

AWS
re:Invent



SEC314

Security best practices the AWS Well-Architected way

Ben Potter
Security Lead, Well-Architected
AWS

Agenda

Security foundations

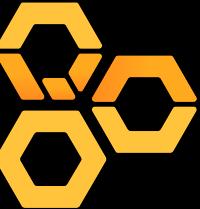
Identity and access management

Detection

Infrastructure protection

Data protection

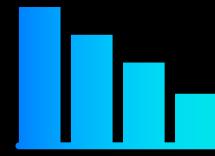
Incident response



Why AWS Well-Architected Framework?



Build and deploy faster



Lower or mitigate risks



Make informed decisions



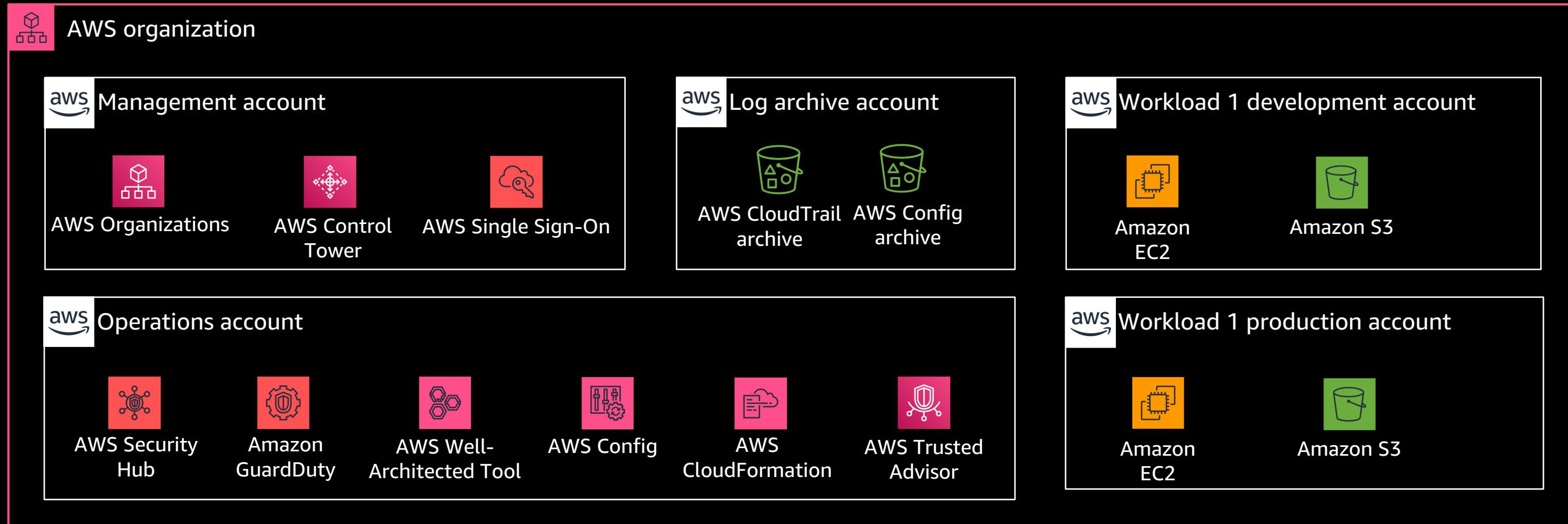
Learn AWS best practices

Security foundations



Key best practices: Security foundations

- Separate workloads using accounts
- Secure AWS account

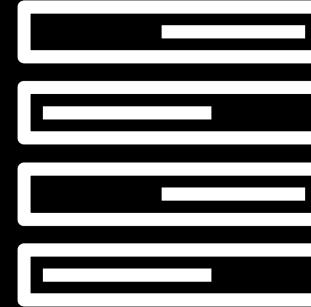


Service control policy guardrails

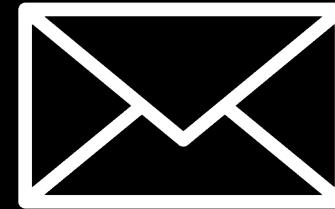
```
{  
    "version": "2012-10-17",  
    "Statement": {  
        "Effect": "Deny",  
        "Action": [  
            "iam>CreateAccessKey",  
            "iam>CreateUser"  
        ],  
        "Resource": "*"  
    }  
}
```

Key best practices: Security foundations

- Identify and prioritize risks using a threat model
- Keep up to date with security threats and recommendations



