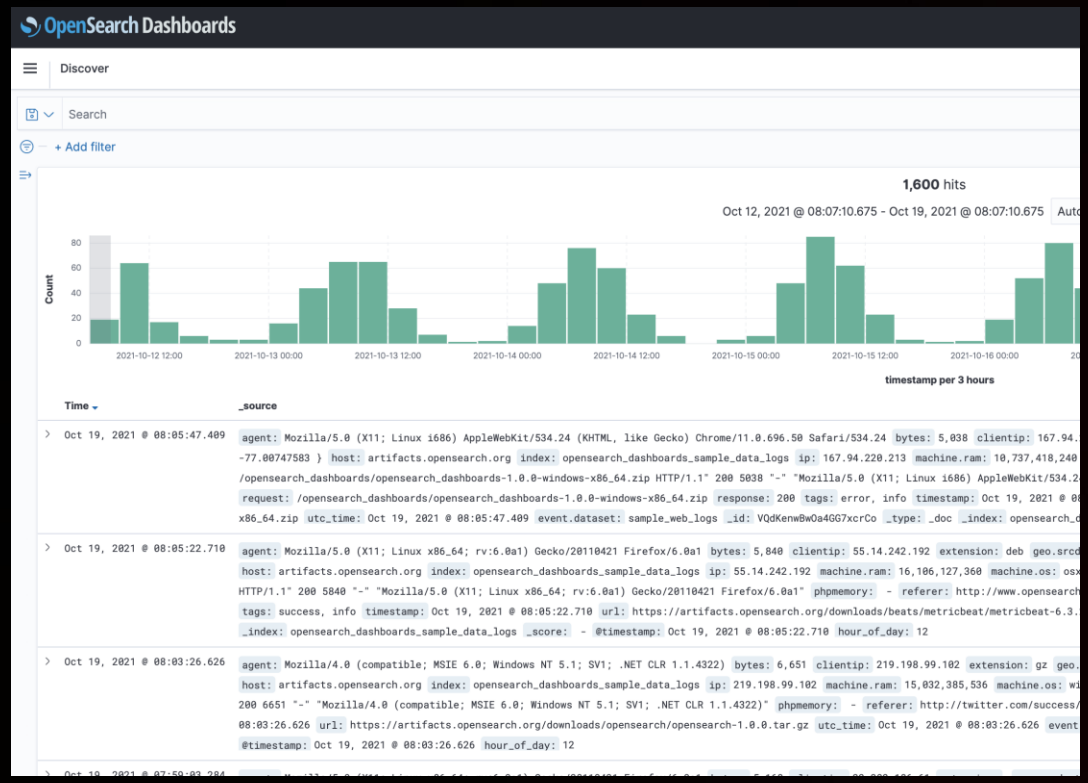
- Enforce tagging using AWS tag policies and service control policies (SCPs)
- Automatically tag your resources
- Keep it simple

