Immutable Security Controls

Immutable security controls are baseline controls or Guardrails that can be defined even before starting with workload deployments

Immutable controls are also considered Guardrails & provides mechanisms for mitigating Insider threats

What Should be my GuardRails:

Account GuardRails

1. **Region Restriction: Except global services, restrict all operations outside your choice of region.**

```
    {

    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "BOM Region",
            "Effect": "Deny",
            "NotAction": [
                "iam:",
                "organizations:",
                "route53:",
                "budgets:",
                "waf:",
                "cloudfront:",
                "globalaccelerator:",
                "importexport:",
                "support:",
                "health:",
                "route53domains:"
            ],
            "Resource": "",
            "Effect": "Deny",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "ap-south-1"

                    ]
                }
            }
        }
    ]
}
```

2. **Allow only required services**

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "AllowList",
    "Effect": "Allow",
    "Action": ["a4b:","access-
analyzer:","account:","acm:","acm-
pca:","amplify:","apigateway:","application-
autoscaling:","applicationinsights:","appmesh:","appmesh-
preview:","appstream:","appsync:","arsenal:","artifact:","a
thena:","autoscaling:","autoscaling-plans:","aws-
marketplace:","aws-marketplace-management:","aws-
portal:","backup:","backup-
storage:","batch:","budgets:","cassandra:","ce:","chatbot:"
,"chime:","cloud9:","clouddirectory:","cloudformation:","cl
oudfront:","cloudhsm:","cloudsearch:","cloudtrail:","cloudw
atch:","codebuild:","codecommit:","codedeploy:","codeguru-
profiler:","codeguru-
reviewer:","codepipeline:","codestar:","codestar-
notifications:","cognito-identity:","cognito-
idp:","cognito-
sync:","comprehend:","comprehendmedical:","compute-
optimizer:","config:","connect:","cur:","dataexchange:","da
tapipeline:","datasync:","dax:","dbqms:","deeplens:","deepr
acer:","detective:","devicefarm:","directconnect:","discove
ry:","dlm:","dms:","ds:","dynamodb:","ebs:","ec2:","ec2-
instance-
connect:","ec2messages:","ecr:","ecs:","eks:","elastic-
inference:","elasticache:","elasticbeanstalk:","elasticfile
system:","elasticloadbalancing:","elasticmapreduce:","elast
ictranscoder:","es:","events:","execute-
api:","firehose:","fms:","forecast:","frauddetector:","free
rtos:","fsx:","gamelift:","glacier:","globalaccelerator:","
glue:","greengrass:","groundstation:","groundtruthlabeling:
","guardduty:","health:","iam:","imagebuilder:","importexpo
rt:","inspector:","iot:","iot-device-
tester:","iot1click:","iotanalytics:","iotevents:","iotsite
wise:","iotthingsgraph:","kafka:","kendra:","kinesis:","kin
esisanalytics:","kinesisvideo:","kms:","lakeformation:","la
mbda:","launchwizard:","lex:","license-
manager:","lightsail:","logs:","machinelearning:","macie:",
"managedblockchain:","mechanicalturk:","mediaconnect:","med
iaconvert:","medialive:","mediapackage:","mediapackage-
vod:","mediastore:","mediatailor:","mgh:","mobileanalytics:
","mobilehub:","mobiletargeting:","mq:","neptune-
db:","networkmanager:","opsworks:","opsworks-
cm:","organizations:","outposts:","personalize:","pi:","pol
ly:","pricing:","qldb:","quicksight:","ram:","rds:","rds-
data:","rds-db:","redshift:","rekognition:","resource-
groups:","robomaker:","route53:","route53domains:","route53
resolver:","s3:","sagemaker:","savingsplans:","schemas:","s
db:","secretsmanager:","securityhub:","serverlessrepo:","se
rvicecatalog:","servicediscovery:","servicequotas:","ses:",
"shield:","signer:","sms:","sms-
voice:","snowball:","sns:","sqs:","ssm:","ssmmessages:","ss
o:","sso-
directory:","states:","storagegateway:","sts:","sumerian:",
"support:","swf:","synthetics:","tag:","textract:","transcr
ibe:","transfer:","translate:","trustedadvisor:","waf:","wa
f-
regional:","wafv2:","wam:","wellarchitected:","workdocs:","
worklink:","workmail:","workmailmessageflow:","workspaces:"
,"xray:"],
    "Resource": ""
  }
}
```

3. **Prevent Uses from modifying Account & Billing settings**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-portal:ModifyAccount",
                "aws-portal:ModifyBilling",
                "aws-portal:ModifyPaymentMethods"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
```

