A unique opportunity for you to be mentored by Amazonians

BeSA

Become a Solutions Architect

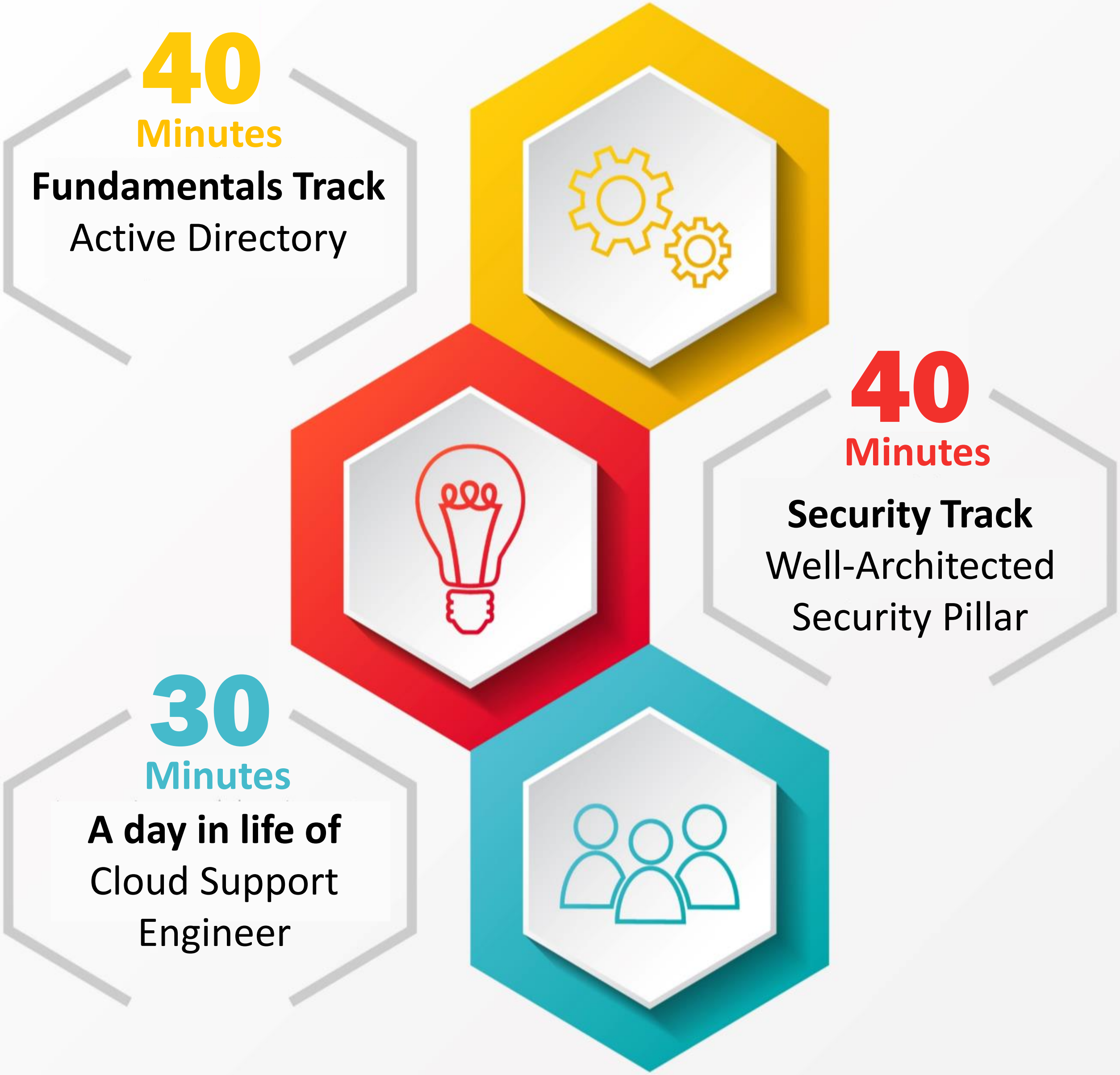
Batch 04

Week 8

26-Aug-2023

Training Motivation Direction Success Advice Goal Coaching Support

Week 08 – 26-Aug



40
Minutes
Fundamentals Track
Active Directory

40
Minutes
Security Track
Well-Architected
Security Pillar

30
Minutes
A day in life of
Cloud Support
Engineer

Nishant Buddhi

Authentication & Authorization

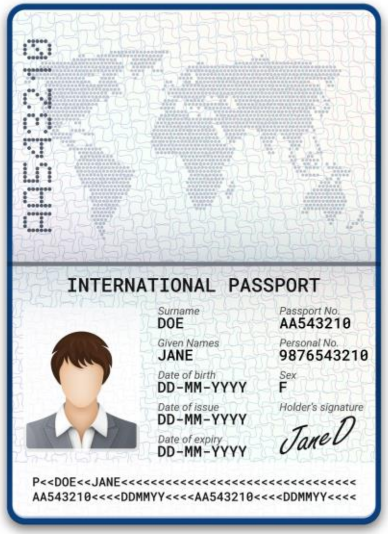
Authentication & Authorization

Authentication
- Who you are?

Authorization
- What can you do?

Authentication & Authorization

Passport



INTERNATIONAL PASSPORT

Surname DOE	*Passport No.* AA543210
Given Names JANE	*Personal No.* 9876543210
Date of birth DD-MM-YYYY	*Sex* F
Date of issue DD-MM-YYYY	*Holder's signature* Jane D
Date of expiry DD-MM-YYYY	

```
P<<DOE<<JANE<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
AA543210<<<<DDMMYY<<<<AA543210<<<<DDMMYY<<<<
```

Authentication

Who you are?

- Name
- Photo
- DOB

visa

Authorization

What can you do?

- Transit
- Work
- Tourism

Directory Services

What is a directory?

- A book containing an alphabetical index of the names and addresses of persons in a city, district, organization, etc., or of a particular category of people.

Directory services in enterprise

- A directory service is a database for storing and maintaining information about users and resources.
- Directory Services are often referred to as directories, user stores, Identity Stores, or LDAP Directory, and they store information such as usernames, passwords, user preferences, information about devices, and more.