CVEs
Social media
Forums



Subscribe



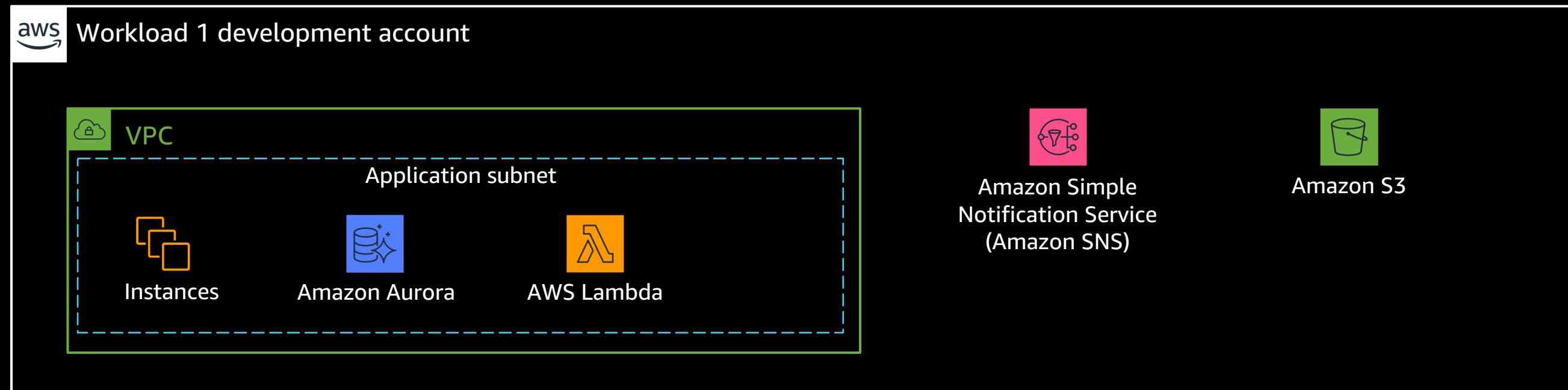
Blogs



AWS Marketplace

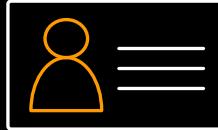
<https://aws.amazon.com/blogs/>
<https://aws.amazon.com/security>
<https://cve.mitre.org/>

Starting architecture



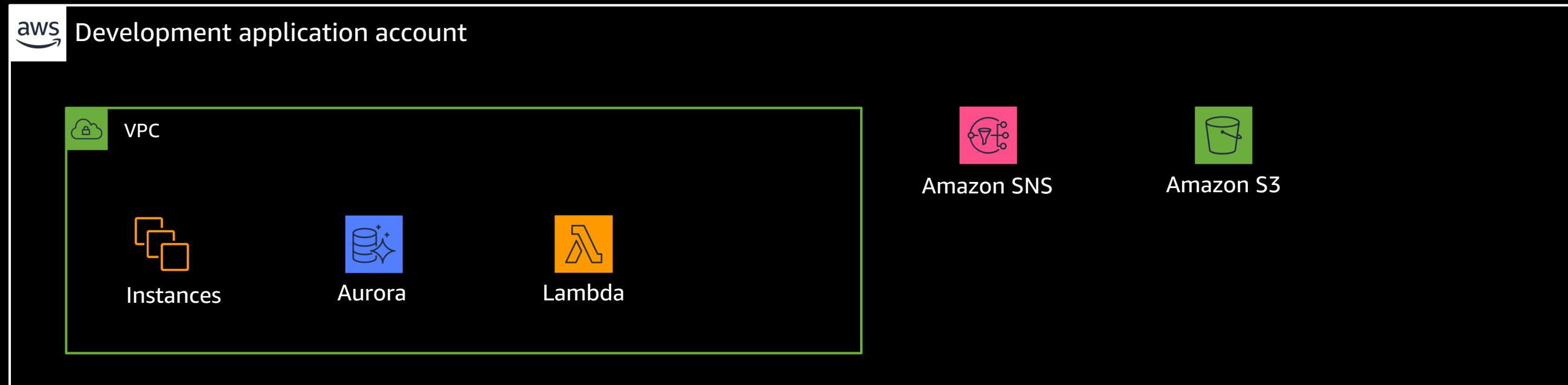
Identity and access management

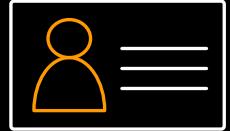




Key best practices: Identities

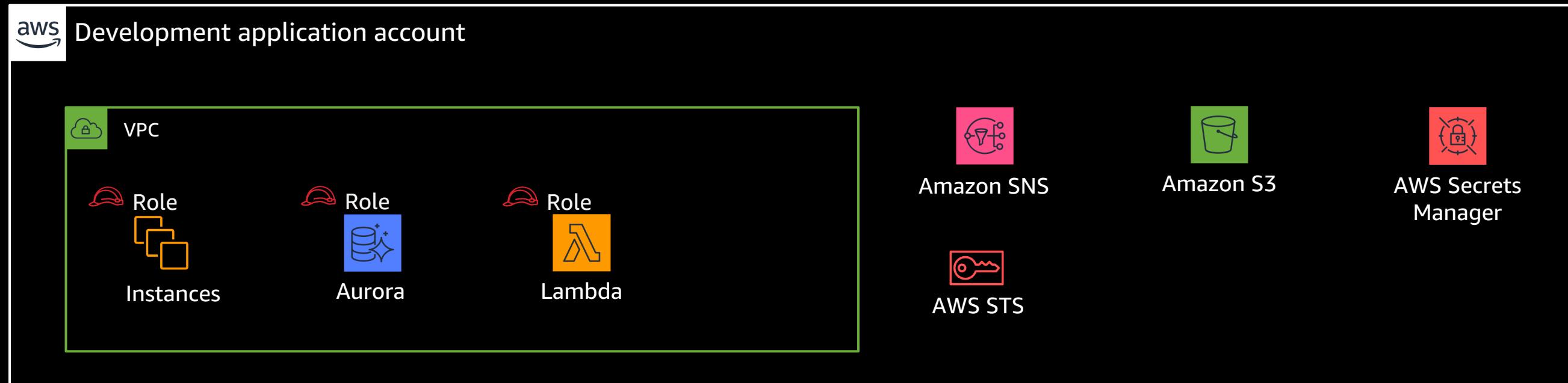
- Rely on a centralized identity provider
- Use strong sign-in mechanisms

