
aws
SUMMIT
INDIA | MAY 25, 2023

SECR001

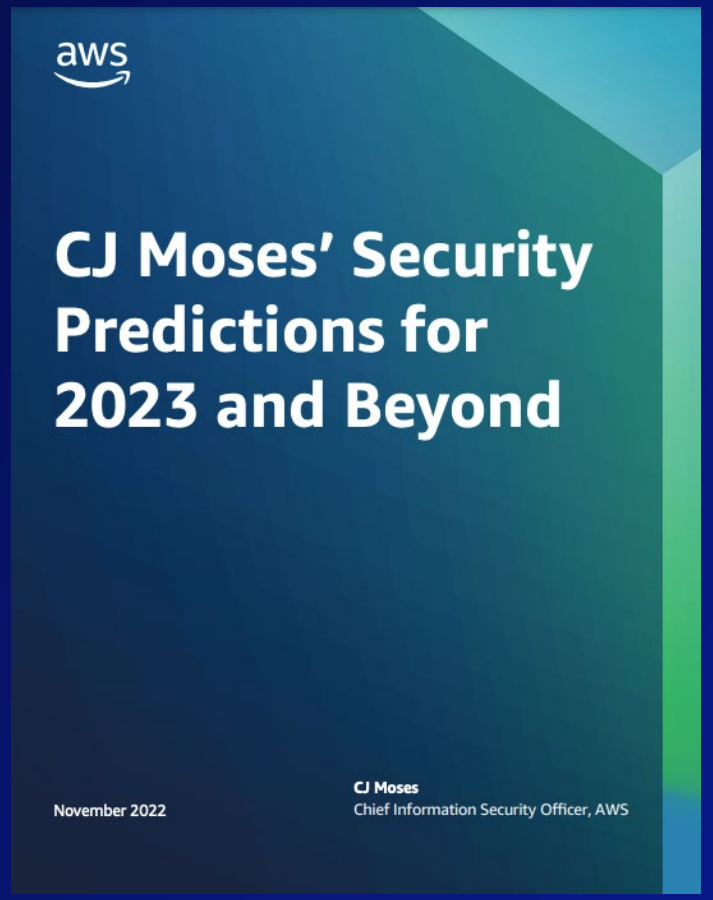
# Cloud is normal, Security is the key differentiator

Lalit Kumar
Principal Security Architect
AWS India

Atish Bhanushali
SVP IT
HDFC Bank

“Knowing what will change is intelligence,
Knowing what will not change is wisdom.”

# 2023 Security trends




1. *Security Will Be Integral to Everything Organizations Do*
2. *Diversity Will Help Address the Continued Security Talent Gap*
3. *Automation Driven by AI/ML Will Enable Stronger Security*
4. *People Will Drive Greater Data Protection Investment*
5. *More Advanced Forms of Multi-Factor Authentication Will Become Pervasive*
6. *Quantum Computing Will Benefit Security*

https://aws.amazon.com/executive-insights/content/6-security-predictions-for-ciso/

# Threat detection, monitoring, and response

## Security monitoring and threat detection

**Integrated with AWS workloads in an AWS account, along with identities and network activity**

**Amazon GuardDuty**

Detect threats and anomalous behavior

**Amazon Macie**

Discover sensitive data

**Access Analyzer**

Access & policy Validation

"We are just scratching the surface of AI/ML in cloud security. With the exponential growth of the cloud, security needs will grow equally quickly, fueling the need for automation and intelligence-driven security."

CJ Moses, Chief Information Security Officer, AWS

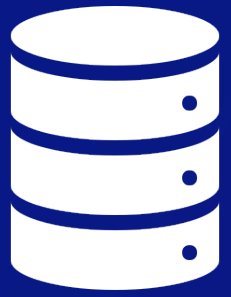
# Dive deep wisdom from another world

Solutions are seductive,
but they rarely *solve* anything
because chasing a “fix” removes our attention from the problem.

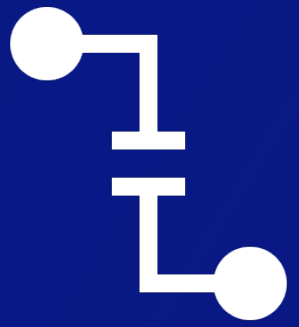
It is only when we understand the fundamental nature of the problem that it is eradicated.

If you understand the *why*,
the *how* takes care of itself.

The minimalist: https://www.theminimalists.com/solution/



# Growing volumes of security data



# Inconsistent and incomplete data

# Lack of direct ownership of your data

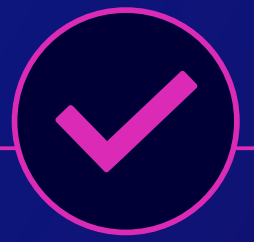
# More data wrangling, less analysis

# Imagine if there was a service that . . .

Automatically builds a security lake in your account

Centralizes and normalizes log collection across your entire enterprise

Provides long-term retention and manages storage cost



Gives complete freedom of choice for analytics

# Open Cybersecurity Schema Framework (OCSF)

AN OPEN STANDARD THAT CAN BE ADOPTED BY ANYONE TO SIMPLIFY SECURITY DATA NORMALIZATION

Open-source project to deliver a simplified and vendor-agnostic taxonomy for security data

Speed data ingestion and analysis without the time-consuming, up-front normalization tasks

Combine data from OCSF compliant sources to break down data silos that slow security teams

Open standard that can be adopted in any environment, application, or solution provider

Over 60 participating organizations across security ISVs, government, education, and enterprise, with many more using OCSF

Preview

# Amazon Security Lake

AUTOMATICALLY CENTRALIZE SECURITY DATA INTO A PURPOSE-BUILT DATA LAKE IN A FEW CLICKS

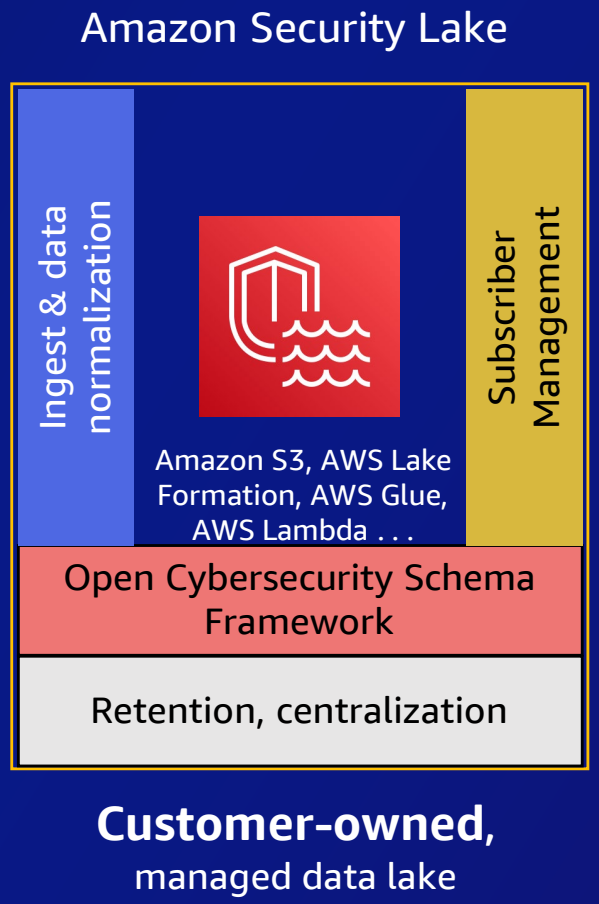
**Centralize** data automatically from cloud, on premises, and custom security sources across regions

