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

COP304

Cloud compliance, assurance, and auditing

Andres Silva
Sr. SSA Leader, CloudOps
Amazon Web Services

Kaartik Viswanath
Sr. SDM, AWS Config
Amazon Web Services

Suchita Verma
Sr. PMT, CloudTrail
Amazon Web Services

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- Meet John Cybersecurity Engineer
- New challenges with compliance
- How AWS Config can help
- How AWS CloudTrail can help
- How AWS Audit Manager can help

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

John Cybersecurity Engineer

- Ramping up on AWS Compliance
- Deployed AWS Control Tower and configured CloudTrail trails
- Customized and deployed conformance packs
- Using Systems Manager Automation for some remediations



re:Inforce session

re:Invent session

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New challenges John is facing

Manage Risks

Simplify Rule authoring

Shift Left for Compliance

Analyze CloudTrail logs

Collect Evidence for Audits



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why AWS Cloud Operations?



Return on Investment (ROI)

241% ROI over 3 years*



Staff productivity

62% more efficient IT infrastructure staff



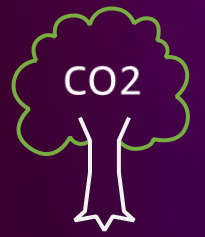
Operational resilience

57% decrease in downtime



Business agility

37% decrease in time to market



Carbon savings

88% reduction in carbon footprint of IT operations

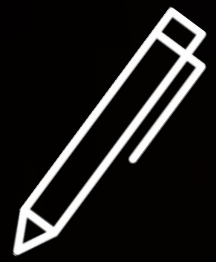
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Based on independent research of 1,500 AWS enterprise customers
*Source: "The Total Economic Impact of AWS Cloud Operations: Cost Savings And Business Benefits Enabled By Operation on AWS. May 2022. A commissioned study conducted by Forrester Consulting on behalf of Amazon Web Services."

Your journey to operating at cloud scale

Get started with AWS Cloud Operations

1) Set up



Establish a secure foundation for governance and compliance

2) Build and migrate



Migrate applications to the cloud or build new applications

3) Operate



Monitor application performance, detect and remediate noncompliance or operational risks quickly

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why are we defining the Cloud Ops model?

Millions + **>1 billion** + **100,000+** + **20+ years**

of active AWS customers every month globally

end users served by our customers

AWS Partners from more than 150 countries

of Amazon's operations management experience

Over 6 quadrillion

metric observations with CloudWatch per month

That's 2.3 billion a second!

600 billion auditing events per day

AWS CloudTrail delivers on average, or seven million auditing events per second.

AWS Config processes over **8 billion resource configuration changes, 9 billion compliance** checks each month.

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Deep Dive AWS Config new features

