NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

# Principles in Cloud Architecture Design - Security

Cloud Infrastructure Engineering

**Nanyang Technological University**
**& Skills Union - 2022/2023**

# Course Content

- Quick Check-In
- Dive into the best practices in terms of Security
- Explore AWS current recommendations to use when designing cloud architectures with security
- Explore Strategies to use when designing cloud architectures
- Build architectures that protect the data and systems
- Build system using AWS recommendations and strategies

| Time | What | How or Why |
| --- | --- | --- |
| 7:15pm - 7:45pm | Part 1 - Presentation | Security Design Principles |
| 7:45pm - 8:10pm | Part 2 - Presentation | Best Practices for Security |
| 8:10pm - 8:20pm | Break | |
| 8:20pm - 8:45pm | Part 3 - Presentation | Best Practices for Security |
| 8:45pm - 10:00pm | Summary & Assignments | |

# Recap

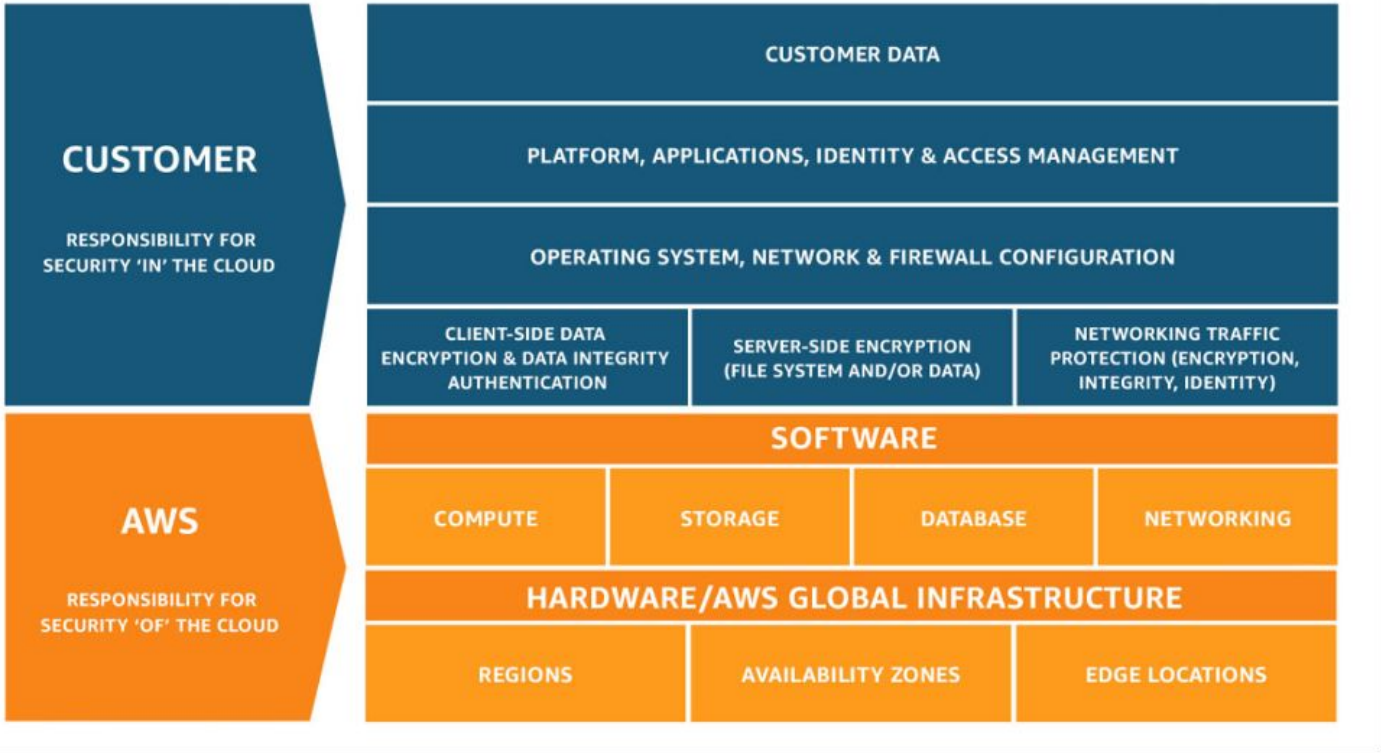
- Edge Locations
- Availability Zones
- Regions
- CDN Use Cases
  - High-speed Content Delivery, Real-time Streaming, Multi-user Scaling
- CDN Benefits
  - Improve Webpages Load Time, Reduce Bandwidth Cost, Increasing Content Availability & Redundancy, Improve Website Security

