Searches & Use Cases

№	Название	Сырой запрос из json файла	Входные паараметры
Searches			
1	Найти, кто удалил фолдер	find <<директория>> -type f -exec cat {} \; | jq '.[] | select(.event_type == "yandex.cloud.audit.resourcemanager.DeleteFolder" and .details.folder_id == "<<идентификатор фолдера>>") | .authentication'	<<идентификатор фолдера>>
2	Найти, кто создал/остановил/перезапустил/удалил виртуальную машину	find <<директория>> -type f -exec cat {} \; | jq '.[] | select((.event_type | test("yandex\\.cloud\\.audit\\.compute\\..*Instance")) and .details.instance_id == "<<идентификатор виртуальной машины>>") | .authentication'	<<идентификатор виртуальной машины>>
3	Какие действия совершал конкретный пользователь за период времени	find <<директория>> -type f -exec cat {} \; | jq '.[] | select(.authentication.subject_id == "<<идентификатор_пользователя>>" and .event_time > "2021-03-01" and .event_time < "2021-04-01")' find <<директория>> -type f -exec cat {} \; | jq '.[] | select(.authentication.subject_name == "<<имя_пользователя>>" and .event_time > "2021-03-01" and .event_time < "2021-04-01")'	<<идентификатор_пользователя>> <<имя_пользователя>>
4	Поиск событий по объектам определенного фолдера	find <<директория>> -type f -exec cat {} \; | jq '.[] | select(.resource_metadata != null and .resource_metadata.path != null) | select(.resource_metadata.path[] | .resource_type == "resource-manager.folder" and .resource_id == "<<идентификатор фолдера>>")'	<<идентификатор фолдера>> <<имя фолдера>>

		find <<директория>> -type f -exec cat {} \; | jq '.[] | select(.resource_metadata != null and .resource_metadata.path != null) | select(.resource_metadata.path[] | .resource_type == "resource-manager.folder" and .resource_name == "<<имя фолдера>>")'	
Use cases AuditTrails			
1	Срабатывание при создании credentials сервисных аккаунтов	find ./ -type f -exec cat {} ; | jq '.[] | select(.event_type == "yandex.cloud.audit.iam.CreateAccessKey" or .event_type == "yandex.cloud.audit.iam.CreateKey" or .event_type == "yandex.cloud.audit.iam.CreateApiKey") '	
6	Срабатывание на событие с созданием машины с белыми IP адресами	find ./ -type f -exec cat {} ; | jq '.[] | select(.event_type == "yandex.cloud.audit.compute.CreateInstance" and .event_type != null and .details.network_interfaces != null and .details != null) | select(.details.network_interfaces[] | .primary_v4_address.one_to_one_nat.ip_version == "IPV4" or .primary_v4_address.one_to_one_nat.ip_version == "IPV6")'	
7	Срабатывание на создания "двуногих" виртуальных машин (с белыми IPv4-адресами и IPv6-адресами) - сценарий внутренних сервисов	find ./ -type f -exec cat {} ; | jq '.[] | select(.event_type == "yandex.cloud.audit.compute.CreateInstance" and .event_type != null and .details.network_interfaces != null and .details != null and .details.network_interfaces[1] != null) | select(.details.network_interfaces[] | .primary_v4_address.one_to_one_nat.ip_version == "IPV4" or .primary_v4_address.one_to_one_nat.ip_version == "IPV6")'	
8	Срабатывание на любое действие под	.authentication.subject_id == "<<идентификатор_пользователя>>" '	<<идентификатор_пользователя>>

	привелигированным account с ролью “resource-manager.clouds.owner”	.authentication.subject_name == "<<имя_пользователя>>"’	<<имя_пользователя>>
9	Аномальное кол-во попыток неуспешной авторизации (!!требует корреляции!!).	. authorization. Authorized == “false” > 5	
10	Создание слишком широкого (небезопасного) ACL Security Group для ipv4, tcp	.event_type == “yandex.cloud.audit.network.CreateSecurityGroup” or .event_type == “yandex.cloud.audit.network.UpdateSecurityGroup” & .details.rules[].direction == “INGRESS” & .details.rules[].cidr_blocks.v4_cidr_blocks[] == “0.0.0.0/0” & .details.rules[].protocol_name == “TCP”	
11	Отслеживание загрузки image с подозрительным названием в облако (!!требует корреляции!!)	.event_type == “yandex.cloud.audit.compute.CreateImage” & .details. image_name IN list_of_suspicious_image_names *При этом list_of_suspicious_image_names лист содержит распространенные значения имен подозрительных image	

