Searches & Use Cases

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
Searches				
1	Find who deleted a folder (requires values)	json_payload.event_type="yandex.cloud.audit.resourcemanager.DeleteFolder" and json_payload.details.folder_name="<название каталога>"	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.resourcemanager.DeleteFolder and cloud.folder.name: <название каталога>	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.resourcemanager.DeleteFolder' and JSON_VALUE(data, "$.details.folder_name") = 'test' limit 100
2	Find who created/stopped/restarted/deleted a virtual machine (requires values)	json_payload.details.instance_id="<<идентификатор виртуальной машины>>" and (json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" or json_payload.event_type="yandex.cloud.audit.compute.UpdateInstance" or json_payload.event_type="yandex.cloud.audit.compute.DeleteInstance" or	event.dataset: yandexcloud.audittrail and event.action : yandex.cloud.audit.compute.*Instance and cloud.instance.name: testdasdas	select * from bindings.`binding` where (JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.compute.DeleteInstance' or JSON_VALUE(data, "$.event_type") =

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
		json_payload.event_type="yandex.cloud.audit.compute.StartInstance" or json_payload.event_type="yandex.cloud.audit.compute.StopInstance" or json_payload.event_type="yandex.cloud.audit.compute.RestartInstance")		'yandex.cloud.audit.compute.CreateInstance') and JSON_VALUE(data, "$.details.instance_id") = 'fhmpgh36fo3vclan2e99' limit 100 ;
3	What actions did a particular user perform over a period of time (requires values)	json_payload.authentication.subject_name="mirtov8@yandex-team.ru" and json_payload.event_time<"2022-03-01" and json_payload.event_time<"2022-04-01"	event.dataset: yandexcloud.audittrail and user.name : mirtov8@yandex-team.ru and event_time < 2022-07-15	select * from bindings.`binding` where JSON_VALUE(data, "$.authentication.subject_name") = 'mirtov8@yandex-team.ru' and cast(JSON_VALUE(data, "$.event_time") as Timestamp) > Date("2022-08-15") limit 10 ;

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
4	Search for events by objects of a specific folder (requires values)	json_payload.resource_metadata.path[1].resource_type="resource-manager.folder" and json_payload.resource_metadata.path[1].resource_name="<имя каталога>") or (json_payload.resource_metadata.path[2].resource_type="resource-manager.folder" and json_payload.resource_metadata.path[2].resource_name="<имя каталога>"	event.dataset:yandexcloud.audittrail and cloud.folder.name:"mirtov-scale"	select * from bindings.`binding` where JSON_VALUE(data, "$.resource_metadata.path[2].resource_name") = 'mirtov-scale' limit 100 ;
Use cases				
IAM				
1	Triggered when creating service account credentials	json_payload.event_type="yandex.cloud.audit.iam.CreateAccessKey" or json_payload.event_type="yandex.cloud.audit.iam.CreateKey" or json_payload.event_type="yandex.cloud.audit.iam.CreateApiKey"	event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.iam.CreateAccessKey or yandex.cloud.audit.iam.CreateKey or andex.cloud.audit.iam.CreateApiKey)	select * from bindings.`binding-yds` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.iam.CreateAccessKey' or JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.iam.CreateKey' or JSON_VALUE(data,

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
				`"$.event_type") = 'yandex.cloud.audit.iam.CreateApiKey' limit 1 ;`
2	Trigger on any action under a privileged account with the role "resource-manager.clouds.owner" and "organization-manager.admin"" (can be a list) (requires values)	`json_payload.authentication.subject_name="mirtov8@yandex-team.ru" or json_payload.authentication.subject_name="kirill@yandex-team.ru"`	`event.dataset: yandexcloud.audittrail and user.name : mirtov8@yandex-team.ru kirill8@yandex-team.ru`	-
3	Abnormal number of failed authorization attempts (requires values)	---	`event.dataset: yandexcloud.audittrail and error.message: Permission denied`	-
4	Assignment of admin rights (for resources: folder, cloud)	`json_payload.details.access_binding_deltas.access_binding.role_id="admin"`	`event.dataset: yandexcloud.audittrail and details.access_binding_`	``select * from bindings.`binding` where``