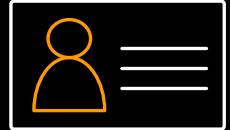




Key best practices: Identities

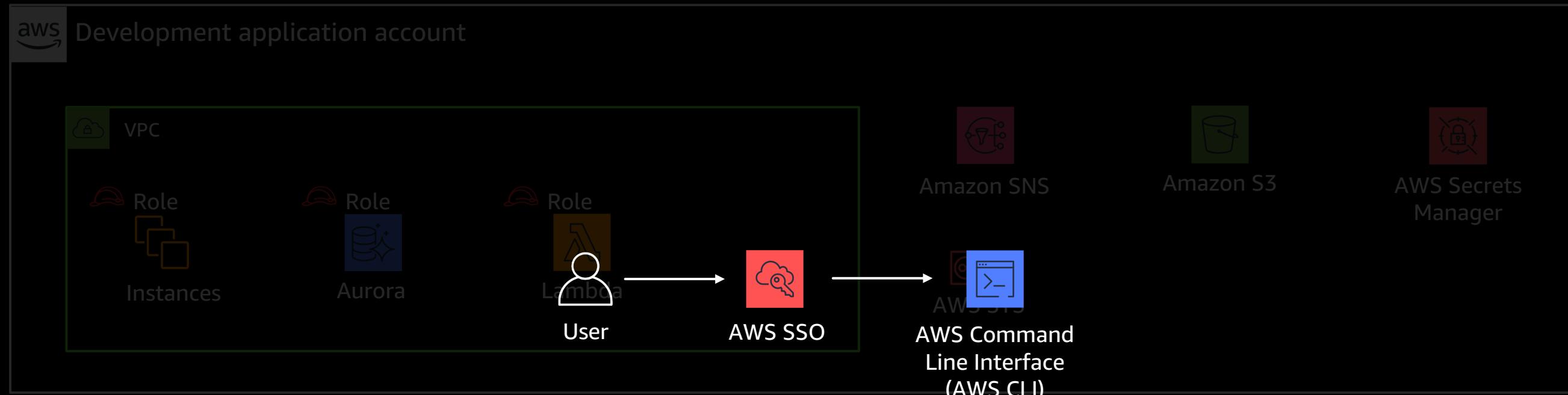
- Use temporary credentials
- Store and use secrets securely

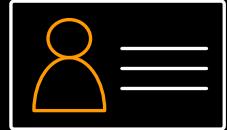




Key best practices: Identities

- Use temporary credentials
- Store and use secrets securely



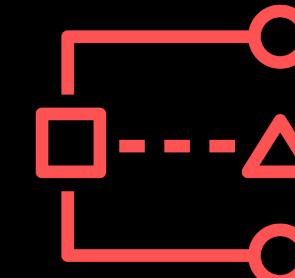


Key best practices: Permissions

- Share resources securely
- Analyze public and cross-account access
- Grant least-privileged access



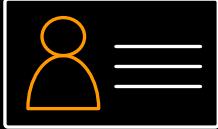
AWS Resource Access Manager



AWS Identity and Access Management (IAM) access analyzer

Active findings						
	Finding ID	Resource	External principal	Condition	Access level	Updated
<input type="checkbox"/>	9b90c68...	KMS Key 08385788-f529-487...	AWS Account [REDACTED]	-	Write, Permissions	5 minutes ago
<input type="checkbox"/>	628aa53...	KMS Key 08385788-f529-487...	AWS Account [REDACTED]	-	Permissions, Write	5 minutes ago
<input type="checkbox"/>	5067d32f...	IAM Role vue-201810291353...	Federated User cognito-identity.amazonaws.com	-	Write	5 minutes ago
<input type="checkbox"/>	6ed6585...	IAM Role helloworld-2018102...	Federated User cognito-identity.amazonaws.com	-	Write	5 minutes ago
<input type="checkbox"/>	58bb820...	IAM Role vue-201810291353...	Federated User cognito-identity.amazonaws.com	-	Write	5 minutes ago
<input type="checkbox"/>	8761842...	IAM Role test-201810261411...	Federated User cognito-identity.amazonaws.com	-	Write	5 minutes ago
<input type="checkbox"/>	a0fd4d45...	IAM Role AwsSecurityNacun...	AWS Account [REDACTED]	-	Write	5 minutes ago
<input type="checkbox"/>	c0a8871...	IAM Role GatedGardenAudit	AWS Account [REDACTED]	-	Write	5 minutes ago

Least-privileged: IAM policy condition keys



```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AllowS3ActionsThroughAthena",  
      "Effect": "Allow",  
      "Principal": {"AWS": "arn:aws:iam::111122223333:role/examplerole"},  
      "Action": [  
        "s3:GetBucketLocation",  
        "s3:GetObject",]  
      ],  
      "Resource": [  
        "arn:aws:s3:::doc-example-bucket",  
        "arn:aws:s3:::doc-example-bucket/prefix*"]  
    },  
    {"Condition": {  
      "ForAnyValue:StringEquals": {  
        "aws:CalledVia": [  
          "athena.amazonaws.com"]}}}]}
```

