***Build a Secure Cloud***

1. **CloudWatch Alarms and Event Rules**

Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real time. CloudWatch alarms send notifications or automatically make changes to the resources you are monitoring based on rules that you define.

Amazon CloudWatch Events delivers a near real-time stream of system events that describe changes in Amazon Web Services (AWS) resources. Using event rules, you can get notifications when certain events are matched and/or trigger responses through Lambda functions

1. **Config Rules**

Use AWS Config rule to evaluate the configuration settings of your AWS resources. While AWS Config continuously tracks the configuration changes that occur among your resources, it checks whether these changes violate any of the conditions in your rules. If a resource violates a rule, AWS Config flags the resource and the rule as noncompliant.

1. **Auto Remediation Rules**

A collection of Automatic Remediation rules to automatically respond to misconfigurations in an AWS account. Rules use Config Rules for detection and *CloudWatch Event Rules and SSM Automations* for response. Auto Remediation rules cover various AWS services such EC2 and S3.

Some Auto Remediation Rules:

The following rules are available:

* **S3:**
  + Enable S3 Object Versioning if disabled
  + Enable S3 Server-Side Encryption if disabled
  + Enable S3 Server Access Logging if disabled
* **EC2**
  + Stop or Terminate EC2 instances with public IPs
  + Stop or Terminate EC2 instances with unapproved type or tenancy mode
  + Stop or Terminate EC2 instances with unapproved AMIs
* **Other**
  + Automatically release Elastic IPs that are not attached to network interfaces.

In addition to the above services, the following additional configuration can be enabled:

* **AWS Config** which must be enabled to add Config Rules.
* **Email Notifications**: Enable notifications for Config Rules compliance change events using **CloudWatch Event Rules** and **SNS**.

1. **Amazon GuardDuty**

Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers.

1. **AWS Security Hub**

A collection of AWS Security controls for AWS Security Hub. Configuration items include templates to set up AWS Security Hub in an account as well as templates to enable compliance standards checking such as CIS Foundation benchmarks for AWS.

1. **Billing and Cost Management**

AWS controls and solutions to help manage costs in an AWS environment. Controls include *AWS Budgets and CloudWatch alarms.*

1. **Logging & Monitoring Configurations**

Native AWS logging configurations and services that you can leverage to provide greater visibility near to real time for occurrences in the AWS environment. Currently this includes *AWS CloudTrail and AWS Config*.

1. **Service Control Policies**

Service Control Policies (SCPs) that can be applied to accounts managed by *AWS Organizations*. SCPs enable you to restrict, at the account level of granularity, what services and actions the users, groups, and roles in those accounts can do.

1. **AWS Systems Manager**

A collection of AWS Systems Manager (SSM) configuration templates for the automation of security and operation tasks in AWS environments. Configuration items include templates to configure patching, maintenance windows, required IAM roles for SSM operations, as well as security configurations to support AWS SSM such as IAM policies, config rules, and more.

1. **Security Groups & NACLs**

A security group acts as a virtual firewall that controls the traffic for one or more EC2 or RDS instances. EC2 or RDS instances can be associated with one or more security groups.

A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC

1. **IAM Policies**

A list of IAM policies that can help you define permissions for your IAM identities.

1. **AWS Logging Services**

A configuration package to enable AWS security logging and activity monitoring services: AWS CloudTrail, AWS Config, and Amazon GuardDuty. You can use an S3 bucket to store CloudTrail and Config history logs, as well as an CloudWatch log group to receive CloudTrail logs.

1. **EC2 Security Strategy**

Resources for implementing a comprehensive EC2 security strategy. Included are customizable configuration items and packages, as well as guides for encryption, authentication, access control, monitoring and compliance, vulnerability and patch management, backup options and more.

**Encryption**

Enable at-rest encryption for all EC2 instances by configuring **default EBS encryption** on the region level for the AWS account. For additional security, create a new KMS encryption key for the default encryption (otherwise use the default AWS managed key).

**Network Access and Security**

Control network access to and from EC2 instances using **Security Groups**. Security groups whitelist traffic by protocols, ports, and source IP addresses (or security groups). For an additional layer of security, use **Network Access Lists (NACLs)** to allow or deny traffic on the subnet level.