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
			deltas.access_binding.role_id: admin	JSON_VALUE(data, "$.details.access_binding_deltas.access_binding.role_id") = 'admin' limit 1 ;
5	Assigning the vpc.public.admin role	json_payload.details.access_binding_deltas.access_binding.role_id="vpc.publicAdmin"	event.dataset: yandexcloud.audittrail and details.access_binding_deltas.access_binding.role_id: vpc.publicAdmin	select * from bindings.`binding` where JSON_VALUE(data, "$.details.access_binding_deltas.access_binding.role_id") = 'vpc.publicAdmin' limit 1 ;
6	Calling the API using YC or terraform under a suspicious user or ip	json_payload.request_metadata.user_agent:"YC" or json_payload.request_metadata.user_agent:"Terraform"	event.dataset: yandexcloud.audittrail and (user_agent.original.keyword: *YC/* or user_agent.original.keyword: *Terraform*)	select * from bindings.`binding` where JSON_VALUE(data, "$.details.request_metadata.user_agent") = 'YC' or JSON_VALUE(data,

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
				"$.details.request_metadata.user_agent") = 'Terraform' limit 1 ;
7	coming soon A new certificate has been added to the federation	---	---	
8	coming soon Changed federation settings	---	---	
9	new *Any action using a cloud service account from a range of IP addresses outside the cloud*	not json_payload.request_metadata.remote_address:"51.250"….	event.dataset: yandexcloud.audittrail and user.type: SERVICE_ACCOUNT and not source.ip: ("51.250.0.0/17" or "31.44.8.0/21" or "62.84.112.0/20" or "84.201.128.0/18" or "84.252.128.0/20" or "130.193.32.0/19" or "178.154.192.0/18" or "178.170.222.0/24" or "185.206.164.0/22" or "193.32.216.0/22" or	-

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
			"217.28.224.0/20") and source.ip: *	
			Compute	
10	Triggering on an event with the creation of a VM with a white IP address	json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and json_payload.details.network_interfaces.primary_v4_address.one_to_one_nat.address exists	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.CreateInstance and details.network_interfaces.primary_v4_address.one_to_one_nat.address: *	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.compute.CreateInstance' and JSON_EXISTS(data, "$.details.network_interfaces.primary_v4_address.one_to_one_nat.address") limit 1 ;
11	Triggered to create "two-legged" virtual machines	json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and json_payload.details.network_interfaces[1].index="1"	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.CreateInstance and details.network_interfaces.index: 1	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.compute.CreateInstance' and JSON_VALUE(data,

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
				"$.details.network_interfaces[1].index") = '1' limit 1 ;
12	Uploading an image to the cloud from a non-fixed S3 Bucket (requires values)	json_payload.event_type="yandex.cloud.audit.compute.CreateImage" and not json_payload.details.source_uri:"https://storage.yandexcloud.net/action-log-123"	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.CreateImage and not cloud.image.source_uri: "https://storage.yandexcloud.net/action-log-123"	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.compute.CreateImage' and JSON_VALUE(data, "$.details.source_uri") != 'https://storage.yandexcloud.net/action-log-123' limit 1 ;
13	Create VM with image_id from Marketplace	not json_payload.details.product_ids[0]=null	event.dataset: yandexcloud.audittrail and details.product_ids: *	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") =

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
				'yandex.cloud.audit.compute.CreateInstance' and JSON_VALUE(data, "$.details.product_ids[0]") != 'null' limit 1 ;
14	Adding a public IP address to an existing virtual machine	json_payload.event_type="yandex.cloud.audit.compute.AddInstanceOneToOneNat"	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.AddInstanceOneToOneNat	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.compute.AddInstanceOneToOneNat' limit 1 ;
15	VM creation/modification events - enabling the serial port	json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and json_payload.details.metadata_serial_port_enable="1"	event.dataset: yandexcloud.audittrail and event.outcome : success and event.action: yandex.cloud.audit.compute.CreateInstance and details.metadata_serial_port_enable: 1	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.compute.CreateInstance' and JSON_VALUE(data,