# Self Study Check-In

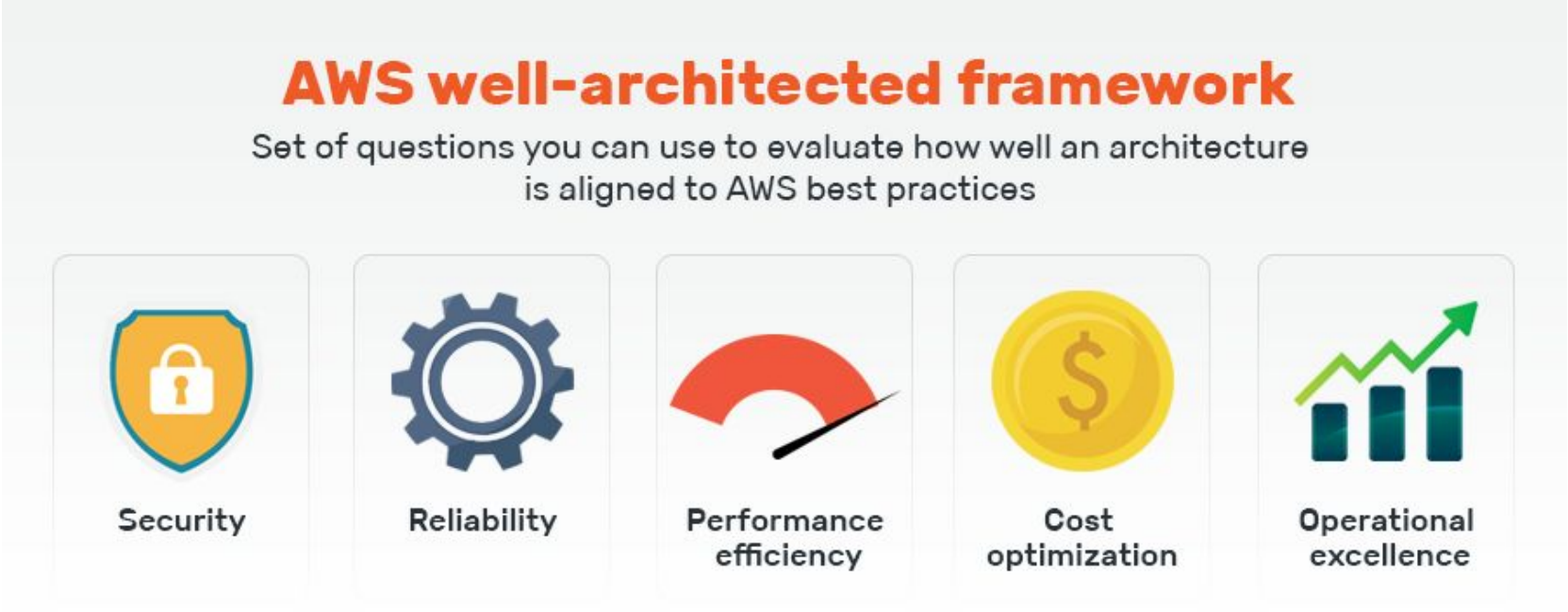
# Q1) How do you manage permissions for people and machines?

# Overview

# Responsibilities On The Cloud



# Overview


AWS well-architected framework
Set of questions you can use to evaluate how well an architecture is aligned to AWS best practices
Security
Reliability
Performance efficiency
Cost optimization
Operational excellence

# Overview

This module focuses on the **security** pillar. This will help to **meet the business and regulatory requirements** by following current AWS recommendations.

It’s intended for those in technology roles, such as chief technology officers (CTOs), chief information security officers (CSOs/CISOs), architects, developers, and operations team members.

# Overview

We will **understand AWS current recommendations and strategies to use when designing cloud architectures with security** in mind.

This module doesn't provide implementation details or architectural patterns but does include references to appropriate resources for this information.

By **adopting the practices** in this module, we can build architectures that protect our data and systems, control access, and respond automatically to security events.

# Security Design Principles

# Security Design Principles Summary

- Implement a Strong Identity Foundation
- Enable Traceability
- Apply Security At All Layers
- Automate Security Best Practices
- Protect Data In-Transit & At-Rest
- Keep People Away From Data
- Prepare For Security Events

# Implement a Strong Identity Foundation

Implement the **principle of least privilege** and **enforce separation of duties with appropriate authorization** for each interaction with your AWS resources.

