
AWS
re:Invent

SEC314

Security best practices the AWS Well-Architected way

Ben Potter

Security Lead, Well-Architected

AWS

AWS re:Invent

Agenda

Security foundations

Identity and access management

Detection

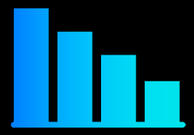
Infrastructure protection

Data protection

Incident response

Why AWS Well-Architected Framework?

Build and deploy faster



Lower or mitigate risks

Make informed decisions

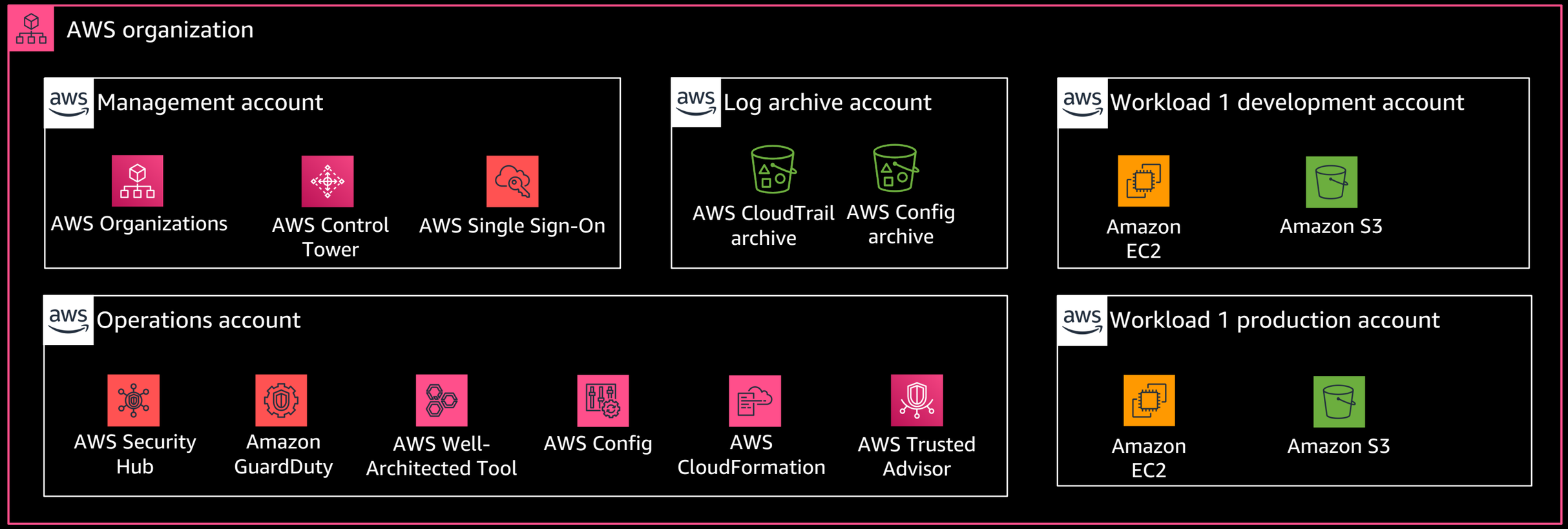
Learn AWS best practices

Security foundations

AWS re:Invent

Key best practices: Security foundations

- Separate workloads using accounts
- Secure AWS account



