AWS re:Invent

ARC338-R

How Goldman Sachs minimizes the impact of managing events

Elaine Hardwick
Vice President
Goldman Sachs

Sujoy Saha
Software Engineer
Goldman Sachs

Brian Carlson
Operational Excellence Lead
AWS Well-Architected
Amazon Web Services

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Agenda

- Introduction
- Operational challenges
- Automating operational excellence
- Case studies: Lambda deployment and Amazon EC2 backup
- Conclusions

Introduction

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

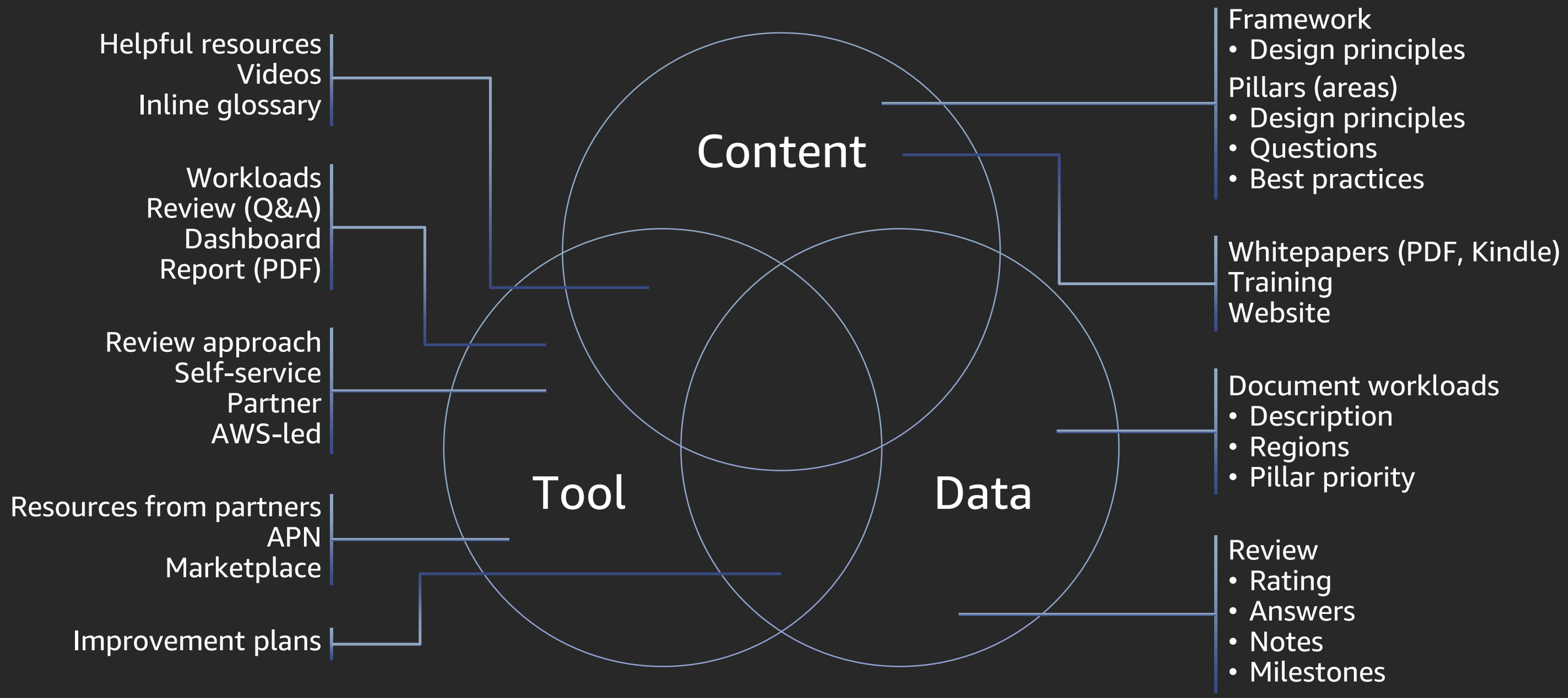
aws

AWS Well-Architected

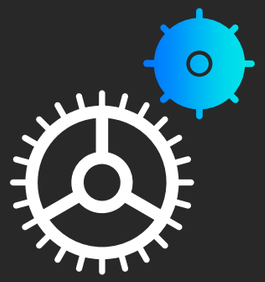
https://aws.amazon.com/well-architected/

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is AWS Well-Architected?



Pillars of AWS Well-Architected



Operational excellence



Security



Reliability

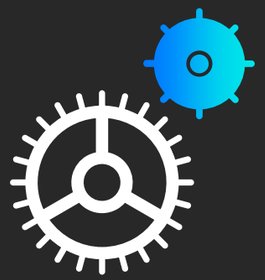


Performance efficiency



Cost optimization

The operational excellence pillar



Operational excellence

The operational excellence pillar includes the ability to run systems and gain insight into their operations in order to deliver business value, and to continuously improve supporting processes and procedures

Operational excellence design principles

- Perform operations as code
- Refine operations procedures frequently
- Anticipate failure
- Learn from all operational failures










Design with Ops in Mind

Operational excellence with AWS Systems Manager OpsCenter

Measure the achievement of business outcomes

Understand the health of your workload

Alert when outcomes are at risk

Automate responses to well-understood events

gate operational issues

- Use Amazon CloudWatch Events and AppInsights to identify operational issues
- Centrally manage work items from across AWS services

Anticipate failure

Use a process for event and incident management

Define escalation paths

Diagnose and remediate

- OpsItems bring together relevant info to investigate and diagnose issues
- Take direct action using Systems Manager automation
- Reduce MTTR (mean time to resolution)

Anticipate failure

Perform operations as code

Refine operations procedures frequently

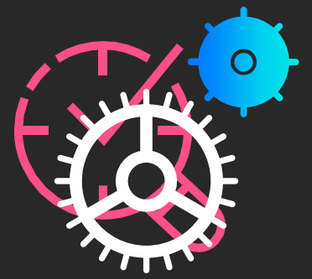
Have a process per alert

Refine operations procedures frequently

Learn from all operational failures



AWS Systems Manager



OpsCenter

Operational excellence

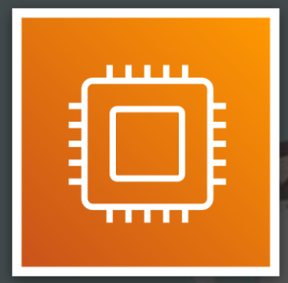
Who we are

- Goldman Sachs brings people, capital, and ideas together to help our clients and the communities we serve
- **Innovation** is at the heart of Goldman Sachs
- As our services grow and evolve, we believe that public cloud brings the scaling, flexibility, and innovation we need
- Partnering with AWS has helped us adopt public cloud while focusing on **operational excellence**



