
AWS
re:Inforce
JUNE 13 - 14, 2023 | ANAHEIM, CA

TDR233

How LLA reduces incident response time with AWS Systems Manager

Jesus Federico
Principal Solutions Architect
AWS

Sarah Holberg
Principal Product Manager
AWS

Joaquin Cameselle
Senior Manager, Cloud Services
Liberty Latin America

Agenda

Liberty Latin America (LLA) and their security challenges

Overview of AWS security services

LLA security framework and deployment

Q&A

Liberty Latin America: Operations and brands

140 years leading innovation

Leading operator in Latin America and the Caribbean

Operating in over 20 consumer markets and over 30 B2B markets

Extensive and unique submarine fiber network, connecting more than 40 markets with 50,000 kilometers of fiber optic cables

Revenue: $4.4 billion dollars

4.4 million homes passed, 8 million mobile subscribers

3.9 million RGUs (video, internet, and landline subscribers)

Employees: 11,000

LIBERTY NETWORKS Latin America

LIBERTY Costa Rica

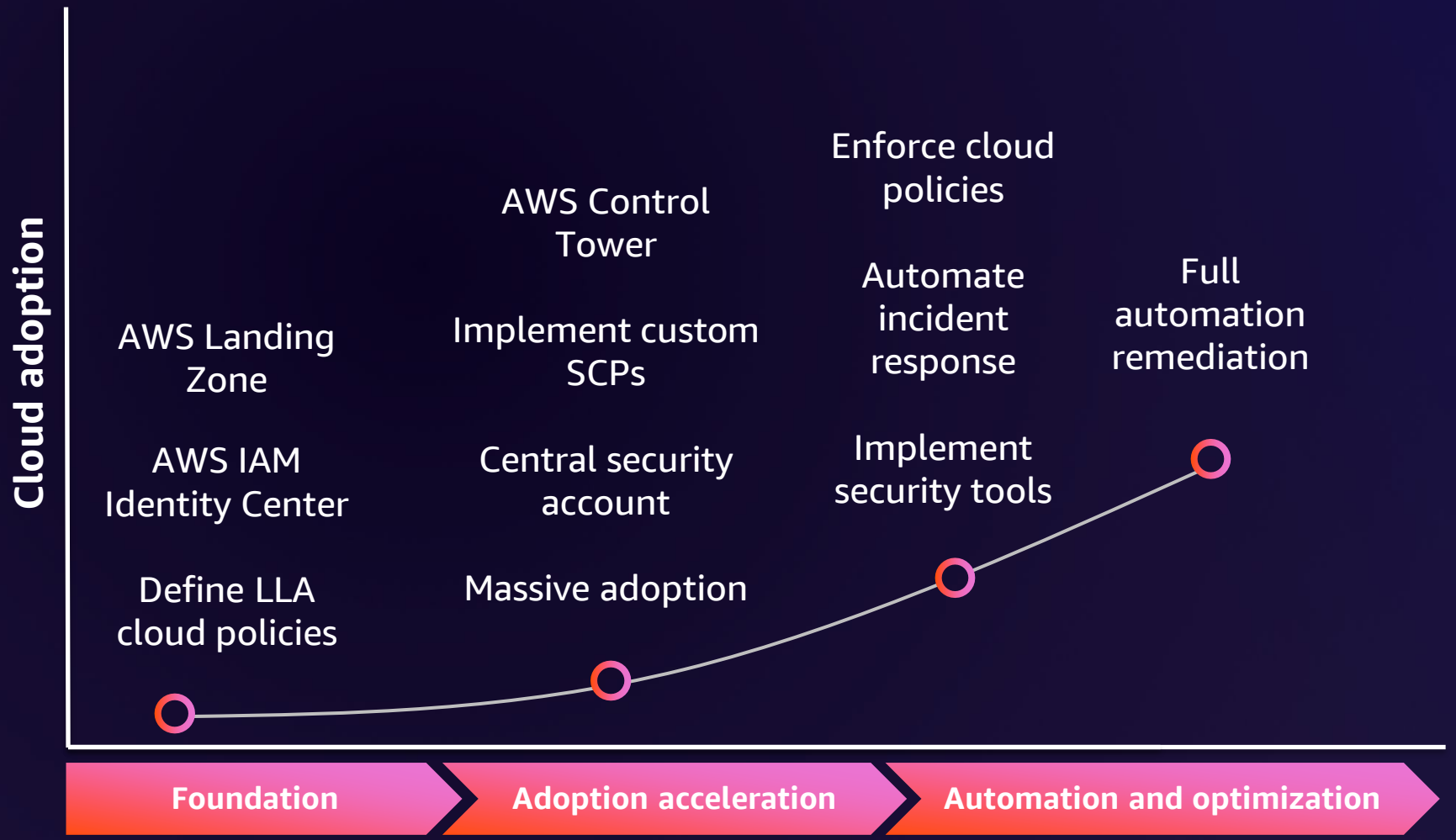
Liberty Puerto Rico

BTC Bahamas

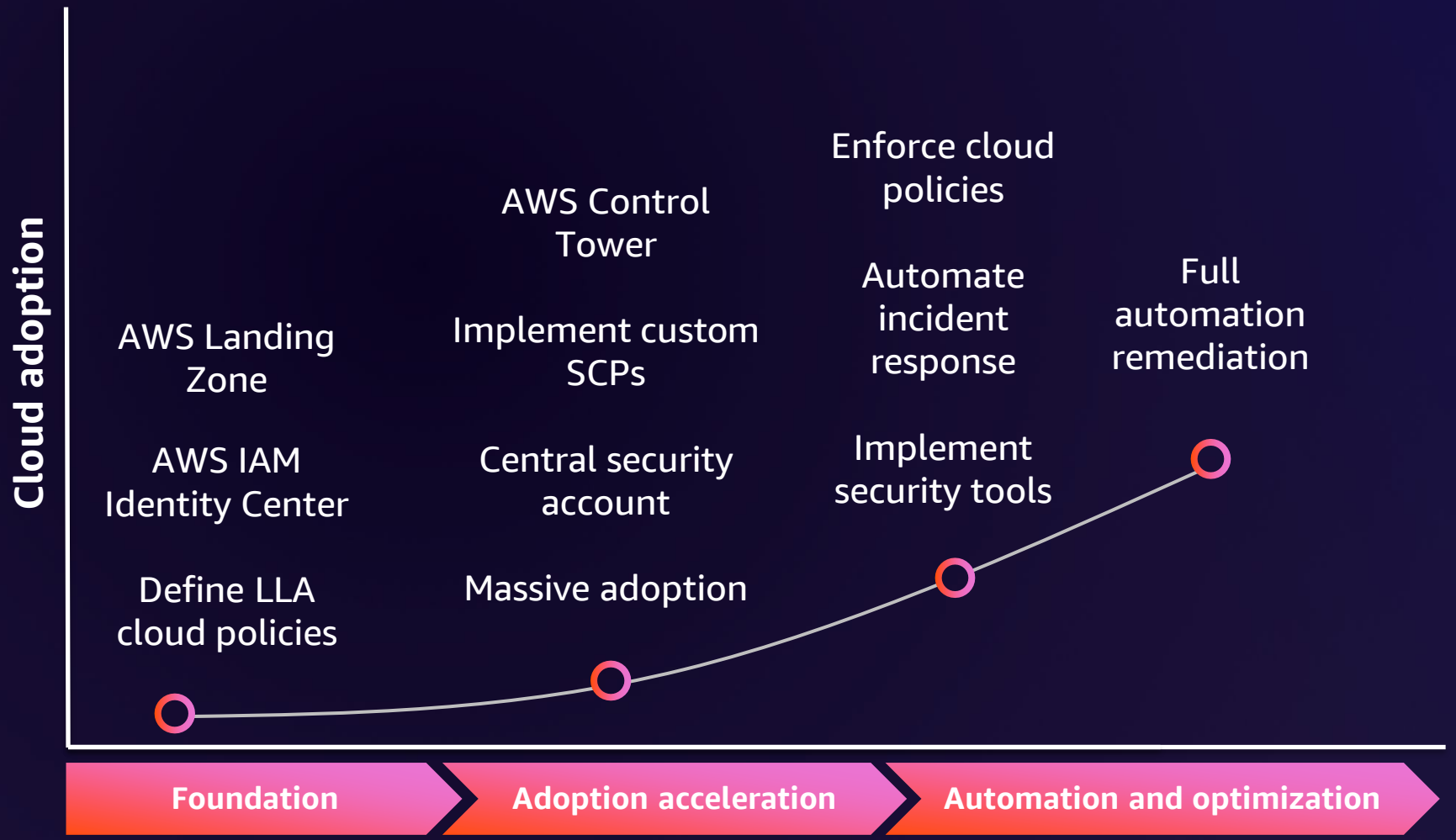
FLOW Caribbean

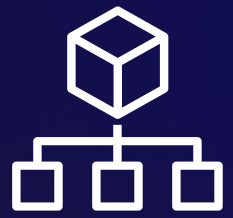
+móvil Panama

Cloud adoption and security challenges



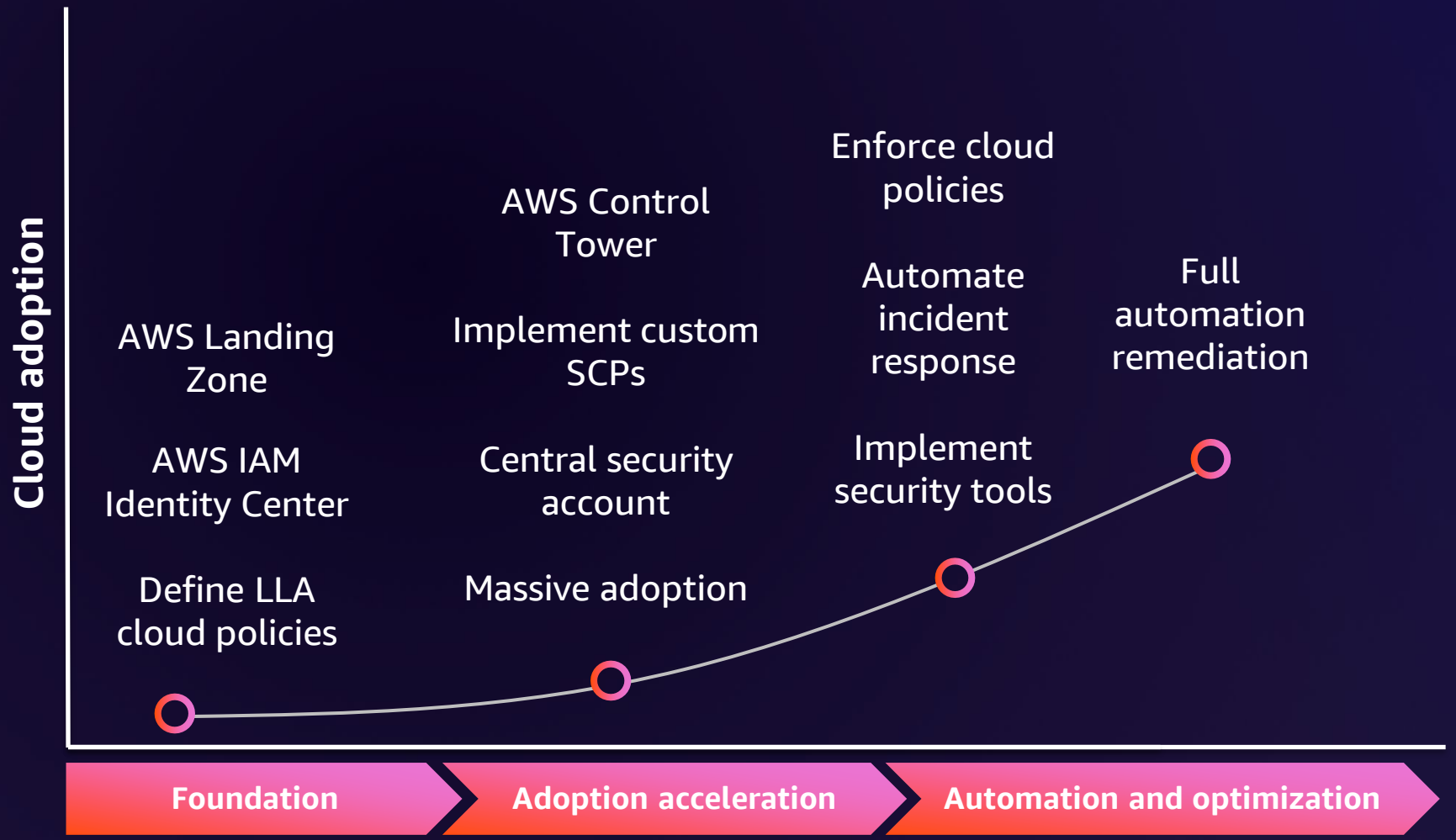
Cloud adoption and security challenges





180+ AWS accounts

Cloud adoption and security challenges



180+ AWS accounts