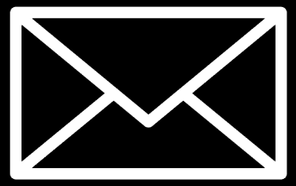
Service control policy guardrails

```
{
    "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



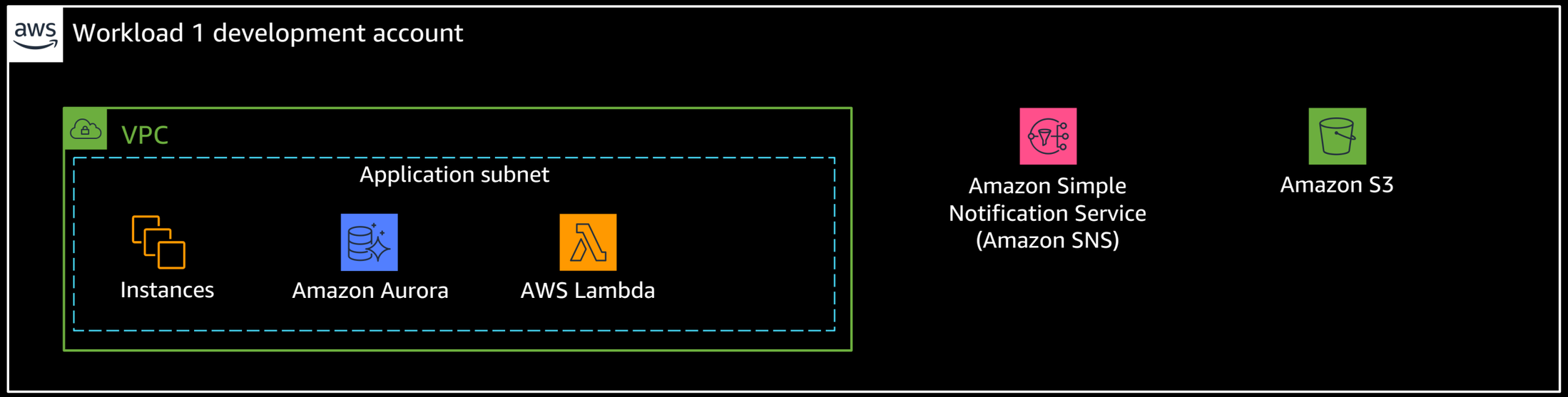
Subscribe

Blogs

AWS Marketplace

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

Starting architecture

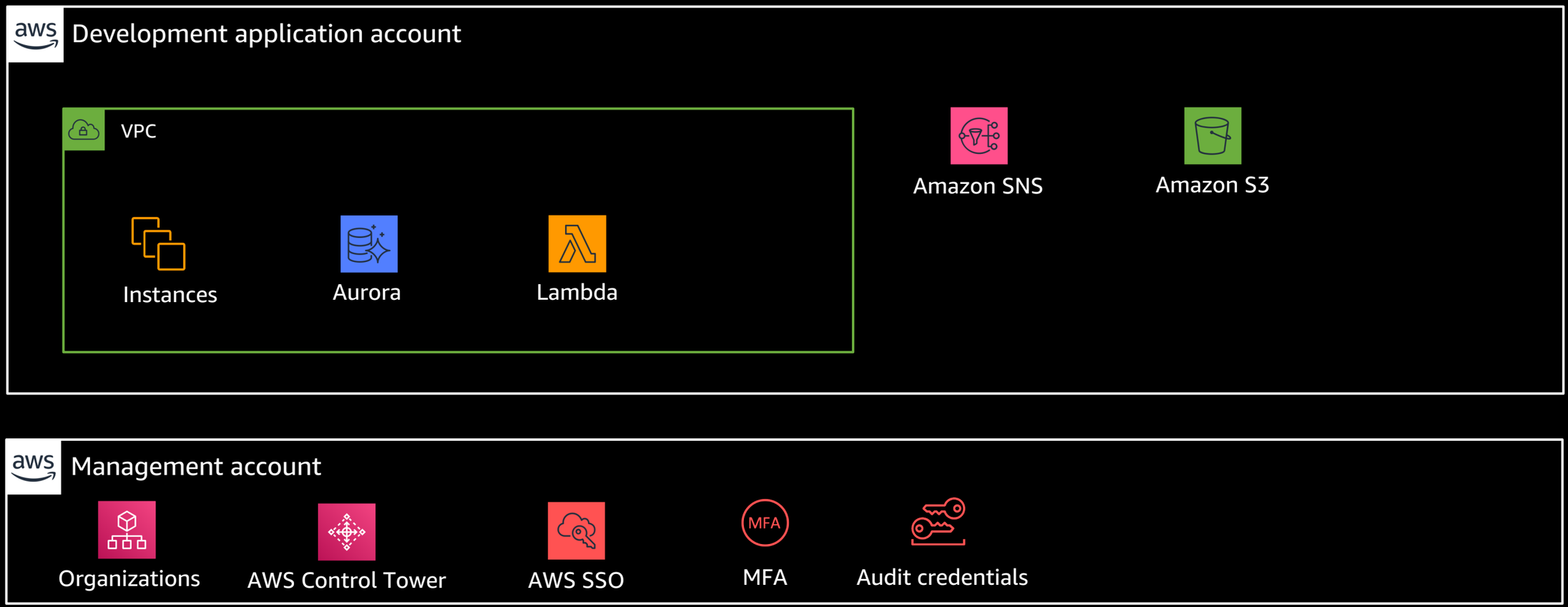


Identity and access management

AWS re:Invent

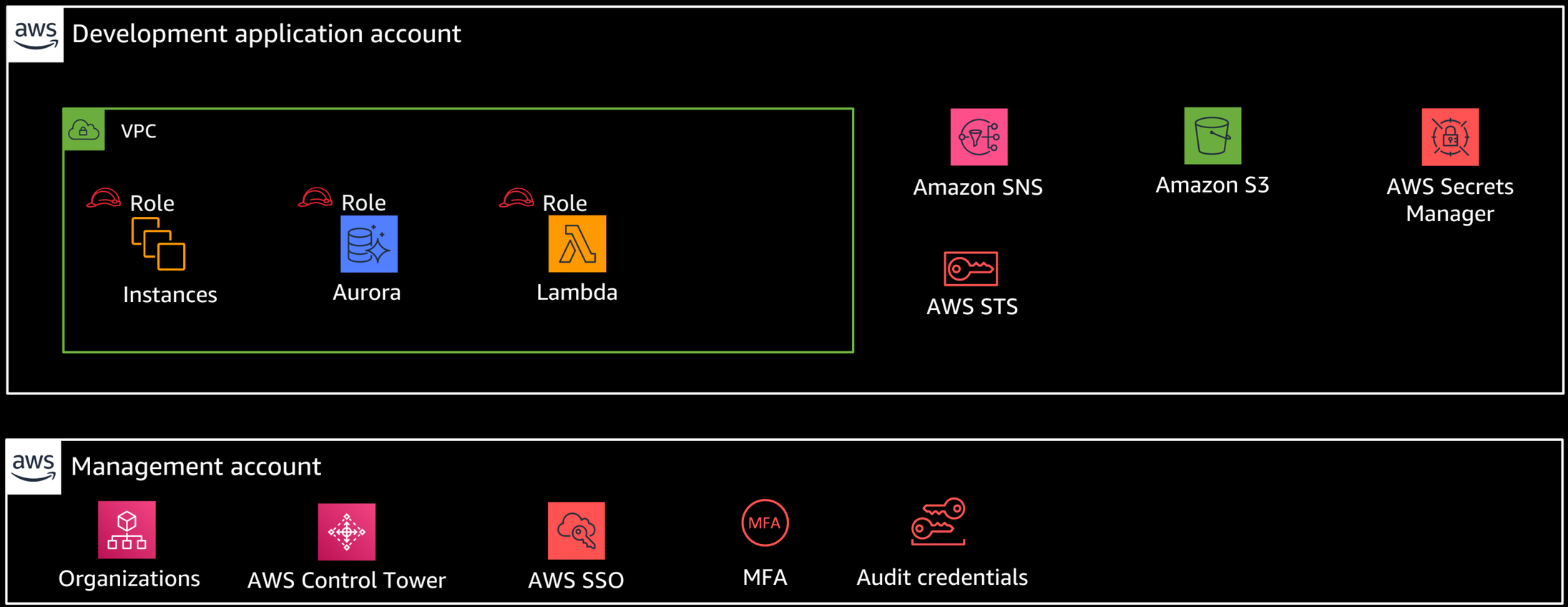
Key best practices: Identities

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



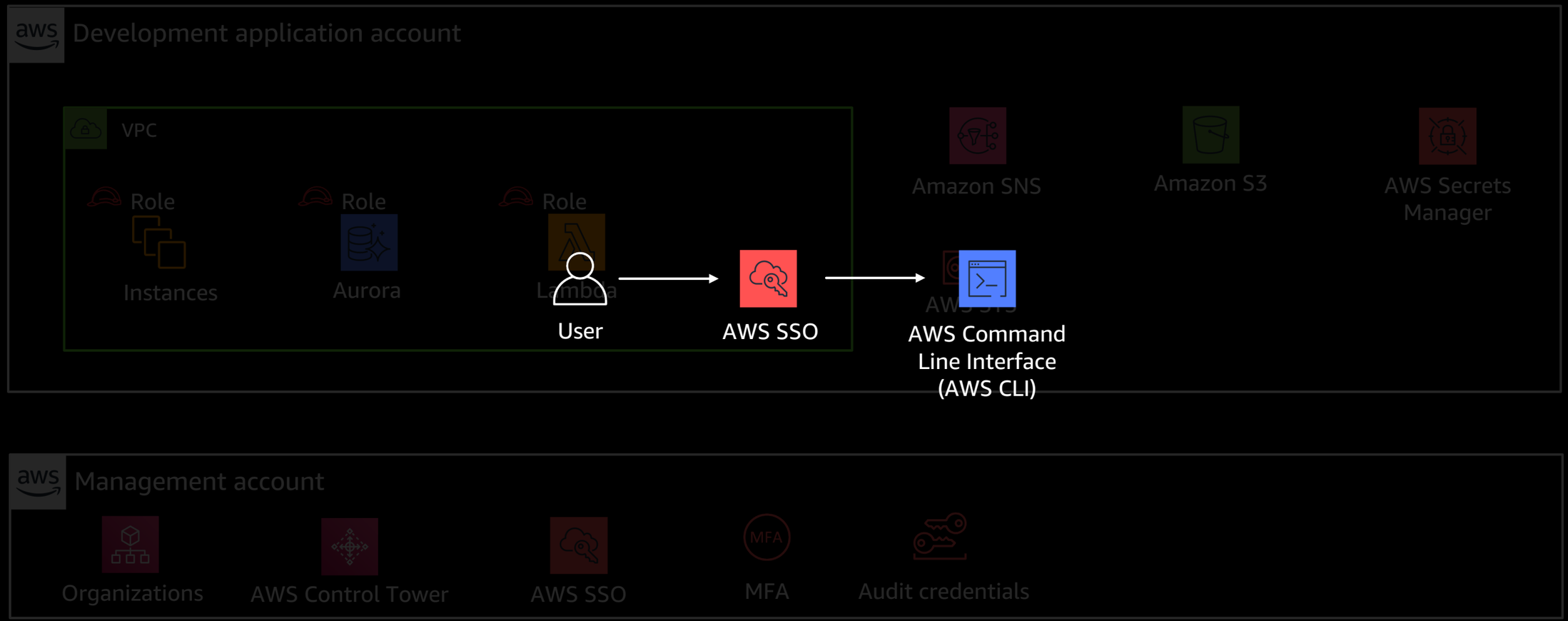
Key best practices: Identities

- Use temporary credentials
- Store and use secrets securely



Key best practices: Identities