For new environments, build a secure VPC with separate subnet tiers for public and private resources, and utilize multiple availability zones (AZs) for high availability. Build a custom VPC that fits your environment

**Internet Connectivity**

Internet access from EC2 instances is required to access AWS API endpoints, download software updates and patches, or for other application requirements.

Use VPC Endpoints to provide private access from VPCs to AWS API endpoints, without allowing internet access.

Where internet access is required, proxy solutions can be used to whitelist allowed URLs and domains on the internet.

**Authentication**

Use AWS SSM **Session Manager** or **EC2 Connect** to access EC2 instances without relying on long-term keys, and to provide an audit trail for users access instances. Session Manager also allows logging users' sessions to CloudWatch Logs or S3:

* **AWS Session Manager**: Uses the AWS Systems Manager (SSM) agent to provide a bash or powershell session for the IAM user, without having to open any inbound ports on the instance.
* **EC2 Connect**: Supported on CentOs and Amazon Linux, and allows pushing a temporary SSH key for one-time sessions over SSH.

Both services use IAM for authentication (which can be federated to Active Directory or other providers), and CloudTrail for audit logging.

**IAM Access and Permissions**

Define appropriate permissions to EC2 instances by using custom IAM policies with least-privilege principles.

**Image Security**

Set up a **Golden Image Pipeline** to regularly create new Amazon Machine Images (AMIs) with the latest updates and patches, hardening requirements, and any required application packages. The pipeline can also be integrated with Amazon Inspector or 3rd party products for vulnerability scanning. EC2 Image Builder simplifies the process of building the pipeline:

[**Automate OS Image Build Pipelines with EC2 Image Builder**](https://aws.amazon.com/blogs/aws/automate-os-image-build-pipelines-with-ec2-image-builder/)

EC2 Image Builder makes it easier to build and maintain secure OS images for Windows Server and Amazon Linux 2, using automated build pipelines. The pipelines that you can configure for EC2 Image Builder include the image recipe, infrastructure configuration, distribution, and test settings, to produce the resulting images. This includes the ability to automatically provision images as new software updates, including security patches, become available

**Vulnerability Management and Patching**

Set up automated vulnerability and patching for EC2 instances to ensure they are not affected by the latest vulnerabilities and have the latest patches applied regularly:

* **Amazon Inspector** is an agent-based solution that can be used to run recurring vulnerability assessments (as well as other packaged assessments such as CIS standards and security best practices).
* **AWS Systems Manager (SSM) Patch Manager** scans and installs missing patches on EC2 instances. Create **SSM Maintenance Windows** to regularly run these operations and control how patching is applied.

**Monitoring and Compliance**

Set up a comprehensive monitoring and compliance strategy by configuring the relevant AWS services and setting up alarms and notifications for critical events:

* **VPC Flow Logs** can be enabled to log network traffic to and from EC2 instances.
* **AWS CloudTrail** logs all API activity in the account including the creation/modification/deletion of EC2 resources.
* **AWS Config** tracks configuration changes in an environment and provides a historical view of EC2 resources throughout their lifetime.
* **AWS Config Rules** allows the configuration of compliance rules to ensure resources in the environment are configured properly and securely.
* **CloudWatch Alarms** can be used to alert based on CloudTrail and VPC Flow Logs events.

**Backup**

Create an automated backup policy for EBS volumes using **Data Lifecycle Manager** which automated snapshot creation and retention for EC2 instances. It is important to note that EC2 snapshots are crash-consistent.

Application-consistent snapshots can be taken for Windows instances using AWS Systems Manager Run Command to create **VSS Snapshots**.

Configure a Data Lifecycle Manager (DLM) policy to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes.

1. **S3 Security Strategy**

Resources for implementing a comprehensive S3 security strategy. Included are customizable configuration items and packages, as well as guides for encryption, access control, logging, monitoring and compliance, backup and resilience options and more.

**Prevent Public Access**

Ensure S3 public access is not allowed by enabling the **S3 Block Public Acces**s feature. This can be enabled on the account-level or bucket-level. This setting will override any bucket or object ACLs that might expose data in S3 buckets to the public.

