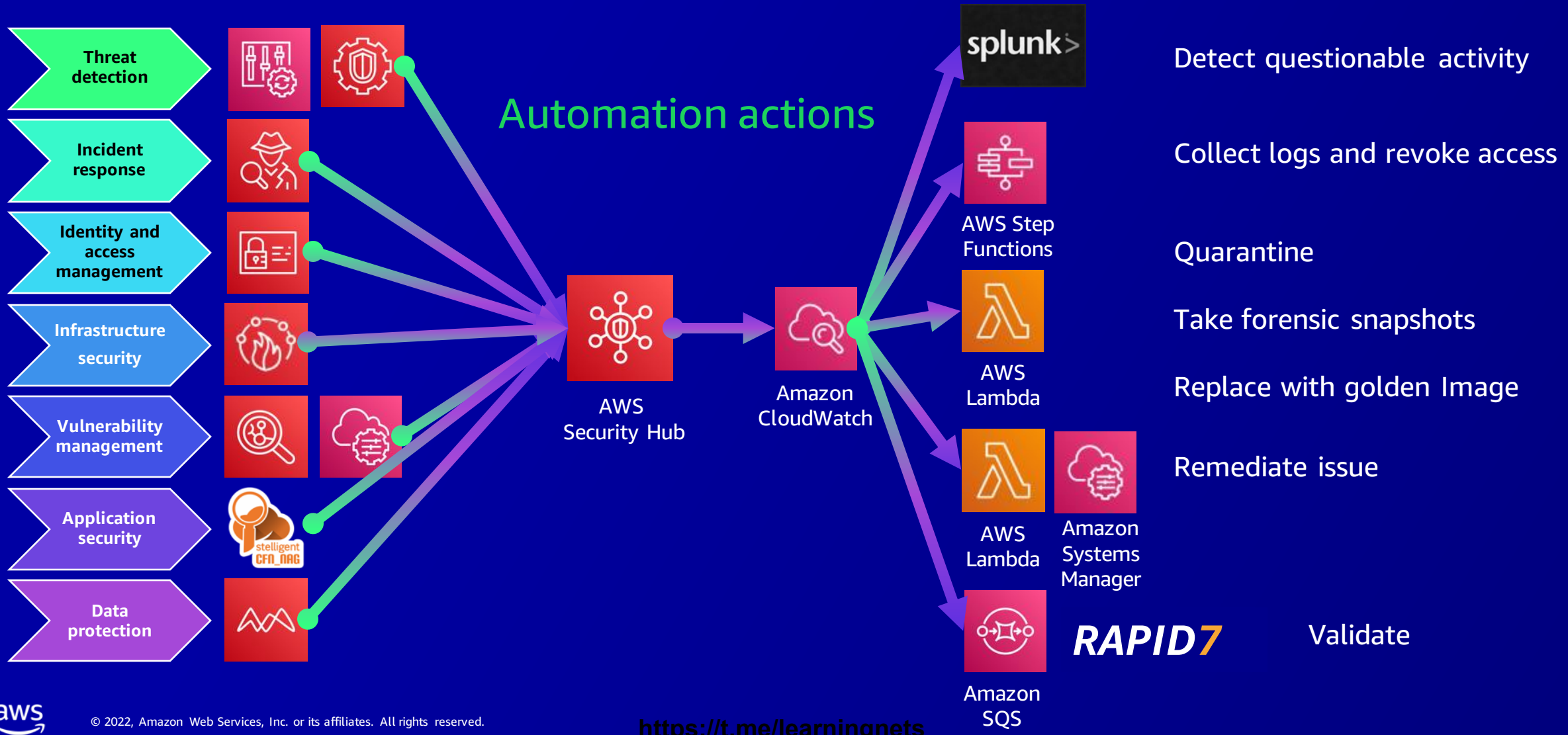
Crawl, walk, run: Accelerating security maturity

Security Hub Example



Accelerating security maturity

Crawl

- Plan: Getting started on the journey
- Build: Lay the groundwork
- Assess: Assess the posture