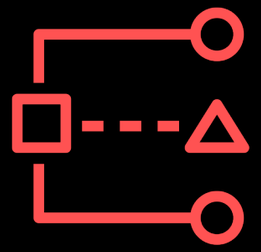
- Use temporary credentials
- Store and use secrets securely



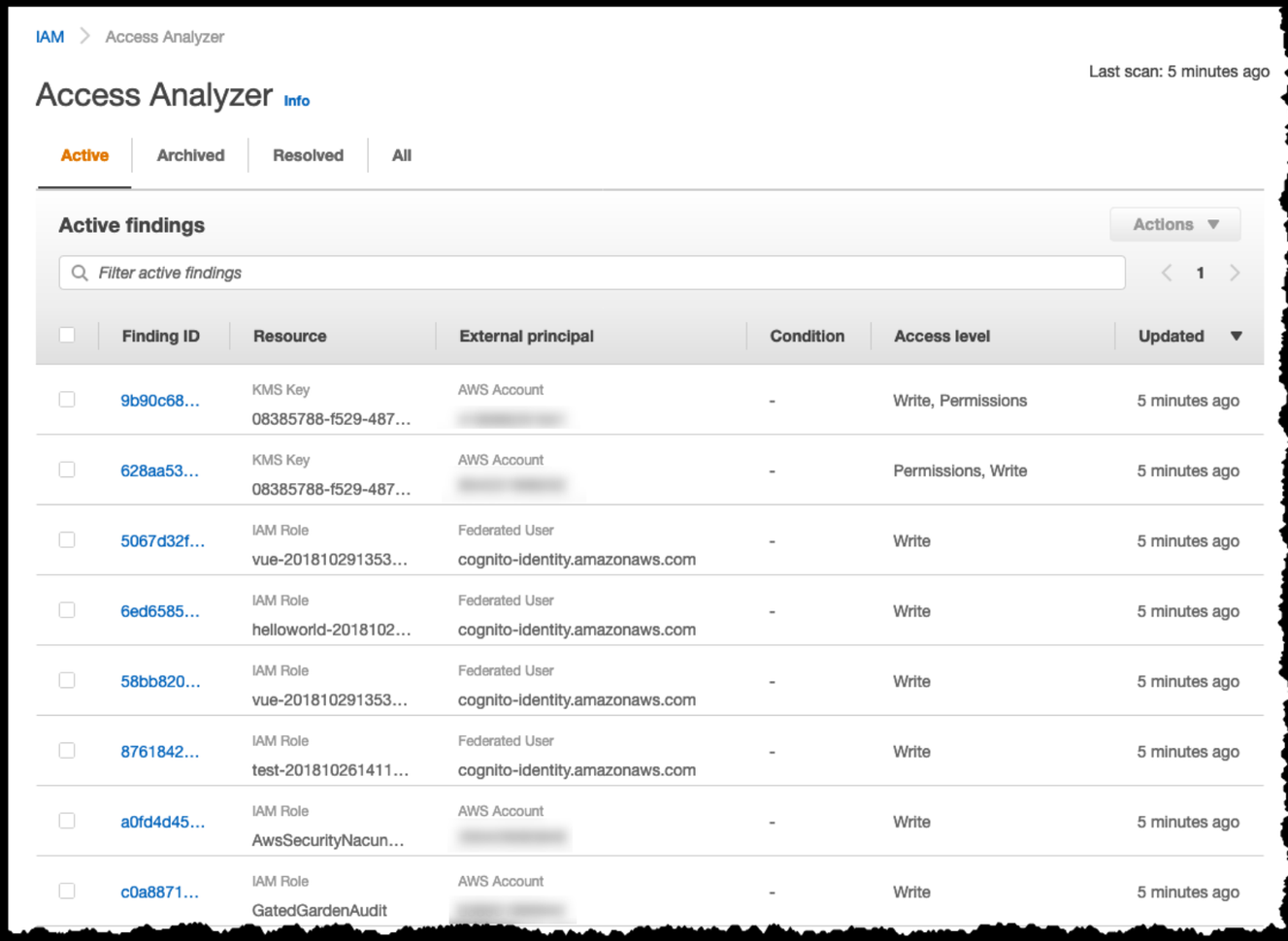
Key best practices: Permissions

- 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



Least-privileged: IAM policy condition keys

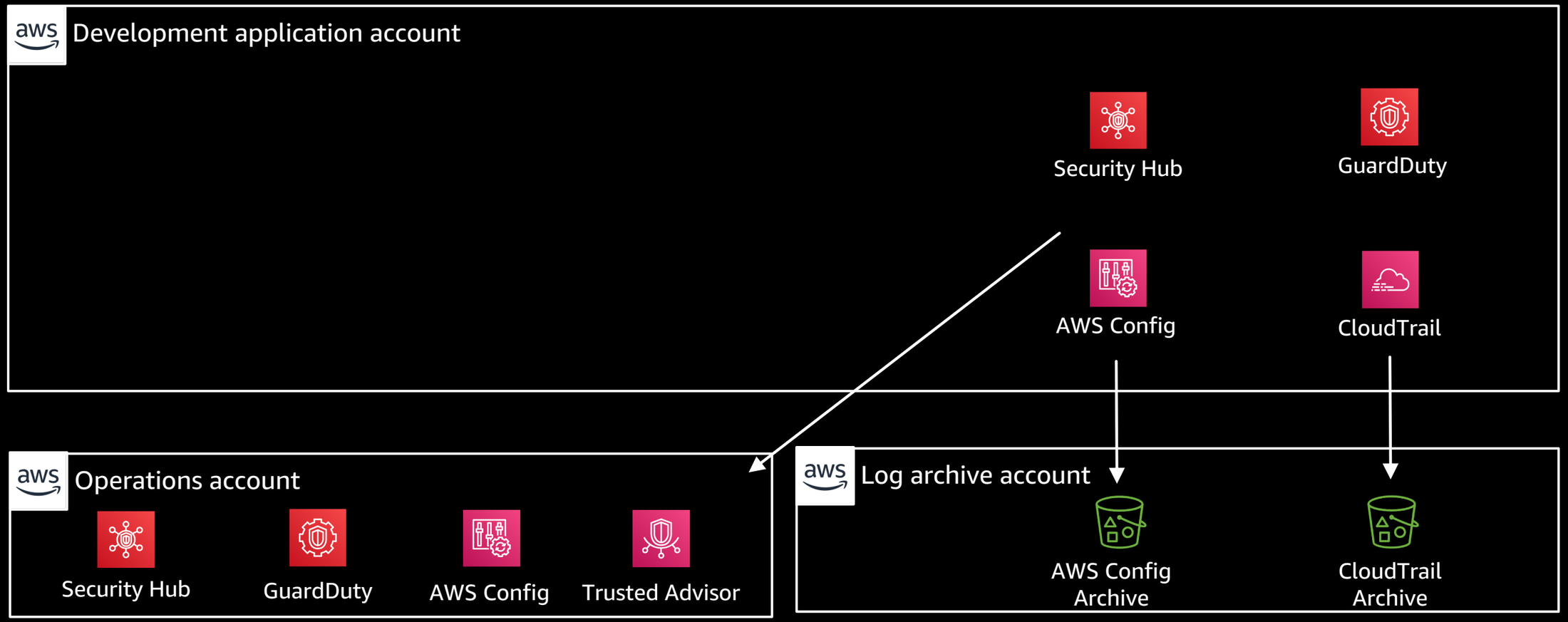
```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Sid": "AllowS3ActionsThroughAthena",
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::111122223333:role/examplerole"},
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",],
      "Resource": [
        "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

