FSI203

State Farm: Enabling rapid deployment with risk automation

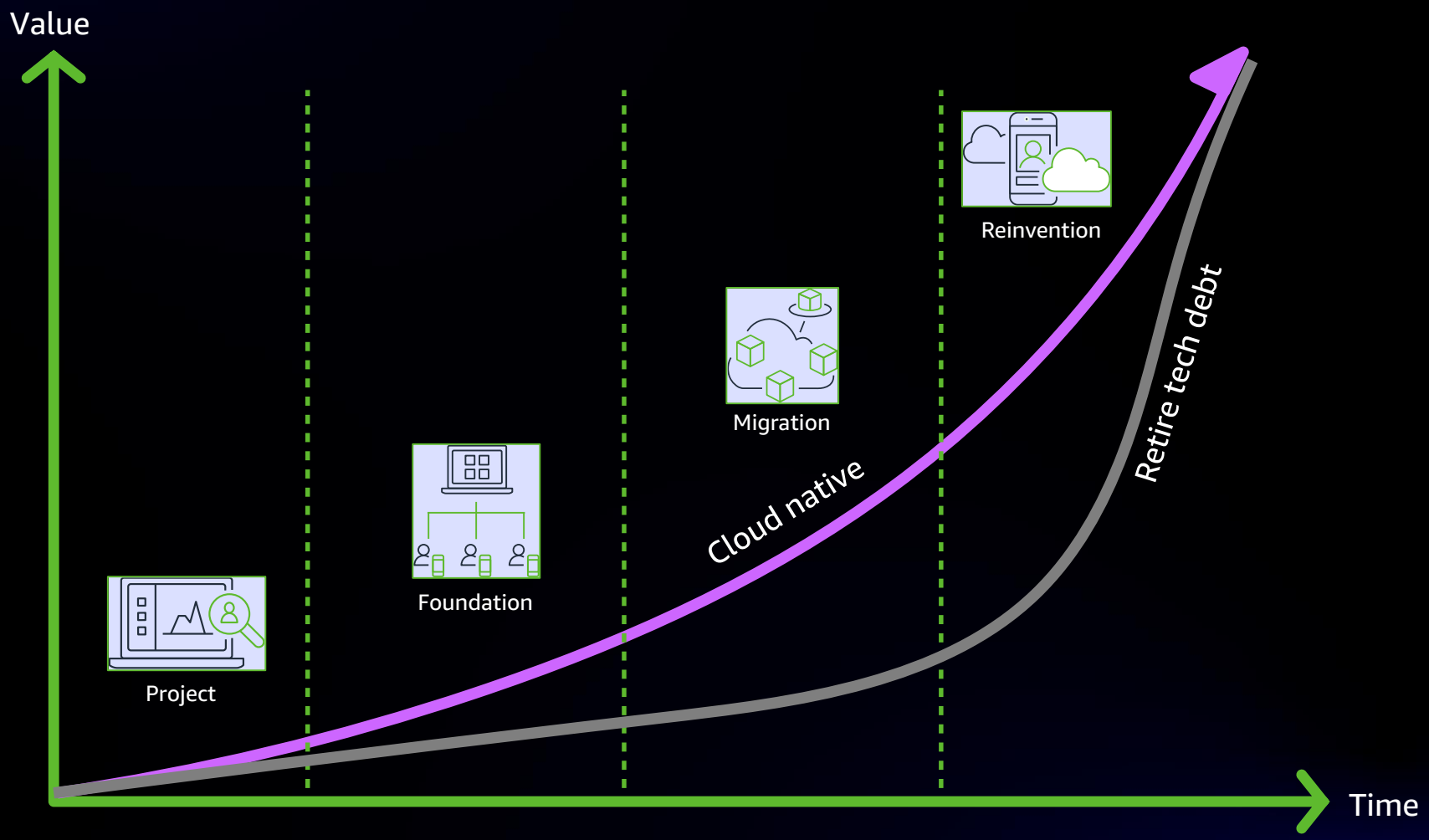
Dennis Kampen
Architect Manager, Public Cloud Adoption Team
State Farm