Use cases

Cloud adoption



Compute extension



Lift & shift



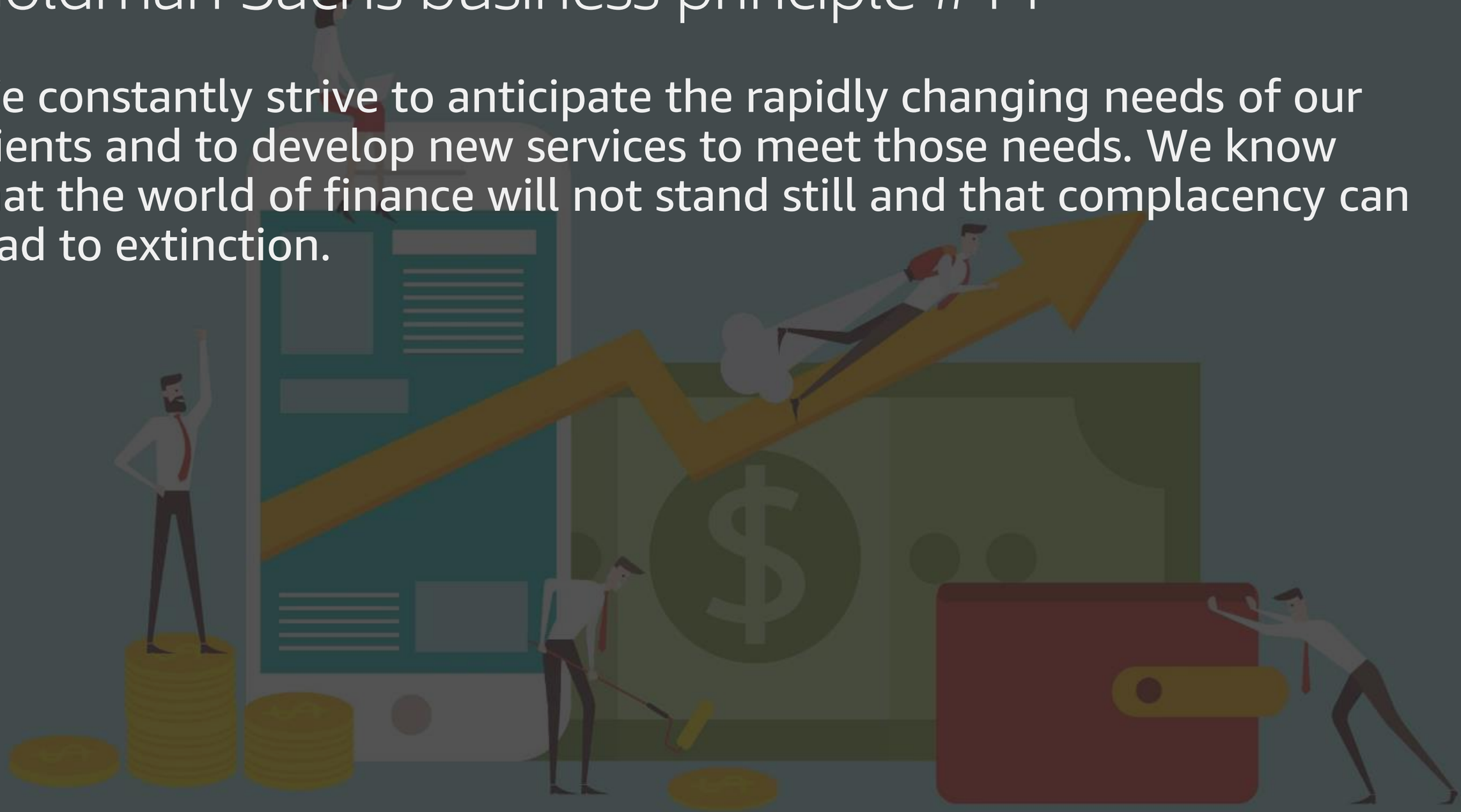
New innovation



Business continuity/resiliency

Goldman Sachs business principle #11

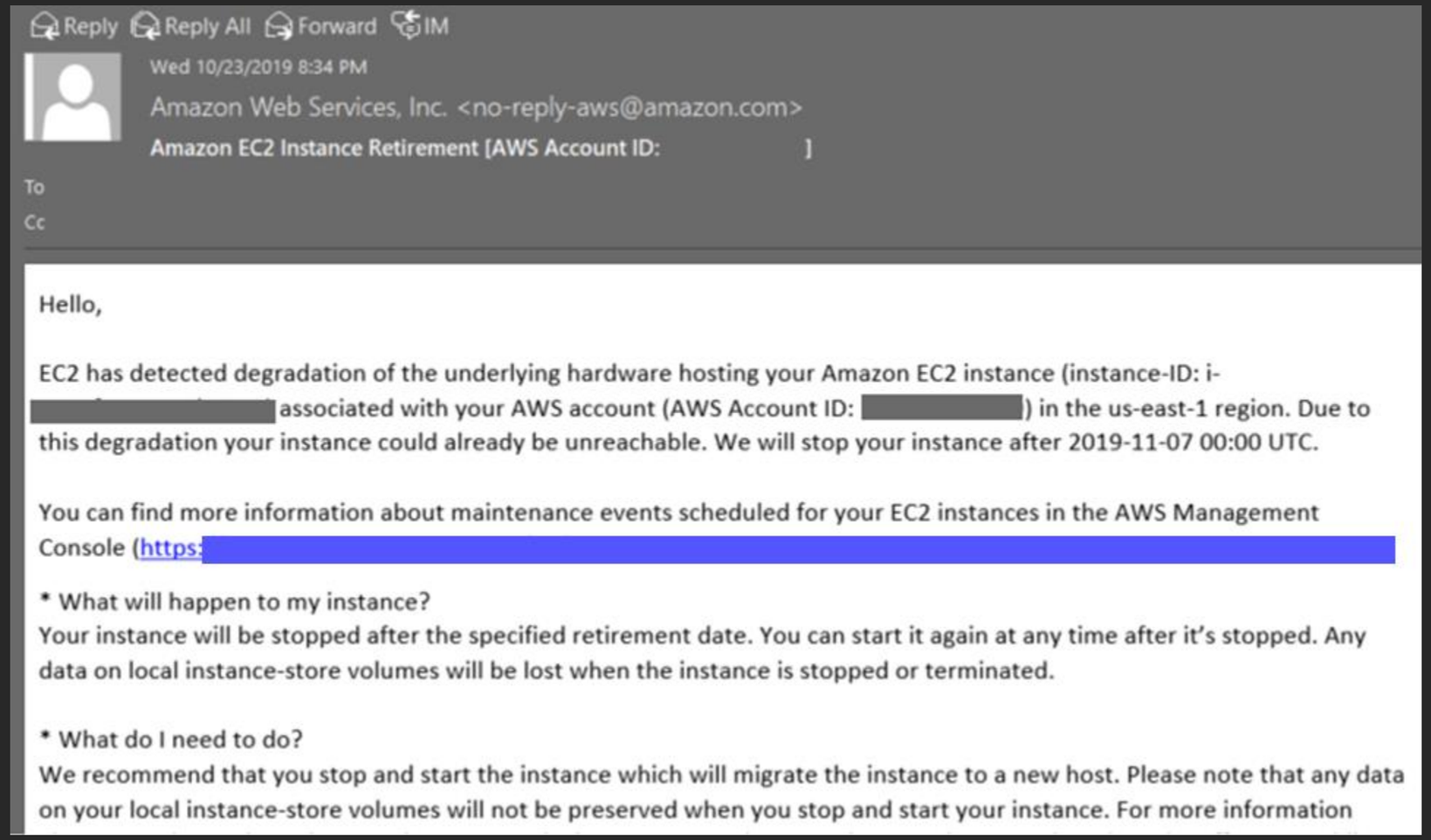
We constantly strive to anticipate the rapidly changing needs of our clients and to develop new services to meet those needs. We know that the world of finance will not stand still and that complacency can lead to extinction.



Operational challenges

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What would you do?



Reply Reply All Forward IM

Wed 10/23/2019 8:34 PM

Amazon Web Services, Inc. <no-reply-aws@amazon.com>

Amazon EC2 Instance Retirement [AWS Account ID:]

To

Cc

Hello,

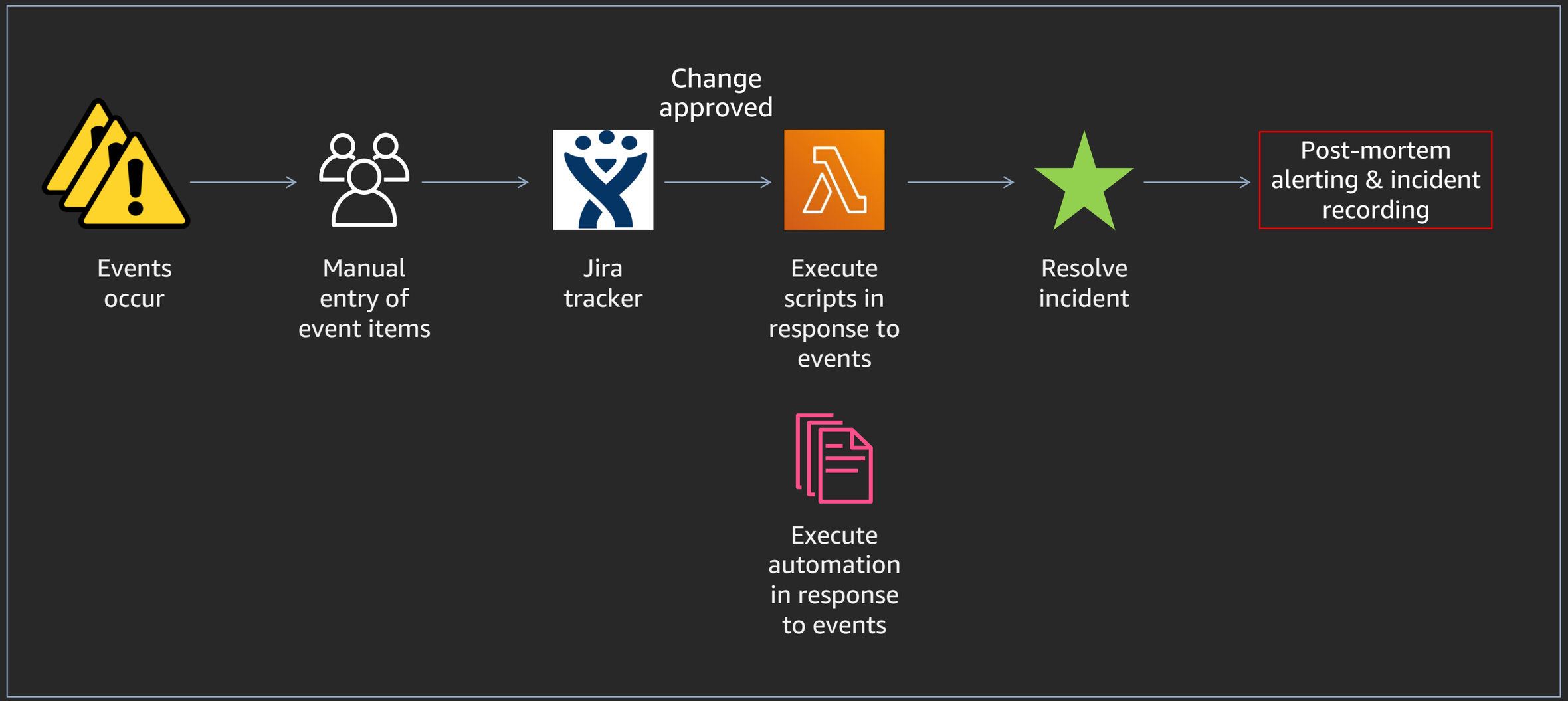
EC2 has detected degradation of the underlying hardware hosting your Amazon EC2 instance (instance-ID: i-[redacted] associated with your AWS account (AWS Account ID: [redacted]) in the us-east-1 region. Due to this degradation your instance could already be unreachable. We will stop your instance after 2019-11-07 00:00 UTC.