Walk

- Operationalize: Centralize tools and processes
- Mature: Tune and measure

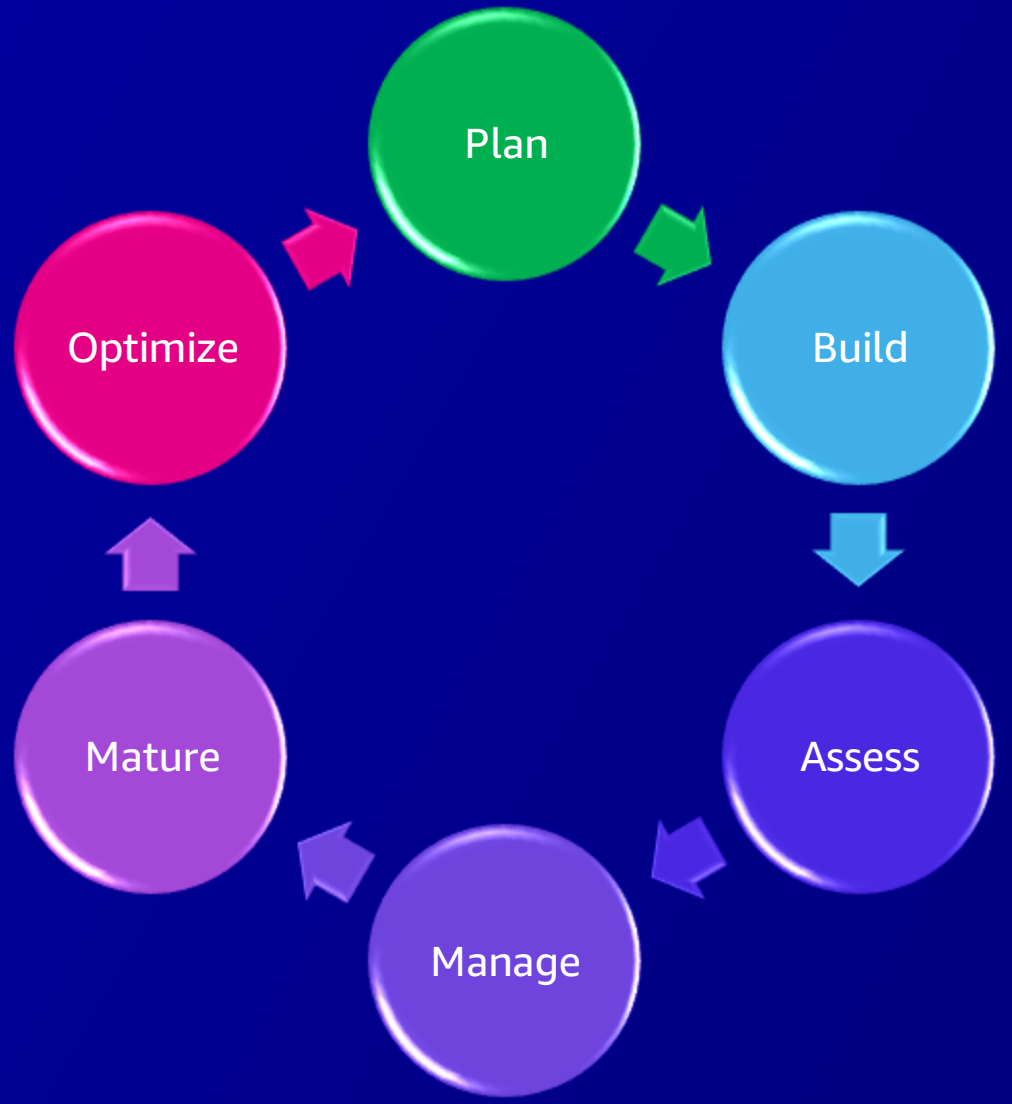
Run

- Optimize: Continuous assessment and automation

Plan: Getting started on the security journey

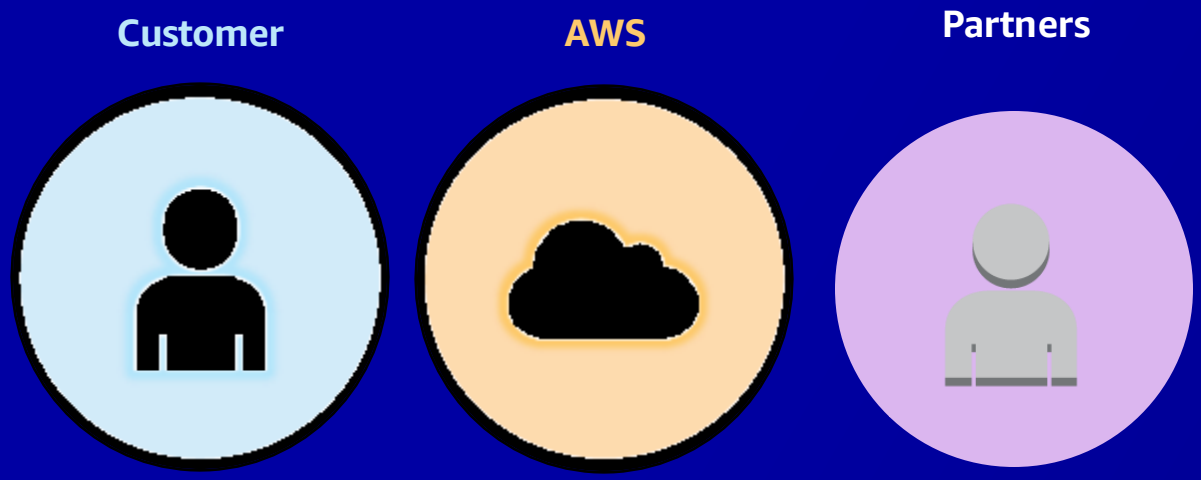
Getting started with planning

- Understand the scope
- Understand the models and approaches
- Understand the planned outcomes
- Be willing to iterate
- Do not start with services



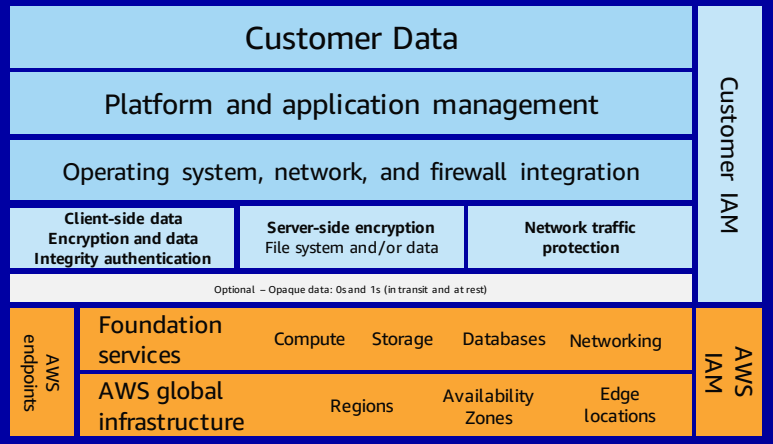
Plan: Understanding the security scope

Security in the cloud is a shared responsibility

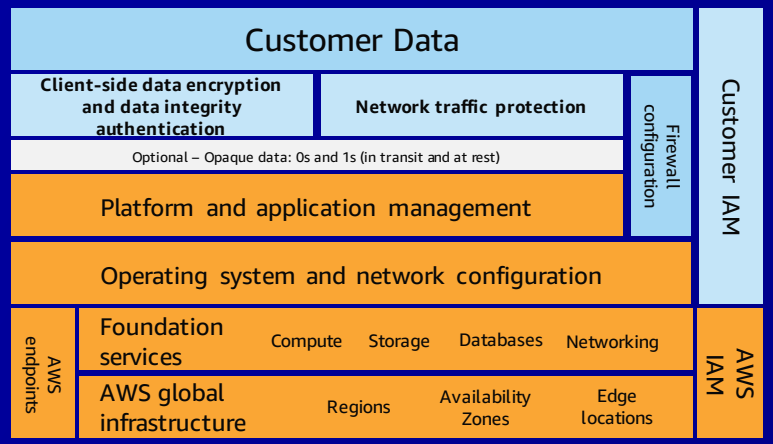


Shared responsibility is not static

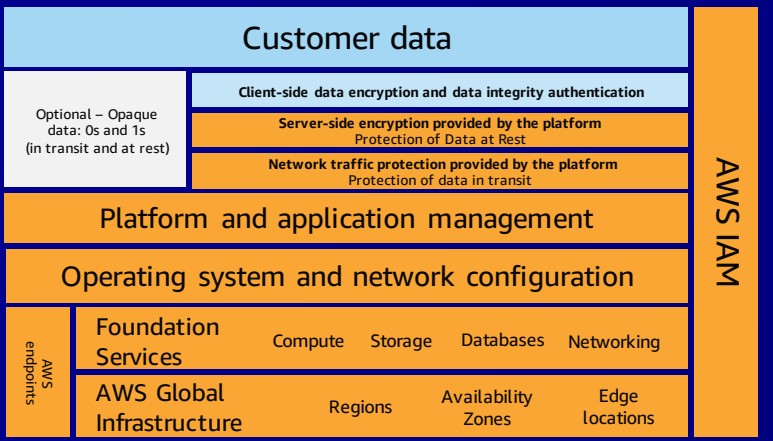
Infrastructure services



Container services



Serverless services



Plan: Understanding the models

Architectural approach

Maturity model approach

Governance approach

Business objective approach

Considerations

- Audience
- Business processes
- Goals/outcomes
- Use one approach or blended

Plan: Understanding the models

AWS SRA link

Architectural approach

Benefits:

- SRA/HIPAA/HITRUST
- Architectural view
- Aligns to large cloud strategies and guidance
  - AWS Cloud Adoption Framework (AWS CAF)
  - AWS Well-Architected Framework

Disadvantage:

- Technically focused not business focused

AWS Security Reference Architecture (AWS SRA)

Plan: Understanding the models

AWS SMM link

Maturity model approach

Benefits:

- Security focused
- Stepping stone model
- Fast reduction of risk

Disadvantage:

- Not business focused

Security governance	Assign Security contacts; Select the region(s)
Security assurance	Automate alignment with best practices using AWS Security Hub
Identity and access management	Multi-Factor Authentication; Avoid using Root and audit it; Access and role analysis with IAM Access Analyzer
Threat detection	Threat Detection with Amazon GuardDuty and review your findings; Audit API calls with AWS CloudTrail; Remediate security findings found by AWS Trusted Advisor; Billing alarms for anomaly detection
Vulnerability management	
Infrastructure protection	Limit Security Groups
Data protection	Amazon S3 Block Public Access; Analyze data security posture with Amazon Macie
Application security	AWS WAF with managed rules
Incident response	Act on Amazon GuardDuty findings

AWS Security Maturity Model

Plan: Understanding the models

Cloud Foundation

Governance approach

Benefits:

- Broad IT focus
- Reliability component
- Operational mindset

Disadvantage:

- Not business focused

AWS Cloud Foundation

Plan: Understanding the models

Business objective approach

Benefits:

- Cost justification built in
- Clear business-aligned security direction
- Measurements defined upfront

Disadvantage:

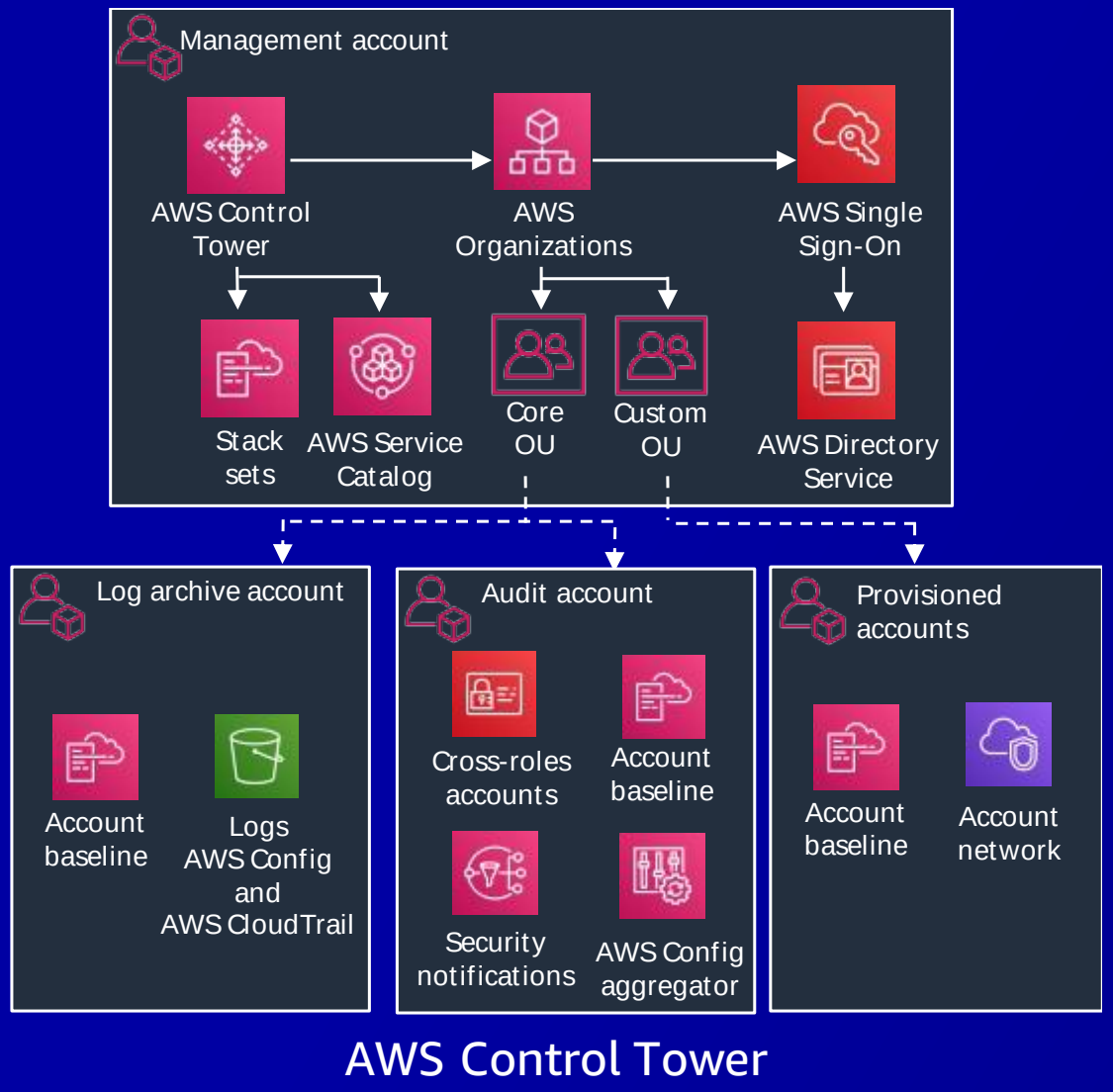
- Time consuming
- One step removed from prescriptive technical guidance

Business objective example

AWS Identity and Access Management (IAM) business outcome:

Enable accelerated provisioning of new users and environments by automating visibility and measuring against best practices to continuously drive down risk

Build: Lay the groundwork



AWS Control Tower

AWS Control Tower

AWS Control Tower

A preconfigured, secure, scalable, multi-account AWS environment based on best practice blueprints

- Multi-account management
- Identity and federated access management
- Centralized log archive
- Cross-account audit access
- End user account provisioning
- Centralized monitoring and notifications