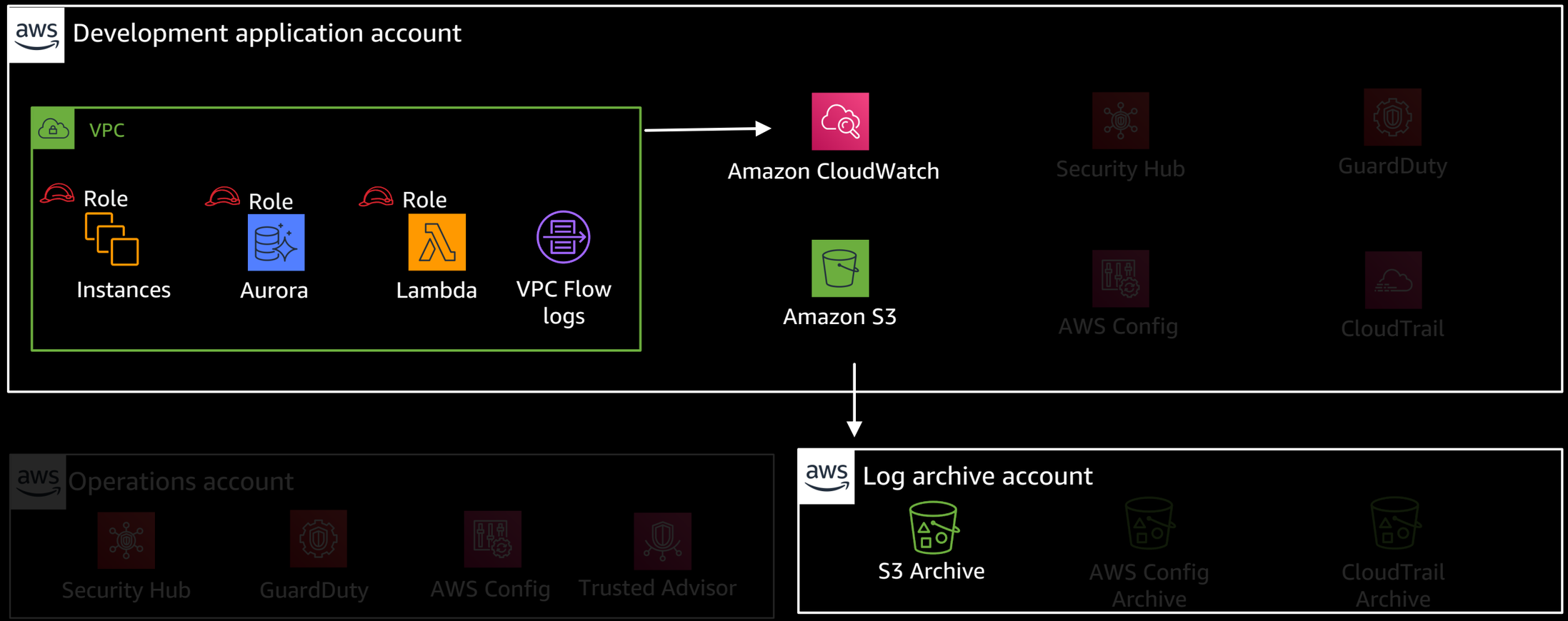
Key best practices: Detection

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

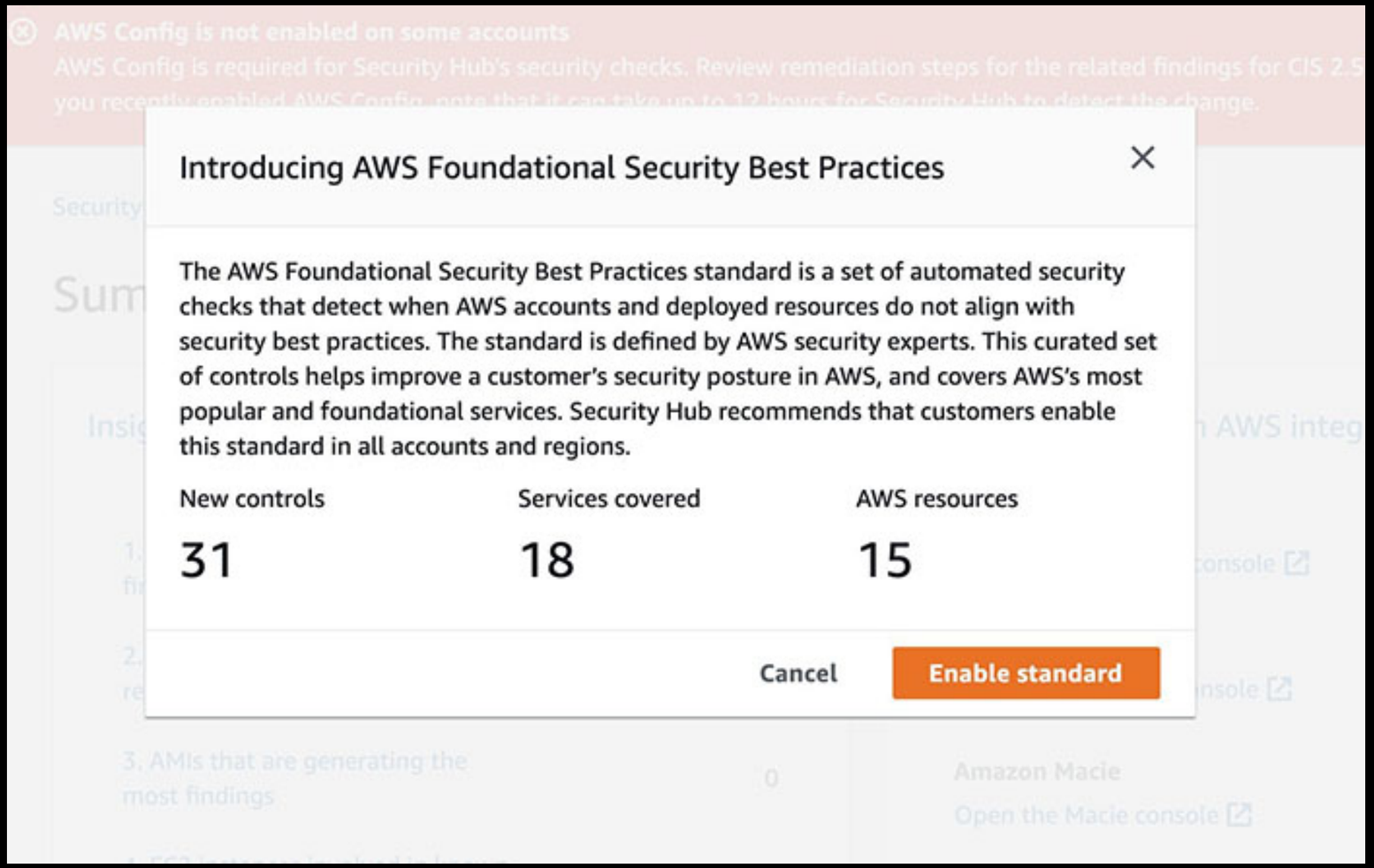


Key best practices: Detection

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



Security Hub foundational checks



https://amzn.to/3j8TTXS

