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

ARC309

A real-world resilience evolution in the cloud framework

Anderson Mota
Head of Technology Architecture
Banco Itaú

Robert Fuente
Principal Technical Account Manager
AWS

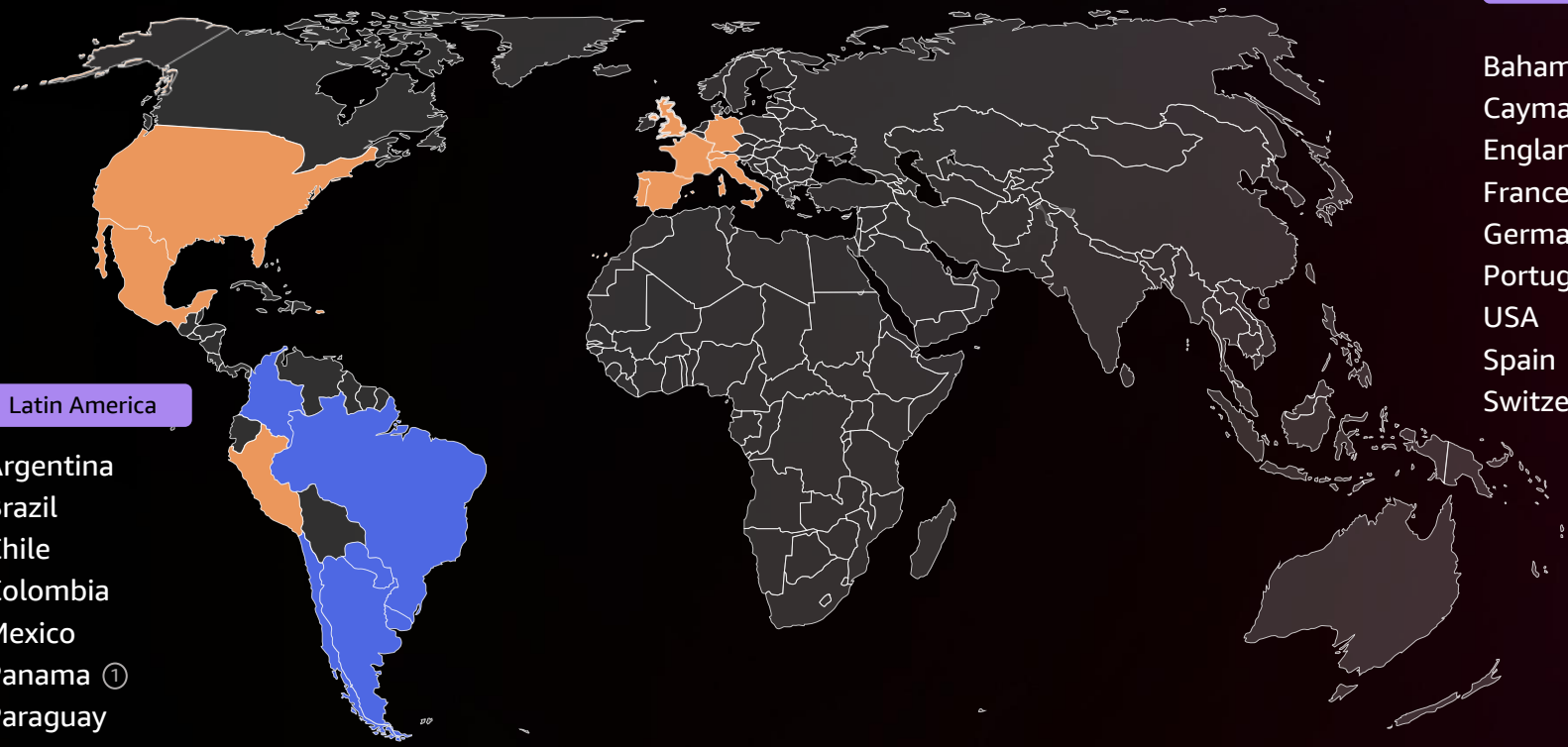
Gus Santana
Cloud Acceleration Team Director
AWS

Agenda

- Banco Itaú's cloud journey
- Resilience evolution program
- Chaos engineering and testing
- Critical dependencies and deployment strategy review
- Internet account rearchitecture and service quota table
- Operations and observability changes

Itaú Unibanco

A universal bank | 98 years of history | Latin America's largest financial institution



Latin America

Argentina
Brazil
Chile
Colombia
Mexico
Panama ①
Paraguay
Peru
Uruguay ①

Rest of the world

Bahamas ①③
Cayman Is. ①②③
England ①②
France ①
Germany ①
Portugal ①
USA ①②③
Spain ①
Switzerland ③

Key

Multiple banks
Other operations

① Corporate & investment banking ② Asset management ③ Private banking

Brazil's most valuable brand
7+ billion USD

65M+ customers

20M+ digital customers

~100K employees

4K business services

Largest bank in market value; (2) 2022 Brand Finance Brazil Ranking; (3) In Q2 FY22
https://bit.ly/3GrVarg
Dollar exchange rate (Nov. 25, 2021)

Our ability to innovate and adapt has allowed us to get here

Over the years, customer expectations and habits have changed

They value experiences rather than just products and services

But what does it mean to be

digital in essence?

Being digital goes beyond operating on digital channels; it is a **cultural change** that requires differentials in the way of operating and thinking about new solutions

- Technology is at the **core of the business** and in all its products and services
- Products **are loved by customers**, make sense, and have value for them and the business
- Multidisciplinary teams share goals and accelerate decisions
- Industry boundaries are more blurred, new revenue streams are explored

As part of this strategy

Our modernization strategy has a **structured roadmap**

What value modernization brings

Platform **designed to evolve** and be easily adaptable, following market parameters

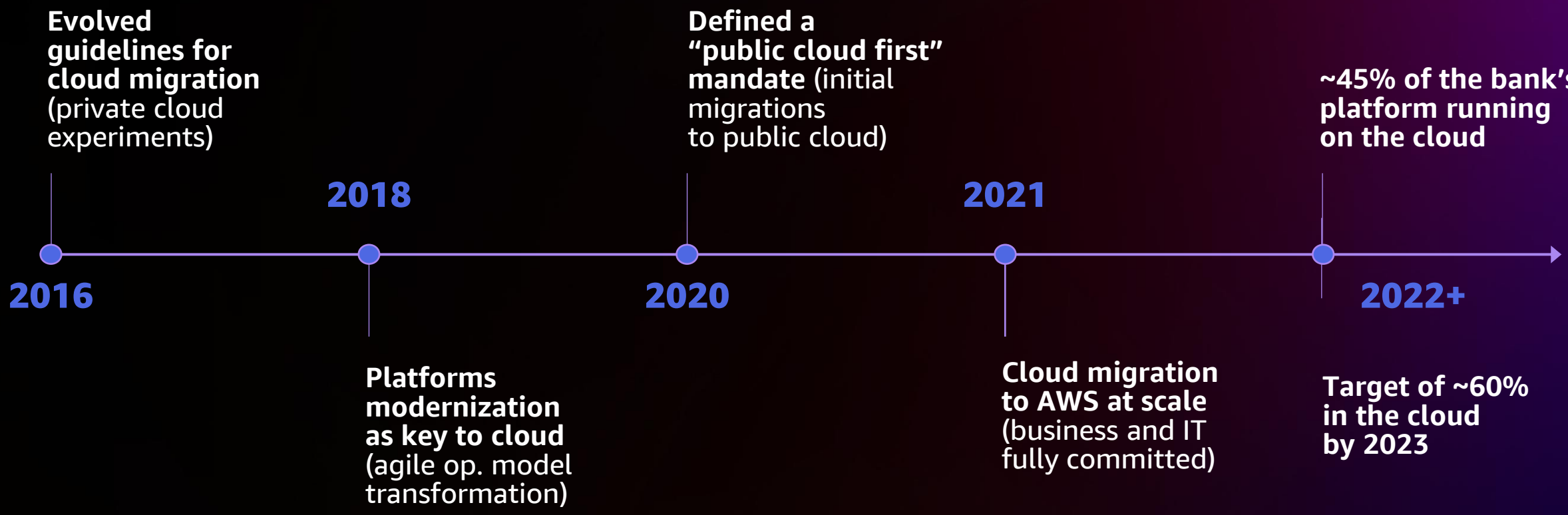
Decreased dependencies and adoption of a **decoupled cellular architecture**, based on microservices

More agility and autonomy for teams to innovate through the use of reusable solutions

Increased delivery frequency, **with shorter cycles**, improving time to market

Analytics by design and observability: use of tools that help to better monitor the customer experience and evolve the platform

Although we started working with AWS in 2021, Itaú's public cloud journey started a couple of years earlier



Source: McKinsey & Company

Why a resilience evolution program?