Microsoft Active Directory

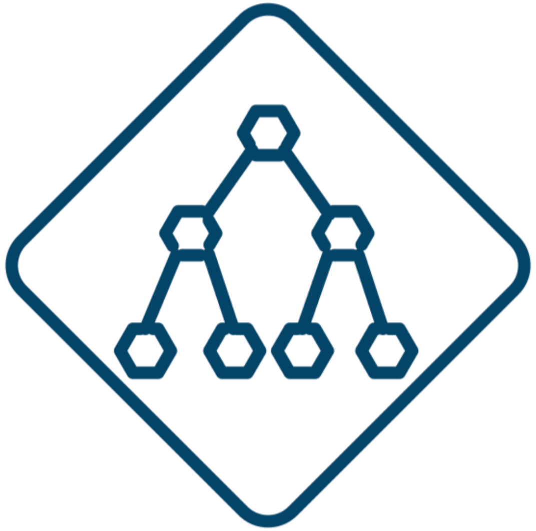
- Microsoft Active Directory, provides the methods for storing directory data and making this data available to network users and administrators.

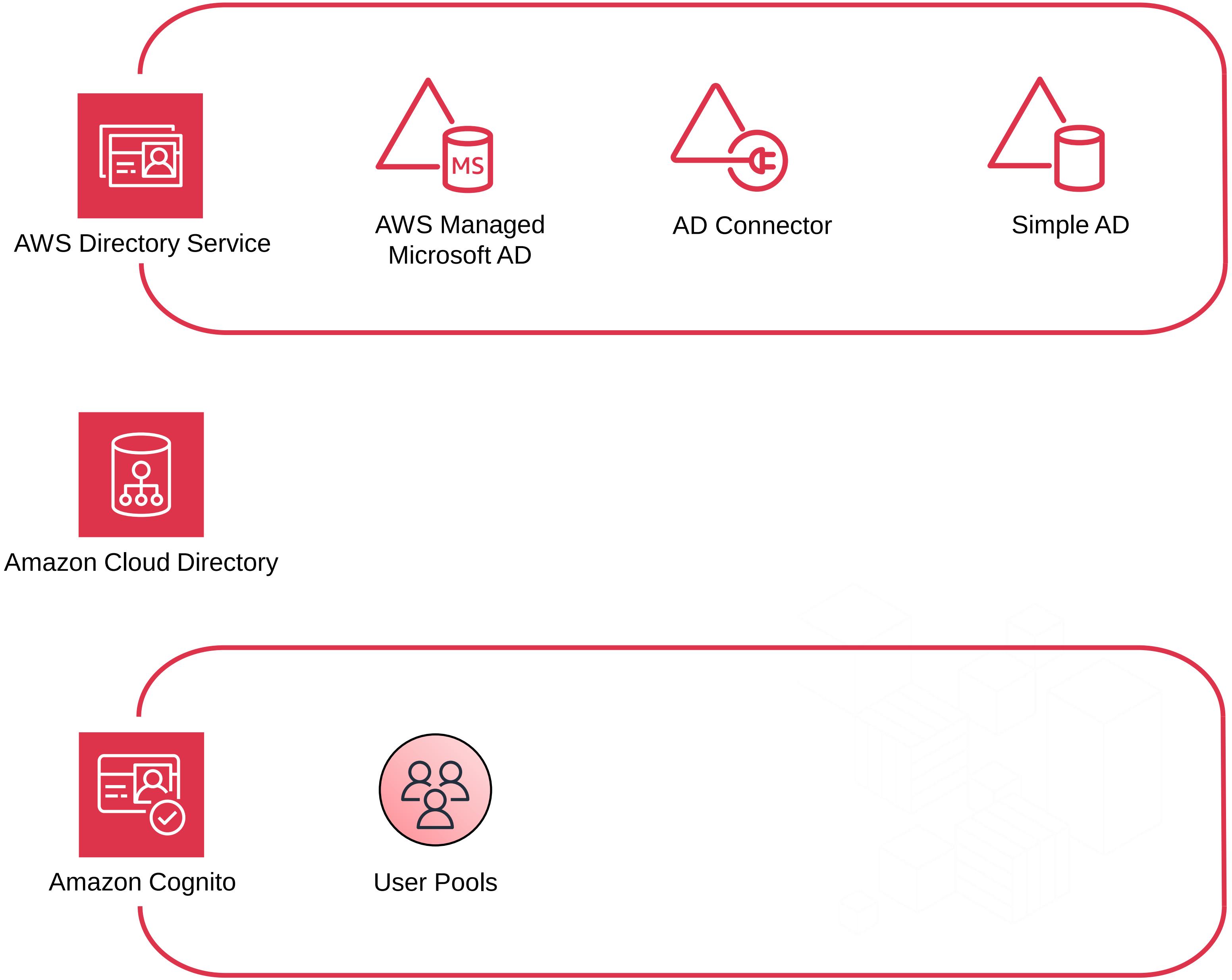
- For example, it stores information about user accounts, such as names, passwords, phone numbers, and so on.

- Security is integrated with Active Directory through logon authentication and access control to objects in the directory.

Directory Services on AWS

Directory Service
helps you store information and manage access to resources.





AWS Directory Service

AWS Managed Microsoft AD

AD Connector

Simple AD

Amazon Cloud Directory

Amazon Cognito

User Pools

AWS Directory Service

AWS Directory Service

AWS Managed Microsoft AD

- **AWS Managed Microsoft AD**
  - With AWS Managed Microsoft AD, you can easily enable your Active Directory-aware workloads and AWS resources to use managed actual Microsoft Active Directory in the AWS Cloud.

AD Connector

- **AD Connector**
  - AD Connector is a proxy for redirecting directory requests to your existing Microsoft Active Directory without caching any information in the cloud.

Simple AD

- **Simple AD**
  - Simple AD is a standalone managed directory that is powered by a Linux-Samba Active Directory–compatible server.

Which to choose?

AWS Managed Microsoft AD

- Select AWS Directory Service for Microsoft Active Directory (Standard Edition or Enterprise Edition) if you need an actual Microsoft Active Directory in the AWS Cloud.

AD Connector

- Use AD Connector if you only need to allow your on-premises users to log in to AWS applications and services with their Active Directory credentials. You can also use AD Connector to join Amazon EC2 instances to your existing Active Directory domain.

Simple AD

- Use Simple AD if you need a low-scale, low-cost directory with basic Active Directory compatibility that supports Samba 4–compatible applications, or you need LDAP compatibility for LDAP-aware applications.

Amazon Cloud Directory

Amazon Cloud Directory

- Cloud Directory is a high-performance, serverless, hierarchical data store.
- At its core, Cloud Directory is a specialized graph-based directory store that provides a foundational building block for developers.
- Cloud Directory is not a directory service for IT Administrators who want to manage or migrate their directory infrastructure.
- Cloud Directory comes ready with sample schemas for Organizations, Persons, and Devices.