**Optimize** and manage security data for more efficient storage and query performance

**Normalize** data to an open standard to easily share and use with multiple analytics tools

**Analyze** using your preferred analytics tools while retaining control and ownership of your security data

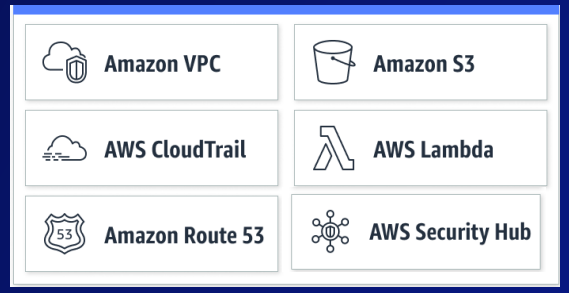
# How it works




**Customer-owned**, managed data lake

# How it works

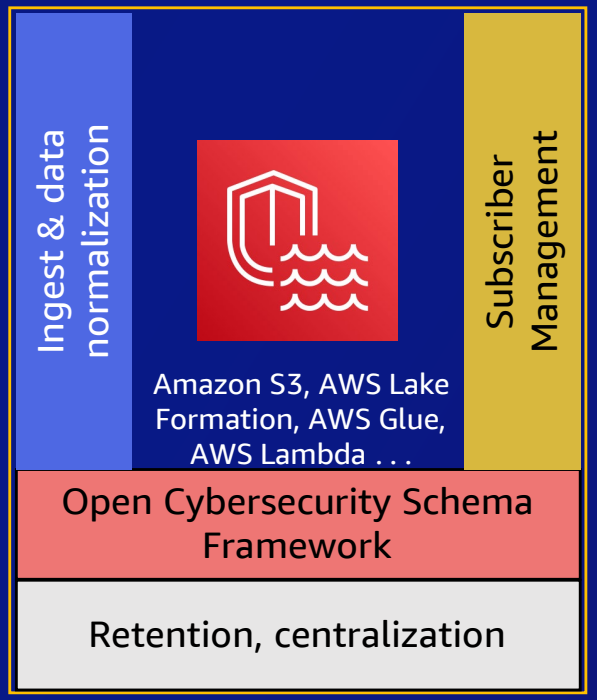
AWS logs sources + findings from over 50 security solutions




AWS Partner enterprise security solutions

Your own data

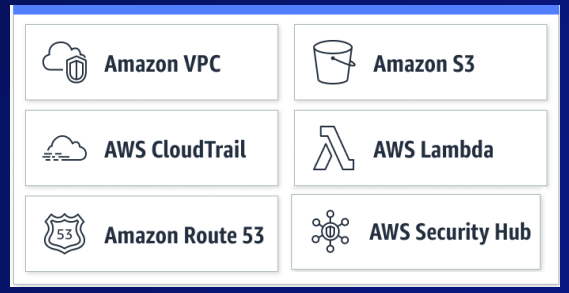
Amazon Security Lake




**Customer-owned**, managed data lake

# How it works

AWS logs sources + findings from over 50 security solutions




AWS Partner enterprise security solutions

Your own data

Amazon Security Lake

Ingest & data normalization

Amazon S3, AWS Lake Formation, AWS Glue, AWS Lambda . . .

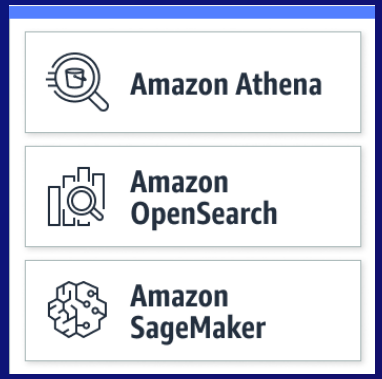
Subscriber Management

Open Cybersecurity Schema Framework

Retention, centralization

**Customer-owned**, managed data lake

AWS Analytics




AWS Partner analytics & XDR platforms

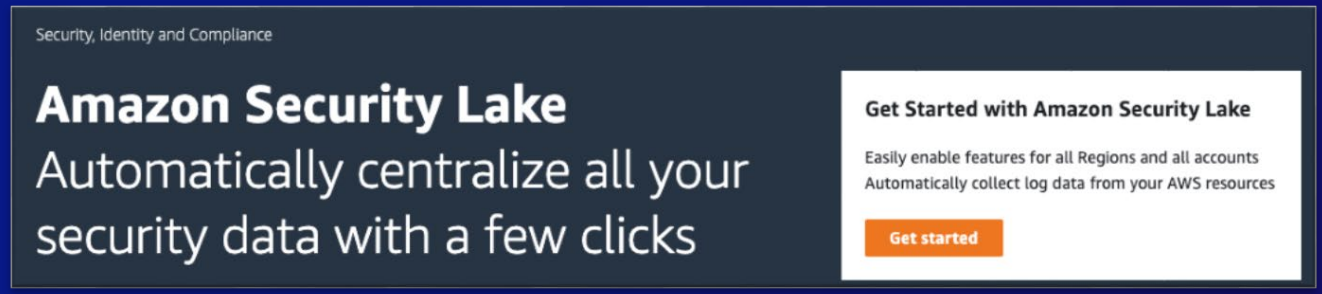
# Amazon Security Lake Partners

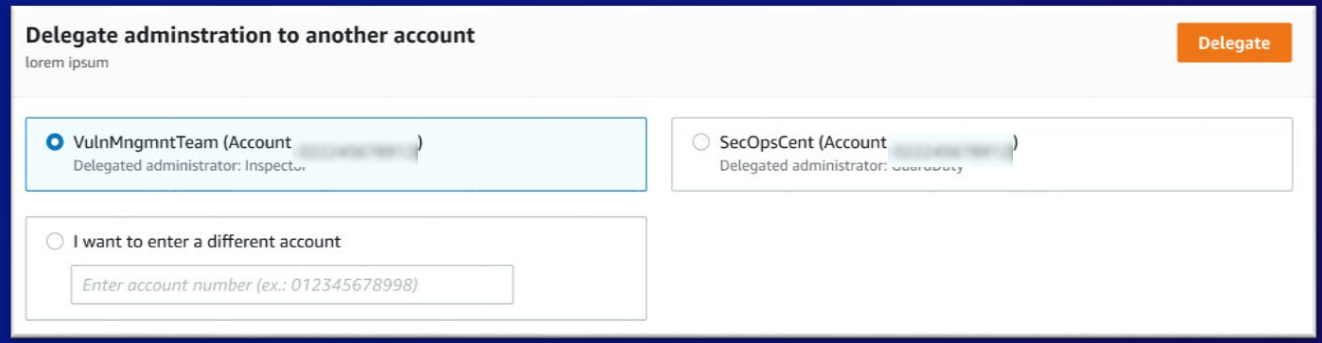
# Getting started – Enterprise-wide enablement