Even with the process of modernizing our applications to AWS, we understood that our expected **level of resilience** had not yet been reached

We needed to have **more visibility** into the health of the services used in our applications and **map the dependencies** of the services, ensuring that the framework could be used on a **large scale**

Itaú's critical workloads on AWS

pix powered by Banco Central

- Brazilian Central Bank's instantenous system
- Itaú takes care of 25M transactions/day
- 30% of country's volume

Digital Channels

- Itaú's "storefront"
- Mobile and Internet
- 7.2M customers/day
- Peak of 2.5M concurrent customers

Credit Card Operations

- Credit card operations
- 51M transactions/day

kafka

- Distributed data store optimized for ingesting and processing streaming data in real time
- EC2 instances
- 5.9B messages/day

Itaú-AWS Resilience Evolution Program Pillars

Monitoring

1 Evolve applications' observability
Create dashboards that matter

Tests

2 Create a framework for Chaos Engineering

Dependencies

3 Map the dependencies
Reduce blast radius

Enhancements

4 Increase resilience and reliability of applications

Governance

5 Revise governance and suggest improvements based on needs

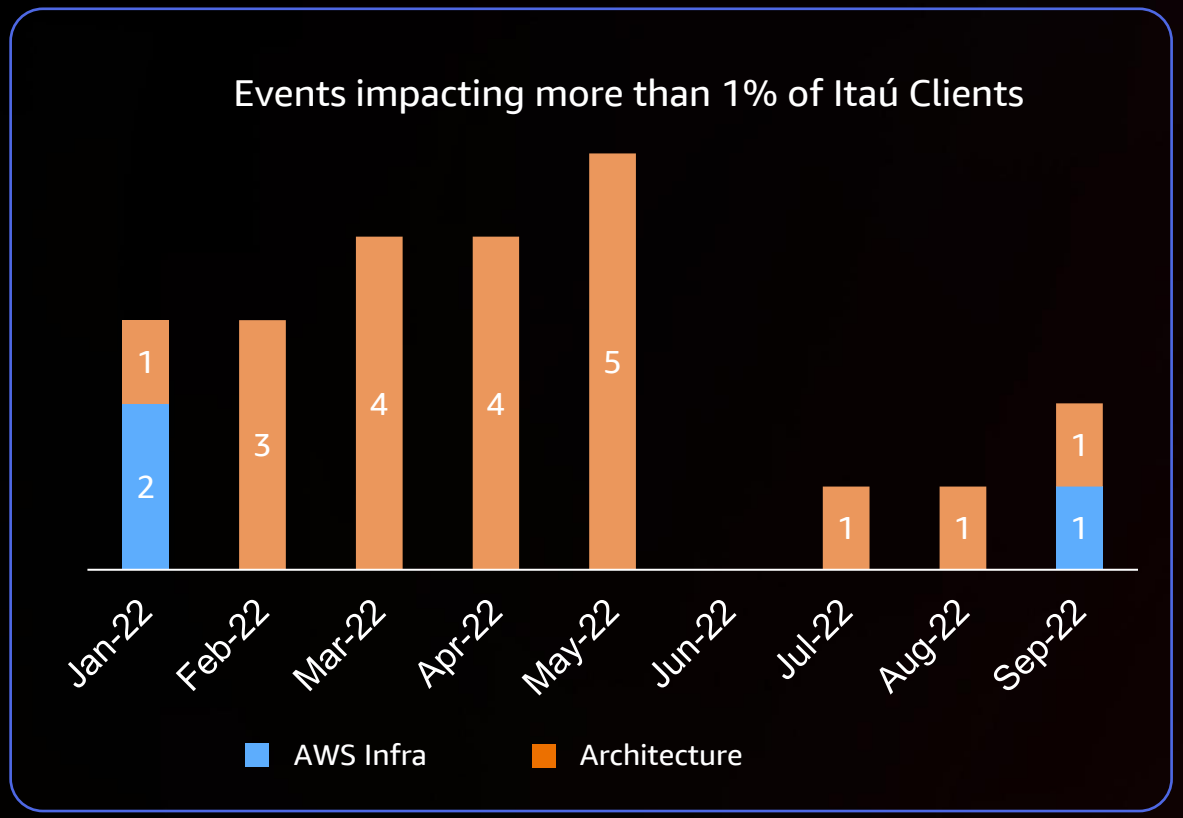
Mechanisms

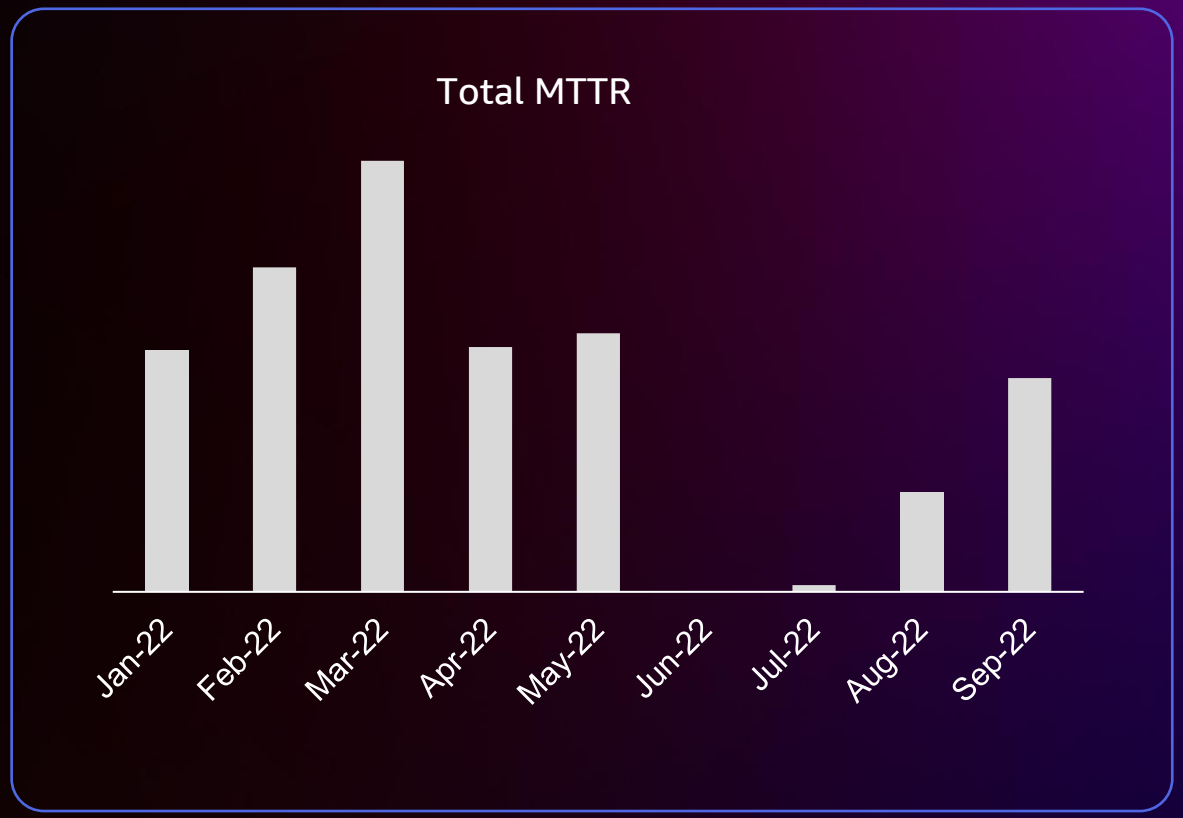
6 Based on the lessons learned from the 5 pillars, a mechanism was built to scale these improvements to all new critical applications.

