AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

COP208

AWS Managed Services: Security, compliance, and operations

Stephen Bowie (He/Him)
Security Leader
AWS Managed Services

Manuel Morales (He/Him)
Sr. Product Manager – Technical
AWS Managed Services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Who we are and what are we going to do

- Scenario 1: Maintain an asset inventory
- Scenario 2: Make changes in the cloud
- Scenario 3: Threat detection and response
- Scenario 4: Improve health and availability

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 1: Asset inventory

- How do you accurately identify assets in the cloud so that you can protect them?
- How can you query the current configuration state of AWS resources for audit, compliance, or operational troubleshooting?



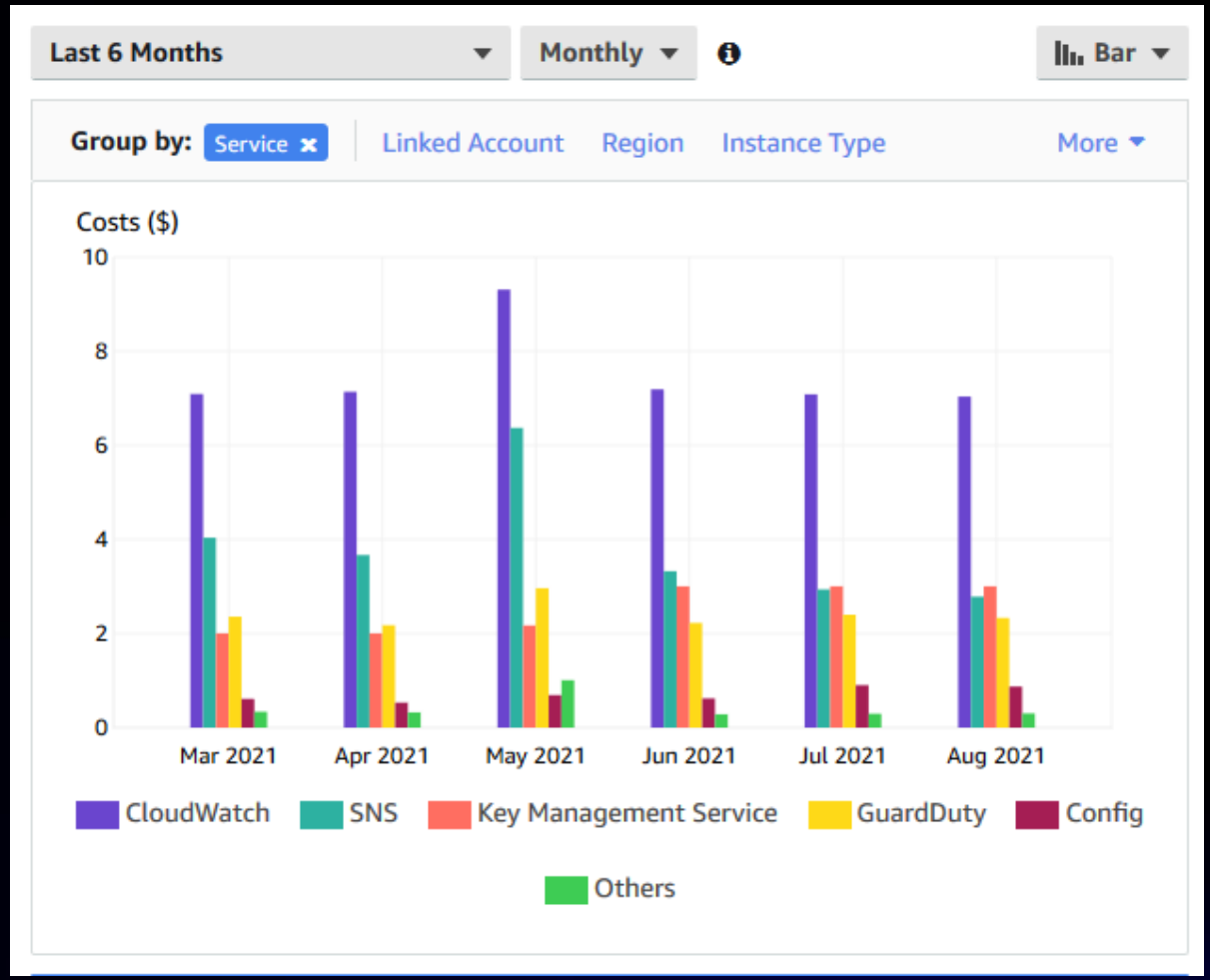
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 1: Asset inventory

