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

STP306-R

Evolving your security capabilities through key growth stages

Jay Michael

Principal Solutions Architect – Startups
AWS

Faisal Farooq

Senior Solutions Architect – Startups
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- Startup Security – Challenges
- Startup Stages of Growth
- For Each Stage:
    - Characteristics
    - Security Considerations
    - Implementation Guidance

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Disclaimer

Our goal is to raise awareness of different techniques you can use to secure your operation on AWS and how they help at various stages of growth.

We are not recommending that you forego implementing any of these techniques from the sole basis that your business is not at that particular stage of growth.

Every business is unique and needs to make its own decisions about what techniques to ultimately use and when they make the most sense to implement.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Holistic Security Resources

The Well-Architected Security Pillar



https://go.aws/3OsDqhe

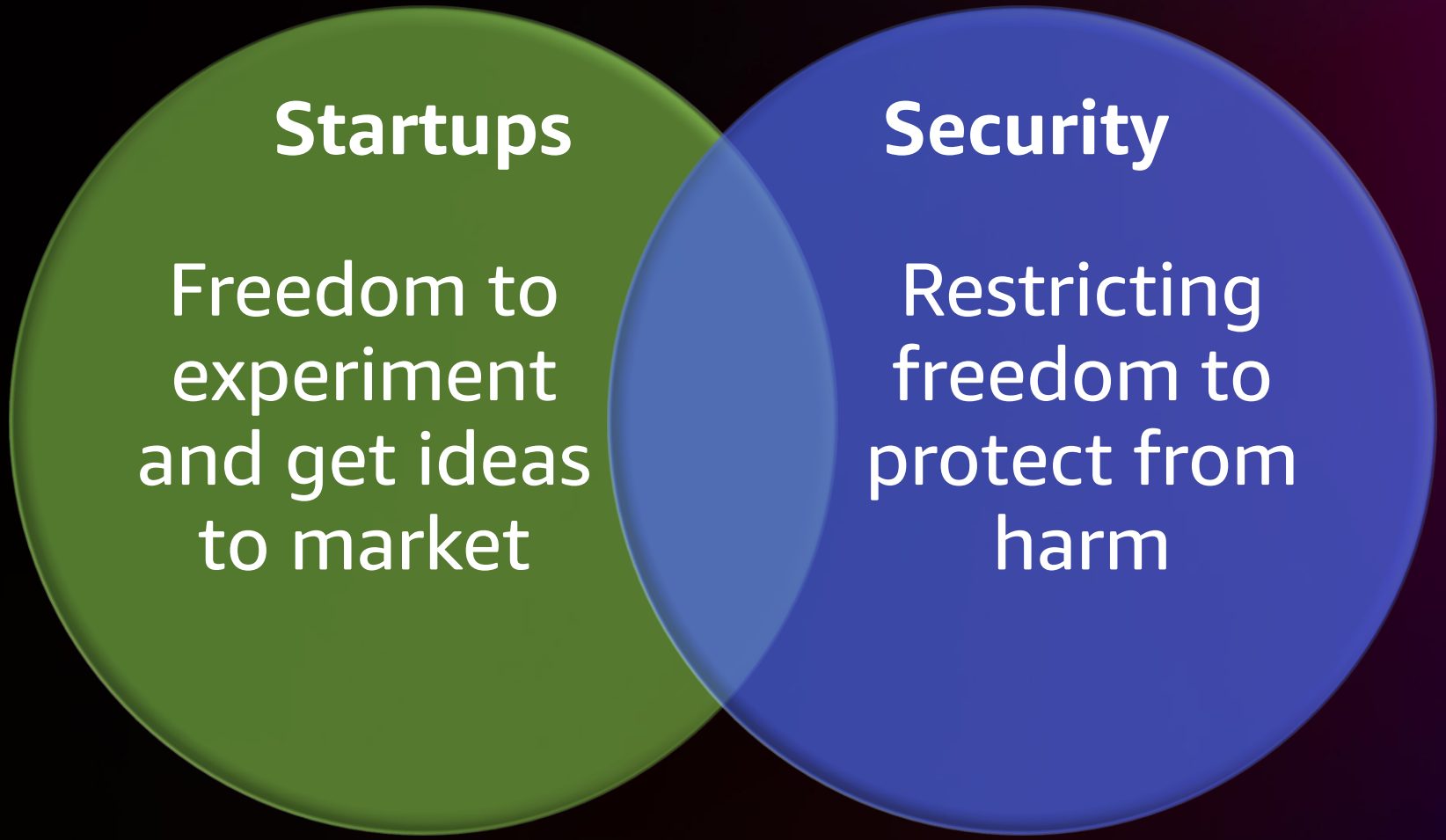
AWS Security Reference Architecture



https://go.aws/3tTlcMI

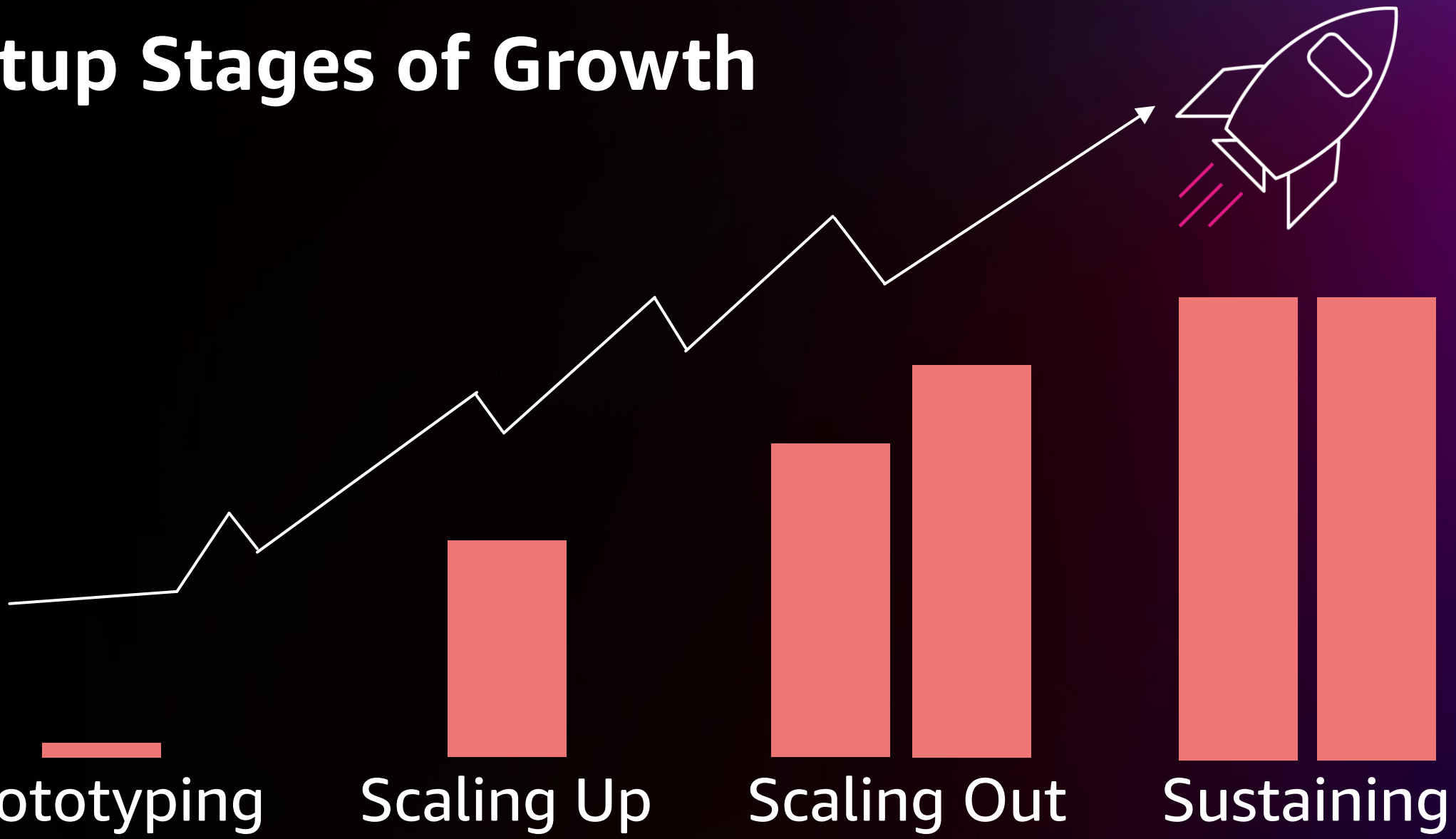
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Startup Security Challenges



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Startup Stages of Growth



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

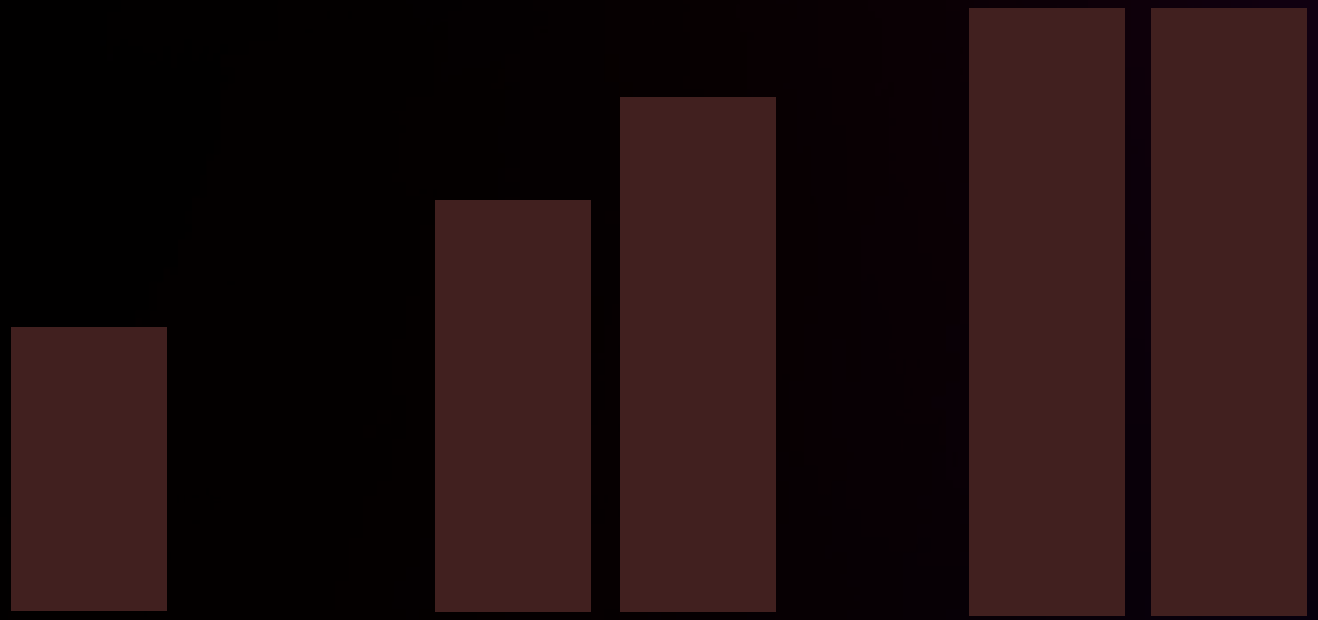
Stage 1 - Prototyping

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Prototyping - Characteristics

- Pre-Seed/Angel
- Founding Team
- Building MVP
- No, or few, customers

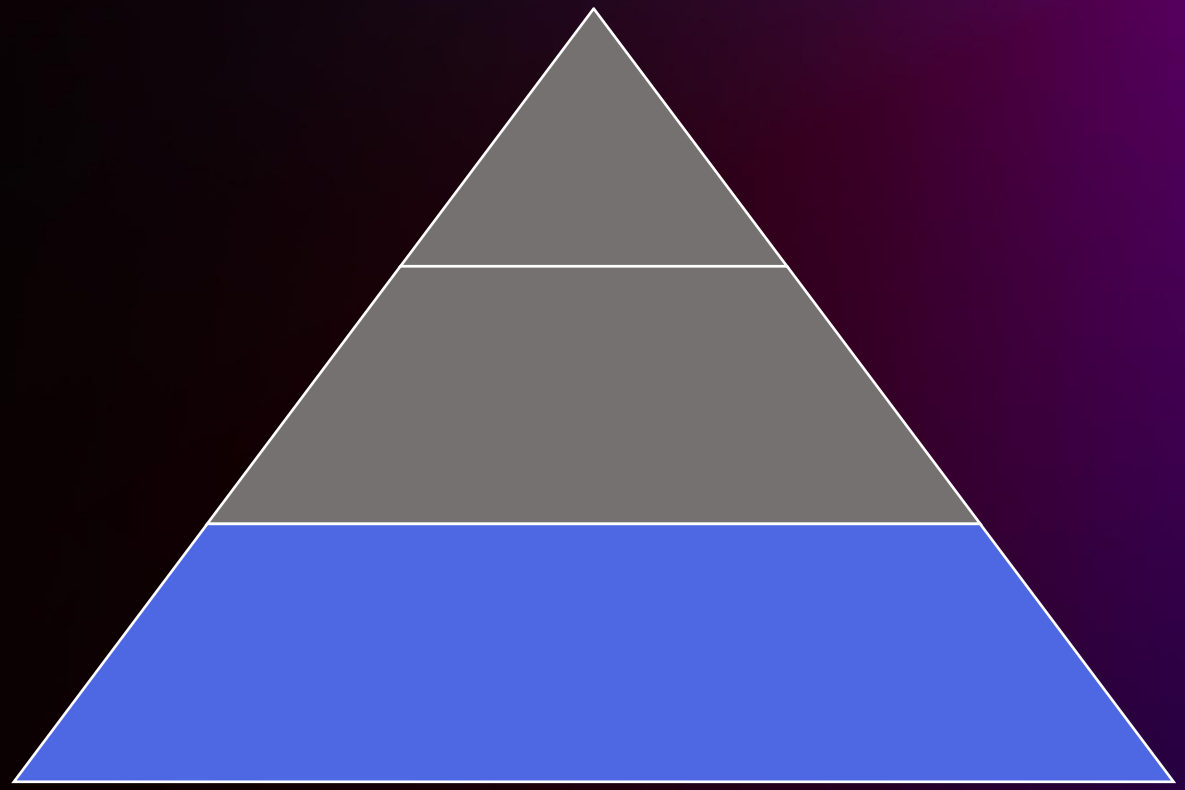




aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Prototyping - Posture

- Organization & Identity
  - Properly Configured Account
  - Per-User Access
- Security Operations
  - Audit Logging
  - Foundational Threat Detection



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Guide: AWS Startup Security Baseline

- Getting started on the right track
- Starting with a secure foundation
- Specifically written for early-stage startups



https://go.aws/3GdR06e

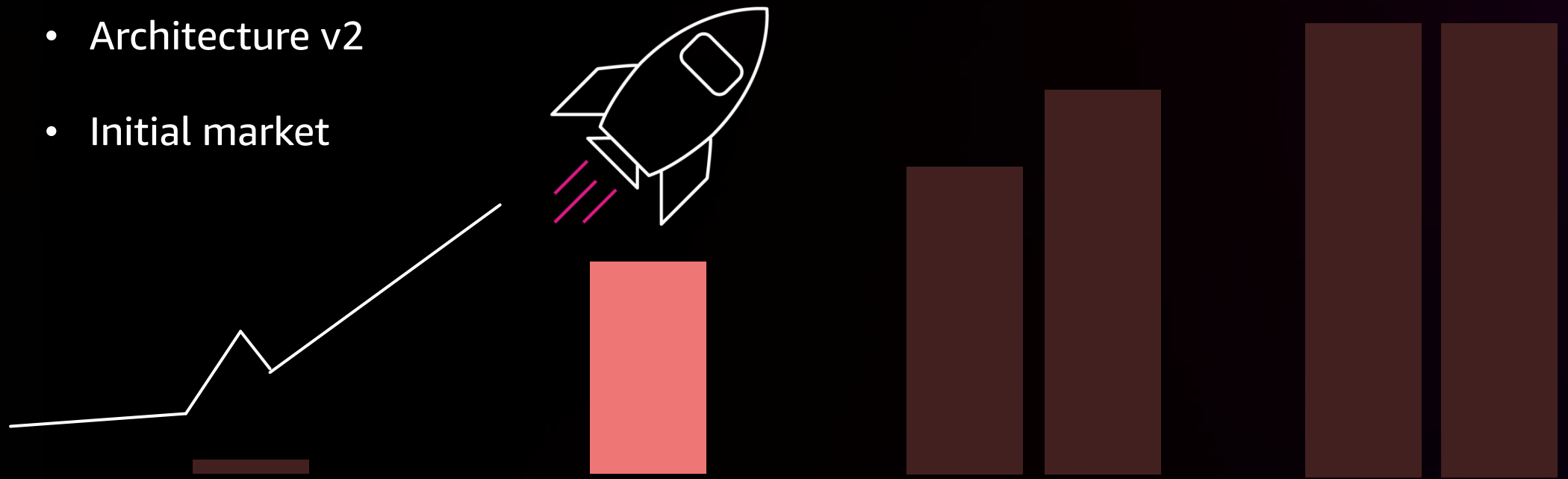
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Stage 2 – Scaling Up

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up - Characteristics

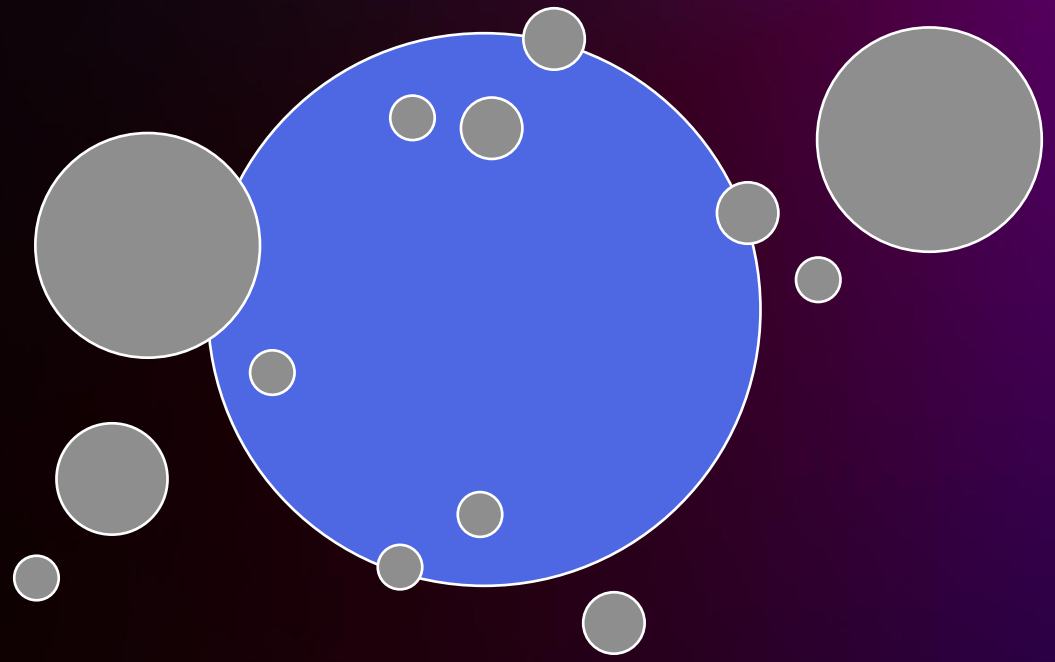
- Seed/Series A
- Team of generalists
- Architecture v2
- Initial market



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Posture

- Organization & Identity
  - Environment Isolation
  - Centralized Identity Management
  - Periodic Access Analysis
  - Automatic Credential Rotation
- Security Operations
  - Centralized Logging
  - Foundational Security Reporting
  - Managed Security Monitoring
  - Compliance Preparation