Manage Risk

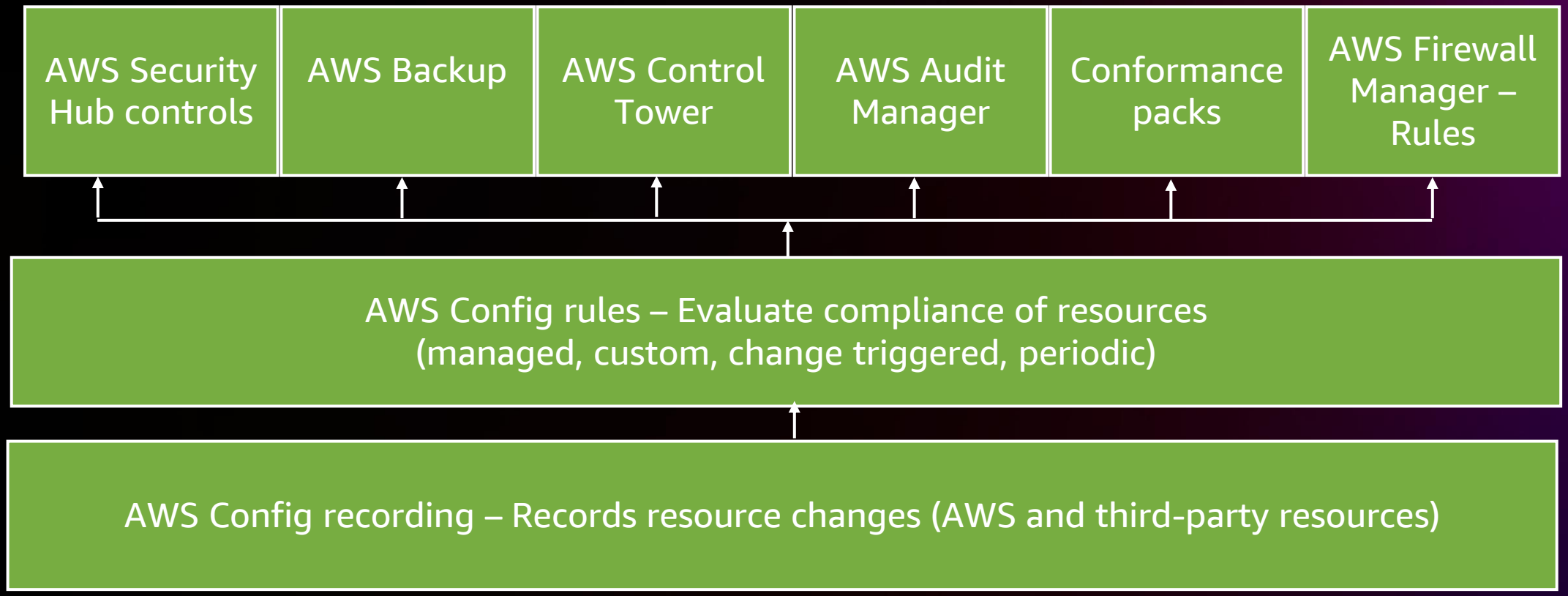
Simplify Rule authoring

Shift Left for Compliance



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Config – Core