Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.GCP.NET.AG6.VMInstance.61621.TCI	Public VMInstance with service Cassandra OpsCenter agent(TCP:61621) is exposed to the entire internet	High	Databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to only the applications, services and endpoints that requires access. This rule detects network settings that may expose an instance or a database Cassandra to a too permissive network access.	name	GCP Dome9 Network Alerts GCP Dome9 Best Practices
D9.GCP.NET.AG7.VMInstance.61621.TCI	Public VMInstance with service Cassandra OpsCenter agent(TCP:61621) is exposed to a wide public network	High	Databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to only the applications, services and endpoints that requires access. This rule detects network settings that my expose an instance or a database Cassandra to a too permissive network access.	name	GCP Dome9 Network Alerts GCP Dome9 Best Practices
D9.GCP.NET.AG8.VMInstance.61621.TCI	Public VMInstance with service Cassandra OpsCenter agent(TCP:61621) is exposed to a small public network	Medium	Databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to only the applications, services and endpoints that requires access. This rule detects network settings that my expose an instance or a database Cassandra to a too permissive network access.	name	GCP Dome9 Network Alerts GCP Dome9 Best Practices
D9.GCP.NET.AG9.VMInstance.61621.TCI	VMInstance with service Cassandra OpsCenter agent(TCP:61621) is exposed to a wide network scope	Medium	Databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to only the applications, services and endpoints that requires access. This rule detects network settings that may expose an instance or a database Cassandra to a too permissive network access.	name	GCP Dome9 Network Alerts GCP Dome9 Best Practices
D9.GCP.NET.AG10.VMInstance.61621.TC	VMInstance with service Cassandra OpsCenter agent(TCP:61621) is exposed to a small network scope	Low	Databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to only the applications, services and endpoints that requires access. This rule detects network settings that may expose an instance or a database Cassandra to a too permissive network access.	name	GCP Dome9 Network Alerts GCP Dome9 Best Practices

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG6.Instance.61621.TCP	Public Instance with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to the entire internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG6.ELB.61621.TCP	Public ELB with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to the entire internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG6.NetworkLoadBalancer	Public NetworkLoadBalancer with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to the entire internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG6.ApplicationLoadBalan	Public ApplicationLoadBalancer with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to the entire internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG7.Instance.61621.TCP	Public Instance with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a wide public network	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG7.ELB.61621.TCP	Public ELB with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a wide public network	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG7.NetworkLoadBalancer	Public NetworkLoadBalancer with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a wide public network	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG7.ApplicationLoadBalan	Public ApplicationLoadBalancer with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a wide public network	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG8.Instance.61621.TCP	Public Instance with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a small public network	Medium	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG8.ELB.61621.TCP	Public ELB with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a small public network	Medium	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG8.NetworkLoadBalancer	Public NetworkLoadBalancer with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a small public network	Medium	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG8.ApplicationLoadBalan	Public ApplicationLoadBalancer with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a small public network	Medium	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG9.Instance.61621.TCP	Instance with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a wide network scope	Medium	