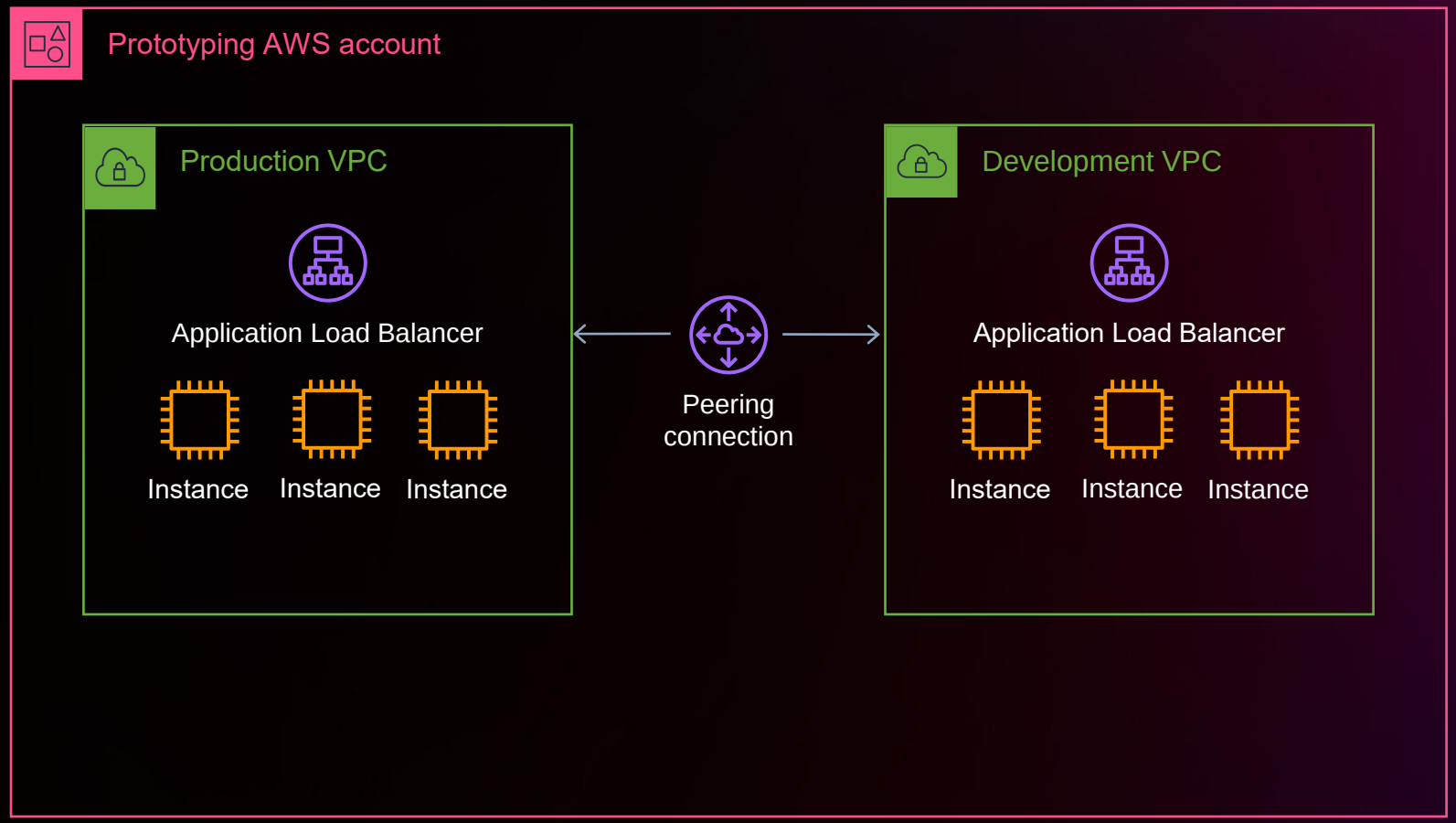


Centralization

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

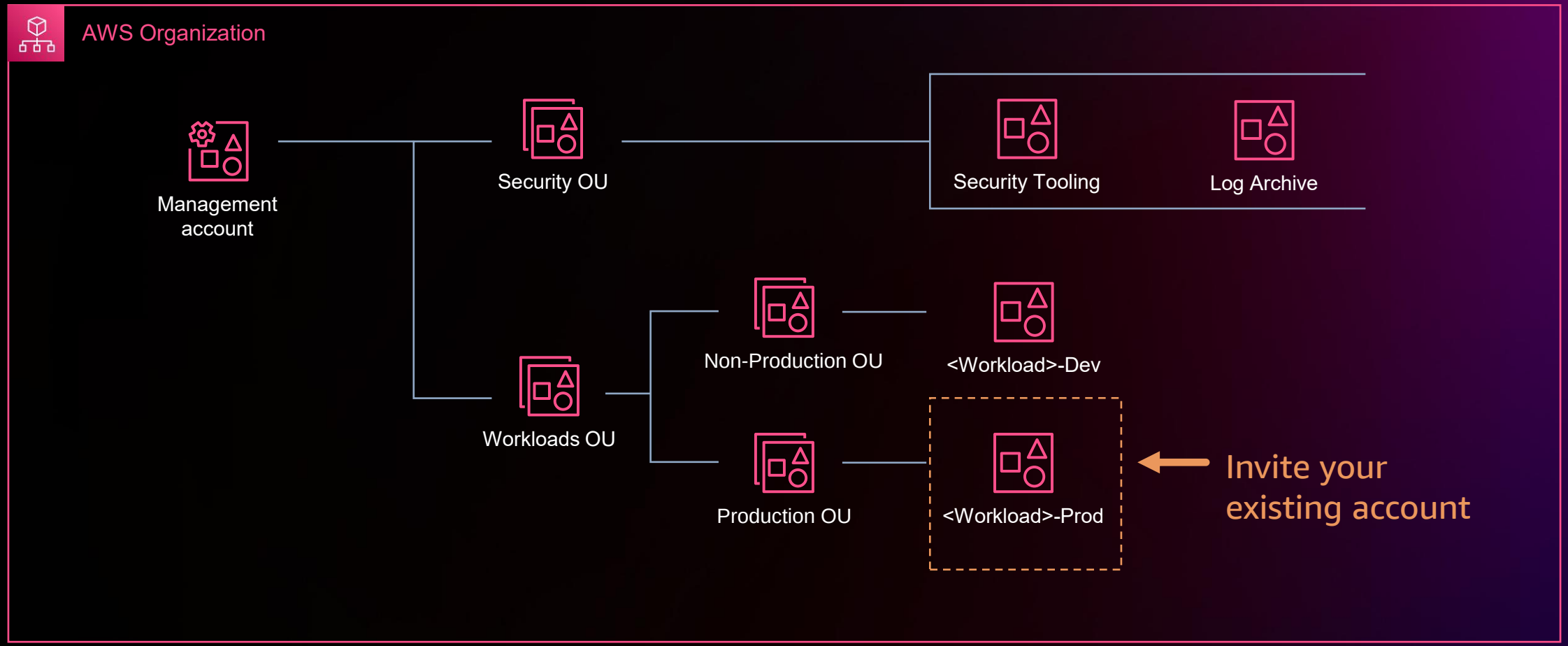
Scaling Up – Environment Isolation



Prototyping – Single AWS Account

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

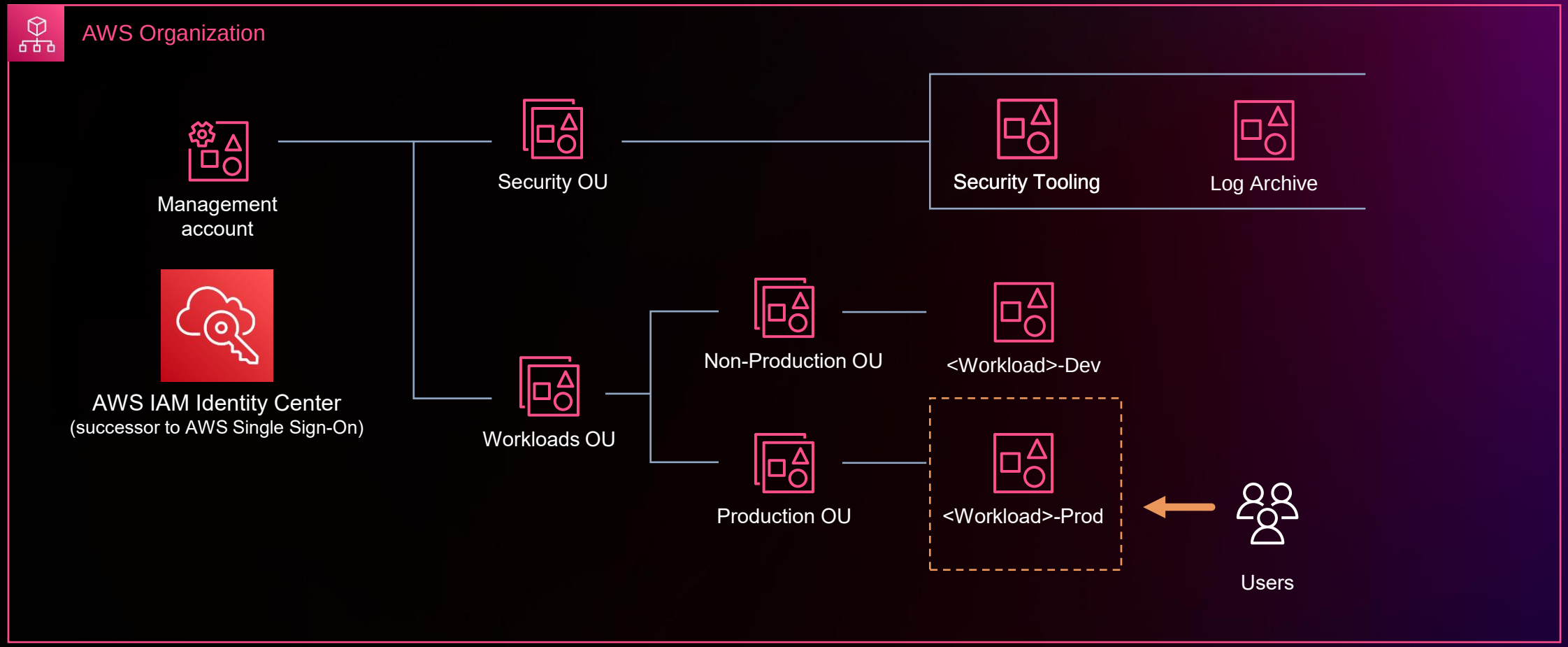
Scaling Up – Environment Isolation



Scaling up – Organization

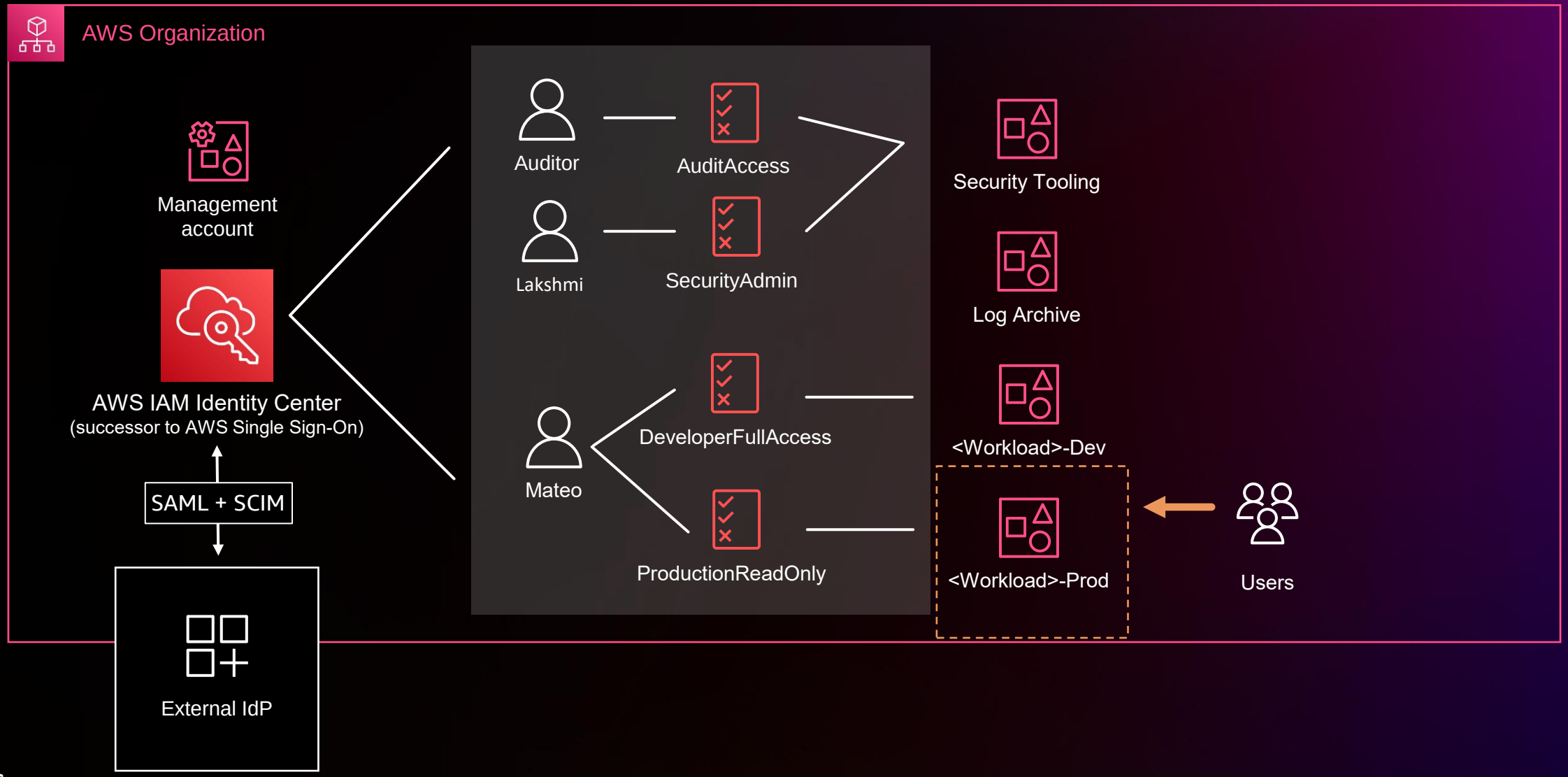
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Identity Management



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Identity Management



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Guide: Transitioning to Multiple Accounts

- Set up an AWS Organization following best practices
  - Consider using AWS Control Tower!
- Configure centralized identity management and networking
- Migrate resources from your existing account



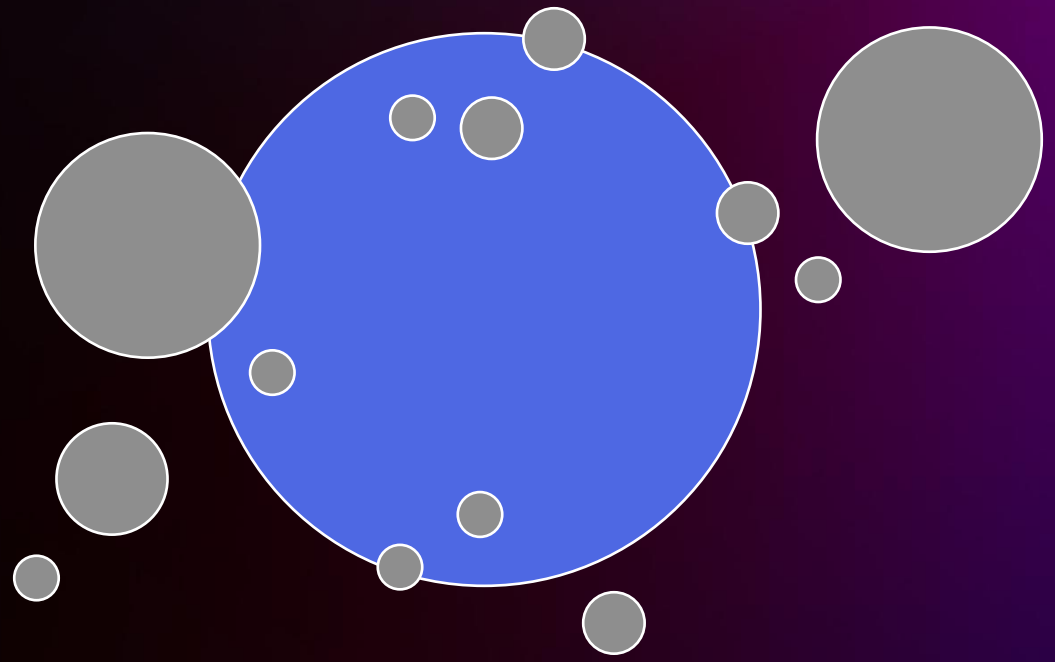
https://go.aws/3TCHMUc

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Posture

- Organization & Identity
  - ☑ Environment Isolation
  - ☑ Centralized Identity Management
  - → Periodic Access Analysis
  - → Automatic Credential Rotation
- Security Operations
  - Centralized Logging
  - Foundational Security Reporting
  - Managed Security Monitoring
  - Compliance Preparation



Centralization

aws

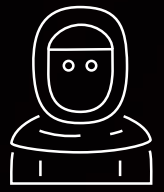
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Access Analysis



Developers

Create policies for the workloads they are building



DevOps

Catch policy issues and errors before they get deployed



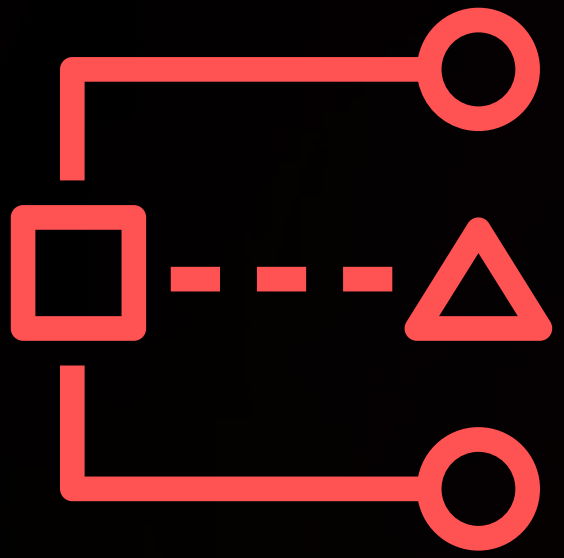
Security Lead

Ensure misconfigured policies are caught and fixed quickly

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Access Analysis



AWS Identity and Access Management Access Analyzer

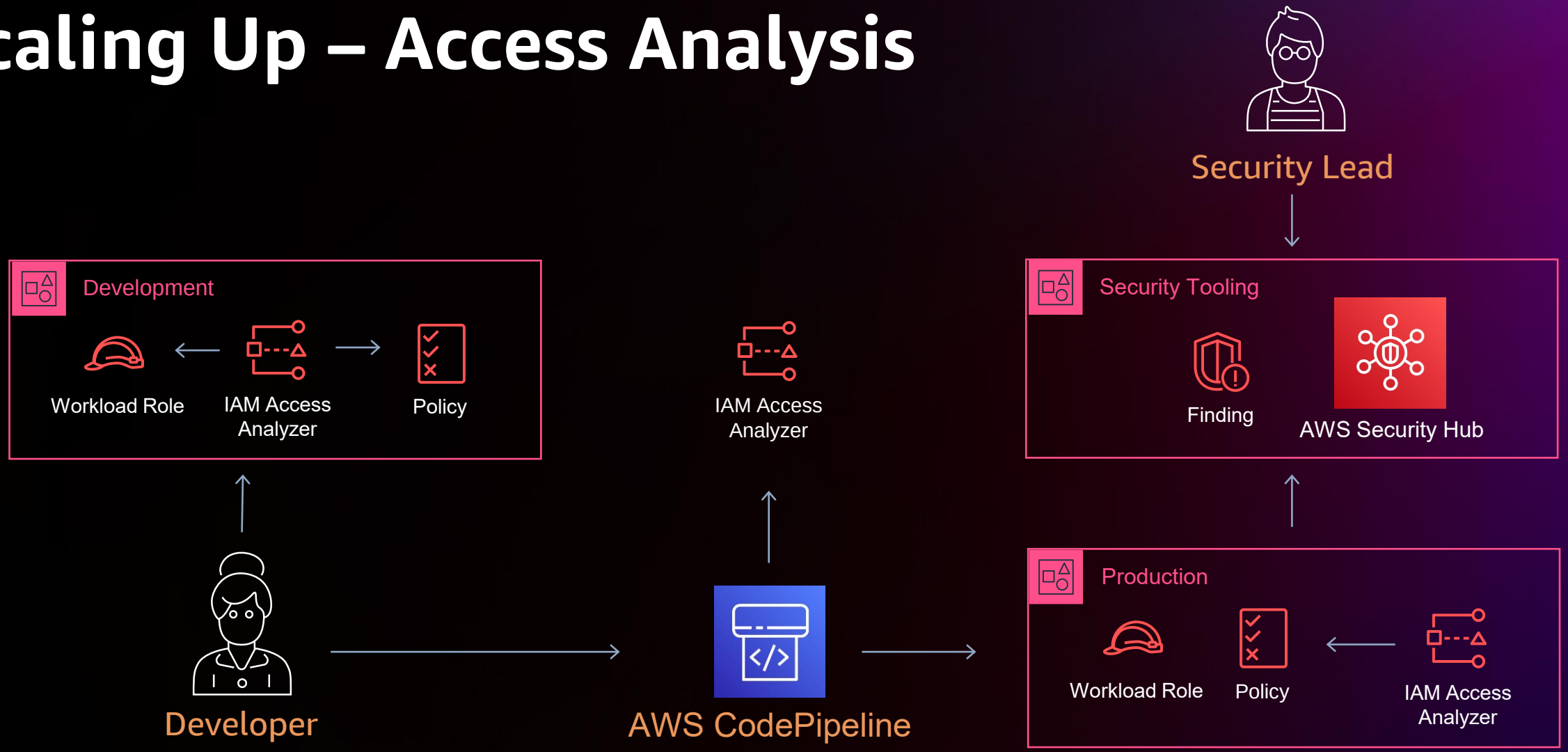
Create policies based on observed access with policy generation