Key best practices: Detection

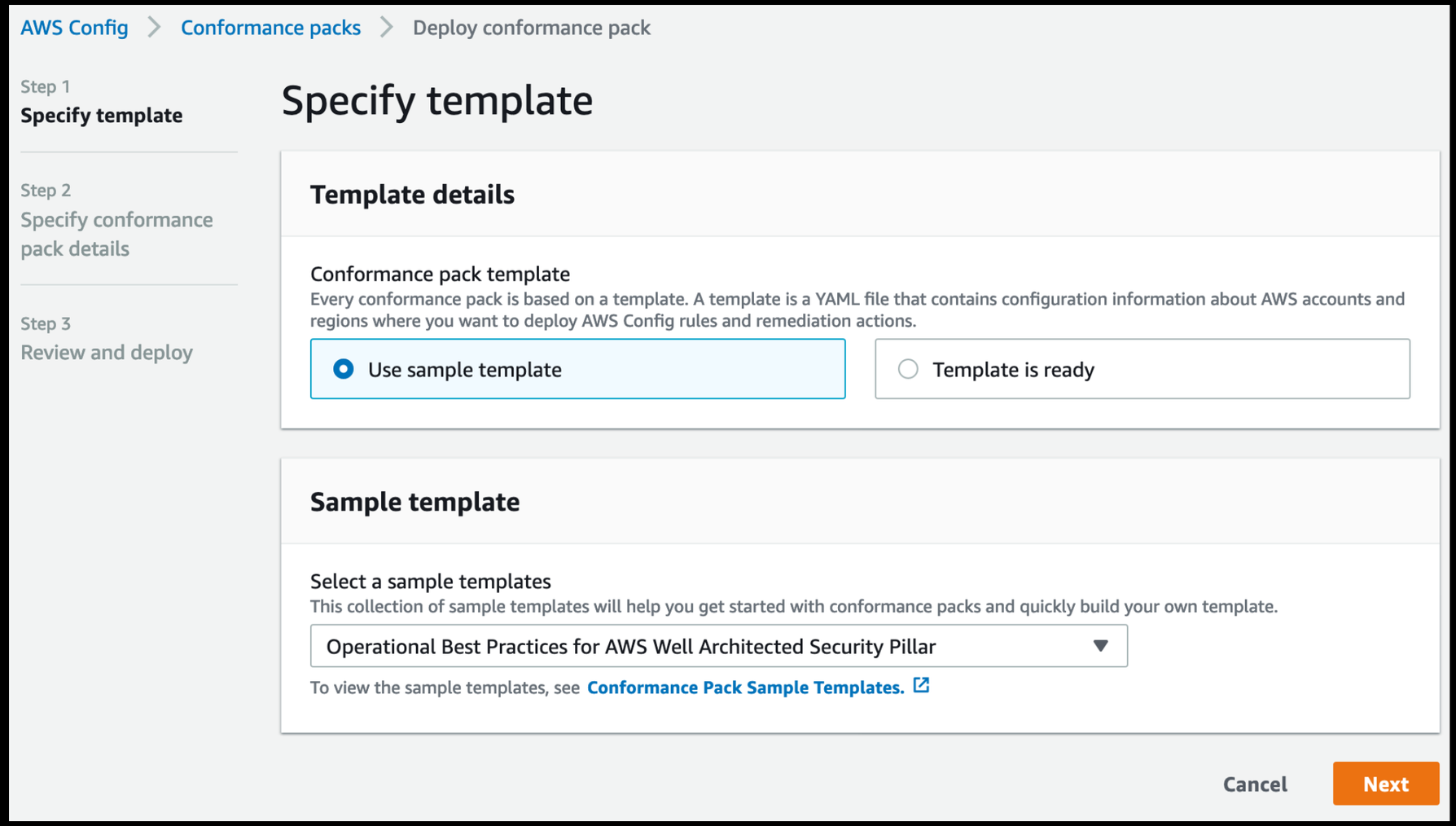
- Implement actionable security events

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

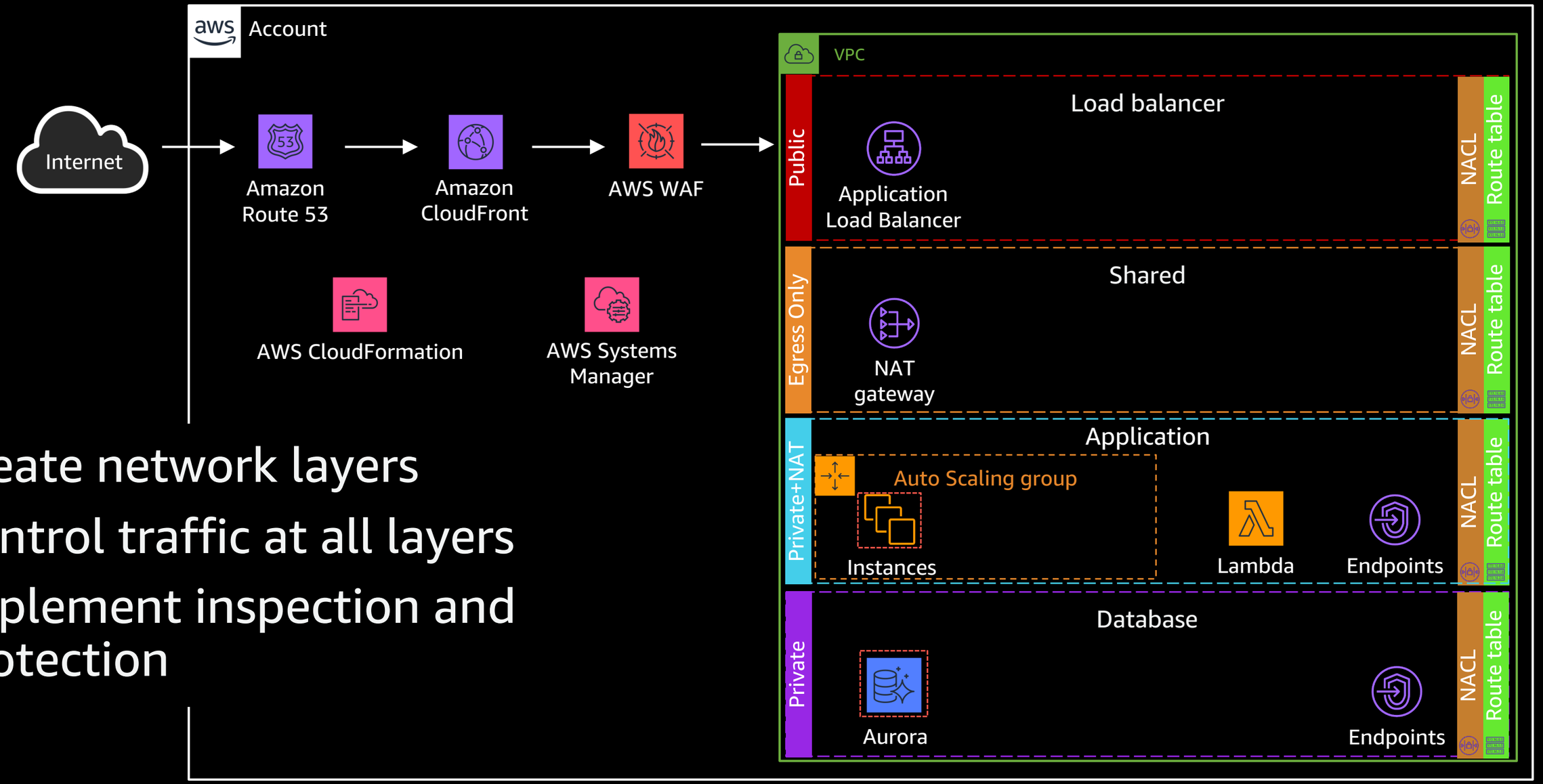


https://amzn.to/2GzUcw8

Infrastructure protection

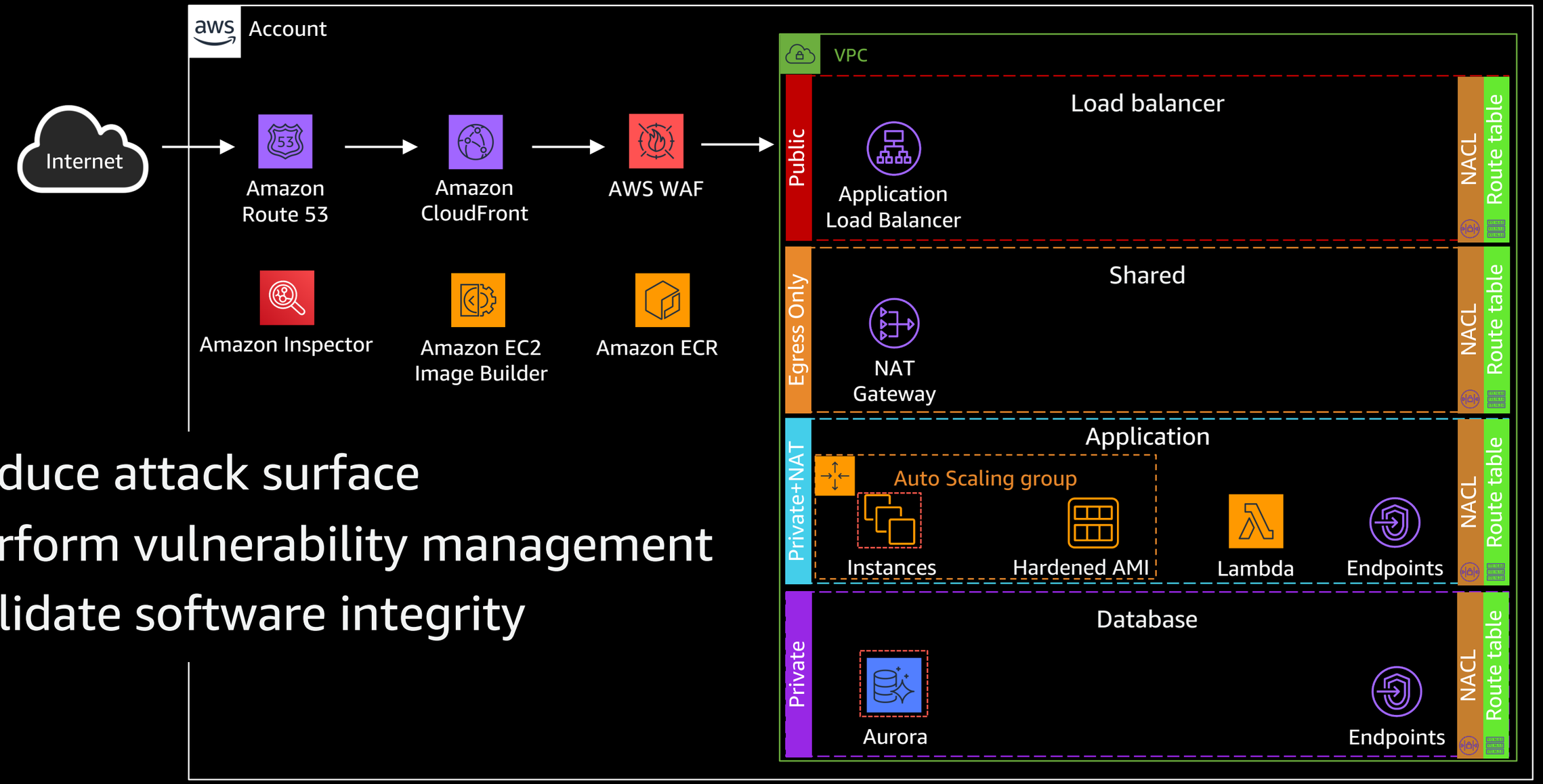
AWS re:Invent

Key best practices: Infrastructure protection



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

Key best practices: Infrastructure protection



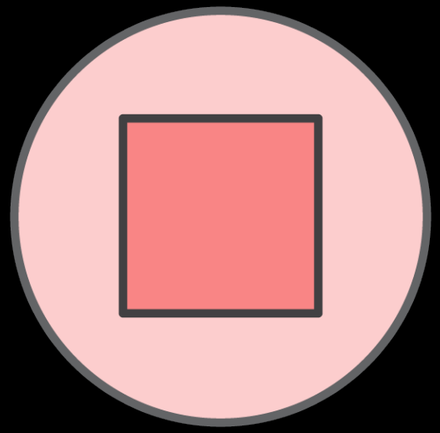
- Reduce attack surface
- Perform vulnerability management
- Validate software integrity