Amazon Cloud Directory

Amazon Cognito

Amazon Cognito User Pools

- Amazon Cognito user pools are a managed service that lets you add secure authentication and authorization to your apps, and can scale to support millions of users.

- A User Pool is your user directory that you can configure for your web and mobile apps. A User Pool securely stores your users’ profile attributes.

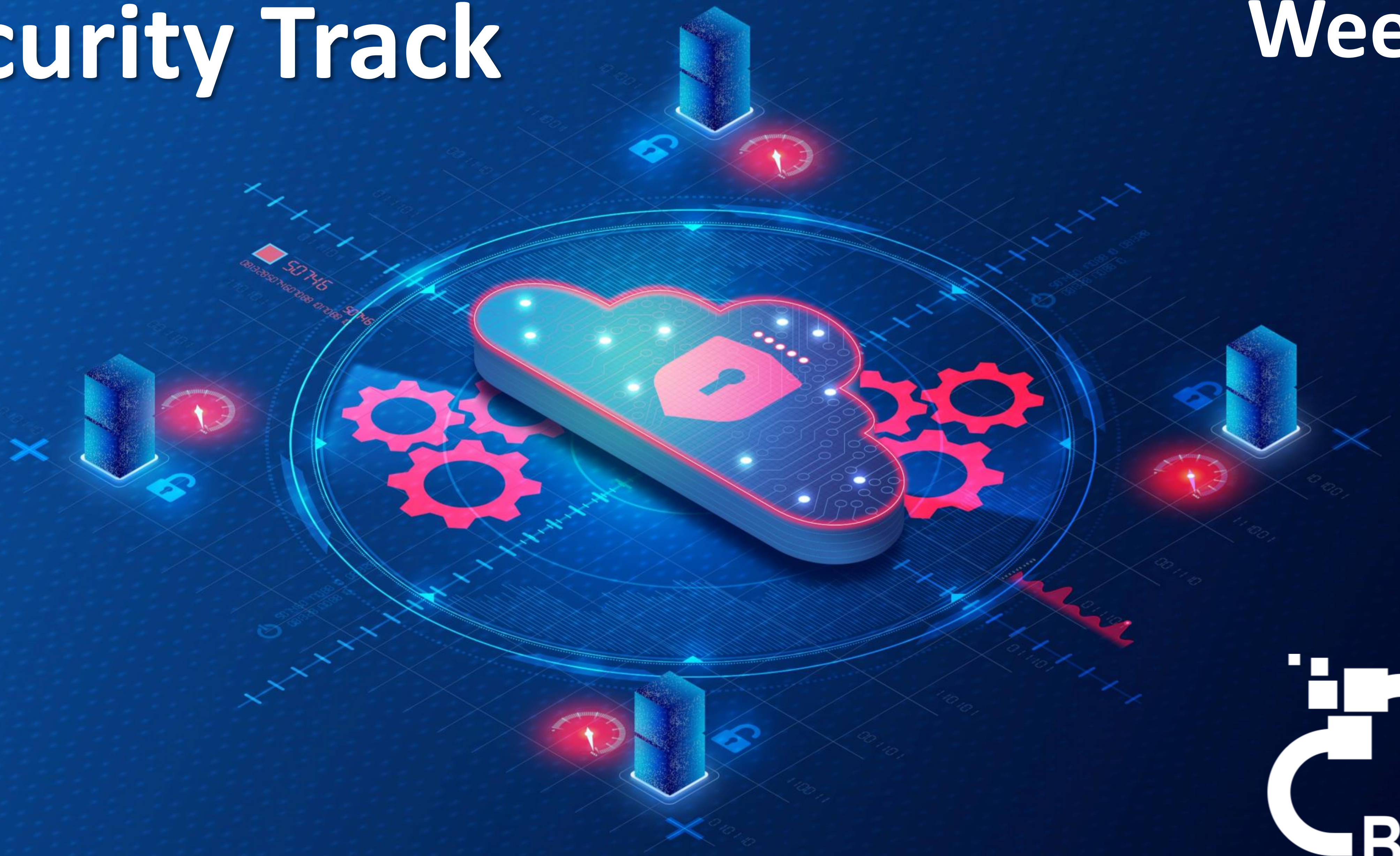
- Use Amazon Cognito if you develop high-scale SaaS applications and need a scalable directory to manage and authenticate your subscribers and that works with social media identities.