1,000+ users with AWS access (internal stakeholders and third-party partners)
50+ permission sets

Cloud adoption and security challenges

Cloud adoption and security challenges

Inaccurate
AWS account contact
information

Cloud adoption and security challenges

Inaccurate
AWS account contact information

Insecure
AWS resource configuration

Cloud adoption and security challenges

Inaccurate
AWS account contact
information

Insecure
AWS resource
configuration

Unintended disclosure
of security credentials
and secrets

Cloud adoption and security challenges

Inaccurate
AWS account contact
information

Insecure
AWS resource
configuration

Unintended disclosure
of security credentials
and secrets

Ineffective response to
detective controls

Cloud adoption and security challenges

Inaccurate
AWS account contact
information

Insecure
AWS resource
configuration

Unintended disclosure
of security credentials
and secrets

Ineffective response to
detective controls

Lack of continuous
vulnerability management

Users with different
cloud skills

Liberty Latin America security framework: Logical design

Liberty Latin America security framework

Liberty Latin America security framework

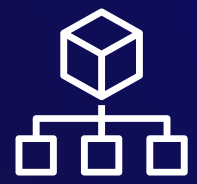
Workload isolation using AWS Organizations

Threat detection with Amazon GuardDuty

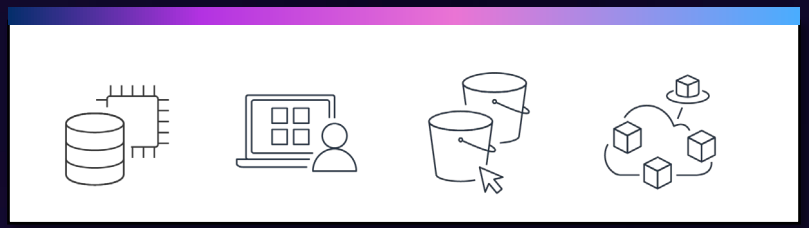
AWS Security Hub for centralizing security data and alerts