MULTIPLE OPTIONS

With AWS, you can use multiple tools to see exactly what cloud assets your company is using at any moment

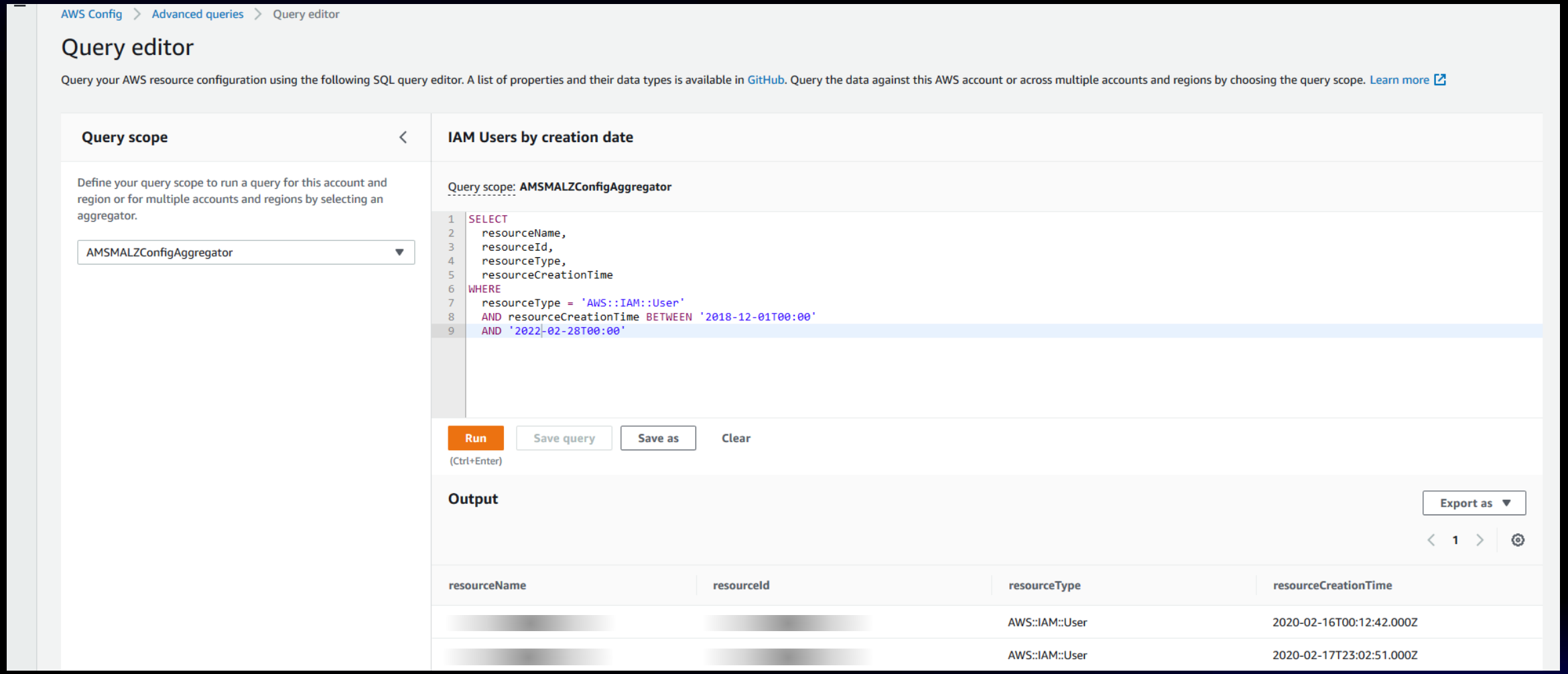
- AWS Cost Explorer
- Tag Editor
- AWS Systems Manager
- AWS Config