Amazon Cognito
User Pools

5 Minutes Break

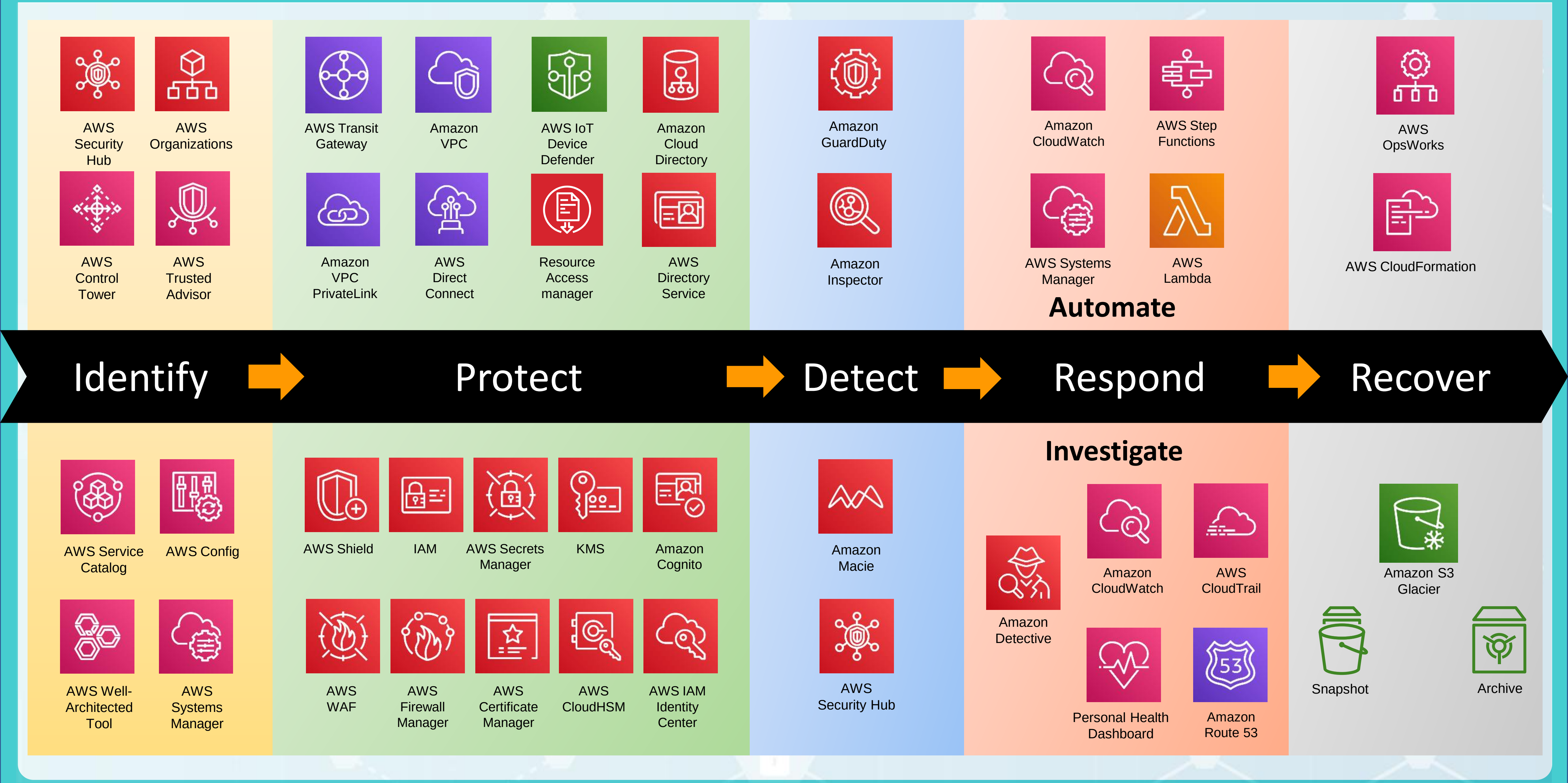
Security Track

Week 8



BeSA

AWS Foundational and Layered Security Services



Identify → Protect → Detect → Respond → Recover

Identify

AWS Security Hub
AWS Organizations
AWS Control Tower
AWS Trusted Advisor
AWS Service Catalog
AWS Config
AWS Well-Architected Tool
AWS Systems Manager

Protect

AWS Transit Gateway
Amazon VPC
AWS IoT Device Defender
Amazon Cloud Directory
Amazon VPC PrivateLink
AWS Direct Connect
Resource Access manager
AWS Directory Service
AWS Shield
IAM
AWS Secrets Manager
KMS
Amazon Cognito
AWS WAF
AWS Firewall Manager
AWS Certificate Manager
AWS CloudHSM
AWS IAM Identity Center

Detect

Amazon GuardDuty
Amazon Inspector
Amazon Macie
AWS Security Hub

Respond

Automate

Amazon CloudWatch
AWS Step Functions
AWS Systems Manager
AWS Lambda

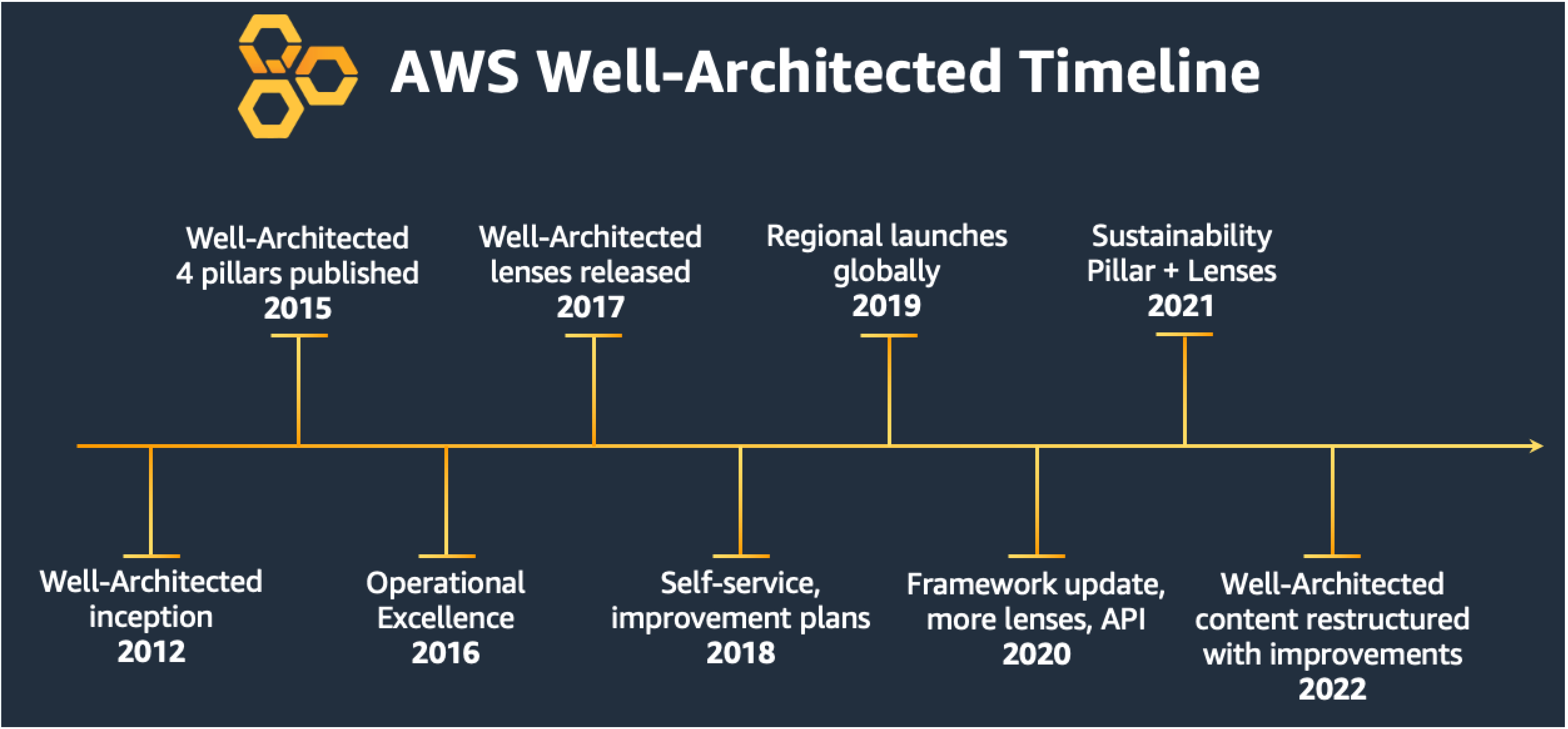
Investigate

Amazon Detective
Amazon CloudWatch
AWS CloudTrail
Personal Health Dashboard
Amazon Route 53