You can find more information about maintenance events scheduled for your EC2 instances in the AWS Management Console (https:[redacted]

* What will happen to my instance?
Your instance will be stopped after the specified retirement date. You can start it again at any time after it's stopped. Any data on local instance-store volumes will be lost when the instance is stopped or terminated.

* What do I need to do?
We recommend that you stop and start the instance which will migrate the instance to a new host. Please note that any data on your local instance-store volumes will not be preserved when you stop and start your instance. For more information

Operation Event Management System



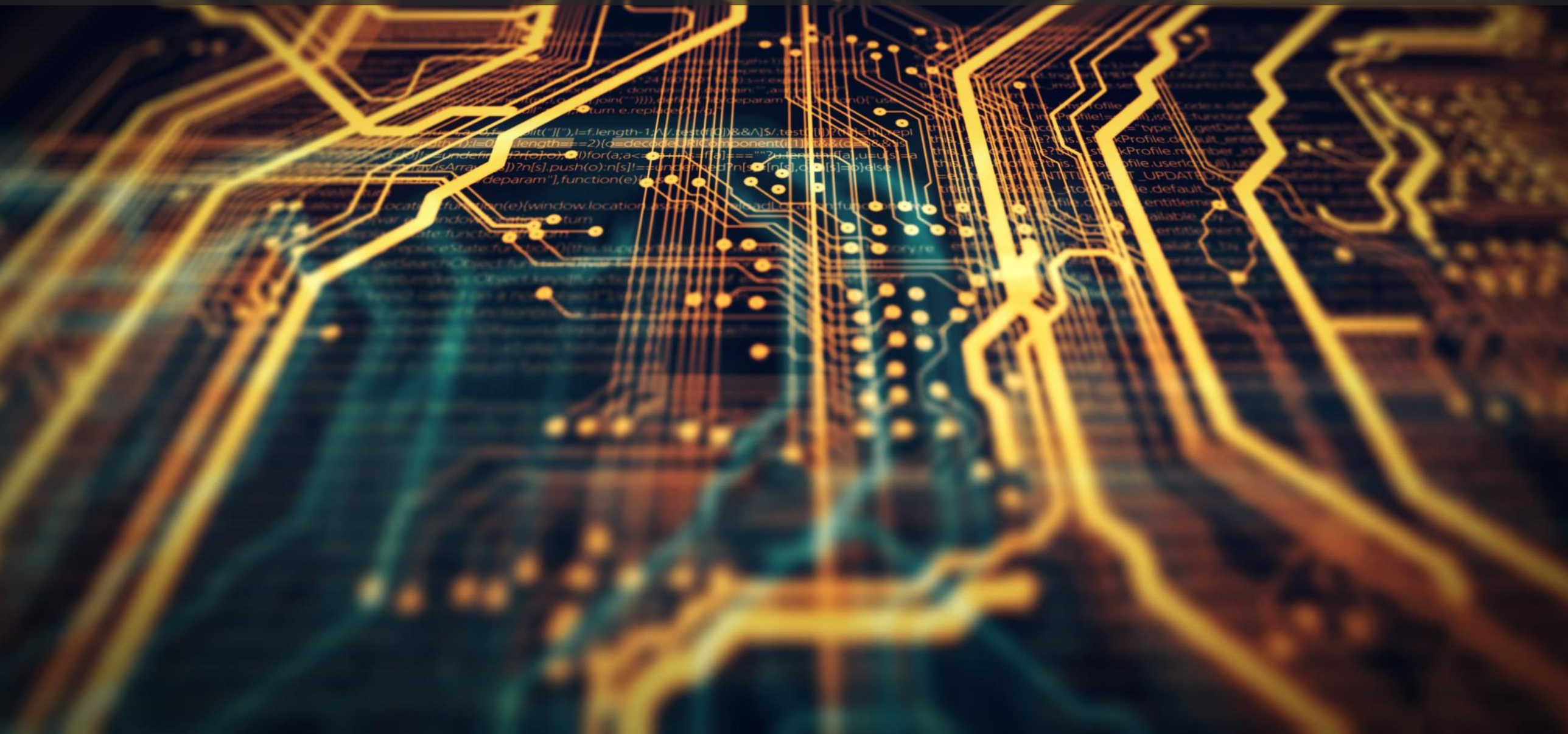
Monitoring operations across multiple accounts and regions



Manual intervention is overwhelming



Escalation paths not clearly defined

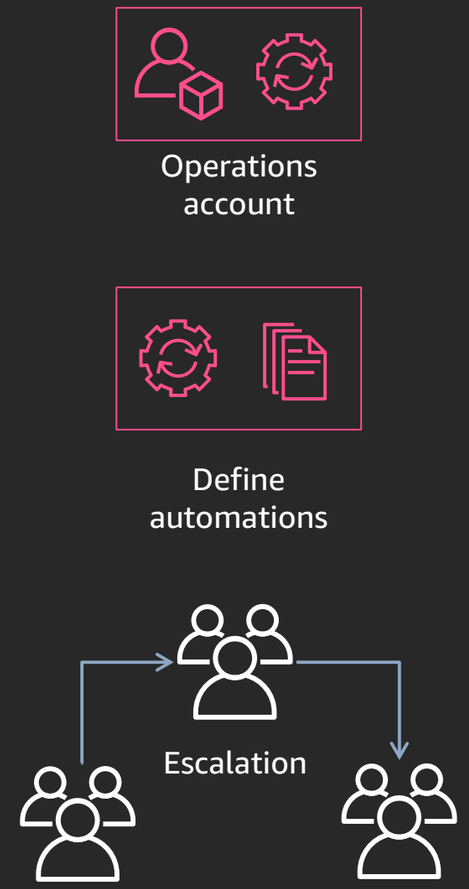


Resolution operations are not codified



Operations excellence in micro account model

- Aggregate operation items centrally
- Define automated workflows for frequent incidents
- Define escalation path for non-resolvable incidents



GS requirements for operations excellence

- Track incidents and events
- End-to-end incident recording for audit
- Reduce incident occurrences
- Reduce manual intervention