Jeff Michels
Software Developer
State Farm

John Lucking
Principal Solutions Architect
AWS

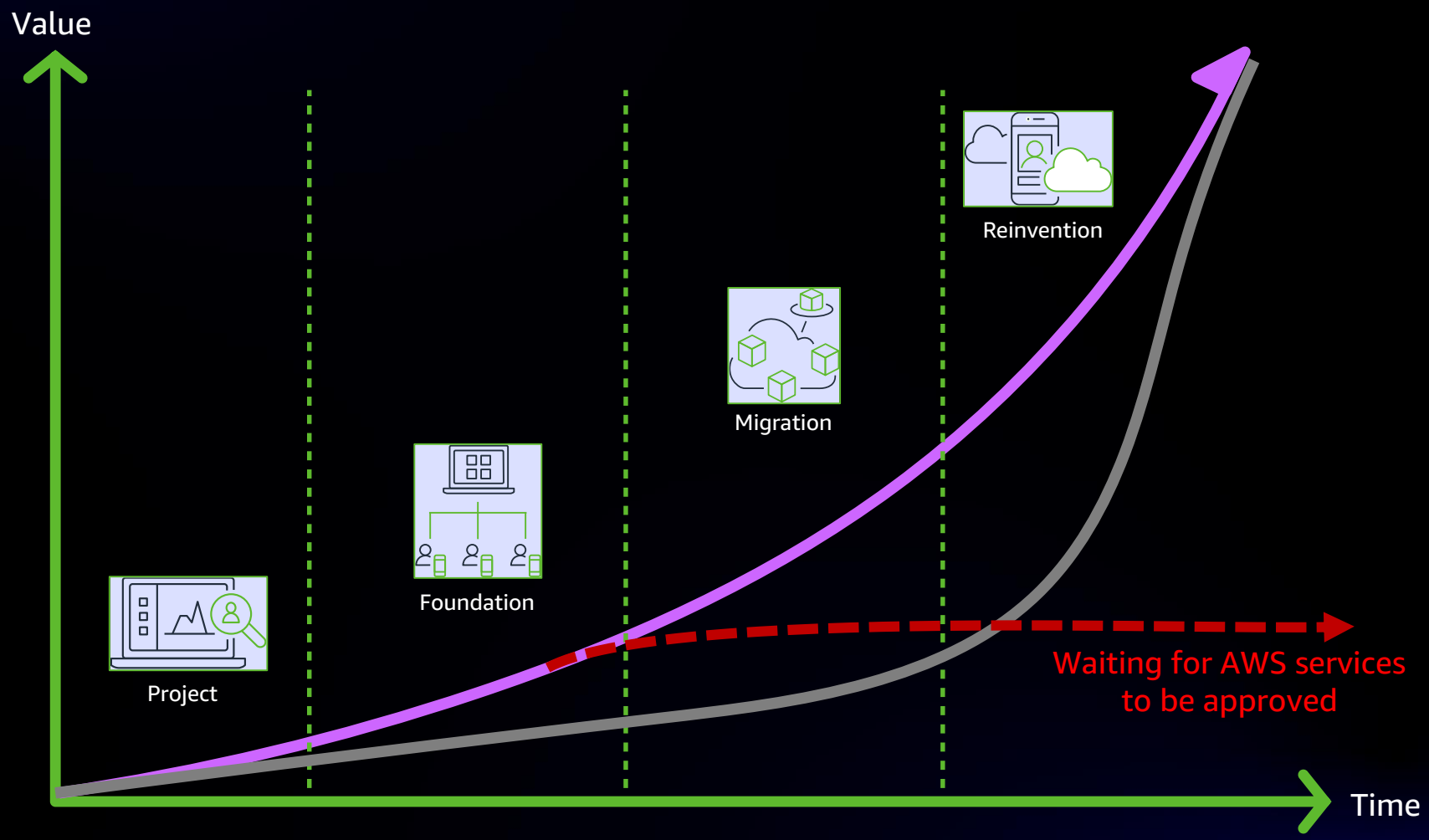
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Stages of cloud adoption



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How to avoid the great stall



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

5 keys to AWS service adoption

1. Achieving compliance
2. Data protection
3. Isolation of compute environments
4. Automating audits with APIs
5. Operational access and security



FSI Service Spotlight Blog Series
https://go.aws/30e9kJz

How financial institutions can approve AWS services for highly confidential data
https://go.aws/3C5QS31

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key AWS services

1. Compliance



AWS Artifact



AWS Audit Manager

2. Data



AWS CloudTrail



AWS Certificate Manager (ACM)

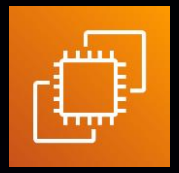


AWS Key Management Service (AWS KMS)

3. Compute



Amazon Virtual Private Cloud (Amazon VPC)



Amazon Elastic Compute Cloud (Amazon EC2)