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
				"$.details.metadata_serial_port_enable") = '1' limit 1 ;
16	new Modifying VM - Adding Access to Serial Console	json_payload.event_type="yandex.cloud.audit.compute.UpdateInstance" or json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and json_payload.details.metadata_serial_port_enable="1"	event.dataset: yandexcloud.audittrail and event.outcome : success and event.action: (yandex.cloud.audit.compute.CreateInstance or yandex.cloud.audit.compute.UpdateInstance) and details.metadata_serial_port_enable: 1	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.compute.UpdateInstance' and JSON_VALUE(data, "$.details.metadata_serial_port_enable") = '1' limit 1 ;
17	new VM custom metadata value suspected to contain sensitive data	(json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" or json_payload.event_type="yandex.cloud.audit.compute.UpdateInstance") and json_payload.details.metadata_keys[0]: secret	event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.compute.UpdateInstance or yandex.cloud.audit.compute.CreateInstance) and details.metadata_keys: secret key password pass token oauth	-

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
			aws_access_key_id and event.outcome : success	
18	Creating a VM without SG	json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and not json_payload.details.network_interfaces.security_group_ids EXISTS	event.dataset: yandexcloud.audittrail and event.outcome : success and event.action: yandex.cloud.audit.compute.CreateInstance and not details.network_interfaces.security_group_ids: *	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.compute.CreateInstance' and JSON_EXISTS(data, "$.details.network_interfaces[0].security_group_ids") = False limit 4 ;
VPC				
19	Creating too wide (insecure) ACL Security Group	json_payload.event_type="yandex.cloud.audit.network.CreateSecurityGroup" or json_payload.event_type="yandex.cloud.audit.network.UpdateSecurityGroup" and json_payload.details.rules[0].direction="INGRESS" and json_payload.details.rules[0].cidr_blocks.v4_cidr_blocks[0]="0.0.0.0/0"	event.dataset: yandexcloud.audittrail and (event.action: yandex.cloud.audit.network.CreateSecurityGroup or yandex.cloud.audit.network.UpdateSecurityGroup) and details.rules.direction : INGRESS and details.rules.cidr_bloc	select * from bindings.`binding` where (JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.network.CreateSecurityGroup' or JSON_VALUE(data, "$.event_type") =

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
			ks.v4_cidr_blocks: *0.0.0.0*	'yandex.cloud.audit.network.UpdateSecurityGroup') and (JSON_VALUE(data, "$.details.rules[0].direction") = 'INGRESS' and JSON_VALUE(data, "$.details.rules[0].cidr_blocks.v4_cidr_blocks[0]") = '0.0.0.0/0') limit 1 ;
20	Creating a public address without a DDoS protection checkbox	json_payload.event_type="yandex.cloud.audit.network.CreateAddress" and not json_payload.details.external_ipv4_address.requirements.ddos_protection_provider exists	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.network.CreateAddress and not details.external_ipv4_address.requirements.ddos_protection_provider: qrator	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.network.CreateAddress' and JSON_EXISTS(data, "$.details.external_ipv4_address.requirements.ddos_protection_provider") = False limit 2

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
				;
21	new Creating / applying a security group by an account not from the list of allowed (requires values)	(json_payload.event_type="yandex.cloud.audit.network.CreateSecurityGroup" or json_payload.event_type="yandex.cloud.audit.network.UpdateSecurityGroup") and not json_payload.authentication.subject_name="mirtov8@yandex-team.ru"	event.dataset: yandexcloud.audittrail and (event.action: yandex.cloud.audit.network.CreateSecurityGroup or yandex.cloud.audit.network.UpdateSecurityGroup) and not user.name: mirtov8@yandex-team.ru kirill@yandex-team.ru	-
22	Any action with Security Group objects	json_payload.event_type="yandex.cloud.audit.network.CreateSecurityGroup" or json_payload.event_type="yandex.cloud.audit.network.UpdateSecurityGroup"	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.network.*SecurityGroup	select * from bindings.`binding` where (JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.network.CreateSecurityGroup' or JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.network.UpdateSecurityGroup') limit 5 ;

