



PUBLIC SECTOR SYMPOSIUM

BRUSSELS | MARCH 28, 2023

BTT205

Securing and automating compliance with AWS

Laura Verghote
Solutions Architect
AWS

Cristina Rios Iribarren
Solutions Architect
AWS



Agenda

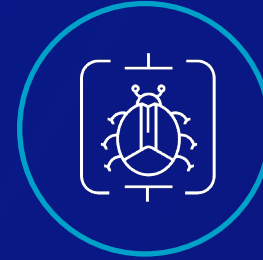
- Challenges in Public Sector
- AWS tools and guidance to enable compliance
- AWS Services to automate compliance + Demo
- Multi-account strategy

Challenges in Public Sector

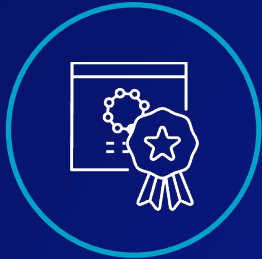
[*Compliance*]



Dynamic
landscape



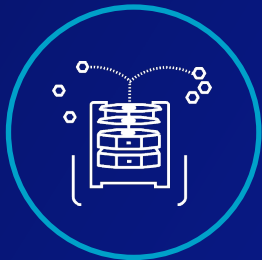
Pace of
innovation



Volume, variety,
and velocity



Familiarity with
the cloud



Global/
geographic



Different compliance
and security needs

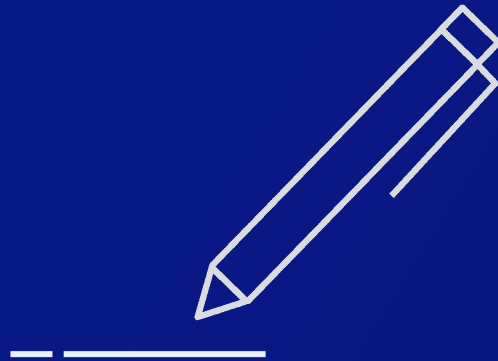
*You are not
alone!*

AWS Artifact

AWS Artifact provides on-demand access to security and compliance reports and select online agreements.



Access AWS compliance reports on demand



Review, accept, and manage agreements with AWS



Access compliance reports from third-party auditors

Shared Responsibility Model - Security

Customer is responsible for security **in** the cloud

Customer
AWS

Customer responsibility is determined by the AWS Cloud services a customer selects.

AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud.

AWS is responsible for security **of** the cloud

Shared Responsibility Model – Compliance and Regulation



AWS is responsible for compliance **of** the cloud

Customer Story



Making America's Neighborhoods Safer with IDEMIA Cloud-Based Fingerprinting Software

*STORM ABIS needed to adhere to **strict security and compliance regulations** from local, state, and federal agencies. AWS offered IDEMIA the security configurations they required, along with access to a team of cloud experts that could help build the solution from scratch. With a compliant and secure foundation to build on, **IDEMIA and AWS worked together to design a cloud-first application** that was made by examiners, for examiners.*