[**Use AWS Config to Monitor for and Respond to Amazon S3 Buckets Allowing Public Access**](https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-buckets-allowing-public-access/)

This blog post shows how to use AWS Config to monitor Amazon Simple Storage Service (S3) bucket ACLs and policies for violations which allow public read or public write access. If AWS Config finds a policy violation, it will trigger an Amazon CloudWatch Event rule to trigger an AWS Lambda function which either corrects the S3 bucket ACL, or notifies you via Amazon Simple Notification Service (Amazon SNS) that the policy is in violation and allows public read or public write access.

If this AWS account is part of an AWS Organization, use a Service Control Policy (SCP) to prevent users in the account from modifying this setting.

**Encryption At-Rest**

Enable S3 Bucket Default Encryption to enforce encryption on all objects stored in an S3 bucket. Default encryption can be configured to use server-side encryption with either Amazon S3-managed keys (SSE-S3) or customer master keys (CMKs) stored in AWS Key Management Service (AWS KMS).

[**Automatic Remediation Rule: Enable S3 Bucket Encryption If Not Configure**](https://asecure.cloud/a/ar_ssm_s3_bucket_encryption/)**d**

Auto remediation configuration to enable S3 Bucket Encryption if an S3 bucket created without server side encryption. Detection uses a managed AWS Config Rule and remediation is with SSM Automation.

**Encryption In-Transit (TLS)**

S3 Buckets default to TLS encrypted communication, but the S3 API also supports HTTP connections. It is best practice to use **S3 bucket policies** to ensure clear-text communication is denied.

**Access Control**

Access to S3 buckets is controlled through a combination of identity-based policies (IAM Policies applied to IAM principals such as users or roles), and resource-based policies (S3 Bucket Policies applied on the S3 buckets). Use S3 bucket policies to ensure only authorized principles are allowed to access the bucket and data:

**VPC Access Control**

Use VPC Endpoints to provide private access from VPCs to S3 Buckets directly without having to provide Internet access to the VPC. VPC Endpoints also provide an additional access control mechanism through Endpoint Policies which allow further control on what S3 buckets and actions are allowed through the VPC. S3 bucket policies can also be used to restrict access to S3 buckets to specific VPCs or VPC Endpoints only.

**Access Logs**

S3 Buckets don't provide logging for object-level activity (data-plane logs) such as viewing or downloading files on an S3 bucket. AWS provides two methods for enabling access logging on S3:

* **Server Access Logs**: Configured on the S3 bucket. Logs are stored in a target S3 bucket (can be the same bucket) in the same AWS account. This logging method is free.
* **CloudTrail Data Events**: Data events can be configured to capture object-level events on an S3 bucket, multiple S3 buckets or all S3 buckets in an AWS account. Logs can be stored in S3 or forwarded to CloudWatch Logs. CloudTrail pricing applies.

**Monitoring and Compliance**

In addition to enabling access logs for S3 buckets, it is important to set up a comprehensive monitoring and compliance strategy by configuring the relevant AWS services and setting up alarms and notifications for critical events:

* **AWS CloudTrail** logs all API activity in the account including the creation/modification/deletion of S3 buckets or policies.
* **AWS Config** tracks configuration changes in an environment and provides a historical view of S3 Buckets throughout their lifetime.
* **AWS Config Rules** allows the configuration of compliance rules to ensure resources in the environment are configured properly and securely.
* **CloudWatch Alarms** can be used to alert based on CloudTrail activity to alert on important S3 related events.

Use the following packages to enable the required logging services, as well as compliance and monitoring rules for S3:

**Backup and Resilience**

Amazon S3 provides several features to protect data against accidental or malicious deletion or corruption:

* **Cross-Region** or **Same-Region Replication**: Enables automatic, asynchronous copying of objects in S3 buckets. The target buckets can be in the same AWS account or a different account.
* **Object Versioning**: Enable versioning on the S3 bucket to keep multiple versions of each object on the S3 bucket.
* **MFA Delete**: If enabled on an S3 bucket, only the bucket owner (with MFA authentication) can delete objects or change the versioning state of the bucket.
* **Object Lock**: Enable object lock to prevent an object from being deleted for a fixed amount of time or indefinitely.

**Data Classification and DLP**

A data classification strategy is required to prevent data loss in an environment. **Amazon Macie** (as well as 3rd-party partner tools) help with automatically discovering, classifying, and monitoring data on S3 buckets.