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 1: Asset inventory

USE AWS CONFIG AGGREGATOR TO HAVE A VIEW OF YOUR RESOURCES



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 2: Change management

- How do you mitigate security risks while making changes?
- How do you keep your infrastructure compliant?
- How do you scale your security and Ops team over time?
- How do you handle risky changes?



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 2: Detective model

UNLEASH THE SPEED OF YOUR DEVELOPER TEAMS



Detect

Gain visibility into your organization's security and compliance posture



Respond and remediate

Leverage event-driven automation to quickly remediate and secure your AWS environment in near-real time



Track and iterate

Review your accepted and non-remediated risks frequently. Define goals to remediate findings over time

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 2: Preventative model

IDEAL FOR HIGHLY REGULATED ENVIRONMENTS



Keep people away from changes and data

Define who can make changes with a strong identity foundation



Define standards and automate changes

Build a library of automated changes that are pre-vetted by security and operations teams



Anticipate, learn, and refine

Create a process for emergency, risky, or non-standard changes. Drive automation from lessons learned and track risks

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How would you react to these requests for change?

• Operator requests persistent FTP access from a legacy data center into the production VPC	Yes, for 30 days only
• Application owner asks for SMBv1 to be enabled to support an application	Yes, for 30 days only
• Customer engineer requests that an EC2 instance is made directly accessible from the internet	Yes, app vendor requirement
• App owner escalates asking to only patch a server quarterly	Depends
• Developer requests persistent access to the production VPC from their personal computer at home	Absolutely not

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 3: Threat detection and response

- How can you detect account compromise threats?
- How do you keep your resources secure and compliant to your standards?
- How do you effectively respond to security findings at scale?



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 3: Threat detection and response

MANAGING THREAT DETECTION AT SCALE

1. Deploy security tools and controls to keep them operating

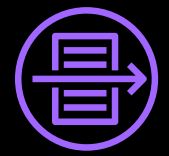

Amazon GuardDuty


Amazon Macie


AWS Config


AWS CloudTrail


AWS Marketplace


VPC Flow logs

2. Have a process to receive and respond to security events
3. Reduce noise, prioritize alarms, automate responses
4. Test your response to different scenarios with GameDays

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 4: Health and availability

- How do you monitor the health of your AWS infrastructure?
- How can you make continuous and incremental improvement to evolve your operations?



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 4: Monitoring and response

THE USUAL PATH



'Someone' detects something is wrong



Relies on people to respond to incidents



Manual investigation of failures

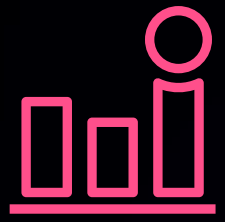


Trial-and-error remediation

THE AMS PATH



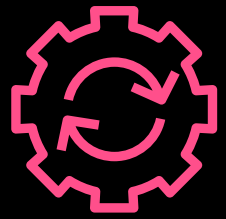
Metrics automatically collected using Amazon CloudWatch



Library of Amazon CloudWatch alarms detect when resources are unhealthy



An OpsItem gets created with information about the resources and automated runbooks