Recover

AWS OpsWorks
AWS CloudFormation
Amazon S3 Glacier
Snapshot
Archive

Well-Architected Framework



AWS Well-Architected Timeline

Well-Architected inception
2012

Well-Architected 4 pillars published
2015

Operational Excellence
2016

Well-Architected lenses released
2017

Self-service, improvement plans
2018

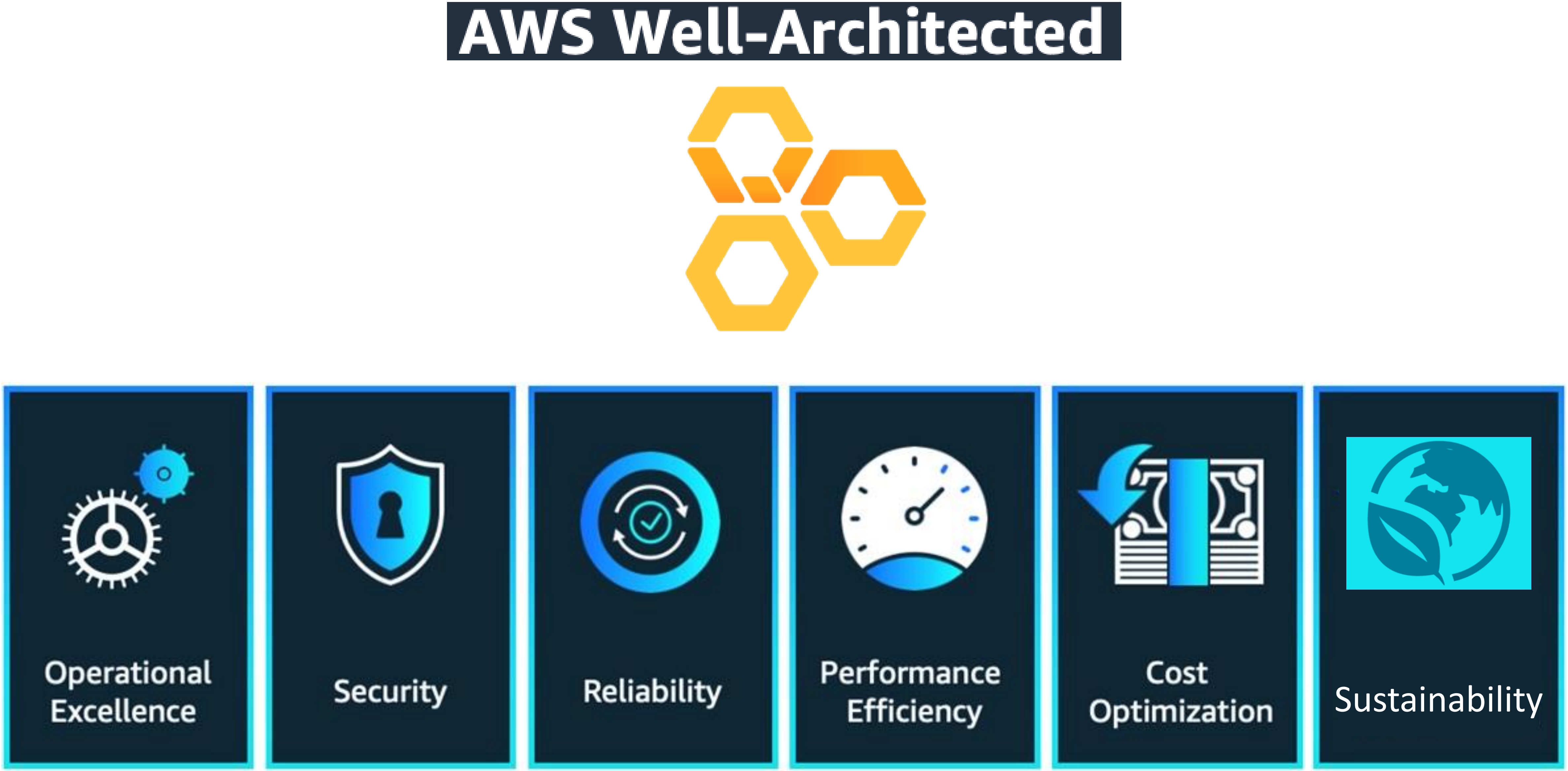
Regional launches globally
2019

Framework update, more lenses, API
2020

Sustainability Pillar + Lenses
2021

Well-Architected content restructured with improvements
2022

Six Pillars



AWS Well-Architected

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimization
- Sustainability

Security Pillar - Design Principals

- Implement a strong identity foundation
- Maintain traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Keep people away from data
- Prepare for security events

Implement a strong identity foundation

- Use the least privilege principle by creating segregation of duties (SoD), using the proper IAM roles and permissions, defining the appropriate authorization for each resource that will interact with the AWS Cloud, and limiting and centralizing privileged accesses and eliminating long-term credentials when possible

AWS Identity and Access Management (IAM)

Amazon Cognito

AWS Identity Center
(successor to AWS Single Sign-On)