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG9.ELB.61621.TCP	ELB with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a wide network scope	Medium	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG9.NetworkLoadBalancer	NetworkLoadBalancer with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a wide network scope	Medium	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG9.ApplicationLoadBalan	ApplicationLoadBalancer with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a wide network scope	Medium	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG10.Instance.61621.TCP	Instance with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a small network scope	Low	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG10.ELB.61621.TCP	ELB with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a small network scope	Low	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG10.NetworkLoadBalance	NetworkLoadBalancer with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a small network scope	Low	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AWS.NET.AG10.ApplicationLoadBala	ApplicationLoadBalancer with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a small network scope	Low	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 Network Alerts AWS Dome9 Best Practices
D9.AZU.NET.AG6.VirtualMachine.61621.	VirtualMachine with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to the entire internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	Azure Dome9 Network Alerts Azure Dome9 Best Practices
D9.AZU.NET.AG7.VirtualMachine.61621.	VirtualMachine with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a wide public network	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	Azure Dome9 Network Alerts Azure Dome9 Best Practices
D9.AZU.NET.AG8.VirtualMachine.61621.	VirtualMachine with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a small public network	Medium	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	Azure Dome9 Network Alerts Azure Dome9 Best Practices
D9.AZU.NET.AG9.VirtualMachine.61621.	VirtualMachine with service Cassandra OpsCenter agent (TCP:61621) is exposed to a wide network scope	Medium	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	Azure Dome9 Network Alerts Azure Dome9 Best Practices

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AZU.NET.AG10.VirtualMachine.61621	VirtualMachine with service 'Cassandra OpsCenter agent' (TCP:61621) is exposed to a small network scope	Low	Cassandra OpsCenter agent is considered a protocol that should only be exposed in private networks, for a limited scope, allowing access to only applications and services that requires access. Limiting access is a good practice that prevents exploits through public interfaces or east west lateral movement. This rule detects network settings that allow over permissive network access for Cassandra OpsCenter agent	name description	Azure Dome9 Network Alerts Azure Dome9 Best Practices
D9.AZU.CRY.12	Ensure that the expiry date is set on all keys	High	Ensure that all Keys in Azure Key Vault have an expiry time set.	logic	Azure HIPAA Azure Dome9 SOC2 based on AICPA TSC 2017 Azure CSA CCM v.3.0.1 Azure CIS Foundations v. 1.0.0 Azure NIST 800-53 Rev 4 Azure ISO 27001:2013 Azure GDPR Readiness Azure NIST CSF v1.1 Azure PCI-DSS 3.2 Azure Dome9 Best Practices
D9.AZU.CRY.13	Ensure that the expiry date is set on all secrets	High	Ensure that all Secrets in Azure Key Vault have an expiry time set.	logic	Azure HIPAA Azure Dome9 SOC2 based on AICPA TSC 2017 Azure CSA CCM v.3.0.1 Azure CIS Foundations v. 1.0.0 Azure NIST 800-53 Rev 4 Azure ISO 27001:2013 Azure GDPR Readiness Azure NIST CSF v1.1 Azure PCI-DSS 3.2 Azure Dome9 Best Practices
D9.AWS.IAM.45	Ensure that your Amazon Lambda functions do not share the same AWS IAM execution role	Medium	It is recommended to have one IAM role per each Lambda function in order to follow the Principle of Least Privilege. This way you can ensure that your Lambda functions will have the minimum privileges needed to perform the required tasks.	logic	AWS Dome9 Serverless Architectures Security AWS HIPAA AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 SOC2 based on AICPA TSC 2017 AWS Dome9 Best Practices
D9.GCP.CRY.01	Ensure VM disks are encrypted with Customer-Supplied Encryption Keys (CSEK)	High	By default, GCP encrypts all data with GCP owned keys. You should provide your own encryption keys to manage the Customer-Supplied encryption keys.	logic	GCP Dome9 Best Practices - Sample GCP CIS Foundations v. 1.0.0 GCP PCI-DSS 3.2 GCP NIST 800-53 Rev 4 GCP ISO 27001:2013 GCP NIST CSF v1.1 GCP Dome9 Best Practices