Assess: Assess the posture

Prowler

Cloud posture assessment tools

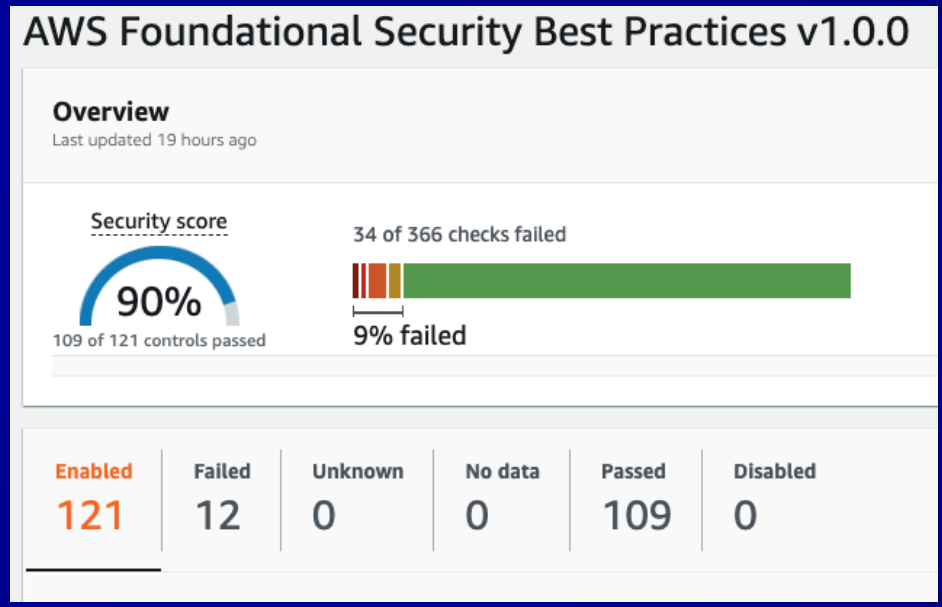
Prowler:

- External, open source
- Flexible deployment options
- Snap shot and baseline

AWS Security Hub:

- Unified dashboard
- Continuous assessment and alerting

AWS Security Hub

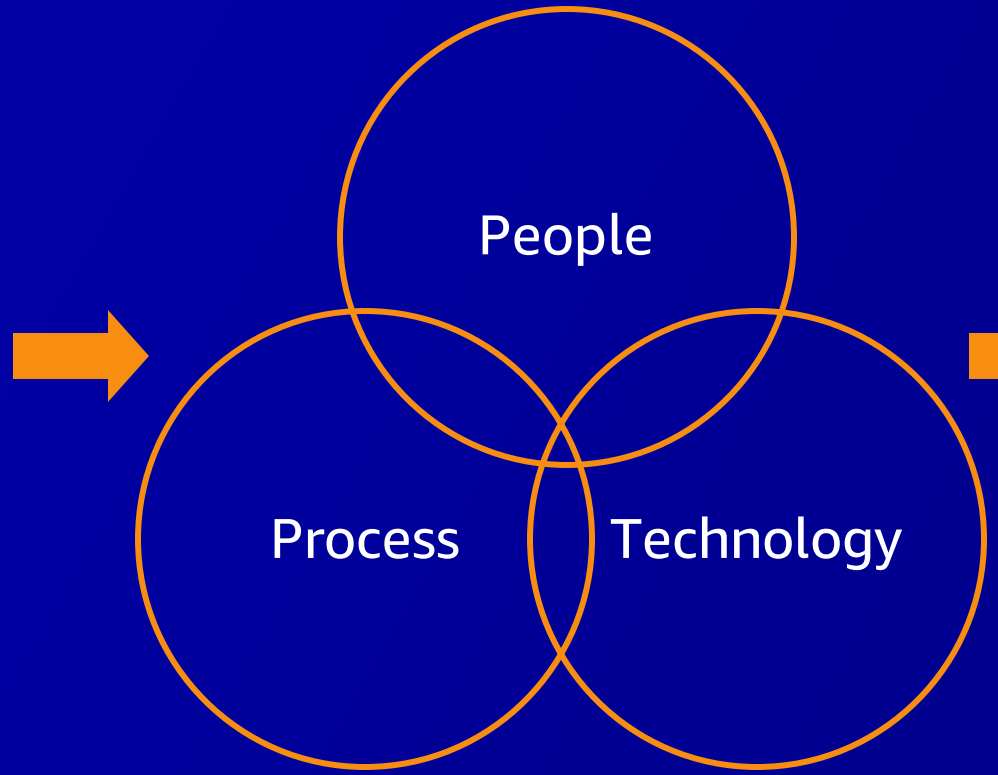


Operationalize: Tools and processes

Security CAF

AWS Cloud Adoption Framework (CAF)

Non-technical	**Business** Value realization
	People Role and readiness
	Governance Prioritization and control
Technical	**Platform** Applications and infrastructure
	Security Risk and compliance
	Operations Hybrid and dynamic



Expected outcomes

- DevSecOps pipeline and process
- Tagging and asset management
- Monitoring and detective integration (SIEM)
- Cloud incident response plan and program
- Cloud vulnerability management
- Cloud posture management
- Cloud security training

Operationalize: Tools and processes

CFN_NAG

Expected outcomes:

- DevSecOps pipeline and process
- Tagging and asset management
- Monitoring and detective integration (SIEM)
- Cloud incident response plan and program
- Cloud vulnerability management
- Cloud posture management

Key tools:

- Static code analyzer
- AWS Config
- Amazon GuardDuty
- Amazon Detective
- Amazon Inspector
- AWS Security Hub

