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			
1	создание, изменение, удаление объекта Constraint	{"kind":"Event","apiVersion":"audit.k8s.io/v1","level":"RequestResponse","auditID":"c8ffdc9f-7231-4919-9d5b-32fb95458f84","stage":"RequestReceived","requestURI":"/apis/constraints.gatekeeper.sh/v1beta1/k8spspallowprivilegeescalationcontainer/psp-allow-privilege-escalation-container","verb":"delete","user":{"username":"kubernetes-admin","groups":["system:masters","system:authenticated"]},"sourceIPs":["10.129.0.19"],"userAgent":"kubectl/v1.21.0 (linux/amd64) kubernetes/cb303e6","objectRef":{"resource":"k8spspallowprivilegeescalationcontainer","name":"psp-allow-privilege-escalation-container","apiGroup":"constraints.gatekeeper.sh","apiVersion":"v1beta1"},"requestReceivedTimestamp":"2021-06-15T12:13:35.411422Z","stageTimestamp":"2021-06-15T12:13:35.411422Z"}	
2	установка и удаление Gatekeeper. Предлагается отслеживать по событиям:	{"kind":"Event","apiVersion":"audit.k8s.io/v1","level":"RequestResponse","auditID":"6a0f117b-4ddd-4229-bcd8-eb79ba411bc4","stage":"RequestReceived","requestURI":"/apis/admission	

	создание или удаление объекта «validatingwebhookconfigurations/gatekeeper-validating-webhook-configuration» (пример события внизу)	registration.k8s.io/v1beta1/validatingwebhookconfigurations/gatekeeper-validating-webhook-configuration","verb":"delete","user":{"username":"kubernetes-admin","groups":["system:masters","system:authenticated"]},"sourceIPs":["10.129.0.19"],"userAgent":"kubectl/v1.21.0 (linux/amd64) kubernetes/cb303e6","objectRef":{"resource":"validatingwebhookconfigurations","name":"gatekeeper-validating-webhook-configuration","apiGroup":"admissionregistration.k8s.io","apiVersion":"v1beta1"},"requestReceivedTimestamp":"2021-06-15T12:16:34.162990Z","stageTimestamp":"2021-06-15T12:16:34.162990Z"}	
3	-дополнительно можно/полезно отслеживать срабатывания по Constraint – когда Admission Controller Gatekeeper запрещал или разрешал действие		
4	Нехарактерное подключение с конфигом кластера (например, с IP-адреса, который находится в иной стране).	{"kind":"Event","apiVersion":"audit.k8s.io/v1","level":"RequestResponse","auditID":"6a0f117b-4ddd-4229-bcd8-eb79ba411bc4","stage":"ResponseComplete","requestURI":"/apis/admissionregistration.k8s.io/v1beta1/validatingwebhookconfigurations/gatekeeper-validating-webhook-configuration","verb":"delete","user":{"username":"kubernetes-admin","groups":["system:masters","system:authenticated"]},"sourceIPs":["10.129.0.19"],"userAgent":"kubectl/……	
5	Использовать аудит события, например по созданию, удалению, изменению	{"kind":"Event","apiVersion":"audit.k8s.io/v1","level":"RequestResponse","auditID":"2386ad9c-dbe7-4122-8769-85b462592239","stage":"ResponseComplete","requestURI":"/apis/networking.k8s.io/v1/namespaces/default/networkpolicies?fieldManager=kubectl-client-side-apply","verb":"create","user":{"username":"kubernetes-	

	объектов networkpolicies. Пример:	admin","groups":["system:masters","system:authenticated"]},"sourceIPs":["10.129.0.19"],"userAgent":"kubectl/v1.21.0 (linux/amd64) kubernetes/cb303e6","objectRef":{"resource":"networkpolicies","namespace":"default","name":"test-network-policy","apiGroup":"networking.k8s.io","apiVersion":"v1"},"responseStatus":{"metadata":{},"code":201},"requestObject":{"kind":"NetworkPolicy","apiVersion":"networking.k8s.io/v1","metadata":{"name":"test-network-policy","namespace":"default","creationTimestamp":null,"annotations":{"kubectl.kubernetes.io/last-applied-conf	
6	выполнение pods/exec, pods/portforward, pods/proxy, services/proxy, verb в контейнер	request, response по Secrets, ConfigMaps, and TokenReviews	
7	модификация pod, deployments		
8	edit ресурсов: network policy, RBAC policy		
9	новая привелигированная роль		
10	создание нового service, который наружу		
11	большое кол-во отрицательных попыток доступа к ресурсам		
12	Срабатывание OPA Gatekeeper		