Dome9 Compliance - June1

Date of previous commit	Commit Date	Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles	Description
2019-05-23T18:37:08Z	2019-06-01T07:07:35Z	D9.AWS.CRY.17	Use encrypted connection between CloudFront and origin server	High	description logic	AWS Dome9 Best Practices - Sample AWS ISO 27001:2013 AWS NIST 800-53 Rev 4 AWS Dome9 SOC2 based on AICPA TSC 2017 AWS HIPAA AWS CSA CCM v.3.0.1 AWS NIST CSF v1.1 AWS PCI-DSS 3.2 AWS Dome9 Best Practices	Enforce HTTPS-only traffic between a CloudFront distribution and the origin. It is recommended to use HTTPS for secure communications between your CloudFront distribution and end users to guarantee encryption of traffic and prevent malicious actors from intercepting your traffic. Note: This rule runs on all the origins except S3 Buckets
2019-05-23T18:37:08Z	2019-06-04T22:39:21Z	D9.GCP.GKE.15	Ensure GKE Cluster HTTP load balancing is enabled	Medium	complianceTag	GCP Dome9 Best Practices	Checks for GCP Kubernetes Engine Clusters that have HTTP load balancing disabled. When this is enabled, the Kubernetes Engine can terminate unauthorized HTTP/HTTPS requests and make better context-aware load balancing decisions.
2019-05-23T18:37:08Z	2019-06-04T22:39:21Z	D9.GCP.GKE.16	Ensure the GKE Cluster alpha cluster feature is disabled	Medium	complianceTag	GCP Dome9 Best Practices	Checks for GCP Kubernetes Engine Clusters that have enabled alpha cluster. It is recommended to not use alpha clusters or alpha features for production workloads.
2019-05-23T18:37:08Z	2019-06-04T22:39:21Z	D9.GCP.GKE.17	Ensure GKE Clusters use specific purpose-designed networks instead of the default network	Medium	name complianceTag	GCP Dome9 Best Practice	Checks for Google Kubernetes Engine (GKE) clusters that are configured to use the default network. It is recommended not to use the default network on GKE.