

Dome9 - March08 Compliance Updates

New Bundles							
Commit Date	Bundle ID	Bundle Name					
2019-02-05T22:08	D9_AZU_HIPAA	Azure HIPAA					
2019-02-05T22:08	D9_AZU_SOC2	Azure Dome9 SOC2 based on AICPA TSC 2017					
2019-02-05T22:08	D9_GCP_SOC2	GCP Dome9 SOC2 based on AICPA TSC 2017					
2019-02-05T22:08	D9_AWS_SOC2	AWS Dome9 SOC2 based on AICPA TSC 2017					
Changes to existing Rules							
Date of previous c	Commit Date	Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.GCP.IAM.02	Ensure that corporate login credentials are used in	High	Gmail accounts are	logic	GCP Dome9 Best Practices - Sample GCP CSA CCM v.3.0.1 GCP NIST CSF v1.1 GCP NIST 800-53 Rev 4 GCP ISO 27001:2013 GCP PCI-DSS 3.2 GCP Dome9 Best Practices
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.IAM.02	Avoid using names like 'Admin' for an Azure SQL	Medium	You must designat	name	Azure Dome9 Best Practices - Sample Azure ISO 27001:2013 Azure GDPR Readiness Azure PCI-DSS 3.2 Azure NIST 800-53 Rev 4 Azure NIST CSF v1.1 Azure Dome9 Best Practices
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.NET.07	Ensure that at least one Network Security Group is	High	Attach a Network	logic	Azure Dome9 Best Practices - Sample Azure ISO 27001:2013 Azure PCI-DSS 3.2 Azure NIST 800-53 Rev 4 Azure NIST CSF v1.1 Azure Dome9 Network Alerts Azure Dome9 Best Practices
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.IAM.01	Avoid using names like 'Admin' for an Azure SQL	Medium	Configure one Azu	name	Azure ISO 27001:2013 Azure GDPR Readiness Azure PCI-DSS 3.2 Azure NIST 800-53 Rev 4 Azure NIST CSF v1.1 Azure Dome9 Best Practices
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.NET.02	Ensure entire Azure infrastructure doesn't have ac	High	Azure connections	name	Azure ISO 27001:2013 Azure NIST 800-53 Rev 4 Azure NIST CSF v1.1 Azure Dome9 Network Alerts Azure Dome9 Best Practices
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.GCP.CRY.04	Ensure oslogin is enabled for a Virtual Machine	High	Enabling osLogin	logic	GCP NIST CSF v1.1 GCP NIST 800-53 Rev 4 GCP ISO 27001:2013 GCP PCI-DSS 3.2 GCP Dome9 Best Practices

Dome9 - March08 Compliance Updates

2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.CRY.19	ECS Cluster At-Rest Encryption	High	Ensure that AWS I logic	AWS Dome9 Best Practices - Sample AWS HIPAA AWS CSA CCM v.3.0.1 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS NIST 800-53 Rev 4 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
2019-01-03T21:18	2019-02-05T22:02:43Z	D9.AWS.LOG.04	Ensure AWS Config is enabled in all regions	High	AWS Config is a v logic	AWS CIS Foundations v. 1.1.0 AWS CSA CCM v.3.0.1 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS NIST 800-53 Rev 4 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.LOG.14	Ensure VPC Flow Logging is Enabled in all Appl	High	VPC Flow Logs is description	AWS HIPAA AWS CSA CCM v.3.0.1 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS NIST 800-53 Rev 4 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.NET.17	RDS should not have Public Interface open to a p	High	RDS should not be complianceTag	AWS HIPAA
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.NET.15	Remove Unused Security Groups	Medium	A security group s complianceTag	AWS NIST 800-53 Rev 4
New Rules						
Date of previous c	Commit Date	Rule ID	Rule Name	Severity	Description	Affected Bundles
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.CRY.01	Ensure that KeyVault is in use	Low	Use the Azure Key	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.CRY.02	Ensure that logging for Azure KeyVault is 'Enabl	High	Enable AuditEvent	Azure CSA CCM v.3.0.1 Azure ISO 27001:2013 Azure PCI-DSS 3.2
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.CRY.03	Ensure that the expiry date is set on all SQL Data	Medium	It is recommended	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.CRY.04	Ensure that the expiry date is set on all SQL Serv	High	It is recommended	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.CRY.05	Ensure that the Redis Cache accepts only SSL cor	High	It is recommended	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.CRY.06	Ensure that 'Secure transfer required' is enabled fo	High	Enable secure tran	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.CRY.07	Ensure that 'Storage service encryption' is enabled	High	Enable data encryp	Azure CSA CCM v.3.0.1 Azure ISO 27001:2013 Azure GDPR Readiness Azure PCI-DSS 3.2 Azure NIST 800-53 Rev 4
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.CRY.08	Ensure that 'Storage service encryption' is enabled	High	Enable data encryp	Azure CSA CCM v.3.0.1 Azure ISO 27001:2013 Azure GDPR Readiness Azure PCI-DSS 3.2 Azure NIST 800-53 Rev 4
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.CRY.10	Ensure that storage account access keys are perio	Medium	Regenerate storage	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.CRY.11	Ensure that 'Data encryption' is set to 'On' for Azu	High	Encrypt SQL Data	Azure CSA CCM v.3.0.1