AWS Config

Amazon GuardDuty

Amazon Detective

Amazon Inspector

AWS Security Hub

Mature: Tune and measure processes

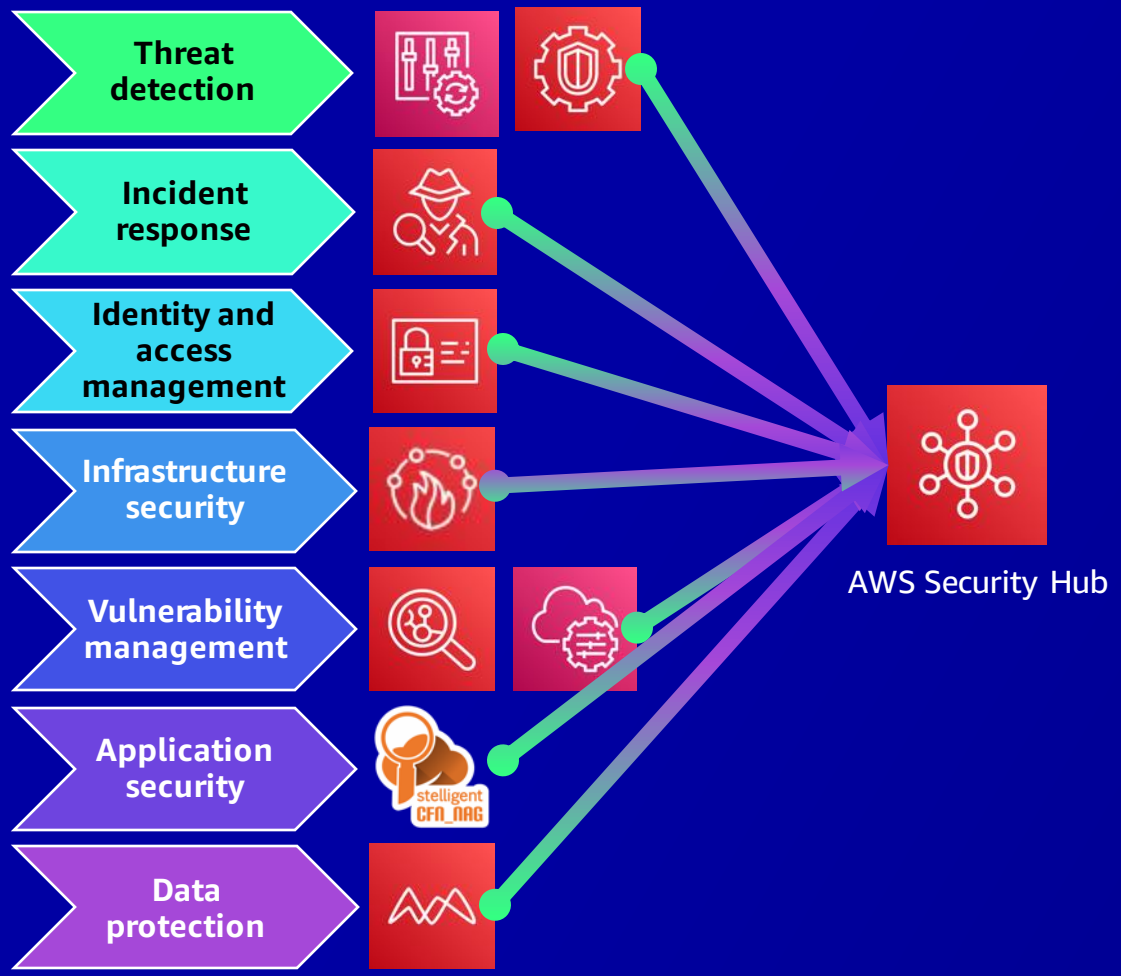
Agile guidance

Agile security:

- Specialize to accelerate
- Innovate not operations
- Move quickly in sprints
- Align with operations
- Focus training
- Backlog (roadmaps/gaps)

Mature: Tune and measure tools

Security Hub



Security Hub Integrations

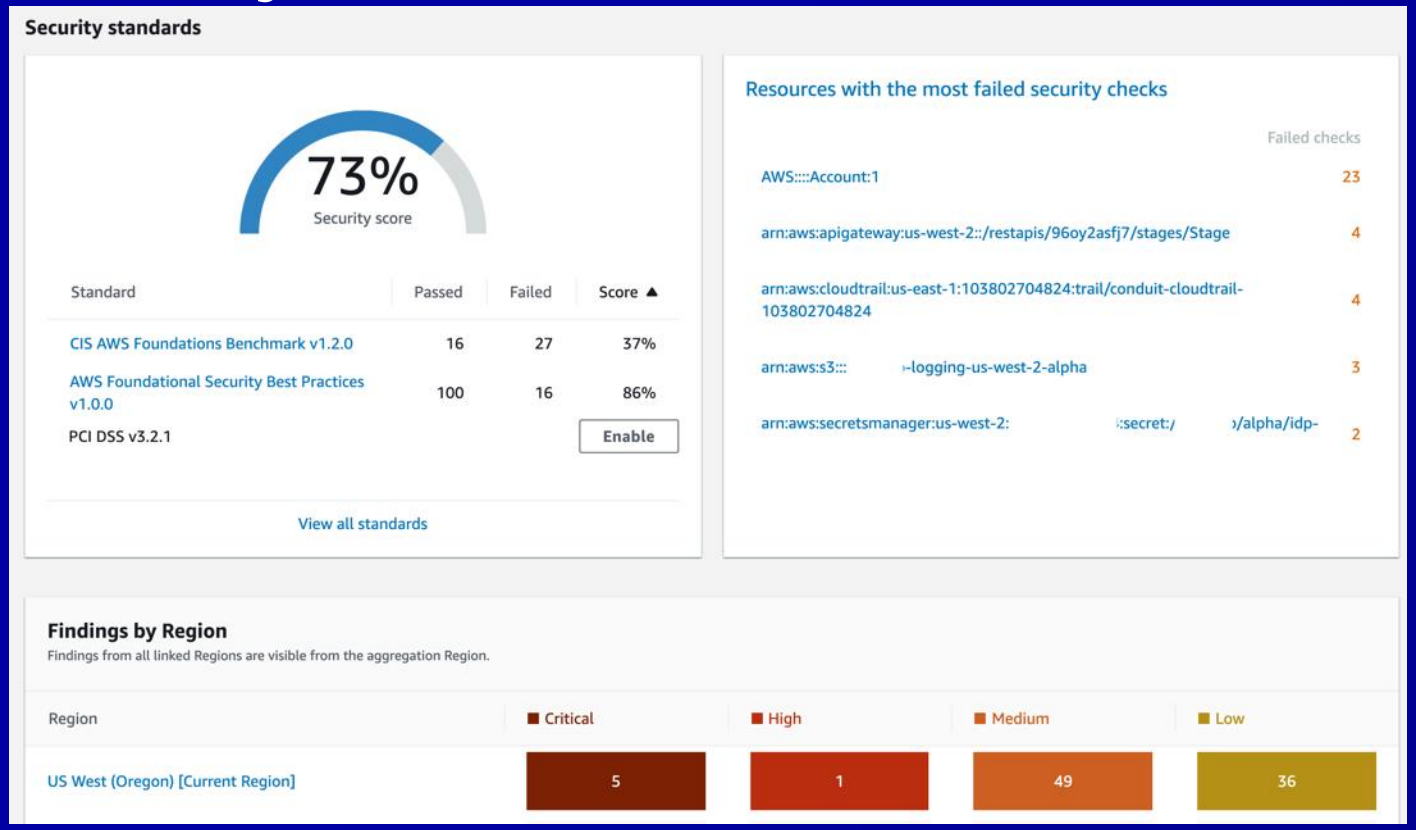
Measure and report:

- Unified dashboard
- Built in integrations with AWS security services
- Third-party integrations
- Custom integrations
  - Security Hub API
  - AWS CLI
  - AWS Security Finding Format (ASFF)

Mature: Tune and measure risk

AWS Security Hub

Security Hub



Measure and report:

- Continuous assessment
- Centralized management
- Measure against standard baselines
- AWS foundational security best practices
- Visibility at account level for DevSecOps
- Risk by region and resource