Blog post:
<https://amzn.to/3d65Ef1>

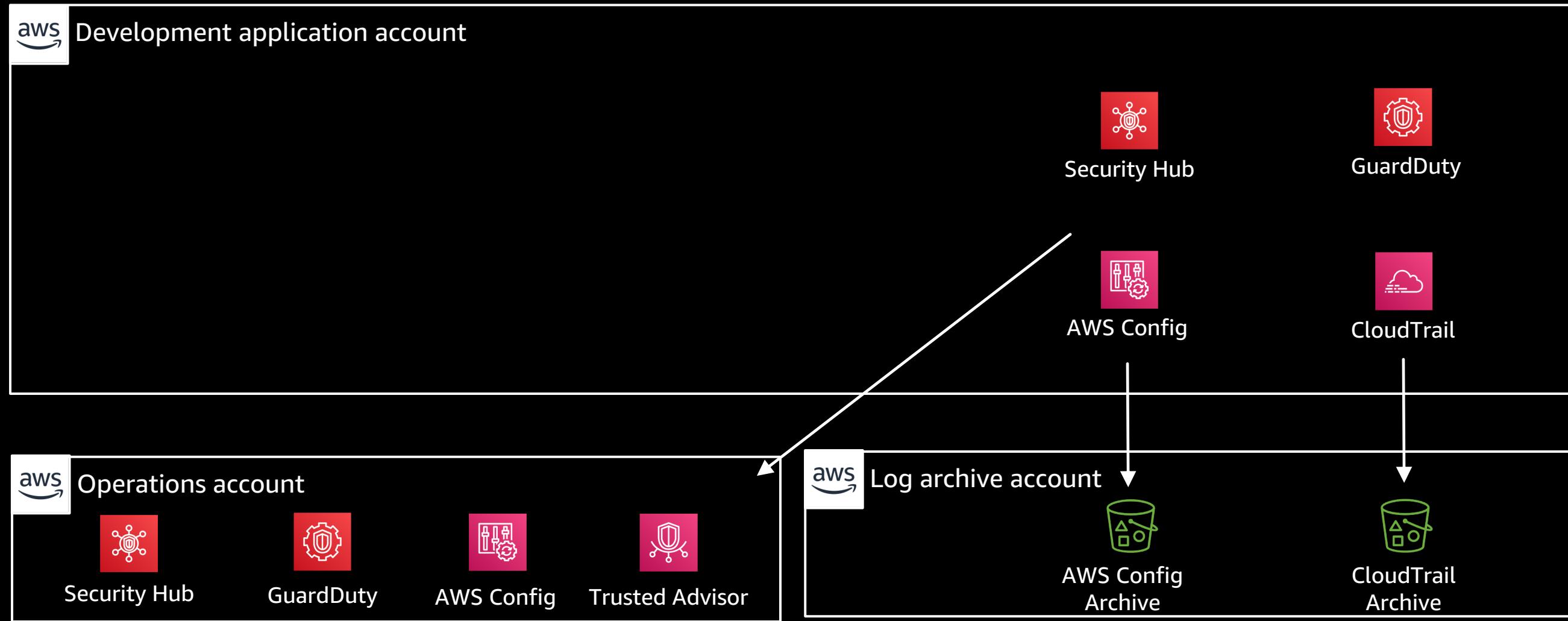
Detection



Key best practices: Detection



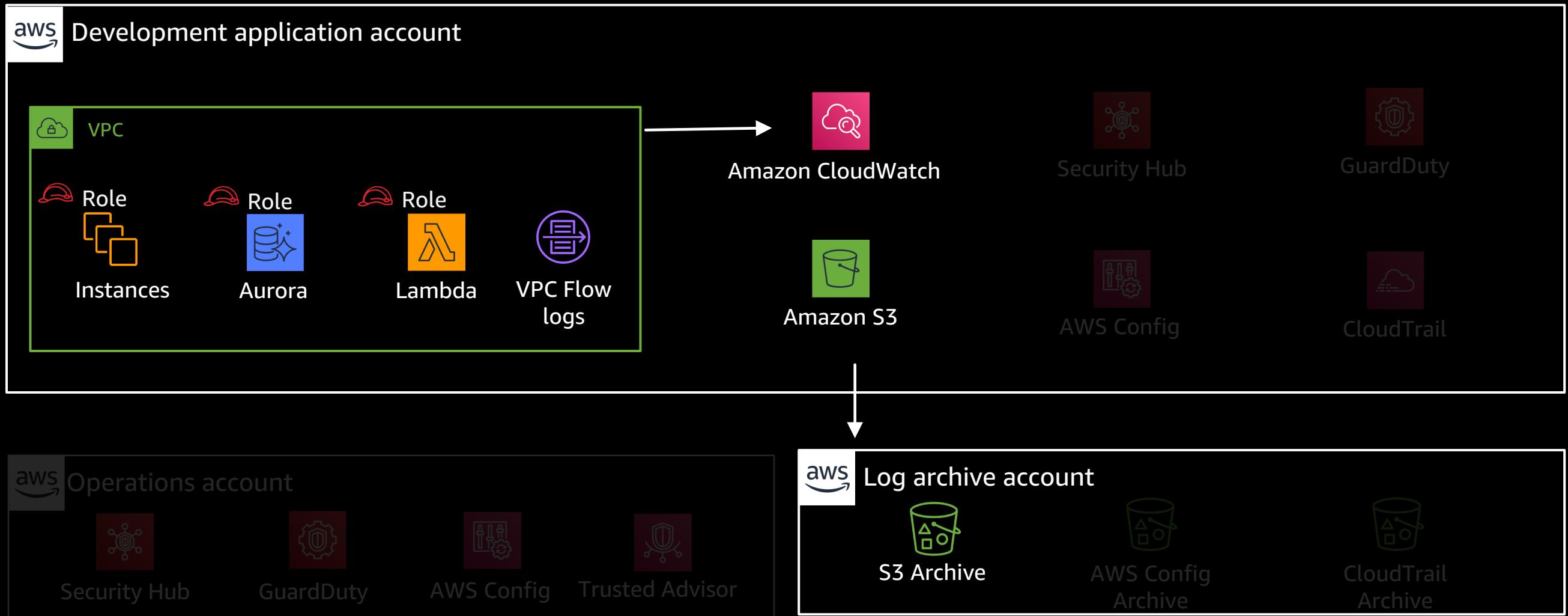
- Configure service and application logging
- Analyze logs, findings, and metrics centrally



Key best practices: Detection



- Configure service and application logging
- Analyze logs, findings, and metrics centrally



Security Hub foundational checks



ⓘ AWS Config is not enabled on some accounts
AWS Config is required for Security Hub's security checks. Review remediation steps for the related findings for CIS 2.5 if you recently enabled AWS Config; note that it can take up to 12 hours for Security Hub to detect the change.