Fix security issues and errors, implement suggestions with policy validation

Find misconfigured access with automated access analysis

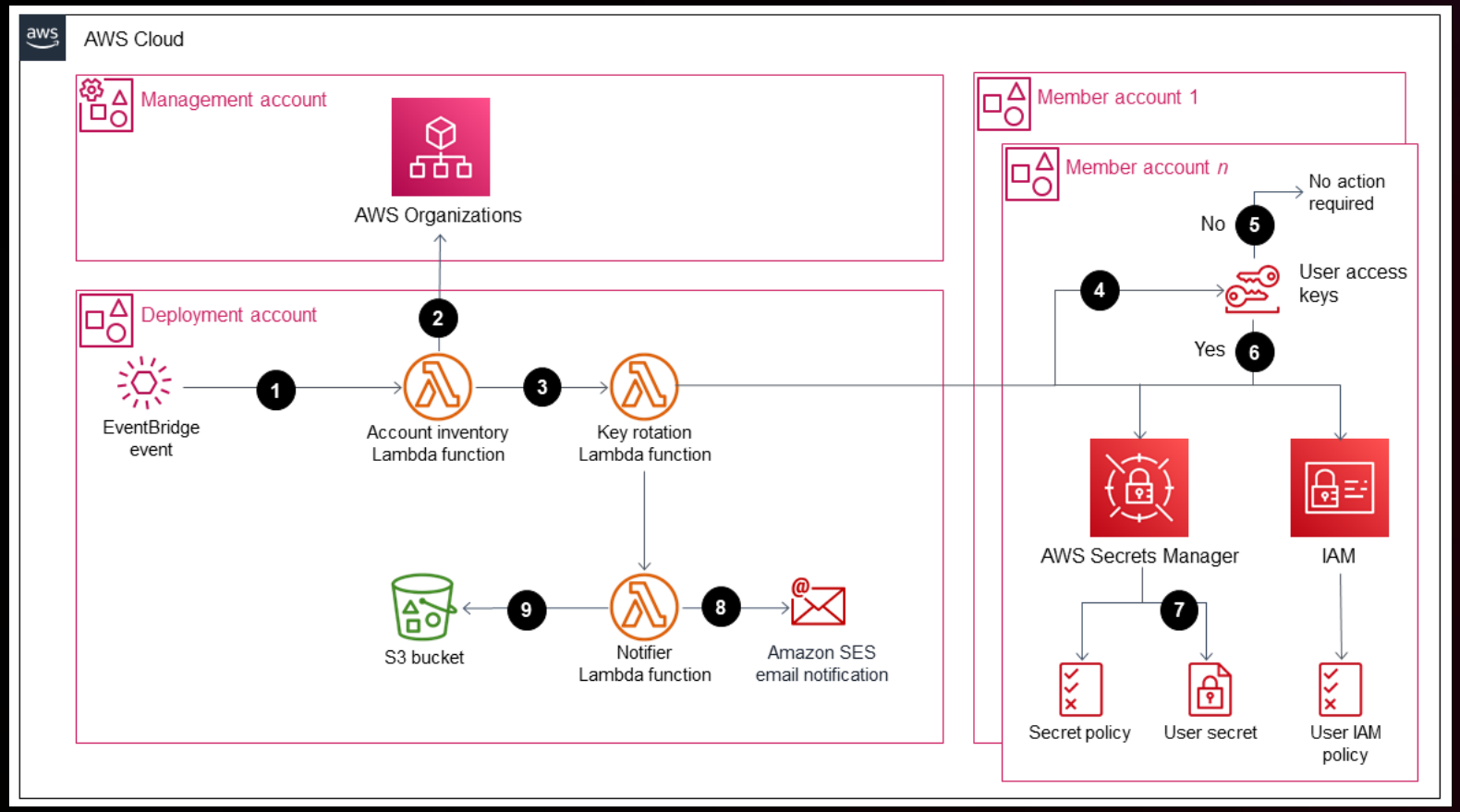
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Access Analysis



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Credential Rotation

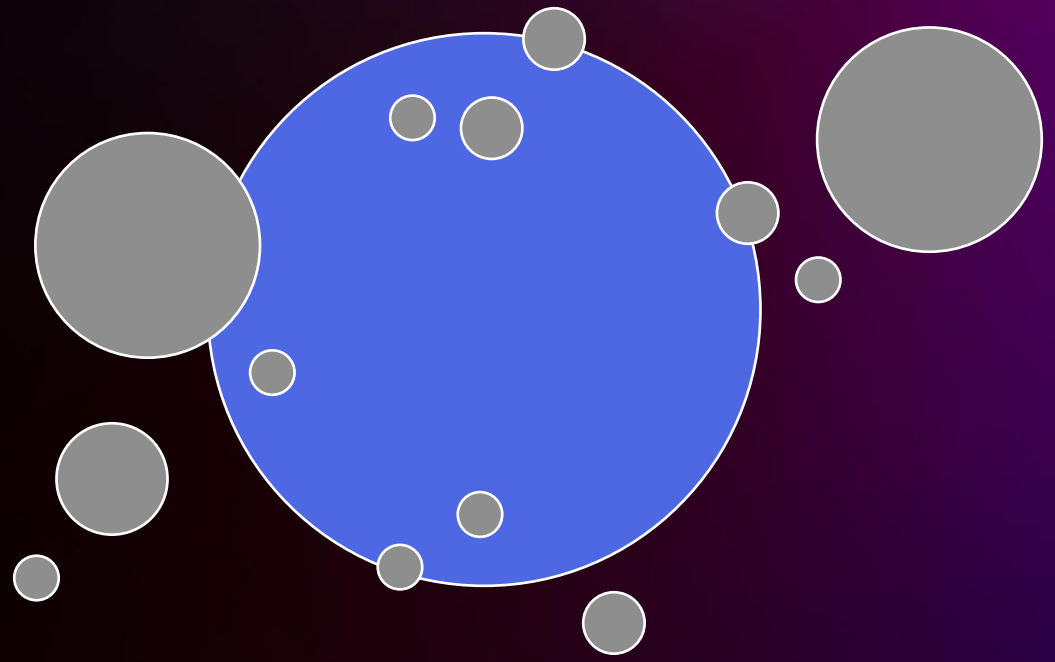


https://go.aws/3UTNcem

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Posture

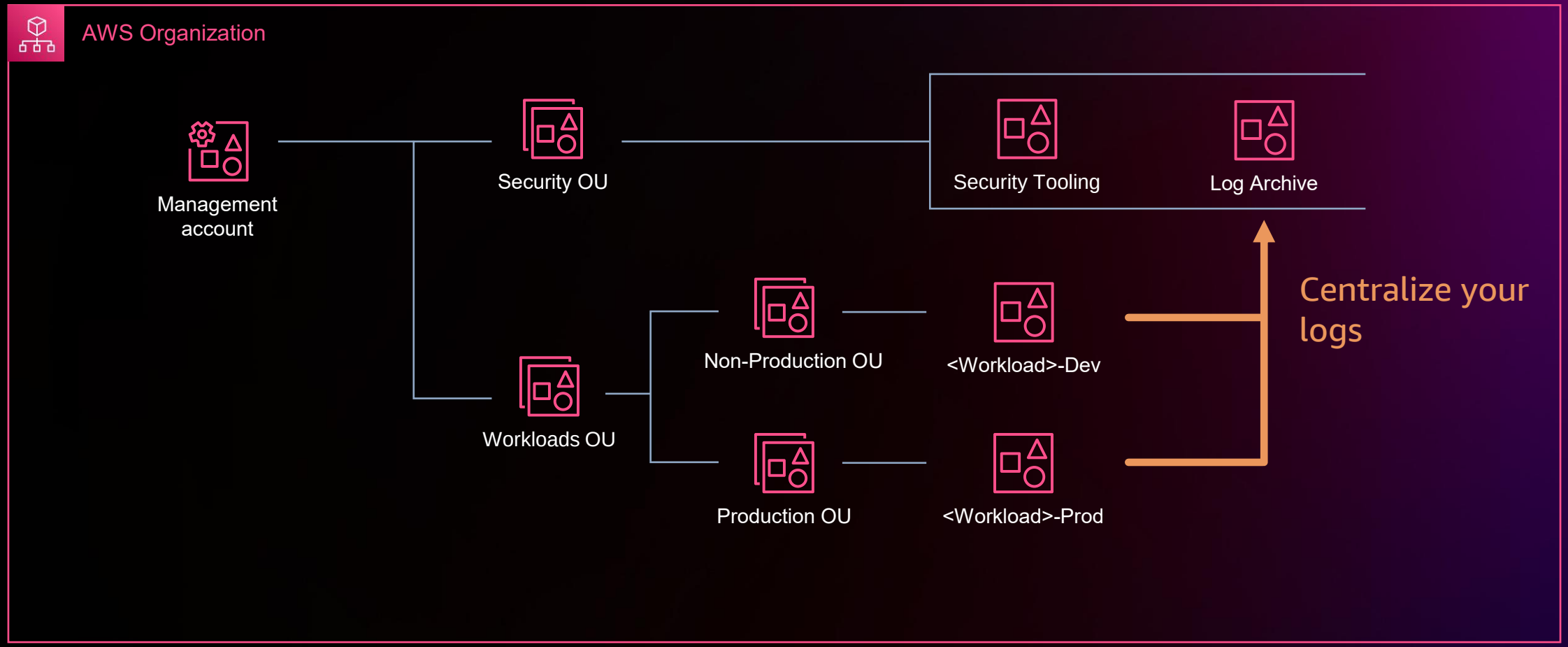
- Organization & Identity
  - ☑ Environment Isolation
  - ☑ Centralized Identity Management
  - ☑ Periodic Access Analysis
  - ☑ Automatic Credential Rotation
- Security Operations
  - ⊡ Centralized Logging
  - ⊡ Foundational Security Reporting
  - Managed Security Monitoring
  - Compliance Preparation



Centralization

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

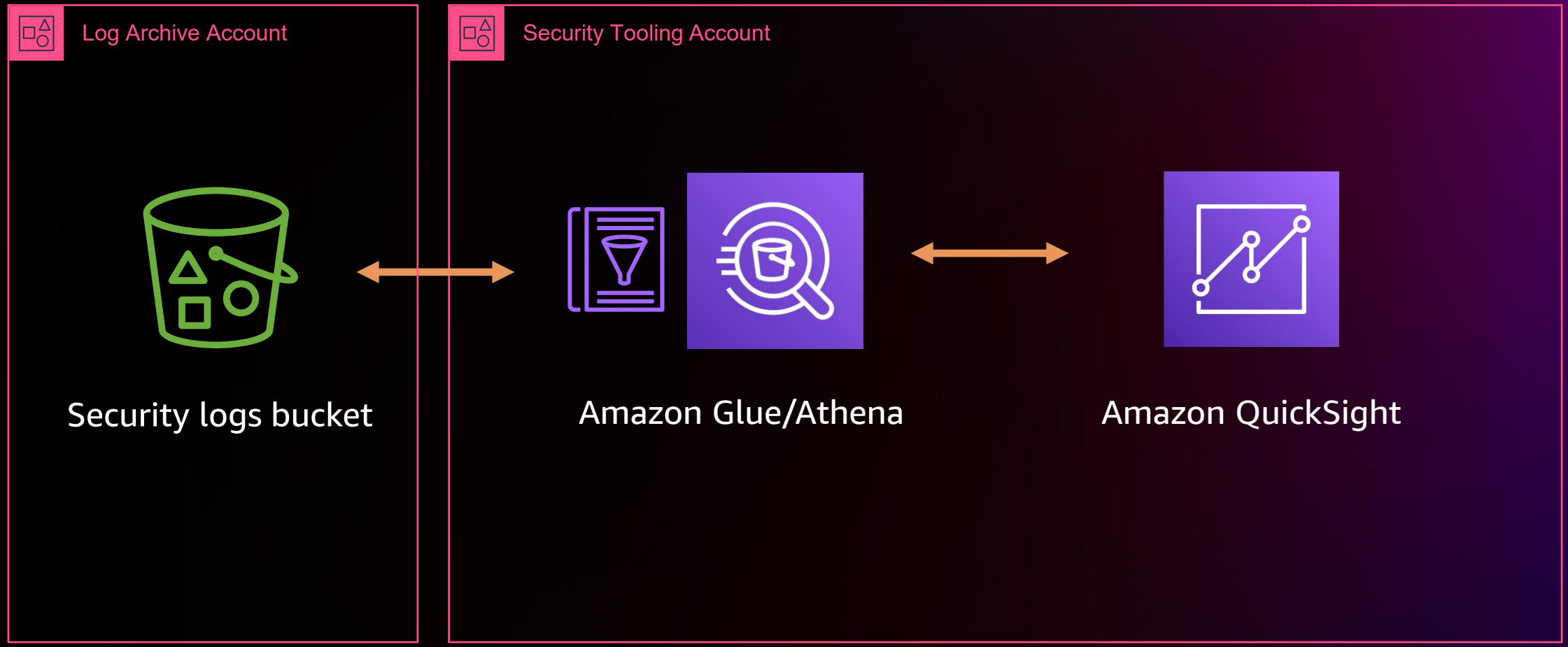
Scaling Up – Centralized Logging



Scaling up – Organization

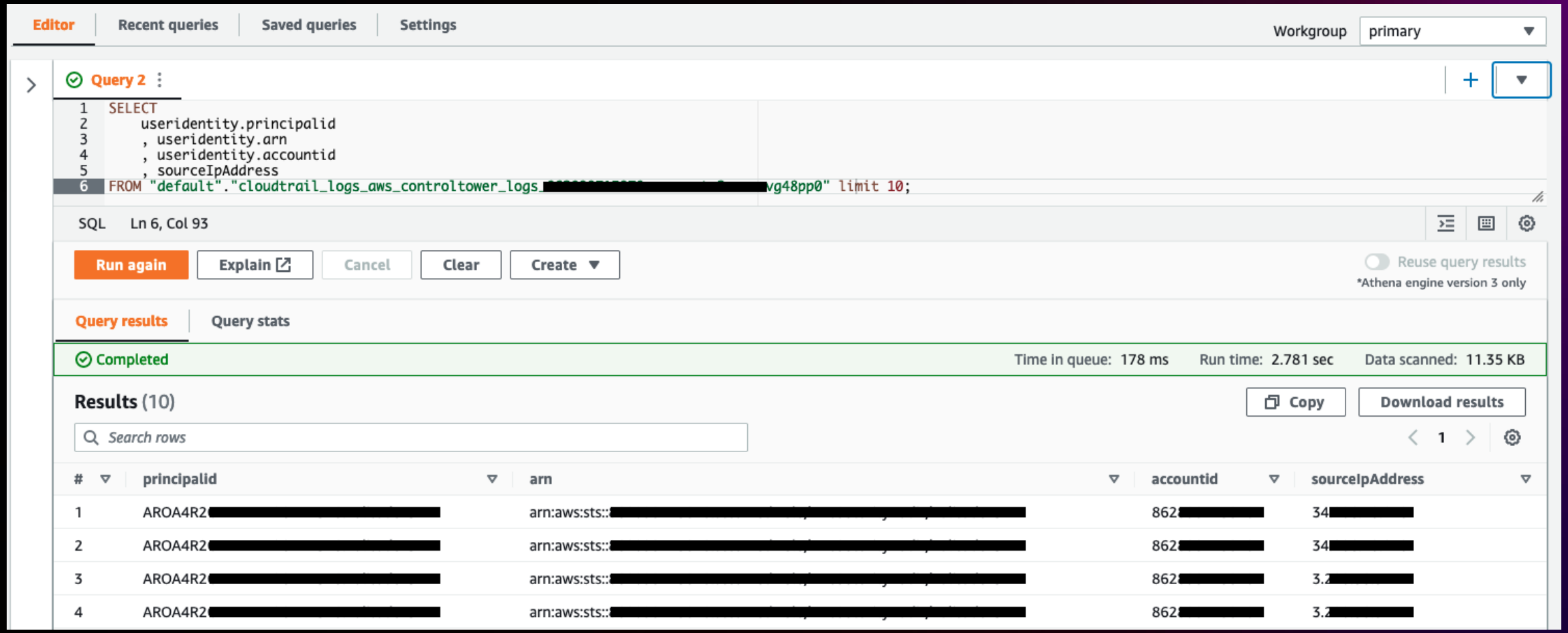
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Security Reporting



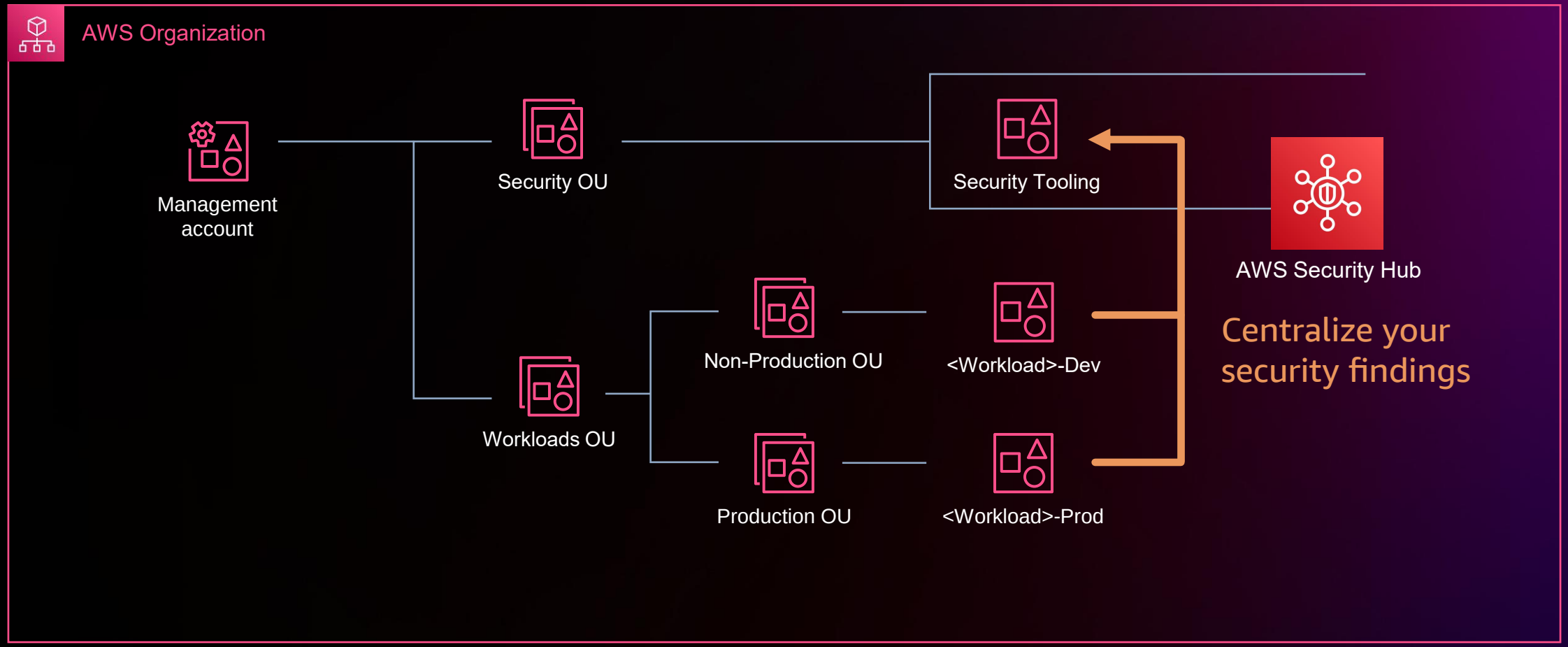
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Security Reporting



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Security Reporting



Scaling up – Organization

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Security Reporting



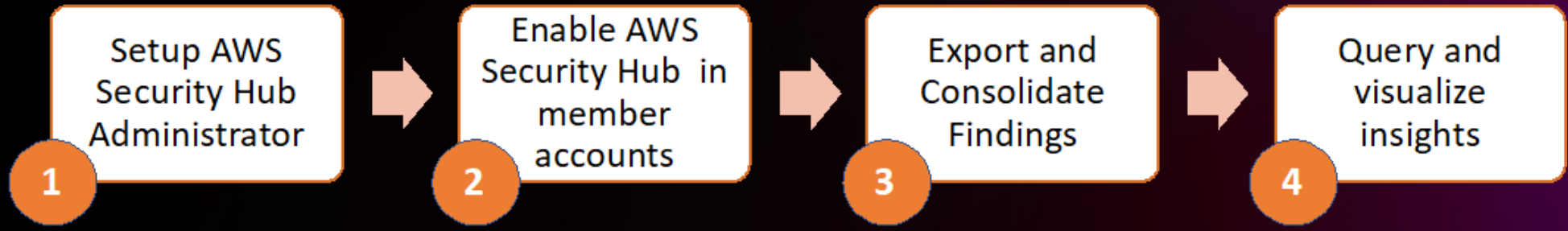
AWS Security Hub

Enabling Security Hub

1. In the Management account, navigate to Security Hub
2. Enter Security Tooling account ID under Delegation
3. Navigate to Security Hub in Security Tooling account
4. In Settings, enable auto-enrolling for your Org

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

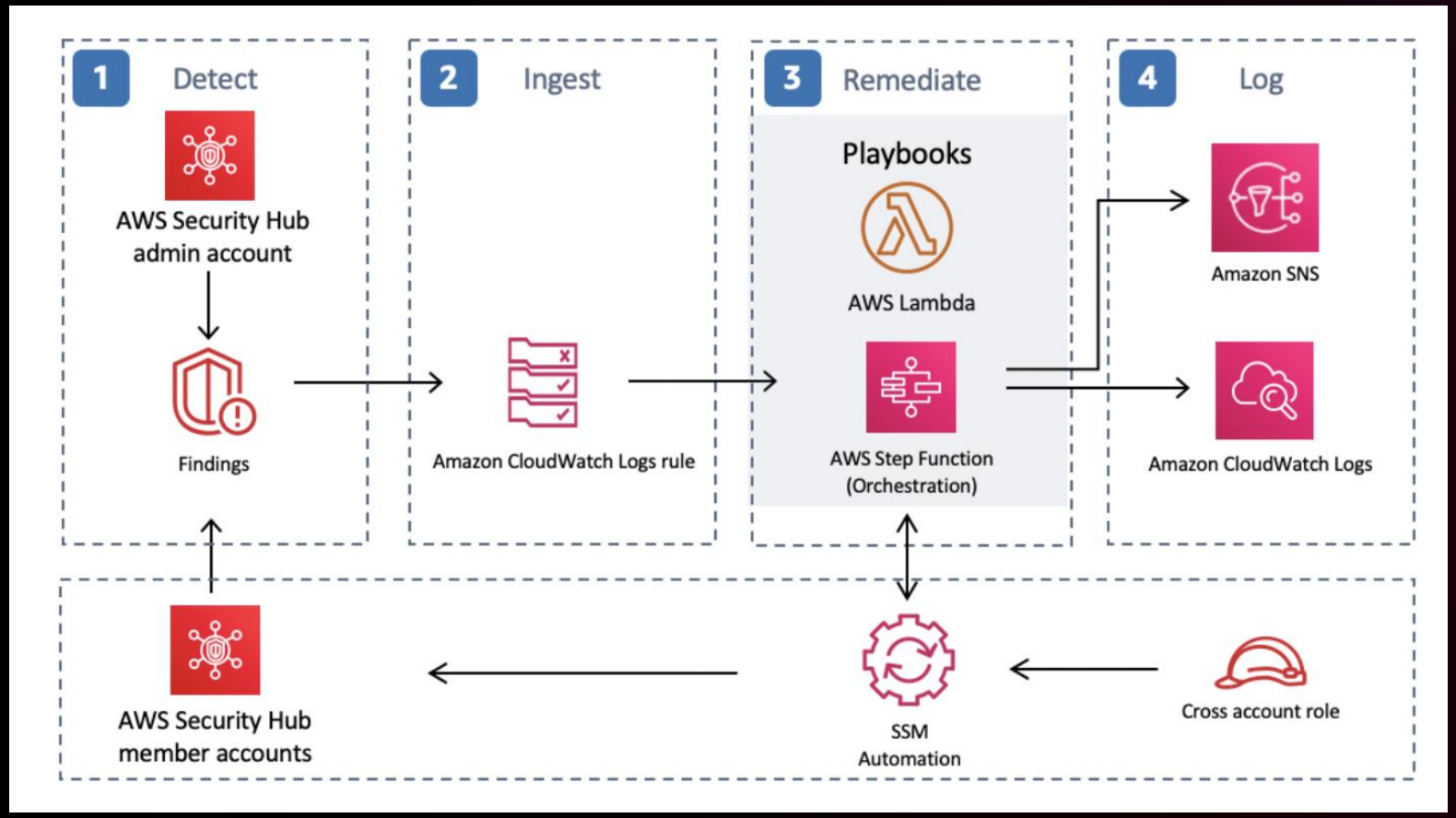
Guide: Visualize Security Hub Findings



https://go.aws/3UTumny

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Code: Automated Security Response