Mature: Threat detection example

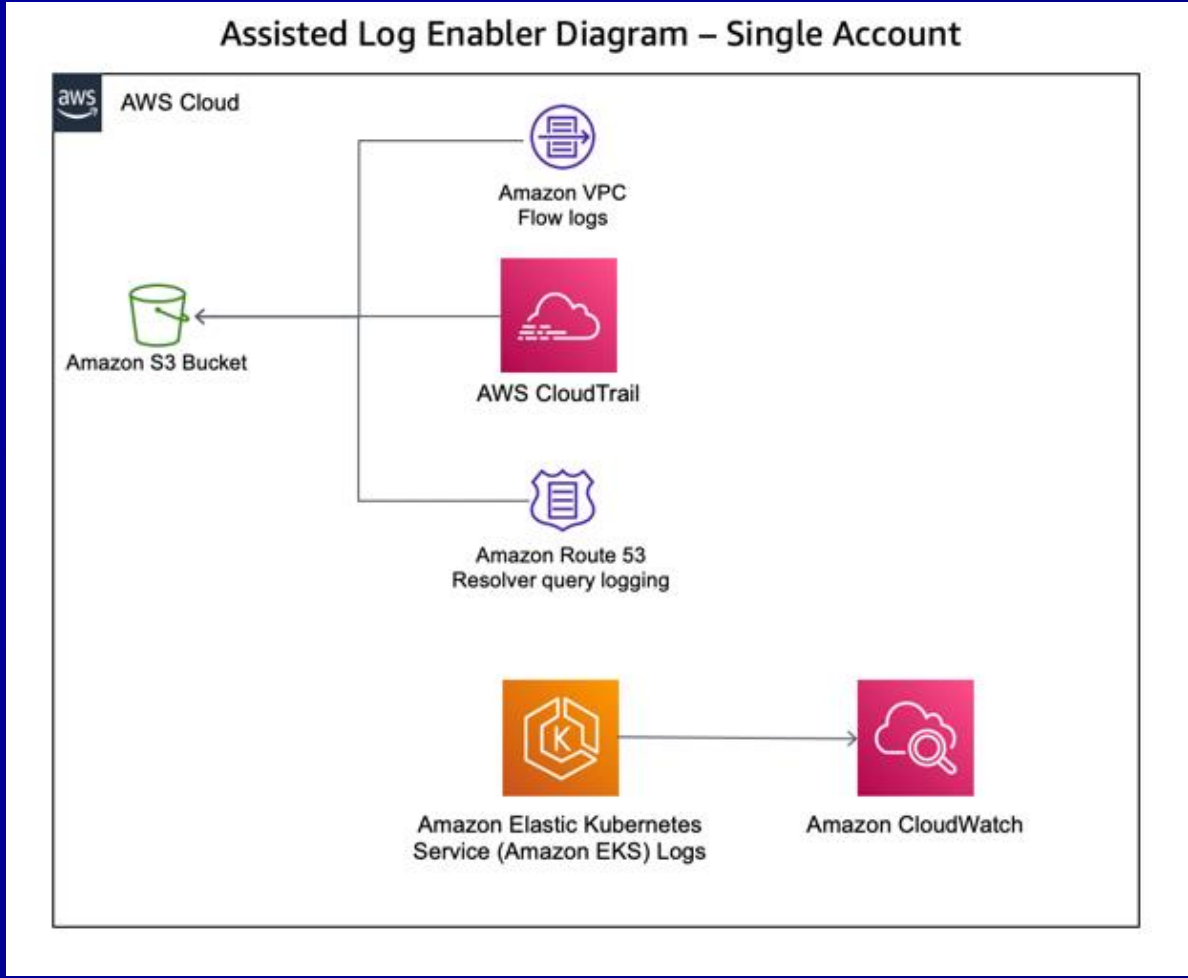
Log Enabler

Detective business outcome:

Increase visibility and speed of detection of cloud incidents in order to lower risk and enable accelerated use and development of cloud resources

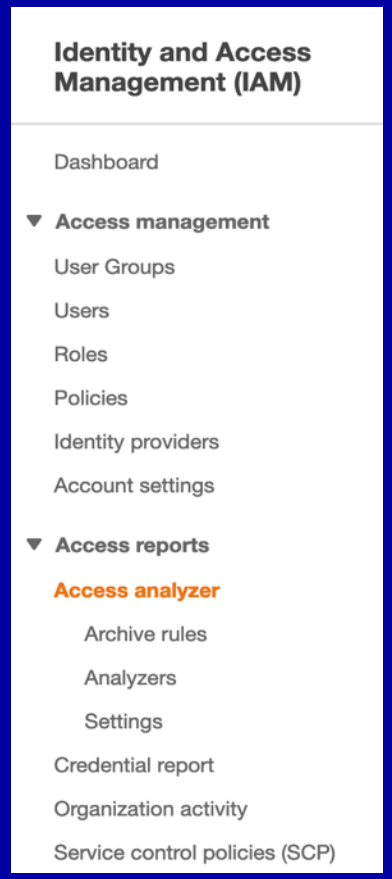
Tool: AWS Assisted Log Enabler

- Single or multi-account
- Dry run feature/check
- Select specific services
- Throttle up or down for use case



Mature: IAM example

IAM Access Analyzer



IAM business outcome:

Enable secure, external connections and speed provisioning of new users and environments by automating visibility and measuring against best practices to continuously drive down risk

Tool: IAM Access Analyzer

- IAM Access Analyzer helps identify resources in your organization and accounts that are shared with an external entity:
- IAM Access Analyzer validates IAM policies against policy grammar and best practices:
- IAM Access Analyzer generates IAM policies based on access activity in your AWS CloudTrail logs:

Mature: IAM Example

Amazon S3 Bucket “Storage” Policy:

S3 IAM Policy (simplified):
Allow Amazon S3 storage
Full Access
Policy applies to “ALL S3 storage”

Run Access Analyzer on the policy:
Recommendations based on last 90 days:

Allow Amazon S3 storage
Full Access - Unneeded access instead:
Put items into storage
Get items from storage
List items from storage
Policy applies to “ALL S3 storage” Unneeded access:
Policy applies to “S3 Storage A”

Then outputs in code that can be implemented

Amazon EC2 Server Policy:

IAM Policy (simplified):
Allow Amazon EC2 servers to be
“Started”
“Stopped”
“Terminated”
”Created”
Policy applies to “ALL EC2 Servers”

Run Access Analyzer on the policy:
Recommendations based on last 90 days:

Allow Amazon EC2 severs to be
“Started”
“Stopped”
“Terminated” –Not Used / Remove
”Created” – Not Used / Remove
Policy applies to “ALL” - Unneeded access instead
Policy applies to “EC2 instances A, B, and C”

Then outputs in code that can be implemented

Mature: IAM Example

Security Hub Integration

Amazon S3 Bucket “Storage” Policy:

Amazon S3 IAM Policy (simplified):
Allow Amazon S3 storage
Full Access
This rule applies to “ALL S3 storage”

Run Access Analyzer on the rule:
Automatic recommends based on last 90 days:

Allow Amazon S3 storage
Full Access - Unneeded access instead:
Put items into storage
Get items from storage
List items from storage
This rule applies to “ALL S3 storage” Unneeded access:
This rule applies to “S3 Storage A”