## Security Lake works with AWS Organizations

Start from your organization management account

Elect a delegated admin account to manage your security data



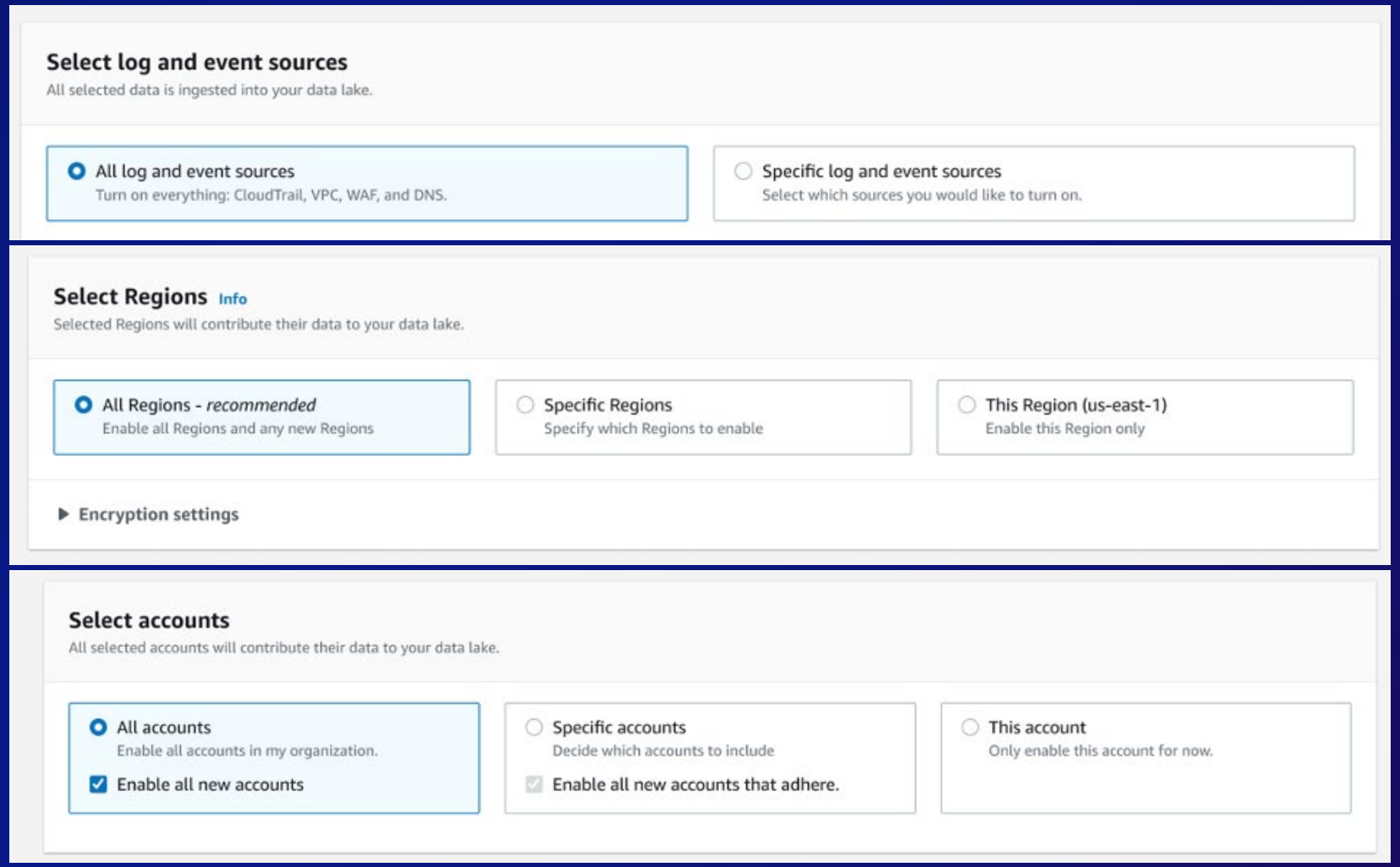



# Getting started – Collect everything

Everything on by default

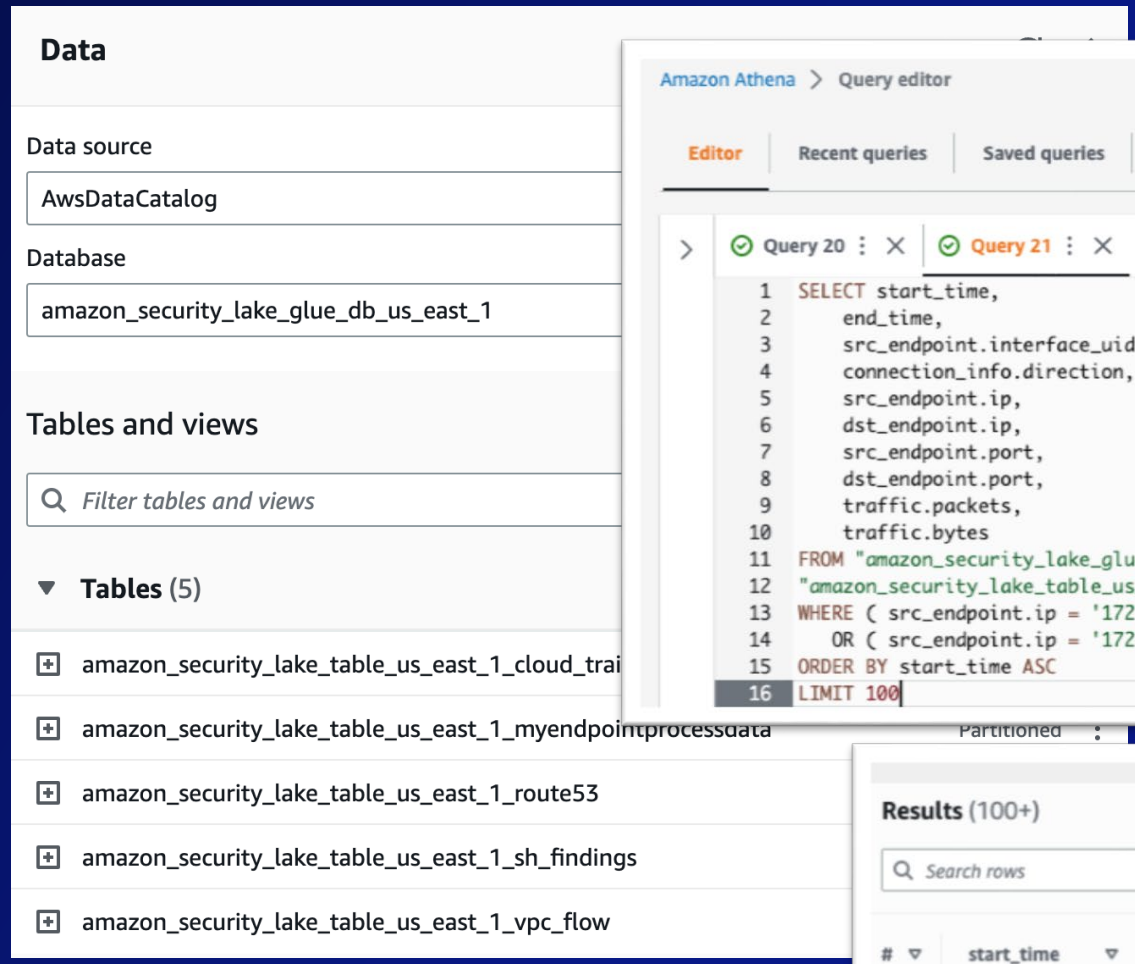
Multi-Region enablement

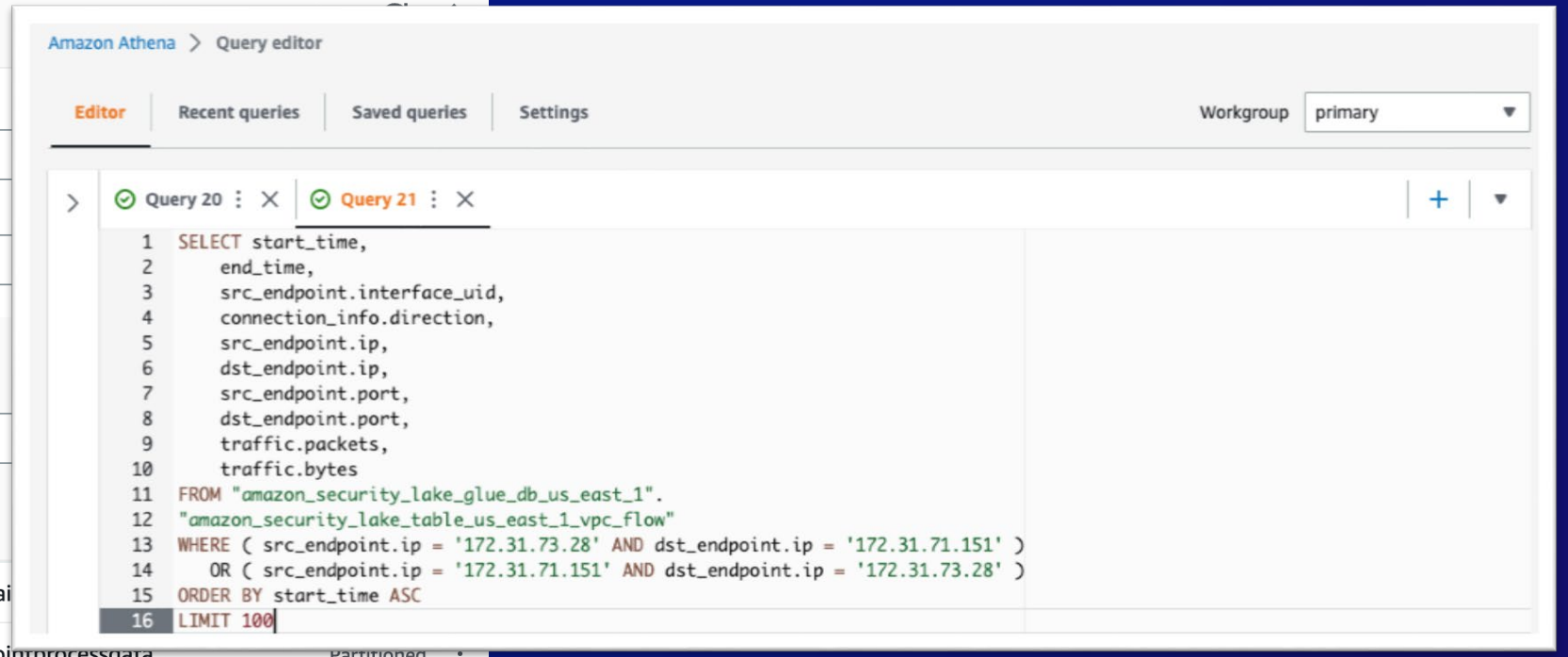
All accounts in your organization

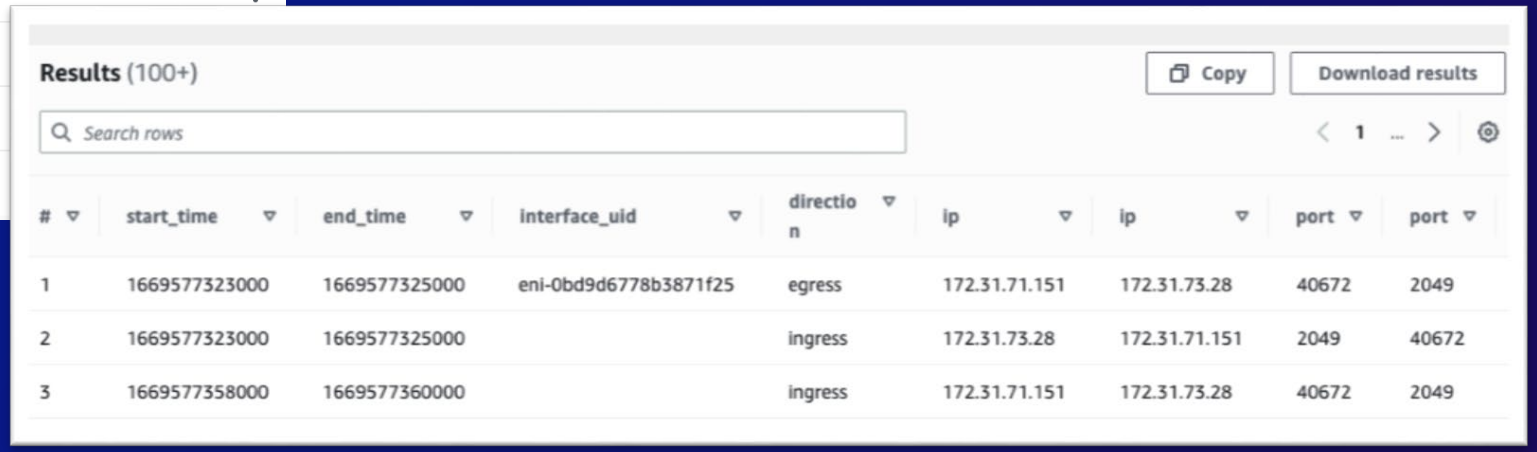


# You can immediately query your data

Amazon Athena




| # | start_time | end_time | interface_uid | direction | ip | ip | port | port |
|---|---|---|---|---|---|---|---|---|
| 1 | 1669577323000 | 1669577325000 | eni-0bd9d6778b3871f25 | egress | 172.31.71.151 | 172.31.73.28 | 40672 | 2049 |
| 2 | 1669577323000 | 1669577325000 | | ingress | 172.31.73.28 | 172.31.71.151 | 2049 | 40672 |
