Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.AZU.CRY.10	Ensure that storage account access keys are periodically regenerated	Medium	Compliance Tag - added to Bundle	Azure NIST 800-53 Rev 4
D9.AZU.NET.02	SQL Server accessibility to the entire Azure Infrastructure	High	Compliance Tag - added to Bundle	Azure NIST 800-53 Rev 4
D9.AZU.NET.03	SQL Server accessibility to wide address range	Medium	Compliance Tag - added to Bundle	Azure NIST 800-53 Rev 4
D9.AWS.LOG.12	S3 bucket should have server access logging enabled	Medium	Compliance Tag - added to Bundle	AWS HIPAA AWS GDPR Readiness AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.GCP.NET.06	Unused firewall rules	Medium	Compliance Tag - added to Bundle	GCP NIST 800-53 Rev 4
D9.GCP.CRY.01	Ensure VM disks are encrypted with Customer-Supplied Encryption Keys (CSEK)	High	Compliance Tag - added to Bundle	GCP NIST 800-53 Rev 4
D9.AWS.IAM.28	S3 bucket should not be world-listable from anonymous users	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.29	S3 bucket should not be world-listable	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.30	S3 bucket should not be world-writable from anonymous users	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.31	S3 bucket should not be world-writable	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.32	S3 bucket should not have writable permissions from anonymous users	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.33	S3 bucket should not have world-writable permissions	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.34	S3 bucket should not have world-readable permissions from anonymous users	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.35	S3 bucket should not have world-readable permissions	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.36	S3 bucket should not allow delete actions from all principals	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.37	S3 bucket should not allow get actions from all principals	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4

Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.AWS.IAM.38	S3 bucket should not allow list actions from all principals	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.39	S3 bucket should not allow put actions from all principals	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.40	S3 bucket should not allow all actions from all principals	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.41	S3 bucket should not allow put or restore actions from all principals	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4
D9.AWS.IAM.43	S3 bucket should have versioning MFA delete enabled	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2
D9.AWS.LOG.10	S3 bucket CloudTrail logs ACL should not allow public access	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2
D9.AWS.LOG.11	S3 bucket CloudTrail logs policy should not allow public access	High	Compliance Tag - added to Bundle	AWS PCI-DSS 3.2
D9.AWS.CRY.15	Use KMS CMK customer-managed keys for Redshift clusters	High	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4
D9.AWS.IAM.42	S3 buckets should not grant any external privileges via ACL	High	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4
D9.AWS.IAM.44	Use managed policies instead of inline IAM Policies	Medium	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4
D9.AWS.MON.15	Ensure appropriate subscribers to each SNS topic	Low	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4
D9.AWS.NET.11	Process for Security Group Management - Managing security groups	High	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4
D9.AWS.NET.12	Instances are Configured under Virtual Private Cloud	Medium	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4
D9.AWS.NET.15	Remove Unused Security Groups	Medium	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4
D9.AWS.NET.16	RDS should not have Public Interface	High	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4
D9.AWS.NET.17	RDS should not have Public Interface open to a public scope	High	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4
D9.AWS.NET.18	RDS should not have be open to a large scope	High	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4
D9.AWS.NET.22	Process for Security Group Management - Detection of new Security Groups	Medium	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4

Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.AWS.VLN.01	EC2 Instance - there shouldn't be any High level findings in Inspector Scans	High	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4
D9.AWS.VLN.02	Instances without Inspector runs in the last 30 days	High	Compliance Tag - added to Bundle	AWS NIST 800-53 Rev 4
D9.AZU.CRY.11	Ensure that 'Data encryption' is set to 'On'	High	logic	Azure CIS Foundations v. 1.0.0 Azure GDPR Readiness Azure PCI-DSS 3.2 Azure NIST 800-53 Rev 4 Azure Dome9 Best Practices
D9.AZU.MON.03	Ensure that 'Threat Detection' is set to 'On'	Medium	logic	Azure CIS Foundations v. 1.0.0 Azure GDPR Readiness Azure PCI-DSS 3.2 Azure NIST 800-53 Rev 4 Azure Dome9 Best Practices
D9.AZU.MON.07	Ensure that 'Auditing' Retention is 'greater than 90 days'	Low	logic	Azure CIS Foundations v. 1.0.0 Azure PCI-DSS 3.2 Azure NIST 800-53 Rev 4 Azure Dome9 Best Practices
D9.AZU.CRY.03	Ensure that the expiry date is set on all Keys- SQL Database KeyVault key rotation every 90 days	Medium	complianceTag	Azure NIST 800-53 Rev 4
D9.AZU.CRY.07	Ensure that 'Storage service encryption' is set to Enabled for Blob Service	High	complianceTag	Azure NIST 800-53 Rev 4
D9.AZU.CRY.08	Ensure that 'Storage service encryption' is set to Enabled for File Service	High	complianceTag	Azure NIST 800-53 Rev 4
D9.AZU.NET.01	Ensure that SQL server access is restricted from the internet	High	complianceTag	Azure NIST 800-53 Rev 4
D9.AZU.NET.11	Redis should not have a Firewall rule allowing unrestricted access from azure	High	complianceTag	Azure NIST 800-53 Rev 4
D9.AZU.NET.12	Redis should not have a Firewall rule allowing unrestricted access from the internet	High	complianceTag	Azure NIST 800-53 Rev 4

Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.AZU.NET.13	Redis Cache should not have a firewall rule allowing access to a large number of source IPs	Medium	complianceTag	Azure NIST 800-53 Rev 4
D9.AZU.NET.15	Redis attached subnet Network Security Group should allow ingress traffic only to ports 6379 or 6380	High	complianceTag	Azure NIST 800-53 Rev 4
D9.AZU.NET.16	Redis attached subnet Network Security Group should allow egress traffic only to ports 6379 or 6380	High	complianceTag	Azure NIST 800-53 Rev 4
D9.AWS.CRY.17	Use encrypted connection between CloudFront and origin server	High	description logic	AWS HIPAA AWS PCI-DSS 3.2 AWS NIST 800-53 Rev 4 AWS Dome9 Best Practices
D9.GCP.NET.01	Ensure the default network does not exist in a project	High	name	GCP NIST 800-53 Rev 4 GCP PCI-DSS 3.2 GCP Dome9 Network Alerts GCP Dome9 Best Practices
D9.AWS.PRE.01	Credentials report was generated in the last 24 hours	Low	complianceTag	AWS Dome9 Best Practices
D9.AWS.PRE.02	Enforce Password Policy	High	complianceTag	AWS Dome9 Best Practices