S.N.	Alert Name	Event Pattern	Filter Name	Metric Name	Metric Namespace	Unit	Metric Value	Default Value	Threshold
1	IAM Policy changes	($.eventName = DeleteGroupPolicy) \|\| ($.eventName = DeleteRolePolicy) || ($.eventName = DeleteUserPolicy) \|\| ($.eventName = PutGroupPolicy) || ($.eventName = PutRolePolicy) \|\| ($.eventName = PutUserPolicy) || ($.eventName = CreatePolicy) \|\| ($.eventName = DeletePolicy) || ($.eventName = CreatePolicyVersion) \|\| ($.eventName = DeletePolicyVersion) || ($.eventName = AttachRolePolicy) \|\| ($.eventName = DetachRolePolicy) || ($.eventName = AttachUserPolicy) \|\| ($.eventName = DetachUserPolicy) || ($.eventName = AttachGroupPolicy) \|\| ($.eventName = DetachGroupPolicy) }	IAMAuthConfigChange	IAMPolicyEventCount	CloudTrailMetrics	Count	1	0	>=1
2	Disabling or scheduled deletion of customer managed keys	{ ($.eventSource = kms.amazonaws.com) && (($.eventName = DisableKey) || ($.eventName = ScheduleKeyDeletion)) }	AWSCMKChange	CMKEventCount	CloudTrailMetrics	Count	1	0	>=1
3	Usage of root user	{ $.userIdentity.type = "Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent" }	RootAccountUsage	RootAccountUsageEventCount	CloudTrailMetrics	Count	1	0	>=1
4	Changes to Network Gateways	{ ($.eventName = CreateCustomerGateway) \|\| ($.eventName = DeleteCustomerGateway) || ($.eventName = AttachInternetGateway) \|\| ($.eventName = CreateInternetGateway) || ($.eventName = DeleteInternetGateway) \|\| ($.eventName = DetachInternetGateway) }	VPCGatewayConfigChange	GatewayEventCount	CloudTrailMetrics	Count	1	0	>=1
5	Changes to NACLs	{ ($.eventName = CreateNetworkAcl) \|\| ($.eventName = CreateNetworkAclEntry) || ($.eventName = DeleteNetworkAcl) \|\| ($.eventName = DeleteNetworkAclEntry) || ($.eventName = ReplaceNetworkAclEntry) \|\| ($.eventName = ReplaceNetworkAclAssociation) }	NetworkACLConfigChange	NetworkAclEventCount	CloudTrailMetrics	Count	1	0	>=1
6	AWS Management Console authentication failures	{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }	AWSConsoleSignInFailure	ConsoleSigninFailureCount	CloudTrailMetrics	Count	1	0	>=1
7	Management Console sign-in without MFA	{ $.eventName = "ConsoleLogin" && $.additionalEventData.MFAUsed = "No" }	ConsoleSignInWithoutMfa	ConsoleSignInWithoutMfaCount	CloudTrailMetrics	Count	1	0	>=1
8	Route table changes	{ ($.eventName = CreateRoute) \|\| ($.eventName = CreateRouteTable) || ($.eventName = ReplaceRoute) \|\| ($.eventName = ReplaceRouteTableAssociation) || ($.eventName = DeleteRouteTable) \|\| ($.eventName = DeleteRoute) || ($.eventName = DisassociateRouteTable) }	RouteTableConfigChange	RouteTableEventCount	CloudTrailMetrics	Count	1	0	>=1
	~~Management Console sign-in without MFA~~								
9	VPC changes	{ ($.eventName = CreateVpc) \|\| ($.eventName = DeleteVpc) || ($.eventName = ModifyVpcAttribute) \|\| ($.eventName = AcceptVpcPeeringConnection) || ($.eventName = CreateVpcPeeringConnection) \|\| ($.eventName = DeleteVpcPeeringConnection) || ($.eventName = RejectVpcPeeringConnection) \|\| ($.eventName = AttachClassicLinkVpc) || ($.eventName = DetachClassicLinkVpc) \|\| ($.eventName = DisableVpcClassicLink) || ($.eventName = EnableVpcClassicLink) }	VPCNetworkConfigChange	VpcEventCount	CloudTrailMetrics	Count	1	0	>=1
10	S3 bucket policy changes	{ ($.eventSource = s3.amazonaws.com) && (($.eventName = PutBucketAcl) || ($.eventName = PutBucketPolicy) \|\| ($.eventName = PutBucketCors) || ($.eventName = PutBucketLifecycle) \|\| ($.eventName = PutBucketReplication) || ($.eventName = DeleteBucketPolicy) \|\| ($.eventName = DeleteBucketCors) || ($.eventName = DeleteBucketLifecycle) \|\| ($.eventName = DeleteBucketReplication)) }	S3BucketConfigChange	S3BucketEventCount	CloudTrailMetrics	Count	1	0	>=1
11	Unauthorized API calls	{($.errorCode = "*UnauthorizedOperation") \|\| ($.errorCode = "AccessDenied*")}	UnauthorizedOperation	UnauthorizedOperation	CloudTrailMetrics	Count	1	0	>=1
12	AWS Config configuration changes	{ ($.eventSource = config.amazonaws.com) && (($.eventName = StopConfigurationRecorder)||($.eventName = DeleteDeliveryChannel)\|\|($.eventName = PutDeliveryChannel)||($.eventName = PutConfigurationRecorder)) }	AWSConfigChange	ConfigEventCount	CloudTrailMetrics	Count	1	0	>=1
13	Security group changes	{ ($.eventName = AuthorizeSecurityGroupIngress) \|\| ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) \|\| ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup) \|\| ($.eventName = DeleteSecurityGroup) }	SecurityGroupConfigChange	SecurityGroupEventCount	CloudTrailMetrics	Count	1	0	>=1