Security event processing with Amazon EventBridge

Incident management with AWS Incident Manager



Threat detection, monitoring, and response



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

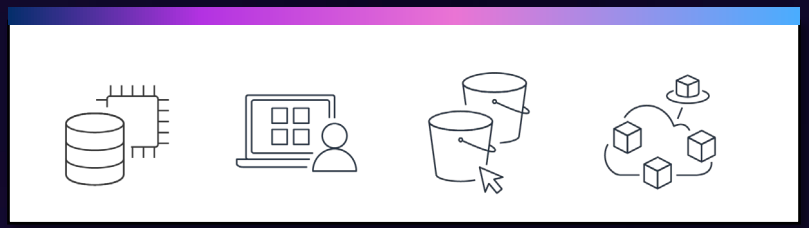
Amazon Inspector
Detect vulnerabilities

AWS Security Hub
Automate security checks and centralize security alerts

Amazon Detective
Investigate events and findings

Amazon Security Lake
Normalize and analyze security data

Threat detection, monitoring, and response



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

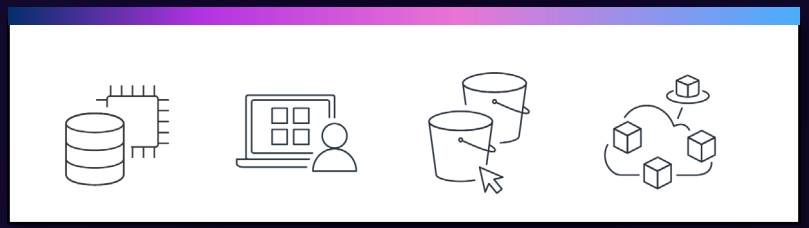
Amazon Inspector
Detect vulnerabilities

AWS Security Hub
Automate security checks and centralize security alerts

Amazon Detective
Investigate events and findings

Amazon Security Lake
Normalize and analyze security data

Threat detection, monitoring, and response



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

Amazon Inspector
Detect vulnerabilities

AWS Security Hub
Automate security checks and centralize security alerts

Amazon Detective
Investigate events and findings

Amazon Security Lake
Normalize and analyze security data

Amazon GuardDuty

Data sources

- VPC Flow Logs
- DNS logs
- Login events
- CloudTrail events
- S3 data plane events
- Amazon EKS control plane logs and runtime activity

Security analytics

- Machine learning
- Threat intelligence
- Continuous learning

Security findings

- Actionable
- Accurate
- Contextual

Integration

- Amazon Detective
- AWS Security Hub
- Amazon EventBridge
- AWS Partner Network

AWS Security Hub

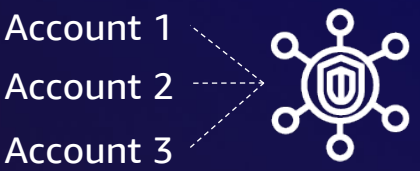
Centrally view and manage security alerts and automate security checks

Save time with aggregated findings

Improve security posture with automated checks

Review curated security best practices

Seamlessly integrate with standardized findings format



Activate multi-account support

AWS Security Hub

Amazon GuardDuty

Amazon Macie

AWS Firewall Manager

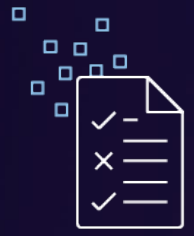
AWS Config

Amazon Inspector

IAM Access Analyzer

Third-party integrations

AWS Security Hub



Aggregate and prioritize findings

Conduct automated security checks against benchmarks

Take action to investigate or respond and remediate

Better visibility into **security issues** Easier to stay in **compliance**

Security Hub information flows

Findings ingestions

AWS Config

Amazon GuardDuty

Amazon Inspector

IAM

Amazon Macie

AWS Firewall Manager

CROWDSTRIKE

And many more

Standards and controls

PCI DSS

NIST

AWS FSBP

CIS AWS Foundations Benchmark

Service-managed standards

AWS Security Hub

Amazon EventBridge

Findings integrations

Amazon Detective

AWS Audit Manager

Amazon Security Lake

AWS Trusted Advisor

AWS Chatbot

Remediation actions

AWS Lambda

AWS Systems Manager

AWS Step Functions

Take action with partners

Plus many others

This is not a complete list. To view all AWS Partners for this category, visit AWS Partner Solutions Finder. This list of partners is current as of May 17, 2023.

AWS Systems Manager Incident Manager

RESOLVE APPLICATION ISSUES FASTER WITH AUTOMATED RESPONSE PLANS

1. Prepare for the **who**, **what**, and **where** in a response plan

2. Attach **response plans** to monitors

3. Manage and track in **Incident Manager**

Response plan

- Escalation plans & contacts — **Who you engage**
- Automated runbooks — **What you do**
- AWS Chatbot — **Where you collaborate**