12	Загрузка image в облако не из разрешенного S3 Bucket (!!требует корреляции!!)	.event_type == “yandex.cloud.audit.compute.CreateImage” & .details. source_uri NOT IN list_of_approoved_image_sources *При этом list_of_approoved_image_sources лист содержит значение разрешенных источников загрузки Images (разрешенные url S3 bucket)	
13	Подозрительные дейсвия с хранилищем логов AuditTrails (S3 Bucket)	.event_type == “yandex.cloud.audit.storage.BucketAclUpdate” Or .event_type == “yandex.cloud.audit.storage.BucketPolicyUpdate” Or .event_type == “yandex.cloud.audit.storage. BucketDelete” Or .event_type == “yandex.cloud.audit.storage. BucketUpdate” Or .event_type == “yandex.cloud.audit.storage.ObjectDelete” & .details.bucket_id == “<ID вашего Bucket>”	<<ID вашего Bucket>>
14	Назначение привелигированных прав доступа сервисному аккаунту на Folder. Роль admin.	.event_type == “yandex.cloud.audit.resourcemanager.UpdateFolderAccessBindings” & .details. access_binding_deltas[]. access_binding. role_id == “admin” & .details. access_binding. subject_type == “SERVICE_ACCOUNT”	
15	Назначение привелигированных прав доступа любому аккаунту на folder, cloud – admin, editor и др.		

16	Срабатывание на изменение прав доступа на симметричные ключи шифрования KMS	.event_type == “yandex.cloud.audit. kms. UpdateSymmetricKeyAccessBindings”	
17	Создание ВМ с image_id из Marketplace	.event_type == “yandex.cloud.audit.compute.CreateInstance” & .product_ids != null (впринципе существует)	
18	Добавление публичного IP-адреса существующей виртуальной машине	.event_type == “yandex.cloud.audit.compute.AddInstanceOneToOneNat”	
19	Назначение роли vpc.public.admin		
20	Обращение к API с помощью YC или terraform под подозрительным пользователем или ip	$(request_metadata. user_agent) = YC* or Terraform*	
21	Создание публичного адреса без галочки защиты от ддос	• "requirements" : -{ ○ "ddos_protection_provider" : qrator • }	
22	События создания ВМ с включенным серийным портом		
23	Бакет стал публичным при изменении объекта		

24	Бакет стал публичным при создании	Тикет https://st.yandex-team.ru/MDS-15776	
25	В федерацию добавили новый сертификат		
26	Изменили настройки федерации		
27	Удаление ключа KMS		
28	Назначение/Обновление прав на секрет LockBox	SetSecretAccessBindings/ UpdateSecretAccessBindings	
Use cases kubernetes			
Общие			
1	События отказа в доступе - 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	Назначение cluster-admin или admin роли (clusterrolebinding или 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	Успешное подключение к кластеру с внешнего IP адреса	event.dataset : yandexcloud.k8s_audit_logs and source.ip : * and not responseStatus.status : Failure	
4	NetworkPolicies: создание, удаление, изменение	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 внутрь контейнера (шелл внутрь контейнера)	event.dataset : yandexcloud.k8s_audit_logs and objectRef.subresource.keyword: exec	
	Создание pod с image НЕ из Yandex container registry (не актуально для Клиентов использующих собственный 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 requestObject.status.containerStatuses.image.keyword: (*falco* or *openpolicyagent* or *kyverno* or *k8s.gcr.io*)	
	Создание pod в 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*)	
Falco			
6	Любой Alert от Falco	event.dataset : yandexcloud.k8s_falco and not objectRef.namespace: falco	
7	Falco удален	event.dataset : yandexcloud.k8s_audit_logs and verb : delete and objectRef.namespace.keyword: falco and objectRef.resource.keyword : daemonsets	
OPA Gatekeeper			
8	Срабатывание OPA Gatekeeper – denied events (только в режиме enforce)	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	
9	Удаление Gatekeeper из кластера k8s	event.dataset : yandexcloud.k8s_audit_logs and objectRef.name.keyword: gatekeeper-validating-webhook-configuration and verb : delete	

10	Изменение/удаление объекта Constraint	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			
11	Срабатывание Kyverno – denied events (только в режиме enforce)	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	
	Удаление Kyverno из кластера k8s	event.dataset : yandexcloud.k8s_audit_logs and objectRef.name.keyword: kyverno-resource-validating-webhook-cfg and verb : delete	
	Изменение/удаление объекта Kyverno Policy	event.dataset : yandexcloud.k8s_audit_logs and objectRef.apiGroup.keyword: kyverno.io and (verb : delete or update) and objectRef.resource.keyword: *policies	