4. **Restrict the use of Root User in AWS Accountd**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:root"
                    ]
                }
            }
        }
    ]
}
```

5. **Deny Creation of New IAM Users or Access Keys**

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": ["iam:CreateAccessKey",
"iam:CreateUser"],
        "Resource": "*"
    }
}
```

6. **Prevent Creation of New IAM Users or Access Keys with an Exception for an Administrator Role**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:CreateUser",
                "iam:CreateAccessKey"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Deny",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalARN":
"arn:aws:iam::*:role/"
                }
            }
        }
    ]
}
```

7. **Prevent modification to an important IAM Role**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/CHANGEME"
      ]
    }
  ]
}
```

8. **Prevent IAM changes to a specified IAM Role**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:AttachRolePolicy",
                "iam:DeleteRole",
                "iam:DeleteRolePermissionsBoundary",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:PutRolePermissionsBoundary",
                "iam:PutRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": [
                "arn:aws:iam::*:role/"
            ],
            "Effect": "Deny"
        }
    ]
}
```

9. **Prevent users from disabling IAM Access Analyzer**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "access-analyzer:DeleteAnalyzer"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

10. **Prevent account from creating or deleting resources shares within the organization**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventResourceSharing",
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare",
                "ram:DeleteResourceShare",
                "ram:EnableSharingWithAwsOrganization"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

11. **Prevent users from leaving AWS Orgnizations**

```
{
"Version": "2012-10-17",
"Statement": [
{
"Action": [
"organizations:LeaveOrganization"
],
"Resource": "*",
"Effect": "Deny"
}
]
}
```

Protecting Security Baseline

1. **Prevent users from deleting or stopping CloudTrail**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "cloudtrail:StopLogging",
                "cloudtrail:DeleteTrail"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

2. **Prevent users from disabling AWS Config or changing its rules**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "config:DeleteConfigRule",
                "config:DeleteConfigurationRecorder",
                "config:DeleteDeliveryChannel",
                "config:StopConfigurationRecorder"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

3. **Prevent users from disabling GuardDuty**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "guardduty:DeleteDetector",
                "guardduty:DeleteInvitations",
                "guardduty:DeleteIPSet",
                "guardduty:DeleteMembers",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:StopMonitoringMembers"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

4. **Prevent users from disrupting CloudWatch**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DeleteDashboards",
                "cloudwatch:DisableAlarmActions",
                "cloudwatch:PutDashboard",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:SetAlarmState"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

5. **Prevent users from deleting VPC Flow logs**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DeleteFlowLogs",
                "logs:DeleteLogGroup",
                "logs:DeleteLogStream"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

5. **Prevent any VPC that doesn’t already have Internet access from getting it**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachInternetGateway",
                "ec2:CreateInternetGateway",
                "ec2:AttachEgressOnlyInternetGateway",
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection"
            ],
            "Resource": "*",
            "Effect": "Deny"
        },
        {
            "Action": [
                "globalaccelerator:Create*",
                "globalaccelerator:Update*"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

6. **Protect VPC connectivity settings from modification**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNatGateway",
                "ec2:CreateInternetGateway",
                "ec2:DeleteNatGateway",
                "ec2:AttachInternetGateway",
                "ec2:DeleteInternetGateway",
                "ec2:DetachInternetGateway",
                "ec2:CreateClientVpnRoute",
                "ec2:AttachVpnGateway",
                "ec2:DisassociateClientVpnTargetNetwork",
                "ec2:DeleteClientVpnEndpoint",
                "ec2:DeleteVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection",
                "ec2:CreateNatGateway",
                "ec2:ModifyClientVpnEndpoint",
                "ec2:CreateVpnConnectionRoute",
                "ec2:RevokeClientVpnIngress",
                "ec2:RejectVpcPeeringConnection",
                "ec2:DetachVpnGateway",
                "ec2:DeleteVpnConnectionRoute",
                "ec2:CreateClientVpnEndpoint",
                "ec2:AuthorizeClientVpnIngress",
                "ec2:DeleteVpnGateway",
                "ec2:TerminateClientVpnConnections",
                "ec2:DeleteClientVpnRoute",
                "ec2:ModifyVpcPeeringConnectionOptions",
                "ec2:CreateVpnGateway",
                "ec2:DeleteNatGateway",
                "ec2:DeleteVpnConnection",
                "ec2:CreateVpcPeeringConnection",
                "ec2:CreateVpnConnection"
            ],
            "Resource": "*",
            "Effect": "Deny"
        },
        {
            "Action": [
                "directconnect:CreatePrivateVirtualInterfac
e",
                "directconnect:DeleteBGPPeer",
                "directconnect:DeleteLag",
                "directconnect:AssociateHostedConnection",
                "directconnect:CreateInterconnect",
                "directconnect:CreatePublicVirtualInterface
",
                "directconnect:CreateLag",
                "directconnect:CreateDirectConnectGateway",
                "directconnect:AssociateVirtualInterface",
                "directconnect:AllocateConnectionOnIntercon
nect",
                "directconnect:AssociateConnectionWithLag",
                "directconnect:AllocatePrivateVirtualInterf
ace",
                "directconnect:DeleteInterconnect",
                "directconnect:AllocateHostedConnection",
                "directconnect:DeleteDirectConnectGateway",
                "directconnect:DeleteVirtualInterface",
                "directconnect:DeleteDirectConnectGatewayAs
sociation",
                "directconnect:CreateDirectConnectGatewayAs
sociation",
                "directconnect:DeleteConnection",
                "directconnect:CreateBGPPeer",
                "directconnect:AllocatePublicVirtualInterfa
ce",
                "directconnect:CreateConnection"
            ],
            "Resource": "*",
            "Effect": "Deny"
        },
        {
            "Action": [
                "globalaccelerator:DeleteListener",
                "globalaccelerator:DeleteAccelerator",
                "globalaccelerator:UpdateListener",
                "globalaccelerator:UpdateAccelerator",
                "globalaccelerator:CreateEndpointGroup",
                "globalaccelerator:UpdateAcceleratorAttribu
tes",
                "globalaccelerator:UpdateEndpointGroup",
                "globalaccelerator:CreateListener",
                "globalaccelerator:CreateAccelerator",
                "globalaccelerator:DeleteEndpointGroup"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

7. **Protect VPC Internet & NAT Gateway setting from modification**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNatGateway",
                "ec2:CreateInternetGateway",
                "ec2:DeleteNatGateway",
                "ec2:AttachInternetGateway",
                "ec2:DeleteInternetGateway",
                "ec2:DetachInternetGateway"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

8. **Prevent Users from disabling AWS Security Hub in an account**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "securityhub:DeleteInvitations",
                "securityhub:DisableSecurityHub",
                "securityhub:DisassociateFromMasterAccount"
,
                "securityhub:DeleteMembers",
                "securityhub:DisassociateMembers"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

9. **Prevent users from disabling Macie in an account**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "macie2:DisassociateFromMasterAccount",
                "macie2:DisableOrganizationAdminAccount",
                "macie2:DisableMacie",
                "macie2:DeleteMember"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

Data GuardRails

1. **Allow only India Region buckets**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyIndiaS3Buckets",
            "Effect": "Deny",
            "Action": [
                "s3:CreateBucket"
            ],
            "Resource": "arn:aws:s3:::*",
            "Condition": {
                "ForAnyValue:StringNotLike": {
                    "s3:LocationConstraint": [
                        "ap-southeast-1"
                        
                    ]
                }
            }
        }
    ]
}
```