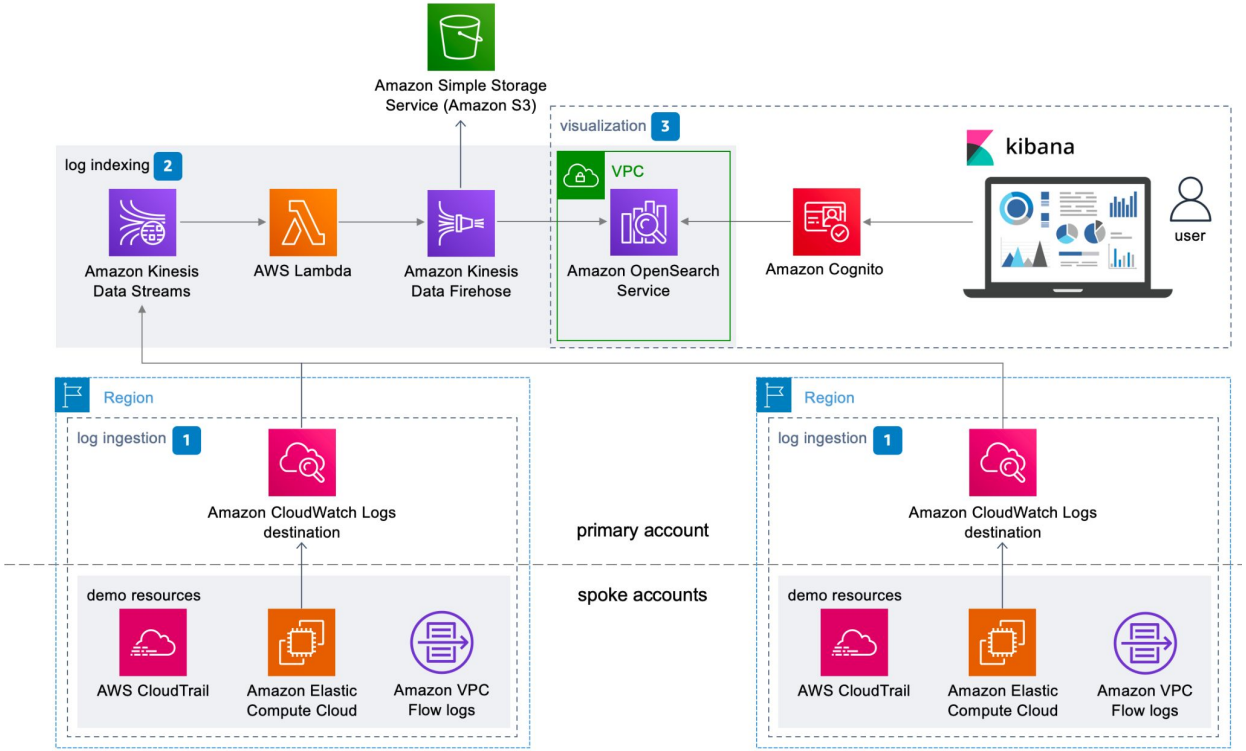
**Centralize identity management**, and aim to **eliminate reliance on long-term static credentials**.

# Enable Traceability

**Monitor, alert, and audit actions and changes** to your environment in real time.

**Integrate log and metric collection** with systems to automatically investigate and take action.

# Enable Traceability

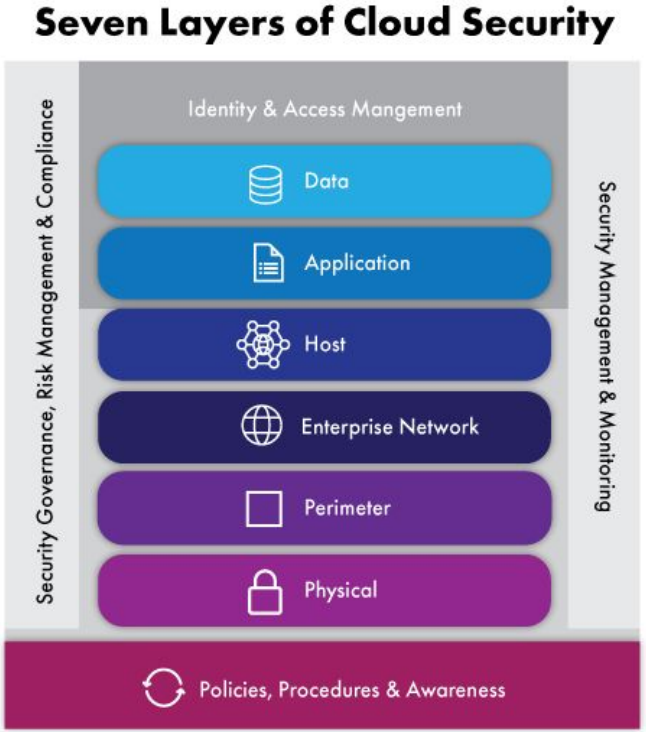


# Apply Security At All Layers

Apply a **defense in depth approach** with multiple security controls.

Apply to all layers (for example, edge of network, VPC, load balancing, every instance and compute service, operating system, application, and code).