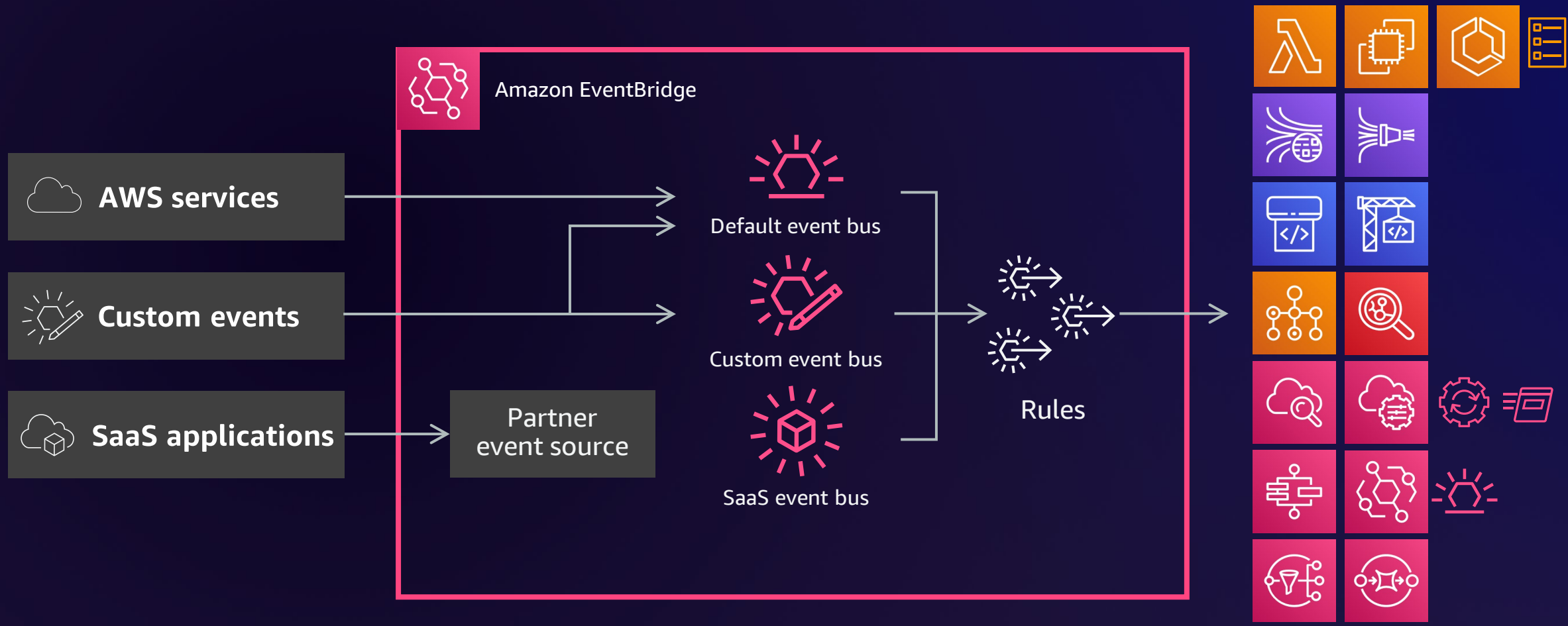
Triggers (event sources)