2. **Prevent uses from deleting S3 Buckets or Objects**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

3. **Requires encryption on all Amazon S3 buckets in AWS Account**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption":
"AES256"
                }
            }
        },
        {
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "Bool": {
                    "s3:x-amz-server-side-encryption":
false
                }
            }
        }
    ]
}
```

4. **Prevent users from modifying S3 Block Public Access Settings**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

5. **Prevent users from deleting KMS keys**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "kms:ScheduleKeyDeletion",
                "kms:Delete*"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

EC2 instance Control

1. **Specify type of EC2 instance**

1.
   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Action": [
           "ec2:RunInstances"
         ],
         "Resource": "*",
         "Effect": "Deny",
         "Condition": {
           "StringNotEquals": {
             "ec2:InstanceType": "t2.micro"
           }
         }
       }
     ]
   }
   ```
2. **Require the use of IMDSv2 for all EC2 Roles**

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

3. **Enforce IMDSv2 on any newly created EC2**

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "RequireImdsV2",
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:MetadataHttpTokens": "required"
            }
        }
    }
}
```

4. **Deny Instance metadata service modification**

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:ModifyInstanceMetadataOptions",
        "Resource": "*"
    }
}
```

5. **MFA to Stop or terminate an instance**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": false
                }
            }
        }
    ]
}
```

6. **Require EC2 encryption**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Require EC2 Encryption",
            "Effect": "Deny",
            "Action": [
                "ec2:RunInstances"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "false"
                }
            },
            "Resource": [
                "*"
            ]
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "restrictregion",
            "Effect": "Deny",
            "NotAction": [
                "iam:*",
                "organizations:*",
                "route53:*",
                "budgets:*",
                "waf:*",
                "cloudfront:*",
                "globalaccelerator:*",
                "importexport:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "ap-southeast-1",
                        "ap-south-1",
                        "us-east-1",
                        "us-east-2"
                    ]
                }
            }
        }
    ]
}
```