# Apply Security At All Layers

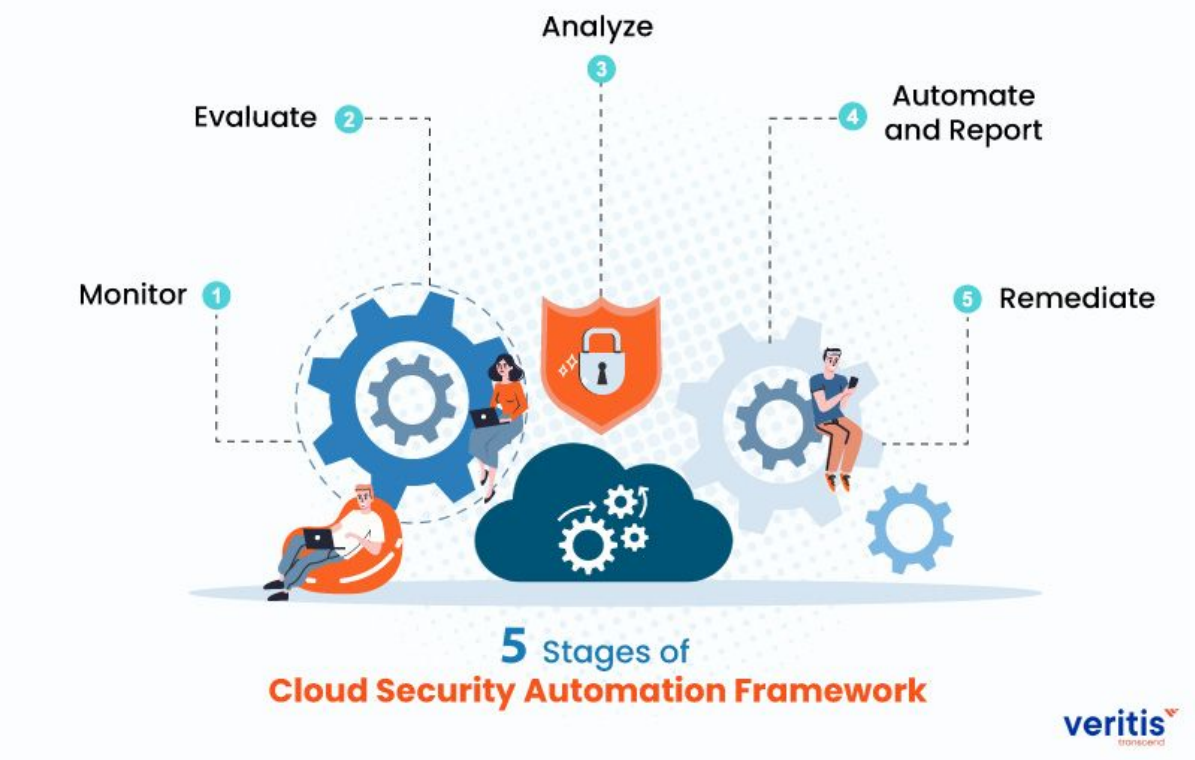


# Automate Security Best Practices

Automated software-based security mechanisms **improve your ability to securely scale more rapidly and cost-effectively**.

Create secure architectures, including the **implementation of controls that are defined and managed as code in version-controlled templates**.

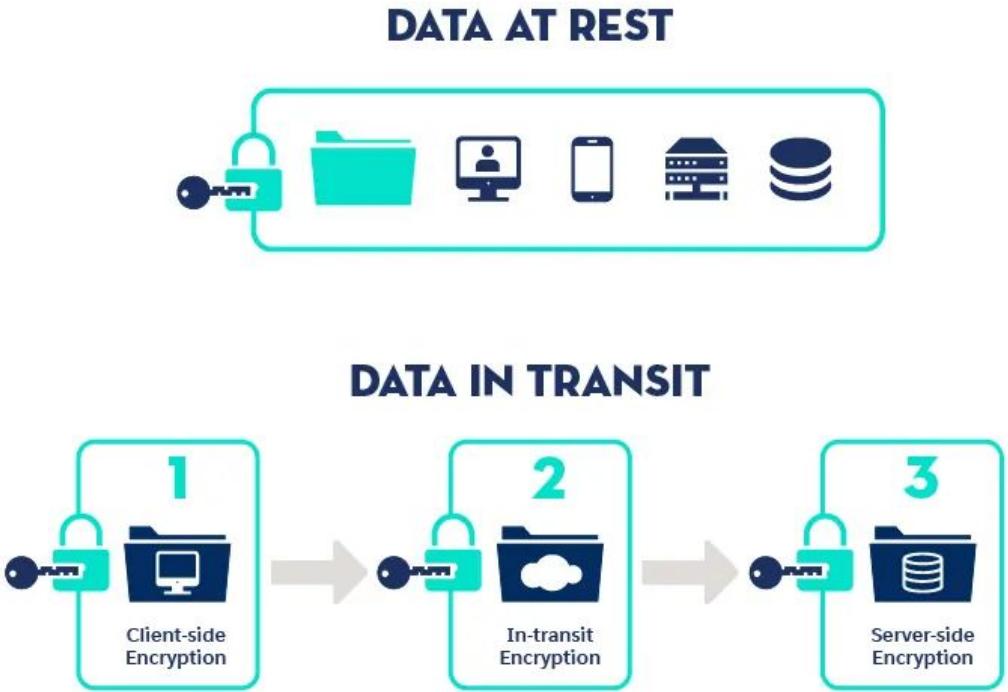
# Automate Security Best Practices



# Protect Data In-Transit & At-Rest

Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control where appropriate.