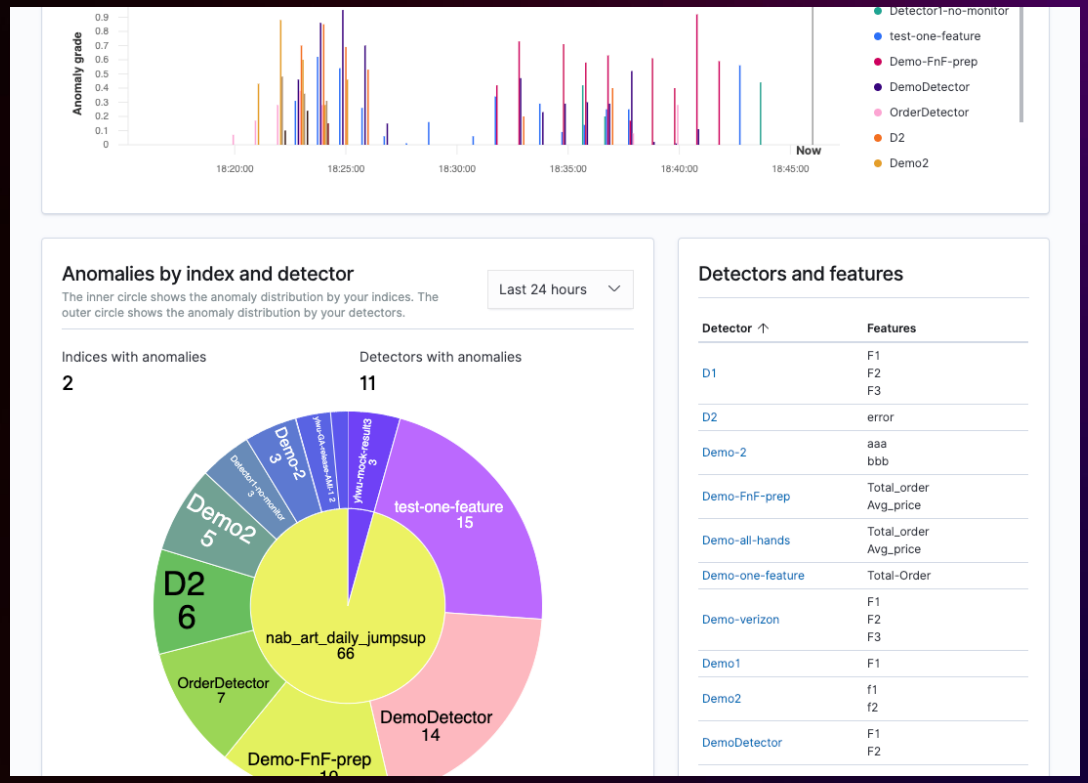
Report on metrics

Introduction to Amazon OpenSearch service

REPORT ON METRICS

Amazon OpenSearch Service securely enables real-time search, monitoring, and analysis of operational data





Security Hub and OpenSearch Service benefits

REPORT ON METRICS

Using Security Hub with OpenSearch Service

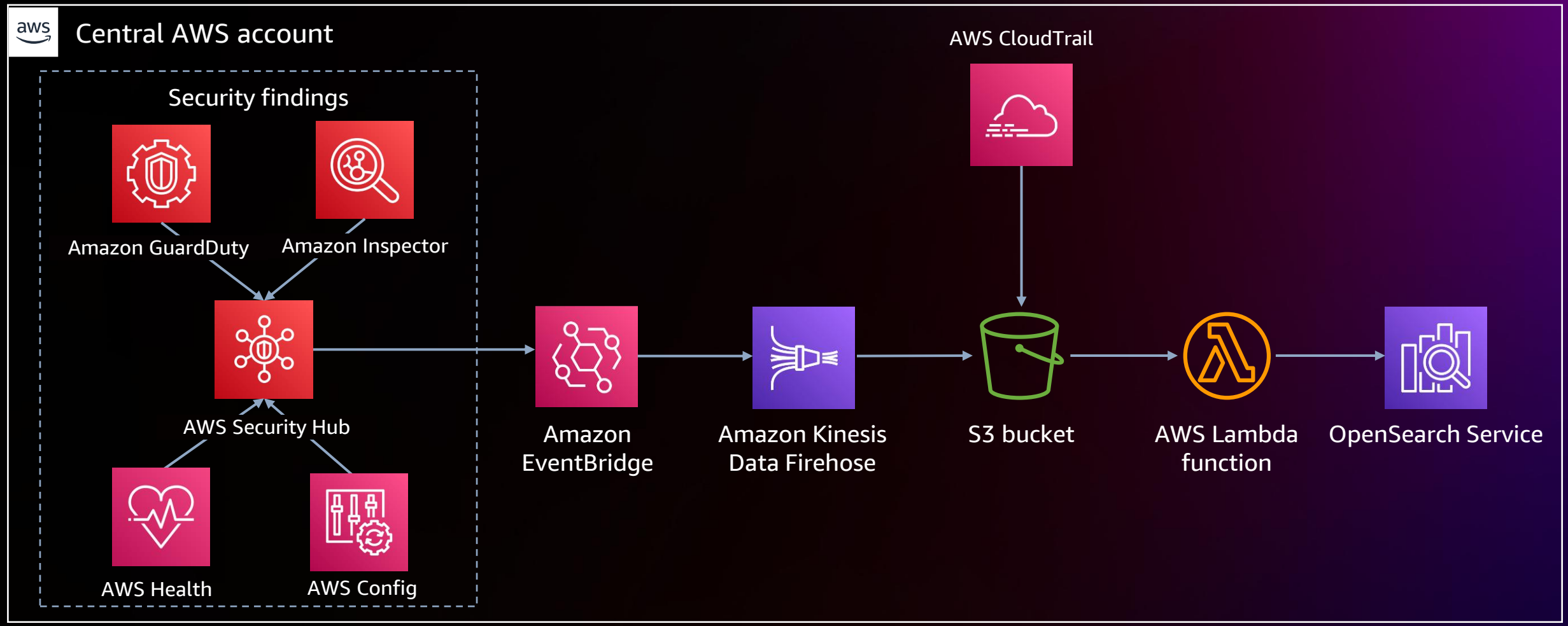
- Correlate Security Hub findings and other log sources
- Store findings for longer than 90 days after the last update
- Aggregate findings across multiple administrator accounts
- OpenSearch Service enables you to query logs and create dashboards within one AWS service