Introducing AWS Foundational Security Best Practices X

The AWS Foundational Security Best Practices standard is a set of automated security checks that detect when AWS accounts and deployed resources do not align with security best practices. The standard is defined by AWS security experts. This curated set of controls helps improve a customer's security posture in AWS, and covers AWS's most popular and foundational services. Security Hub recommends that customers enable this standard in all accounts and regions.

New controls	Services covered	AWS resources
31	18	15

Cancel **Enable standard**

3. AMIs that are generating the most findings 0 Amazon Macie
Open the Macie console

<https://amzn.to/3j8TTXS>

Key best practices: Detection



- Implement actionable security events



Amazon Chime

GuardDuty Helper (Webhook)

GuardDuty detected instance i-1234567890abcdef0 is performing outbound portscan and requires further investigation. Please investigate using runbook EC2 outbound portscan and escalate as per escalation process. Ask @secops if you need help at any time.



Conformance packs

AWS Config > Conformance packs > Deploy conformance pack

Step 1
Specify template

Step 2
Specify conformance
pack details

Step 3
Review and deploy

Specify template

Template details

Conformance pack template

Every conformance pack is based on a template. A template is a YAML file that contains configuration information about AWS accounts and regions where you want to deploy AWS Config rules and remediation actions.

Use sample template

Template is ready

Sample template

Select a sample templates

This collection of sample templates will help you get started with conformance packs and quickly build your own template.

Operational Best Practices for AWS Well Architected Security Pillar ▾

To view the sample templates, see [Conformance Pack Sample Templates](#).