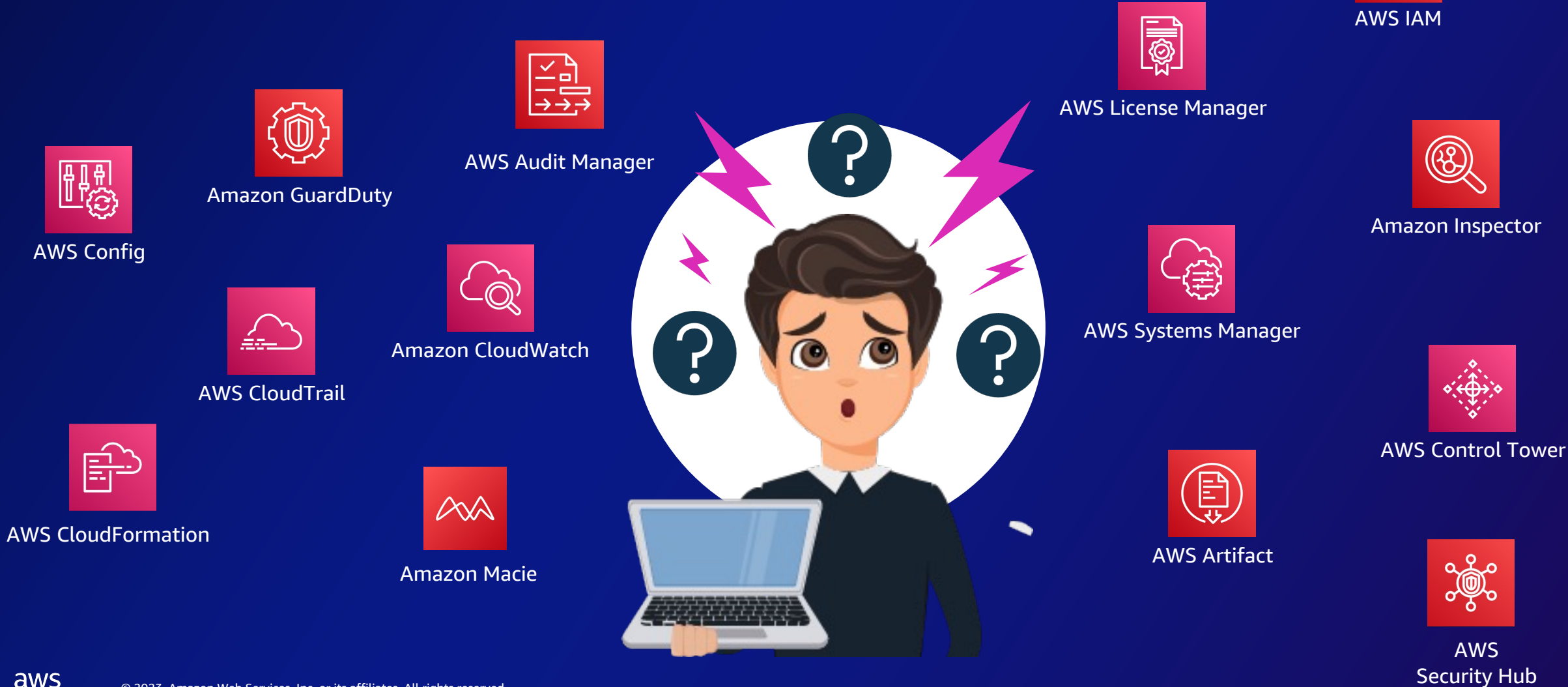


AWS Services used to automate compliance



Which one do you use for compliance?

- Wide range of AWS capabilities



AWS CloudFormation



- Infrastructure as code
- Provisions AWS resources in a predictable, repeatable, and automated fashion
- Version control to track changes to your infrastructure

Infrastructure as code



WebSG:

Type: `AWS::EC2::Securitygroup`

Properties:

SecurityGroupIngress:

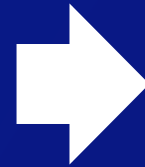
- **CidrIP:** `0.0.0.0/0`

FromPort: `80`

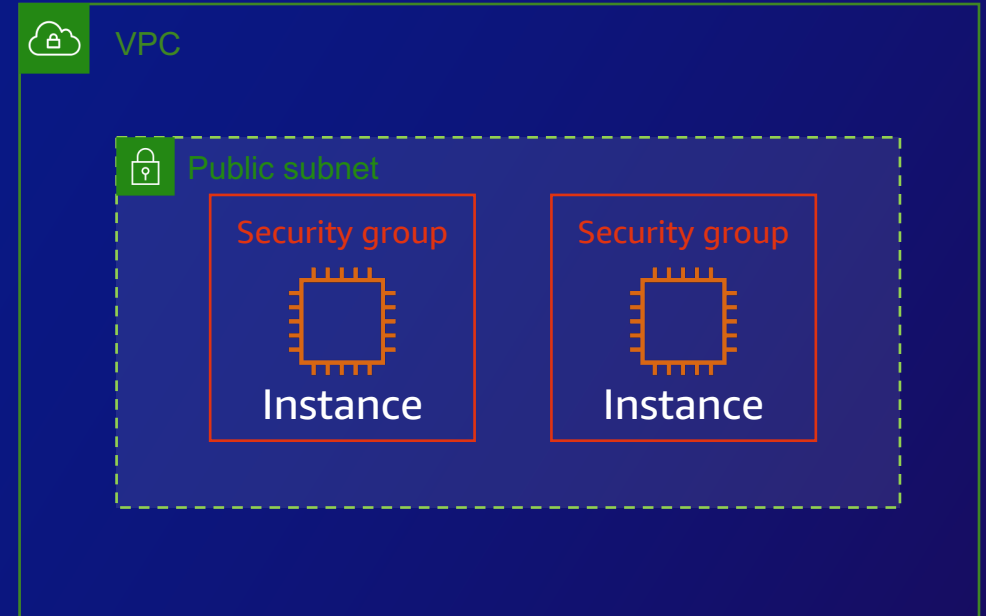
ToPort: `80`

IpProtocol: `tcp`

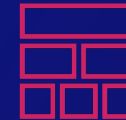
VpcId: `!Ref MyVPC`



AWS CloudFormation
engine



AWS CloudFormation
Template



AWS CloudFormation
Stack

Why should we automate?



consistency



Speed




Reusability



Auditing

How can AWS CloudFormation be used to automate compliance?

```
WebSG:
  Type: AWS::EC2::SecurityGroup
  Properties:
    SecurityGroupIngress:
      - CidrIP: 0.0.0.0/0
        FromPort: 80
        ToPort: 80
        IpProtocol: tcp
    VpcId: !Ref MyVPC
```