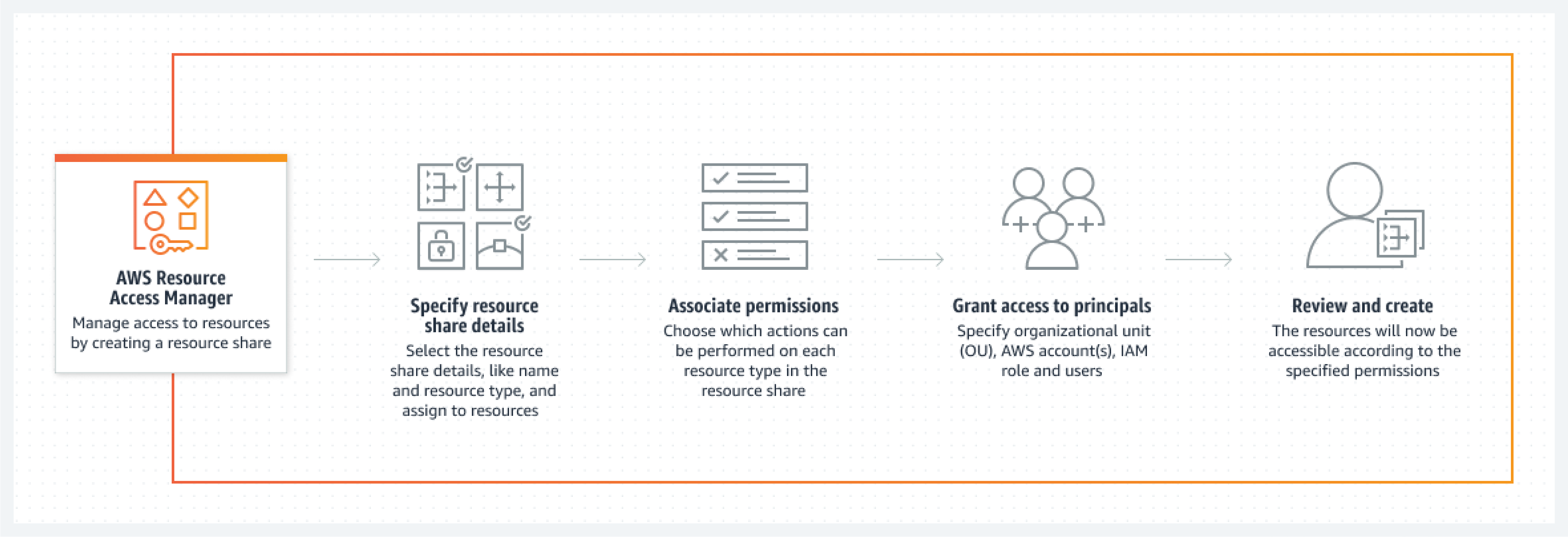
AWS Organizations

AWS Directory Service

AWS Resource Access Manager (AWS RAM)

AWS Resource Access Manager

- AWS RAM helps you securely share your resources across AWS accounts, within your organization or organizational units (OUs), and with IAM roles and users for supported resource types.



AWS Resource Access Manager

Manage access to resources by creating a resource share

Specify resource share details

Select the resource share details, like name and resource type, and assign to resources

Associate permissions

Choose which actions can be performed on each resource type in the resource share

Grant access to principals

Specify organizational unit (OU), AWS account(s), IAM role and users

Review and create

The resources will now be accessible according to the specified permissions

Enable traceability

- Enable audit logs by centralizing log collection, ingestion, protection, and enrichment, and by creating alerts that should be monitored by one or several teams that will respond to each kind of alert, based on required runbooks and playbooks

AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Amazon CloudWatch

AWS Config

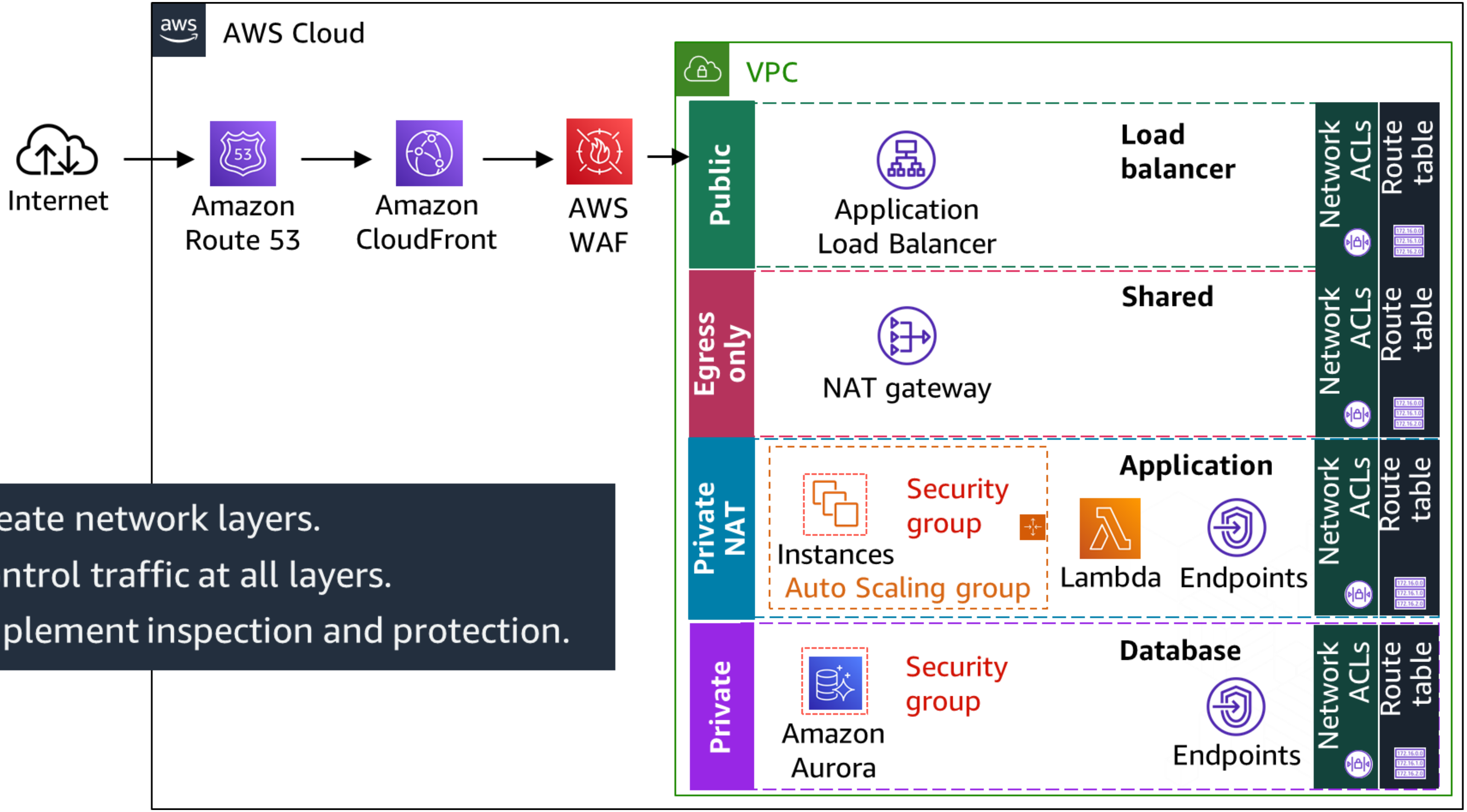
AWS CloudTrail

VPC Flow Logs

Apply Security at All Layers

- Defence-in-depth is a must; you cannot use just one layer of protection but must implement network security, OS security, load balancer security, application security, and so on. You must implement security best practices in all AWS Cloud services and components that will be a part of your application