Cancel

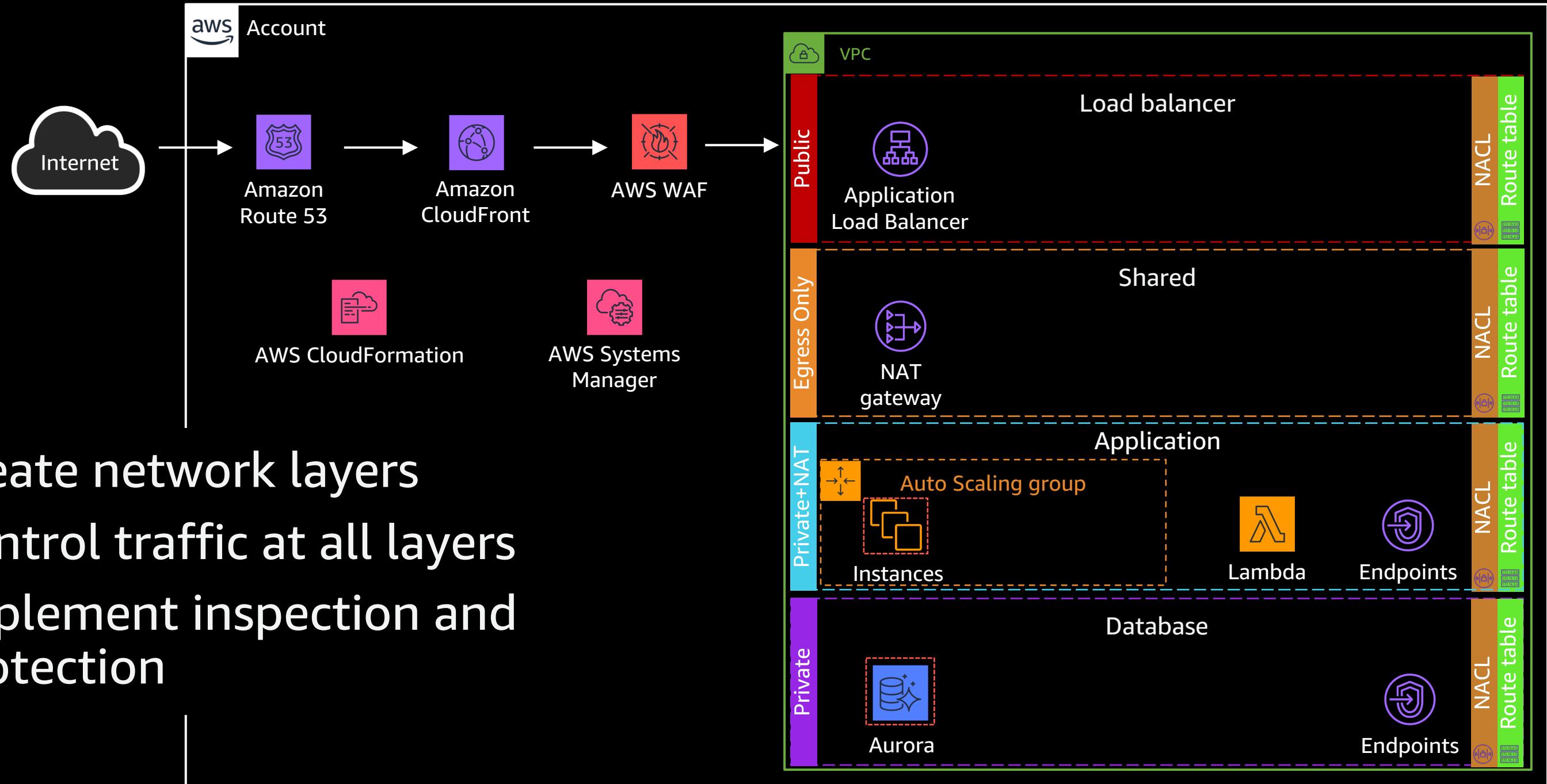
Next

<https://amzn.to/2GzUcw8>

Infrastructure protection

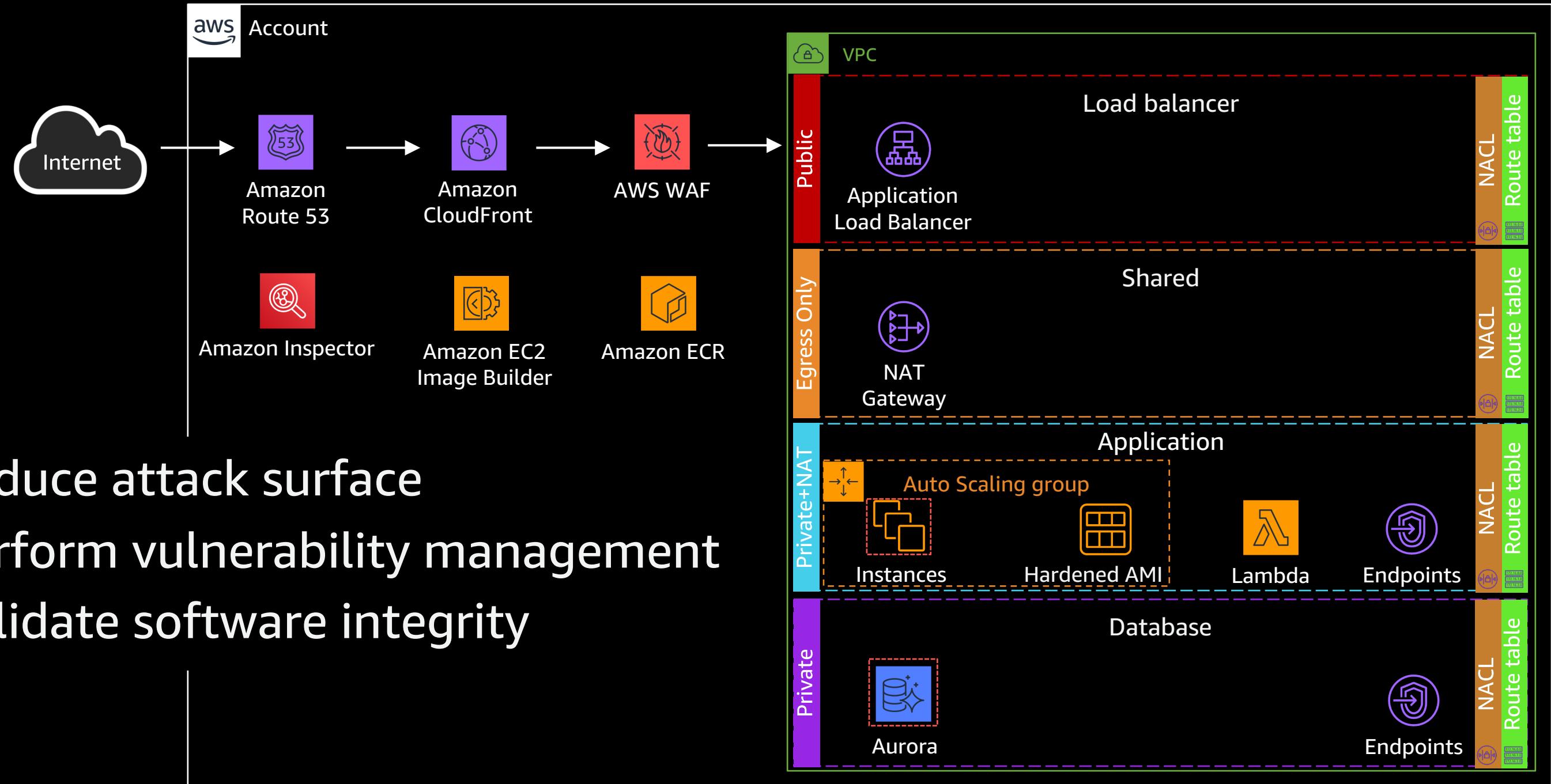


Key best practices: Infrastructure protection



- Create network layers
- Control traffic at all layers
- Implement inspection and protection

Key best practices: Infrastructure protection



- Reduce attack surface
- Perform vulnerability management
- Validate software integrity