Program metrics

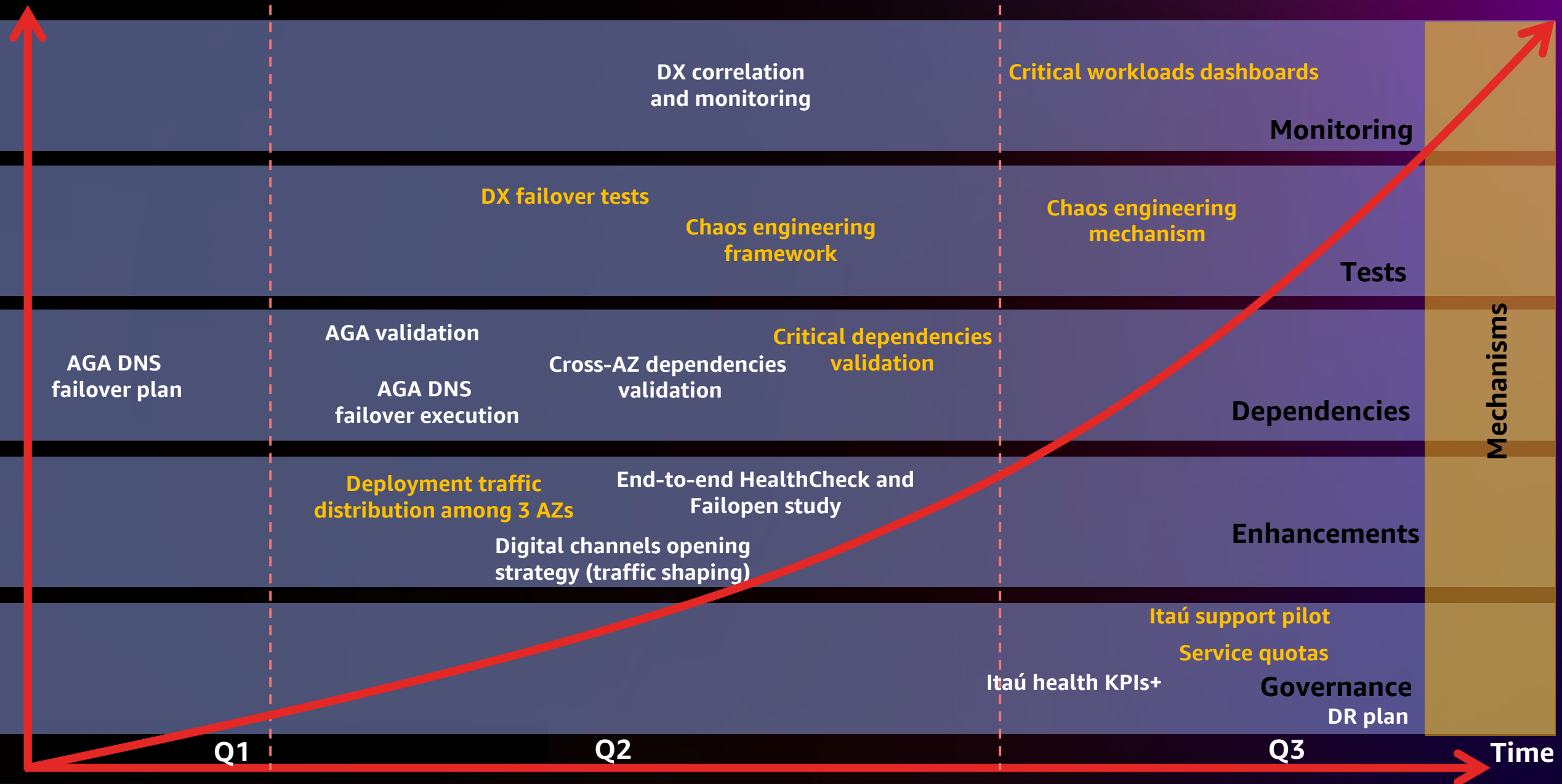
Observations

- Total MTTR (hours)
- Reduction of 75% of events and MTTR

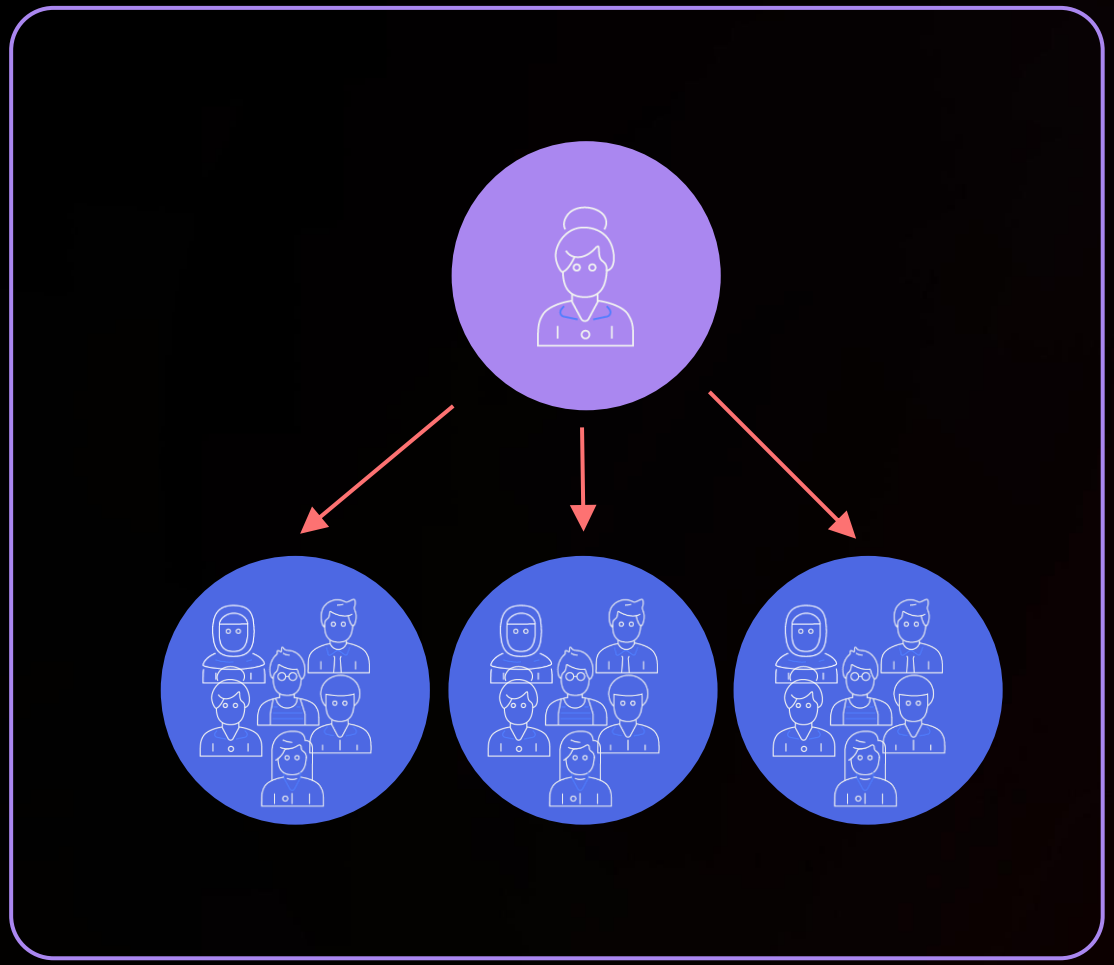




Itaú-AWS resilience evolution program at a glance



Single-threaded leader (Amazon's definition)



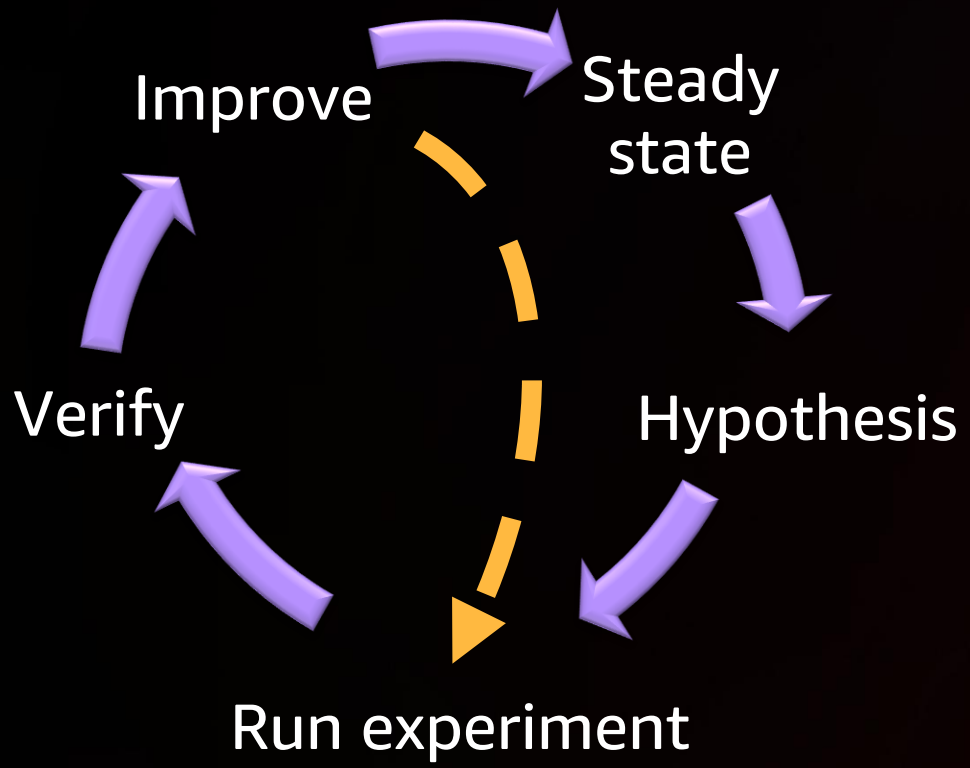
- Person who is responsible for the **goals** of the team ("wakes up every day thinking about them")
- This person understands **status**, **dates**, and **blockers**
- Leaders of **two-pizza teams** (2PTs) and also for programs (which generally involve multiple teams)

Resilience evolution STLs responsibilities

1. Be the primary resources capable of **escalating quickly** within AWS and Itaú
2. Recognize **areas of engagement** between Itaú and AWS and find areas that require deep technical experts to collaborate
3. Review and guide **failover testing**, run test regularly, and capture learnings from these tests
4. Operate in two continuous modes: **avoiding incidents** and **treating incidents**
5. Conduct **periodic reviews with executive leadership to discuss improvement opportunities**