AWS Lambda

4. Audits



AWS Config



AWS CloudTrail

5. Security



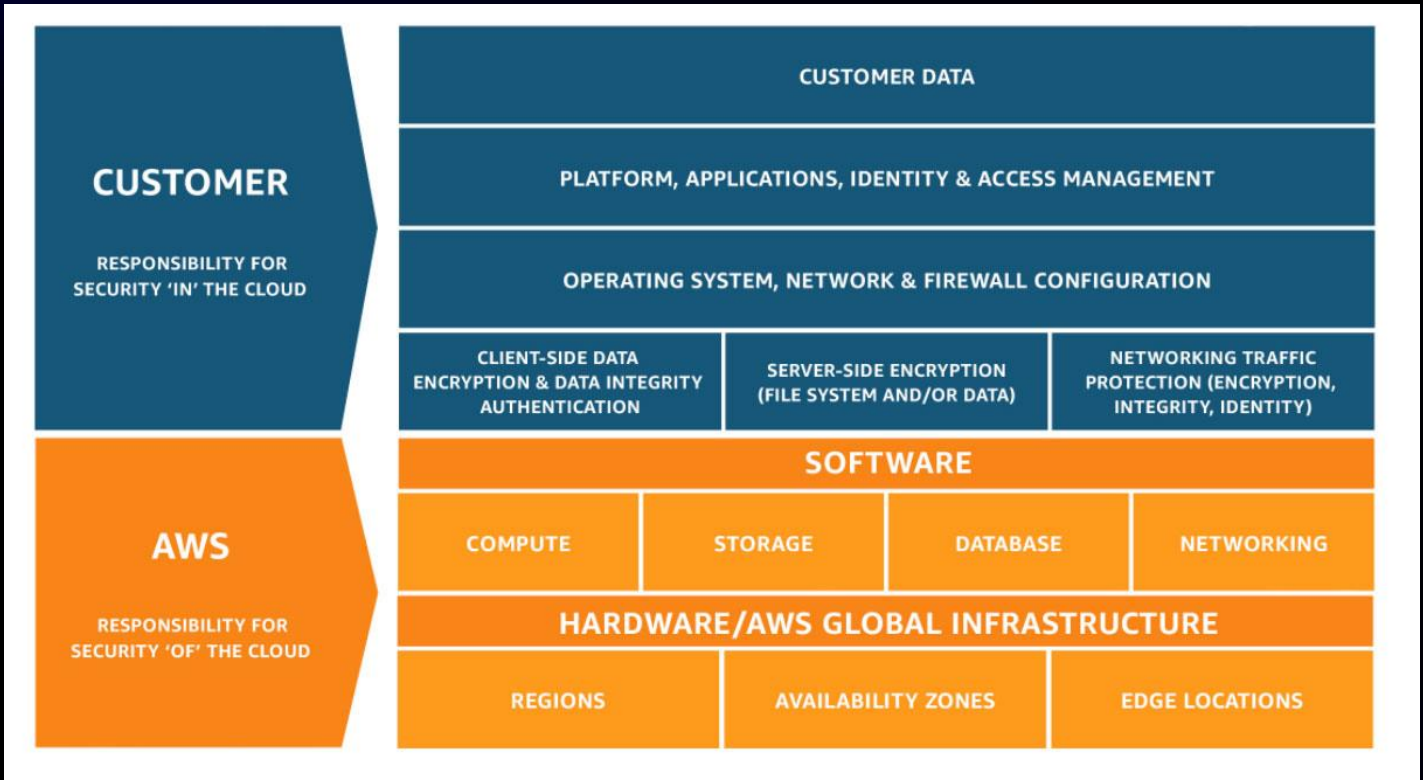
AWS Nitro System

- Cards
- Security chip
- Hypervisor
- Enclaves

AWS Well-Architected Security Pillar https://go.aws/3bYbrDN

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Undifferentiated heavy lifting



1. Serverless first
2. Managed infrastructure
3. Managed services
4. COTS → Amazon EC2

Shared Responsibility Model
https://go.aws/3wzhkRi

"We build muck, so you don't have to," Jeff Barr noted in 2006; developers spend much of their time on backend work
https://go.aws/3C6Rp4F