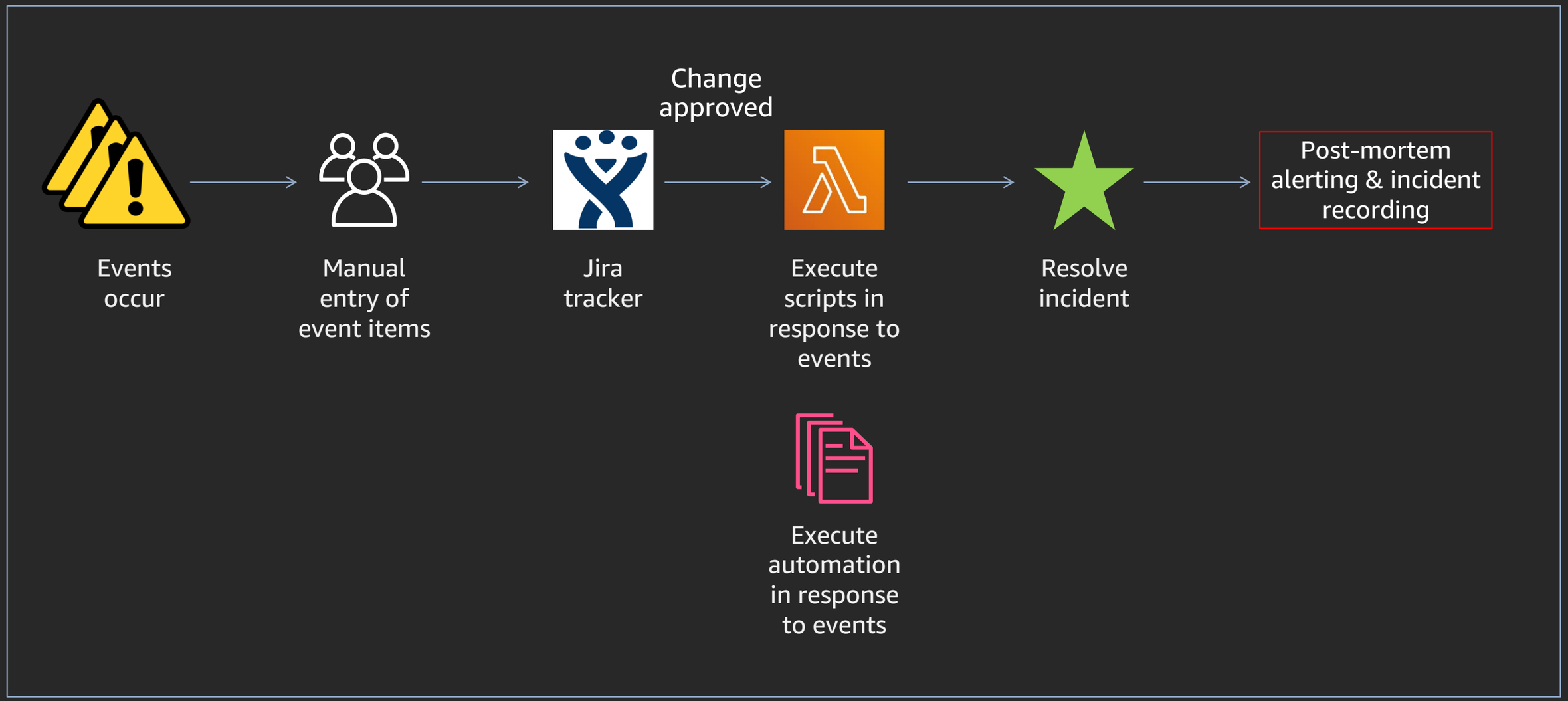


Incident recording

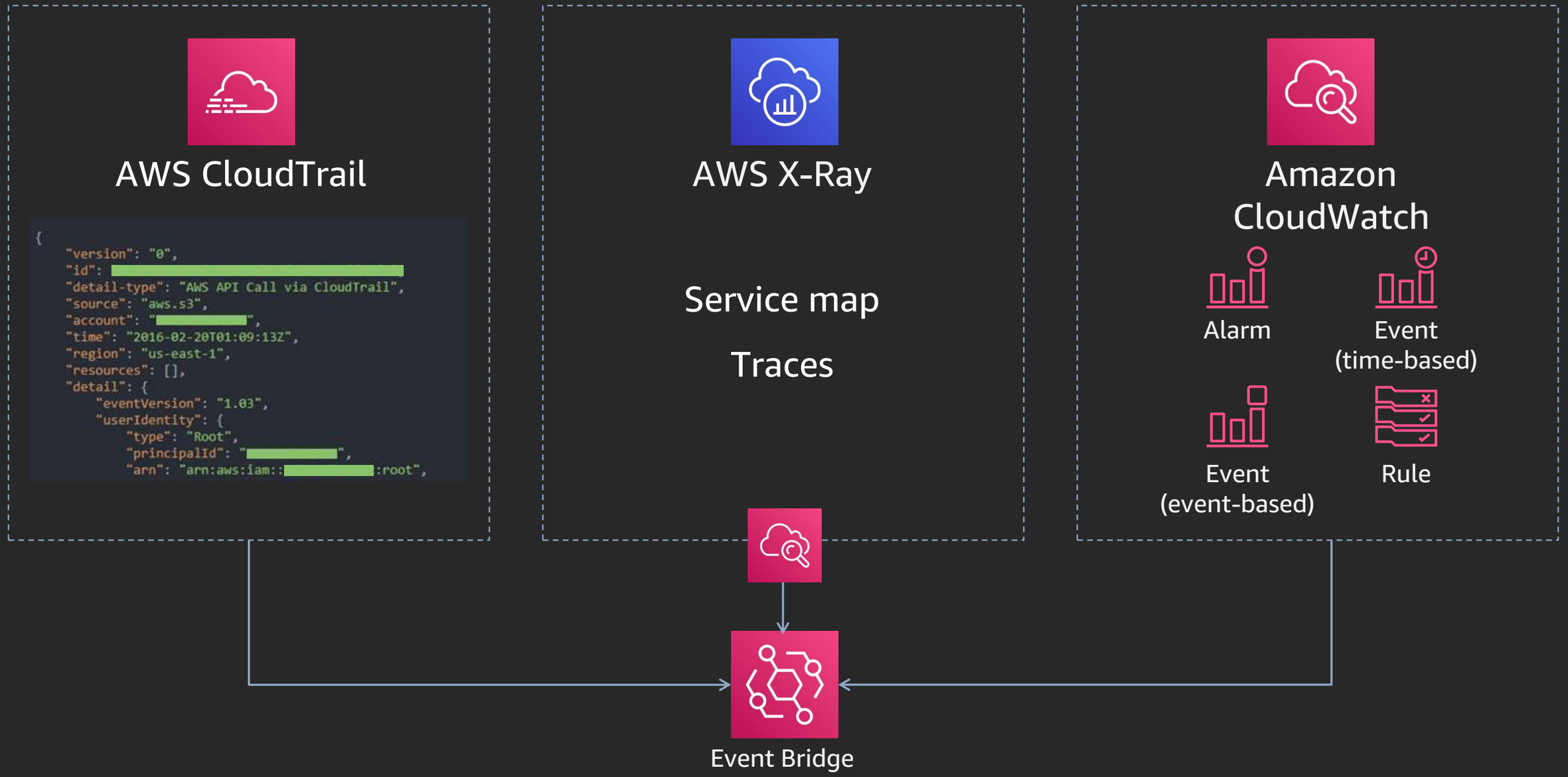
Achieving operational excellence

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Operation Event Management System