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
ObjectStorage(S3)				
23	Suspicious activities with S3 Bucket	json_payload.event_type="yandex.cloud.audit.storage.BucketAclUpdate" or json_payload.event_type="yandex.cloud.audit.storage.BucketPolicyUpdate"	event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.storage.BucketAclUpdate or yandex.cloud.audit.storage.BucketPolicyUpdate)	select * from bindings.`binding` where (JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.storage.BucketAclUpdate' or JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.storage.BucketPolicyUpdate') limit 5 ;
24	new Bucket become public	json_payload.event_type="yandex.cloud.audit.storage.BucketUpdate" and (json_payload.details.objects_access: "true" or json_payload.details.settings_read_access: "true" or json_payload.details.list_access: "true")	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.storage.BucketUpdate and (details.objects_access : true or details.settings_read_access: true or details.list_access: true)	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.storage.BucketUpdate' and (JSON_VALUE(data, "$.details.objects_acces

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
				s") = 'true' or JSON_VALUE(data, "$.details.settings_read_access") = 'true' or JSON_VALUE(data, "$.details.list_access") = 'true') limit 5 ;
25	new Object storage bucket (S3) became public when created/modified via ACL	json_payload.event_type="yandex.cloud.audit.storage.BucketAclUpdate" and json_payload.details.acl.grants.grant_type: "ALL_USERS"	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.storage.BucketAclUpdate and details.acl.grants.grant_type: "ALL_USERS"	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.storage.BucketUpdate' and JSON_VALUE(data, "$.details.acl.grants.grant_type") = 'ALL_USERS' limit 5 ;
Lockbox/KMS				
26	Triggered by changing access rights to KMS	json_payload.event_type="yandex.cloud.audit.kms.UpdateSymmetricKeyAccessBindings" or	event.dataset: yandexcloud.audittrail and event.action:	select * from bindings.`binding`

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
	symmetric encryption keys	json_payload.event_type="yandex.cloud.audit.kms.CreateSymmetricKeyAccessBindings"	yandex.cloud.audit.kms.*SymmetricKeyAccessBindings	where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.kms.UpdateSymmetricKeyAccessBindings' or JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.kms.CreateSymmetricKeyAccessBindings' limit 5 ;
27	Removing a KMS key	json_payload.event_type="yandex.cloud.audit.kms.DeleteSymmetricKey"	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.kms.DeleteSymmetricKey	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.kms.DeleteSymmetricKey' limit 5 ;
28	Assigning/Updating LockBox Secret Rights	json_payload.event_type="yandex.cloud.audit.lockbox.UpdateSecretAccessBindings"	event.dataset: yandexcloud.audittrail and event.action:	-

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
			yandex.cloud.audit.lockbox.UpdateSecretAccessBindings	
29	new Assigning a person with access to a lockbox service account secrets on the VM (requires values)	json_payload.event_type="yandex.cloud.audit.compute.UpdateInstance" and json_payload.details.service_account_id: "ajeg2ar8m8o25u63dj9f"	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.UpdateInstance and details.service_account_id: ajeg2ar8m8o25u63dj9f	-
30	new Reading a secret from Lockbox from an IP address different from the cloud address range (requires values)	json_payload.event_type="yandex.cloud.audit.lockbox.GetPayload" and not json_payload.request_metadata.remote_address:"51.250"….	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.lockbox.GetPayload and not source.ip: ("51.250.0.0/17" or "31.44.8.0/21" or "62.84.112.0/20" or "84.201.128.0/18" or "84.252.128.0/20" or "130.193.32.0/19" or "178.154.192.0/18" or "178.170.222.0/24" or "185.206.164.0/22" or	-