for compliance evaluations



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

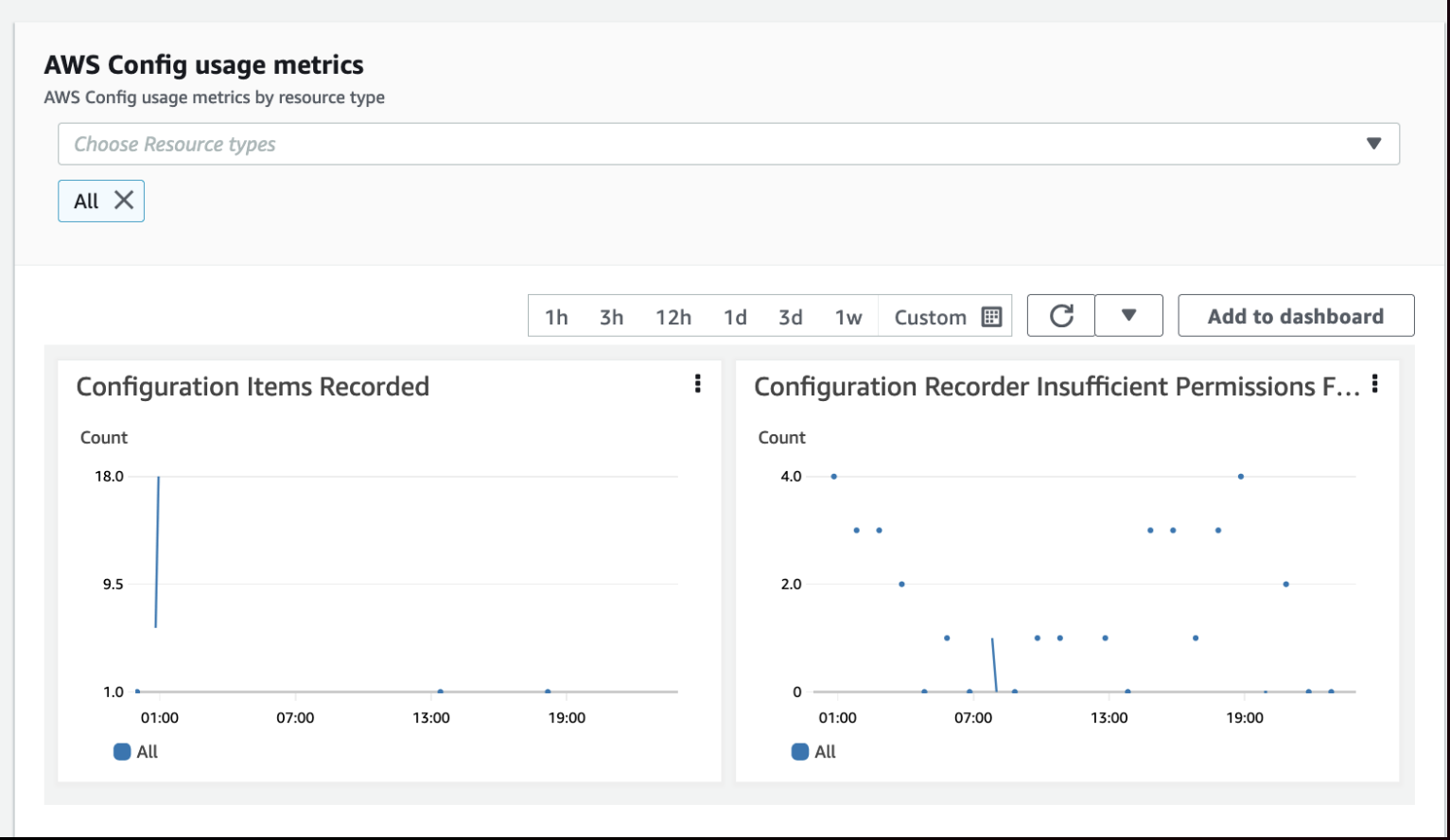
Manage risk – Drift detection in Recorder