Infrastructure as code with compliance controls

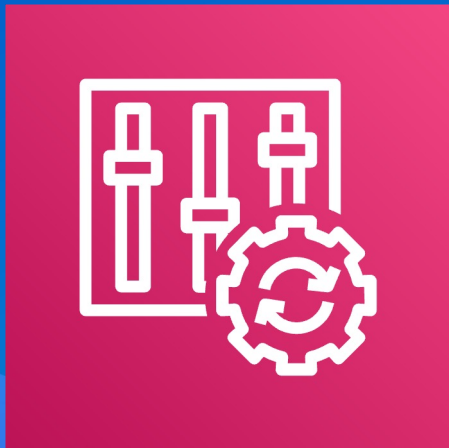
=

Consistency and repeatability



Integration with other AWS services

AWS Config



Continuous monitoring and **assessment** service that provides an inventory of AWS resources and captures configuration changes associated with your resources

- Sends notifications when changes occur
- Integrates with other AWS services to remediate issues
- Can be used to trigger an AWS Lambda function

AWS Config - rules



Managed rules

- Defined and maintained by AWS
- Require minimal to no configuration
- E.g. EBS volume Encryption, RDS Instance Backup Enabled, EC2 Instance changes



Administrator

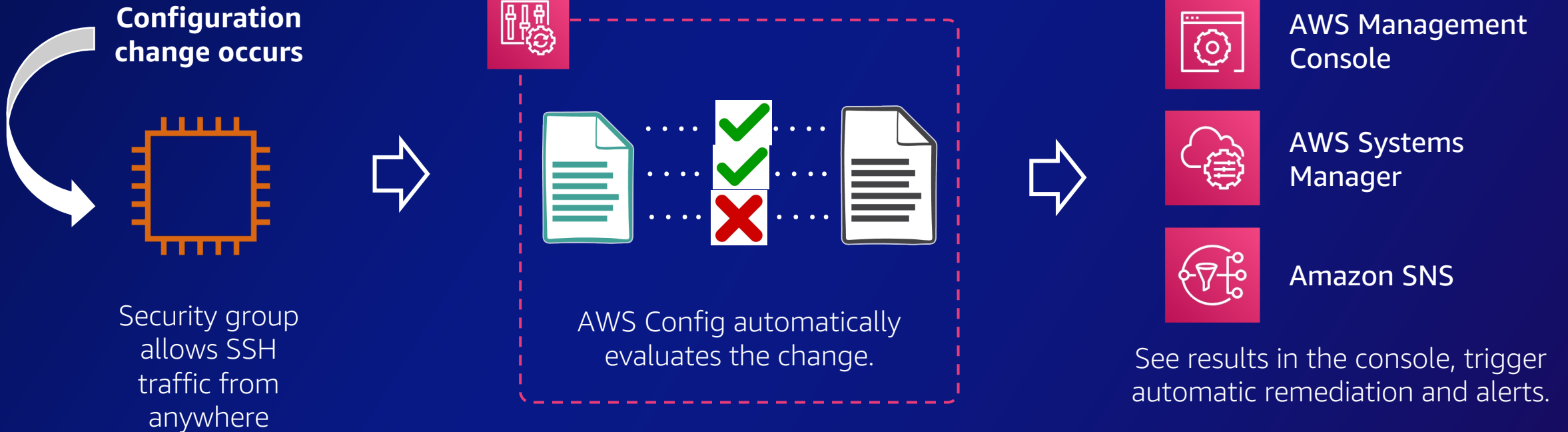
Custom rules

- Use AWS Lambda functions
- Maintained by the customer
- E.g. Tagging compliance, Security Group compliance, Cost Optimization

AWS Config conformance packs

- Manage the compliance of your AWS resources at scale
- Integrated with AWS Organizations
- Package and deploy a collection of rules and remediation actions
- Supports both managed and custom rules

Evaluating rules





Services

Search

[Alt+S]



London

Admin/lauvrl-Isengard @ aws-laura-trainer

- Resource Groups & Tag Editor
- EC2
- AWS Artifact
- S3
- IAM
- Lambda

Console Home [Info](#)

Reset to default layout

+ Add widgets

Recently visited [Info](#)



EC2



Config



Route 53



Amazon SageMaker



S3



CloudFront



AWS Glue



DynamoDB



Trusted Advisor



AWS Well-Architected Tool

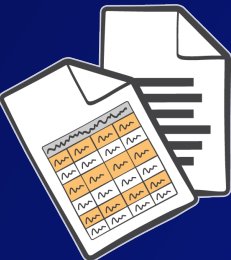


Database Migration Service



Lightsail [↗](#)

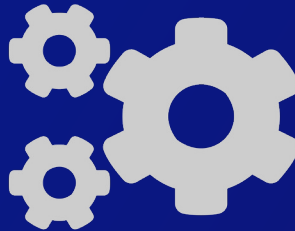
How can AWS Config be used to automate compliance?