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
			"193.32.216.0/22" or "217.28.224.0/20")	
31	new Reading a secret from Lockbox using an account that is different from the target (requires values)	json_payload.event_type="yandex.cloud.audit.lockbox.GetPayload" and not json_payload.authentication.subject_id: "ajesnkfkc77lbh50isvg" and json_payload.details.secret_id= "e6q7q5msguqg22ji78e0"	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.lockbox.GetPayload and not user.id: ajeg2ar8m8o25u63dj9f and details.secret_name: secret1	-
MDB				
32	new Creating an MDB cluster by a cloud user not from the list of administrators (requires values)	json_payload.event_type: "yandex.cloud.audit.mdb." and not json_payload.authentication.subject_name: "test"	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.mdb.*.CreateCluster and not user.name : mirtov8@yandex-team.ru kirill@yandex-team.ru	-
33	new Creating/Changing an MDB User	json_payload.event_type: "CreateUser" or json_payload.event_type: "UpdateUser"	event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.mdb.*.UpdateUser or yandex.cloud.audit.mdb.*.CreateUser)	select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.mdb.

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
				`postgresql.CreateUser' or JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.mdb.postgresql.UpdateUser' limit 5 ;`
34	new Deleting an MDB Cluster	`json_payload.event_type: "DeleteCluster"`	`event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.mdb.*.DeleteCluster`	`select * from bindings.`binding` where JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.mdb.postgresql.DeleteCluster' or JSON_VALUE(data, "$.event_type") = 'yandex.cloud.audit.mdb.postgresql.UpdateUser' limit 5 ;`
35	new Administrative actions with MDB from ip	`(json_payload.event_type: "DeleteCluster" or json_payload.event_type: "CreateCluster") and not`	`event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.mdb.*.UpdateUser or`	-

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
	addresses that are different from the trusted range (requires values)	json_payload.request_metadata.remote_address: "51.250"	yandex.cloud.audit.mdb.*.CreateUser or yandex.cloud.audit.mdb.*.CreateCluster or yandex.cloud.audit.mdb.*.UpdateCluster) and source.ip : ("2a00:1fa0:474:9876:4cac:6c43:12aa:2bd2" or "2a00:1fa0:474:9876:4cac:6c43:12aa:2bd1")	
36	coming soon Enabling a dangerous setting when creating a cluster	-доступ из datalens -публичный доступ -доступ из консоли управления -доступ из serverless	---	
37	coming soon Enabling a dangerous setting when changing a cluster	-доступ из datalens -публичный доступ -доступ из консоли управления -доступ из serverless	---	
38	coming soon Not enabled / unchecked	--	---	

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
	"Protection from deletion" when creating/changing			
39	coming soon Changing settings affecting the collection of audit logs from MDB when creating / changing	-настройки log_statements and log_connections	---	
40	coming soon Issuing privileged GRANT mdb_admin to a user	---	---	
41	coming soon Creating/Modifying a Cluster without a Security Group Installed	---	---	

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
The following Use cases are not part of Audit Trails, but are native k8s audit logs, and currently they cannot be analyzed in CloudLogging				
Kubernetes (for k8s events, you need to set up a solution)				
General				
1	Access denied events - unauthorized	---	event.dataset : yandexcloud.k8s_audit_logs and responseStatus.reason : Forbidden and not user.name : (system*node* or *gatekeeper* or *kyverno* or *proxy* or *scheduler* or *anonymous* or *csi* or *controller*)	
2	Assigning a cluster-admin or admin role (clusterrolebinding or rolebinding)	---	event.dataset : yandexcloud.k8s_audit_logs and requestObject.roleRef.name.keyword:(cluster-admin or admin) and objectRef.resource.keyword:(clusterrolebindings or rolebindings) and verb : create and not responseObject.reason : AlreadyExists	
3	Successful connection to the cluster from	---	event.dataset : yandexcloud.k8s_audit_logs and source.ip : * and not responseStatus.status : Failure	

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
	an external IP address			
4	NetworkPolicies: create, delete, change	---	event.dataset : yandexcloud.k8s_audit_logs and requestObject.kind.keyword: (NetworkPolicy or CiliumNetworkPolicy or DeleteOptions) and verb : (create or update or delete) and objectRef.resource : networkpolicies	
5	Exec inside the container (shell inside the container)	---	event.dataset : yandexcloud.k8s_audit_logs and objectRef.subresource.keyword: exec	
6	Creating a pod with image NOT from Yandex container registry (not relevant for Clients using their own cr)	---	event.dataset : yandexcloud.k8s_audit_logs and not requestObject.status.containerStatuses.image.keyword: *cr.yandex/* and requestObject.status.containerStatuses.containerID : *docker* and verb : patch and not	