- New CI to track changes to Config recorder
- Enabled by default
- Integrates with Config Aggregator & Adv. Query

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Manage risk – Integrate with CloudWatch Metrics

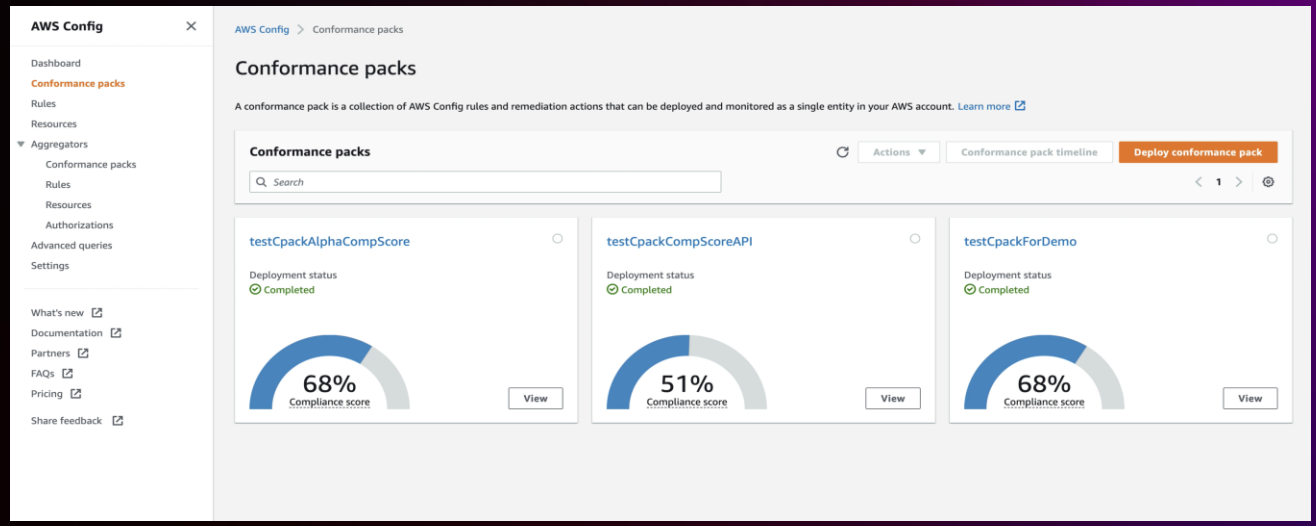


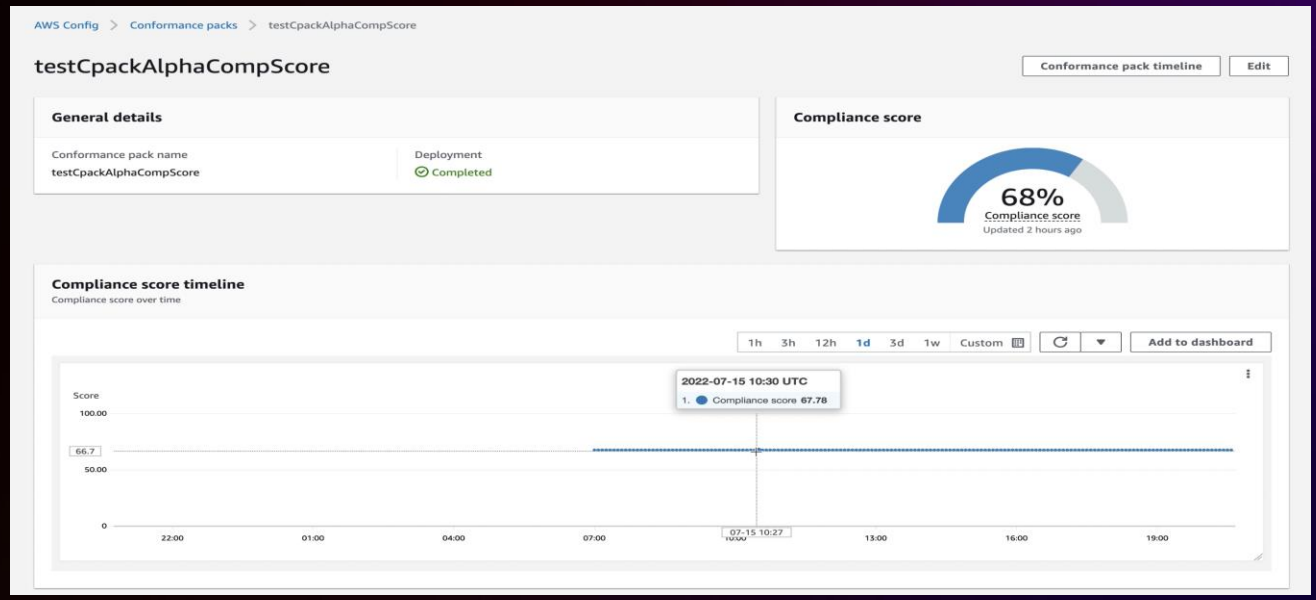
- Integrate with CloudWatch metrics to deliver usage & error metrics
- Usage: # of CIs recorded by resource type
- Track accidental deletion of permissions

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Manage risk – AWS Config Compliance Score for Conformance Packs

- Get a quantitative measure of compliance status at a glance
- Measures compliance for rule/resource combination
- Historical view of compliance of Conformance Packs
- Measure impact of changes
- Prioritize the non-compliance Conformance Packs





© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Authoring rules made simple

AWS Config DSL rules

- This sample custom rule written in Python evaluates if an instance type is in the allowed list type for compliance. Note how many lines of code are needed.

```
import boto3
import json

# Set to True to get the lambda to assume the Role attached on the Config Service (useful for cross-account).
ASSUME_ROLE_MODE = False

def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )
# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)
# Convert from the API model to the original invocation model
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Config DSL rules

- Author Config rule using CloudFormation Guard (Domain-specific language)

Same rule to evaluate instance type now written in cnf-guard syntax

```
# DESIRED_INSTANCE_TYPE Rule with parameter. Pass parameter in putconfigrule with name "instanceType".