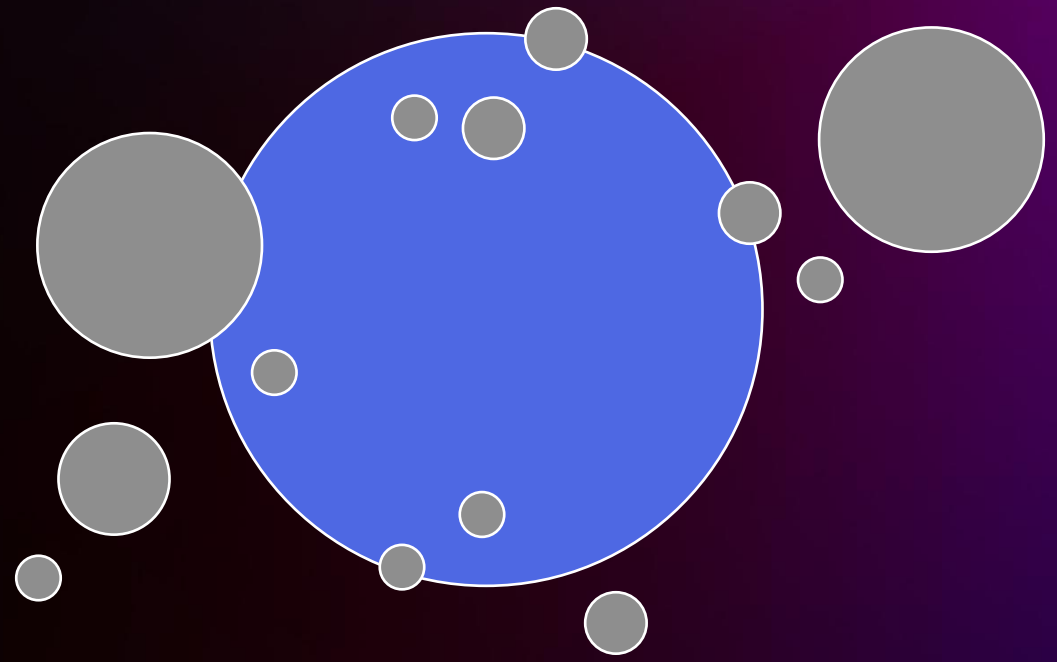


https://go.aws/3Ezdmh4

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Posture

- Organization & Identity
  - ☑ Environment Isolation
  - ☑ Centralized Identity Management
  - ☑ Periodic Access Analysis
  - ☑ Automatic Credential Rotation
- Security Operations
  - ☑ Centralized Logging
  - ☑ Foundational Security Reporting
  - → Managed Security Monitoring
  - → Compliance Preparation

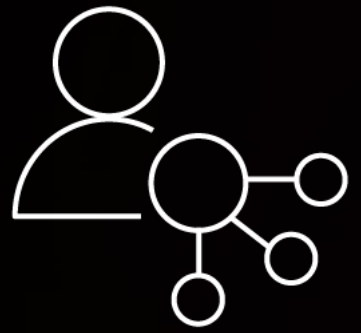


Centralization

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Managed Security Monitoring



24/7 Incident Response



Vulnerability Management



DDoS Response

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Managed Security Monitoring

AWS Security Competency Certified Partners

https://go.aws/3g8idwp

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Compliance Preparation







Identify compliance targets & start formulating controls

Identify a compliance partner

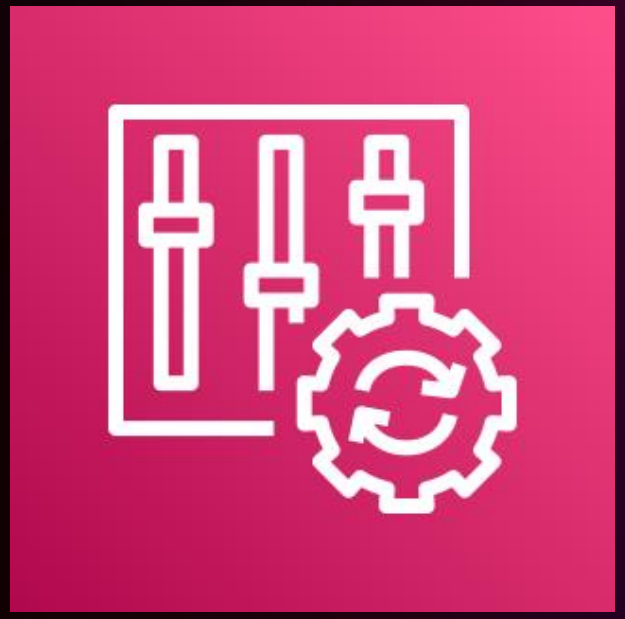
AWS services that can help with compliance

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Compliance Preparation



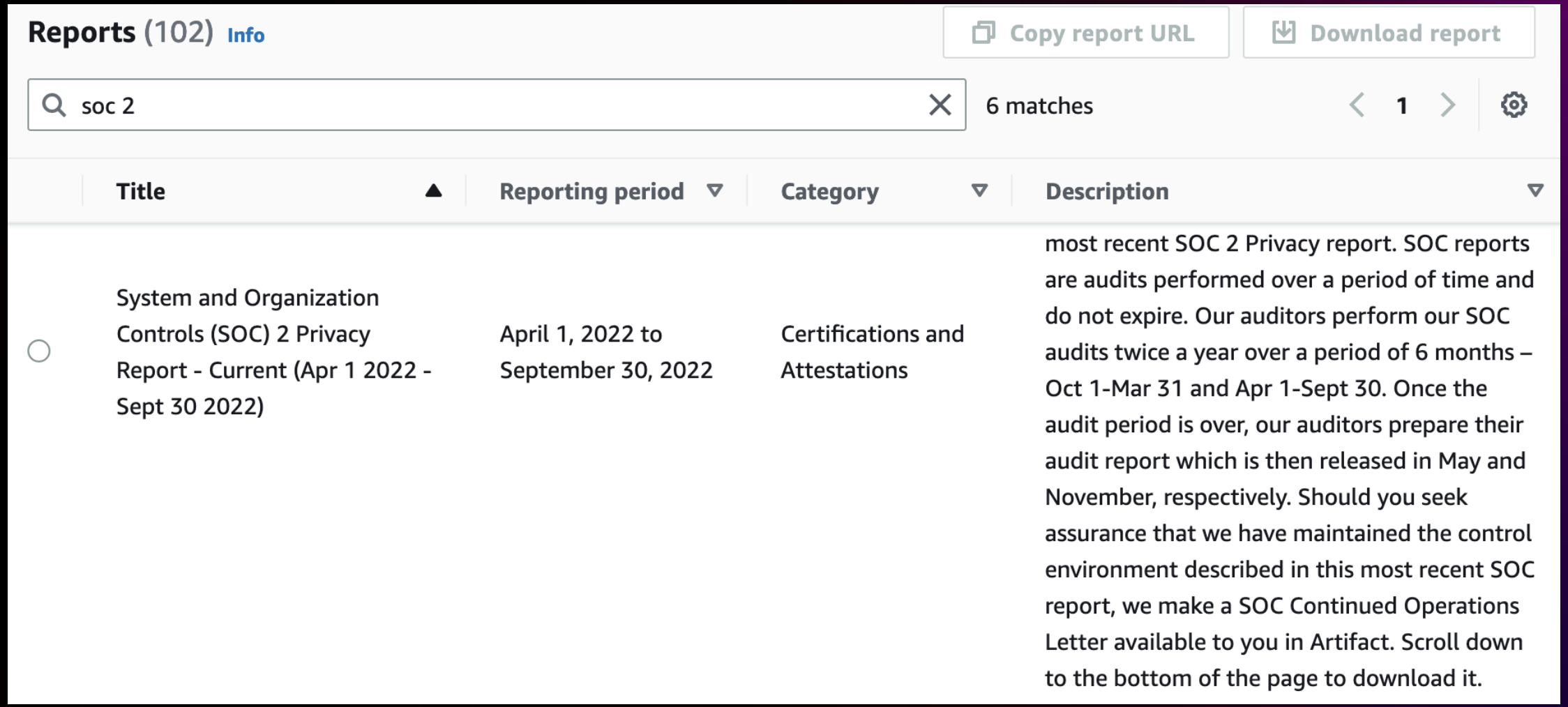
AWS Artifact



AWS Config

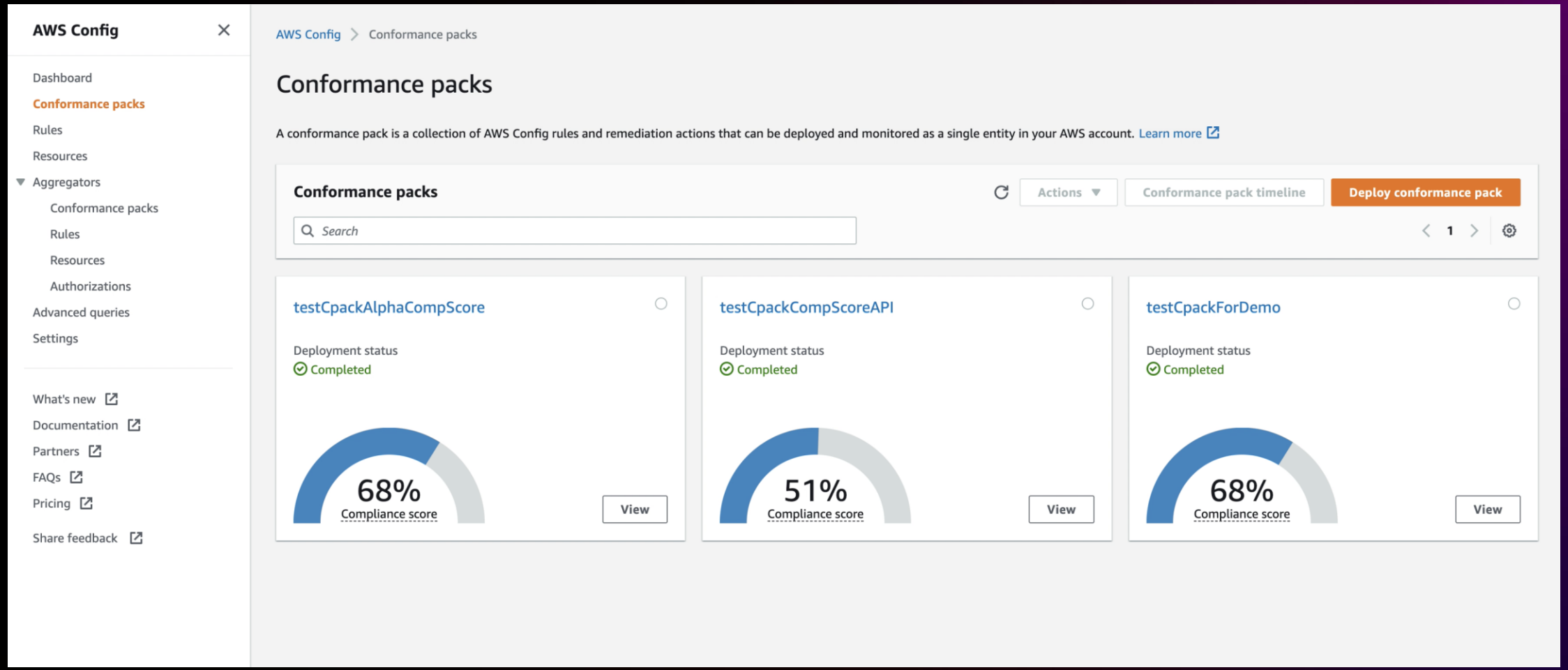
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Compliance Preparation



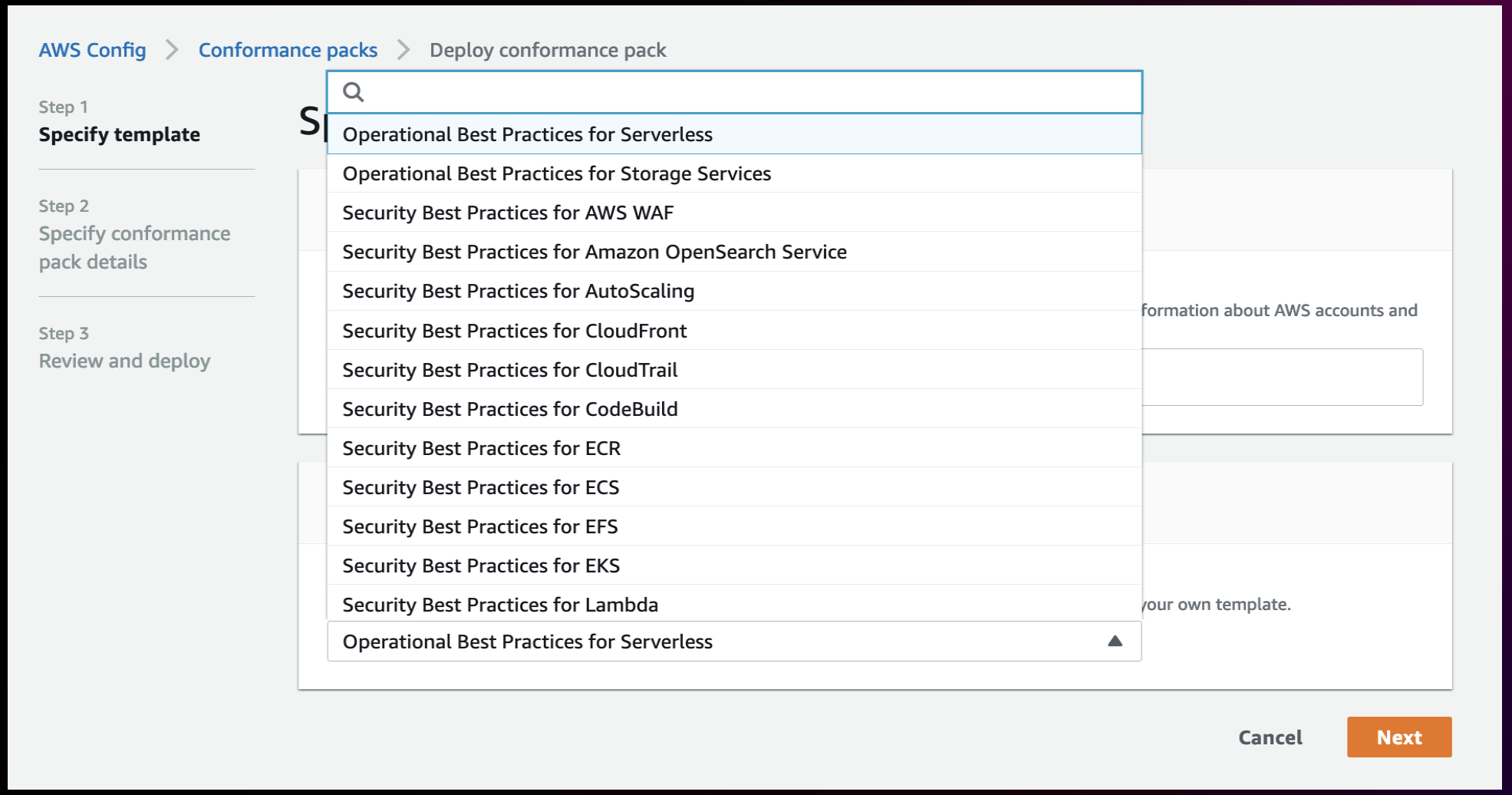
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Compliance Preparation



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

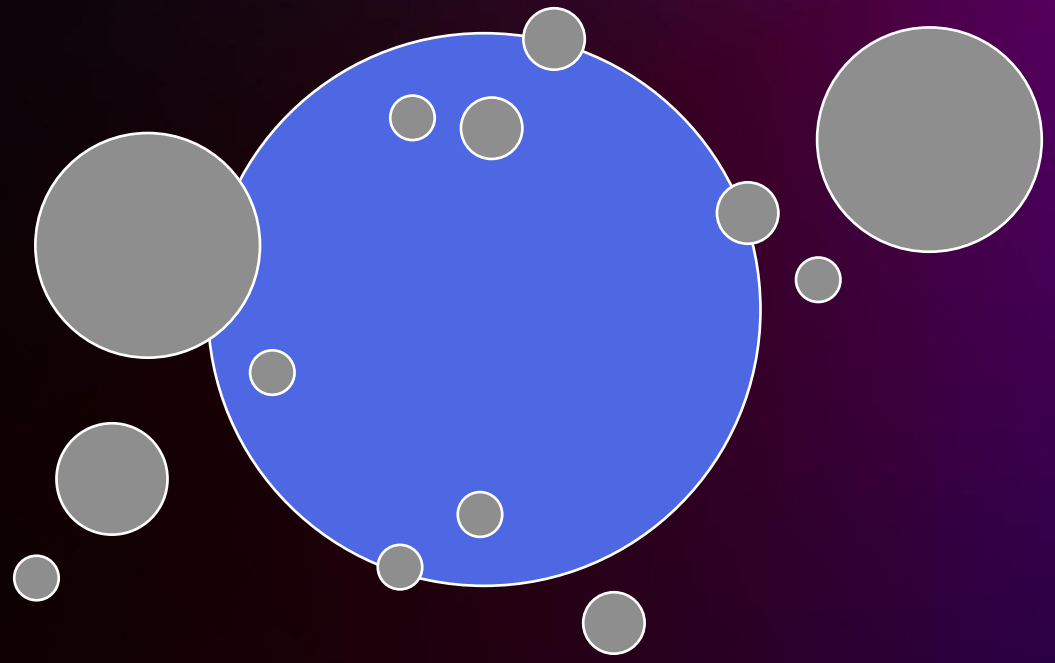
Scaling Up – Compliance Preparation



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Posture

- Organization & Identity
  - ☑ Environment Isolation
  - ☑ Centralized Identity Management
  - ☑ Periodic Access Analysis
  - ☑ Automatic Credential Rotation
- Security Operations
  - ☑ Centralized Logging
  - ☑ Foundational Security Reporting
  - ☑ Managed Security Monitoring
  - ☑ Compliance Preparation



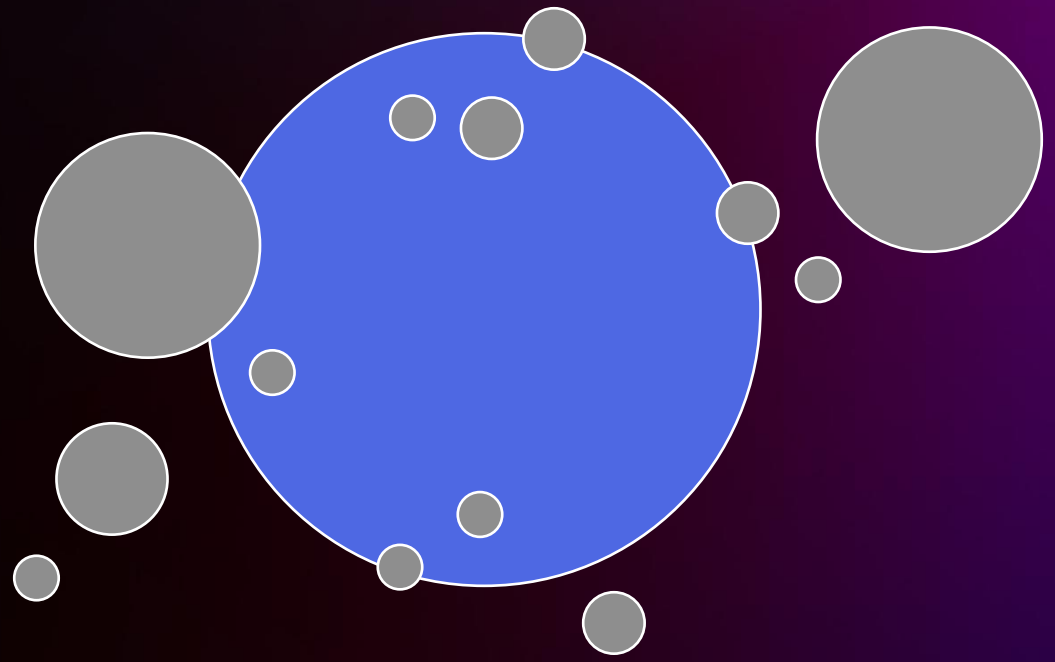
Centralization

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Up – Takeaways

- Identity
  - With Identity Center
- Logging
  - With the Log Archive Account
- Reporting
  - With Athena
- Monitoring
  - With Security Hub