Resource inventory



Compliance checks



Change management



Integration with other AWS services

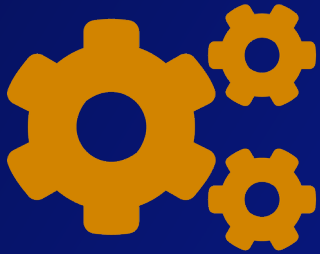
AWS Systems Manager



Centrally manage the security and hardening of your applications and OS

- System inventory
- OS patch updates
- Automated AMI creation
- OS and application configuration at scale
- Session manager

Security benefits



Automate complex and repetitive tasks

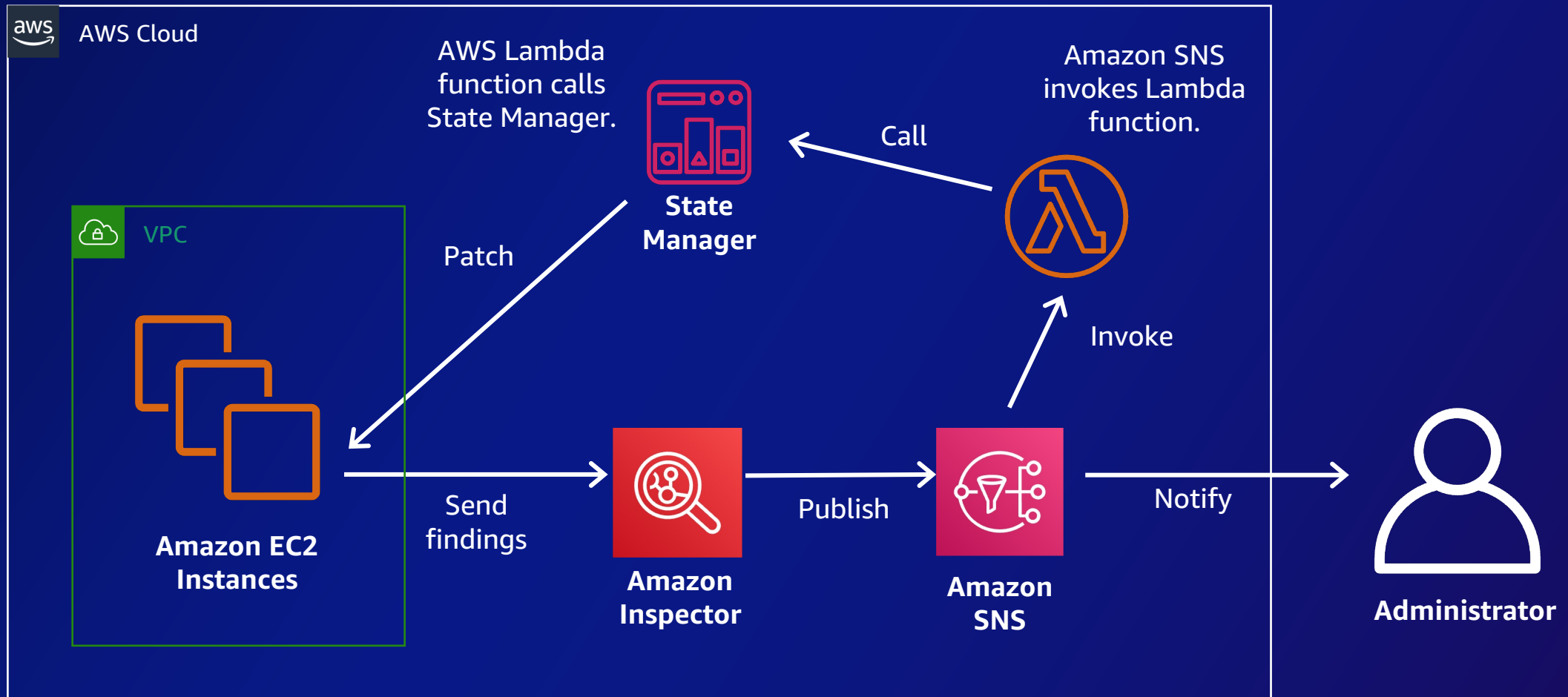


Maintain software compliance by defining and enforcing policies



Collect software configuration and inventory

Use case: patching instances



AWS Security hub



Performs security best practice checks, aggregates alerts, and enables automated remediation.

- Fully managed service
- Consolidates security findings across accounts, services, and third-party products
- Collects and prioritizes findings based on your security and compliance requirements

Security hub integration

Amazon Macie

AWS IAM Access Analyzer

Amazon Inspector

Amazon GuardDuty

AWS Firewall Manager

aws partner network



Summary

Overbridge Default Group (6 Insights)

You have six Insights from 3 providers.