# CONFIG_RULE_PARAMETERS is a reserved keyword used to address any parameters passed in PutConfigRule API


rule desiredInstanceType when

   resourceType == "AWS::EC2::Instance" {

       configuration.instanceType == CONFIG_RULE_PARAMETERS.instanceType

}
```

- Benefits
  - Fewer error handling – permissions, oversized CIs, deleted CIs
  - Assuming roles, PutEval calls & infrastructure management not required
  - Ease of authoring & deployment
  - Policy-as-code

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Proactive compliance

NEW

- Identify non-compliant resource prior to creation
- Benefits:
  - Reduce operational & security risk
  - Save time & cost
- Same rule can be deployed for detective & proactive compliance
- Integrates with CI/CD, CFN

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Proactive compliance – How it works

1. Deploy the rule
2. Invoke the rule
3. Check the status of the execution

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Proactive rules – Deployment

1. Deploy the rule

```
aws configservice put-config-rule
--config-rule {"ConfigRuleName": "s3-bucket-server-side-encryption-enabled",
"RuleExecutionCapabilities": [
{"RuleExecutionMode": "detective"},
{"RuleExecutionMode": "proactive"}],
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Proactive rules – Invoke the rule

2. Invoke the rule

aws configservice start-resource-evaluation
--config-rule-names <value>
--resource-details <value> //CloudFormation schema of resource
--evaluation-context <value>
--evaluation-mode <value> //Proactive
--evaluation-timeout <value> //1 to 3600 seconds
--client-token <value> //For idempotency

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Proactive rules – Check the status

3. Check the status of the execution

aws configservice get-resource-evaluation-summary
--resource-evaluation-id <value> //Unique identifier for the proactive invocation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Deep dive – AWS CloudTrail

Analyze CloudTrail logs



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS CloudTrail

TRACK USER AND RESOURCE ACTIVITY ACROSS YOUR AWS INFRASTRUCTURE AND RESOURCES FOR GOVERNANCE AND AUDITING



Compliance aid: Authoritative source that records and stores AWS activity across Regions and accounts



Security investigation: Analyze permissions, detect data exfiltration



Operational troubleshooting: Review resource level activity

aws

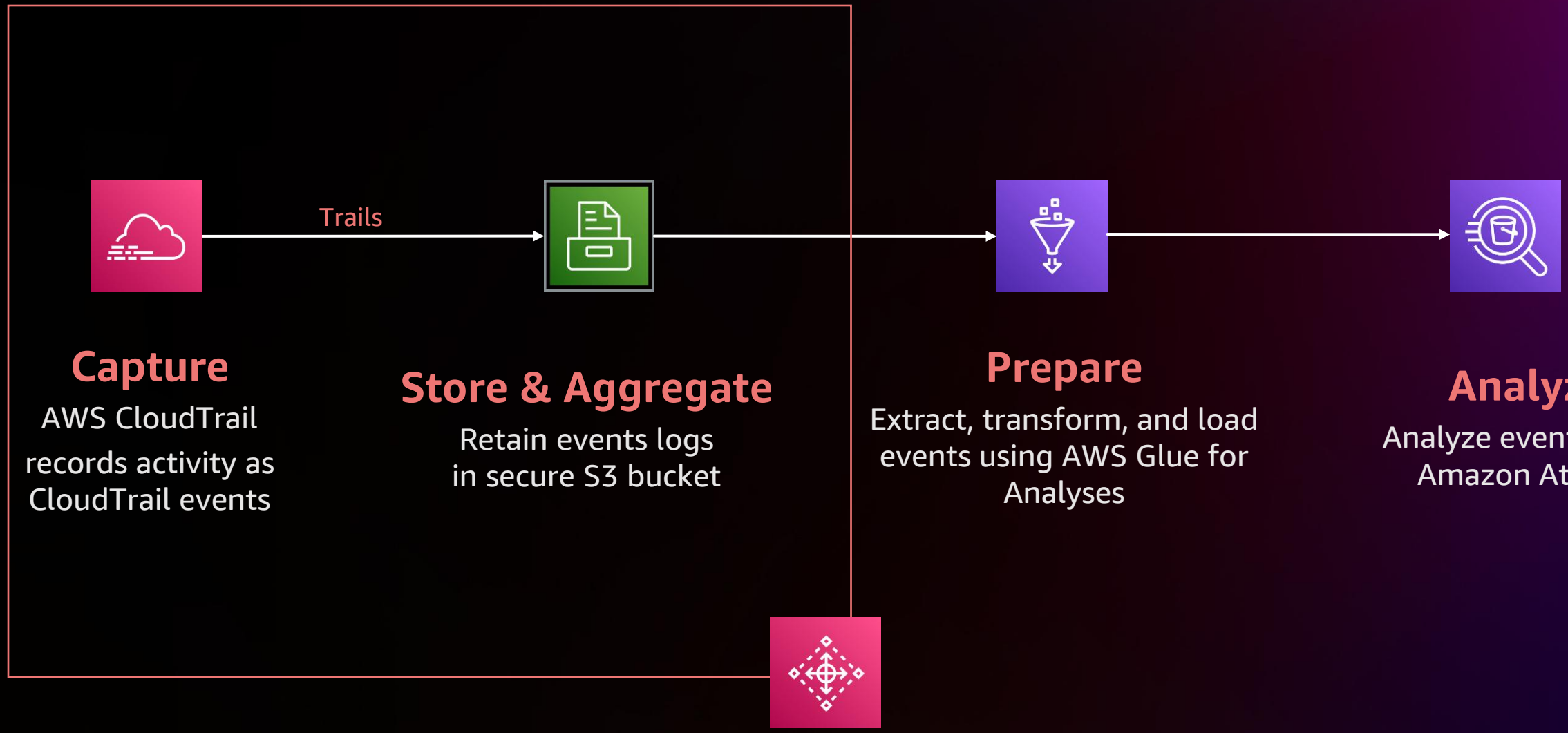
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Questions John needs answered