Centralization

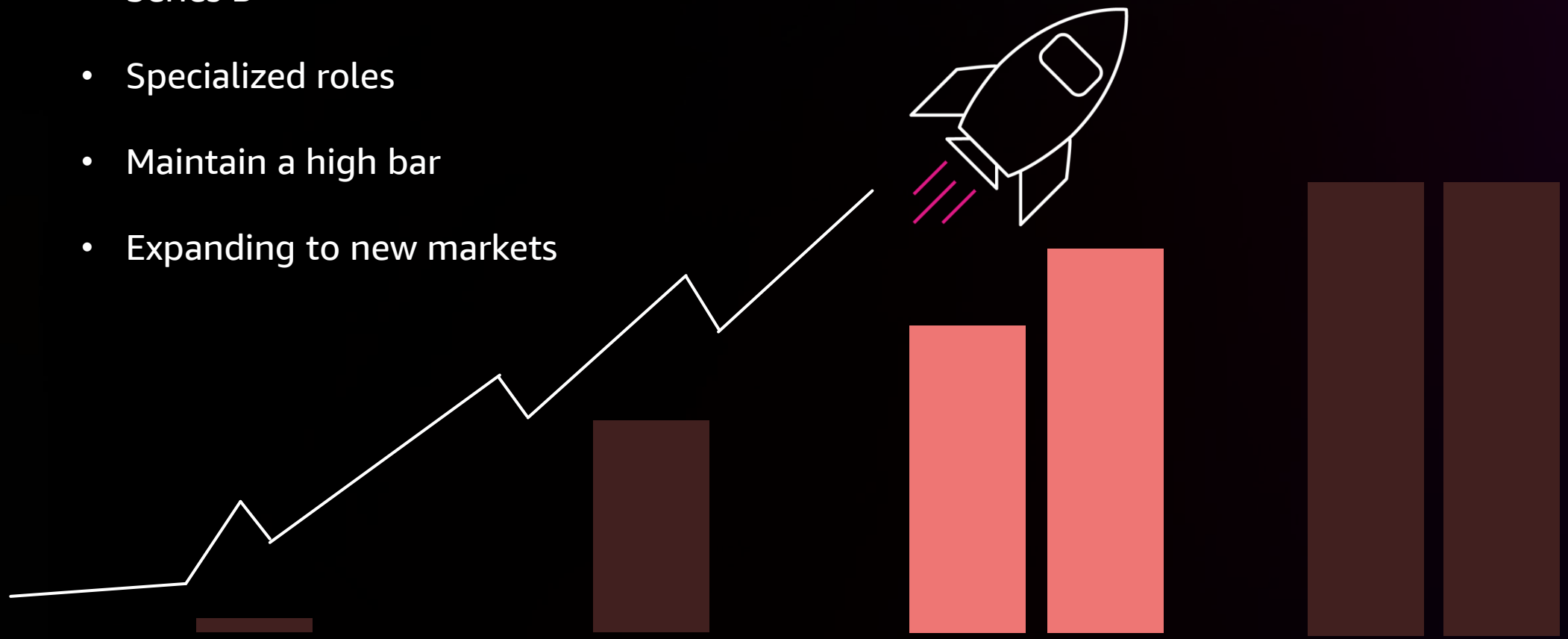
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Stage 3 – Scaling Out

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out - Characteristics

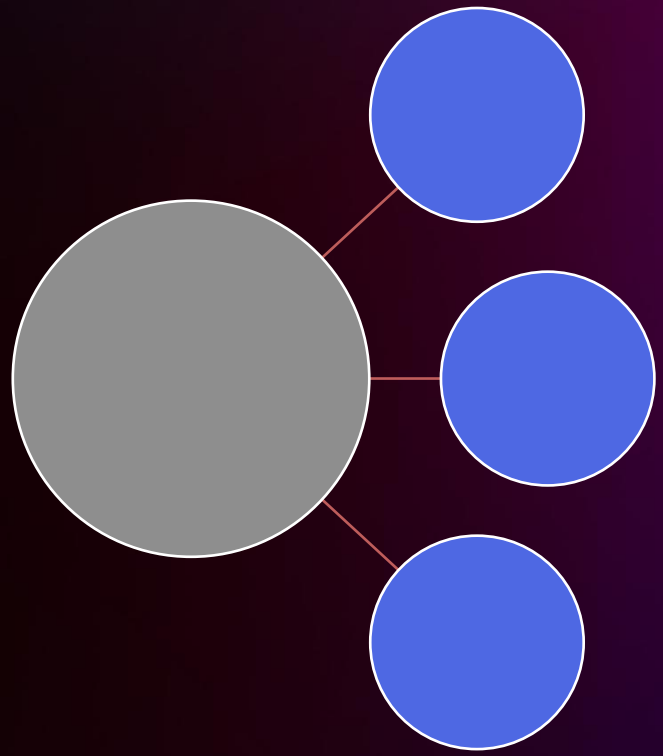
- Series B+
- Specialized roles
- Maintain a high bar
- Expanding to new markets



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Posture

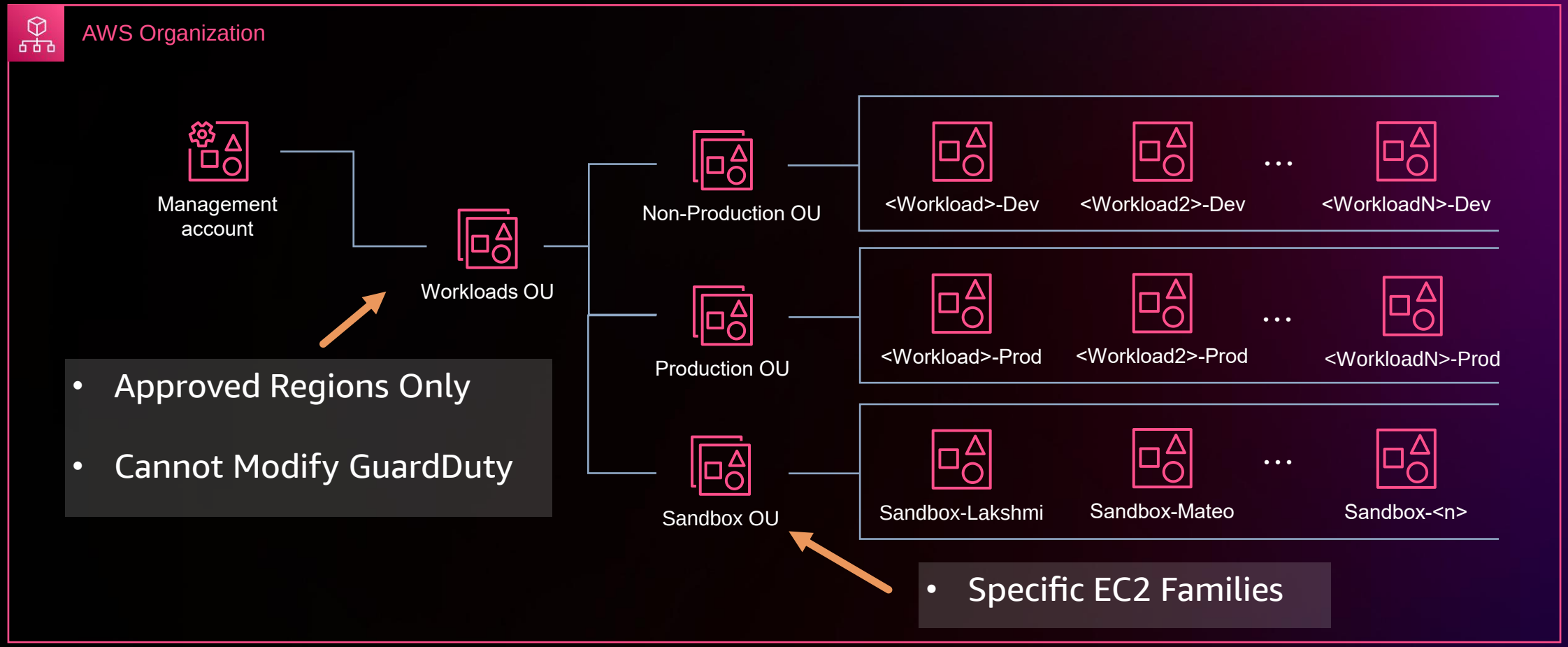
- Organization & Identity
  - Security Invariants
  - Data Perimeters
  - Automated Account Standards
- Security Operations
  - Security Team & Tooling
  - Security Guardians
  - Incident Response Playbooks
  - Compliance Certification



Delegation

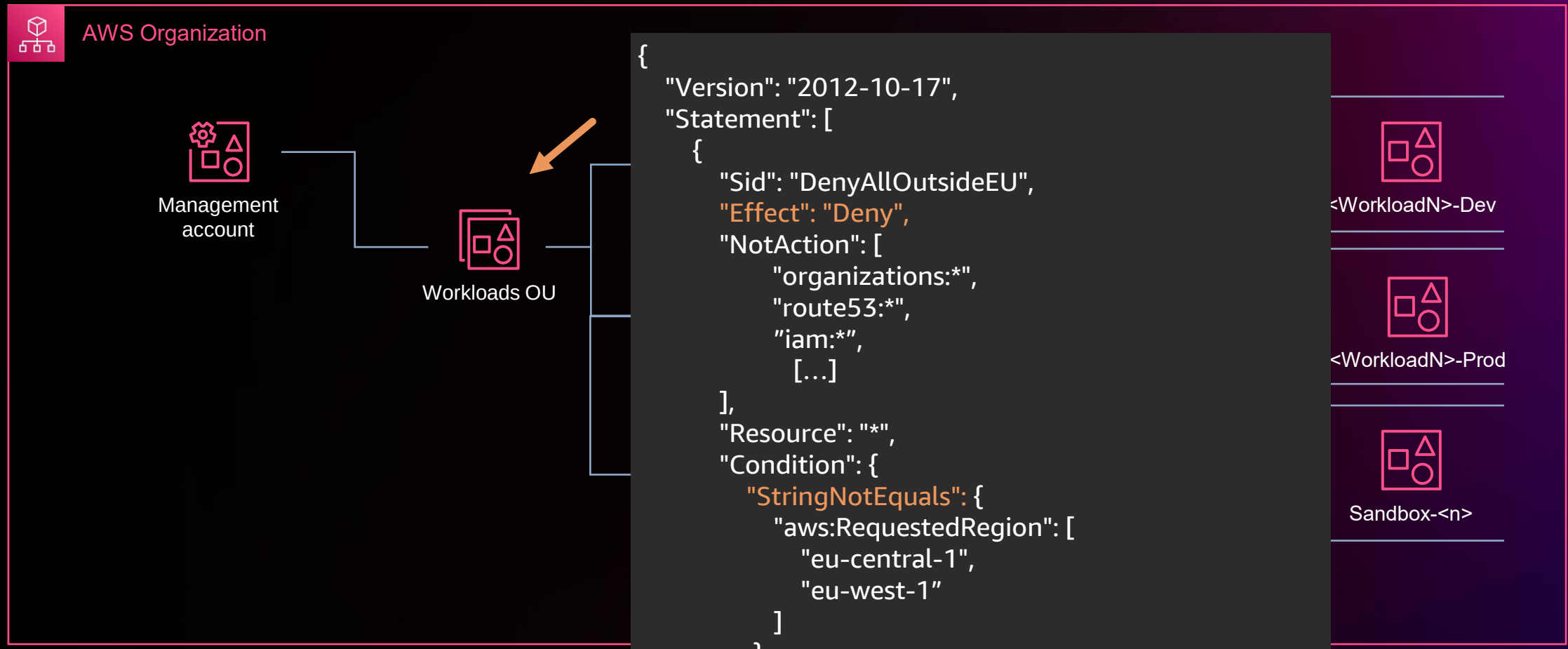
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Security Invariants



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

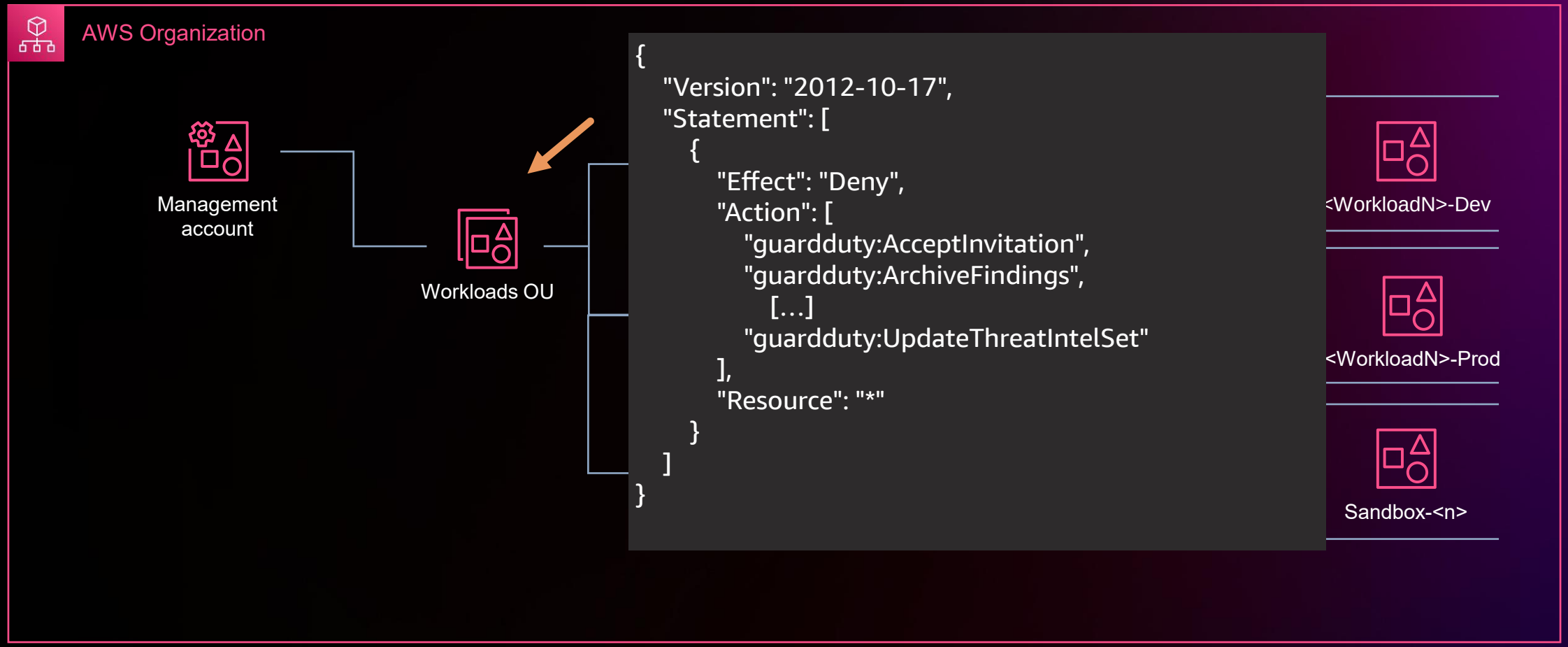
Scaling Out – Security Invariants




```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAllOutsideEU",
      "Effect": "Deny",
      "NotAction": [
            "organizations:*",
            "route53:*",
            ”iam:*”,
              […]
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "eu-central-1",
            "eu-west-1”
          ]
        }
      }
    }
  ]
}
```

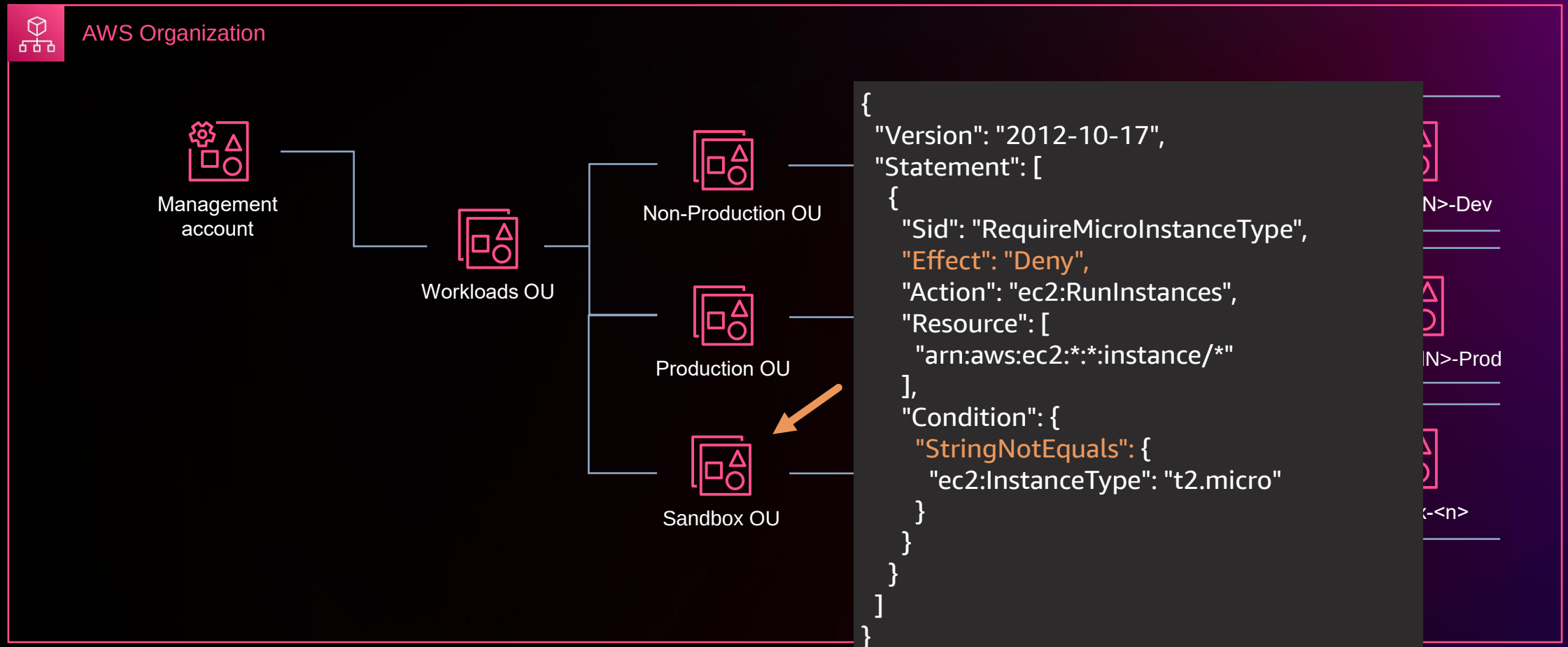
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Security Invariants



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Security Invariants



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

More Examples: Service Control Policies

- Block service access to the root user
- Prevent tampering with CloudWatch
- Restrict which services can be used

… and more



https://go.aws/3O8OOyI

aws

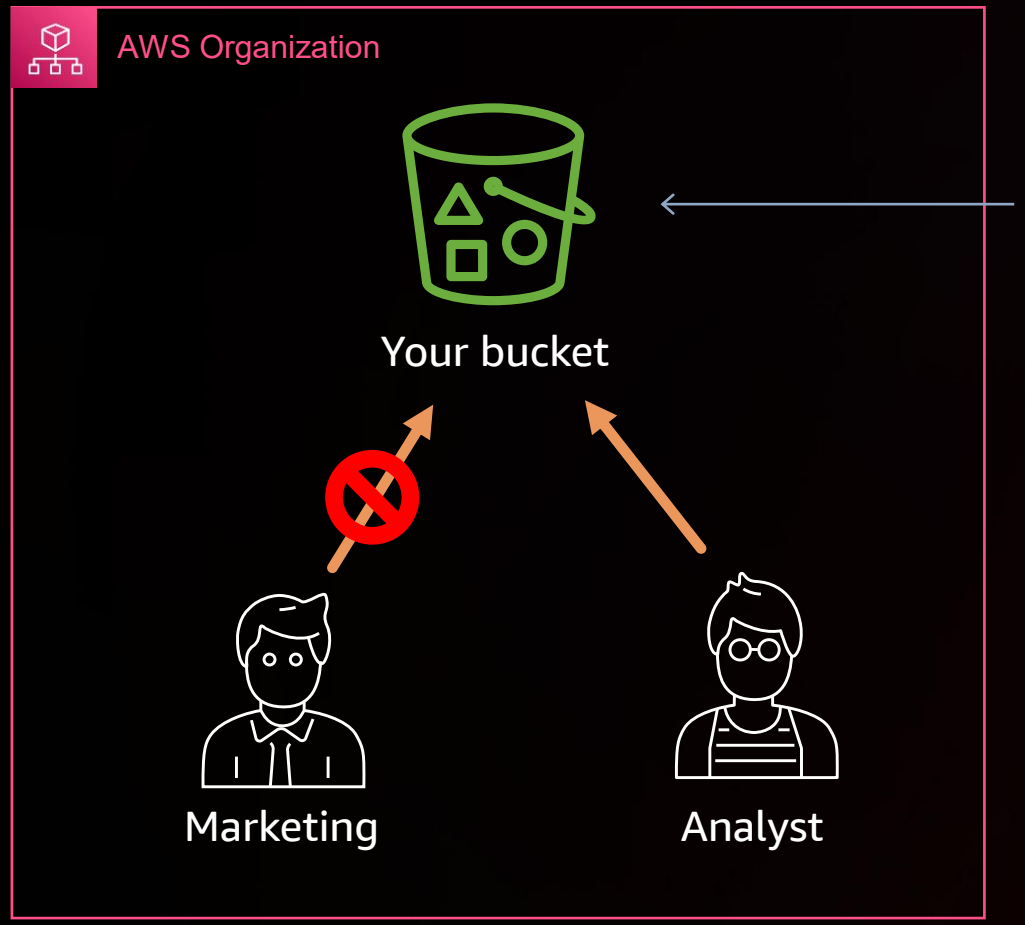
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Data Perimeters