Apply Security at All Layers



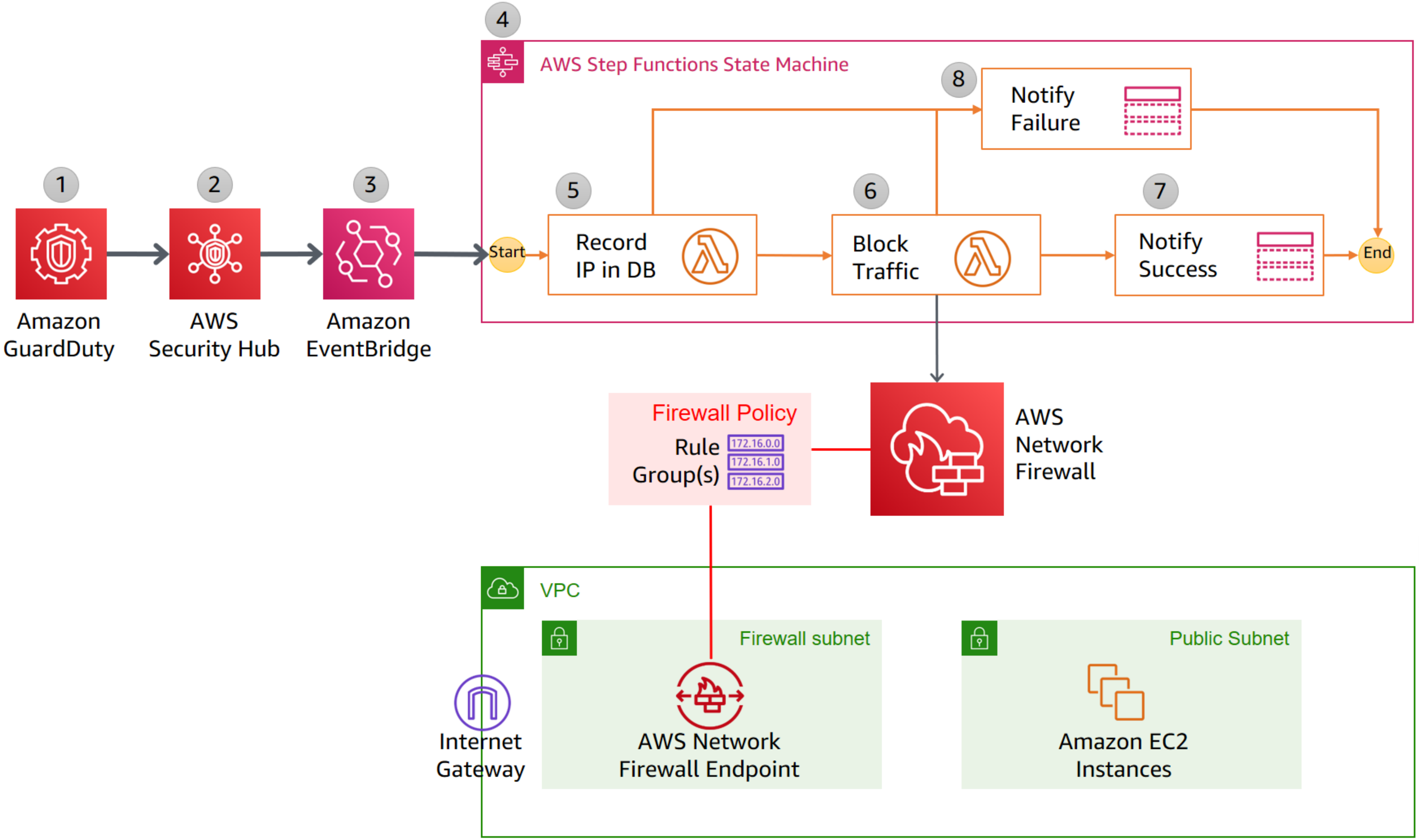
- Create network layers.
- Control traffic at all layers.
- Implement inspection and protection.

Automate security best practices

- Automation is a key function in cloud security. The best way to deploy an agile and secure environment is to leverage automation, implement security as code, and transform your paper security policies into real and coded security controls.

- As you create infrastructure as code and insert embedded security controls to achieve automated security, you can scale your cloud environments while maintaining the same level of protection

Automate security best practices



Protect Data in Transit and at Rest

- You must understand your data in order to protect sensitive information in both data exchange and storage, using encryption, tokenization, and masking resources to achieve it. You should also create and enforce access control policies to limit access to sensitive data wherever it is

Amazon Macie

AWS Key Management Service (AWS KMS)