Then outputs in code that can be implemented

Before:

```
"Effect": "Allow",
        "Action":
        [
        "s3:*"
        ],

        "Resource": "arn:aws:s3:::*"
        }
          ]
```

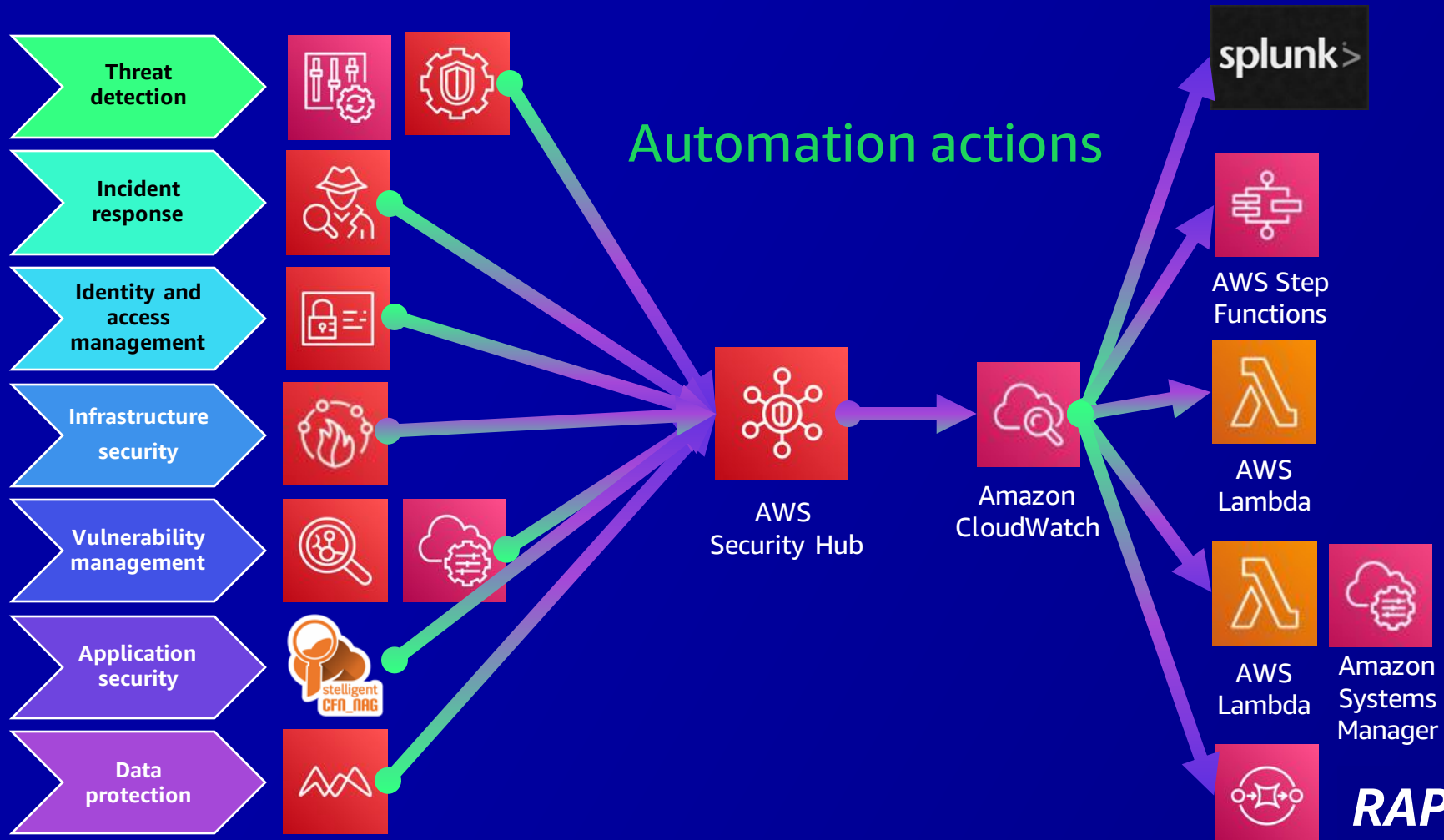
After:

```
"Effect": "Allow",
        "Action":
        [
        "s3:PutObject”,
        “s3:GetObject”,
        “s3:ListBuckets”
        ],

        "Resource": "arn:aws:s3:::${Storage A}"
        }
          ]
```