# Protect Data In-Transit & At-Rest



# Keep People Away From Data

Use mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data.

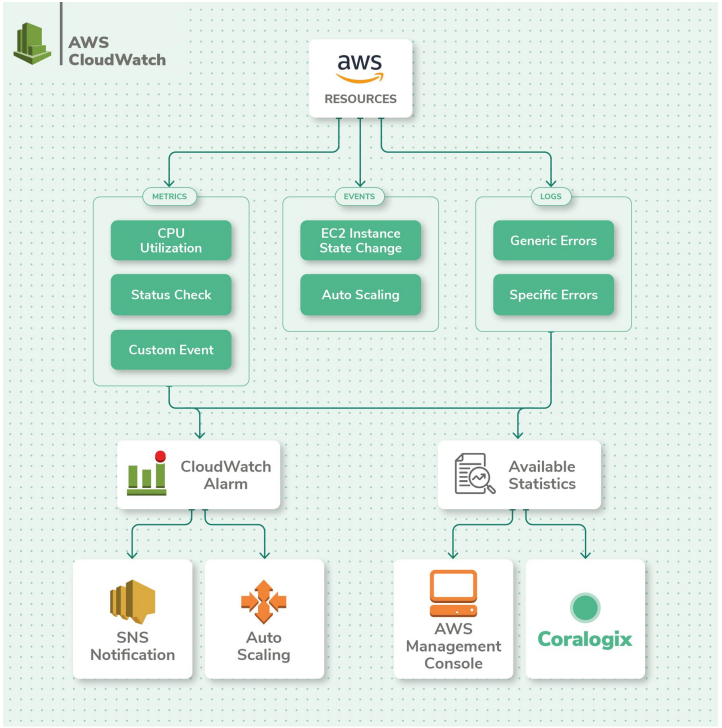
This **reduces the risk of mishandling or modification and human error** when handling sensitive data.

# Prepare For Security Events

Prepare for an incident by **having incident management** and **investigation policy and processes** that align to your organizational requirements.

Run **incident response simulations** and **use tools with automation** to increase your speed for **detection, investigation, and recovery**.

# Prepare For Security Events



# Prepare For Security Events

# Security Design Principles Summary

- Implement a Strong Identity Foundation
- Enable Traceability
- Apply Security At All Layers
- Automate Security Best Practices
- Protect Data In-Transit & At-Rest
- Keep People Away From Data
- Prepare For Security Events

# Group Activity

In this activity, gather into your own group and each group should take on one or two research problem.

Ensure all research problems are taken and presented by the end of this section.

# Group Activity

- Implement a strong identity foundation
- Enable 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

# Best Practices For Security

# Overview

There are six best practice areas for security in the cloud:

- Security
- Identity and Access Management
- Detection
- Infrastructure Protection
- Data Protection
- Incident Response

# Security

To operate our workload securely, we **must apply overarching best practices to every area of security**.

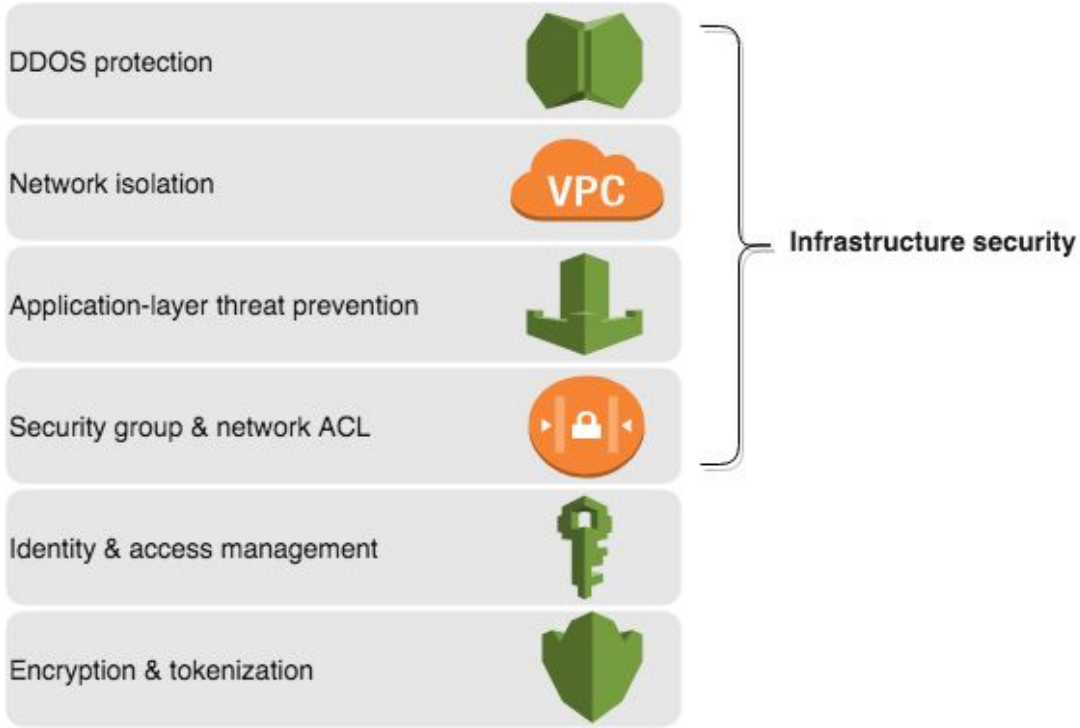
Take requirements and processes that we have defined in operational excellence at an organizational and workload level, and apply them to all areas.

