Dome9 - December 03 Compliance Updates

dateOld	dateNew	bundleName	changeLog	ruleId	nameOld	nameNew	severityOld	severityNew	complianceTagOld	complianceTagNew	logicOld	logicNew	descriptionOld	descriptionNew
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	AWS Dome9 Best Practices	Rule Added	D9.AWS.VLN.03		Amazon GuardDuty service is enabled		Medium		Vulnerability and Threat Management		Region should have guardDutyStatus='Enabled'		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.
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	AWS Dome9 Serverless Architectures Security	Rule Changed	D9.AWS.CRY.20	AWS Kinesis Streams Keys are rotated		Meduim	Medium	Encryption and Key Management		Kinesis where encrypted should have encryptionKey.rotationStatus=true		Rotate the keys of your Kinesis Streams in order to protect your data and metadata from breaches or unauthorized access, and fulfill compliance requirements for key management within your organization.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure NIST 800-53 Rev 4	Rule Changed	D9.AZU.IAM.03	Ensure that Azure SQL Server Admin is configured with AD Authentication		Medium		AC-6|AC-2		SQLServer should have adAdministrators with [name='*']	SQLServer should have adAdministrators contain [name='ActiveDirectory']	Use Azure Active Directory Authentication for authentication with SQL Databases. Azure Active Directory authentication is a mechanism of connecting Microsoft Azure SQL Databases and SQL Data Warehouses using identities in an Azure Active Directory (Azure AD). With Azure AD authentication, you can centrally manage the identities of database users and other Microsoft services in one central location.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure PCI-DSS 3.2	Rule Changed	D9.AZU.IAM.03	Ensure that Azure SQL Server Admin is configured with AD Authentication		Medium		8.1|8.1.1		SQLServer should have adAdministrators with [name='*']	SQLServer should have adAdministrators contain [name='ActiveDirectory']	Use Azure Active Directory Authentication for authentication with SQL Databases. Azure Active Directory authentication is a mechanism of connecting Microsoft Azure SQL Databases and SQL Data Warehouses using identities in an Azure Active Directory (Azure AD). With Azure AD authentication, you can centrally manage the identities of database users and other Microsoft services in one central location.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	AWS HIPAA	Rule Changed	D9.AWS.CRY.20	AWS Kinesis Streams Keys are rotated		Meduim	Medium	164.312(a)(2)(iv)|164.312 (e)(1)|164.312 (e)(2)(ii)		Kinesis where encrypted should have encryptionKey.rotationStatus=true		Rotate the keys of your Kinesis Streams in order to protect your data and metadata from breaches or unauthorized access, and fulfill compliance requirements for key management within your organization.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure ISO 27001:2013	Rule Changed	D9.AZU.IAM.03	Ensure that Azure SQL Server Admin is configured with AD Authentication		Medium		A.9.2.3|A.9.1.2|A.9.4.4		SQLServer should have adAdministrators with [name='*']	SQLServer should have adAdministrators contain [name='ActiveDirectory']	Use Azure Active Directory Authentication for authentication with SQL Databases. Azure Active Directory authentication is a mechanism of connecting Microsoft Azure SQL Databases and SQL Data Warehouses using identities in an Azure Active Directory (Azure AD). With Azure AD authentication, you can centrally manage the identities of database users and other Microsoft services in one central location.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	AWS PCI-DSS 3.2	Rule Changed	D9.AWS.CRY.20	AWS Kinesis Streams Keys are rotated		Meduim	Medium	4.1|2.3|2.2.3|A2.1|A2.2|A2.3		Kinesis where encrypted should have encryptionKey.rotationStatus=true		Rotate the keys of your Kinesis Streams in order to protect your data and metadata from breaches or unauthorized access, and fulfill compliance requirements for key management within your organization.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure GDPR Readiness	Rule Changed	D9.AZU.IAM.03	Ensure that Azure SQL Server Admin is configured with AD Authentication		Medium		Article 25		SQLServer should have adAdministrators with [name='*']	SQLServer should have adAdministrators contain [name='ActiveDirectory']	Use Azure Active Directory Authentication for authentication with SQL Databases. Azure Active Directory authentication is a mechanism of connecting Microsoft Azure SQL Databases and SQL Data Warehouses using identities in an Azure Active Directory (Azure AD). With Azure AD authentication, you can centrally manage the identities of database users and other Microsoft services in one central location.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure NIST CSF v1.1	Rule Changed	D9.AZU.IAM.03	Ensure that Azure SQL Server Admin is configured with AD Authentication		Medium		PR.AC-4|PR.AC-1		SQLServer should have adAdministrators with [name='*']	SQLServer should have adAdministrators contain [name='ActiveDirectory']	Use Azure Active Directory Authentication for authentication with SQL Databases. Azure Active Directory authentication is a mechanism of connecting Microsoft Azure SQL Databases and SQL Data Warehouses using identities in an Azure Active Directory (Azure AD). With Azure AD authentication, you can centrally manage the identities of database users and other Microsoft services in one central location.	