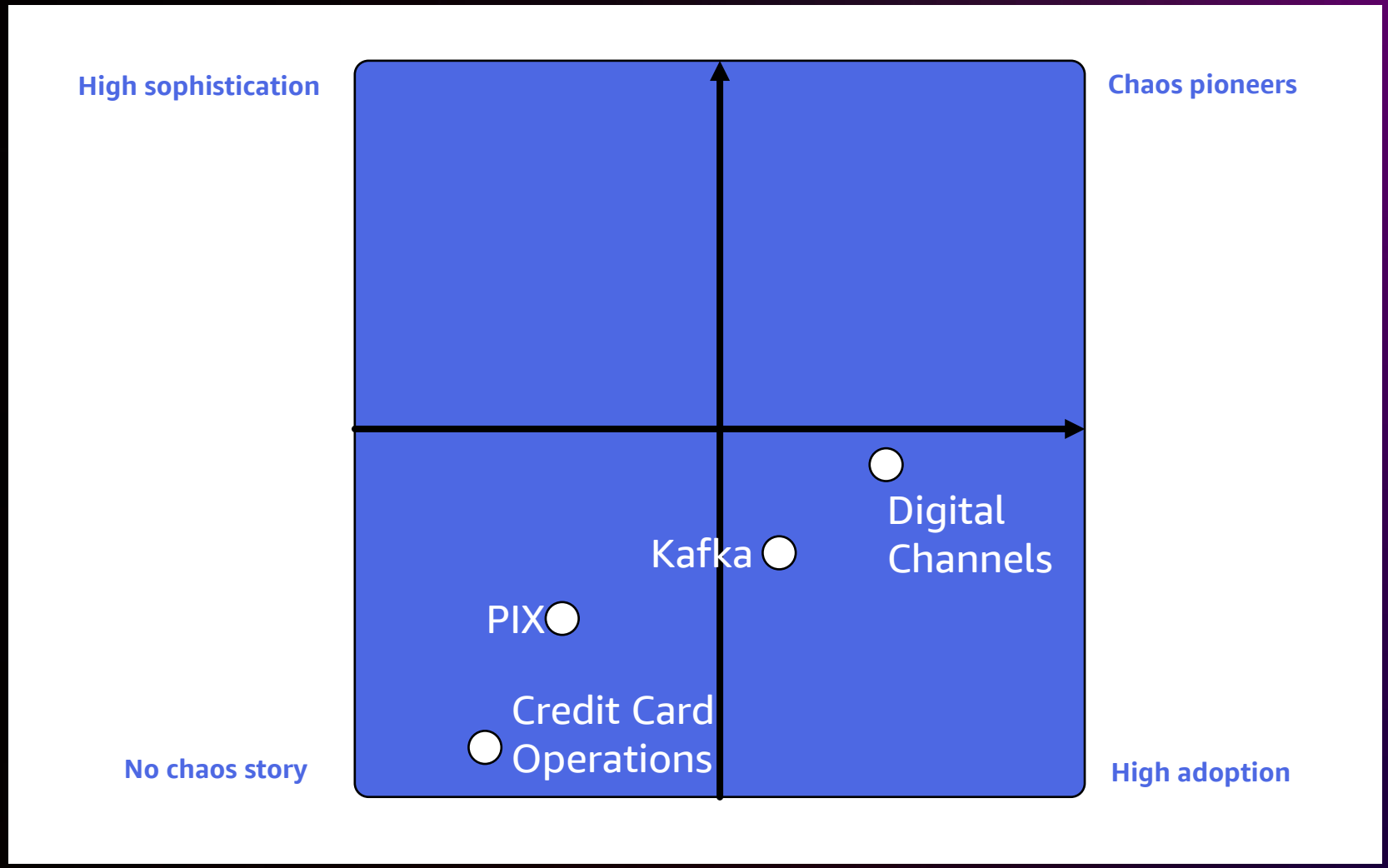
Chaos engineering and testing

Chaos engineering framework for Itaú



- Chaos engineering definitions
- Phased approach (preparation, implementation, and results analysis)
- Chaos engineering maturity model
- Tools
- Example of a GameDay

Chaos engineering maturity model



Chaos engineering hypotheses examples

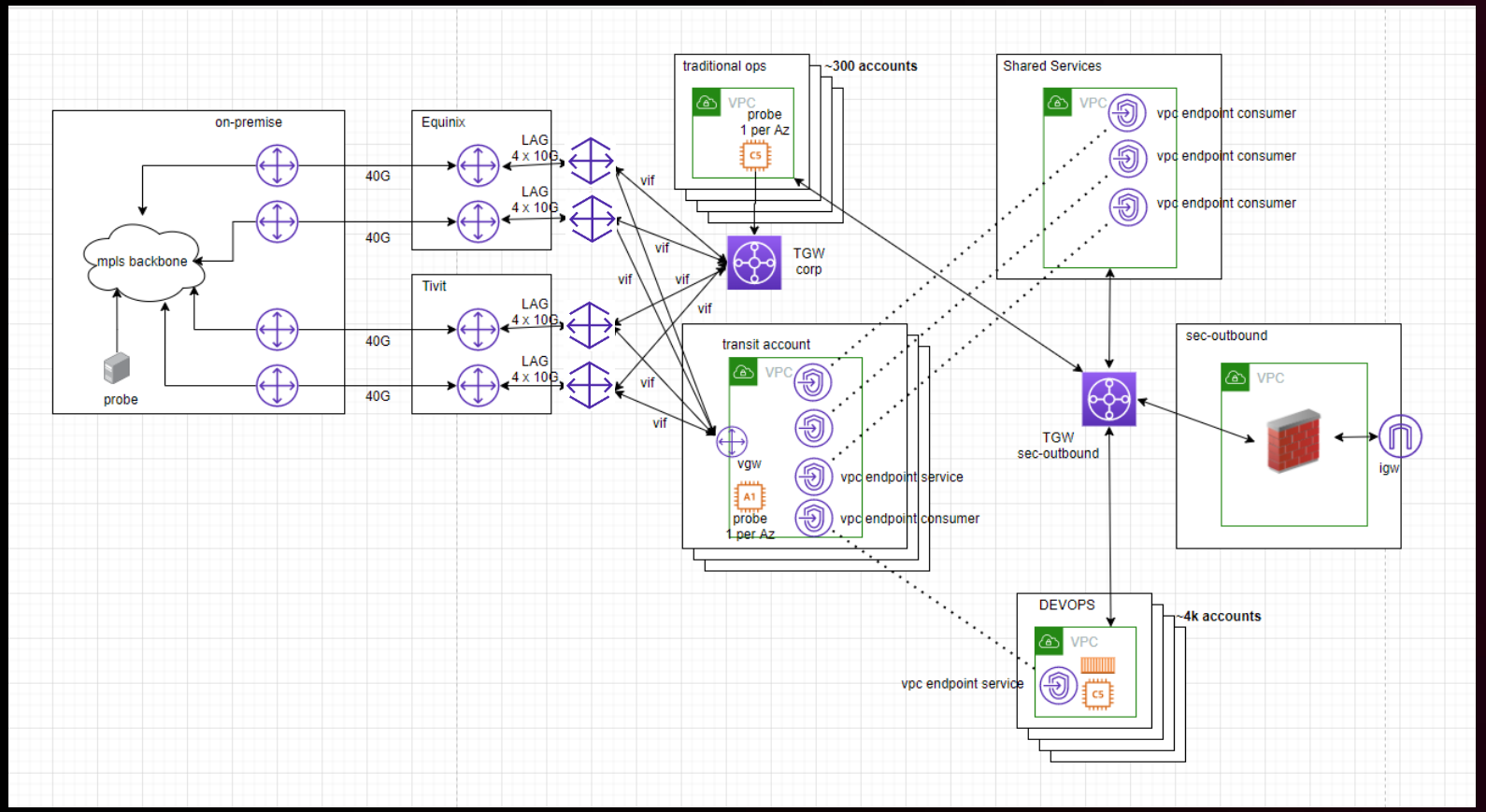
PIX

- Send customer traffic (gradually from 5%–50%) from São Paulo to Virginia
- Reduce number of EC2 instances (“night mode”)

Digital Channels

- Open channels back after complete application interruption
- When the environment becomes overloaded, Digital Channels can be impacted by itself, or even impact the downstream dependencies
- Authorization from the Brazilian Central Bank

Itaú's test plan with AWS Direct Connect



1. **Backup** of all devices involved in the test procedure
2. Validate active routing **paths**
3. **Disable links** to leave only one link per VRF (ensuring traffic asymmetry and avoiding "false positives" in the tests)
4. **Enable links** back one by one
5. Request **validation** from networking, monitoring, and application teams

Direct Connect test plan recommendations

AWS Direct Connect monitoring and failover with Anomaly Detection (AWS solution)

AWS Direct Connect failover test

Periodically review that each failover path has enough bandwidth to support its own primary VRFs and the VRFs that fail over (static stability)

Use more than one link aggregation group for production traffic

Critical dependencies validation and deployment strategy review

Critical dependencies validation

Service	NF2	SI2	PIX - Payments	PIX - DICT	PIX - Wallet	Kafka
API Gateway			Hard	Hard	Hard	
DynamoDB			Hard	Hard	Hard	
Elastic Compute Cloud	Hard	Hard				Hard
Elastic Container Service			Hard	Hard	Hard	
ALB	Hard					
NLB	Soft	Hard	Hard	Hard	Hard	Hard
ElastiCache			Hard	Soft	Soft	
Key Management Service				Hard		Hard
Kinesis Firehose			Soft	Soft		
Lambda	Soft		Hard	Hard	Hard	Soft
Relational Database Service			Hard	Hard	Hard	
Route 53	Hard	Hard	Hard	Hard	Hard	Hard
Secrets Manager			Hard	Hard	Hard	Hard
Simple Notification Service			Hard	Hard	Hard	X
Simple Queue Service			Hard	Hard	Hard	X
Simple Storage Service	Hard		Soft	Hard	Soft	X
WAF	Soft		Soft	Soft	Soft	Soft
Fargate		Hard	Hard	Hard	Hard	X
VPC Endpoint	Hard	Hard	Hard	Hard	Hard	Hard
Transit Gateway (w/ Multicast)	Hard	Hard	Hard	Hard	Hard	Hard
Direct Connect	Hard	Hard	Hard	Hard	Hard	Hard
Global Accelerator	Hard					
Autoscaling	Hard	Hard	Hard	Hard	Hard	Hard
SSM - Run Command	Hard	Hard				
CodePipeline	Soft	Soft	Soft	Soft	Soft	
CodeBuild	Soft	Soft	Soft	Soft	Soft	
CodeDeploy	Hard	Hard	Soft	Soft	Soft	
CodeCommit	Soft	Soft	Soft	Soft	Soft	
ECR			Hard	Hard	Hard	
ACM	Hard	Hard	Hard	Hard	Hard	Hard
Shield Advanced	Hard	Hard				
Cloudwatch Alarm	Hard	Hard	Hard	Hard	Hard	Hard
AWS AppMesh		Hard				
CloudHSM			Hard	Hard		