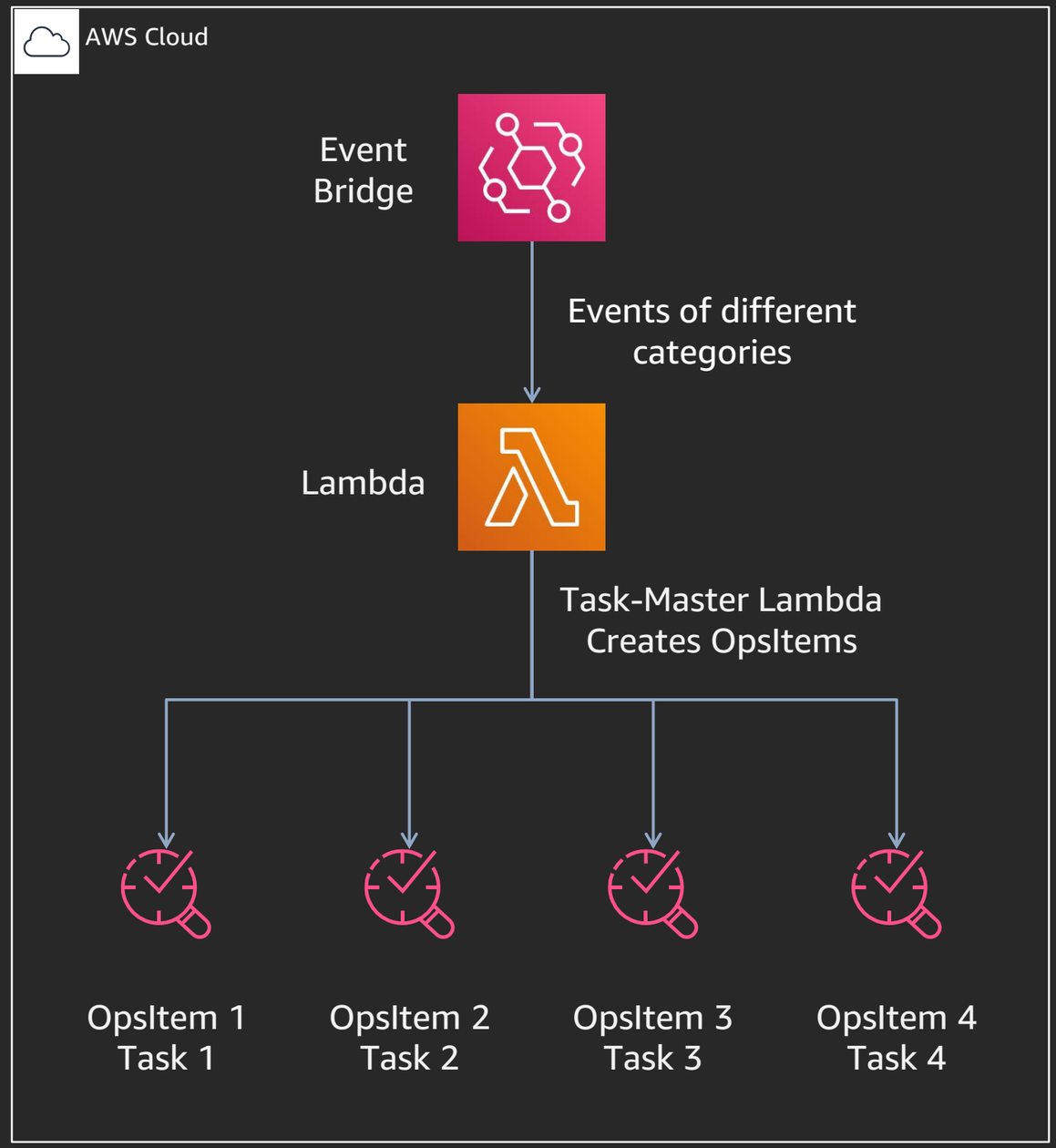


Central event aggregation

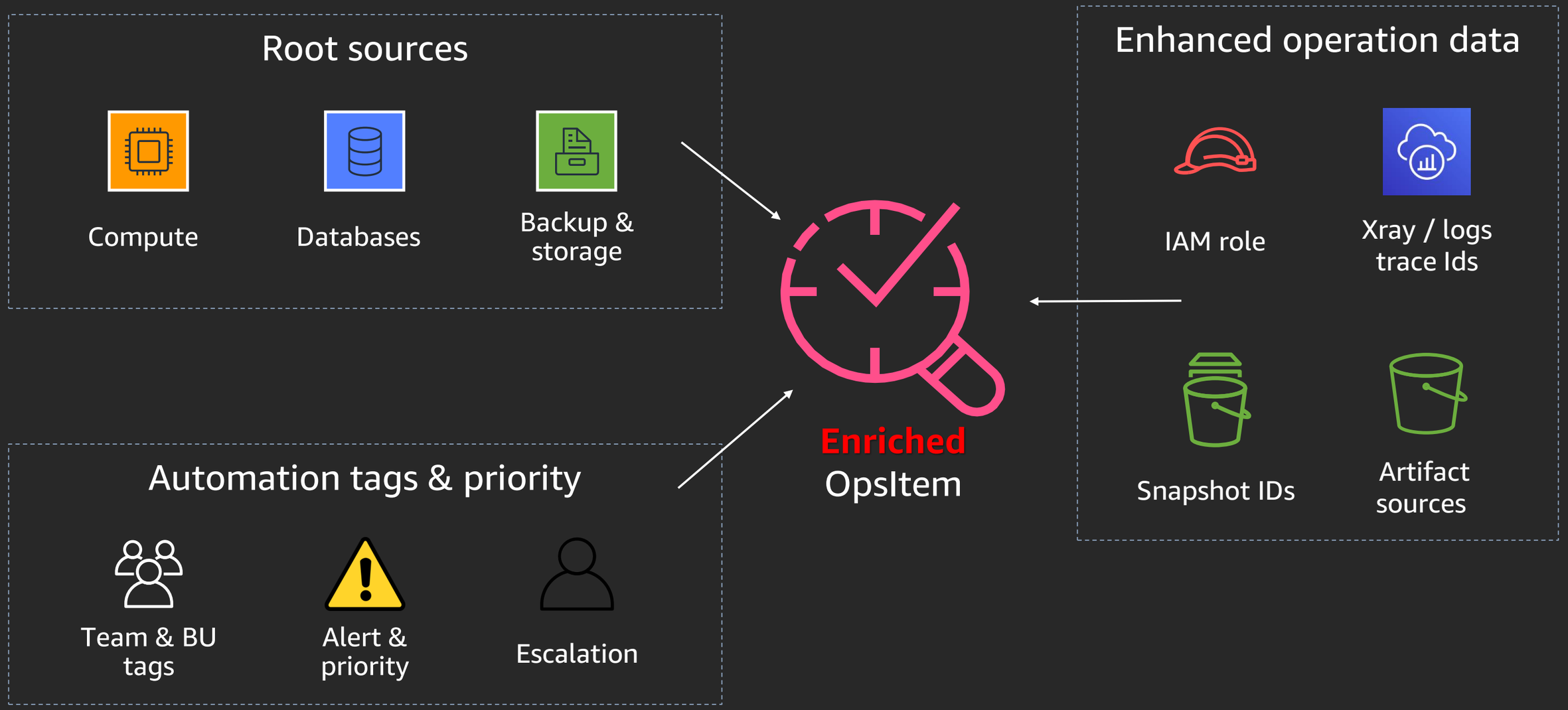


Task-Master Lambda

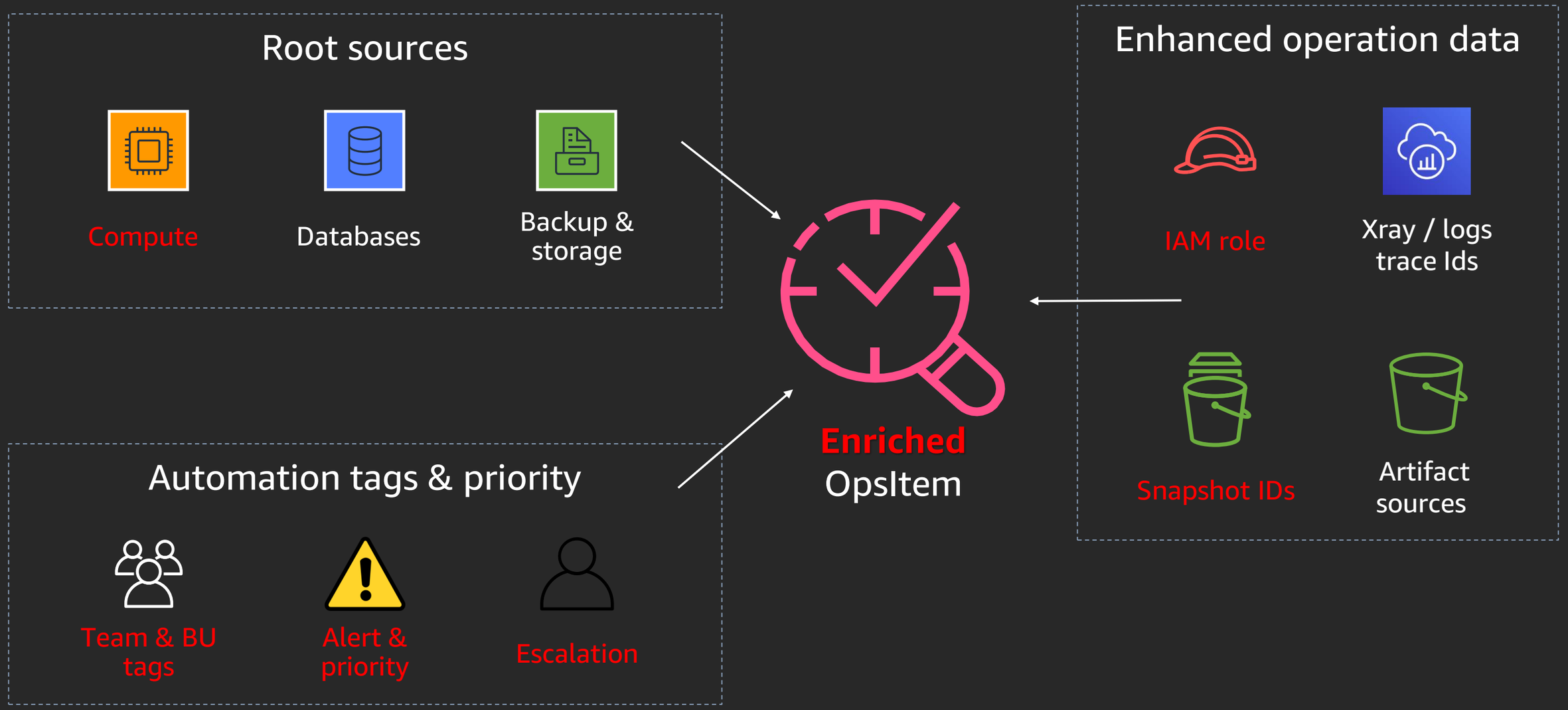
- Parses events/incidents
- Analyze source & event category
- Create and enrich OpsItem with contextual data
- Tag OpsItem with relevant escalation info
- Determine remediation workflow to use