| 3 | 1669577358000 | 1669577360000 | | ingress | 172.31.71.151 | 172.31.73.28 | 40672 | 2049 |

# What's happening under the hood?

Create encrypted Amazon S3 buckets across regions and configure Amazon S3 retention and replication settings

Enable logging across all Regions, accounts, and resources

Transform and partition all incoming data to OCSF and Apache Parquet

Create and update AWS Glue Tables and partitions

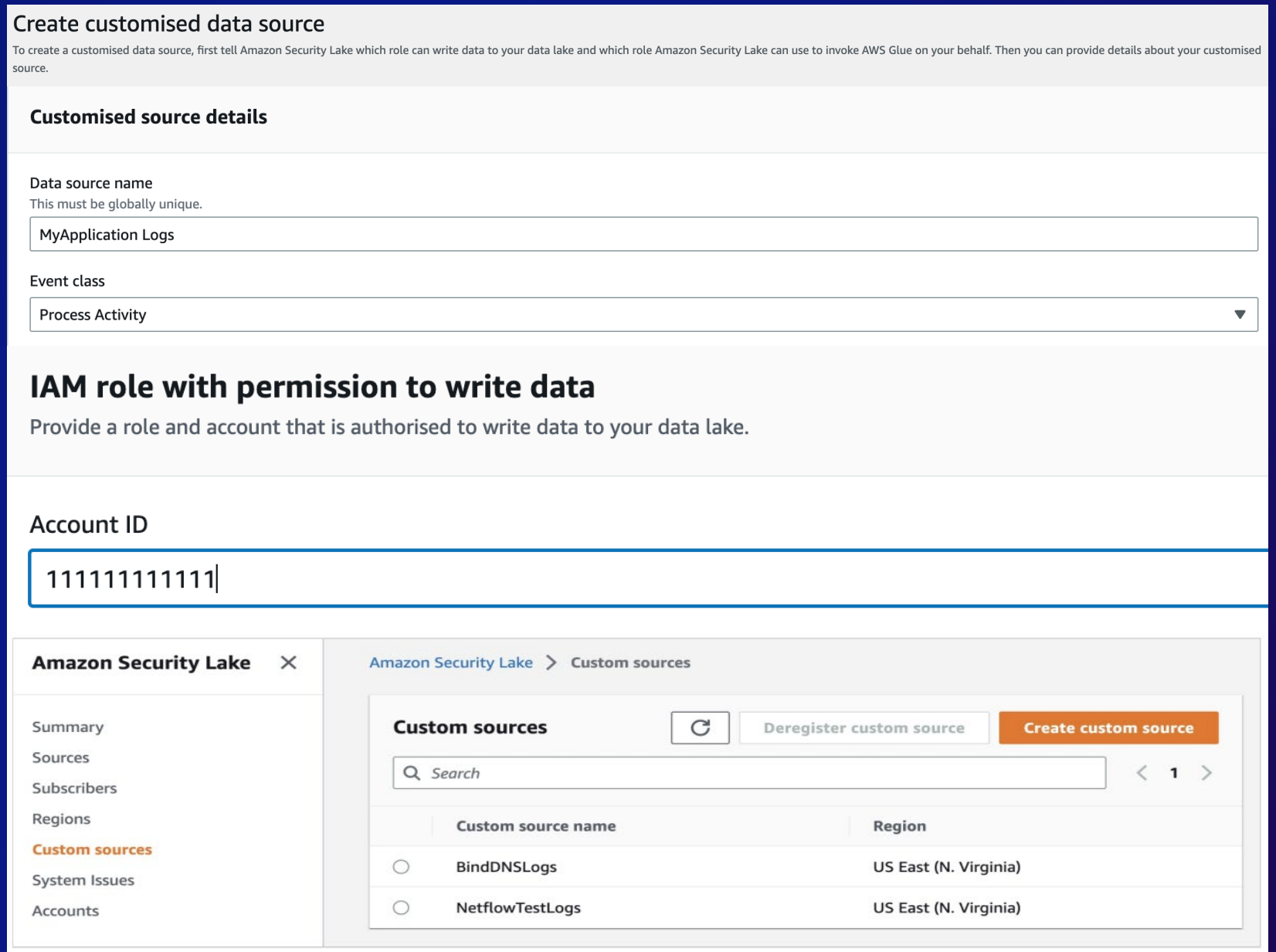
# Bring all your security data

- You can augment your data lake with external OCSF data from partner solutions or your own
- Use the same data lifecycle and access control features as native data
- 20+ partners already provide their data in this format directly to Amazon S3
- Security Lake manages the infrastructure and permissions for you