Data protection

Keep people away from data

-Don’t store

-Don’t grant



-Encrypt

-Mask

-Tokenize

-Isolate

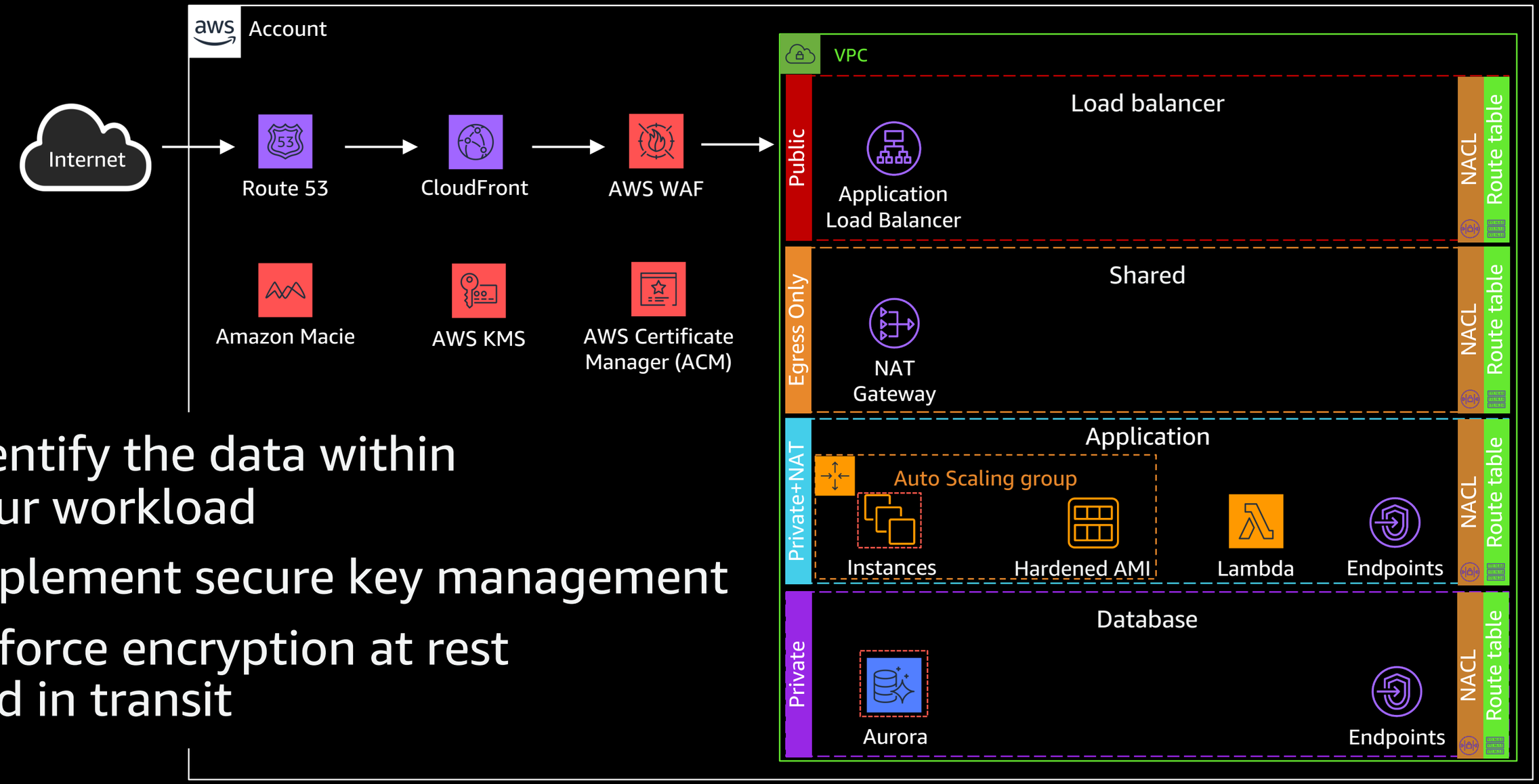
-Tooling

-Eliminate human access

-Operations as code

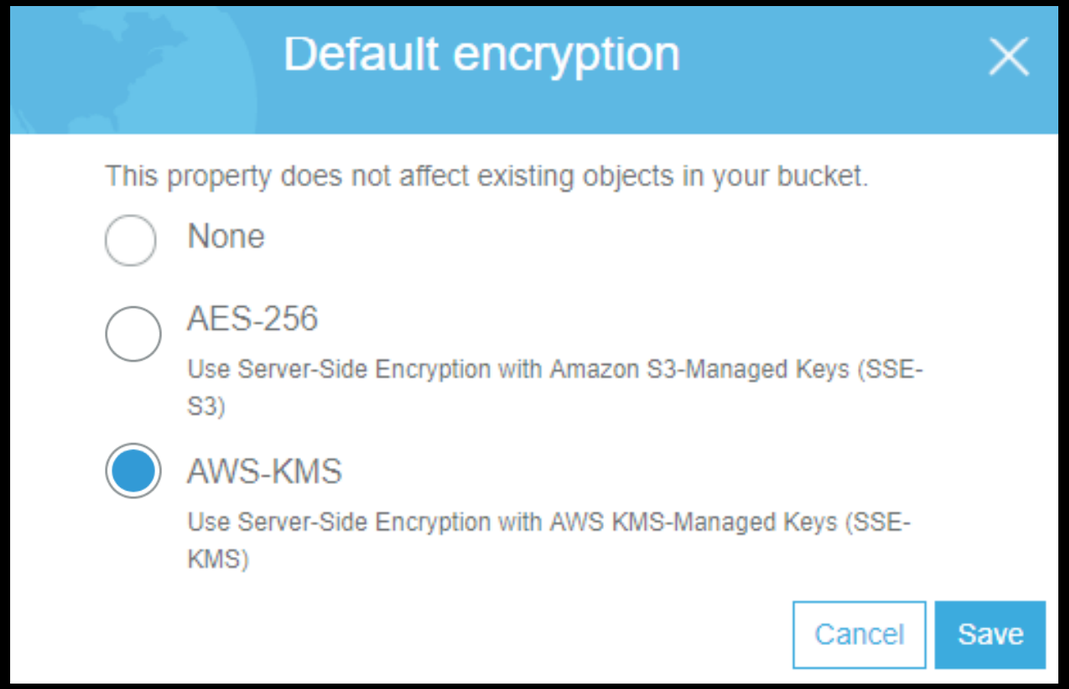
-Version control

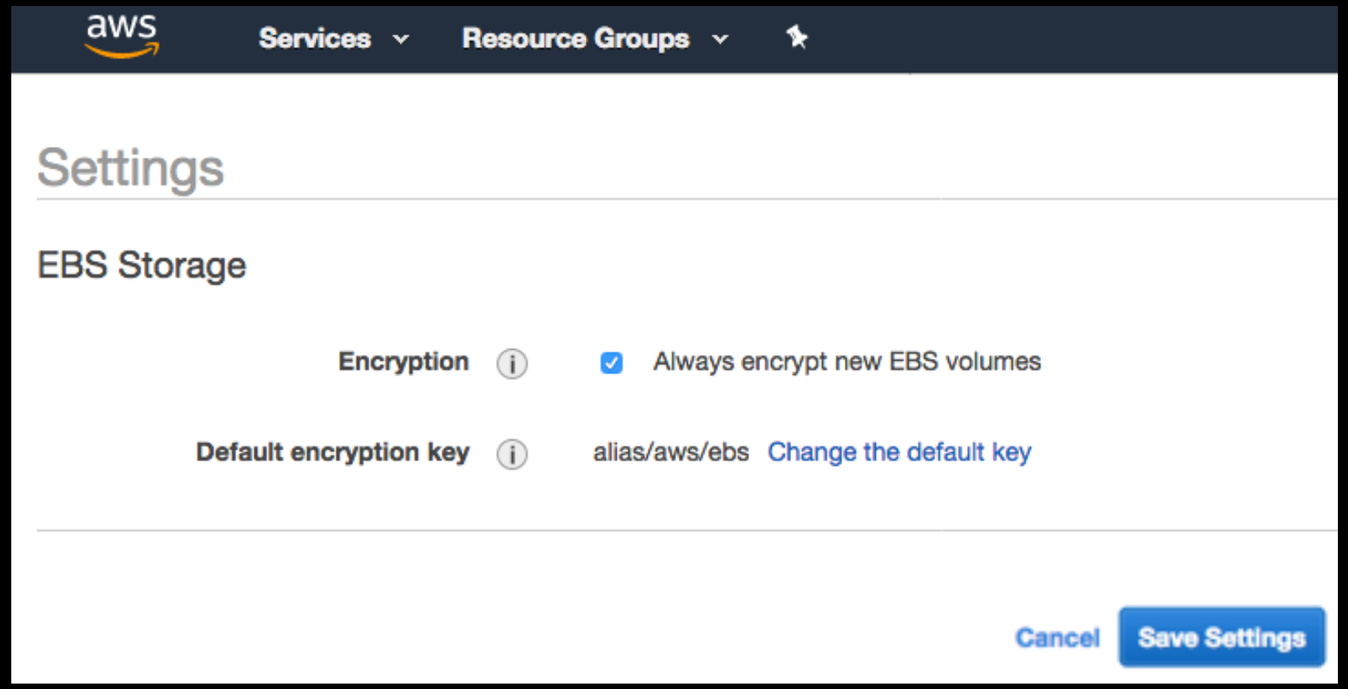
Key best practices: Data protection



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

Enable default encryption