Provider Status

- Alert Logic 3 minutes ago
- Amazon Inspector Unresponsive
- Amazon GuardDuty 2 minutes ago
- Amazon Macie 9 minutes ago
- Symantec 4 minutes ago

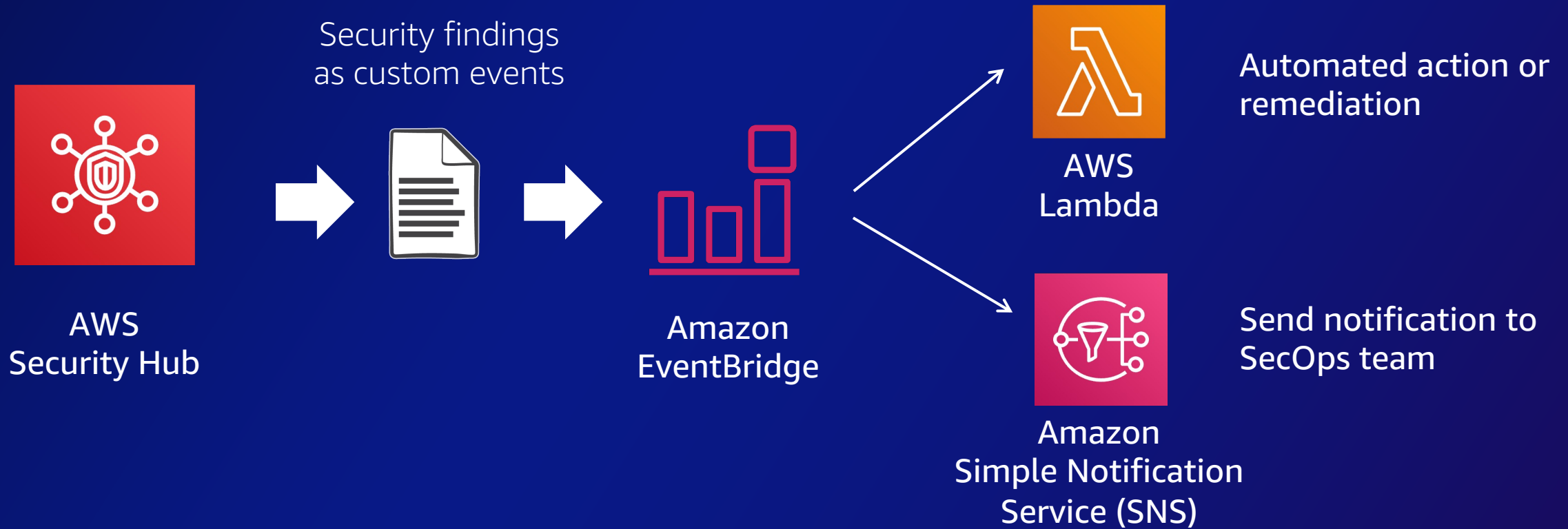
Security News

- Reddit reports user data breach
- AWS unveils security suite
- Security: top-of-mind for everybody

Benchmarks: CIS (78), HIPAA (78), PCI-DSS (78)

Investigate findings and take responsive/remediation actions.

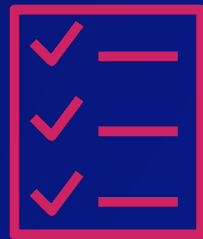
Use case: threat response automation



How can security hub be used to monitor and manage compliance?