Dome9 - December 03 Compliance Updates

dateOld	dateNew	bundleName	changeLog	ruleId	nameOld	nameNew	severityOld	severityNew	complianceTagOld	complianceTagNew	logicOld	logicNew	descriptionOld	descriptionNew
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	AWS NIST 800-53 Rev 4	Rule Changed	D9.AWS.CRY.20	AWS Kinesis Streams Keys are rotated		Meduim	Medium	SC-13|SC-23		Kinesis where encrypted should have encryptionKey.rotationStatus=true		Rotate the keys of your Kinesis Streams in order to protect your data and metadata from breaches or unauthorized access, and fulfill compliance requirements for key management within your organization.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	AWS CSA CCM v.3.0.1	Rule Changed	D9.AWS.CRY.20	AWS Kinesis Streams Keys are rotated		Meduim	Medium	EKM-02|EKM-03		Kinesis where encrypted should have encryptionKey.rotationStatus=true		Rotate the keys of your Kinesis Streams in order to protect your data and metadata from breaches or unauthorized access, and fulfill compliance requirements for key management within your organization.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure Dome9 Best Practices	Rule Changed	D9.AZU.IAM.03	Ensure that Azure SQL Server Admin is configured with AD Authentication		Medium		Identity and Access Management		SQLServer should have adAdministrators with [name='*']	SQLServer should have adAdministrators contain [name='ActiveDirectory']	Use Azure Active Directory Authentication for authentication with SQL Databases. Azure Active Directory authentication is a mechanism of connecting Microsoft Azure SQL Databases and SQL Data Warehouses using identities in an Azure Active Directory (Azure AD). With Azure AD authentication, you can centrally manage the identities of database users and other Microsoft services in one central location.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure CIS Foundations v. 1.0.0	Rule Changed	D9.AZU.IAM.03	Ensure that Azure SQL Server Admin is configured with AD Authentication		Medium		4.1.8		SQLServer should have adAdministrators with [name='*']	SQLServer should have adAdministrators contain [name='ActiveDirectory']	Use Azure Active Directory Authentication for authentication with SQL Databases. Azure Active Directory authentication is a mechanism of connecting Microsoft Azure SQL Databases and SQL Data Warehouses using identities in an Azure Active Directory (Azure AD). With Azure AD authentication, you can centrally manage the identities of database users and other Microsoft services in one central location.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	AWS Dome9 Best Practices	Rule Changed	D9.AWS.VLN.01	EC2 Instance - there shouldn't be any High level findings in Inspector Scans		High		Vulnerability Management	Vulnerability and Threat Management	Instance should not have scanners. findings contain-any [ruleSeverity='High']		Are there are instances with high severity inspector findings. Inspector is an AWS service that helps improve the security and compliance of your AWS resources. Inspector Findings are potential security issues found during the evaluation of selected resources.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	AWS Dome9 Best Practices	Rule Changed	D9.AWS.VLN.02	Instances without Inspector runs in the last 30 days		High		Vulnerability Management	Vulnerability and Threat Management	Instance should have scanners.scans contain [source = 'Inspector' and startTime after(-30, 'days') and state in ('COMPLETED')]		AWS Inspector is a security assessment service, used to assess applications for vulnerabilities or deviations from best practices. It is recommended to run AWS Inspector scans regularly. Dome9 recommends running Inspector at least once a week. This rule makes sure that Inspector runs at least once every 30 days on all instances.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	AWS Dome9 Best Practices	Rule Changed	D9.AWS.CRY.20	AWS Kinesis Streams Keys are rotated		Meduim	Medium	Encryption and Key Management		Kinesis where encrypted should have encryptionKey.rotationStatus=true		Rotate the keys of your Kinesis Streams in order to protect your data and metadata from breaches or unauthorized access, and fulfill compliance requirements for key management within your organization.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	AWS Dome9 Best Practices	Rule Changed	D9.AWS.NET.36	AWS CloudFront ‚Äì WAF Integration	AWS Cloud Front - WAF Integration	Medium		Network Security		CloudFront should have distributionConfig.webACLId		Ensure that all your AWS CloudFront web distributions are integrated with the Web Application Firewall (AWS WAF) service to protect against application-layer attacks	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	AWS NIST CSF v1.1	Rule Changed	D9.AWS.CRY.20	AWS Kinesis Streams Keys are rotated		Meduim	Medium	PR.DS-2		Kinesis where encrypted should have encryptionKey.rotationStatus=true		Rotate the keys of your Kinesis Streams in order to protect your data and metadata from breaches or unauthorized access, and fulfill compliance requirements for key management within your organization.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure NIST 800-53 Rev 4	Rule Removed	D9.AZU.CRY.07	Ensure that 'Storage service encryption' is enabled for the Blob Service		High		SC-13|SC-8|SC-28				Enable data encryption at rest for blobs. Storage service encryption protects your data at rest. Azure Storage encrypts data when it's written, and automatically decrypts it when it is accessed.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure NIST 800-53 Rev 4	Rule Removed	D9.AZU.CRY.08	Ensure that 'Storage service encryption' is enabled for the File Service		High		SC-13|SC-8|SC-28				Enable data encryption at rest for file service. Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in its datacenters, and automatically decrypts it for you as you access it.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure PCI-DSS 3.2	Rule Removed	D9.AZU.CRY.07	Ensure that 'Storage service encryption' is enabled for the Blob Service		High		3.6.3|3.5.3				Enable data encryption at rest for blobs. Storage service encryption protects your data at rest. Azure Storage encrypts data when it's written, and automatically decrypts it when it is accessed.	