# Security

**Staying up to date with AWS and industry recommendations and threat intelligence** helps us evolve our threat model and control objectives.

Automating security processes, testing, and validation allow us to scale our security operations.

# Security


DDOS protection
Network isolation
VPC
Application-layer threat prevention
Security group & network ACL
Identity & access management
Encryption & tokenization
Infrastructure security

# IAM

IAM are key parts of an information security program, **ensuring that only authorized and authenticated users and components** are **able to access** your resources as intended.

For example, we **should define principals** (that is, accounts, users, roles, and services that can perform actions in our account), **build out policies aligned with these principals**, and **implement strong credential management**.

These privilege-management elements form the core of authentication and authorization.

# IAM

In AWS, privilege management is primarily supported by the IAM service, which allows us to **control user and programmatic access** to AWS services and resources.

We should apply **granular policies**, which assign permissions to a user, group, role, or resource.

# IAM

We also have the ability to **require strong password practices**, such as complexity level, **avoiding re-use**, and enforcing **MFA**.

We can use **federation** with our existing directory service.

For workloads that require systems to have access to AWS, IAM enables secure access through roles, instance profiles, identity federation, and **temporary credentials.**

# Detection

We can use detective controls to **identify a potential security threat or incident**.

For example, **conducting an inventory of assets and their detailed attributes** promotes more effective decision making (and lifecycle controls) to help establish operational baselines.

We can also use **internal auditing**, an examination of controls related to information systems, to ensure that practices meet policies and requirements and that we have set the correct automated alerting notifications based on defined conditions.

These controls are important reactive factors that can **help our organization identify and understand the scope of anomalous activity.**

# Detection

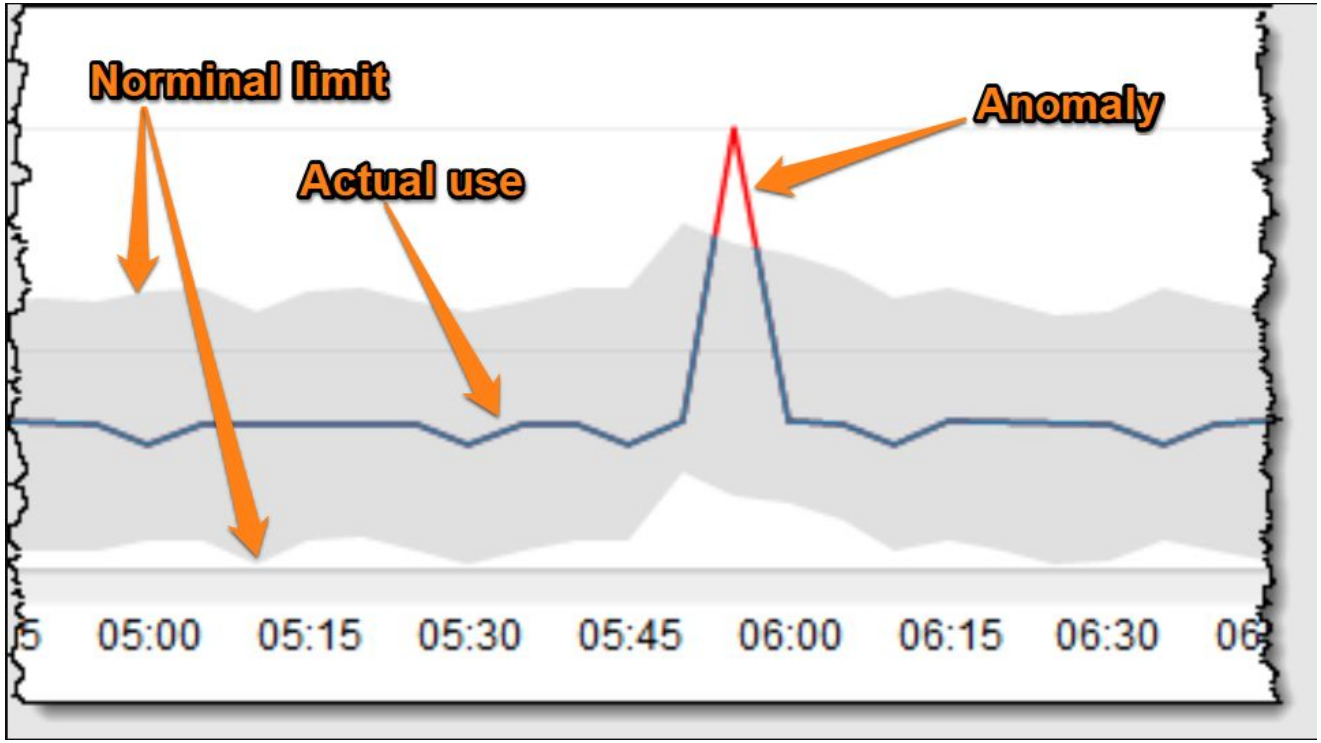
In AWS, we can **implement detective controls** by **processing logs, events, and monitoring that allows for auditing, automated analysis, and alarming**.