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.GCP.NET.14	Ensure Private Google Access is enabled for all subnetworks in VPC Network	High	Private Google Access enables virtual machine instances on a subnet to reach Google APIs and services using an internal IP address rather than an external IP address. External IP addresses are routable and reachable over the Internet. Internal (private) IP addresses are internal to Google Cloud Platform and are not routable or reachable over the Internet. You can use Private Google Access to allow VMs without Internet access to reach Google APIs, services, and properties that are accessible over HTTP/HTTPS.	name	GCP CIS Foundations v. 1.0.0 GCP PCI-DSS 3.2 GCP NIST 800-53 Rev 4 GCP ISO 27001:2013 GCP NIST CSF v1.1 GCP Dome9 Best Practices GCP Dome9 Network Alerts
D9.GCP.CRY.02	Ensure "Block Project-wide SSH keys" enabled for non-windows VM instances	High	Project-wide SSH keys are stored in Compute/Project-meta-data. Project wide ssh keys can be used to login into all the instances within project. Using project-wide ssh keys eases the SSH key management but if compromised, poses the security risk which can impact all the instances within project. It is recommended to use Instance specific SSH keys which can limit the attack surface in case of SSH keys getting compromised.	name logic	GCP CIS Foundations v. 1.0.0 GCP PCI-DSS 3.2 GCP NIST 800-53 Rev 4 GCP ISO 27001:2013 GCP NIST CSF v1.1 GCP Dome9 Best Practices
D9.GCP.GKE.04	Ensure Kubernetes web UI / Dashboard is disabled	High	Dashboard is a web-based Kubernetes user interface. You can use Dashboard to deploy containerized applications to a Kubernetes cluster, troubleshoot your containerized application, and manage the cluster itself along with its attendant resources. You can use Dashboard to get an overview of applications running on your cluster, as well as for creating or modifying individual Kubernetes resources (such as Deployments, Jobs, DaemonSets, etc). For example, you can scale a Deployment, initiate a rolling update, restart a pod or deploy new applications using a deploy wizard. You should disable the Kubernetes Web UI (Dashboard) when running on Kubernetes Engine. The Kubernetes Web UI (Dashboard) is backed by a highly privileged Kubernetes Service Account.	description	GCP CIS Foundations v. 1.0.0 GCP Dome9 Best Practices
D9.GCP.GKE.07	Ensure Container-Optimized OS (cos) is used for Kubernetes Engine Clusters Node image	High	Container-Optimized OS is an operating system image for your Compute Engine VMs that is optimized for running Docker containers. With Container-Optimized OS, you can bring up your Docker containers on Google Cloud Platform quickly, efficiently, and securely.	logic	GCP CIS Foundations v. 1.0.0 GCP Dome9 Best Practices

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AZU.CRY.12	Ensure that the expiry date is set on all keys	High	Ensure that all Keys in Azure Key Vault have an expiry time set.	logic	Azure HIPAA Azure Dome9 SOC2 based on AICPA TSC 2017 Azure CSA CCM v.3.0.1 Azure CIS Foundations v. 1.0.0 Azure NIST 800-53 Rev 4 Azure ISO 27001:2013 Azure GDPR Readiness Azure NIST CSF v1.1 Azure PCI-DSS 3.2 Azure Dome9 Best Practices
D9.AZU.CRY.13	Ensure that the expiry date is set on all secrets	High	Ensure that all Secrets in Azure Key Vault have an expiry time set.	logic	Azure HIPAA Azure Dome9 SOC2 based on AICPA TSC 2017 Azure CSA CCM v.3.0.1 Azure CIS Foundations v. 1.0.0 Azure NIST 800-53 Rev 4 Azure ISO 27001:2013 Azure GDPR Readiness Azure NIST CSF v1.1 Azure PCI-DSS 3.2 Azure Dome9 Best Practices
D9.AWS.IAM.45	Ensure that your Amazon Lambda functions do not share the same AWS IAM execution role	Medium	It is recommended to have one IAM role per each Lambda function in order to follow the Principle of Least Privilege. This way you can ensure that your Lambda functions will have the minimum privileges needed to perform the required tasks.	logic	AWS Dome9 Serverless Architectures Security AWS HIPAA AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 SOC2 based on AICPA TSC 2017 AWS Dome9 Best Practices
D9.GCP.CRY.01	Ensure VM disks are encrypted with Customer-Supplied Encryption Keys (CSEK)	High	By default, GCP encrypts all data with GCP owned keys. You should provide your own encryption keys to manage the Customer-Supplied encryption keys.	logic	GCP Dome9 Best Practices - Sample GCP CIS Foundations v. 1.0.0 GCP PCI-DSS 3.2 GCP NIST 800-53 Rev 4 GCP ISO 27001:2013 GCP NIST CSF v1.1 GCP Dome9 Best Practices