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
			requestObject.status.containerStatuses.image.keyword: (*falco* or *openpolicyagent* or *kyverno* or *k8s.gcr.io*)	
7	Create pod in kube-system namespace	---	event.dataset : yandexcloud.k8s_audit_logs and objectRef.namespace.keyword: kube-system and verb : create and objectRef.resource.keyword: pods and objectRef.name : * and not objectRef.name : (*calico* or *dns* or *npd* or *proxy* or *metrics* or *csi* or *masq*)	
8	Calling k8s-api under a service account from an external ip address	---	`event.dataset : yandexcloud.k8s_audit_logs and user.name : system\\\:serviceaccount\\\:* not source.ip: ("10.0.0.0/8" or " 172.16.0.0/12" or " 192.168.0.0/16"`	
Falco				
9	Any Alert from Falco	---	event.dataset : yandexcloud.k8s_falco and not objectRef.namespace: falco	
10	Falco removed	---	event.dataset : yandexcloud.k8s_audit_logs and	

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
			verb : delete and objectRef.namespace.keyword: falco and objectRef.resource.keyword : daemonsets	
OPA Gatekeeper				
11	OPA Gatekeeper triggered - denied events (only in enforce mode)	---	event.dataset : yandexcloud.k8s_audit_logs and responseObject.status.keyword: Failure and responseObject.message :" admission webhook \\\"validation.gatekeeper.sh\\\" denied the request" and not objectRef.namespace : falco and not user.name : system\\\:serviceaccount\\\:kube-system\\\:daemon-set-controller	
12	Removing a gatekeeper from a k8s cluster	---	event.dataset : yandexcloud.k8s_audit_logs and objectRef.name.keyword: gatekeeper-validating-webhook-configuration and verb : delete	

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
13	Modifying/deleting a Constraint object	---	event.dataset : yandexcloud.k8s_audit_logs and objectRef.apiGroup.keyword: constraints.gatekeeper.sh and (verb : delete or update) and not user.name : "system:serviceaccount:gatekeeper-system:gatekeeper-admin"	
Kyverno				
14	Kyverno triggered - denied events (only in enforce mode)	---	event.dataset : yandexcloud.k8s_audit_logs and responseObject.status.keyword: Failure and responseObject.message :" admission webhook \\\"validate.kyverno.svc\\\" denied the request" and not objectRef.namespace : falco and not user.name : system\\\:serviceaccount\\\:kube-system\\\:daemon-set-controller	
15	Removing Kyverno from the k8s cluster	---	event.dataset : yandexcloud.k8s_audit_logs and objectRef.name.keyword:	

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
			kyverno-resource-validating-webhook-cfg and verb : delete	
16	Changing/deleting a Kyverno Policy object	---	event.dataset : yandexcloud.k8s_audit_logs and objectRef.apiGroup.keyword: kyverno.io and (verb : delete or update) and objectRef.resource.keyword: *policies	
Kyverno-report				
17	Kyvenro triggered: fail status of policy result (Yandexcloud:k8s:kyverno-reporter-detect)	---	event.dataset : yandexcloud.k8s_kyverno and Status : fail	
External Secrets				
18	Changing / creating an external secrets object with an account other than ci / cd (this		event.dataset : yandexcloud.k8s_audit_logs and not user.name: "ajesnkfkc77lbh50isvg" and not user.name: "system:serviceaccount:external-	

№	Name	CloudLogging	Elasticsearch Opensearch	Yandex Query (S3 or YDS)
	object goes to the lockbox and copies the secret from there)		secrets:external-secrets" and objectRef.name: "external-secret" and verb: (patch or create)	
19	Read secrets under user account		event.dataset : yandexcloud.k8s_audit_logs and objectRef.resource: "secrets" and verb: "get" and not user.name: ("system:serviceaccount:external-secrets:external-secrets" or "system:serviceaccount:kube-system:hubble-generate-certs" or "system:serviceaccount:kyverno:kyverno")	