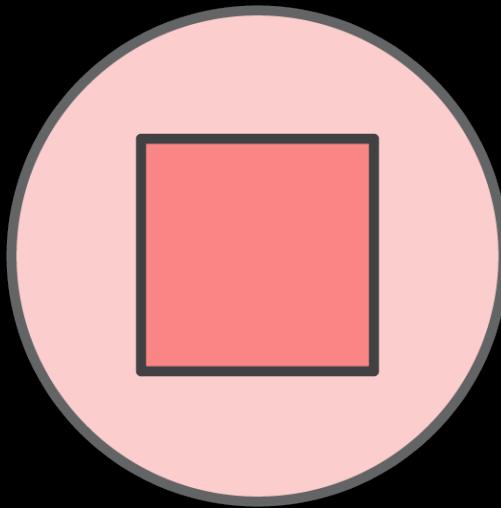
Data protection



Keep people away from data



- Don't store
- Don't grant



- Encrypt
- Mask
- Tokenize



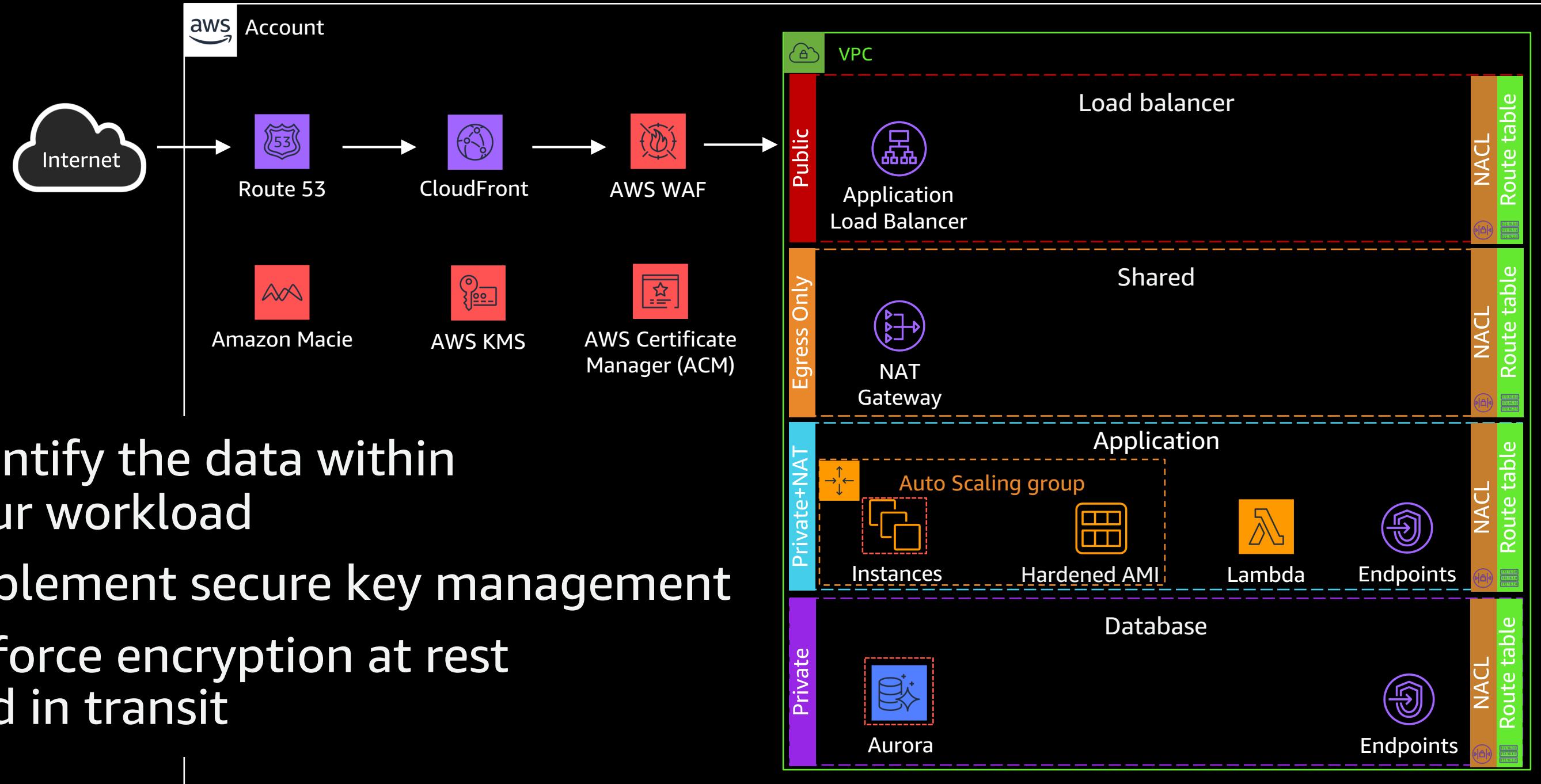
- Isolate
- Tooling
- Eliminate
human access



- Operations
as code
- Version
control



Key best practices: Data protection



- Identify the data within your workload
- Implement secure key management
- Enforce encryption at rest and in transit

Enable default encryption



Default encryption

This property does not affect existing objects in your bucket.

- None
- AES-256
 - Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- AWS-KMS
 - Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

[Cancel](#) [Save](#)

aws Services Resource Groups ⚙

Settings

EBS Storage

Encryption [\(i\)](#) Always encrypt new EBS volumes

Default encryption key [\(i\)](#) alias/aws/ebs [Change the default key](#)

[Cancel](#) [Save Settings](#)

Incident response





Key best practices: Incident response

- Develop incident management plans

Scenario title:

Malicious IP action

Scenario description:

An API was invoked from a known malicious IP address

Data to gather:

CloudTrail + application logs

Investigation steps:

CloudTrail history of IP, ASN, IP info, created resources

Escalation & communication:

