Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.AWS.CRY.19	ECS Cluster At-Rest Encryption	High	name description	AWS HIPAA AWS NIST 800-53 Rev 4 AWS GDPR Readiness AWS Dome9 Best Practices
D9.AWS.IAM.03	Credentials (with first activated accessKey) unused for 90 days or more should be disabled	Medium	name description	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.IAM.04	Credentials (with password enabled) unused for 90 days or more should be disabled	Medium	name description	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.IAM.05	Credentials (with second activated accessKey) unused for 90 days or more should be disabled	Medium	name description	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.IAM.44	Use managed policies instead of inline IAM Policies	Medium	name complianceTag	AWS HIPAA AWS Dome9 Best Practices
D9.GCP.NET.04	Google Instance with public IP	High	name	GCP PCI-DSS 3.2 GCP NIST 800-53 Rev 4 GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.AWS.LOG.01	Ensure multi-regions trail exists for each AWS CloudTrail	Medium	name	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.LOG.07	Ensure CloudTrail is enabled in all regions	Medium	name	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.MON.08	Ensure a log metric filter and alarm exist for S3 bucket policy changes	Medium	logic	AWS Dome9 S3 Bucket Security AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AZU.MON.04	Ensure that 'Threat Detection types' is set to 'All'	Medium	logic	Azure CIS Foundations v. 1.0.0 Azure NIST 800-53 Rev 4 Azure GDPR Readiness Azure PCI-DSS 3.2 Azure Dome9 Best Practices
D9.AWS.CRY.15	Use KMS CMK customer-managed keys for Redshift clusters	High	logic	AWS HIPAA AWS Dome9 Best Practices

Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.AWS.MON.03	Ensure a log metric filter and alarm exist for usage of 'root' account	Medium	logic	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.MON.04	Ensure a log metric filter and alarm exist for IAM policy changes	Medium	logic	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.MON.05	Ensure a log metric filter and alarm exist for CloudTrail configuration	Low	logic	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.MON.07	Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs	Medium	logic	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.MON.09	Ensure a log metric filter and alarm exist for AWS Config configuration changes	Medium	logic	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.MON.11	Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)	Medium	logic	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.MON.12	Ensure a log metric filter and alarm exist for changes to network gateways	Medium	logic	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.MON.13	Ensure a log metric filter and alarm exist for route table changes	Medium	logic	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.MON.14	Ensure a log metric filter and alarm exist for VPC changes	Medium	logic	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices

Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.AWS.MON.06	Ensure a log metric filter and alarm exist for AWS Management Console authentication failures	Medium	logic	AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.MON.10	Ensure a log metric filter and alarm exist for security group changes	Medium	logic	AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AZU.CRY.05	Redis Cache should not accept non-SSL connections	High	description	Azure NIST 800-53 Rev 4 Azure GDPR Readiness Azure PCI-DSS 3.2 Azure Dome9 Best Practices
D9.AWS.IAM.01	Avoid the use of the 'root' account	High	description	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.IAM.08	Password Policy must require at least one uppercase character	Medium	description	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.IAM.09	Password Policy must require at least one lowercase character	Medium	description	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.IAM.10	Password Policy must require at least one symbol	Medium	description	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.IAM.11	Password Policy must require at least one number	Medium	description	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.IAM.12	Password Policy must require minimal length of 14	Medium	description	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS Dome9 Best Practices
D9.AWS.IAM.20	Ensure IAM policies are attached only to groups or roles	Medium	description	AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.GCP.NET.AG1	VMInstance with unencrypted Mongo (TCP: 27017) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts

Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.GCP.NET.AG	VMInstance with unencrypted LDAP (TCP:389) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Cassandra Internode Communication (TCP:7000) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Cassandra Monitoring (TCP:7199) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Cassandra Client (TCP:9042) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Cassandra Thrift (TCP:9160) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Redis (TCP: 6379) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Cassandra OpsCenter Monitoring (TCP:61620) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Cassandra OpsCenter Website (TCP:8888) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Oracle DB (TCP: 2483) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Oracle DB (TCP: 1521) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Elastic search (TCP:9200) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Elastic search (TCP:9300) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Memcached (TCP:11211) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted LDAP (UDP: 389) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Oracle DB (UDP: 2483) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with unencrypted Memcached (UDP:11211) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Cassandra(TCP: 7001) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service MySQL(TCP: 3306) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service MSSQL Server (TCP:1433) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service SQL Server Analysis Services(TCP:2383) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service MSSQL Debugger(TCP:135) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service LDAP SSL (TCP:636) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Oracle DB SSL (TCP:2484) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts

Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.GCP.NET.AG	Public VMInstance with service Postgres SQL (TCP:5432) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Hadoop Name Node(TCP:9000) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Memcached SSL(TCP:11214) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Memcached SSL(TCP:11215) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Postgres SQL (UDP:5432) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Oracle DB SSL (UDP:2484) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Memcached SSL(UDP:11214) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Memcached SSL(UDP:11215) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Prevalent known internal port(TCP:3000) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service NetBIOS Name Service(TCP:137) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service NetBios Datagram Service(TCP:138) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service NetBios Session Service(TCP:139) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service CIFS / SMB (TCP:3020) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service SaltStack Master(TCP:4505) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service SaltStack Master(TCP:4506) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Known internal web port(TCP:8000) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Known internal web port(TCP:8080) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service NetBIOS Name Service(UDP:137) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service NetBios Datagram Service(UDP:138) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts

Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.GCP.NET.AG	Public VMInstance with service NetBios Session Service(UDP:139) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service SNMP(UDP:161) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Cassandra OpsCenter agent port(TCP:61621) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service MSSQL Admin (TCP:1434) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service SQL Server Analysis Service browser(TCP:2382) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Puppet Master (TCP:8140) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service Mongo Web Portal(TCP:27018) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	Public VMInstance with service MSSQL Browser Service(UDP:1434) is exposed to the entire internet	High	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Cassandra(TCP:7001) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service MySQL(TCP:3306) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service MSSQL Server(TCP:1433) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service SQL Server Analysis Services(TCP:2383) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service MSSQL Debugger (TCP:135) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service LDAP SSL(TCP:636) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Oracle DB SSL(TCP:2484) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Postgres SQL(TCP:5432) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Hadoop Name Node (TCP:9000) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Memcached SSL(TCP:11214) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Memcached SSL(TCP:11215) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Postgres SQL(UDP:5432) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Oracle DB SSL(UDP:2484) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Memcached SSL (UDP:11214) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Memcached SSL (UDP:11215) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts

Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.GCP.NET.AG	VMInstance with service Prevalent known internal port(TCP:3000) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service NetBIOS Name Service(TCP:137) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service NetBios Datagram Service(TCP:138) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service NetBios Session Service(TCP:139) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service CIFS / SMB(TCP:3020) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service SaltStack Master(TCP:4505) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service SaltStack Master(TCP:4506) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Known internal web port(TCP:8000) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Known internal web port(TCP:8080) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service NetBIOS Name Service(UDP:137) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service NetBios Datagram Service(UDP:138) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service NetBios Session Service(UDP:139) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service SNMP(UDP:161) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Cassandra OpsCenter agent port(TCP:61621) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service MSSQL Admin(TCP:1434) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service SQL Server Analysis Service browser(TCP:2382) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Puppet Master(TCP:8140) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Mongo Web Portal (TCP:27018) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service MSSQL Browser Service(UDP:1434) is exposed to a wide network scope	Medium	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Cassandra(TCP:7001) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service MySQL(TCP:3306) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts

Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.GCP.NET.AG	VMInstance with service MSSQL Server(TCP:1433) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service SQL Server Analysis Services(TCP:2383) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service MSSQL Debugger (TCP:135) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service LDAP SSL(TCP:636) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Oracle DB SSL(TCP:2484) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Postgres SQL(TCP:5432) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Hadoop Name Node (TCP:9000) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Memcached SSL(TCP:11214) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Memcached SSL(TCP:11215) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Postgres SQL(UDP:5432) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Oracle DB SSL(UDP:2484) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Memcached SSL (UDP:11214) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Memcached SSL (UDP:11215) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Prevalent known internal port(TCP:3000) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service NetBIOS Name Service(TCP:137) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service NetBios Datagram Service(TCP:138) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service NetBios Session Service(TCP:139) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service CIFS / SMB(TCP:3020) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service SaltStack Master(TCP:4505) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service SaltStack Master(TCP:4506) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Known internal web port(TCP:8000) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Known internal web port(TCP:8080) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts

Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.GCP.NET.AG	VMInstance with service NetBIOS Name Service(UDP:137) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service NetBios Datagram Service(UDP:138) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service NetBios Session Service(UDP:139) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service SNMP(UDP:161) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Cassandra OpsCenter agent port(TCP:61621) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service MSSQL Admin(TCP:1434) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service SQL Server Analysis Service browser(TCP:2382) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Puppet Master(TCP:8140) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service Mongo Web Portal (TCP:27018) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.NET.AG	VMInstance with service MSSQL Browser Service(UDP:1434) is exposed to a small network scope	Low	description	GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.AWS.IAM.27	Ensure IAM policies that allow full "*:*" administrative privileges are not created	High	complianceTag description	AWS HIPAA AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.IAM.18	Ensure HARDWARE MFA is enabled for the 'root' account	High	complianceTag description	AWS NIST 800-53 Rev 4 AWS CIS Foundations v. 1.1.0 AWS GDPR Readiness AWS PCI-DSS 3.2 AWS Dome9 Best Practices
D9.AWS.CRY.17	Use encrypted connection between CloudFront and origin server	High	complianceTag	AWS HIPAA
D9.AWS.IAM.28	S3 bucket should not be world-listable from anonymous users	High	complianceTag	AWS HIPAA
D9.AWS.IAM.29	S3 bucket should not be world-listable	High	complianceTag	AWS HIPAA
D9.AWS.IAM.30	S3 bucket should not be world-writable from anonymous users	High	complianceTag	AWS HIPAA
D9.AWS.IAM.31	S3 bucket should not be world-writable	High	complianceTag	AWS HIPAA
D9.AWS.IAM.32	S3 bucket should not have writable permissions from anonymous users	High	complianceTag	AWS HIPAA
D9.AWS.IAM.33	S3 bucket should not have world-writable permissions	High	complianceTag	AWS HIPAA
D9.AWS.IAM.34	S3 bucket should not have world-readable permissions from anonymous users	High	complianceTag	AWS HIPAA
D9.AWS.IAM.35	S3 bucket should not have world-readable permissions	High	complianceTag	AWS HIPAA

Rule ID	Rule Name	Severity	Updated Fields	Affected Bundles
D9.AWS.IAM.36	S3 bucket should not allow delete actions from all principals	High	complianceTag	AWS HIPAA
D9.AWS.IAM.37	S3 bucket should not allow get actions from all principals	High	complianceTag	AWS HIPAA
D9.AWS.IAM.38	S3 bucket should not allow list actions from all principals	High	complianceTag	AWS HIPAA
D9.AWS.IAM.39	S3 bucket should not allow put actions from all principals	High	complianceTag	AWS HIPAA
D9.AWS.IAM.40	S3 bucket should not allow all actions from all principals	High	complianceTag	AWS HIPAA
D9.AWS.IAM.41	S3 bucket should not allow put or restore actions from all principals	High	complianceTag	AWS HIPAA