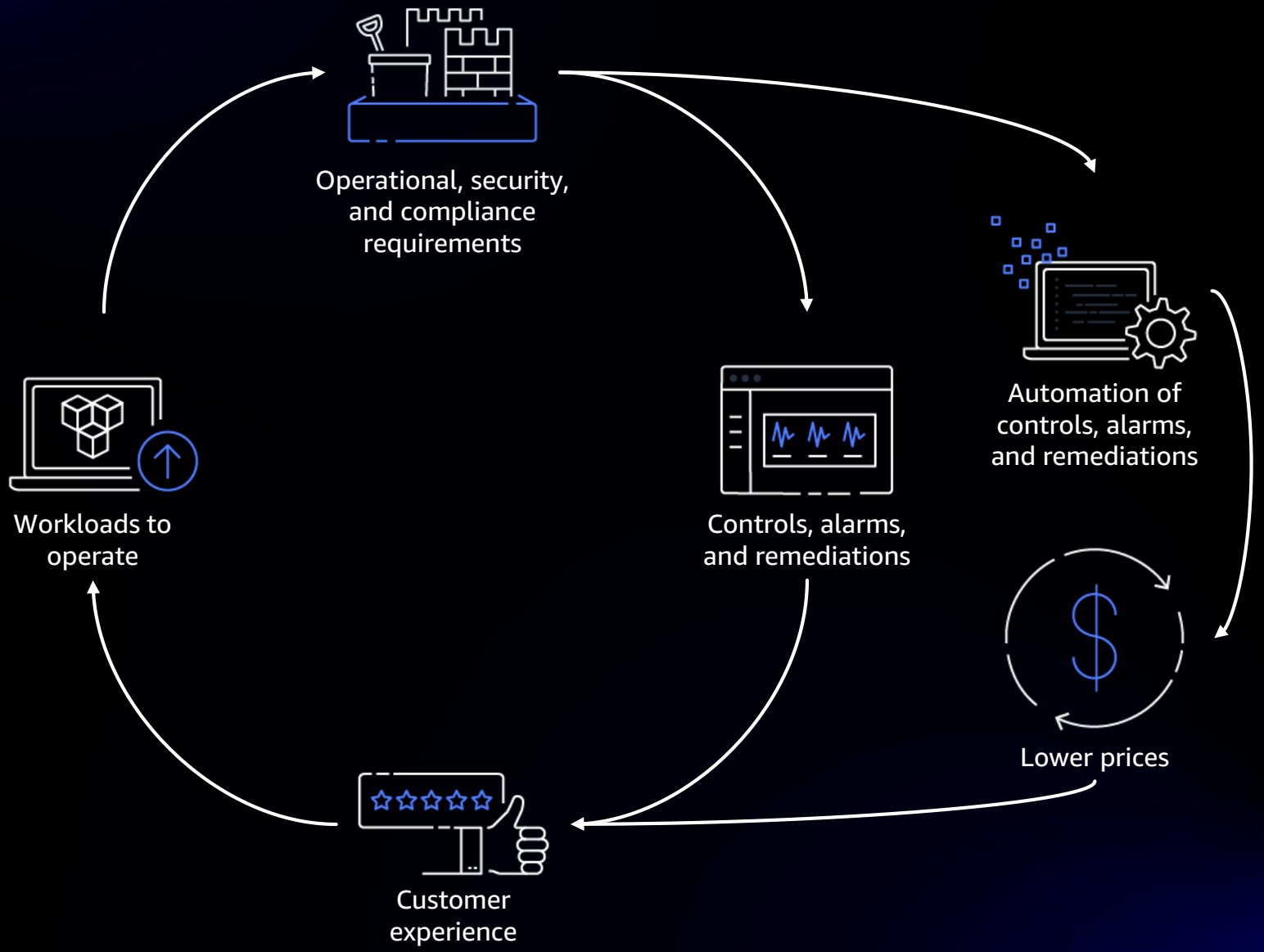
Automated runbooks diagnose, remediate the issue, or contact Operations team

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scenario 4: Monitoring flywheel

THE USUAL PATH



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Additional talks

LEARN MORE ABOUT AMS AND

- COP205 – Cloud operations at scale with AWS Managed Services
- SEC309-R2 – Adversary emulation for incident-response readiness
- COP219 – AWS Cloud Operations Model panel discussion: A 360-degree view

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Stephen Bowie
shb@amazon.com

Manuel Morales
manuleo@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.