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Benefits



Monitoring of cloud configuration data

Leads to

Organizational benefits

Confidence
Effective security posture

Efficiency
Focus on high-risk areas

Scalability
Automation of audit tasks

Automation
Reduction of manual tasks

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A-RAM setting the stage



Infrastructure and application code

Scripts and control checks

Platform control baseline

Detect, notify, and remediate

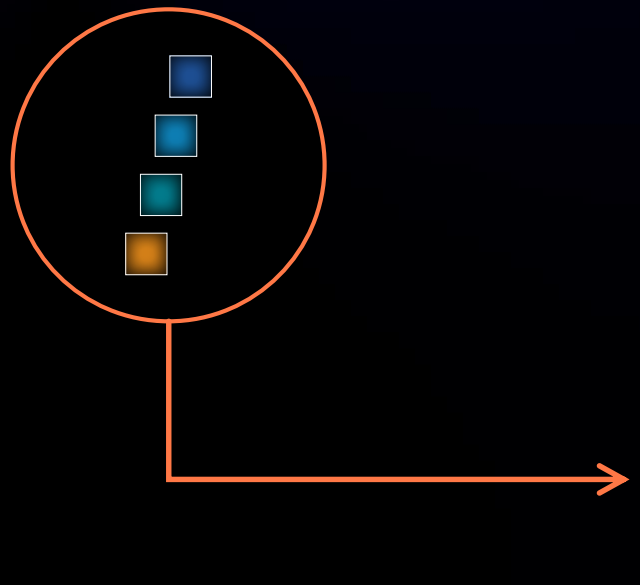
DNR – scans and notifies administrators when out of adherence to platform control baseline

A-RAM

Dashboard – shows control effectiveness and use case adherence to platform control baseline

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Benefits



Automation
Reduction of manual tasks

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure as code



Use case

The foundation for A-RAM is “codification” of

- Infrastructure and application
- Infrastructure as code
- Policy as code

Code

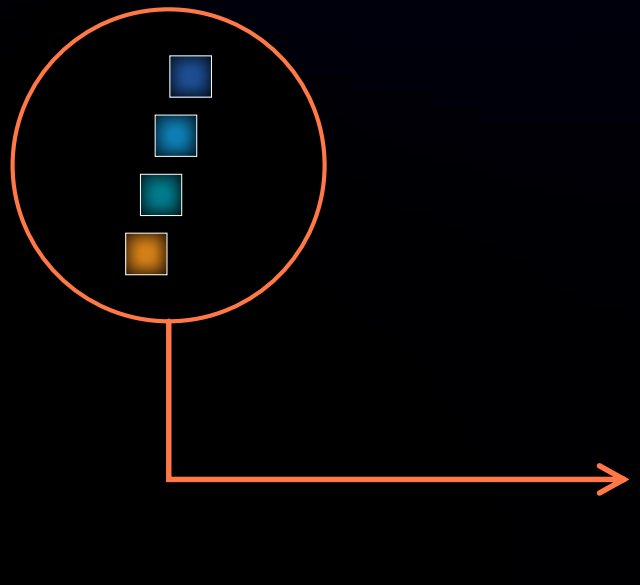
Infrastructure and application code

Scripts and control check

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Benefits



Scalability
Automation of audit tasks

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Platform baseline risk treatments



Use case

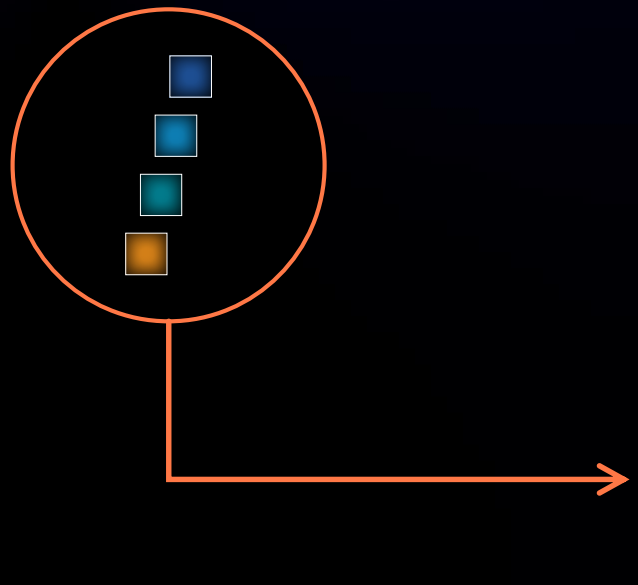
- Platform control baseline
- High-level “control objectives”
- Created as a risk treatment plan to protect all data like it is SPI

Platform controls

Platform control baseline

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Benefits



Efficiency
Focus on high-risk areas

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detect, notify, and remediate



Use case

- All risk treatments are distilled into technical controls
- DNR checks are the technical controls to fulfill the risk treatments