# Bring all your security data

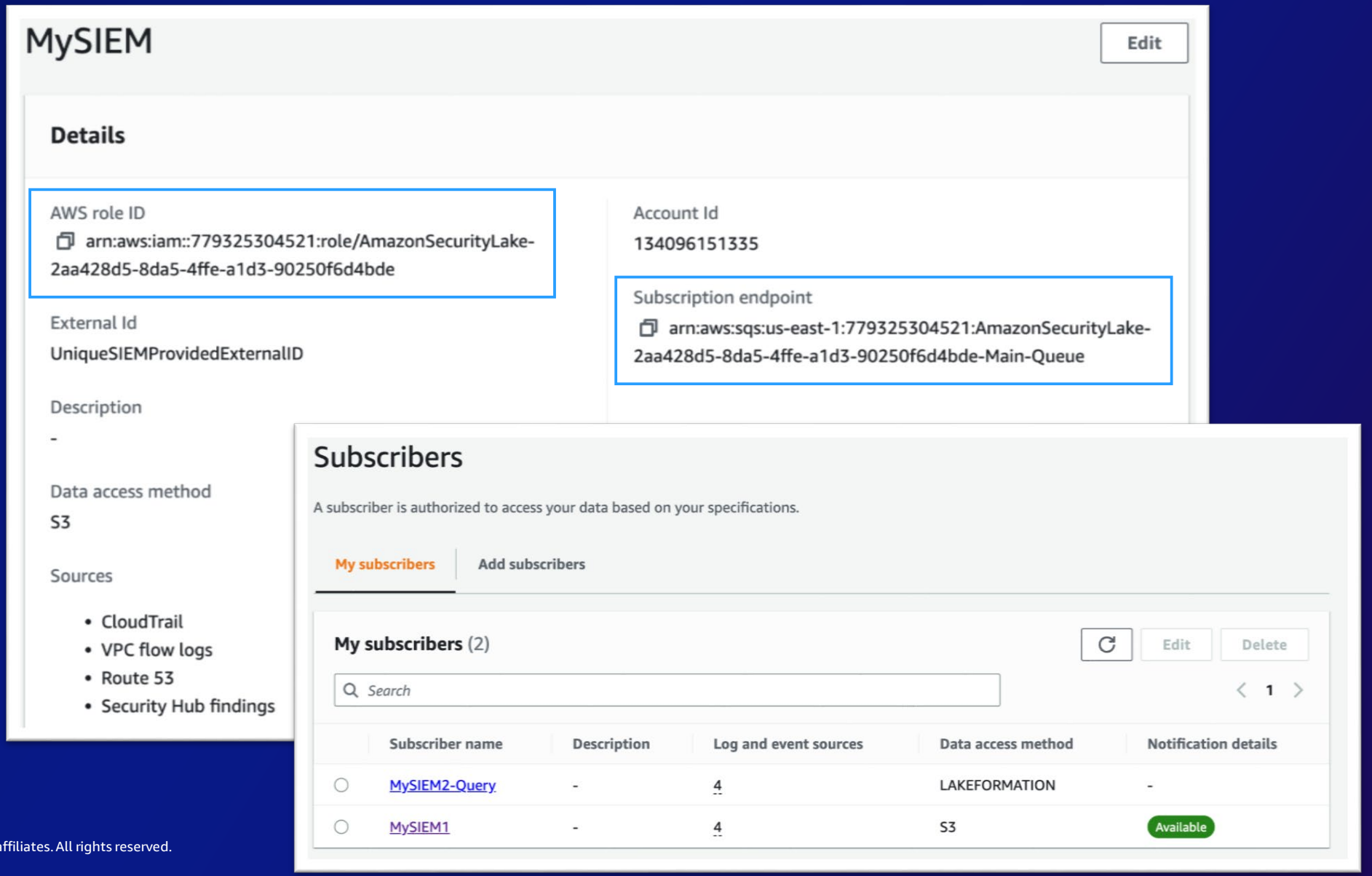
Provide AWS account ID of the source provider