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

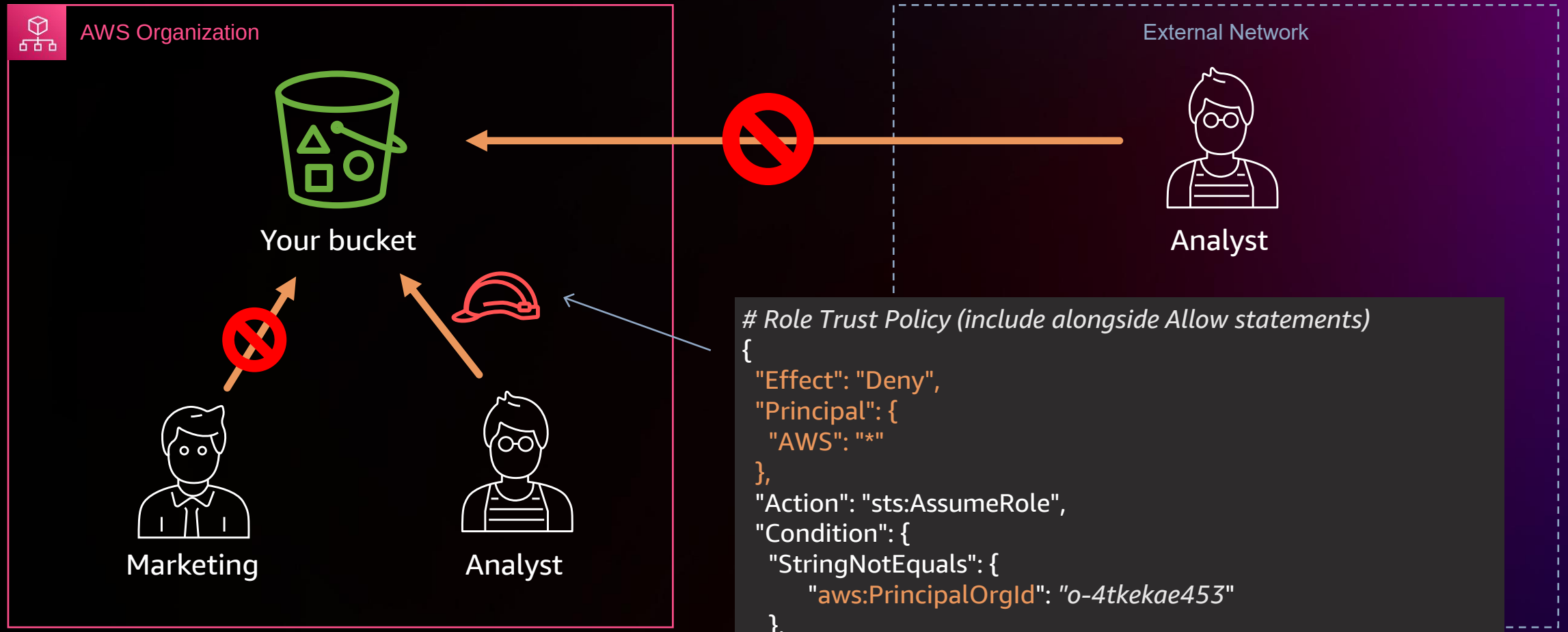
Scaling Out – Data Perimeters




```
# Resource Policy
{ …
    "Effect": "Deny",
    "Principal": "*",
    "Action": "*",
    "Resousrce": [
     "arn:aws:s3:::bucketname",
     "arn:aws:s3:::bucketname/*"
    ],
    "Condition": {
     "StringNotEquals": {
       "aws:PrincipalOrgId": "o-4tkekae453"
     },
     "Bool": {
       "aws:PrincipalIsAWSService": "false"
     }
    }
… }
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

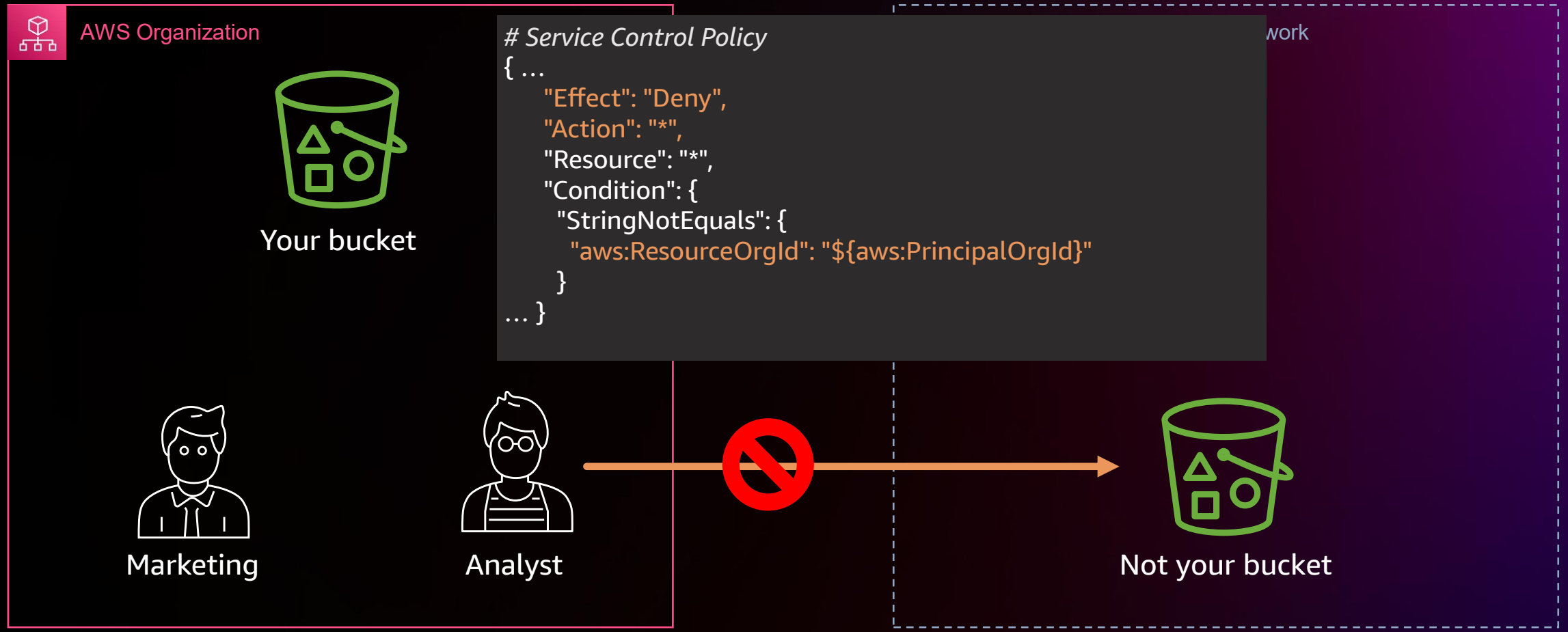
Scaling Out – Data Perimeters




```
# Role Trust Policy (include alongside Allow statements)
{
  "Effect": "Deny",
  "Principal": {
    "AWS": "*"
  },
  "Action": "sts:AssumeRole",
  "Condition": {
    "StringNotEquals": {
          "aws:PrincipalOrgId": "o-4tkekae453"
    },
  }
}
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Data Perimeters



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Whitepaper: Building a Data Perimeter

- What kind of policy to use
- Example policies

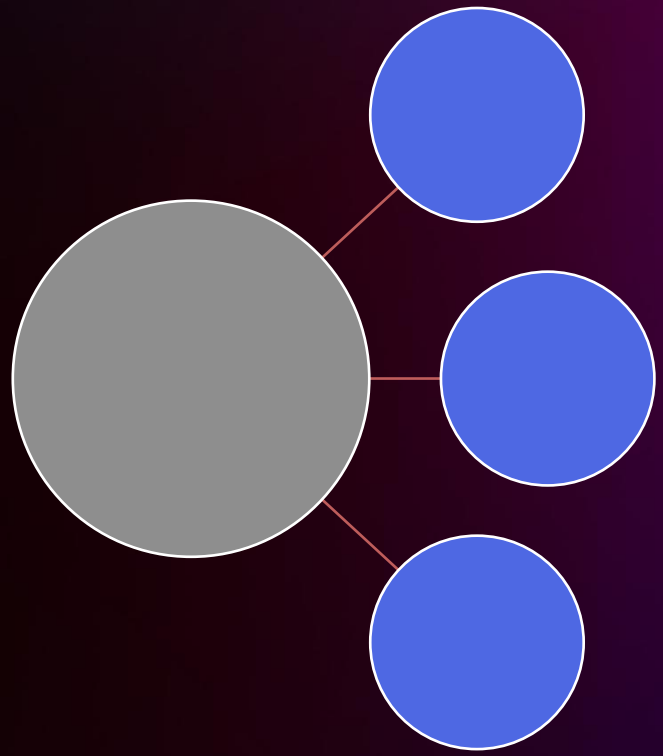


https://go.aws/3fT2x02

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Posture

- Organization & Identity
  - ☑ Security Invariants
  - ☑ Data Perimeters
  - ⊡ Automated Account Standards
- Security Operations
  - Security Team & Tooling
  - Security Guardians
  - Incident Response Playbook
  - Compliance Certification

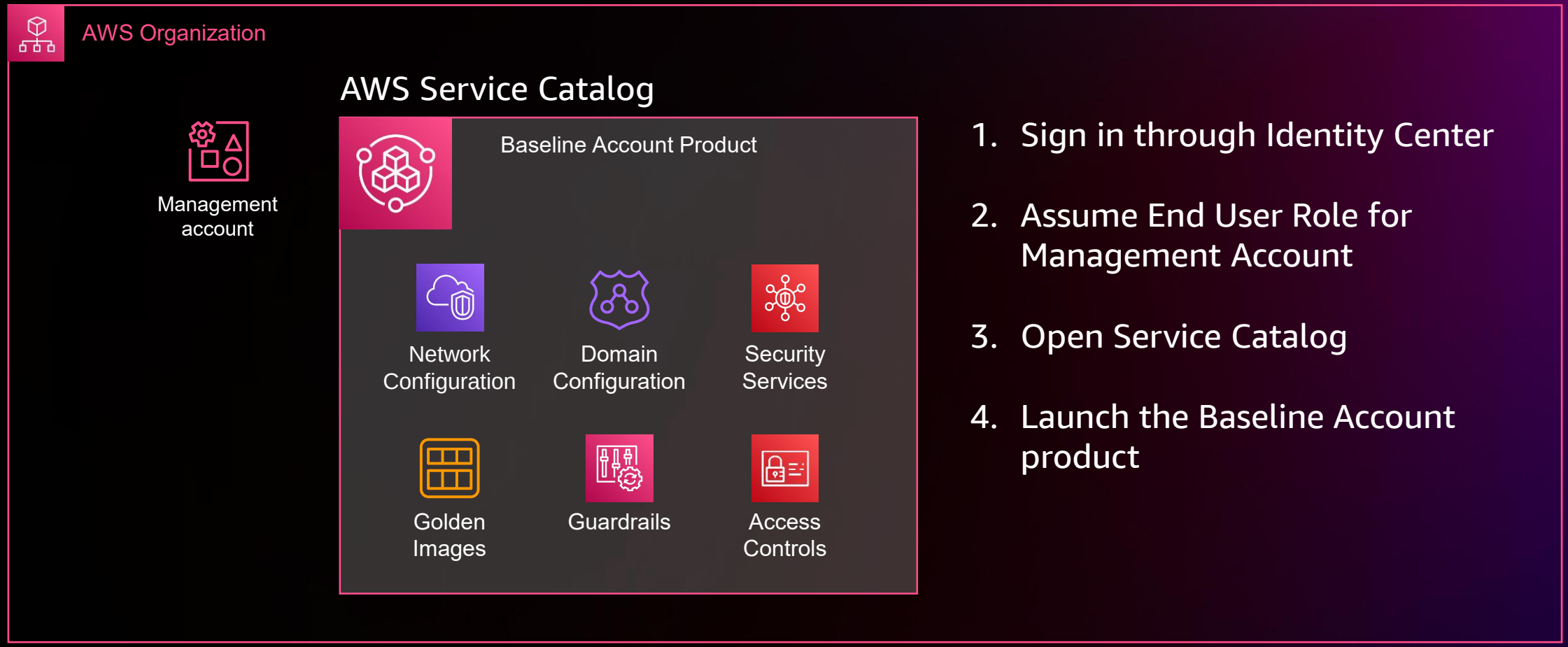


Delegation

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

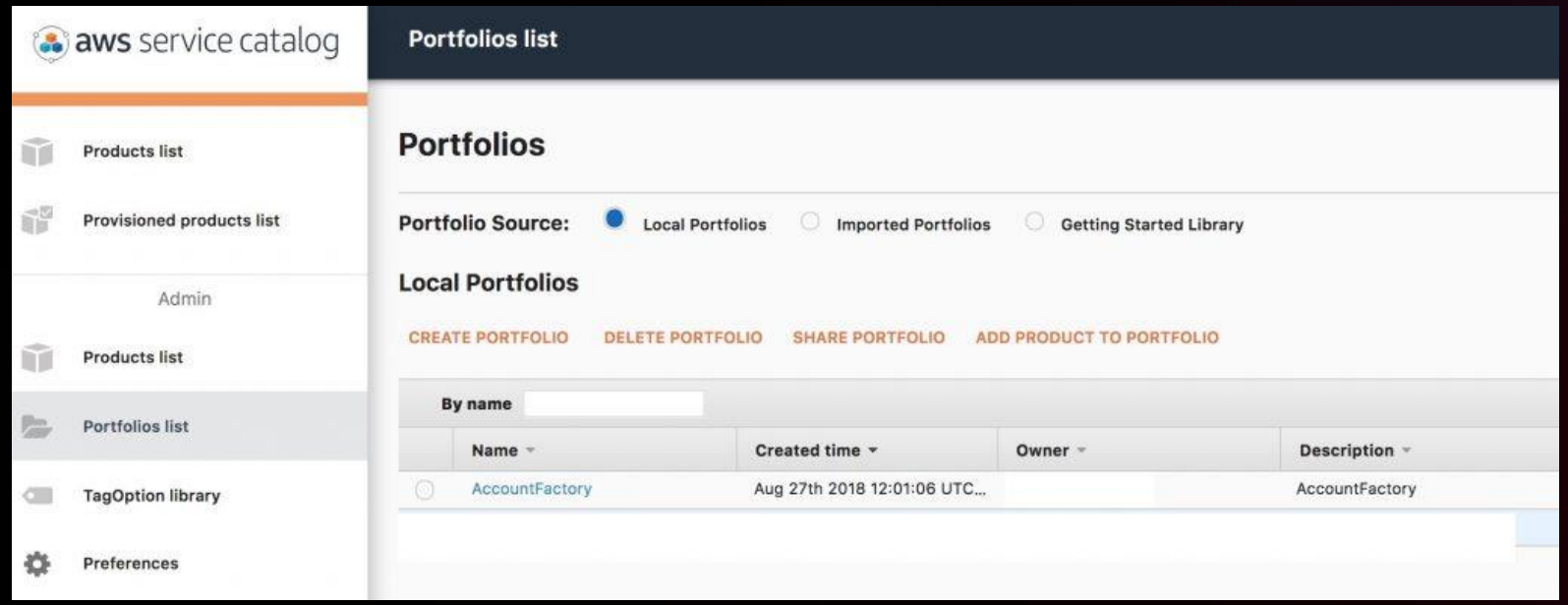
Scaling Out – Automated Account Standards



1. Sign in through Identity Center
2. Assume End User Role for Management Account
3. Open Service Catalog
4. Launch the Baseline Account product

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Code: Automating Account Creation

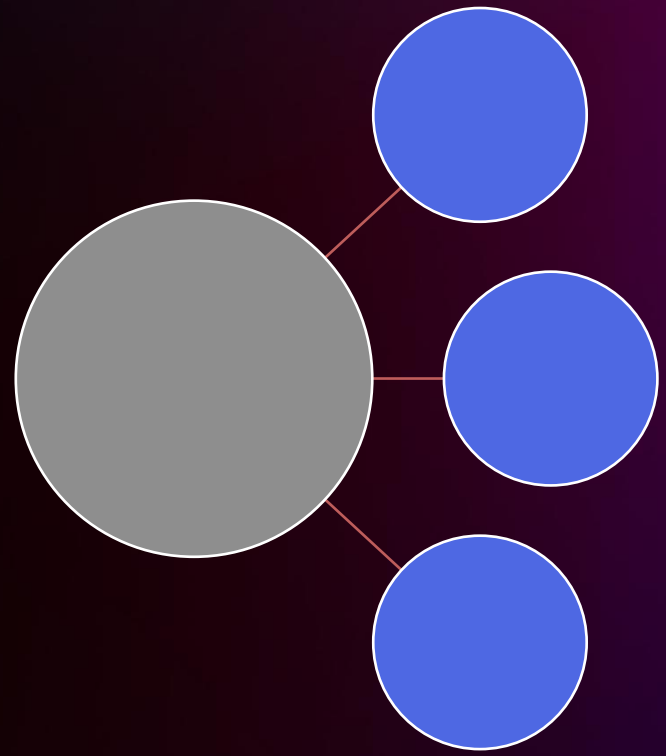


https://go.aws/3EySLJS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Posture

- Organization & Identity
  - ☑ Security Invariants
  - ☑ Data Perimeters
  - ☑ Automated Account Standards
- Security Operations
  - ⊡ Security Team & Tooling
  - ⊡ Security Guardians
  - Incident Response Playbook
  - Compliance Certification

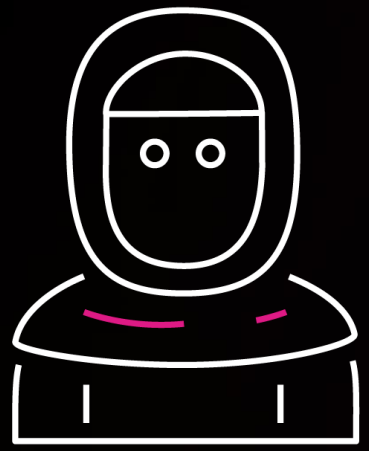


Delegation

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

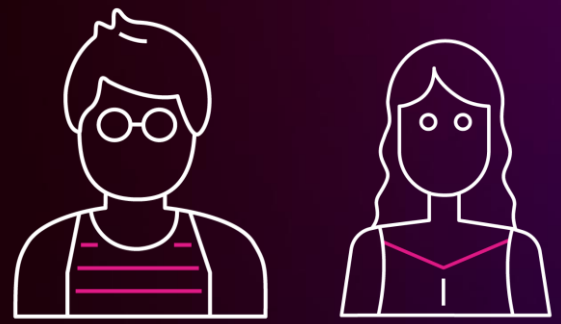
Scaling Out – Security Team



Security Team



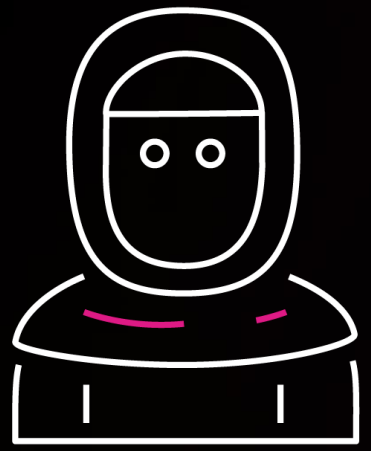
Dev Team



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Security Team



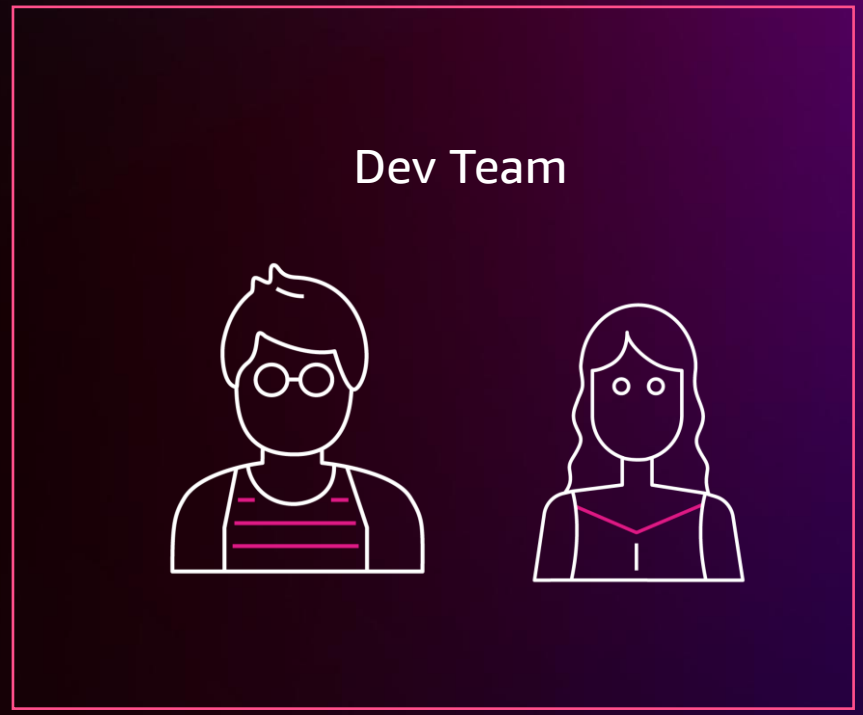
Security Team

- Organization & Account Structure
- Corporate Identity & Access
- Service Control Policies
- Security Tooling, Analysis, Reporting