**CloudTrail logs, AWS API calls, and CloudWatch** provide monitoring of metrics with alarming, and AWS Config provides configuration history.

**GuardDuty** is a **managed threat detection service** that continuously **monitors** for **malicious or unauthorized behavior** to help us protect your AWS accounts and workloads.

Service-level logs are also available, for example, we can use AWS S3 to **log access requests.**

# Detection


Norminal limit
Actual use
Anomaly
05:00
05:15
05:30
05:45
06:00
06:15
06:30

# Infrastructure Protection

Infrastructure protection encompasses control methodologies, such as **defense in depth**, necessary to meet best practices and organizational or regulatory obligations.

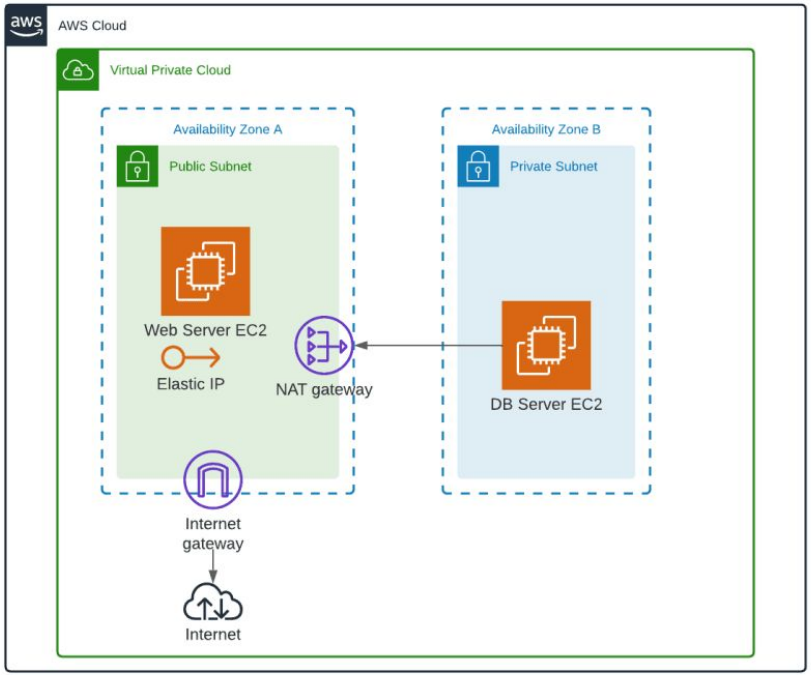
Use of these methodologies is critical for successful, ongoing operations in either the cloud or on-premises.

# Infrastructure Protection

In AWS, we can **implement stateful and stateless packet inspection**, either by using AWS-native technologies or by using partner products and services available through the AWS Marketplace.

We should use VPCs to **create a private, secured, and scalable environment** in which we can define our topology—including gateways, routing tables, and public and private subnets.

# Infrastructure Protection



# Data Protection

Before architecting any system, **foundational practices that influence security should be in place.**

For example, **data classification** provides a way to **categorize organizational data based on levels of sensitivity**, and **encryption protects data** by way of rendering it unintelligible to unauthorized access.

These tools and techniques are important because they support objectives such as preventing financial loss or complying with regulatory obligations.

# Data Protection

In AWS, the following practices facilitate protection of data:

- As an AWS customer **you maintain full control over your data**.
- AWS makes it easier for you to **encrypt your data and manage keys**, including regular key rotation, which can be easily automated by AWS or maintained by you.
- **Detailed logging** that contains important content, such as file access and changes, is available.

# Data Protection

In AWS, the following practices facilitate protection of data:

- AWS has designed storage systems for exceptional **resiliency**. For example, Amazon S3 Standard, S3 Standard–IA, S3 One Zone-IA, and Amazon Glacier are all designed to provide 99.999999999% durability of objects over a given year. **Versioning**, which can be part of a larger data lifecycle management process, can protect against accidental overwrites, deletes, and similar harm.
- AWS never initiates the movement of data between Regions. Content placed in a Region will remain in that Region unless you explicitly enable a feature or leverage a service that provides that functionality.