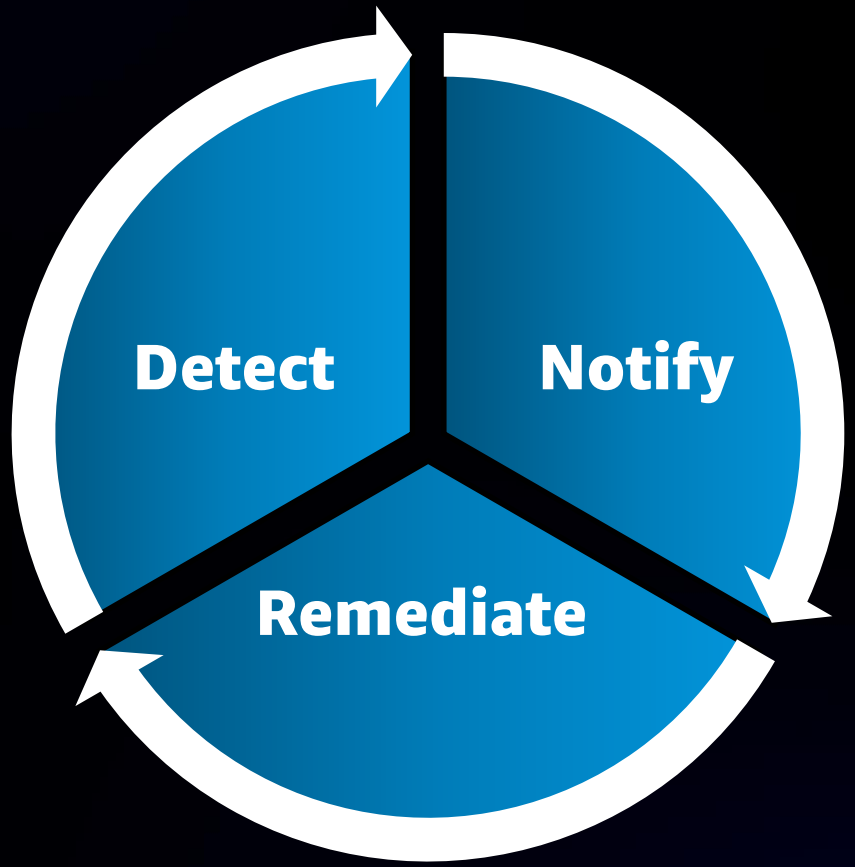
DNR

Detect, notify, and remediate

DNR – scans and notifies administrators when out of adherence to platform control baseline

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

DNR



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detect

State Farm developed a solution utilizing AWS resources

- Developed in Python
- Utilizes Amazon ECS Fargate
- Deployed to one account
- Data stored on Amazon DynamoDB

State Farm organization accounts

- ~400 accounts
- Registers new accounts
- Deprecates suspended accounts

Scans – evaluate resources pertinent to the test

- Hourly and daily scans
- ~90 tests being run against each account
- 36,000 tests run each hour
- Multi-threaded for faster processing