Define name and OCSF event class

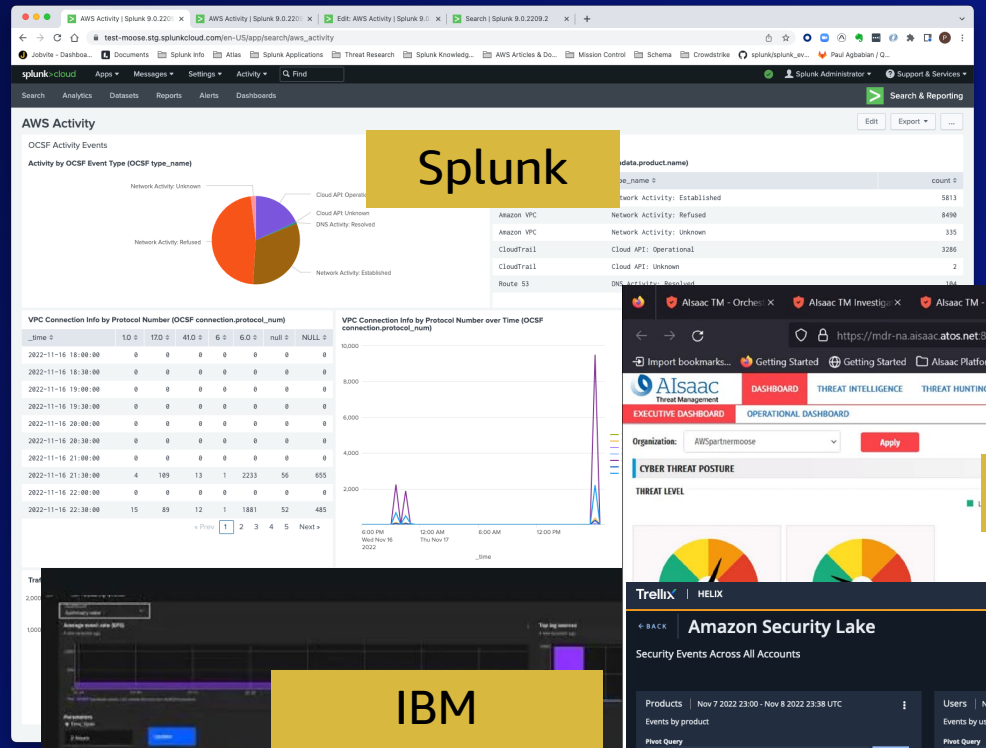


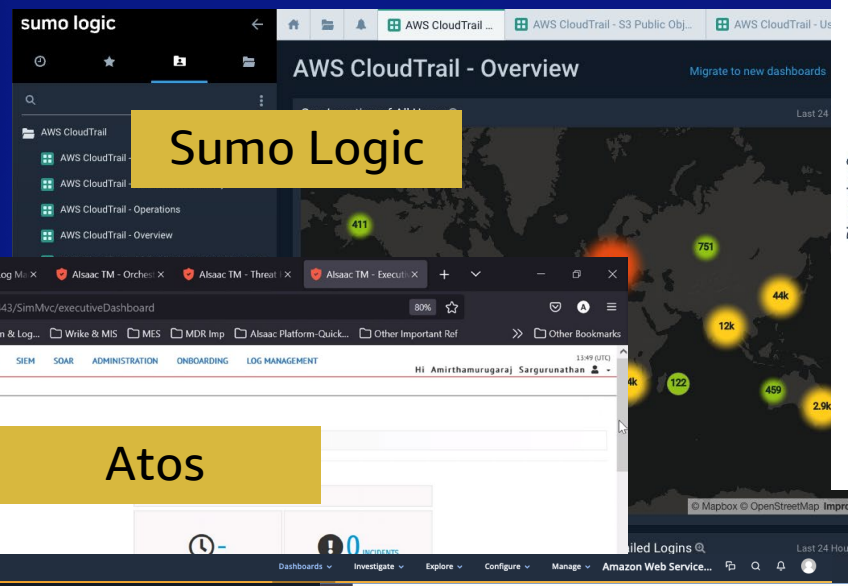
# Configure subscribers

Use Security Lake created resources to configure data access on the subscriber



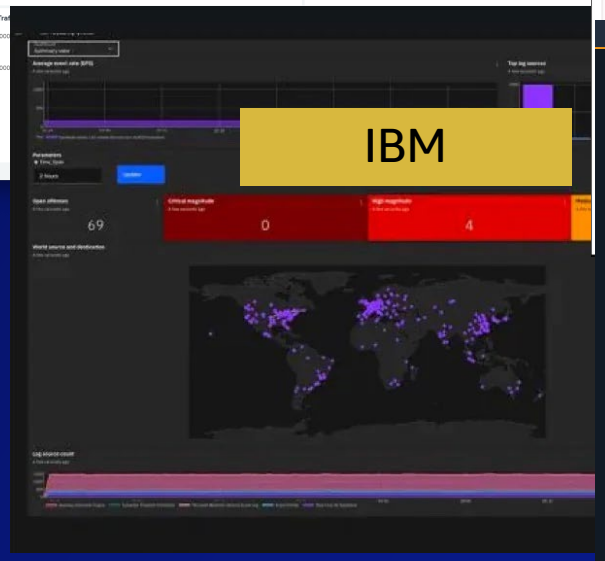
# Choose your analytics

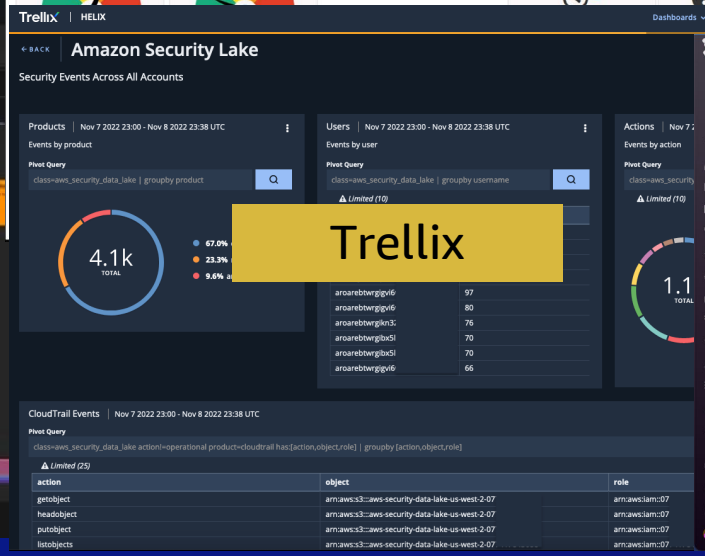


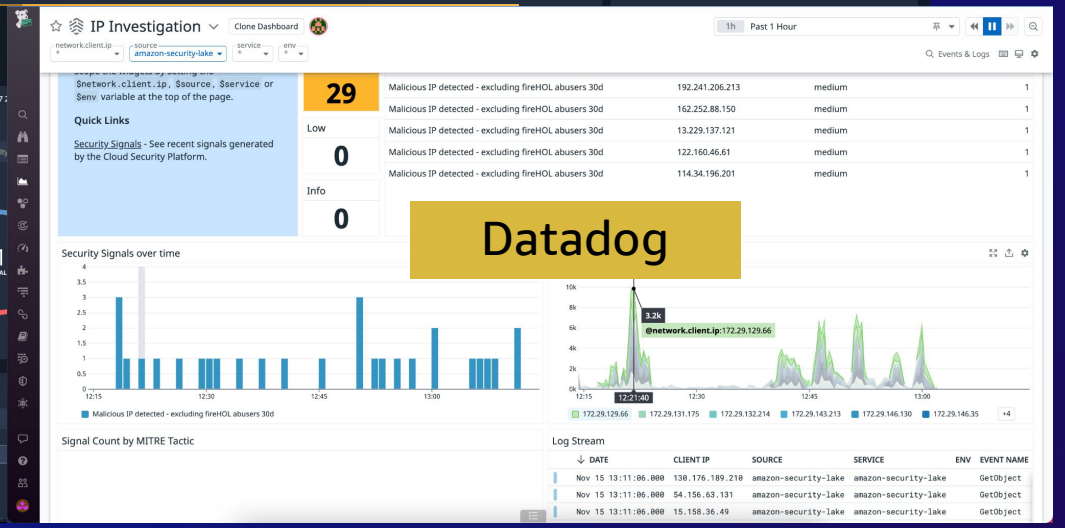







# Introduction

Head – Cloud Infrastructure

- BFSI sector has seen a rise in online banking activities, pushing digital transformation where cloud computing has played a vital role
- Cloud provides transformative opportunities for organisations and is a vital competitive component in today's challenging marketplace for the BFSI industry
- With the cloud adoption, cloud security and compliance need to be implemented with different methodology

# Security charter of the cloud adoption office

security and compliance must cover the following areas to meet business objectives:

## Architecture Alignment

Business alignment

Security Principles

Secure Ref Architectures

Engineering support

## Product Management

Security is increasingly consumed through APIs

Security is increasingly automated

Security Engineering

Vendor Management

## Delivery Management

Increase compliance before and after deployment

Security integration into DevOps

Reduce friction, increase velocity

## Financial Management

Improve security operational excellence

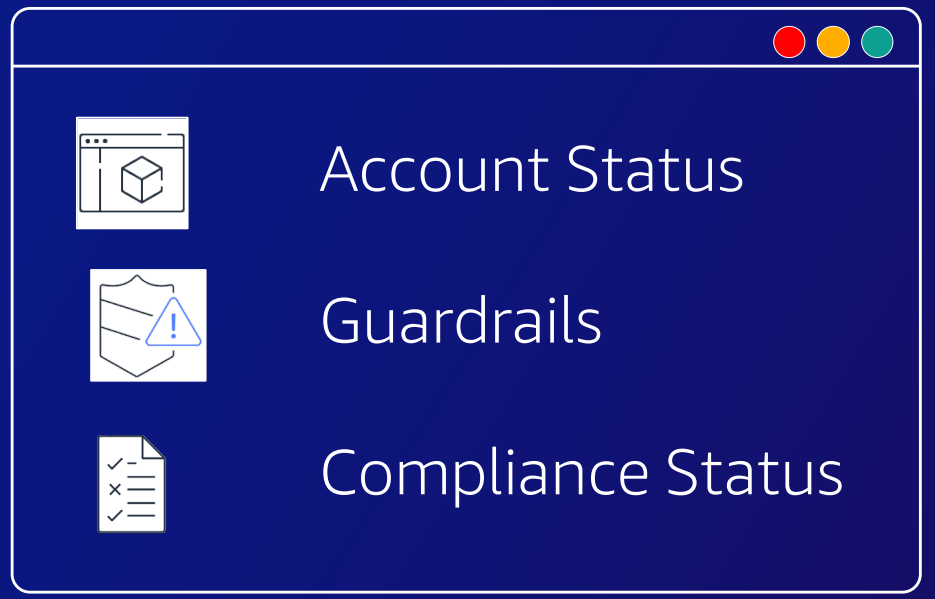
Cloud Security Budget

Metrics

# Governance with landing zones

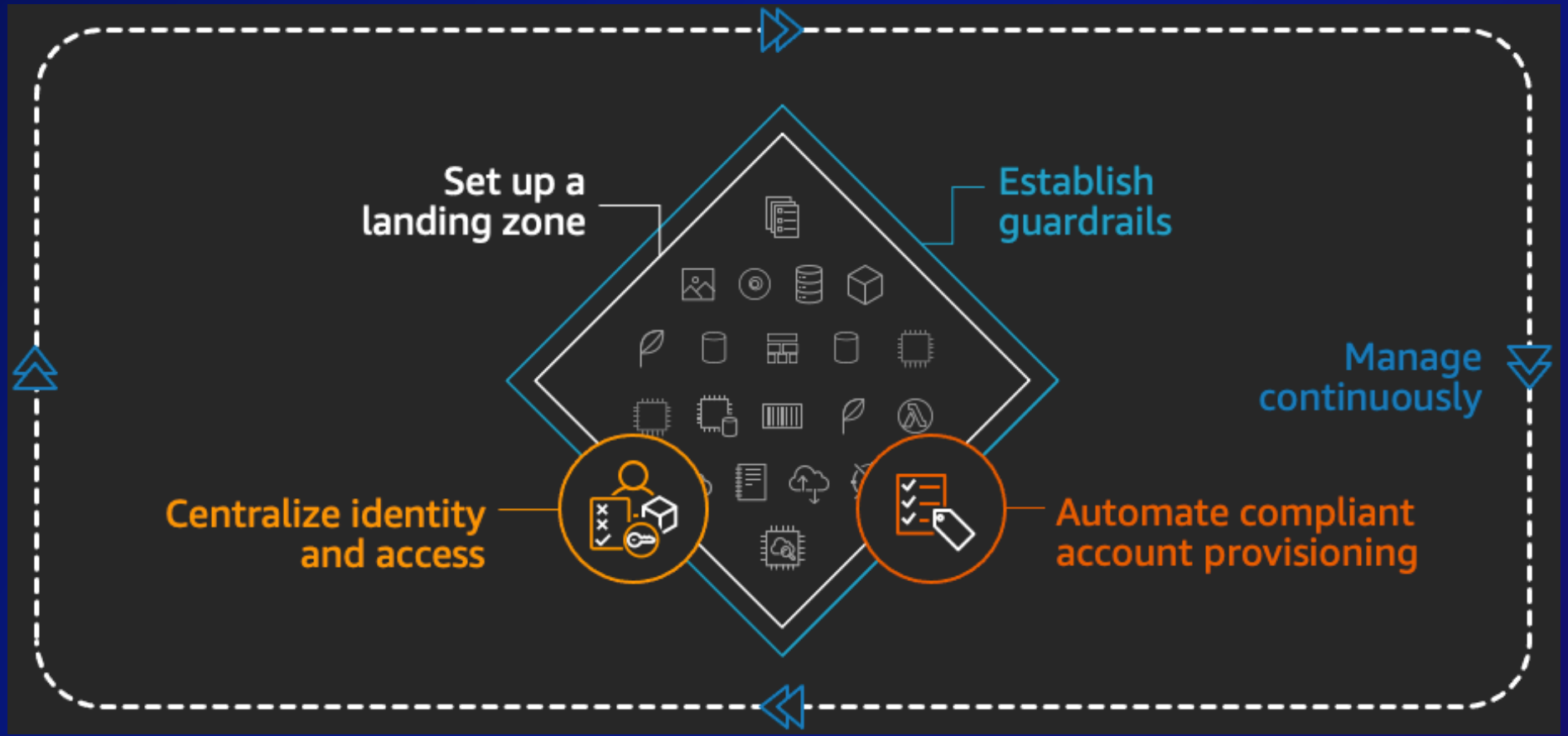
Landing Zones include:

- AWS Account Structure – Define your security reference architecture
- **Centrally managed guardrails – build your own guardrails**
- Centralized federated identity management – SSO
- **Centralized logging and monitoring**
- Centralized compliance management & Security Baseline



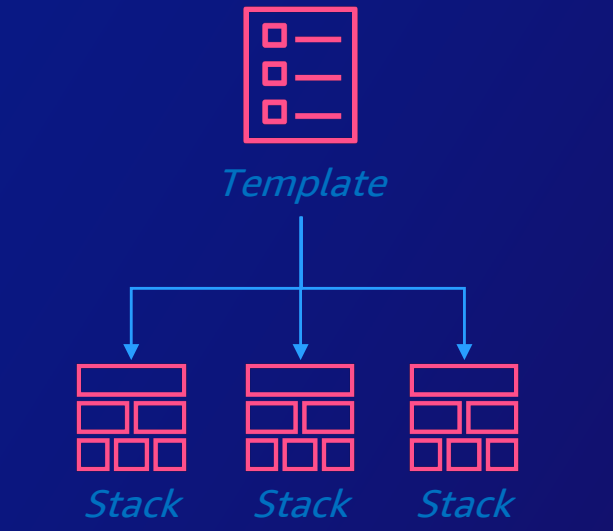

AWS Control Tower sets the baseline – Operate & evolve

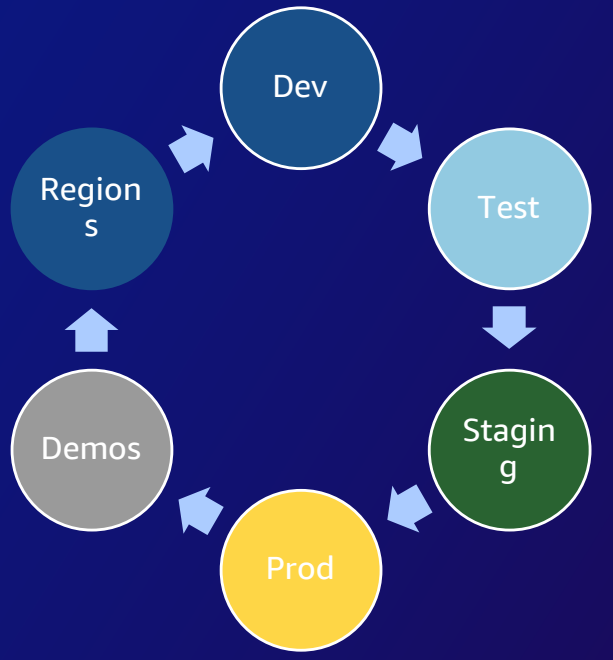
# Define your operating model



# Pattern: Evolution of Infrastructure as Code (IaC)

- Single source of truth to deploy the whole stack
- Infrastructure that you can replicate, re-deploy, and re-purpose
- Control versioning on your infrastructure and your application together
- Service rolls back to the last good state on failures
- Build your infrastructure and run it through your CI/CD pipeline with IAC security integrated