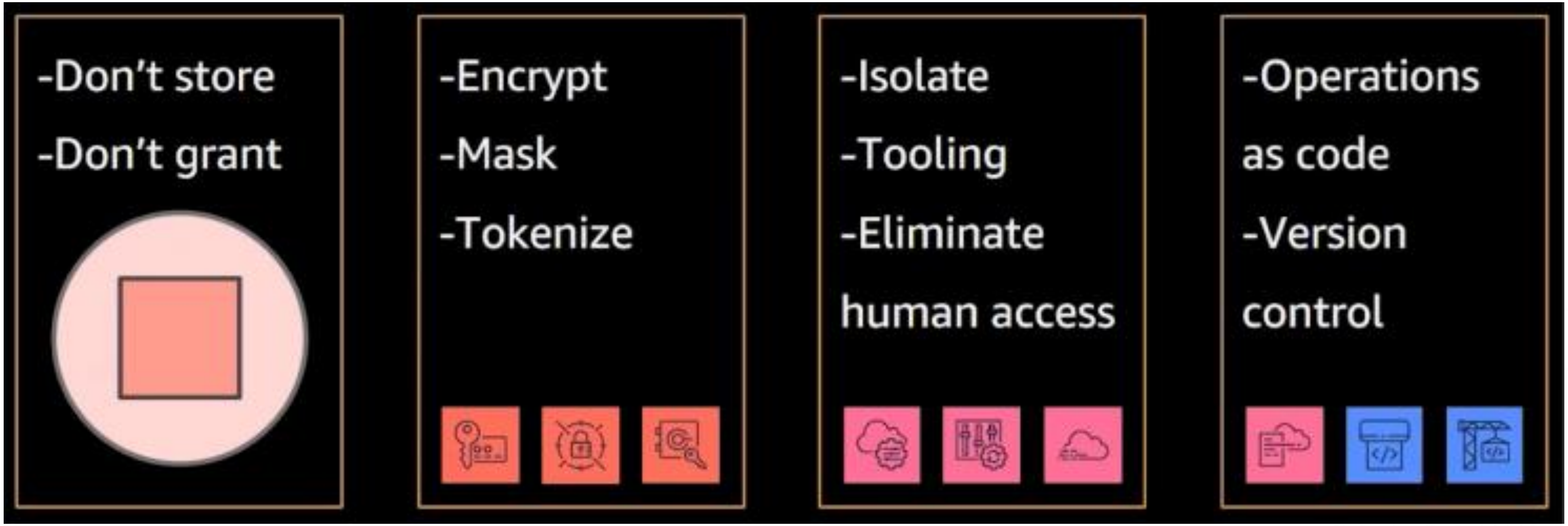
AWS CloudHSM

AWS Certificate Manager (ACM)

Server-side encryption (SSE)

Keep People Away from Data

- You must create mechanisms and tools to reduce or eliminate manual and human access to production data, thus reducing operation risks related to human mistakes when handling sensitive data



-Don’t store

-Don’t grant

-Encrypt

-Mask

-Tokenize

-Isolate

-Tooling

-Eliminate human access

-Operations as code

-Version control

Prepare for Security Events

- You must define an incident response management practice, running incident simulations, creating tools, using automation, and running playbooks to improve the security incident capabilities

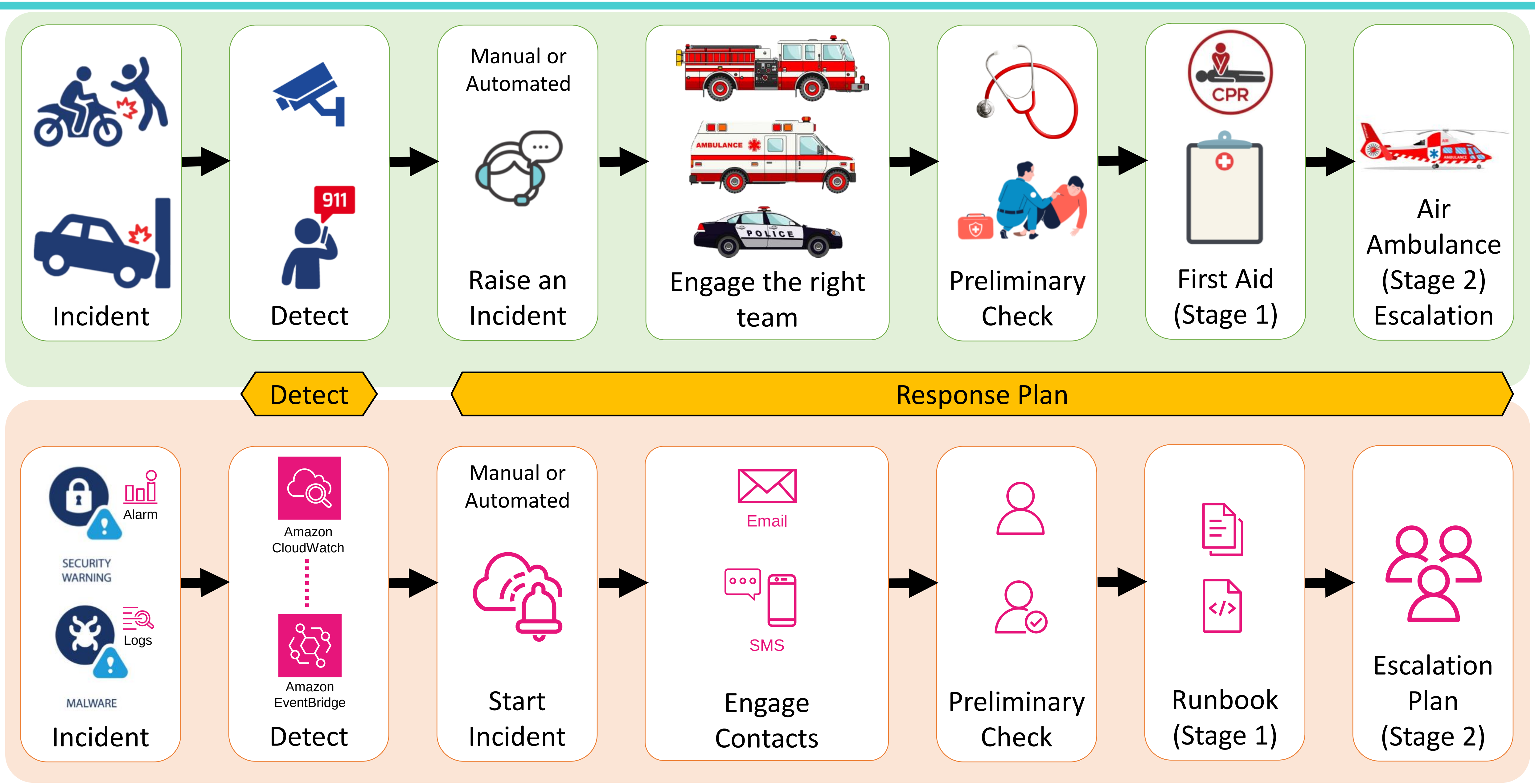
Incident Manager

- Incident
  - General Definition – Unusual or unexpected happening
  - IT Definition – An issue with application or service
- AWS Systems Manager Incident Manager provides a step-by-step framework based on best practices to identify and react to incidents, such as service outages or security threats.
- The primary focus of Incident Manager is to help restore affected services or applications to normal as quickly as possible through a complete incident lifecycle management solution.

Example

Incident Manager

Incident Management



Incident → Detect → Manual or Automated Raise an Incident → Engage the right team → Preliminary Check → First Aid (Stage 1) → Air Ambulance (Stage 2) Escalation

Detect

Response Plan

Incident → Detect → Manual or Automated Start Incident → Engage Contacts → Preliminary Check → Runbook (Stage 1) → Escalation Plan (Stage 2)

A day in the life of an Amazonian

Nishant Buddhi

Cloud Support Engineer

Thank you for attending.
See you next Saturday (2-Sep-2023)

BeSA

Become a Solutions Architect

For content check **Resources Link** on BeSA Home Page