OpsItem event enrichment

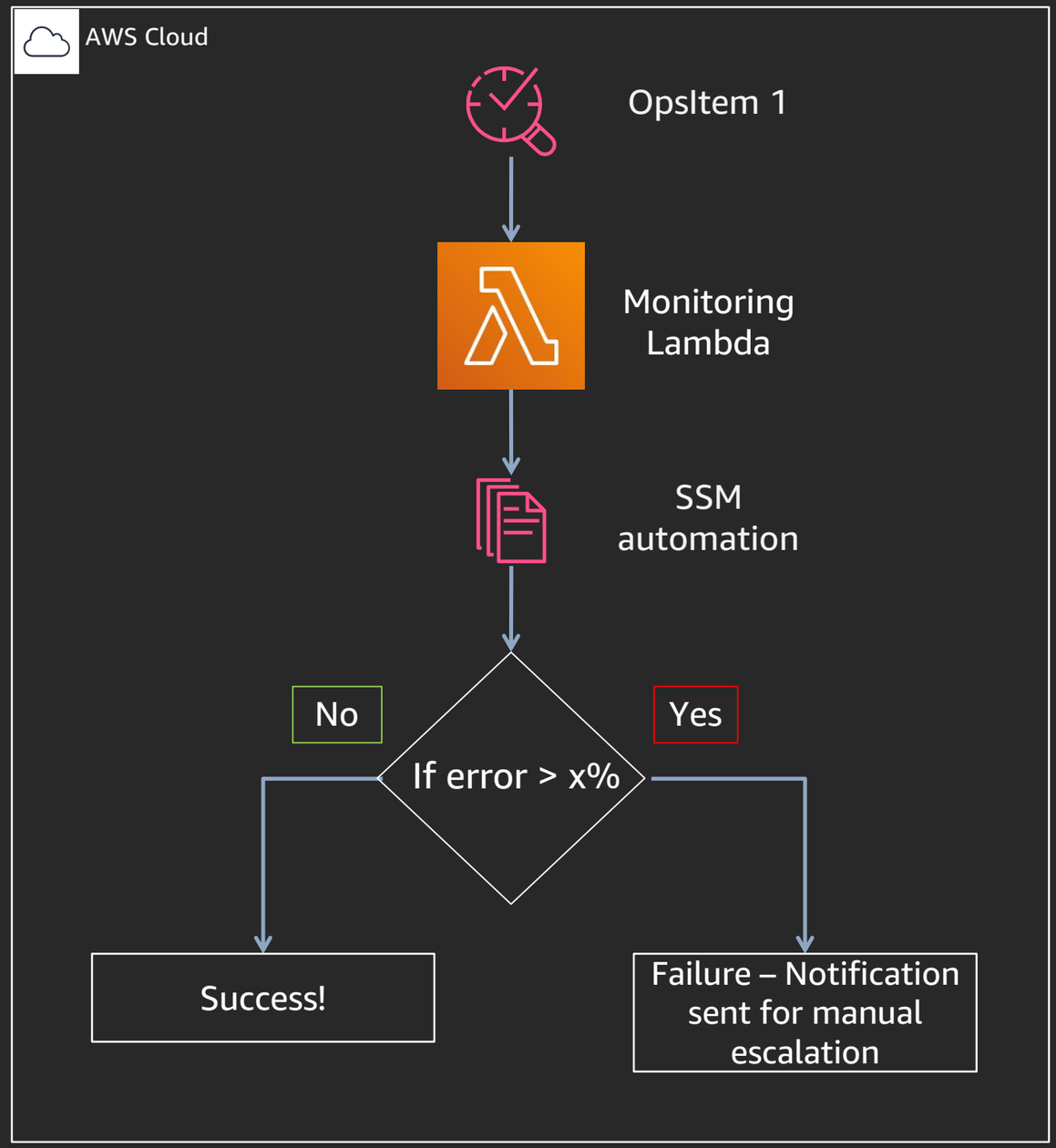


EC2 degradation event enrichment



OpsMonitor Lambda

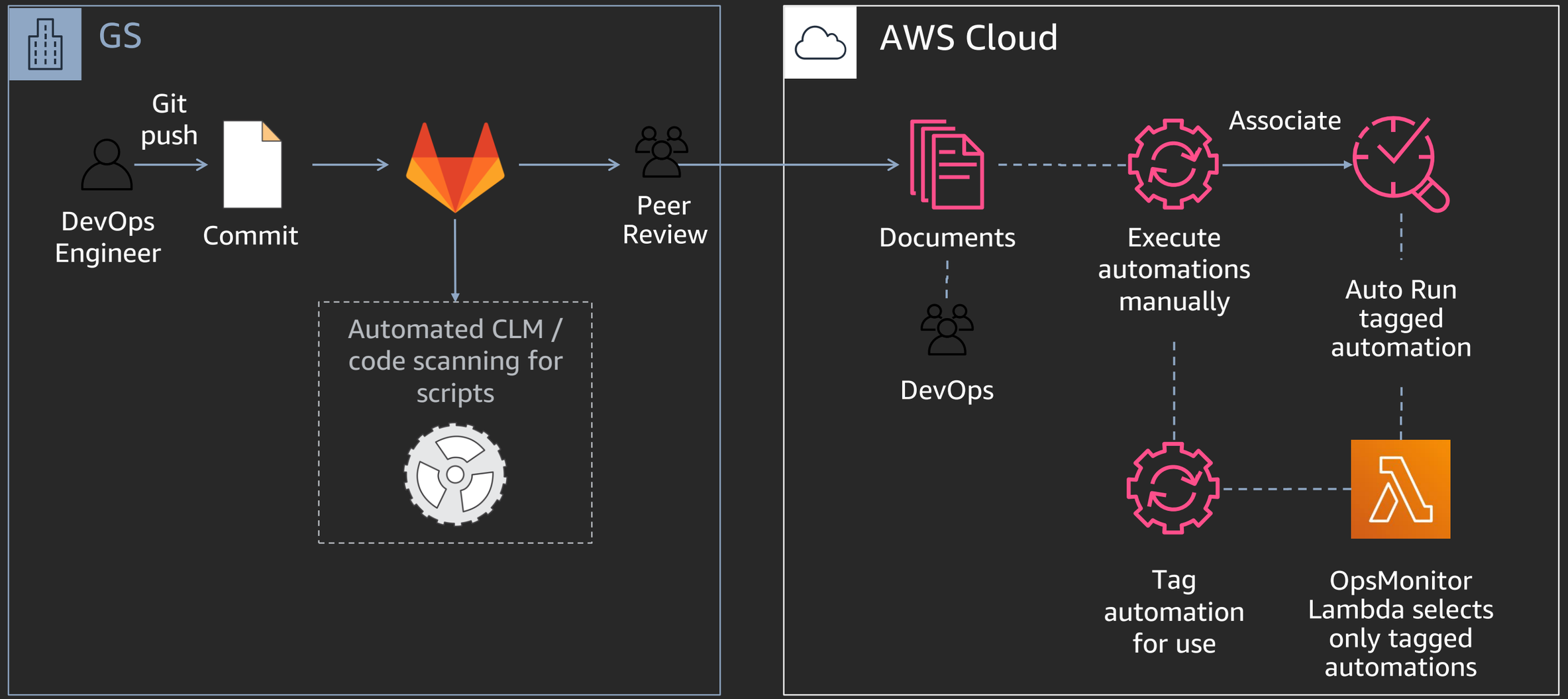
- Triggered by OpsItem creation
- Executes SSM document
- Configures rate controls for automation execution



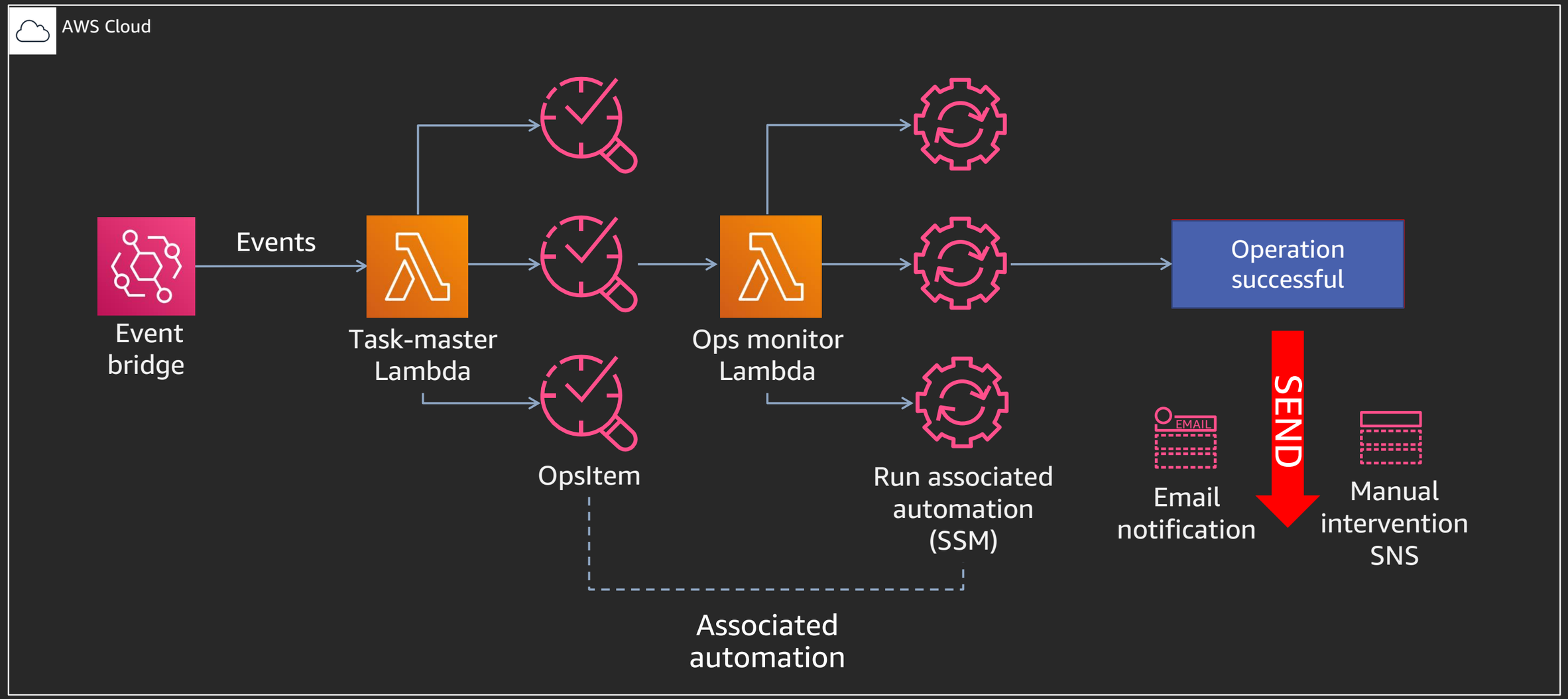
Alerting on automation failure

Alert categories	Failure form	Sample notification platforms	Escalation & awareness	Track
Critical	Automation has 100% failed, manual intervention needed	Team email/pager duty/other alert platforms	L1 Support, L2 Support, DevOps	Yes
High	Failures > threshold, manual interaction needed	Team email/pager duty	L1 Support, L2 Support	Yes
Medium	Minor failures < threshold during automation run time	Team email	L1 Support	Yes
Low	Any transient error, no impact on operation outcome	SNS alerts/capture details	None	No