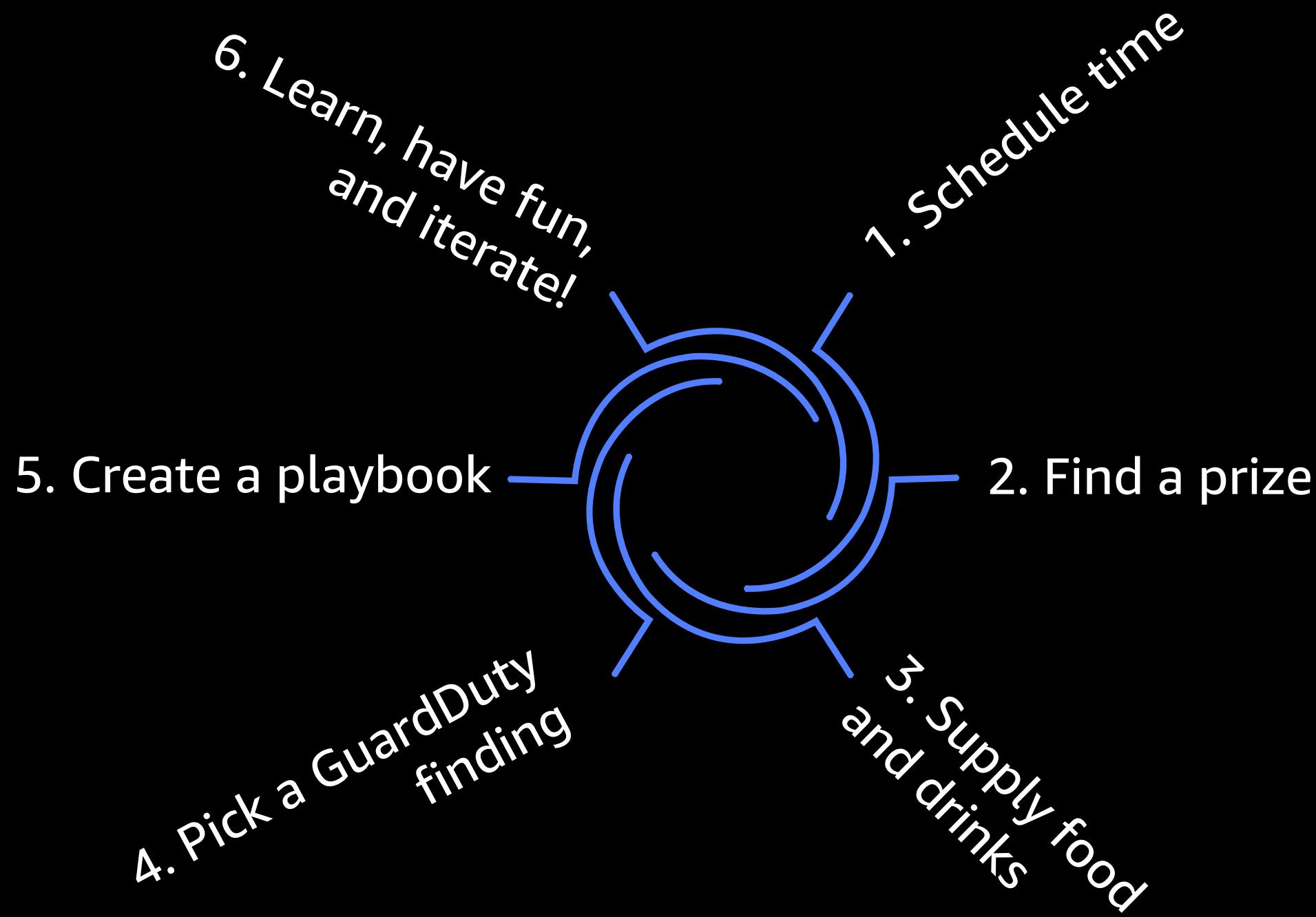
High severity infosec ticket

Resolution steps:

Disabled credentials, remove resources

Example runbooks: <https://bit.ly/2WhZvoR>

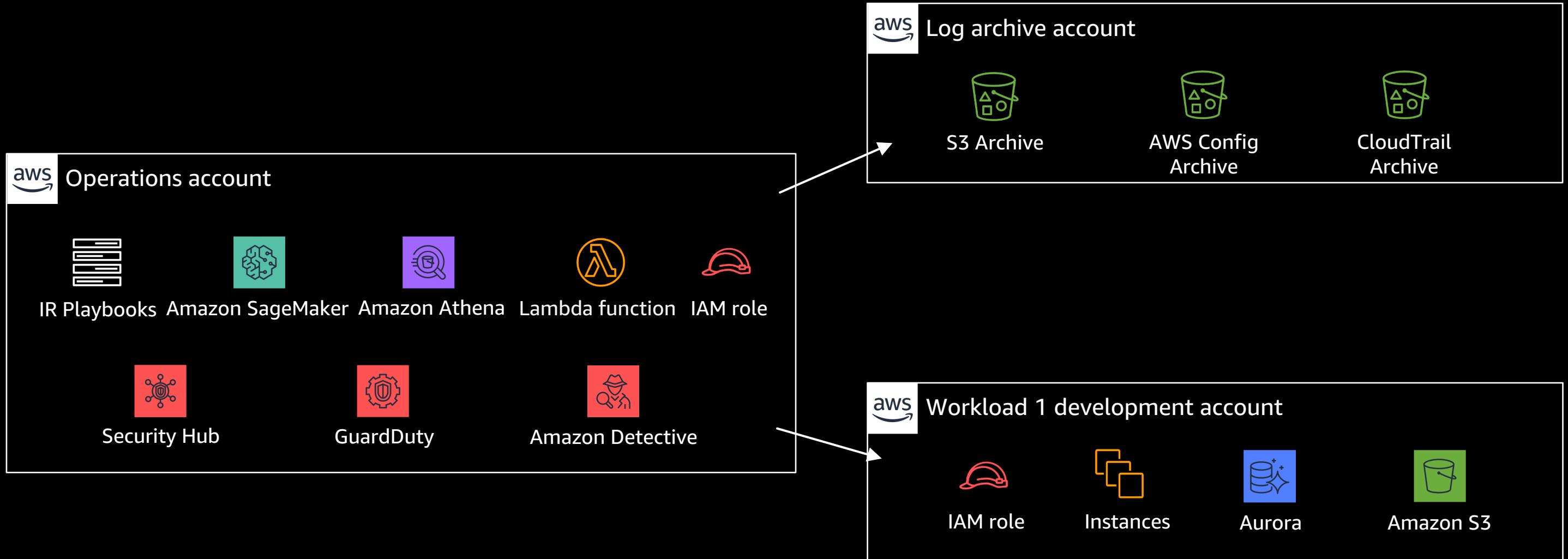
How to run a gameday





Key best practices: Incident response

- Pre-provision access and tools



Well-Architected resources

Main: <https://aws.amazon.com/well-architected/>

Tool: <https://aws.amazon.com/well-architected-tool/>

Labs: <https://www.wellarchitectedlabs.com/>

Solutions: <https://aws.amazon.com/solutions>

Thank you!

Ben Potter

@benji_potter



Please complete
the session survey