Security Hub

OpenSearch Service

Capture metrics

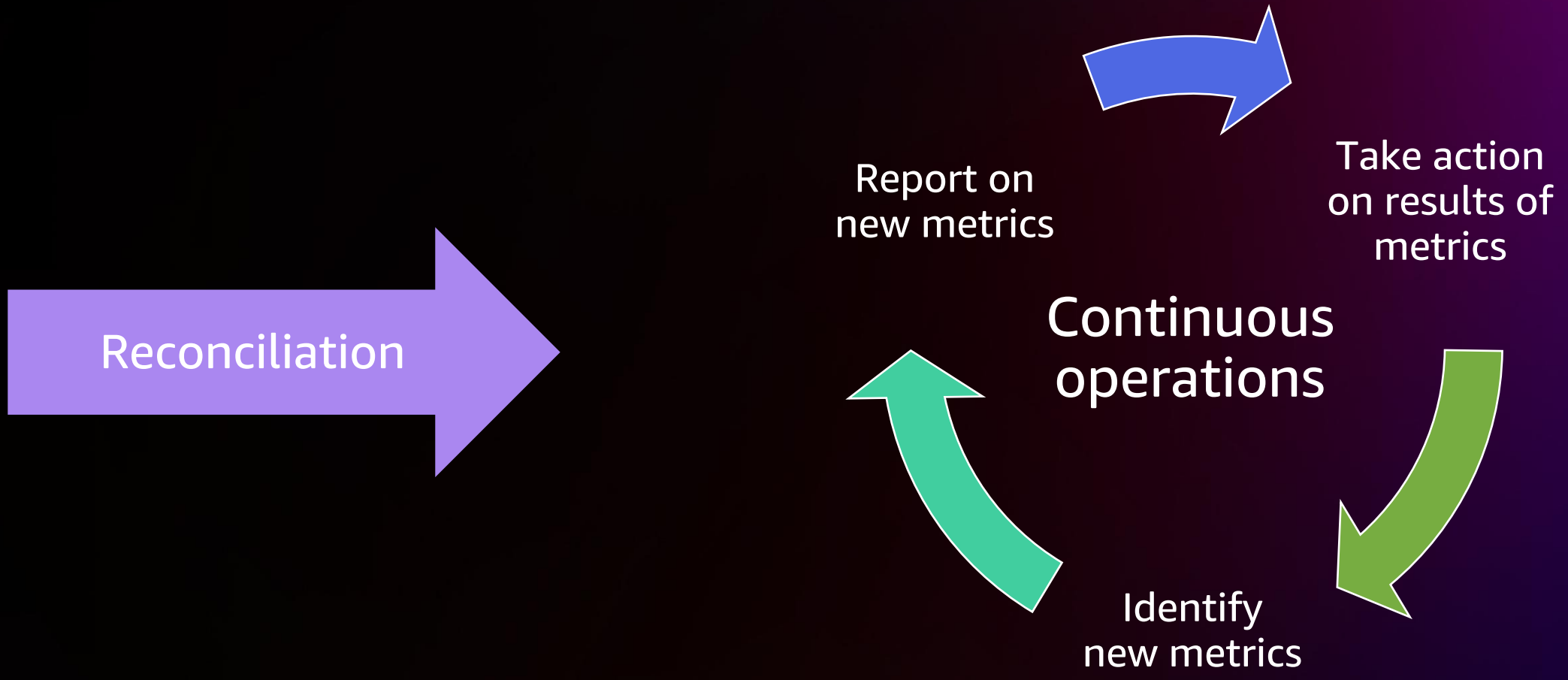
REPORT ON METRICS



Source: https://github.com/aws-samples/siem-on-amazon-opensearch-service

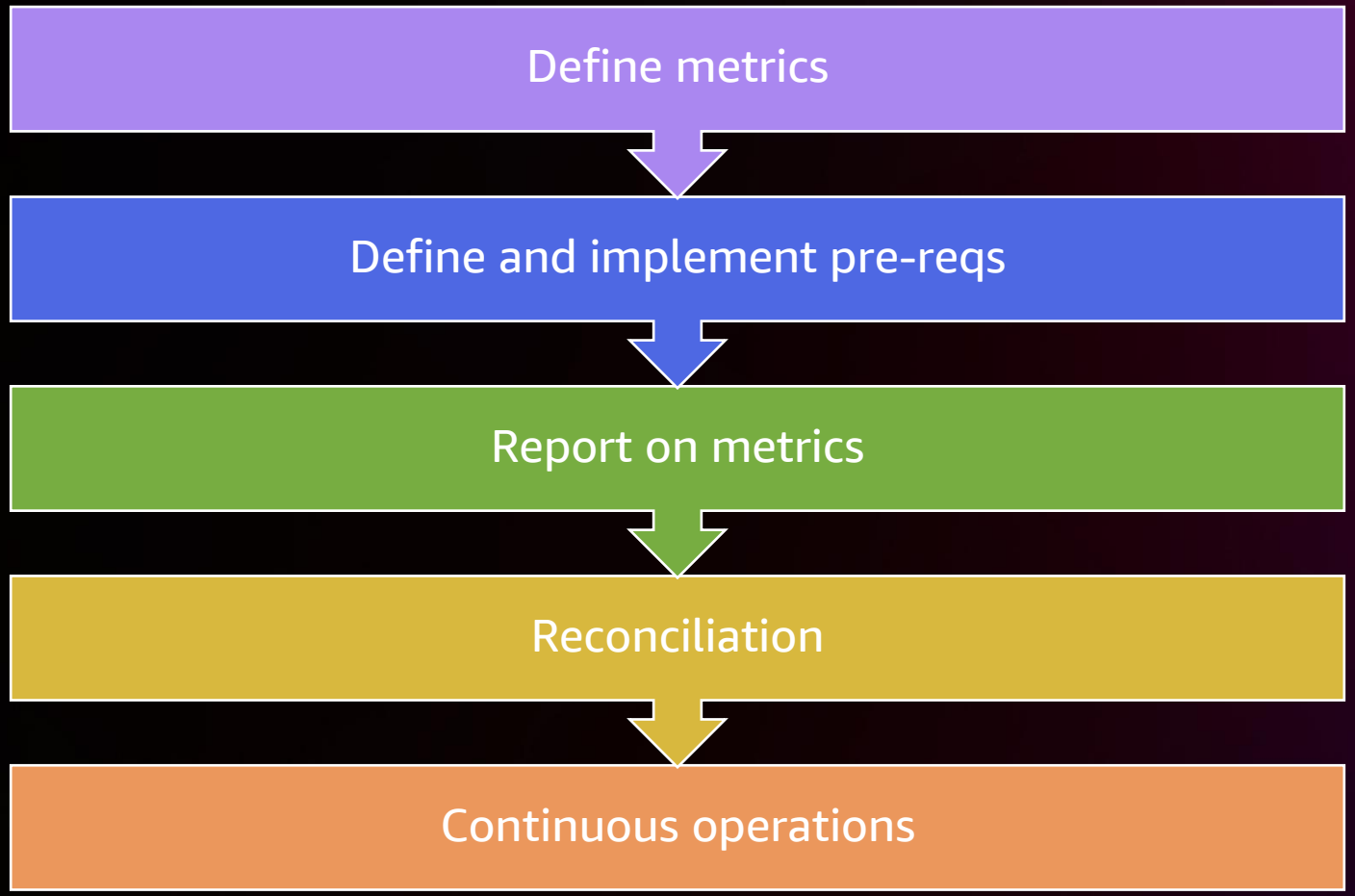
Reconciliation and continuous operations

Reconciliation and continuous operations



What metrics are we missing?

Summary



Thank you!

Please complete the session survey in the **mobile app**