Outages for **hard** dependencies imply that your dependent system is out as well

Outages for **soft** dependencies should have no impact on your service if they were designed appropriately

Digital Channels old deployment strategy

	sa-east-1			us-east-1
Day of the week	**AZ 1**	**AZ 2**	**AZ 3**	**AZ 1**
Saturday	100	0	0	0
Sunday	100	0	0	0
Monday	100	0	0	0
Monday night	0	50	45	5
Tuesday	100	0	0	0
Wednesday	100	0	0	0
Wednesday night	0	50	45	5
Thursday	100	0	0	0
Friday	100	0	0	0
Friday night	0	50	45	5

Digital Channels new deployment strategy

	sa-east-1			us-east-1
Day of the week	**AZ 1**	**AZ 2**	**AZ 3**	**AZ 1**
Saturday	70	0	25	5
Sunday	70	0	25	5
Monday	70	30	0	0
Monday night	0	50	45	5
Tuesday	70	0	25	5
Wednesday	70	30	0	0
Wednesday night	0	50	45	5
Thursday	70	0	25	5
Friday	70	30	0	0
Friday night	0	50	45	5

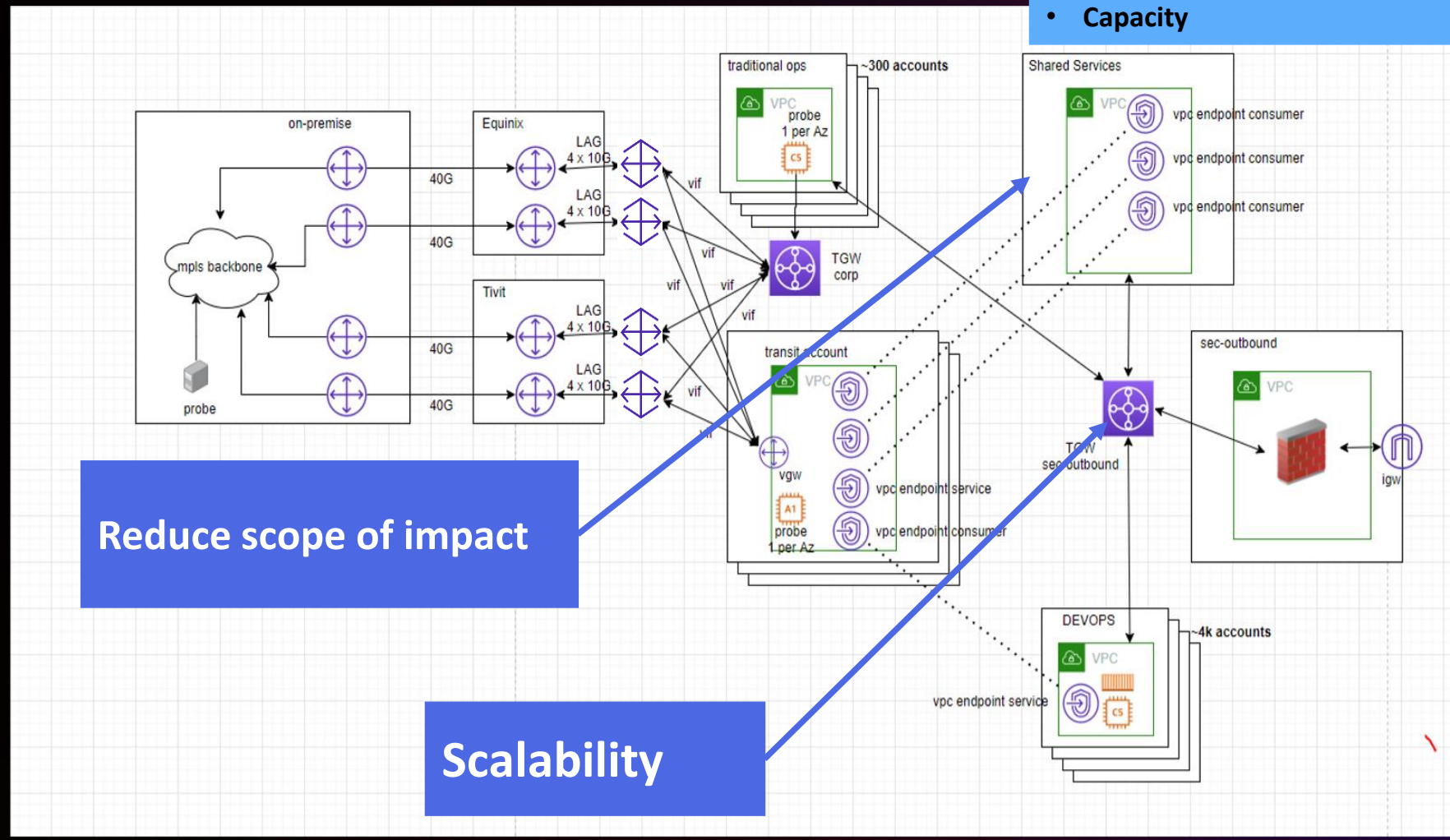
New release

Release -1

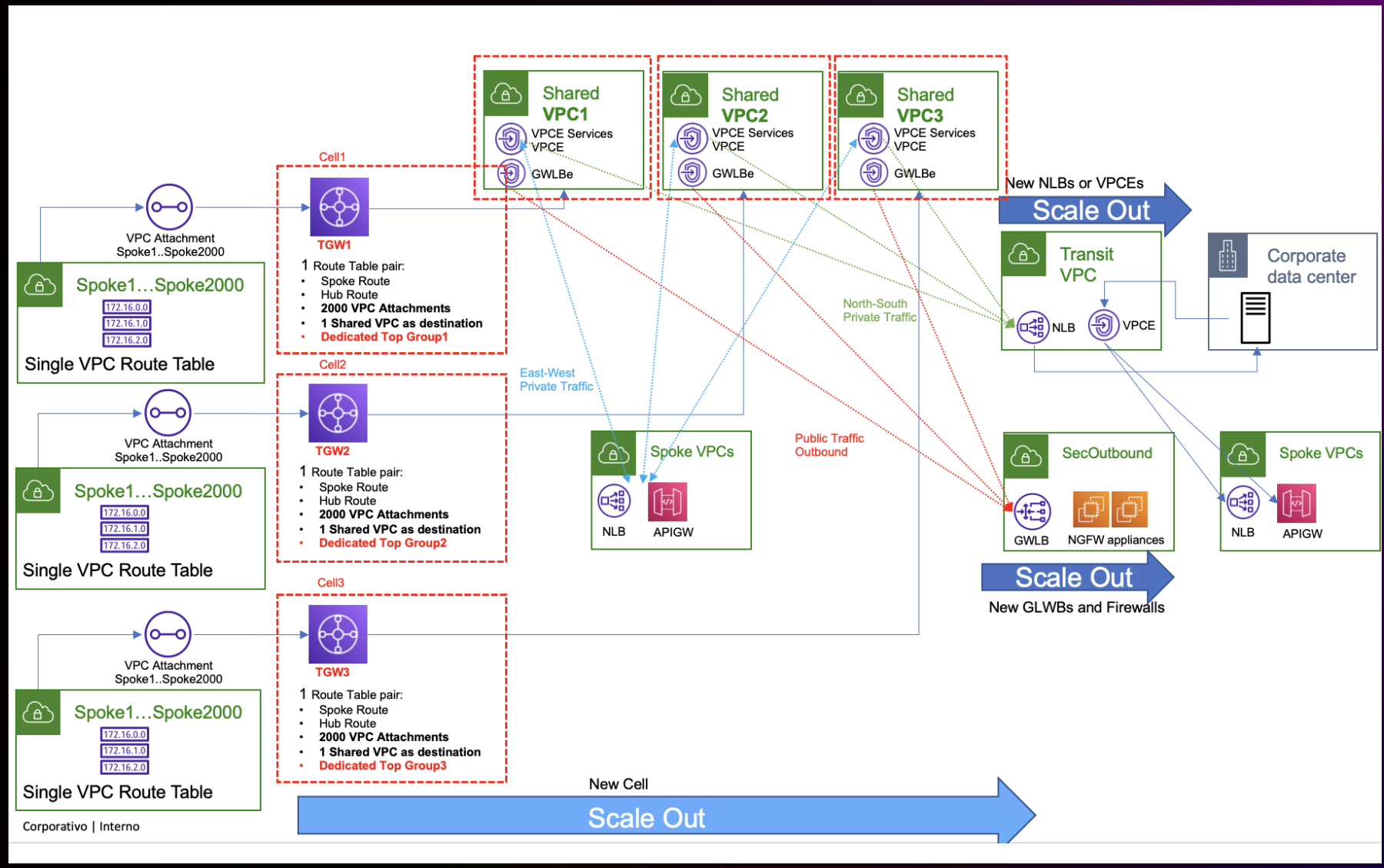
Internet account rearchitecture and service quota table