Automated
compliance checks



Custom
compliance checks



Aggregated view
of compliance



Remediation
Guidance



Integration with
other AWS services

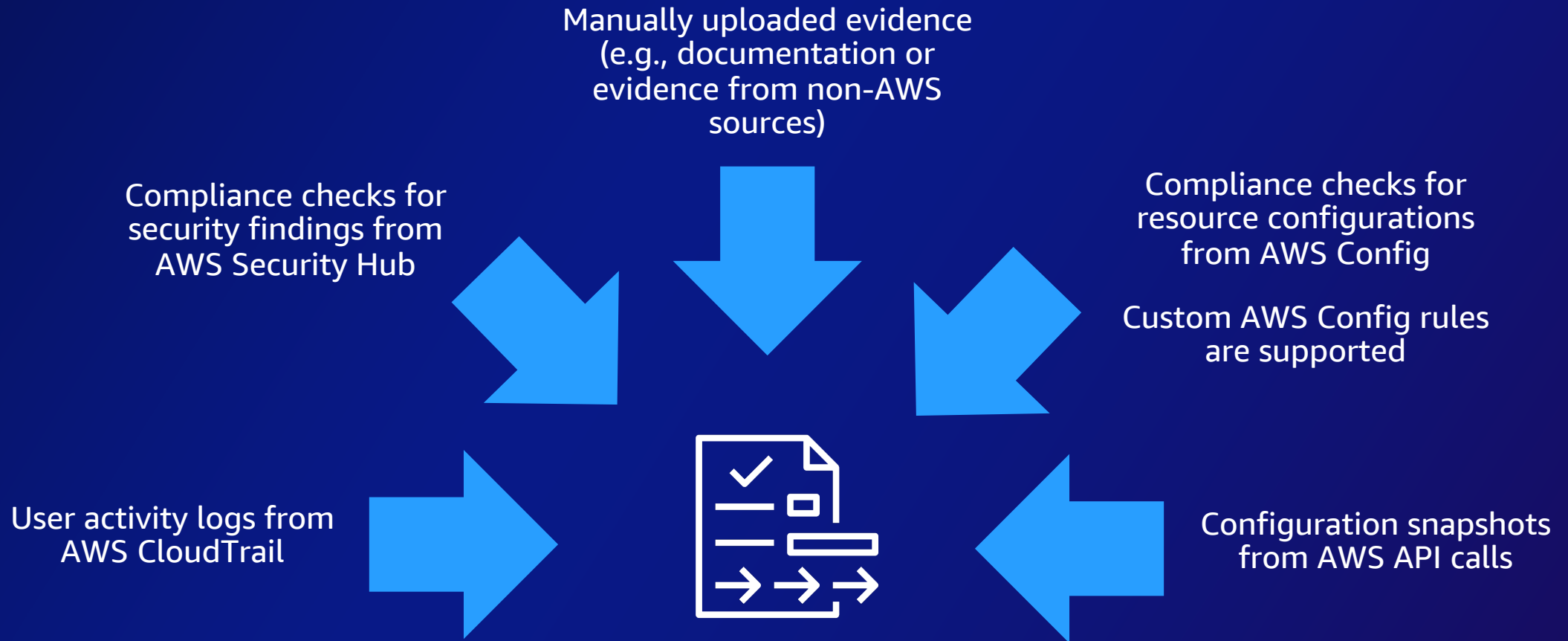
AWS Audit Manager



Continuously audit your AWS usage to simplify risk and compliance assessment

- Maps compliance requirements to AWS usage data
- Uses prebuilt and custom frameworks and automated evidence collection
- You create a framework, define scope of assessment, and generate audit-ready reports

Assurance of risk management – AWS Audit Manager evidence sources



AWS Audit Manager frameworks

INCLUDES PRE-BUILT ASSESSMENT FRAMEWORKS FROM AWS AND AWS PARTNERS

- **NIST 800-53 (Rev. 5)** (Low-Moderate-High) * new
- **CIS** (Center for Internet Security) Foundations Benchmark & CIS Controls v7.1
- **PCI DSS** (Payment Card Industry Data Security Standard)
- **GDPR** (General Data Protection Regulation)
- **GxP** (Good Practice Quality guidelines)
- **GLBA** (Financial Service Modernization Act of 1999)
- **HIPAA** (Health Insurance Portability and Accountability Act)
- **FedRAMP** moderate (Federal Risk and Authorization Management Program)
- **SOC 2** (Service and Organization Controls)
- **ISO 27001** (International Standard for Information Security Controls)
- AWS operational best practices (for Amazon S3, IAM, and Amazon DynamoDB)
- AWS Control Tower framework
- Software licensing

AWS Audit Manager supports custom-defined controls and compliance frameworks

Multi-account strategy for automating compliance



Why should I use multiple accounts?

Group resources for categorization and discovery

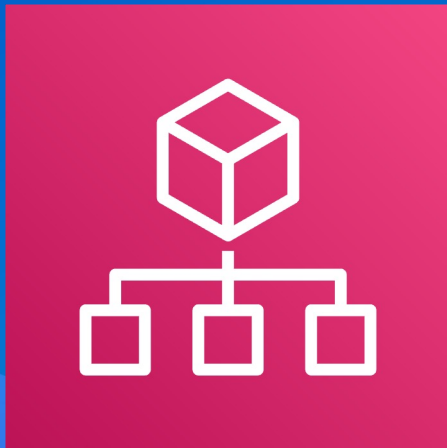
Improve your security posture with a logical boundary