# Incident Response

Even with extremely mature preventive and detective controls, our organization **should still put processes in place to respond to and mitigate the potential impact of security incidents.**

The architecture of our workload strongly affects the ability of your teams to operate effectively during an incident, to isolate or contain systems, and to restore operations to a known good state.

**Putting in place the tools and access ahead of a security incident**, then routinely practicing incident response through game days, **will help you ensure that your architecture can accommodate timely investigation and recovery**.

# Incident Response

In AWS, the following practices facilitate effective incident response:

- **Detailed logging** is available that contains important content, such as file access and changes.
- Events can be **automatically processed and trigger tools that automate responses** through the use of AWS APIs.
- We can **pre-provision tooling** and a "**clean room**" using AWS CloudFormation. This allows us to carry out forensics in a safe, **isolated environment**.

# Security Summary

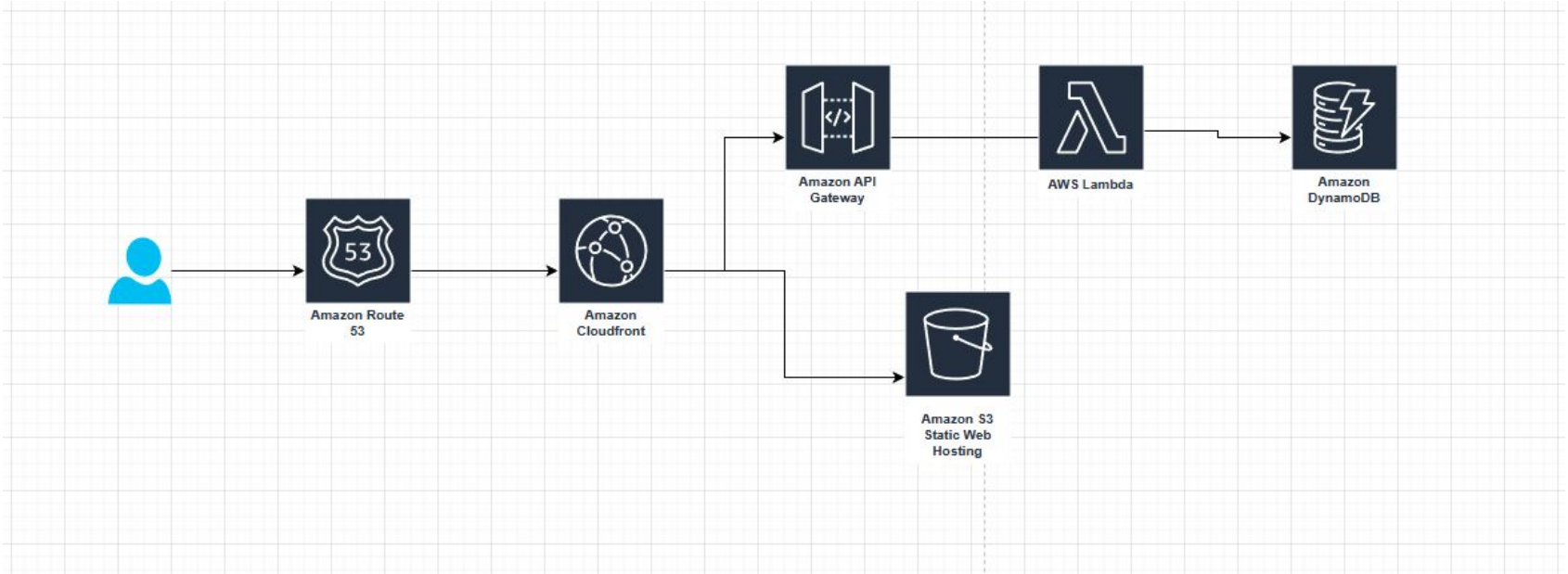
- Security
- Identity and Access Management
- Detection
- Infrastructure Protection
- Data Protection
- Incident Response

# Activity - Understanding Security

In this activity, gather into your own group and each group should take on one or two research problem.

Ensure all research problems are taken and presented by the end of this section.

# Activity - Understanding Security



# Activity - Understanding Security

- How do you securely operate your workload?
- How do you manage identities for people and machines?
- How do you detect and investigate security events?
- How do you protect your data at rest?
- How do you protect your data in transit?
- How do you anticipate, respond to, and recover from incidents?

Bonus: How do you protect your network resources?(If there are)

# Activity - Understanding Security

- How do you securely operate your workload?
- How do you manage identities for people and machines?
- How do you detect and investigate security events?
- How do you protect your network resources?
- How do you classify your data?
- How do you protect your data at rest?
- How do you anticipate, respond to, and recover from incidents?

# Activity

Learner:

- Clean up AWS.
- Remove/delete/terminate all service/ resources that created.

Instructor

- Clean up AWS.
- Remove/delete/terminate all service/ resources that created.
- Check the AWS account after learner clean up.

# What’s Next?