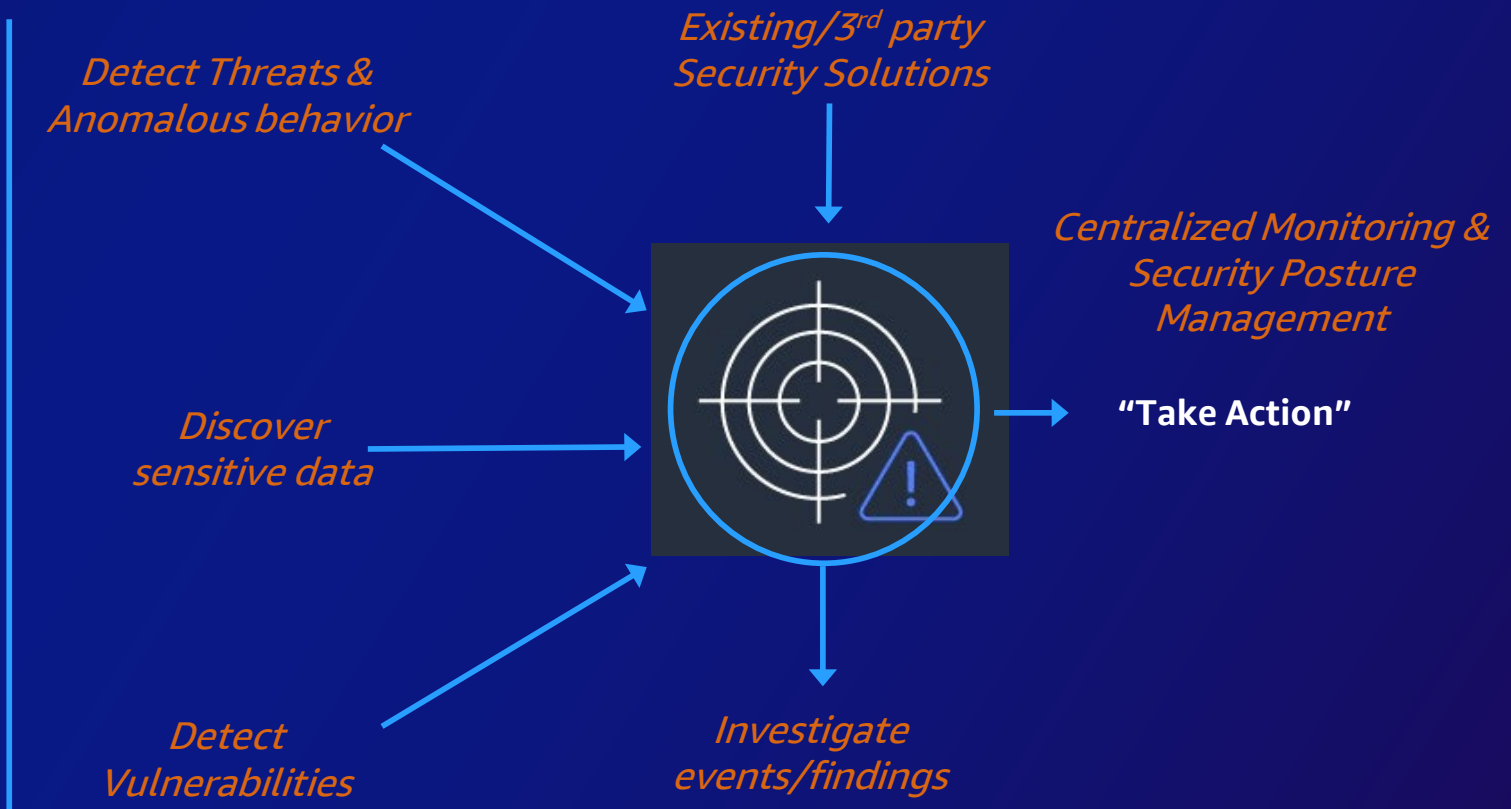


# CSPM - Threat detection, monitoring, compliance and response

No Cloud Security without CSPM

Integrate CSPM with SIEM



# SOC Operating model

# Control validation audit - CloudTrail

TRACK USER AND RESOURCE ACTIVITY FOR GOVERNANCE AND AUDITING.

## Capture

Record activity as CloudTrail events

## Store

Retain events logs in secure S3 bucket

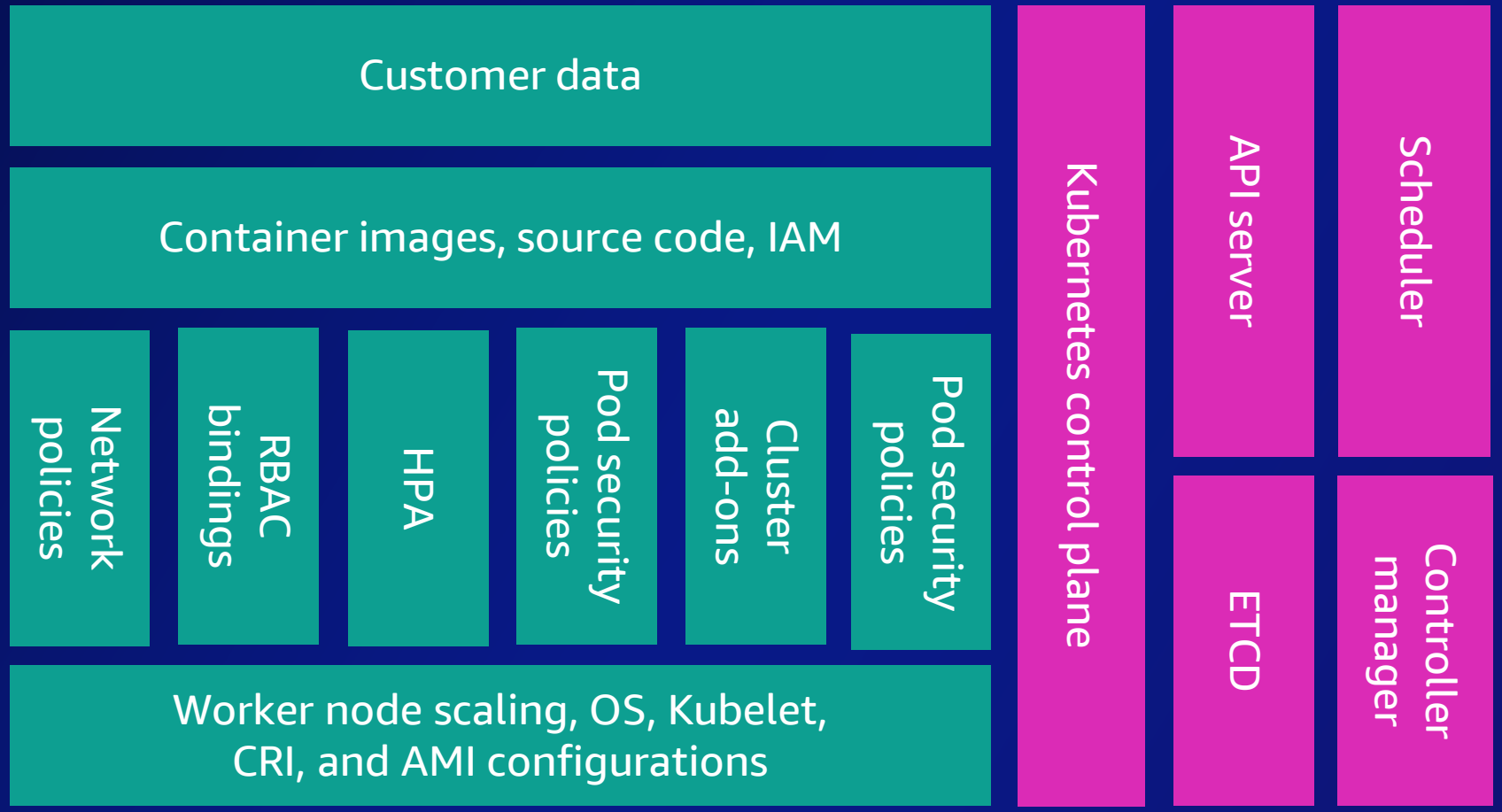
## Act

Trigger actions when important events are detected

## Review

Analyze findings or recent and historical activity

# Pattern: Container security




- Encryption
- Trusted images
- Runtime Defense
- Runtime drift protection
- Container Registry scan
- Container access control
- Vulnerability Management
- Malware protection

# Cloud security is different

PREPARE YOUR SECURITY FOR AN AGILE WORLD

1. Infrastructures are immutable. CI/CD pipelines are always used.
2. Avoid everything long lived (keys, instances). Auto-refresh using DevOps automation.
3. Micro-Segmentation and zero trust is the norm. Authentication uses roles, not static keys.
4. Security automation with serverless functions (contain, enrich, remediate, redeploy)
5. Log and monitor everything.
6. If you can only invest in one initiative then Identity & Access Management is your north star.

**If you are looking for one key success in Cloud Security focus on - IAM, IAM and IAM!**

skillbuilder.aws

# Your time is now

Build in-demand cloud skills your way

# Thank you!

Please complete the session survey


Lalit Kumar
Principal Security Architect
AWS India

Atish Bhanushali
SVP IT
HDFC Bank