Limit blast radius in case of unauthorized access

More easily manage user access to different environments

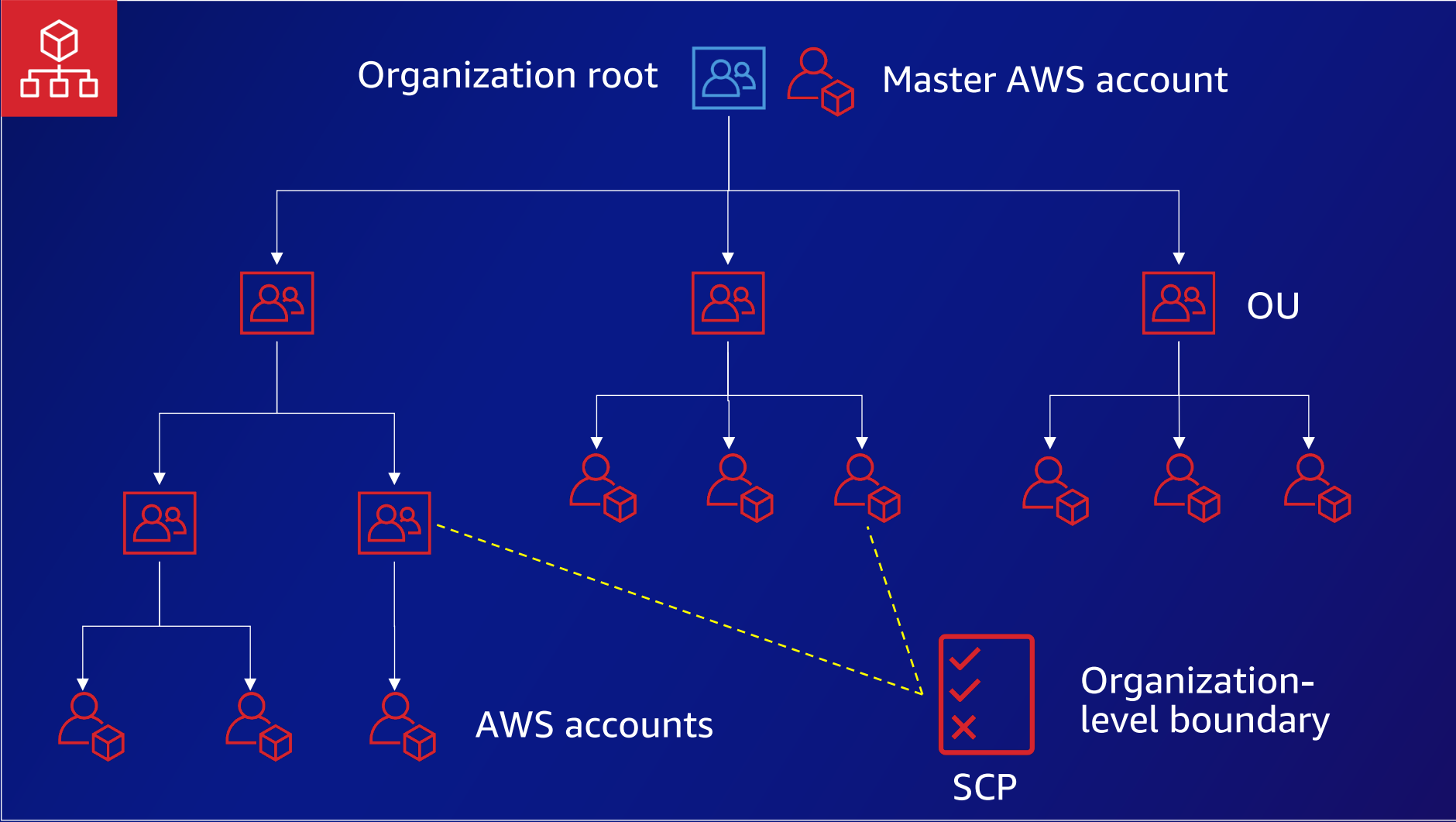
AWS Organizations



Offers policy-based, central management for multiple AWS accounts

- Organize AWS accounts into logical groups called organization units (OUs)
- Manage policies across accounts
- Automate creation of new accounts through APIs
- Consolidated Billing and All Feature modes