Exceptions – procedure to allow known findings to pass

- Exception table
- Tagged exceptions
- Findings stored as exceptions

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

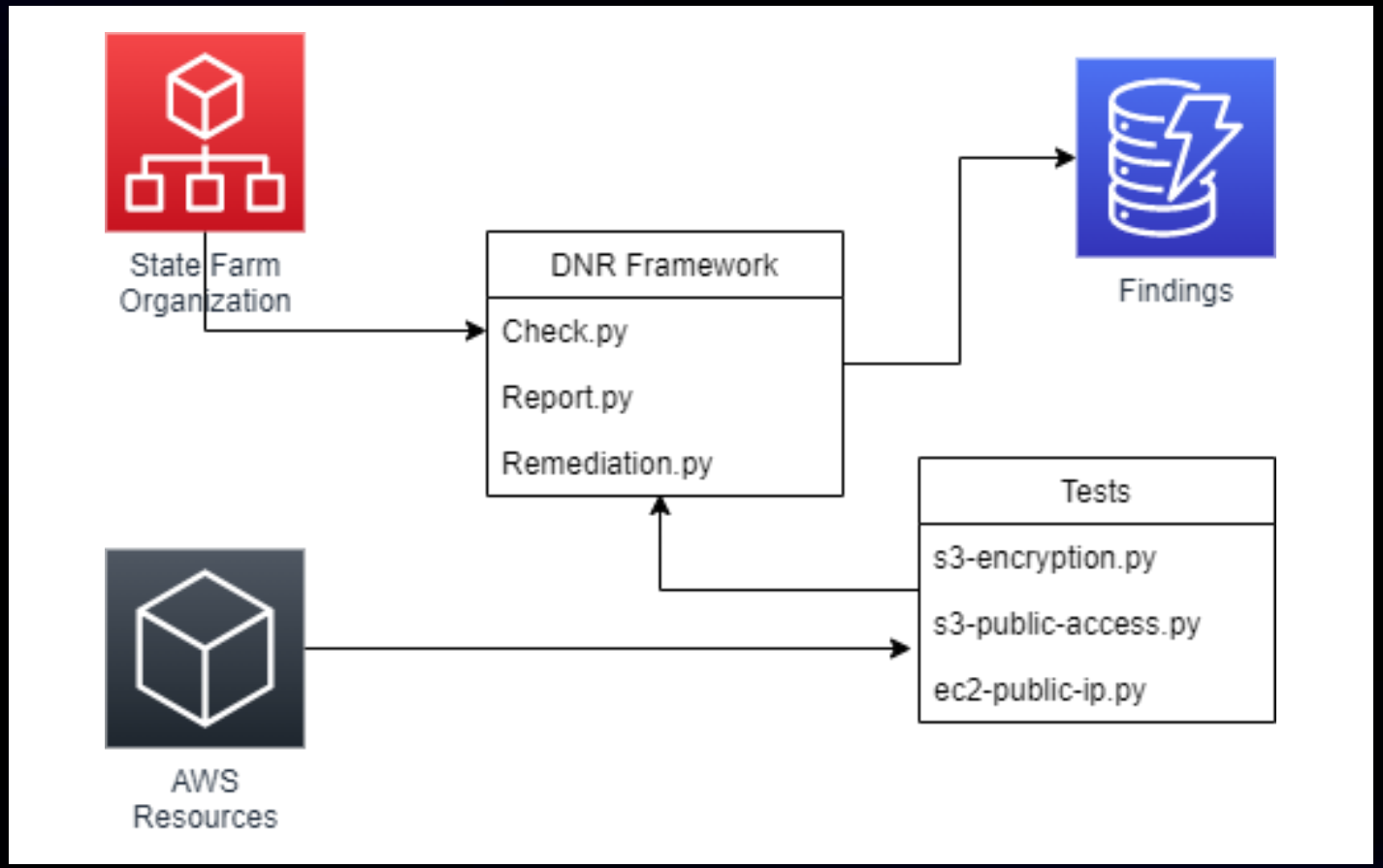
Detect – Tests

Customizable tests

- Each test is a packaged Python script consuming the common DNR framework
- Can be added to the DNR application without impacting other tests
- New test development begins as a request from a business area or risk finding
- Each test is ~50 lines of code, depending on its complexity
- Development usually takes less than a week with the majority of time centered around business-partner communication and documentation
  - A DNR “cookbook” site is maintained with our tests and examples of how to mitigate the finding
- Several environment specific tests unique to State Farm
  - IAM-unmanaged-user – verify local IAM users do not have console access

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detect



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Notify

Daily notification

- Email of all findings related to an account
- Finding sorted in order of escalation
- Sent to account administrators
- Utilizes Amazon Simple Email Service (SES)