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

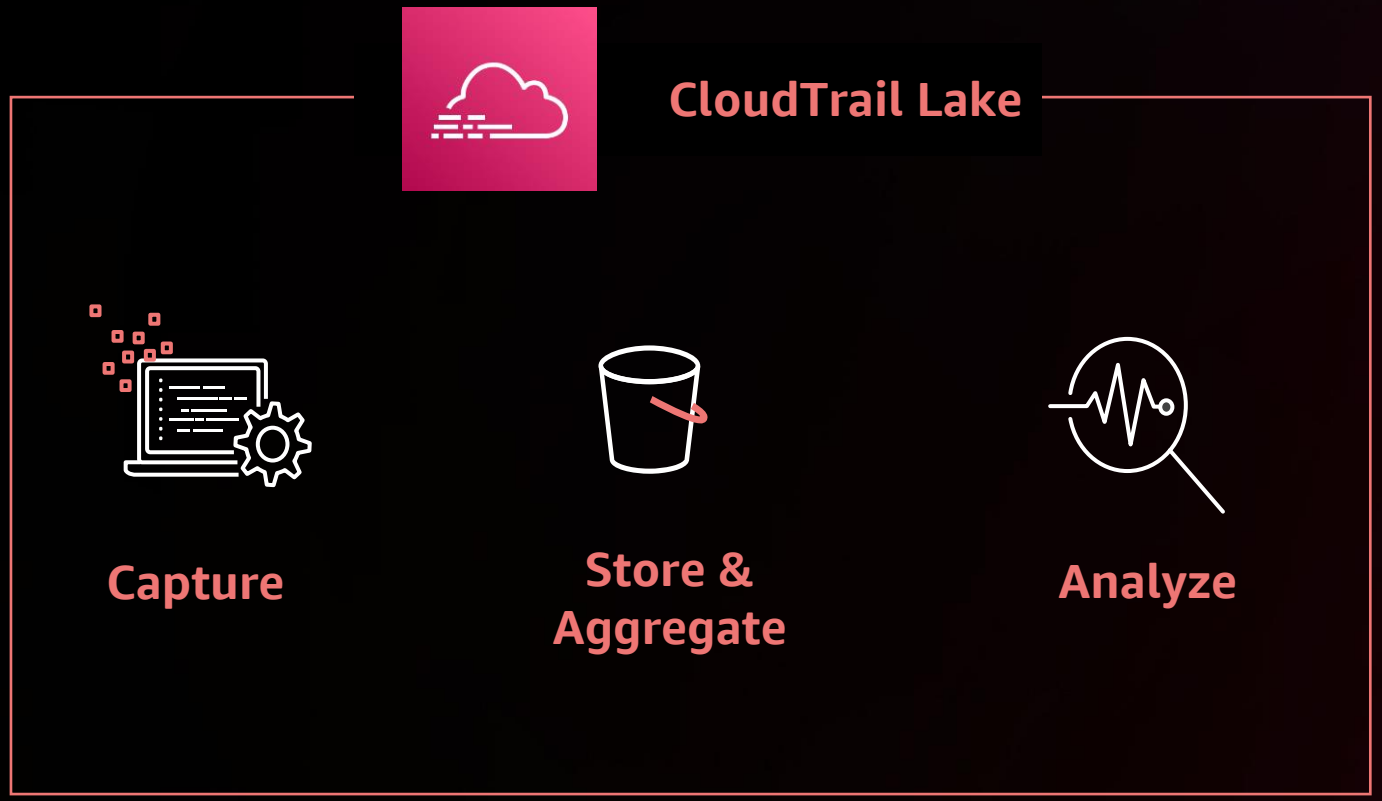
AWS CloudTrail trails



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS CloudTrail Lake

Managed audit data lake to aggregate, immutably store, and analyze audit and security information.



Turn-key solution

Sample queries to get you started

No time spent on ETL

Optimized data ready for querying

Immutable Storage

Read only access for users

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudTrail Lake integrates with AWS Config and AWS Audit Manager

NEW



- Infer who, when & what changed by correlate activity logs with resource configuration & compliance history
- Immutably store and easily search for Audit evidences

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Challenge: Security investigation

Situation: John identified a particular access key that was being used every 10 minutes, but was unable to determine the actions that the user was taking

Solution: John sets up an Event Data Store in CloudTrail Lake, enables management, data events, and configuration items. He then modifies the sample query titled “Investigate user actions”

```
SELECT eventID, eventName, eventSource, eventTime
FROM $EDS_ID
WHERE
userIdentity.accessKeyId = ‘SpecifiedAccessKeyID’
eventTime > '2022-10-06 00:00:00' AND eventTime < '2022-10-09 00:00:00’
AND
userIdentity.username = 'bob’
```

Outcome: John identifies that the user downloaded object (GetObject) from a S3 Bucket.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Challenge – Historical security investigation

Situation: John wants to dig deeper and view all actions taken by the user in the last 30 days for a specific S3 bucket store's customer information

Solution: John imports CloudTrail Logs from the last 30 days, and executes the following query

```
SELECT  userIdentity.arn, eventName, ELEMENT_AT(requestParameters, 'key' )
as S3Object
FROM $EDS_ID
WHERE  ELEMENT_AT(requestParameters, 'bucketName')  = 'SpecifiedBucket'
       AND userIdentity.accesskeyid = 'SpecifiedAccessKeyID'
```

Outcome: John confirms that the user had accessed the information of two customers multiple times in the last 30 days; he shares this information with the central security team for further analysis

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Audit Manager

Collect evidence for audits



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Assurance of risk management – AWS Audit Manager



Assess

Control effectiveness assessment

AWS Audit Manager

Continuously audit your AWS usage to simplify how you assess risk and compliance

Review, customize, or create framework

Review prebuilt frameworks and included controls, customize an existing framework, or define your own

Select a prebuilt or custom framework

Use a prebuilt framework or select your customized framework to begin an assessment