Architecture

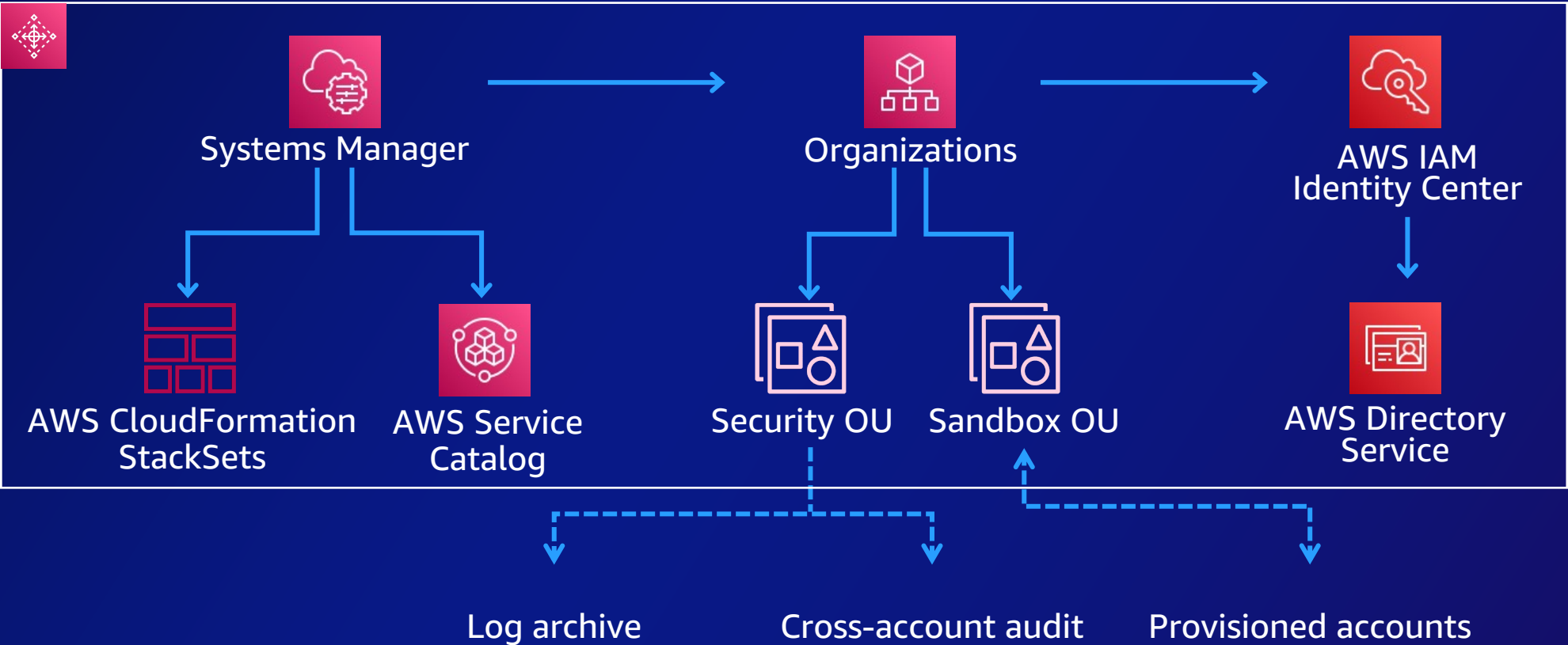


AWS Control Tower



- Automates the setup of multiple accounts based on best practices in a landing zone
- Applies pre-packaged guardrails that provide ongoing governance
- Provides an integrated dashboard to view your landing zone, reports, and guardrails applied to your environment

Control Tower multi-account architecture



What is configured in a landing zone?

- A multi-account environment
- Identity management and federated access
- Audit logging for each account
- AWS Config is enabled by default

- Network settings
- Notifications
- Intelligent threat detection

Guardrail examples

Rule	Type	Behavior
Enable Encryption at Rest for Log Archive	Mandatory	Preventive
Disallow Configuration Changes to CloudTrail	Mandatory	Preventive
Integrate CloudTrail Events with CloudWatch Logs	Mandatory	Preventive
Disallow Public Write Access to Log Archive	Mandatory	Detective
Disallow Internet Connection Through RDP	Strongly Recommended	Detective
Disallow Creation of Access Keys for the Root User	Strongly Recommended	Preventive
Disallow Access to IAM Users Without MFA	Elective	Detective

Dashboard for oversight

The screenshot displays the AWS Control Tower Dashboard. At the top, the AWS logo is on the left, and navigation links for 'Services', 'Resource Groups', 'Oregon', and 'Support' are on the right. The main content area is divided into several sections:

- Recommended actions:** A section for actions that are recommended for the environment.
- Environment summary:** A summary card showing 3 Organizational units and 34 Accounts.
- Guardrail summary:** A summary card showing 28 Preventive guardrails and 12 Detective guardrails.
- Noncompliant resources:** A table listing resources that do not comply with guardrails.
- Organizational units:** A table listing organizational units and their compliance status.
- Accounts:** A table listing accounts and their compliance status.

Noncompliant resources table:

Resource ID	Resource type	Service	Region	Account name	OU	Guardrail
vol-842jhdksj83821234	Volume	EC2	us-west-2	db-uswest-1-gamma	Custom	Enable encryption for EBS volumes at
vol-05flia830kd209897	Volume	EC2	us-east-1	testing-beta-1	Project 1	Enable encryption for EBS volumes at
sg-031234b83bac98765	Security Group	EC2	eu-west-1	ops-test-4	Project 1	Disallow internet connection through

Organizational units table:

Name	Parent OU	Compliance
Core	Root	Compliant
Project 1	Root	Noncompliant
Custom	Root	Noncompliant

Accounts table:

Account name	Account email	Organizational unit	Owner	Compliance status
--------------	---------------	---------------------	-------	-------------------

Summary

1. AWS Services used to automate compliance



AWS CloudFormation



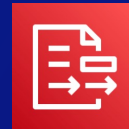
AWS Config



AWS Systems Manager



AWS Security hub



AWS Audit Manager

2. Multi-account strategy for automating compliance



AWS Organizations



AWS Control Tower

Next step: Explore security and compliance resources

Reach out to your Account Manager and/or SA

We are here for you

Training and Certification

skillbuilder.aws



Security & Compliance documentation

Check the dedicated security & compliance chapters

<https://docs.aws.amazon.com/security/>
<https://aws.amazon.com/compliance/>

Thank you!

Laura Verghote

Solutions Architect

 [linkedin.com/in/laura-verghote/](https://www.linkedin.com/in/laura-verghote/)

Cristina Rios Iribarren

Solutions Architect

 [linkedin.com/in/cristina-rios-iribarren/](https://www.linkedin.com/in/cristina-rios-iribarren/)



Please complete the session survey in the mobile app