Internet account – Current architecture

Move from VPN attachment to GWLB
- **Resilience**
- **Management**
- **Capacity**



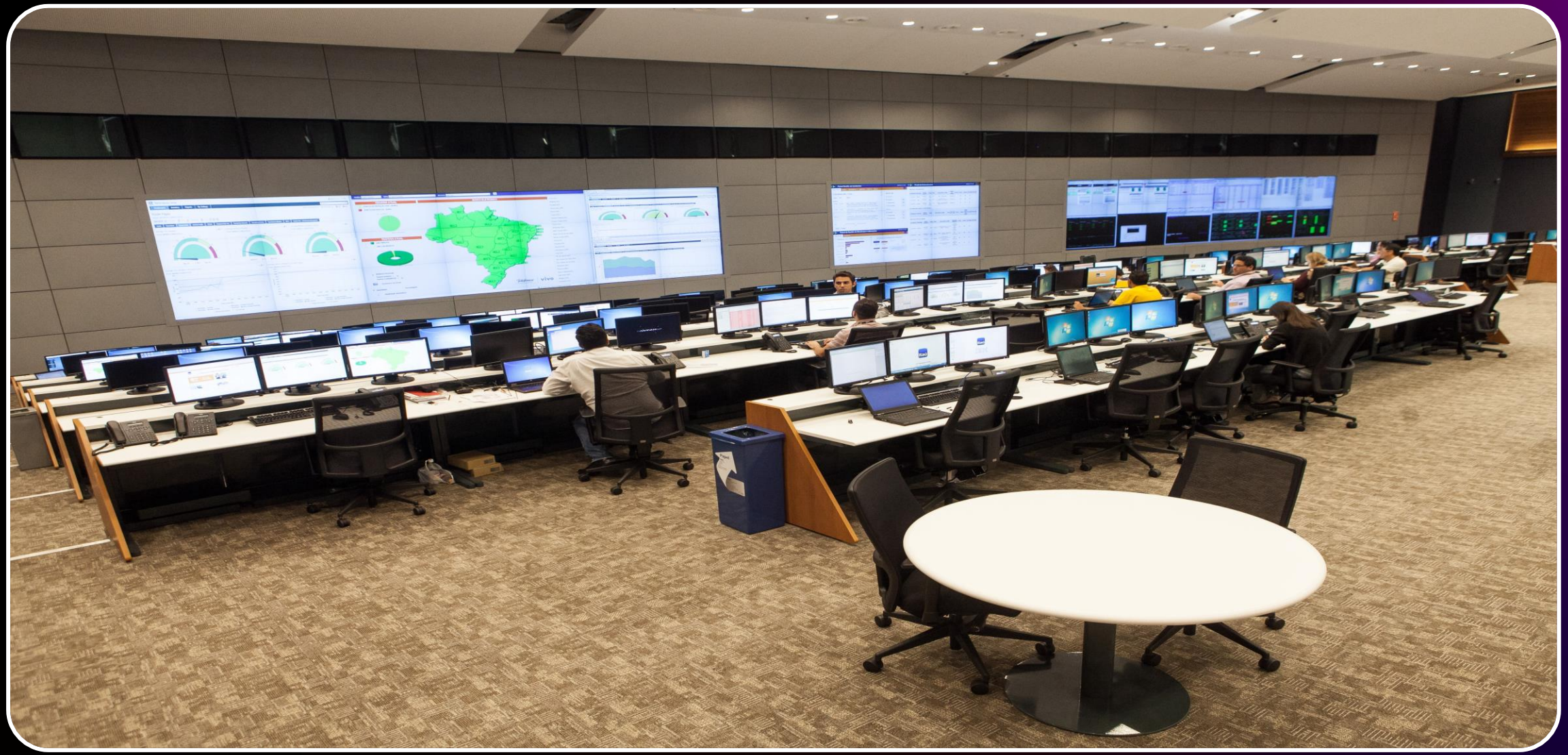
Internet account – New architecture



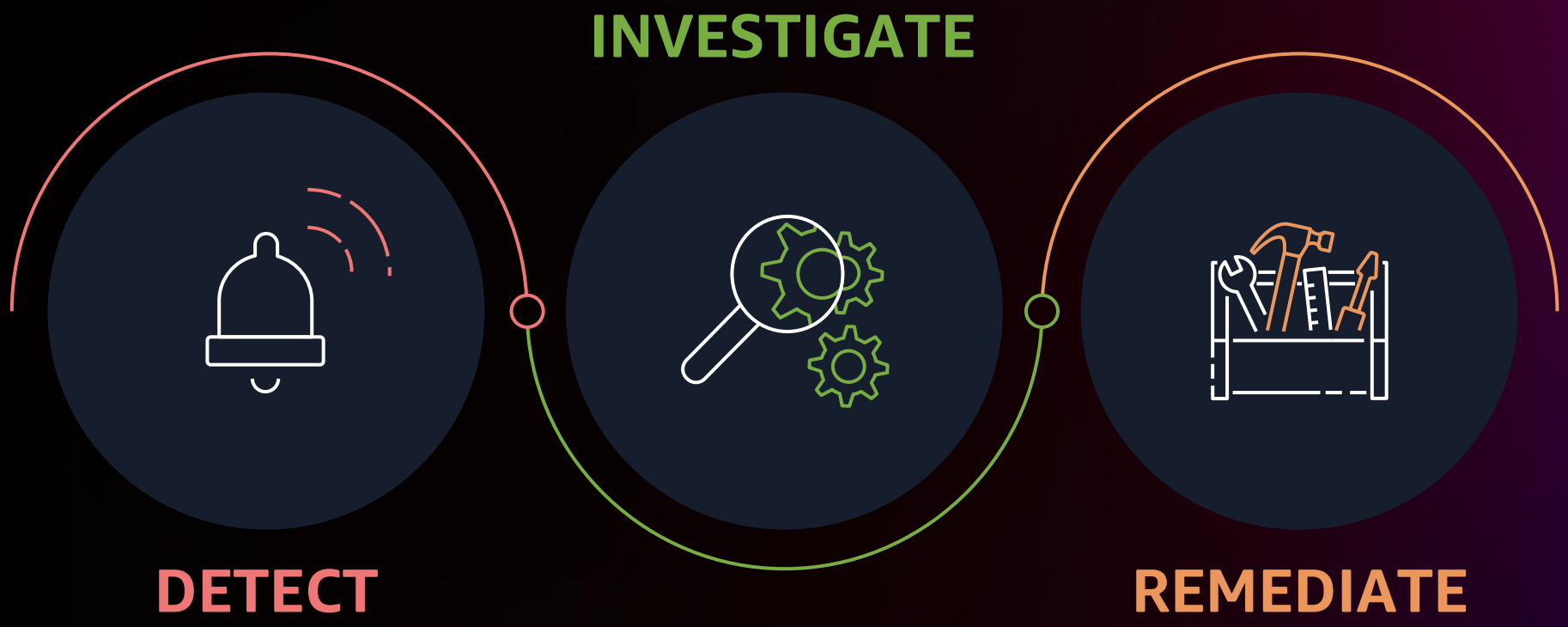
Service quota table

Transit Gateway Bandwidth			CloudWatch Namespace	CloudWatch Metric Dimension
Maximum bandwidth per VPC attachment, AWS Direct Connect gateway, or peered transit gateway connection	Up to 50 Gbps	Hard	AWS/TransitGateway Namespace	TransitGateway/TransitGateway Attachment
Maximum packets per second per transit gateway attachment (VPC, VPN, Direct Connect, and peering attachments)	Up to 5,000,000	Hard	AWS/TransitGateway Namespace	TransitGateway/TransitGateway Attachment
Maximum bandwidth per VPN tunnel	Up to 1.25 Gbps	Hard	AWS/TransitGateway Namespace	TransitGateway/TransitGateway Attachment
Maximum packets per second per VPN tunnel	Up to 140,000	Hard	AWS/TransitGateway Namespace	TransitGateway/TransitGateway Attachment
Maximum bandwidth per Transit Gateway Connect peer (GRE tunnel) per Connect attachment	Up to 5 Gbps	Hard	AWS/TransitGateway Namespace	TransitGateway/TransitGateway Attachment
Maximum packets per second per Connect peer	Up to 300,000	Hard	AWS/TransitGateway Namespace	TransitGateway/TransitGateway Attachment

Operations and observability changes



Observability between application and AWS



Executive dashboards

Dashboards should allow teams and executives who are not application owners a simple view on availability and easily drill down.