Dome9 - March08 Compliance Updates

2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.CRY.12	Ensure that the expiry date is set on all keys	High	Ensure that all Key	Azure CSA CCM v.3.0.1 Azure ISO 27001:2013 Azure GDPR Readiness Azure PCI-DSS 3.2
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.CRY.13	Ensure that the expiry date is set on all secrets	High	Ensure that all Sec	Azure CSA CCM v.3.0.1 Azure ISO 27001:2013 Azure GDPR Readiness Azure PCI-DSS 3.2
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.IAM.03	Ensure that Azure SQL Server Admin is configur	Medium	Use Azure Active	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.MON.02	Ensure that 'Auditing' is enabled for Azure SQL D	Medium	Enable auditing on	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.MON.03	Ensure that 'Threat Detection' is enabled for Azur	Medium	Enable threat detec	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.MON.05	Ensure that 'Send alerts to' is enabled for Azure S	Medium	Configure the ema	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.MON.06	Ensure that 'Email service and co-administrators' i	Low	Configure the serv	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.NET.01	Ensure that SQL server access is restricted from th	High	Ensure that no SQ	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.NET.02	Ensure entire Azure infrastructure doesn't have ac	High	Azure connections	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.NET.03	Restrict Azure SQL Server accessibility to a mini	Medium	It is recommended	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.NET.06	Remove unused Network Security Groups	Medium	Delete all Network	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AZU.NET.07	Ensure that at least one Network Security Group i	High	Attach a Network	Azure CSA CCM v.3.0.1
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.CRY.20	AWS Kinesis Streams Keys are rotated	Medium	Rotate the keys of	AWS ISO 27001:2013
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.CRY.21	AWS Kinesis streams are encrypted with KMS cu	High	Use KMS custome	AWS ISO 27001:2013
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.CRY.22	Ensure that your Amazon EFS file systems are en	High	Enable encryption	AWS ISO 27001:2013
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.CRY.23	Ensure that your Amazon EFS file systems are en	High	When you define a	AWS ISO 27001:2013
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.CRY.24	AWS Kinesis Server data at rest has server side e	High	Enable Server Side	AWS ISO 27001:2013
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.IAM.45	Ensure that your Amazon Lambda functions do no	Medium	It is recommended	AWS ISO 27001:2013
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.IAM.49	ECS Service with Admin Roles	High	It is recommended	AWS ISO 27001:2013
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.IAM.46	Lambda Functions with Admin Privileges are not	High	Determine the spec	AWS ISO 27001:2013
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.CRY.25.PCI	Ensure ElastiCache for Memcached is not in use i	High	Amazon ElastiCac	AWS PCI-DSS 3.2
2019-01-03T21:18	2019-03-01T19:48:38Z	D9.AWS.CRY.26.PCI	Ensure that ElastiCache for Redis version is comp	High	Amazon ElastiCac	AWS PCI-DSS 3.2