Incident response

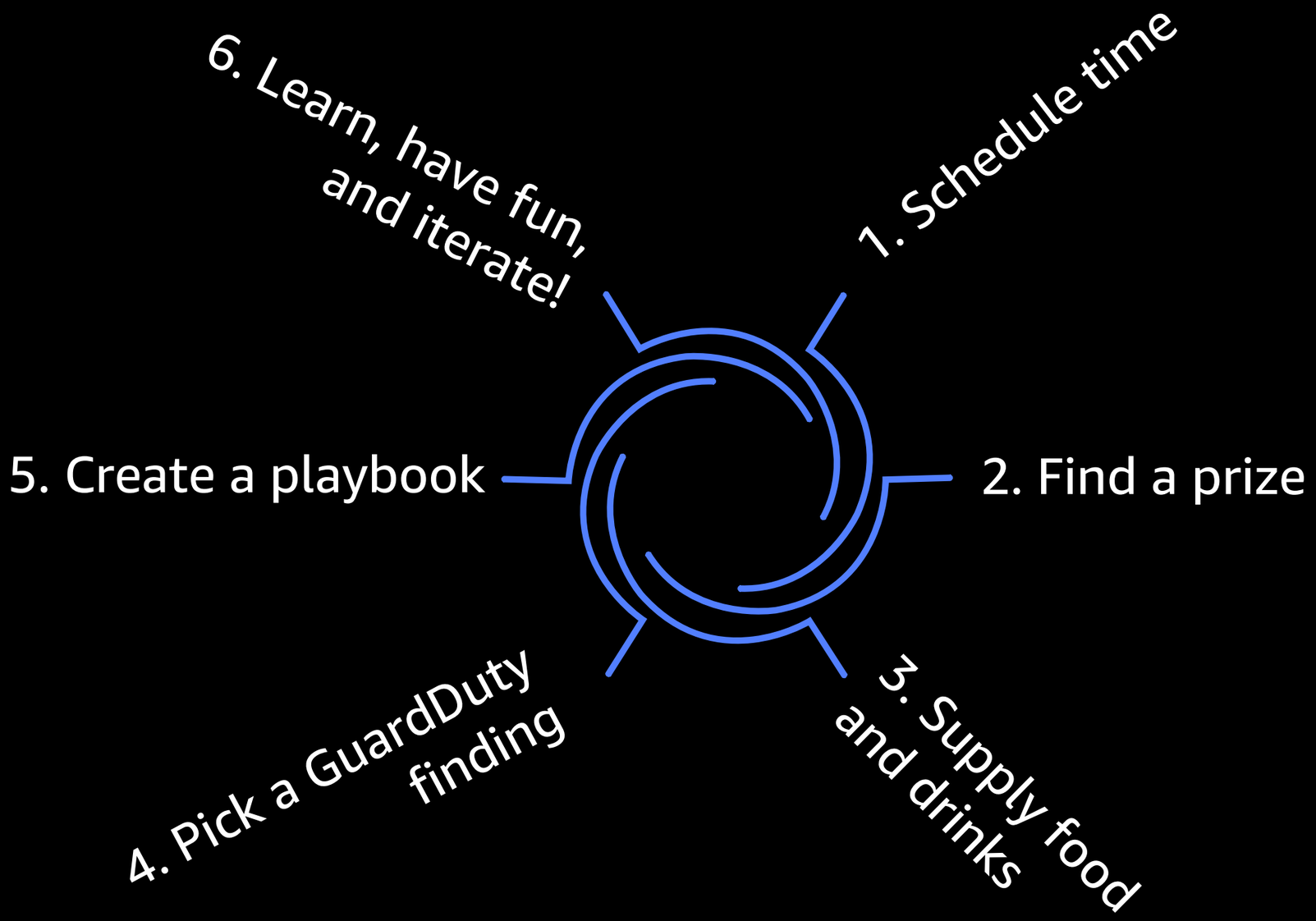
Key best practices: Incident response

- 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
```

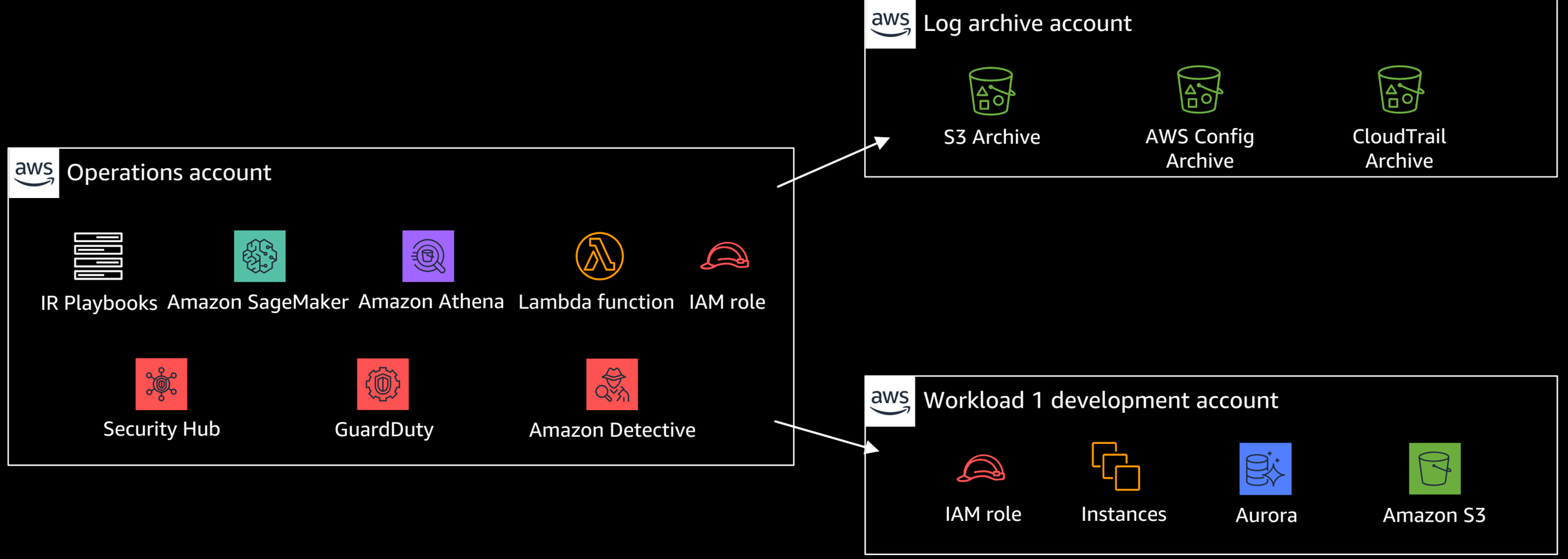
Example runbooks: https://bit.ly/2WhZvoR

How to run a gameday



Key best practices: Incident response

- Pre-provision access and tools



Jupyter lab: https://bit.ly/3nqHQra

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

AWS re:Invent