Manager notification

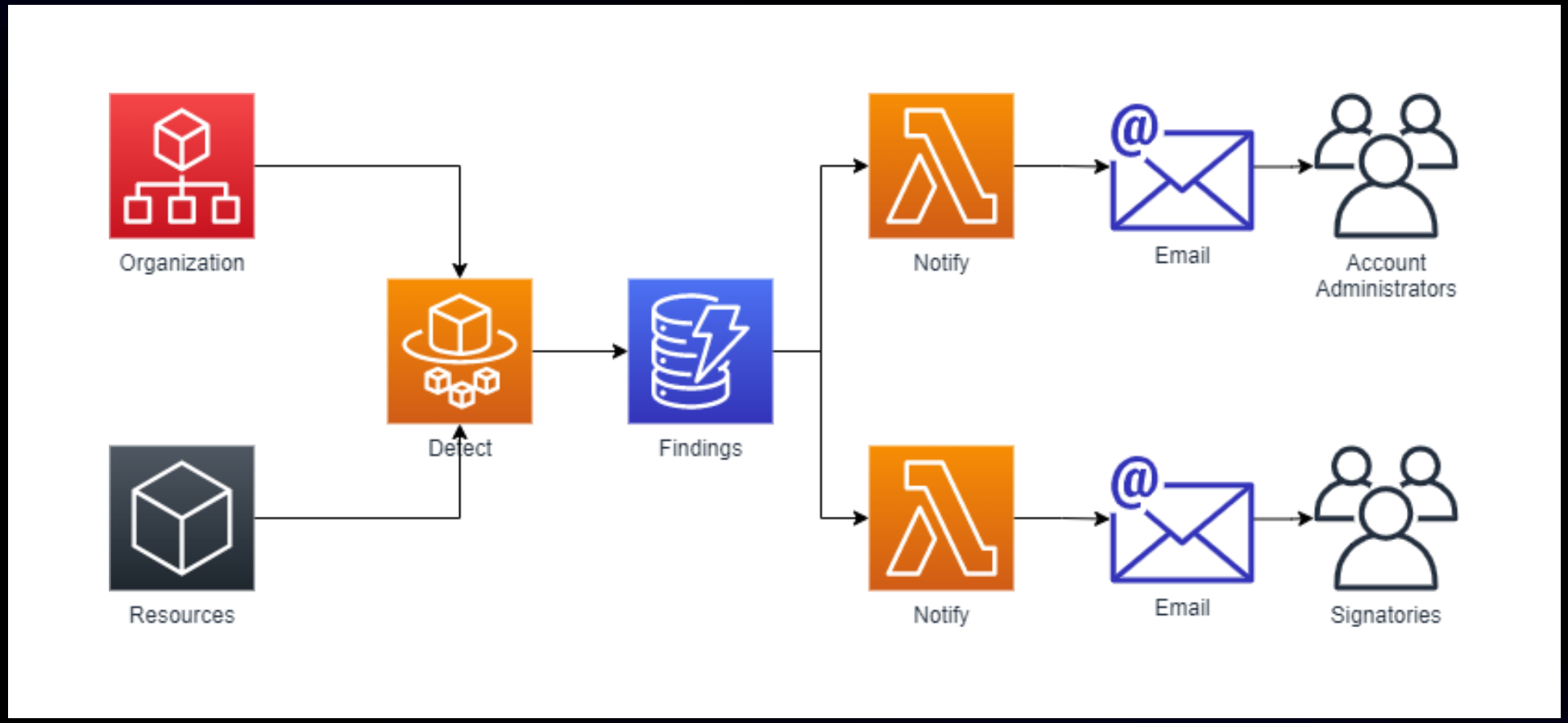
- Email of findings that will be escalated within 7 days
- Sent to account administrators' direct management

Leadership escalation

- Email of findings that have exceeded the defined escalation period for each test
- Sent to executive business use case owner
- Escalations occur 7, 30, 60, or 90 days after discovery, depending on severity

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Notifications



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Remediation (mitigation)

Corrective actions

- Automated or manual
- Online “cookbook” with frequently asked questions and examples

Automated remediation

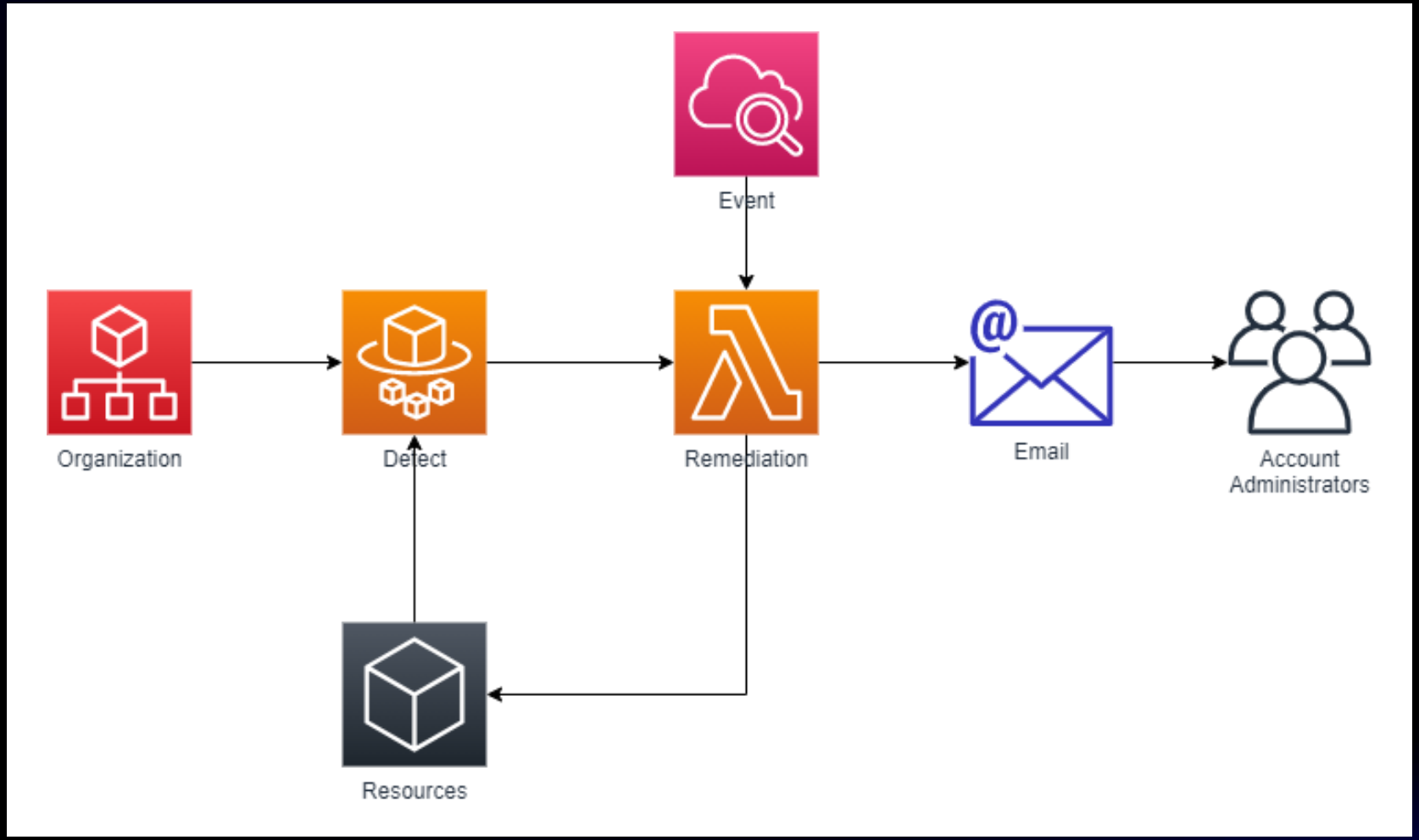
- Automation is reserved for critical findings or when action is determined to be non-disruptive
- Can be event-based or scheduled depending on the finding
- Utilizes AWS Lambda functions to perform actions related to individual services