D9.GCP.NET.14	Ensure Private Google Access is enabled for all subnetworks in VPC Network	High	Private Google Access enables virtual machine instances on a subnet to reach Google APIs and services using an internal IP address rather than an external IP address. External IP addresses are routable and reachable over the Internet. Internal (private) IP addresses are internal to Google Cloud Platform and are not routable or reachable over the Internet. You can use Private Google Access to allow VMs without Internet access to reach Google APIs, services, and properties that are accessible over HTTP/HTTPS.	name	GCP CIS Foundations v. 1.0.0 GCP PCI-DSS 3.2 GCP NIST 800-53 Rev 4 GCP ISO 27001:2013 GCP NIST CSF v1.1 GCP Dome9 Best Practices GCP Dome9 Network Alerts

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.GCP.CRY.02	Ensure "Block Project-wide SSH keys" enabled for non-windows VM instances	High	Project-wide SSH keys are stored in Compute/Project-meta-data. Project wide ssh keys can be used to login into all the instances within project. Using project-wide ssh keys eases the SSH key management but if compromised, poses the security risk which can impact all the instances within project. It is recommended to use Instance specific SSH keys which can limit the attack surface in case of SSH keys getting compromised.	name logic	GCP CIS Foundations v. 1.0.0 GCP PCI-DSS 3.2 GCP NIST 800-53 Rev 4 GCP ISO 27001:2013 GCP NIST CSF v1.1 GCP Dome9 Best Practices
D9.GCP.GKE.04	Ensure Kubernetes web UI / Dashboard is disabled	High	Dashboard is a web-based Kubernetes user interface. You can use Dashboard to deploy containerized applications to a Kubernetes cluster, troubleshoot your containerized application, and manage the cluster itself along with its attendant resources. You can use Dashboard to get an overview of applications running on your cluster, as well as for creating or modifying individual Kubernetes resources (such as Deployments, Jobs, DaemonSets, etc). For example, you can scale a Deployment, initiate a rolling update, restart a pod or deploy new applications using a deploy wizard. You should disable the Kubernetes Web UI (Dashboard) when running on Kubernetes Engine. The Kubernetes Web UI (Dashboard) is backed by a highly privileged Kubernetes Service Account.	description	GCP CIS Foundations v. 1.0.0 GCP Dome9 Best Practices
D9.GCP.GKE.07	Ensure Container-Optimized OS (cos) is used for Kubernetes Engine Clusters Node image	High	Container-Optimized OS is an operating system image for your Compute Engine VMs that is optimized for running Docker containers. With Container-Optimized OS, you can bring up your Docker containers on Google Cloud Platform quickly, efficiently, and securely.	logic	GCP CIS Foundations v. 1.0.0 GCP Dome9 Best Practices

Cloud Guard Dome9- Compliance Updates May23

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1.Instance.27017.TCP					
D9.AWS.NET.AG1.Instance.389.TCP					
D9.AWS.NET.AG1.Instance.7000.TCP					
D9.AWS.NET.AG1.Instance.7199.TCP					
D9.AWS.NET.AG1.Instance.9042.TCP					
D9.AWS.NET.AG1.Instance.9160.TCP					
D9.AWS.NET.AG1.Instance.6379.TCP					
D9.AWS.NET.AG1.Instance.61620.TCP					
D9.AWS.NET.AG1.Instance.8888.TCP					
D9.AWS.NET.AG1.Instance.2483.TCP					
D9.AWS.NET.AG1.Instance.1521.TCP					
D9.AWS.NET.AG1.Instance.9200.TCP					
D9.AWS.NET.AG1.Instance.9300.TCP					
D9.AWS.NET.AG1.Instance.11211.TCP					
D9.AWS.NET.AG1.Instance.389.UDP					
D9.AWS.NET.AG1.Instance.2483.UDP					
D9.AWS.NET.AG1.Instance.11211.UDP					
D9.AWS.NET.AG1.ELB.27017.TCP					
D9.AWS.NET.AG1.ELB.389.TCP					
D9.AWS.NET.AG1.ELB.7000.TCP					
D9.AWS.NET.AG1.ELB.7199.TCP					
D9.AWS.NET.AG1.ELB.9042.TCP					
D9.AWS.NET.AG1.ELB.9160.TCP					
D9.AWS.NET.AG1.ELB.6379.TCP					
D9.AWS.NET.AG1.ELB.61620.TCP					
D9.AWS.NET.AG1.ELB.8888.TCP					
D9.AWS.NET.AG1.ELB.2483.TCP					
D9.AWS.NET.AG1.ELB.1521.TCP					
D9.AWS.NET.AG1.ELB.9200.TCP					
D9.AWS.NET.AG1.ELB.9300.TCP					
D9.AWS.NET.AG1.ELB.11211.TCP					
D9.AWS.NET.AG1.ELB.389.UDP					
D9.AWS.NET.AG1.ELB.2483.UDP					
D9.AWS.NET.AG1.ELB.11211.UDP					
D9.AWS.NET.AG1. NetworkLoadBalancer.27017.TCP					
D9.AWS.NET.AG1. NetworkLoadBalancer.389.TCP					
D9.AWS.NET.AG1. NetworkLoadBalancer.7000.TCP					
D9.AWS.NET.AG1. NetworkLoadBalancer.7199.TCP					
D9.AWS.NET.AG1. NetworkLoadBalancer.9042.TCP					
D9.AWS.NET.AG1. NetworkLoadBalancer.9160.TCP					
D9.AWS.NET.AG1. NetworkLoadBalancer.6379.TCP					
D9.AWS.NET.AG1. NetworkLoadBalancer.61620.TCP					
D9.AWS.NET.AG1. NetworkLoadBalancer.8888.TCP					
D9.AWS.NET.AG1. NetworkLoadBalancer.2483.TCP					
D9.AWS.NET.AG1.					