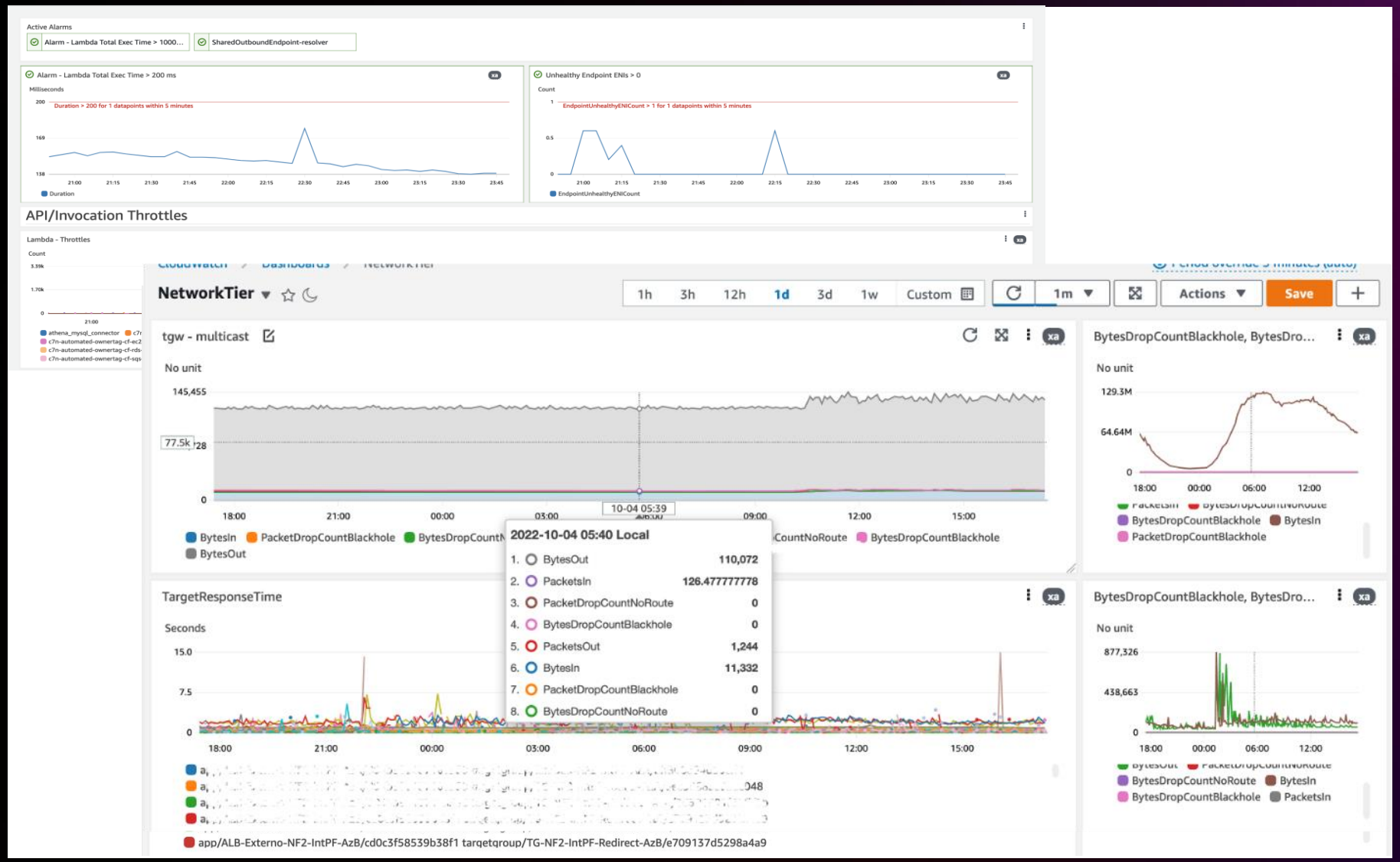
Fabio Napoli
CTO, Itaú

Support experience

Explore ways to improve mean time to detection and mean time to recovery

Workload review to gain context of your workloads and their underlying AWS infrastructure and services

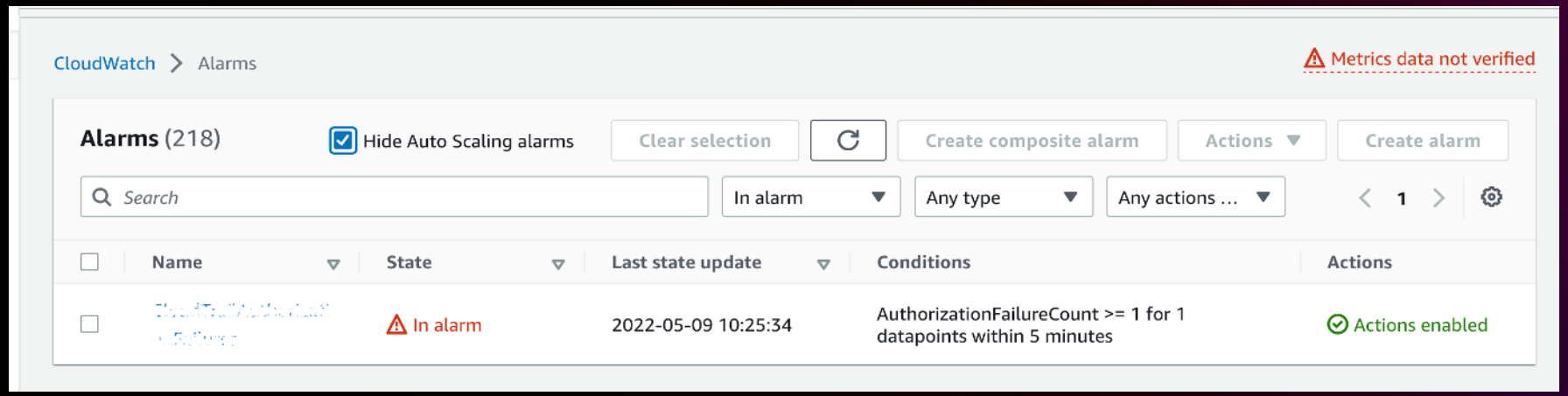
Set up observability to monitor the underlying AWS infrastructure and services employed by workloads



Define critical alarms at the application layer to track the key outcomes of the workload

Define response plans and runbooks for managing critical incidents

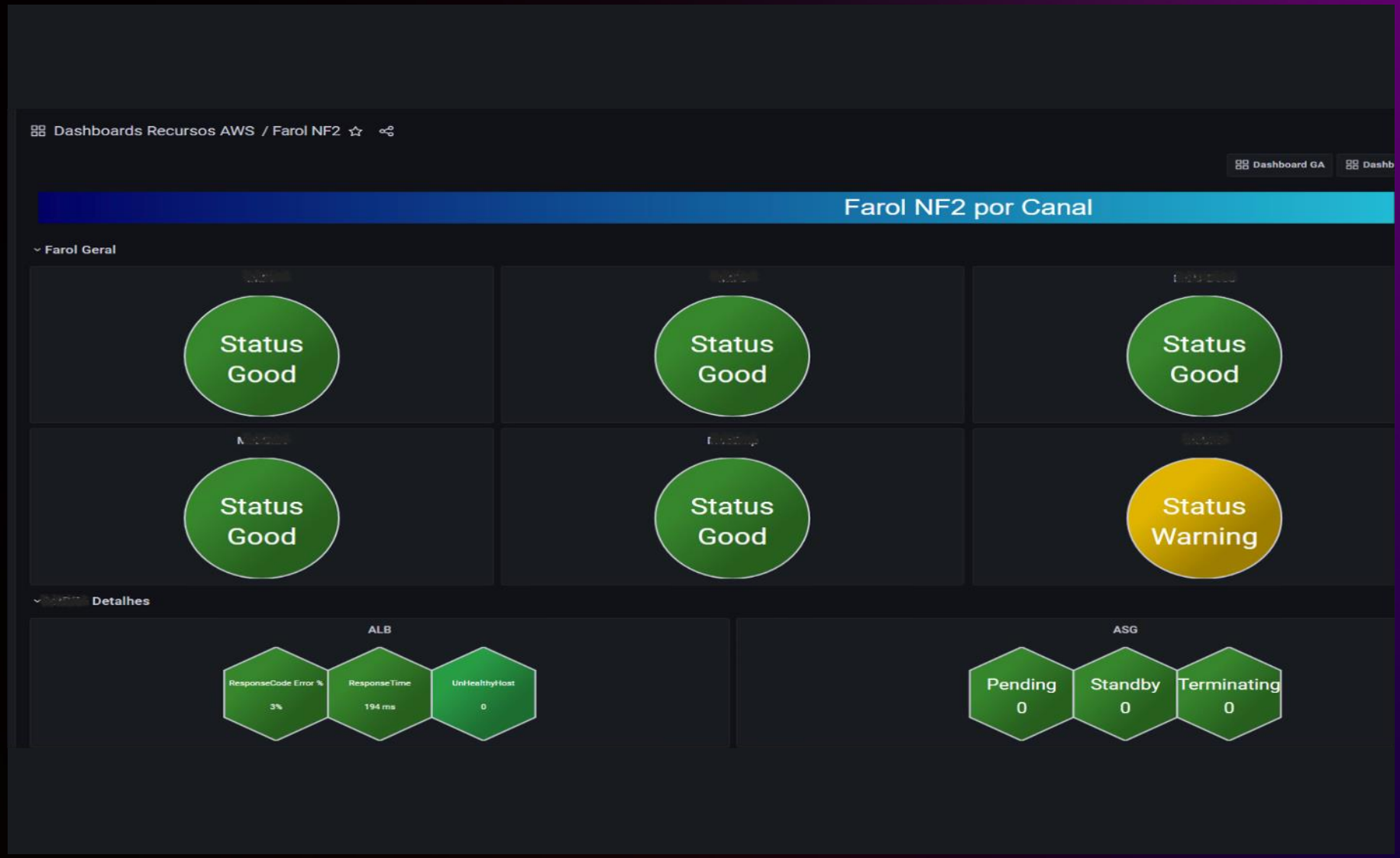
Alarms



“Farol”
(traffic light)