Define the scope of the assessment

Specify the accounts and services in scope in a Region for assessments

Activate assessment to continuously gather evidence

Conduct control reviews and/or delegate to resource owners to validate

Generate audit-ready reports

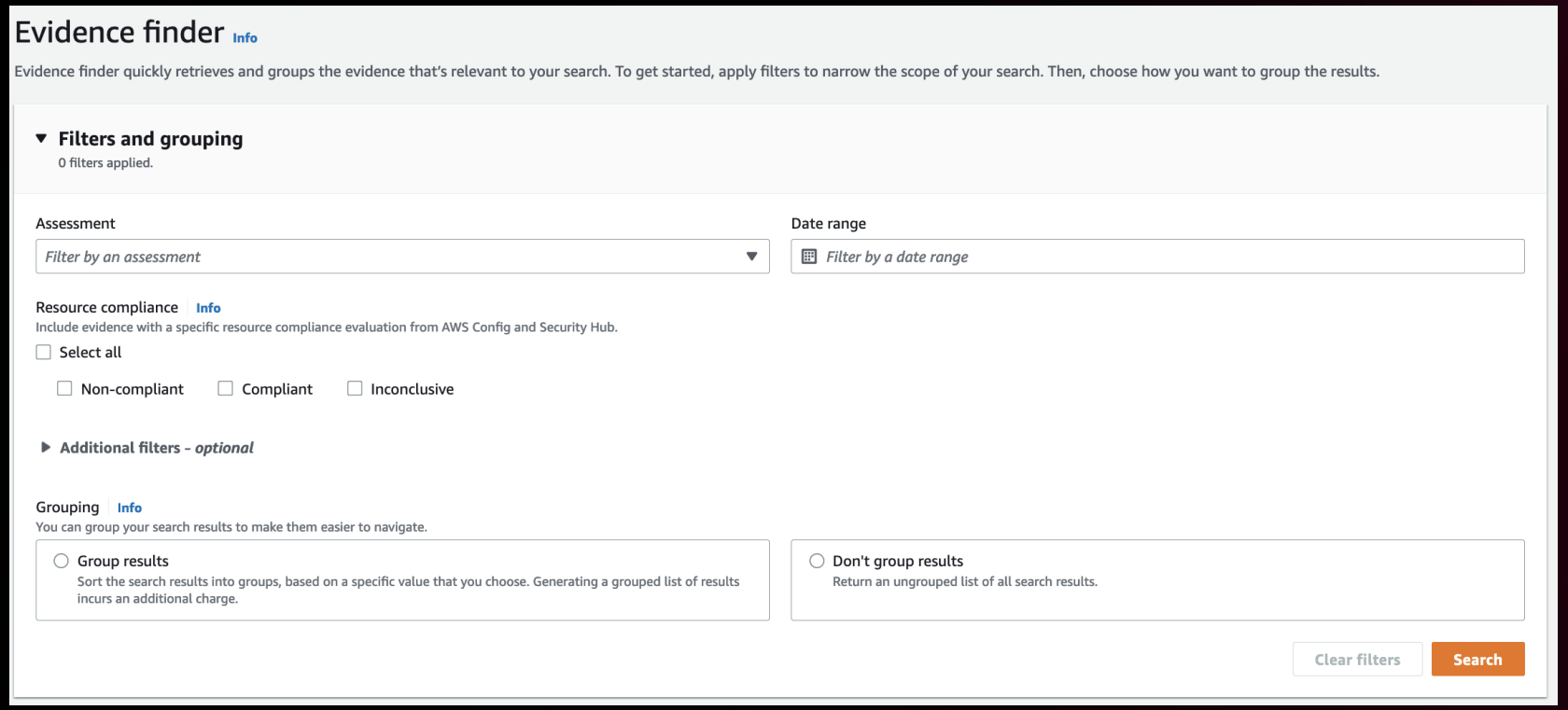
Assessment reports with links to evidence

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Assurance of risk management

AWS AUDIT MANAGER EVIDENCE FINDER

NEW



- Perform targeted searches by multiple criteria, group the results and send the data to an assessment report
- Evidence finder relies on event data store in AWS CloudTrail Lake to allow the query capability

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Demo

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key takeaways



01

AWS Config

Core for compliance evaluation

02

AWS CloudTrail Lake

Expedite operational, compliance, and audit queries at scale

03

AWS AWS Audit Manager

Simplify and automate evidence collection at scale

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Want to see more AWS Cloud Operations?

Please complete the session survey in the mobile app



Ask us anything at our kiosks in the AWS Village Expo



Find related sessions in our re:Invent blog

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources



Cloud compliance and assurance samples
https://bit.ly/3AWupZ5



Cloud operations samples GitHub repo
https://bit.ly/3PE8LwO

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.