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1.Instance.27017.TCP	Instance with unencrypted Mongo (TCP: 27017) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.389.TCP	Instance with unencrypted LDAP (TCP:389) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.7000.TCP	Instance with unencrypted Cassandra Internode Communication (TCP:7000) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.7199.TCP	Instance with unencrypted Cassandra Monitoring (TCP:7199) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.9042.TCP	Instance with unencrypted Cassandra Client (TCP:9042) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1.Instance.9160.TCP	Instance with unencrypted Cassandra Thrift (TCP:9160) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.6379.TCP	Instance with unencrypted Redis (TCP:6379) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.61620.TCP	Instance with unencrypted Cassandra OpsCenter Monitoring (TCP:61620) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.8888.TCP	Instance with unencrypted Cassandra OpsCenter Website (TCP:8888) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.2483.TCP	Instance with unencrypted Oracle DB (TCP: 2483) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1.Instance.1521.TCP	Instance with unencrypted Oracle DB (TCP: 1521) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.9200.TCP	Instance with unencrypted Elastic search (TCP:9200) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.9300.TCP	Instance with unencrypted Elastic search (TCP:9300) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.11211.TCP	Instance with unencrypted Memcached (TCP: 11211) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.389.UDP	Instance with unencrypted LDAP (UDP:389) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1.Instance.2483.UDP	Instance with unencrypted Oracle DB (UDP: 2483) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.Instance.11211.UDP	Instance with unencrypted Memcached (UDP: 11211) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.27017.TCP	ELB with unencrypted Mongo (TCP:27017) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.389.TCP	ELB with unencrypted LDAP (TCP:389) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.7000.TCP	ELB with unencrypted Cassandra Internode Communication (TCP:7000) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1.ELB.7199.TCP	ELB with unencrypted Cassandra Monitoring (TCP:7199) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.9042.TCP	ELB with unencrypted Cassandra Client (TCP:9042) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.9160.TCP	ELB with unencrypted Cassandra Thrift (TCP:9160) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.6379.TCP	ELB with unencrypted Redis (TCP:6379) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.61620.TCP	ELB with unencrypted Cassandra OpsCenter Monitoring (TCP:61620) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1.ELB.8888.TCP	ELB with unencrypted Cassandra OpsCenter Website (TCP:8888) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.2483.TCP	ELB with unencrypted Oracle DB (TCP:2483) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.1521.TCP	ELB with unencrypted Oracle DB (TCP:1521) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.9200.TCP	ELB with unencrypted Elastic search (TCP: 9200) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.9300.TCP	ELB with unencrypted Elastic search (TCP: 9300) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1.ELB.11211.TCP	ELB with unencrypted Memcached (TCP: 11211) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.389.UDP	ELB with unencrypted LDAP (UDP:389) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.2483.UDP	ELB with unencrypted Oracle DB (UDP: 2483) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1.ELB.11211.UDP	ELB with unencrypted Memcached (UDP: 11211) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.27017.TCP	NetworkLoadBalancer with unencrypted Mongo (TCP:27017) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1. NetworkLoadBalancer.389.TCP	NetworkLoadBalancer with unencrypted LDAP (TCP:389) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.7000.TCP	NetworkLoadBalancer with unencrypted Cassandra Internode Communication (TCP: 7000) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.7199.TCP	NetworkLoadBalancer with unencrypted Cassandra Monitoring (TCP:7199) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.9042.TCP	NetworkLoadBalancer with unencrypted Cassandra Client (TCP:9042) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.9160.TCP	