Dome9 - December 03 Compliance Updates

dateOld	dateNew	bundleName	changeLog	ruleId	nameOld	nameNew	severityOld	severityNew	complianceTagOld	complianceTagNew	logicOld	logicNew	descriptionOld	descriptionNew
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure PCI-DSS 3.2	Rule Removed	D9.AZU.CRY.08	Ensure that 'Storage service encryption' is enabled for the File Service		High		3.6.3|3.5.3				Enable data encryption at rest for file service. Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in its datacenters, and automatically decrypts it for you as you access it.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure ISO 27001:2013	Rule Removed	D9.AZU.CRY.07	Ensure that 'Storage service encryption' is enabled for the Blob Service		High		A.18.1.3|A.18.1.5				Enable data encryption at rest for blobs. Storage service encryption protects your data at rest. Azure Storage encrypts data when it's written, and automatically decrypts it when it is accessed.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure ISO 27001:2013	Rule Removed	D9.AZU.CRY.08	Ensure that 'Storage service encryption' is enabled for the File Service		High		A.18.1.3|A.18.1.5				Enable data encryption at rest for file service. Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in its datacenters, and automatically decrypts it for you as you access it.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure GDPR Readiness	Rule Removed	D9.AZU.CRY.07	Ensure that 'Storage service encryption' is enabled for the Blob Service		High		Article 32				Enable data encryption at rest for blobs. Storage service encryption protects your data at rest. Azure Storage encrypts data when it's written, and automatically decrypts it when it is accessed.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure GDPR Readiness	Rule Removed	D9.AZU.CRY.08	Ensure that 'Storage service encryption' is enabled for the File Service		High		Article 32				Enable data encryption at rest for file service. Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in its datacenters, and automatically decrypts it for you as you access it.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure NIST CSF v1.1	Rule Removed	D9.AZU.CRY.07	Ensure that 'Storage service encryption' is enabled for the Blob Service		High		PR.DS-1|PR.DS-5				Enable data encryption at rest for blobs. Storage service encryption protects your data at rest. Azure Storage encrypts data when it's written, and automatically decrypts it when it is accessed.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure NIST CSF v1.1	Rule Removed	D9.AZU.CRY.08	Ensure that 'Storage service encryption' is enabled for the File Service		High		PR.DS-1|PR.DS-5				Enable data encryption at rest for file service. Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in its datacenters, and automatically decrypts it for you as you access it.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure Dome9 Best Practices	Rule Removed	D9.AZU.CRY.07	Ensure that 'Storage service encryption' is enabled for the Blob Service		High		Encryption and Key Management				Enable data encryption at rest for blobs. Storage service encryption protects your data at rest. Azure Storage encrypts data when it's written, and automatically decrypts it when it is accessed.	
2018-11-12T22:01:26Z	2018-12-03T22:08:51Z	Azure Dome9 Best Practices	Rule Removed	D9.AZU.CRY.08	Ensure that 'Storage service encryption' is enabled for the File Service		High		Encryption and Key Management				Enable data encryption at rest for file service. Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in its datacenters, and automatically decrypts it for you as you access it.	