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Security Team

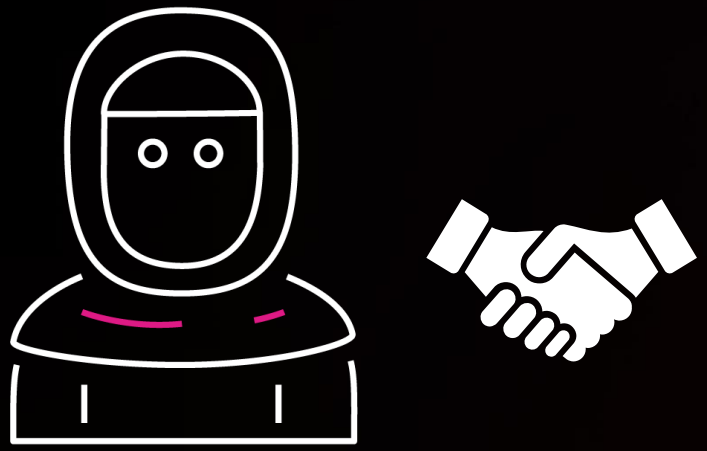
- Workload Permissions
- Code Linting, Review, Resolution
- Software Supply Chain
- Safe Coding Standards



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Security Guardians



Security Team

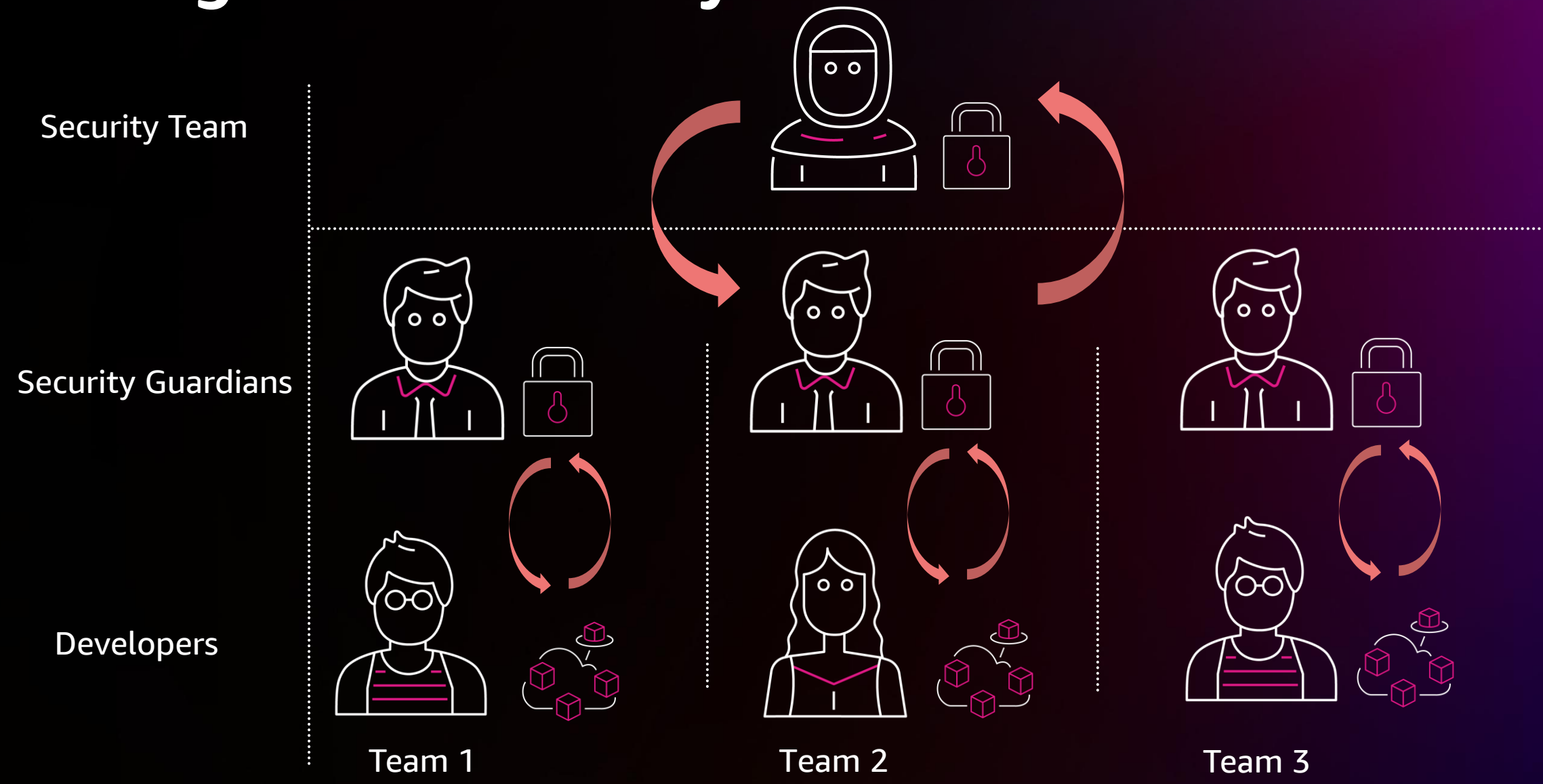
Dev Team



Security Guardian

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Security Guardians



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recommendation: Automated Security Helper

AWS open-source tool to analyze source code

Supported frameworks:

- Code: Git, Python, JavaScript/NodeJS
- Infrastructure: Terraform, CloudFormation



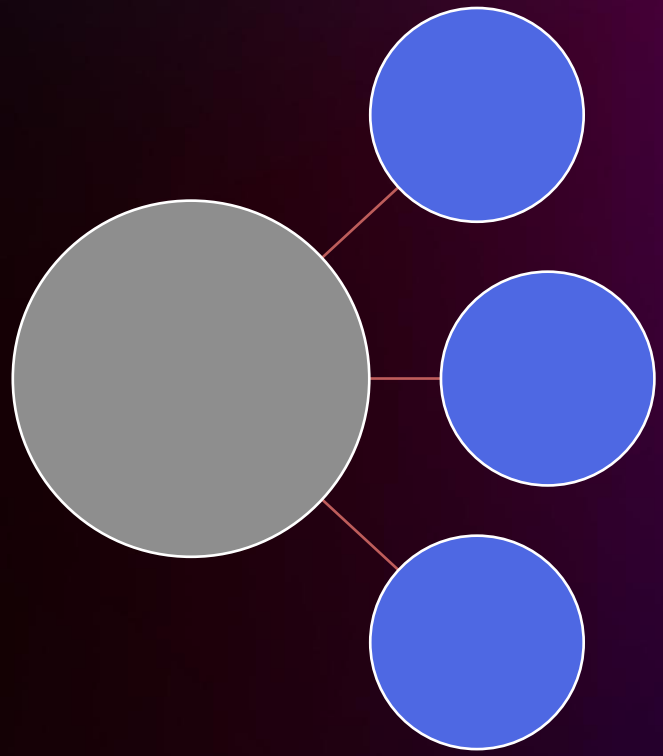
https://bit.ly/3UAUmV8

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Posture

- Organization & Identity
  - ☑ Security Invariants
  - ☑ Data Perimeters
  - ☑ Automated Account Standards
- Security Operations
  - ☑ Security Team & Tooling
  - ☑ Security Guardians
  - → Incident Response Playbooks
  - Compliance Certification



Delegation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Incident Response Playbooks



Prepare



Detect & Analyze



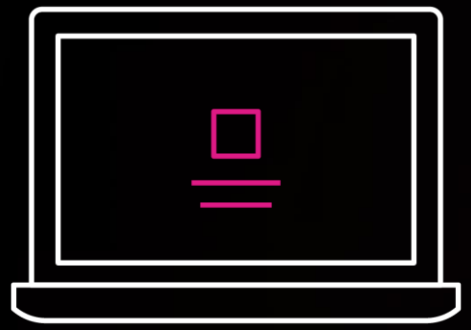
Contain, Eradicate, Recover



Post-Incident Review

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Incident Response Playbooks



Prepare

- The issue being addressed
- The teams involved
- The tools they will use
- The access they require
- The steps they will follow

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Incident Response Playbooks

Response Steps

1. [**ANALYSIS**] Validate alert by checking ownership of exposed credential
2. [**ANALYSIS**] Identity exposed credential owner/custodian
3. [**CONTAINMENT**] Disable exposed credential if approved by owner/customer
4. [**ANALYSIS**] Use Athena to pull 15 days of exposed credential activity from CloudTrail logs
5. [**ANALYSIS**] Use Athena to pull 15 days of source IP addresses used by exposed credential from VPC Flow logs
6. [**ANALYSIS**] Establish reputation for source IP addresses
7. [**ANALYSIS**] Determine which source IP addresses were used against infrastructure resources such as EC2 instances, RDS databases
8. [**ANALYSIS**] Discover all resources provisioned, modified, and deleted by the exposed credential based on CloudTrail logs
9. [**CONTAINMENT**] Perform containment of all rogue resources provisioned by the exposed credential
10. [**CONTAINMENT**] Perform containment of existing resources modified by the exposed credentials with approval from owner/custodian
11. [**ANALYSIS**] Repeat steps 4 to 10 for IAM principals created by the exposed credential
12. [**ANALYSIS**] Determine if data was exfiltrated, modified, or deleted. Figure out the classification for all data sets touched.
13. [**ANALYSIS**] Expand log scope to 90 days or further and repeat steps 1-12. Use your judgment on how far back to go.
14. [**ANALYSIS**] Estimate attribution and attack type (targeted or opportunistic)
15. [**ANALYSIS**] Preserve all relevant infrastructure and service resources for forensics investigation
16. [**ERADICATION**] Perform eradication (delete rogue resources, apply security updates and harden configuration)
17. [**RECOVERY**] Perform recovery by restoring system data and rebuilding components
18. [**POST-INCIDENT ACTIVITY**] Perform post-incident activity for preparation enhancement

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Incident Response Playbooks

Issue Detected: Exposed IAM credentials in the form of ***IAM Access Keys*** or ***IAM User and password combination.***

Response Steps:

Analysis

IAM Access Key with id AKIAIOSFODNN7EXAMPLE was found in plain text in a public git repository

```
aws sts get-access-key-info --access-key-id AKIAIOSFODNN7EXAMPLE --profile
SecurityAnalystRole --region us-east-1
{
    "Account": "777777777777"
}
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources: Incident Response

Example: Incident Response Playbook



https://bit.ly/3g6oYyL

Whitepaper: Security Incident Response



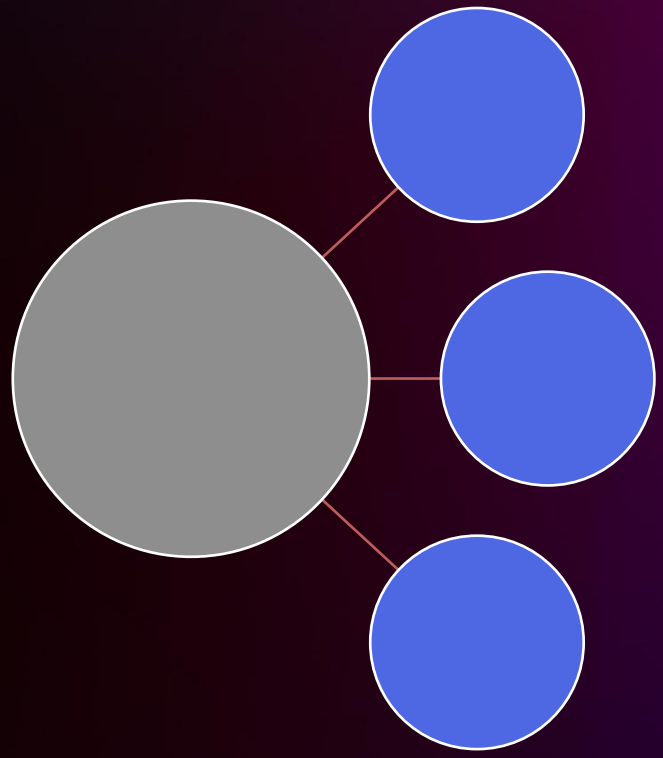
https://go.aws/3EwlT4z

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Posture

- Organization & Identity
  - ☑ Security Invariants
  - ☑ Data Perimeters
  - ☑ Automated Account Standards
- Security Operations
  - ☑ Security Team & Tooling
  - ☑ Security Guardians
  - ☑ Incident Response Playbooks
  - → Compliance Certification



Delegation

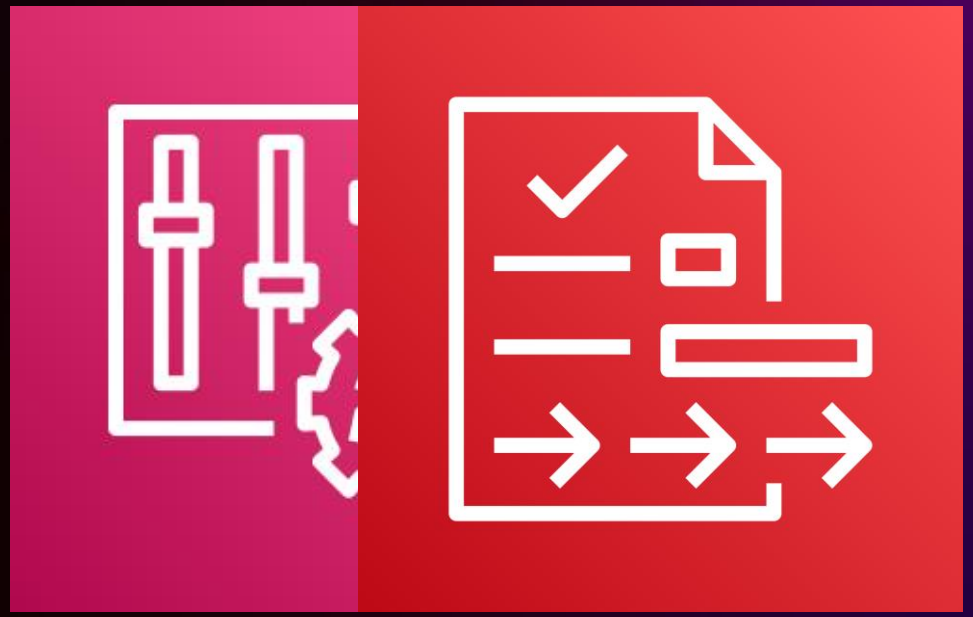
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Compliance Certification



AWS Artifact

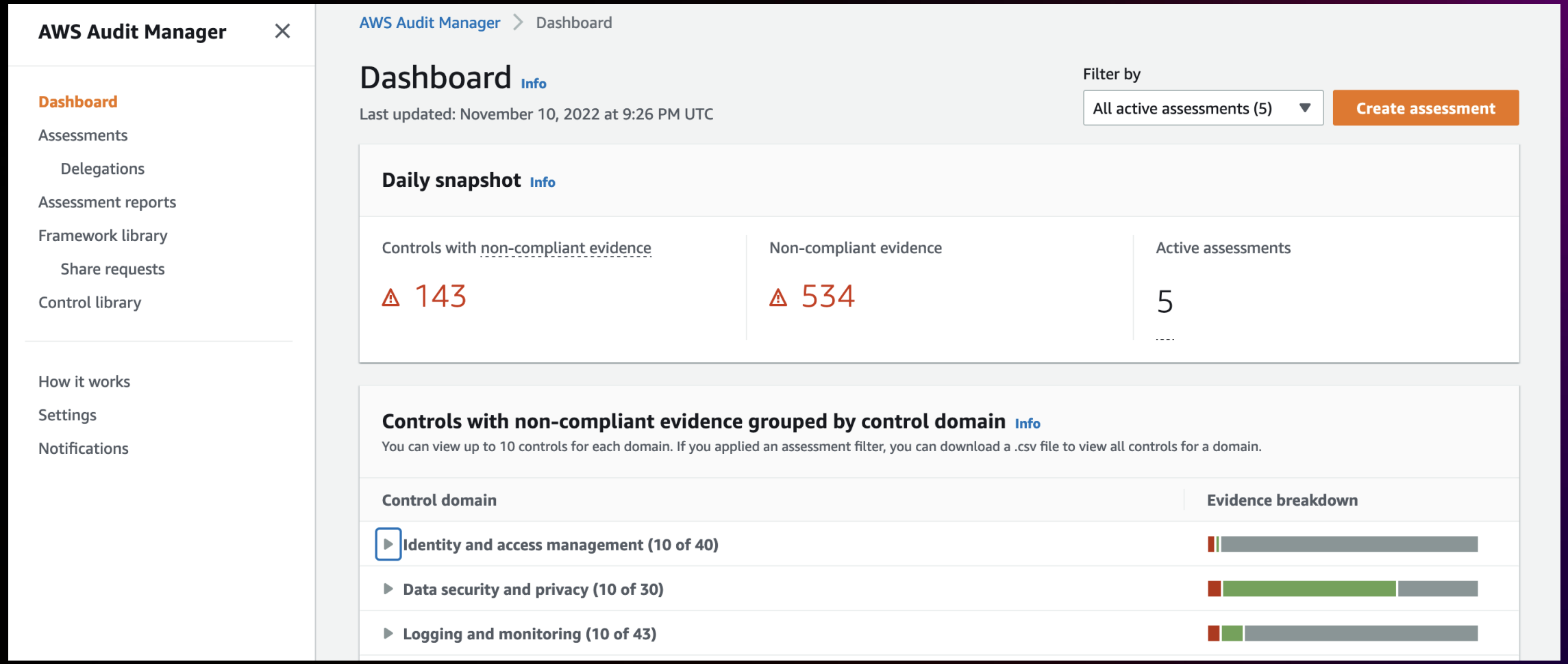


AWS Config

AWS Audit Manager

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Compliance Certification



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resource: Compliance Solutions

- Help with security questionnaires
- Services in scope
- Compliance framework pages
- Targeted Quick Starts and guides



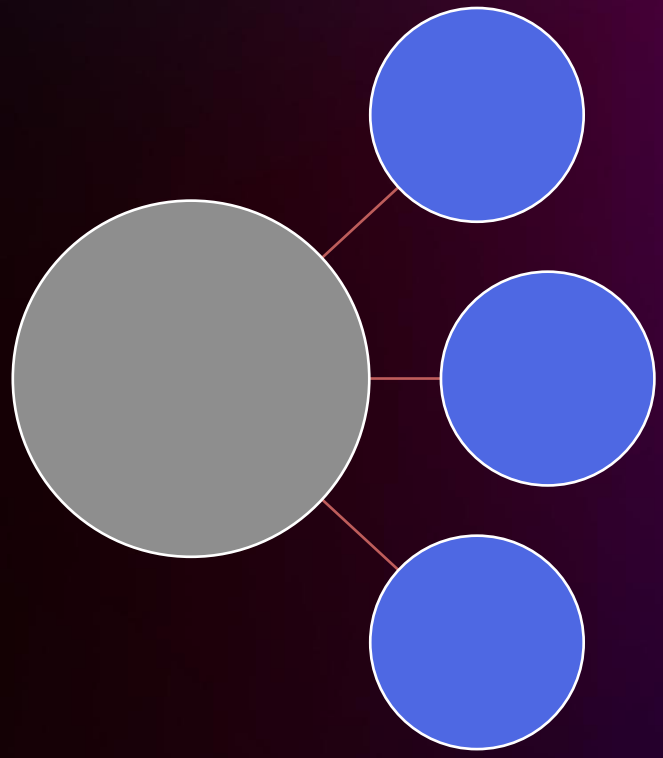
https://go.aws/3O62U41

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Posture

- Organization & Identity
  - ☑ Security Invariants
  - ☑ Data Perimeters
  - ☑ Automated Account Standards
- Security Operations
  - ☑ Security Team & Tooling
  - ☑ Security Guardians
  - ☑ Incident Response Playbooks
  - ☑ Compliance Certification



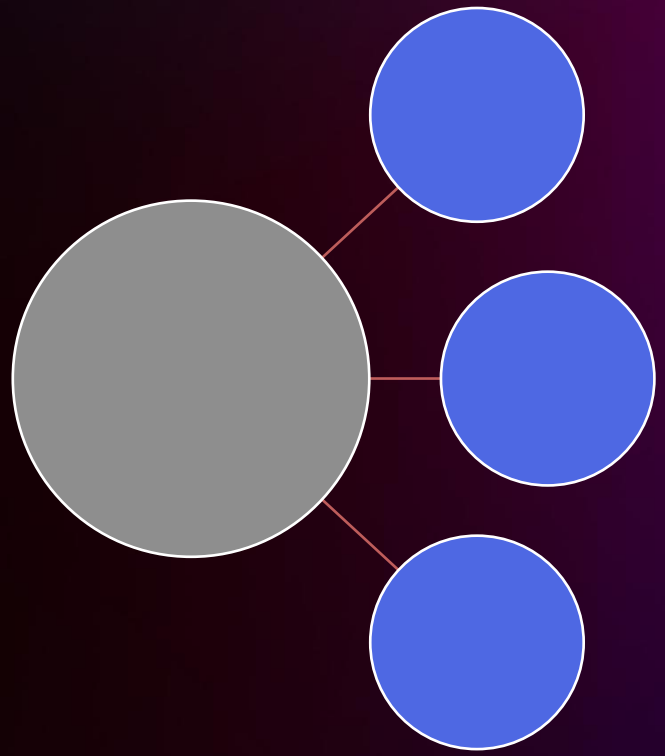
Delegation

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling Out – Takeaways

- Setting Boundaries
  - Security Invariants
  - Data Perimeters
- Collaborating
  - Security Team
  - Security Guardians
- Incident Response
  - Building Playbooks



Delegation

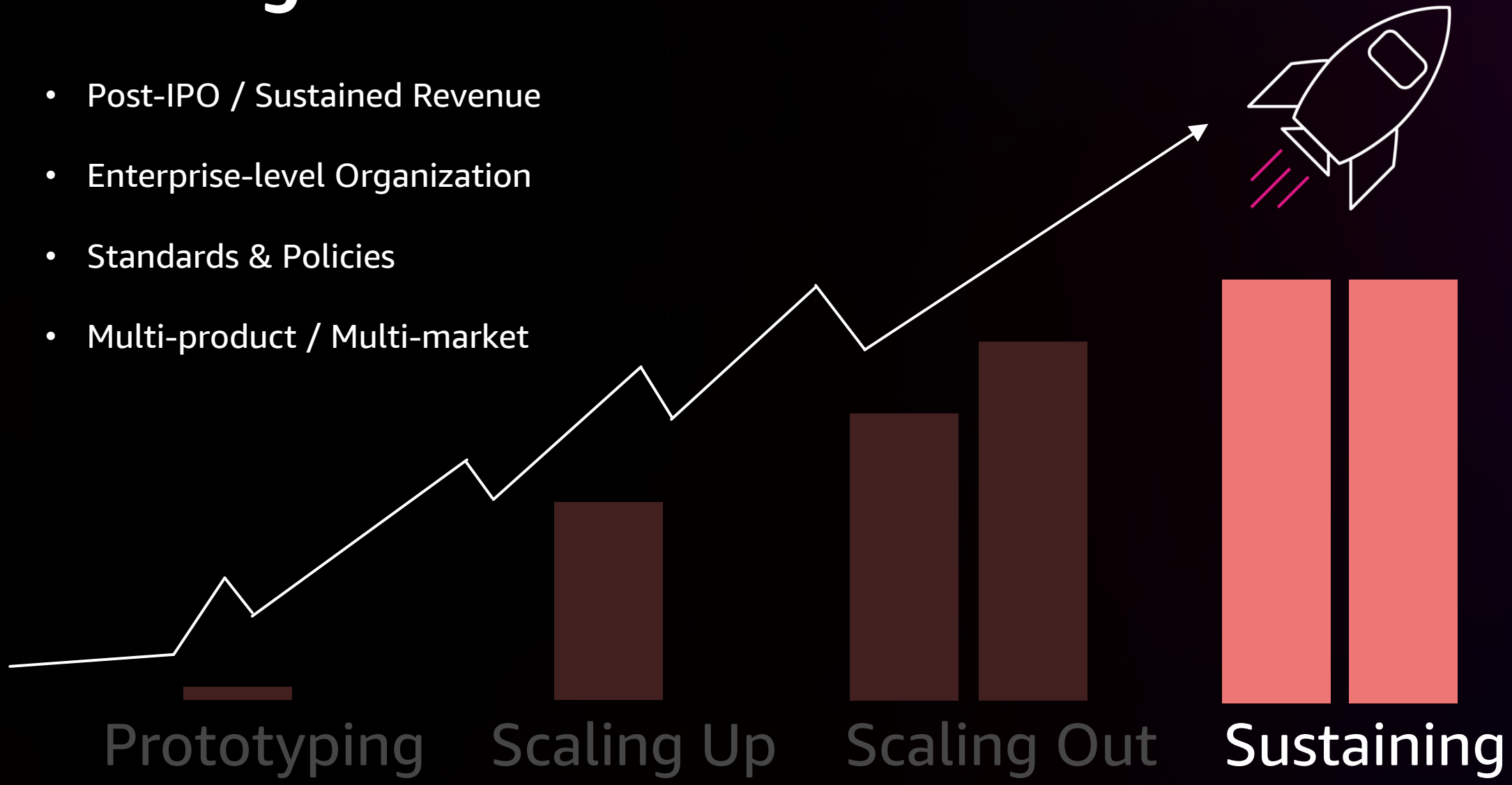
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Stage 4 – Sustaining

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining - Characteristics

- Post-IPO / Sustained Revenue
- Enterprise-level Organization
- Standards & Policies
- Multi-product / Multi-market

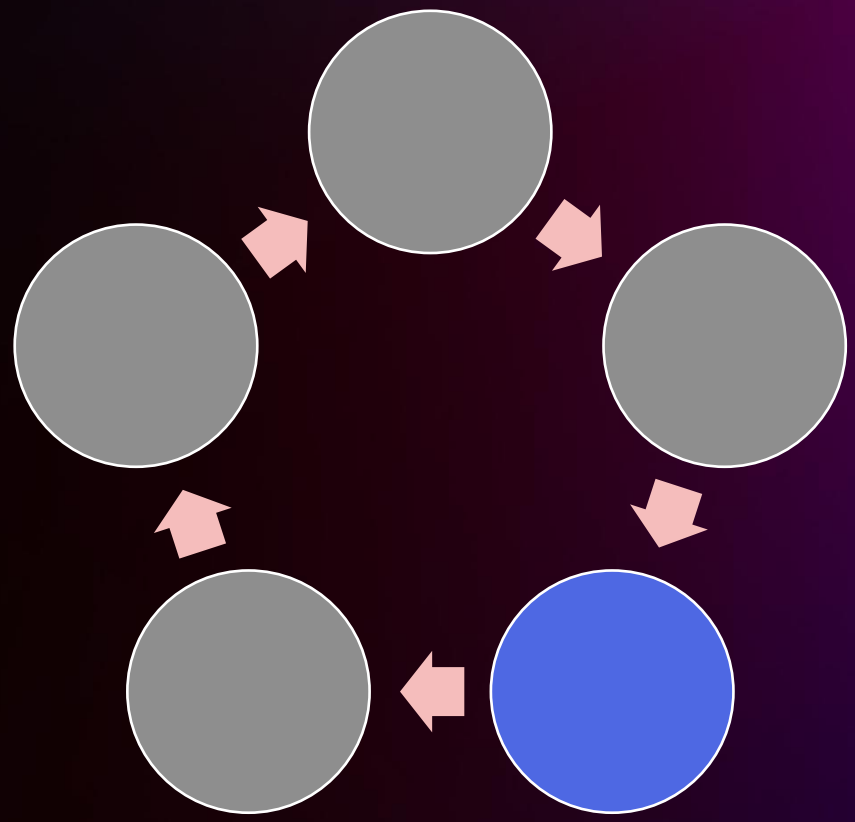


aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Posture

- Organization & Identity
  - Permission Delegation
- Security Operations
  - Incident Response Testing
  - Threat Hunting

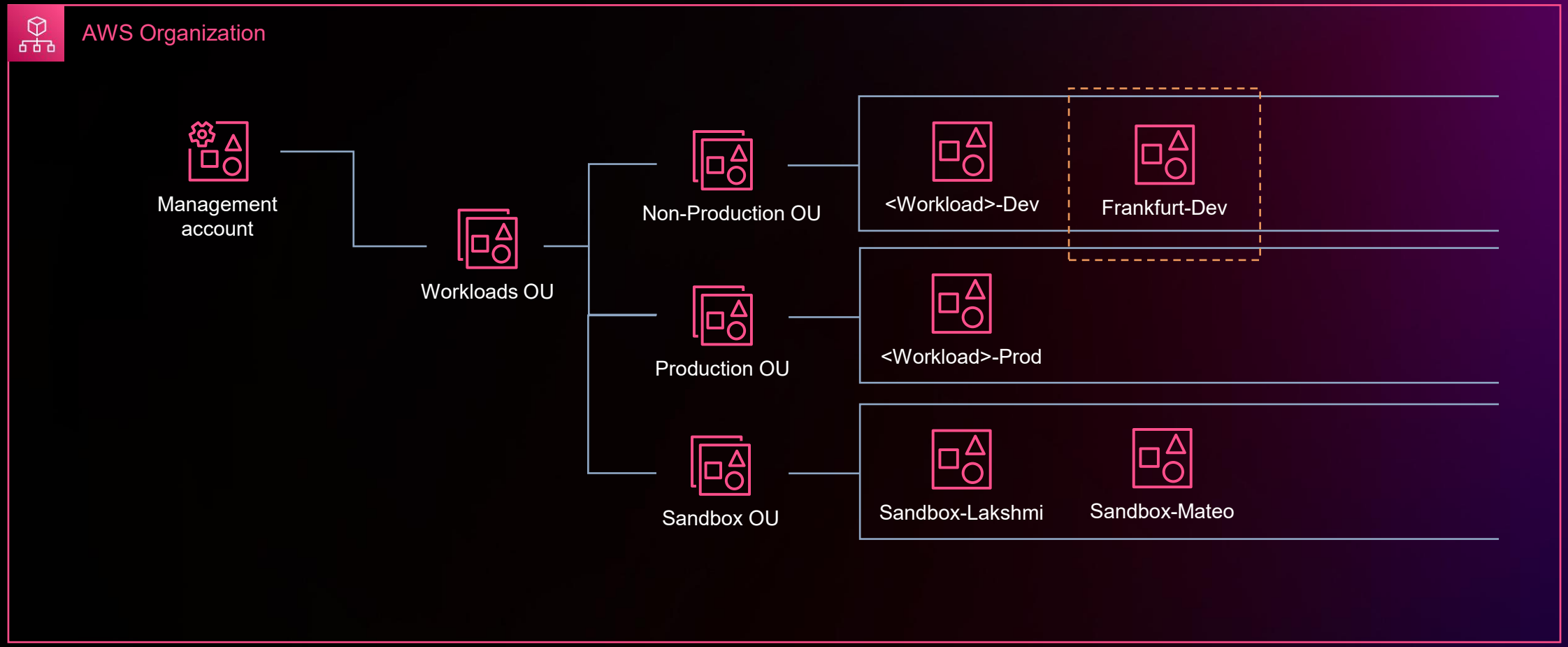
+ Zero Trust



Refinement

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Permission Delegation



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Permission Delegation

Security Admin

1. Create a Permission Boundary policy