V1 dashboard

Executive view “Farol”

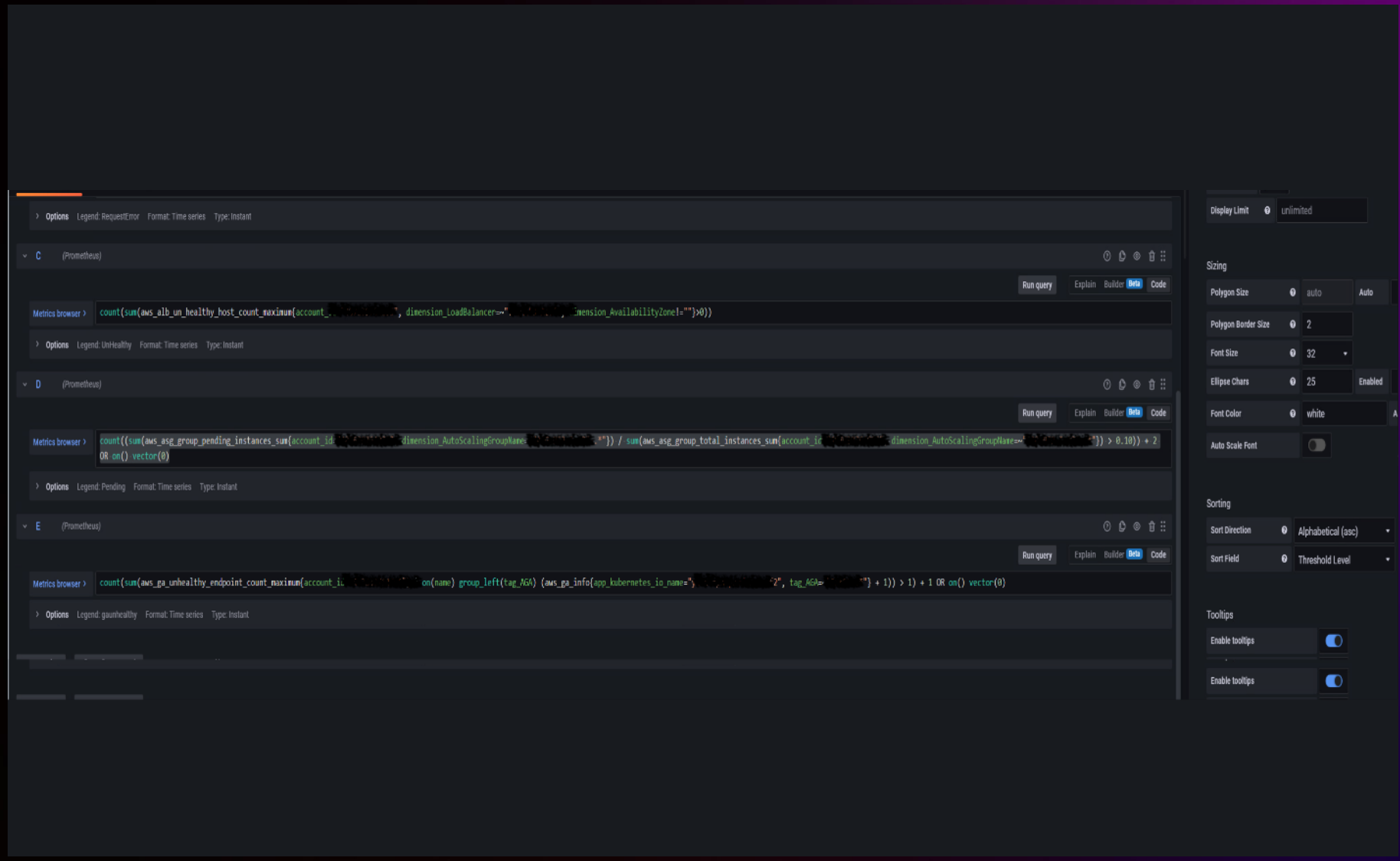


V1 dashboard

Drill down

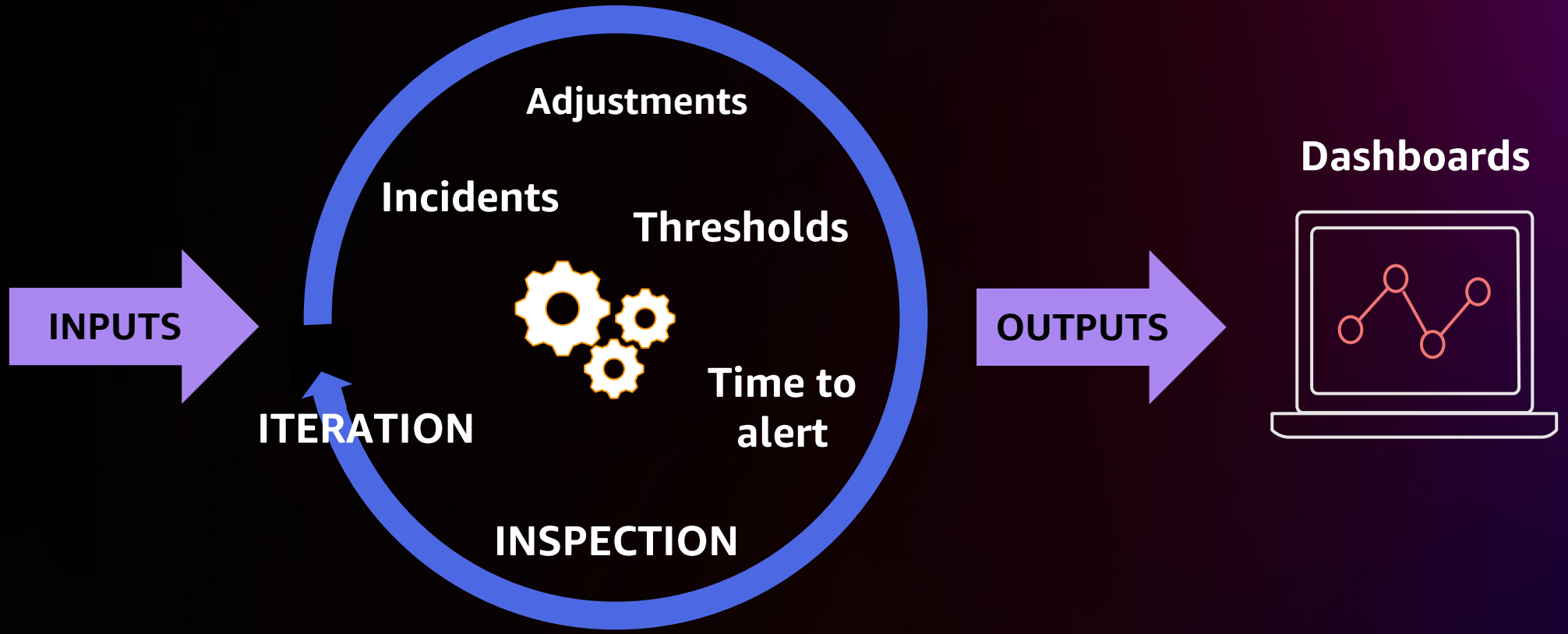
Traffic light logic

Example



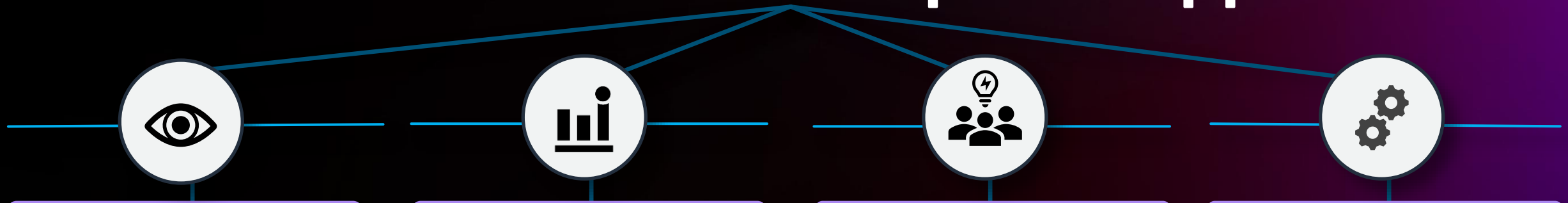
Observability is a journey

Review metrics after events that cause impact to customers, review what lessons were learned and possible improvements, and iterate



What else can we do with operations and observability?

AWS Incident Detection and Response builds on AWS Enterprise Support



Improved observability

- Define critical alarms on the application layer
- Observability on AWS infrastructure and services

Early incident detection

- 24/7 workload monitoring
- AWS engages you within 15 minutes of an incident
- Rapid help from AWS incident management engineer

Faster resolution

- Access to experts to guide you through recovery
- Pre-defined response plans and runbooks
- Live engagement

Reduced potential for failure

- Continuous learning mechanism
- Proactive services
- Post-incident report

Get to know more about Itaú's **digital transformation journey** at our booth

Booth 3405

Next to the Developer Lounge and the Public Sector Pavilion

Thank you!

Anderson Mota

anderson.mota-alves@itau-unibanco.com.br

linkedin.com/in/andersonalves/

Robert Fuente

rffuente@amazon.com

linkedin.com/in/robertfuente/

Gus Santana

gusantan@amazon.com

linkedin.com/in/santanagustavo/

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