Notification to account owners

- Email notifications are sent out immediately to affected account owners of the action taken, resource affected, and when it occurred

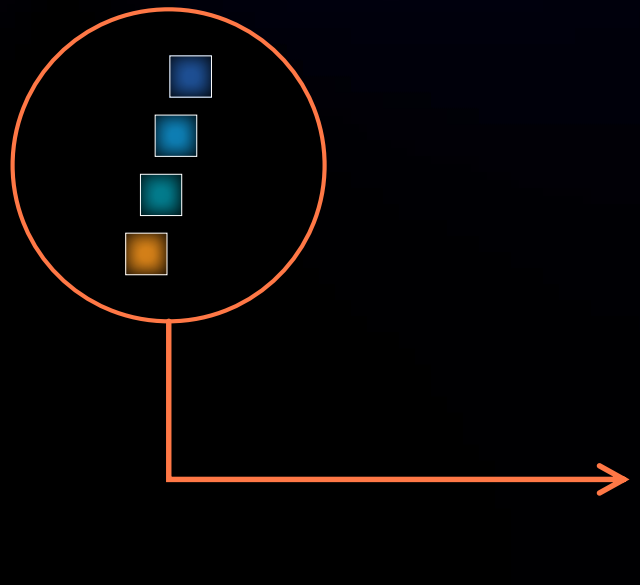
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Remediation



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Benefits





Confidence
Effective security posture

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A-RAM



Use case

- A-RAM tracks both successes and failures
- Enables a platform, risk treatment, and account view
- Enables a data-driven view of risk
- Shows overall adherence to risk treatments and technical controls
- Code required for deployment, but console access still exists
- Prevention via code coupled with detection for manual

A-RAM

A-RAM

Dashboard – shows control effectiveness and use case adherence to platform control baseline

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A-RAM



A-RAM

Dashboard – shows control effectiveness and use case adherence to platform control baseline



Use case

Automated risk assessment and management for cloud

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A-RAM setting the stage



Infrastructure and application code

Scripts and control checks

Platform control baseline

Detect, notify, and remediate

DNR – scans and notifies administrators when out of adherence to platform control baseline

A-RAM

Dashboard – shows control effectiveness and use case adherence to platform control baseline

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Benefits



Monitoring of cloud configuration data

Leads to

Organizational benefits

Confidence
Effective security posture

Efficiency
Focus on high-risk areas

Scalability
Automation of audit tasks

Automation
Reduction of manual tasks

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Dennis Kampen
dennis.kampen.beze@statefarm.com

Jeff Michels
jeff.michels.hrha@statefarm.com

John Lucking
jlucking@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.