```
# Permission Boundary – "Frankfurt_Boundary"
{
 "Version" : "2012-10-17",
 "Statement" : [{
  "Effect": "Allow",
  "Action": [
   "dynamodb:PutItem",
   "dynamodb:UpdateItem",
   "dynamodb:DeleteItem"
  ],
  "Resource": "*",
  "Condition": {
      "StringEquals": {
         "aws:RequestedRegion": "eu-central-1"
      }
  }
 }]
}
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Permission Delegation

Security Admin

1. Create a Permission Boundary policy
2. Create permissions policy for IAM admin role

```
# IAM admin role permission policy
{
 "Version" : "2012-10-17",
 "Statement" : [
 {
  "Sid": "SetPermissionsBoundary",
  "Effect": "Allow",
  "Action": [
   "iam:CreateRole",
   "iam:AttachRolePolicy",
   "iam:DetachRolePolicy"
  ],
  "Resource": "arn:aws:iam::<account>:role/Frankfurt*",
  "Condition": {
   "StringEquals": {
    "iam:PermissionsBoundary":
     "arn:aws:iam::<account>:policy/Frankfurt_Boundary"
   }
  }
 }
 { ... } # Edit policy permissions
}
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Permission Delegation

Security Admin

1. Create a Permission Boundary policy
2. Create permissions policy for IAM admin role

Security Guardian

3. Create a role referencing the boundary

```
# Create bounded IAM role
$ aws iam create-role
  --role-name
       FrankfurtWebRole
  --assume-role-policy-document
       file://assume_role_policy.json
  --permissions-boundary
       arn:aws:iam::<account>:policy/Frankfurt_Boundary
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Permission Delegation

Security Admin

1. Create a Permission Boundary policy
2. Create permissions policy for IAM admin role

Security Guardian

3. Create a role referencing the boundary
4. Attach permission policy to the role

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
  "Effect": "Allow",
  "Action": "dynamodb:*",
  "Resource": [
   "arn:aws:dynamodb:eu-central-1:<account>:table/Users"
  ]
 }]
}
```

```
# Permission Boundary
{ …
   "Action": [
     "dynamodb:PutItem",
     "dynamodb:UpdateItem",
     "dynamodb:DeleteItem"
   ],
}
```

```
# Permission Boundary cont
…
"Condition": {
 "StringEquals": {
 "aws:RequestedRegion":
     "eu-central-1"
}
…
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Blog – Delegating Permission Management

Detailed Walkthrough of Permission Boundaries



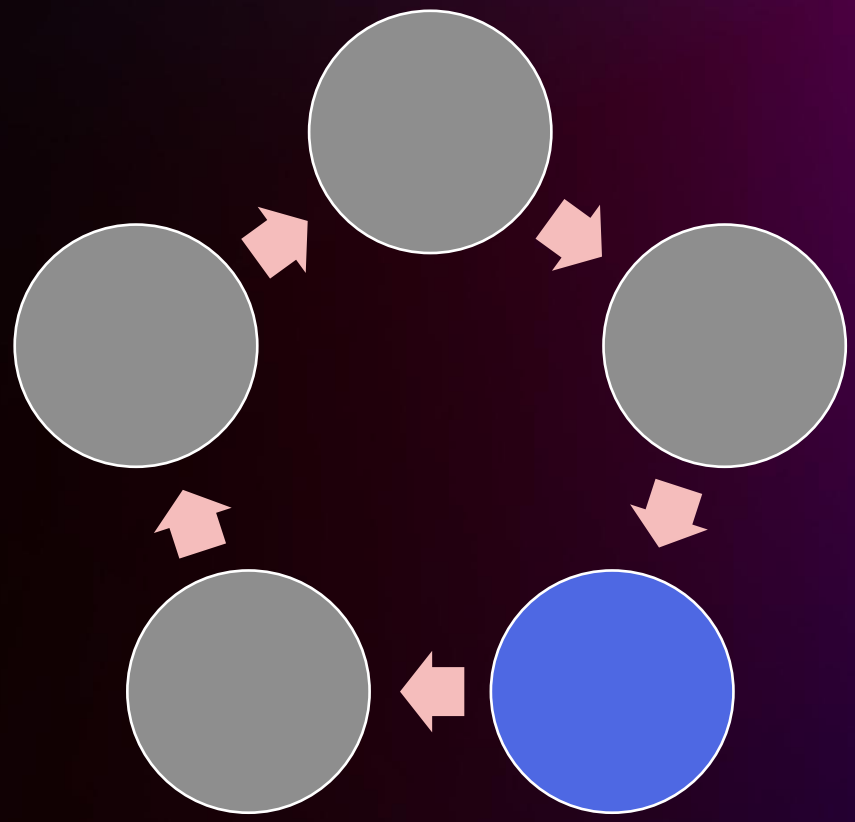
https://go.aws/3hLIMI5

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Posture

- Organization & Identity
  - ☑ Permission Delegation
- Security Operations
  - → Incident Response Testing
  - → Threat Hunting

+ Zero Trust



Refinement

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Incident Response Testing



Event simulation



Tabletop exercise



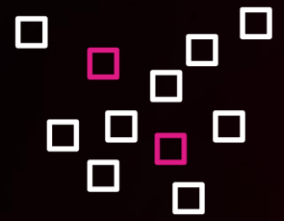
3rd party help

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Threat Hunting



Compromise Indicated



Investigate



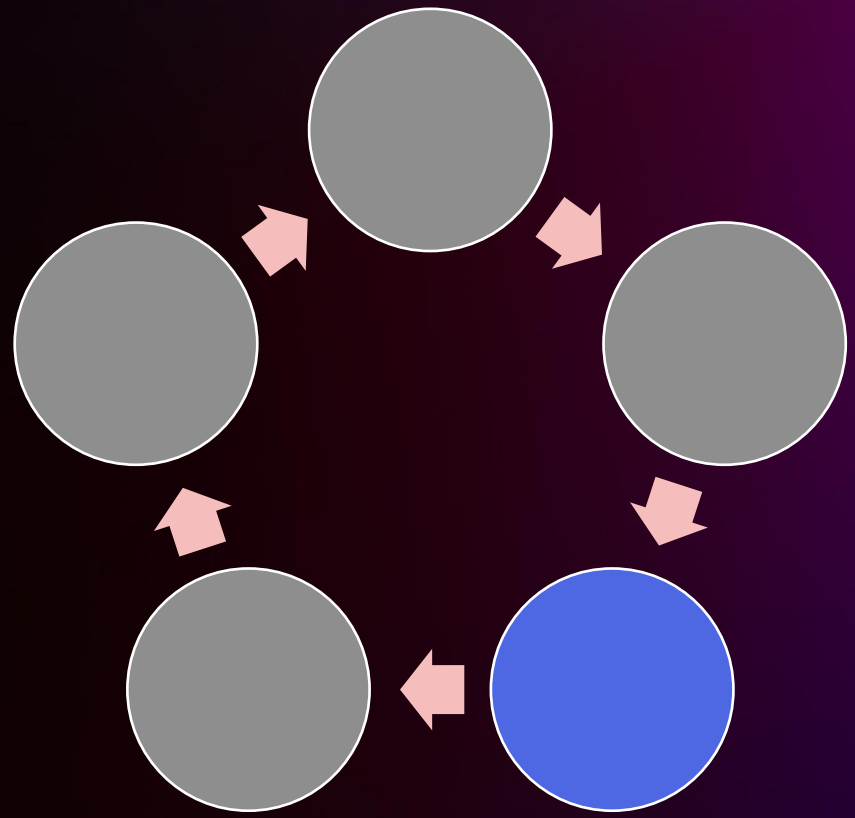
Results

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Posture

- Organization & Identity
  - ☑ Permission Delegation
- Security Operations
  - ☑ Incident Response Testing
  - ☑ Threat Hunting

→ Zero Trust

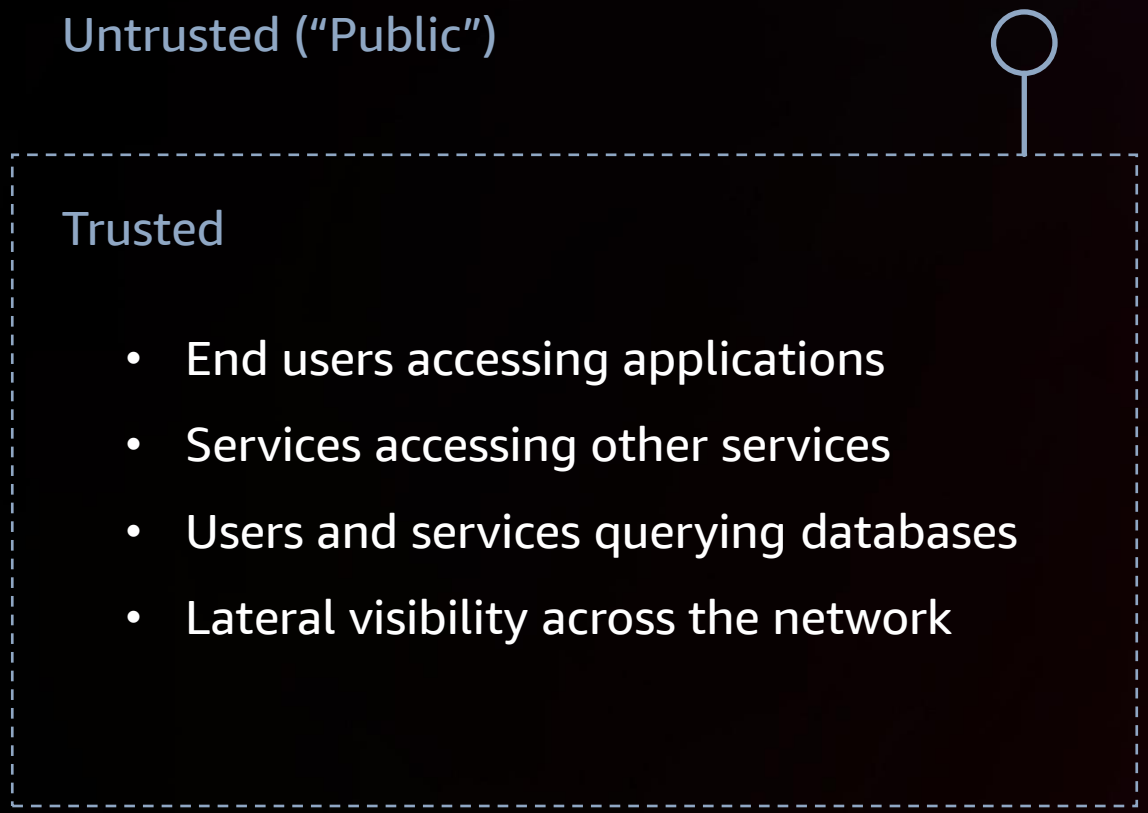


Refinement

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Zero Trust



- Identity
- Authentication
- Authorization
- Auditing
- Access Rules
- Anomalous Behavior Detection
- more…

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Zero Trust

External

Internal

- Users, services, devices all have identity
- Every request authenticated & authorized
- Network is tightly segmented with controlled traffic flows

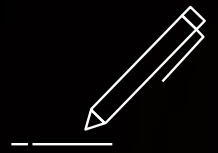
- Identity
- Authentication
- Authorization
- Auditing
- Access Rules
- Anomalous Behavior Detection
- more…

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Zero Trust by AWS



Security of APIs not dependent on network reachability



TLS + Sigv4 secure requests regardless of network



Every request has permissions verified



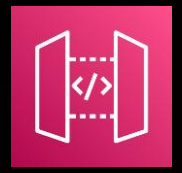
Services use Service-Linked Roles to talk to other services



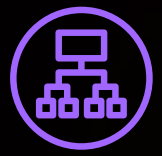
All access is auditable with CloudTrail

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sustaining – Zero Trust with AWS



API Gateway authorization with IAM for internal endpoints



OIDC authorization for Application Load Balancers



Network micro-segmentation with VPCs, subnets, security groups



VPC Endpoints with endpoint policies

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security at Key Stages of Growth

Prototyping

Organization & Identity

Properly Configured Account

Per-User Access

Security Operations

Audit Logging

Initial Threat Detection

Scaling Up

Organization & Identity

Environment Isolation

Central Identities

Credential Rotation

Periodic Access Analysis

Security Operations

Centralized Logging

Foundational Reporting

Managed Monitoring

Compliance Preparation

Scaling Out

Organization & Identity

Security Invariants

Data Perimeters

Automated Accounts

Security Operations

Security Team & Tooling

Security Guardians

Incident Response Playbooks

Compliance Certification

Sustaining

Organization & Identity

Permission Delegation

Zero Trust

Security Operations

Incident Response Testing

Threat Hunting

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Jay Michael
jbako@amazon.com

Faisal Farooq
faifar@amazon.com



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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.