NetworkLoadBalancer with unencrypted Cassandra Thrift (TCP:9160) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1. NetworkLoadBalancer.6379.TCP	NetworkLoadBalancer with unencrypted Redis (TCP:6379) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.61620.TCP	NetworkLoadBalancer with unencrypted Cassandra OpsCenter Monitoring (TCP: 61620) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.8888.TCP	NetworkLoadBalancer with unencrypted Cassandra OpsCenter Website (TCP:8888) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.2483.TCP	NetworkLoadBalancer with unencrypted Oracle DB (TCP:2483) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.1521.TCP	NetworkLoadBalancer with unencrypted Oracle DB (TCP:1521) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1. NetworkLoadBalancer.9200.TCP	NetworkLoadBalancer with unencrypted Elastic search (TCP:9200) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.9300.TCP	NetworkLoadBalancer with unencrypted Elastic search (TCP:9300) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.11211.TCP	NetworkLoadBalancer with unencrypted Memcached (TCP:11211) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.389.UDP	NetworkLoadBalancer with unencrypted LDAP (UDP:389) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. NetworkLoadBalancer.2483.UDP	NetworkLoadBalancer with unencrypted Oracle DB (UDP:2483) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1. NetworkLoadBalancer.11211.UDP	NetworkLoadBalancer with unencrypted Memcached (UDP:11211) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.27017.TCP	ApplicationLoadBalancer with unencrypted Mongo (TCP:27017) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.389.TCP	ApplicationLoadBalancer with unencrypted LDAP (TCP:389) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.7000.TCP	ApplicationLoadBalancer with unencrypted Cassandra Internode Communication (TCP: 7000) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.7199.TCP	ApplicationLoadBalancer with unencrypted Cassandra Monitoring (TCP:7199) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1. ApplicationLoadBalancer.9042.TCP	ApplicationLoadBalancer with unencrypted Cassandra Client (TCP:9042) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.9160.TCP	ApplicationLoadBalancer with unencrypted Cassandra Thrift (TCP:9160) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.6379.TCP	ApplicationLoadBalancer with unencrypted Redis (TCP:6379) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.61620.TCP	ApplicationLoadBalancer with unencrypted Cassandra OpsCenter Monitoring (TCP: 61620) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.8888.TCP	ApplicationLoadBalancer with unencrypted Cassandra OpsCenter Website (TCP:8888) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1. ApplicationLoadBalancer.2483.TCP	ApplicationLoadBalancer with unencrypted Oracle DB (TCP:2483) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.1521.TCP	ApplicationLoadBalancer with unencrypted Oracle DB (TCP:1521) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.9200.TCP	ApplicationLoadBalancer with unencrypted Elastic search (TCP:9200) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.9300.TCP	ApplicationLoadBalancer with unencrypted Elastic search (TCP:9300) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.11211.TCP	ApplicationLoadBalancer with unencrypted Memcached (TCP:11211) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1

Rule ID	Rule Name	Severity	Description	Updated Fields	Affected Bundles
D9.AWS.NET.AG1. ApplicationLoadBalancer.389.UDP	ApplicationLoadBalancer with unencrypted LDAP (UDP:389) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.2483.UDP	ApplicationLoadBalancer with unencrypted Oracle DB (UDP:2483) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1
D9.AWS.NET.AG1. ApplicationLoadBalancer.11211.UDP	ApplicationLoadBalancer with unencrypted Memcached (UDP:11211) is potentially exposed to the public internet	High	Services and databases store data that may be sensitive, protected by law, subject to regulatory requirements or compliance standards. It is highly recommended that access to data will be restricted to encrypted protocols. This rule detects network settings that may expose data via unencrypted protocol over the public internet or to a too wide local scope.	name	AWS Dome9 SOC2 based on AICPA TSC 2017 AWS NIST 800-53 Rev 4 AWS ISO 27001:2013 AWS NIST CSF v1.1 AWS Dome9 Network Alerts AWS Dome9 Best Practices AWS GDPR Readiness AWS PCI-DSS 3.2 AWS CSA CCM v.3.0.1