Yandex Cloud

Checkov PCI-DSS Requirements mapping

№ of check	Description	Requirement
CKV_YC_1	"Ensure security group is assigned to database cluster."	PCI DSS 1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment PCI DSS 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment
CKV_YC_2	"Ensure compute instance does not have public IP."	PCI DSS 1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.
CKV_YC_3	"Ensure storage bucket is encrypted."	PCI DSS 3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:
CKV_YC_4	"Ensure compute instance does not have serial console enabled."	PCI DSS 2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network
CKV_YC_5	"Ensure Kubernetes cluster	PCI DSS 1.3.6 Place system components that store cardholder data (such as a database) in an internal

	does not have public IP address."	network zone, segregated from the DMZ and other untrusted networks.
CKV_YC_6	"Ensure Kubernetes cluster node group does not have public IP addresses."	PCI DSS 1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.
CKV_YC_7	"Ensure Kubernetes cluster auto-upgrade is enabled."	PCI DSS 6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendorsupplied security patches. Install critical security patches within one month of release
CKV_YC_8	"Ensure Kubernetes node group auto-upgrade is enabled."	PCI DSS 6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendorsupplied security patches. Install critical security patches within one month of release
CKV_YC_9	"Ensure KMS symmetric key is rotated."	PCI DSS 3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or…
CKV_YC_10	"Ensure etcd database is encrypted with KMS key."	PCI DSS 3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:
CKV_YC_11	"Ensure security group is assigned to network interface."	PCI DSS 1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment
CKV_YC_12	"Ensure public IP is not assigned to database cluster."	PCI DSS 1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

CKV_YC_13	"Ensure cloud member does not have elevated access."	PCI DSS 7.2 Establish an access control system(s) for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.
CKV_YC_14	"Ensure security group is assigned to Kubernetes cluster."	PCI DSS 1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment
CKV_YC_15	"Ensure security group is assigned to Kubernetes node group."	PCI DSS 1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment
CKV_YC_16	"Ensure network policy is assigned to Kubernetes cluster."	PCI DSS 1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment
CKV_YC_17	"Ensure storage bucket does not have public access permissions."	PCI DSS 1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.
CKV_YC_18	"Ensure compute instance group does not have public IP."	PCI DSS 1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.
CKV_YC_19	"Ensure security group does not contain allow-all rules."	PCI DSS 1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement
CKV_YC_20	"Ensure security group rule is not allow-all."	PCI DSS 1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by

		using an explicit “deny all” or an implicit deny after allow statement
CKV_YC_21	"Ensure organization member does not have elevated access."	PCI DSS 7.2 Establish an access control system(s) for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.
CKV_YC_22	"Ensure compute instance group has security group assigned."	PCI DSS 1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment
CKV_YC_23	"Ensure folder member does not have elevated access."	PCI DSS 7.2 Establish an access control system(s) for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.
CKV_YC_24	"Ensure passport account is not used for assignment. Use service accounts and federated accounts where possible."	PCI DSS 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access

Константин Константинопольский
+7 (999) 556-55-45
kostik@yandex-team