- Amazon CloudWatch
- Amazon EventBridge
- Manual

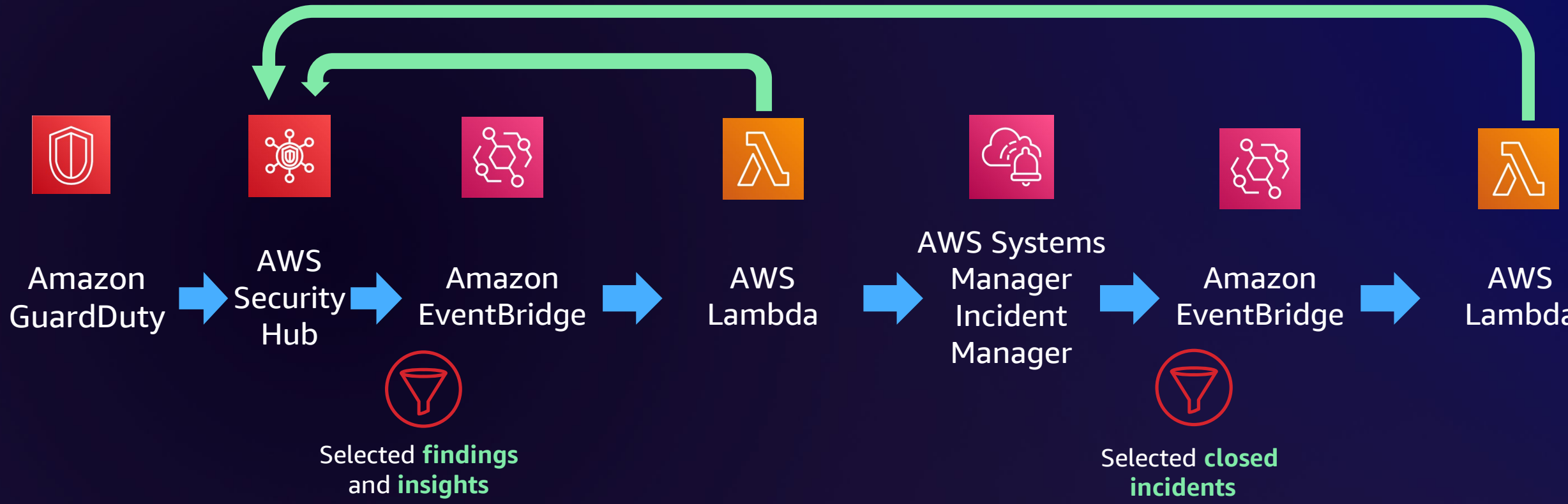
Incident Manager

- Incident timeline
- Integrated runbook
- Triage & analysis

Amazon EventBridge architecture

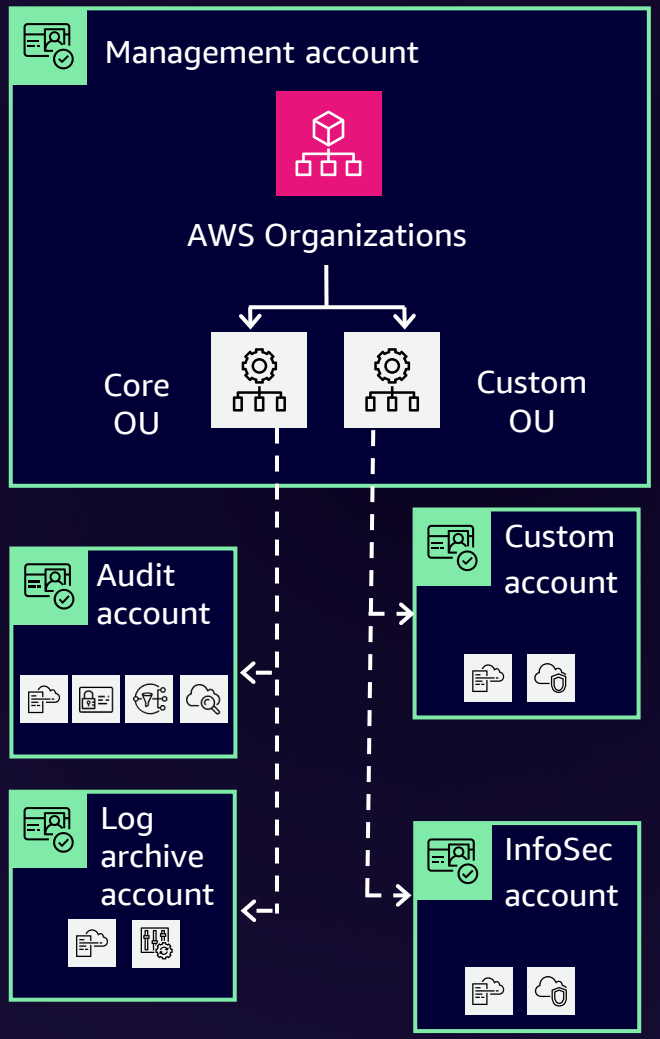


Liberty Latin America security framework



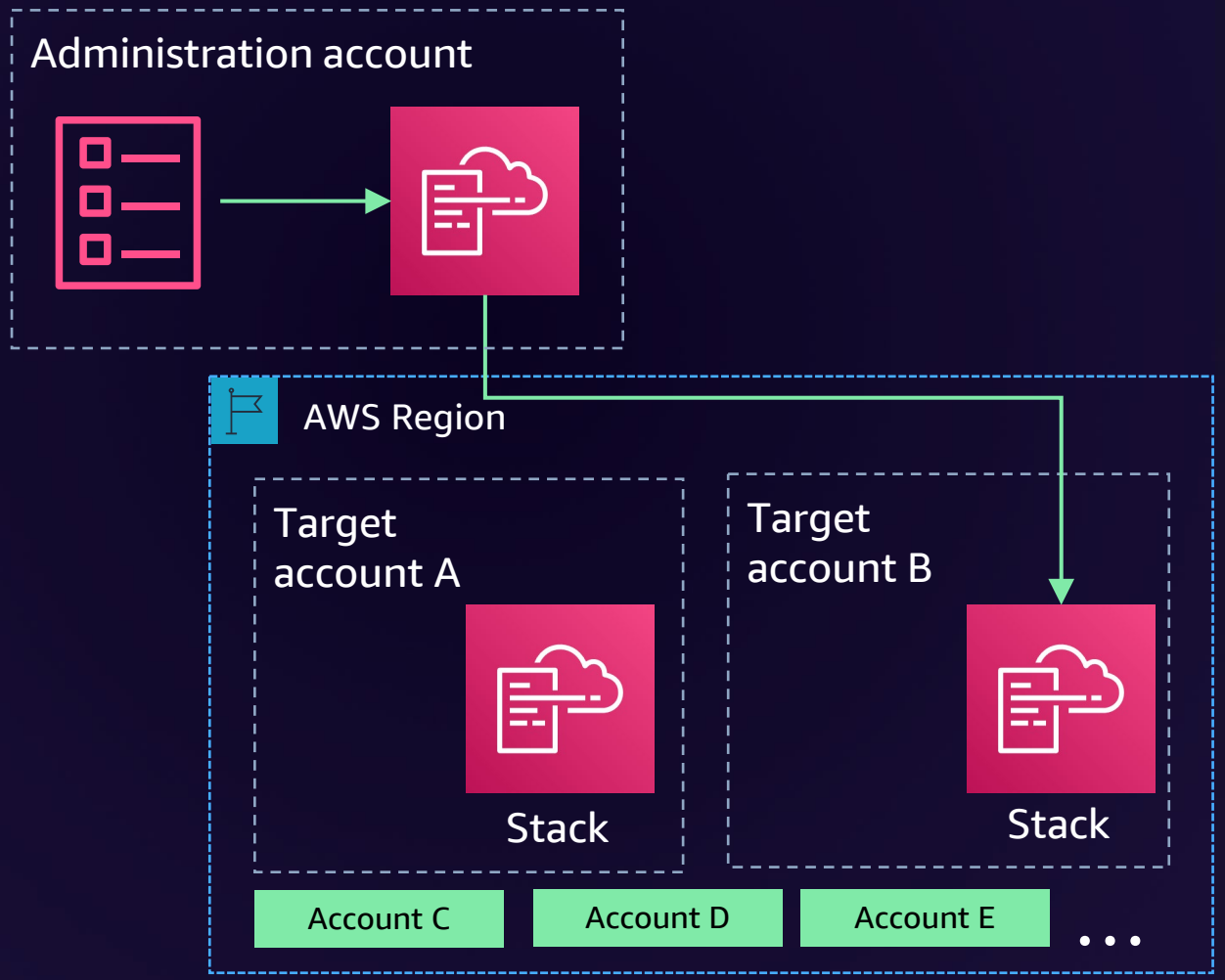
Liberty Latin America security framework: Deployment

Liberty Latin America Multi-account architecture



- Management account – designation of your existing account to create a new organization; also your main payer account
- Organizations have several organizational units (OUs) for workloads
- AWS Control Tower-created accounts (i.e., audit account and log archive account)
- InfoSec account – manage GuardDuty and Security Hub centrally

Deployment: AWS CloudFormation StackSets



Thank you!

Please complete the session survey in the mobile app

Jesus Federico
linkedin.com/in/jesusf/

Sarah Holberg
linkedin.com/in/sarah-holberg/

Joaquin Cameselle
linkedin.com/in/jcameselle/