SDLC for scripts for event response



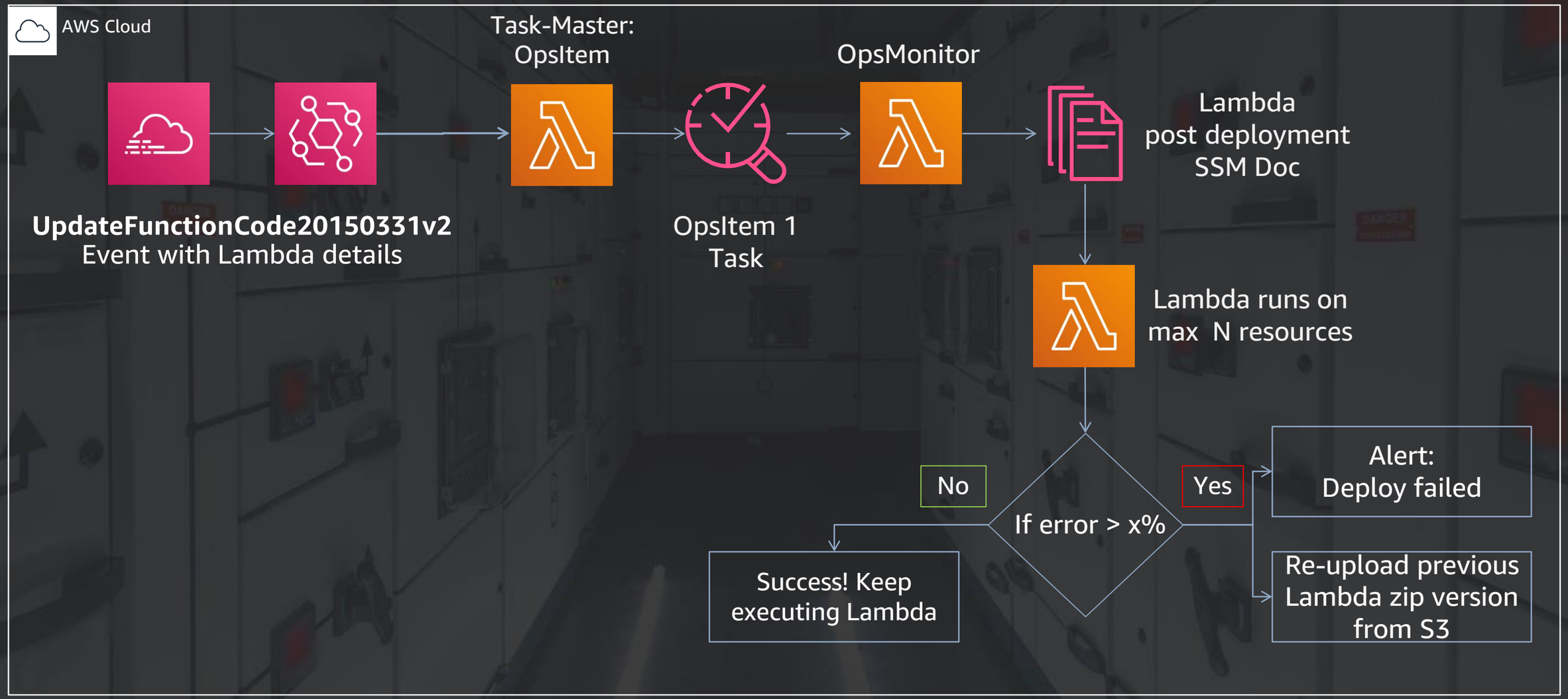
Automated event response system



Case study: Lambda deployments

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lambda post-deployment checkout



Case study: EBS backups

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup

Key operations

- Centrally manage in vaults
- Automate schedules and retention
- Improves compliance



AWS Backup

EBS backup module

Key functionality

- Users select resources with a tag
- LifeCycle policy enabled
- Stored in central vault
- Recovery point tags

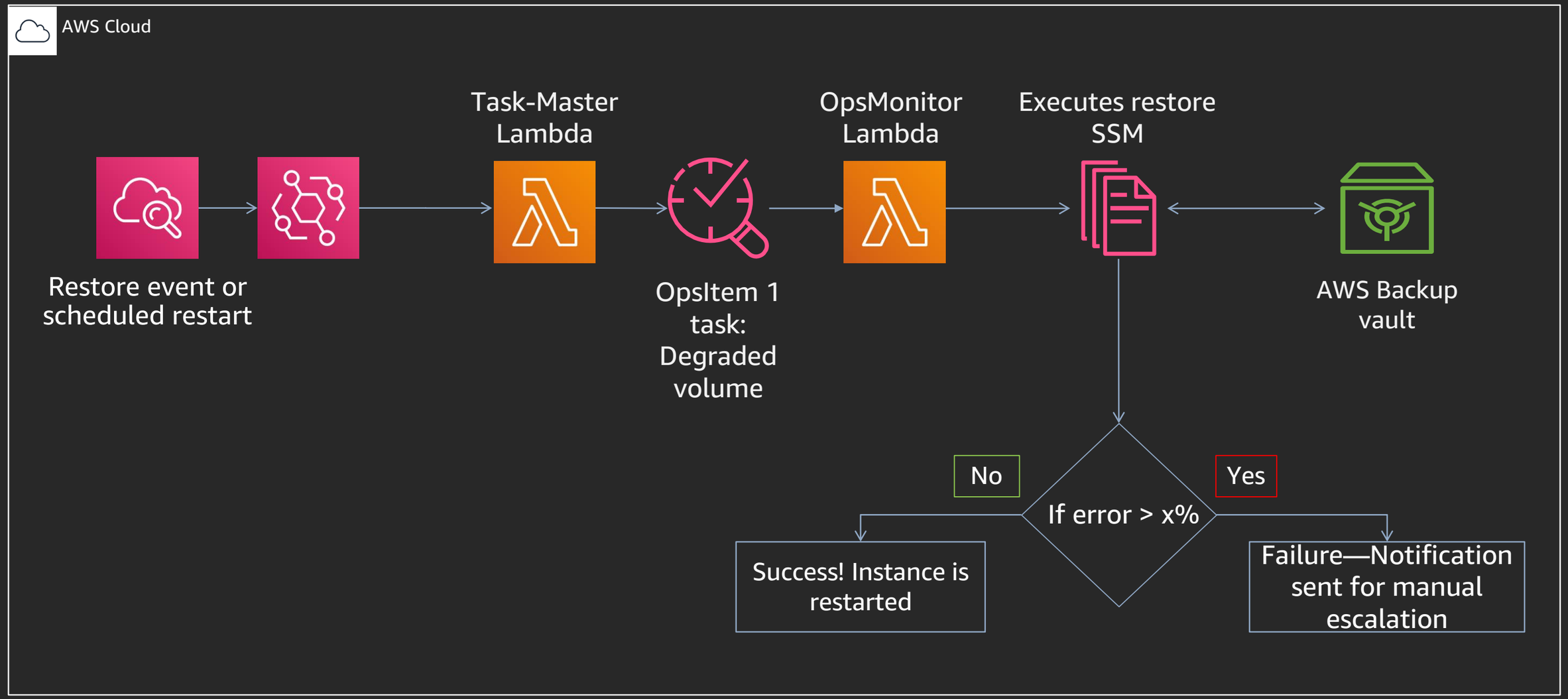
```
resource "aws_backup_plan" "example" {
  name = "tf_example_backup_plan"

  rule {
    rule_name = "tf_example_backup_rule"
    target_vault_name = "${aws_backup_vault.test.name}"
    schedule = "cron(0 12 * * ? *)"
  }

resource "aws_backup_selection" "example" {
  iam_role_arn = "${aws_iam_role.example.arn}"
  name = "tf_example_backup_selection"
  plan_id = "${aws_backup_plan.example.id}"

  selection_tag {
    type  = "STRINGEQUALS"
    key   = “cat"
    value = “nala"
  }
}
```