Optimize: Automate and Iterate

Security Hub



Isolation Automation

Detect questionable activity

Collect logs and revoke access

Quarantine

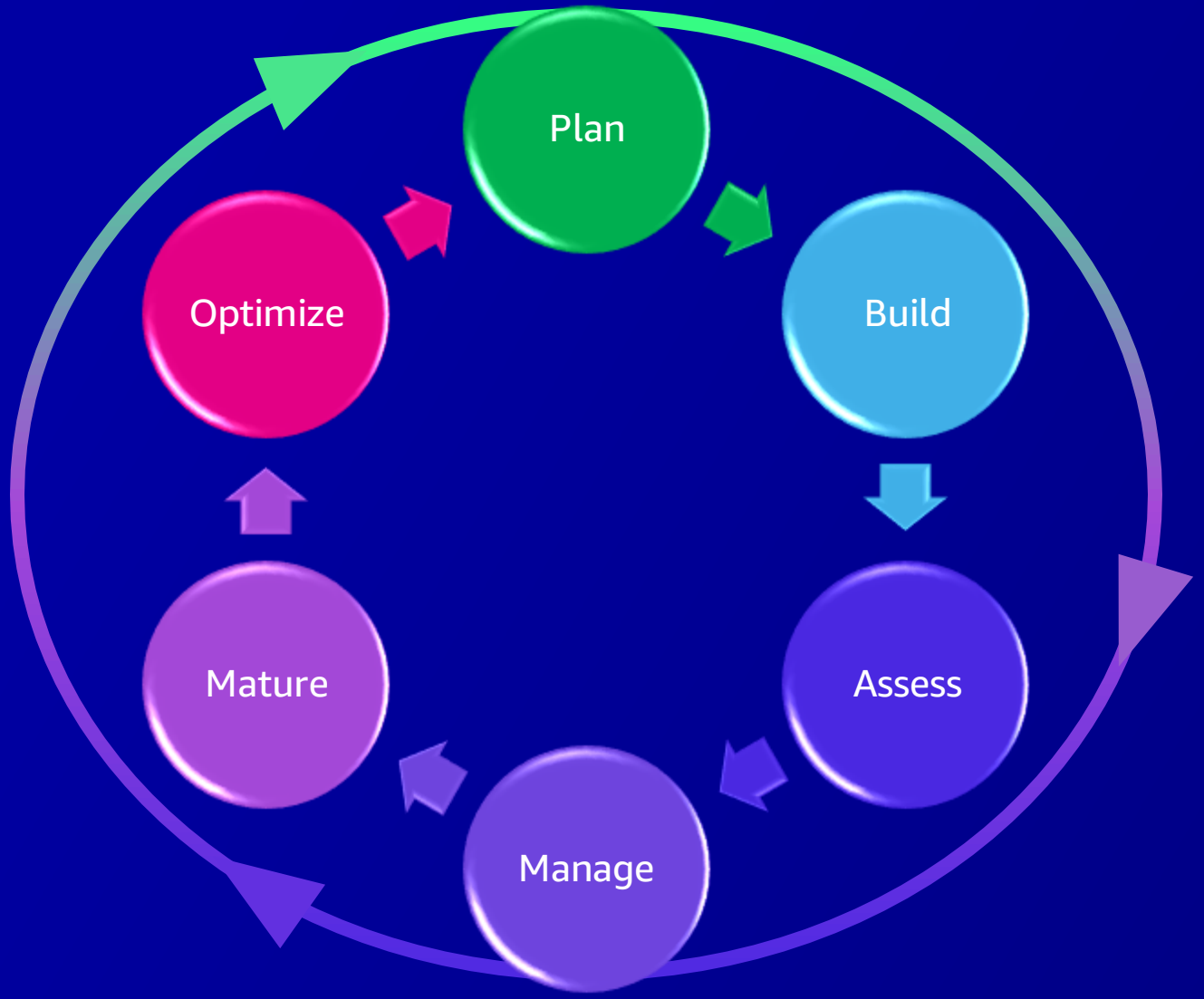
Take forensic snapshots

Replace with golden Image

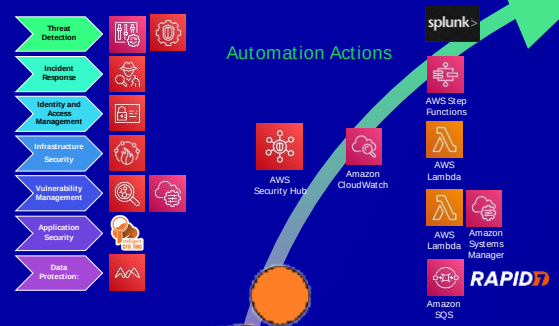
Remediate issue

Validate

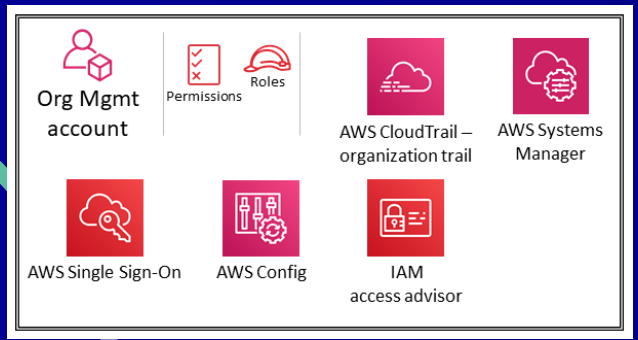
Conclusion: Crawl, Walk, Run

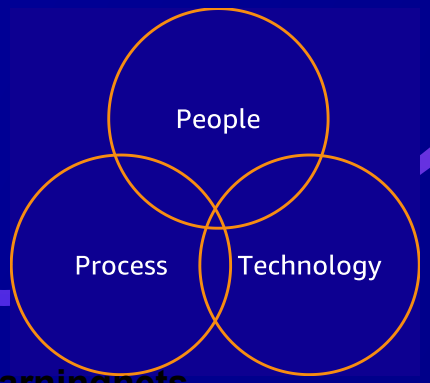


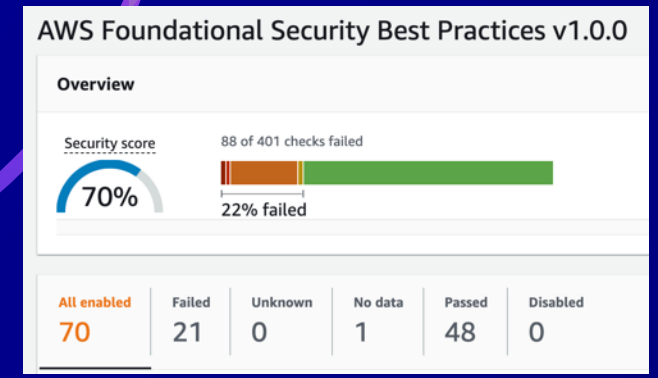
Conclusion: Crawl, walk, run, then fly!



Security governance	Assign Security contacts; Select the region(s)
Security assurance	Automate alignment with best practices using AWS Security Hub
Identity and access management	Multi-Factor Authentication; Avoid using Root and audit it; Access and role analysis with IAM Access Analyzer
Threat detection	Threat Detection with Amazon GuardDuty and review your findings; Audit API calls with AWS CloudTrail; Remediate security findings found by AWS Trusted Advisor; Billing alarms for anomaly detection
Vulnerability management	
Infrastructure protection	Limit Security Groups
Data protection	Amazon S3 Block Public Access; Analyze data security posture with Amazon Macie
Application security	AWS WAF with managed rules
Incident response	Act on Amazon GuardDuty findings







References: Crawl

Plan:

Maturity model
https://bit.ly/3PKVgeR

Security reference architecture
https://go.aws/3PqtiFG

HIPAA and HITRUST reference architectures
https://go.aws/3v6nCZi
https://go.aws/3v9n6JX

Security maturity model
https://bit.ly/3RQYHme

Build:

AWS Control Tower
https://go.aws/3yYmyI6

References: Crawl/Walk

Assess:

Prowler
https://bit.ly/3ITXYg1

Operationalize/Manage:

Cloud Adoption Framework (CAF) - Security
https://go.aws/3b0oJmr

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

CFN_NAG
https://bit.ly/3zoAlsE

References: Walk

Mature:

Agile Security
https://go.aws/3IWV5Li

AWS Security Hub Integrations
https://go.aws/3yXLgbl

CFN_NAG integration to Security Hub
https://go.aws/3v6gnjM

Access Analyzer
https://go.aws/3orpjMU

Access Analyzer Security Hub Integration
https://go.aws/3vuJAFF

Assisted Log Enabler
https://go.aws/3okJ9JI
https://bit.ly/3okg5SD

References: Run

Optimize:

Detect and alert - Splunk Phantom
https://bit.ly/3zqX3AG

Collect logs and revoke access
https://go.aws/3cASCKB

Quarantine and forensics
https://go.aws/3BaEZMi

Remediate Issue
https://go.aws/3OlrWe1

Overview
https://go.aws/3cyjYku

Thank you!

Chad Lorenc

clawssec@amazon.com

https://www.linkedin.com/in/chadlorenc/