EBS backup restore



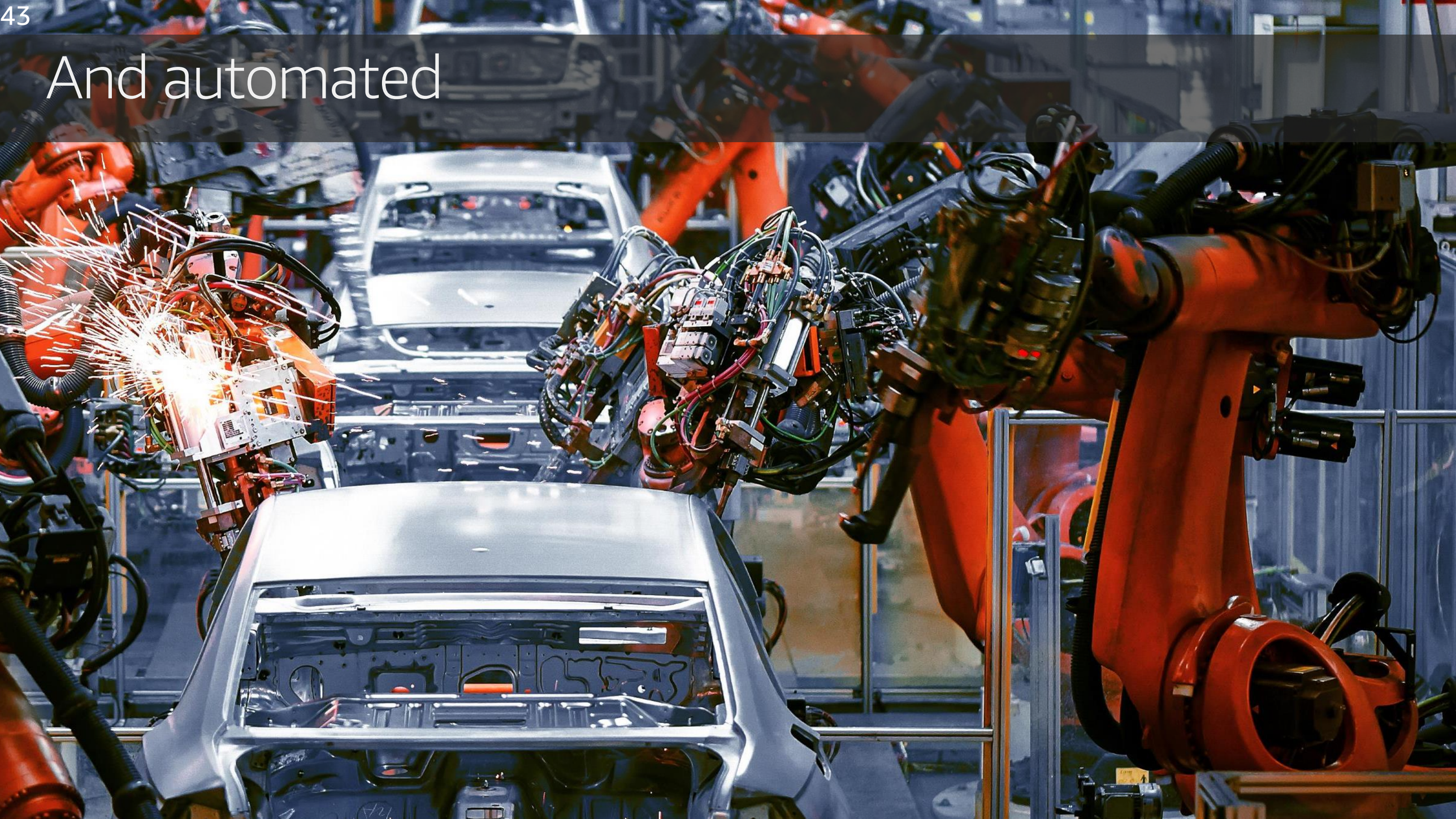
Monitoring operations across multiple accounts and regions



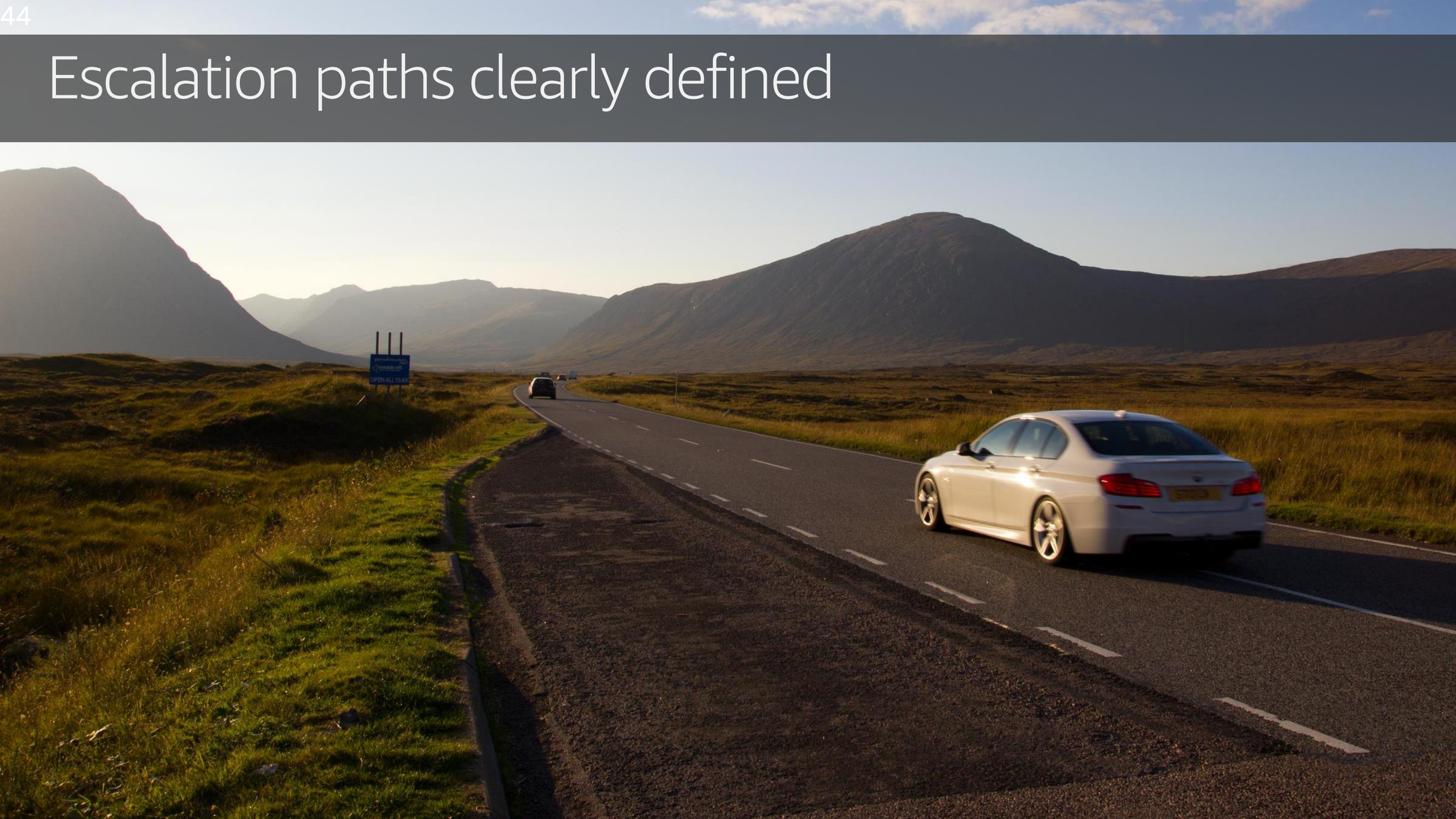
Resolution operations are codified



And automated



Escalation paths clearly defined



Simplified human intervention



Challenges and future work

- Adoption of SSM Documents as standard
- Parsing challenges
- Defining automations for new events
- Managing OpsCenter service limits
- Integration with GS incident management systems



Beneficial outcomes



Operational excellence for deployed AWS resources

Significant reduction in MTTR

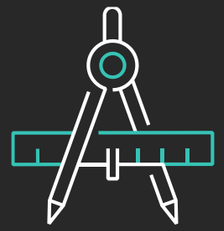
- Days to hours and hours to minutes

Deployments with greater confidence

Entire remediation and service recovery automation

Learn to architect with AWS Training and Certification

Resources created by the experts at AWS to propel your organization and career forward



Free foundational to advanced digital courses cover AWS services and teach architecting best practices



Classroom offerings, including Architecting on AWS, feature AWS expert instructors and hands-on labs



Validate expertise with the **AWS Certified Solutions Architect - Associate** or **AWS Certification Solutions Architect - Professional** exams

Visit aws.amazon.com/training/path-architecting/

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws training and certification

Thank you!

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws



Please complete the session survey in the mobile app.

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.